Version June 2022

SDG Once-Only Collaborative Space

Exported on Jun 27, 2022

Contents

1 Chapter 1: Introduction - High Level Architecture - June 2022 10
1.1 Introduction - High Level Architecture - Q2 2022 10
1.2 Once-Only Technical System High Level Architecture - June 2022 11
1.2.1 Introduction 19
1.2.2 Requirements 21
1.2.3 Once-Only Technical System Architecture 31
1.2.4 Evidence Requester Architecture Elements 35
1.2.5 Evidence Provider Architecture Elements 39
1.2.6 Once-Only Common Services 42
1.2.7 Evidence Exchange and eDelivery 47
1.2.8 Identification and Authentication 56
1.2.9 System Operation 59
1.2.10 Sample Once-Only Flows 59

2 Chapter 2: User Identification, Authentication and Record Matching - June 2022 67
2.1 Identity and Record Matching - June 2022 68
2.1.1 Introduction 68
2.1.2 Use of eIDAS 68
2.1.3 eIDAS optional and sector/additional specific attributes for Natural Person 72
2.1.4 Authentication and re-authentication 75
2.1.5 Sample attribute collection and evidence exchange flow 76
2.1.6 Examples Unique Identifier and Data Service identity matching (Informative) 78
2.2 OOTS eID additional security services - June 2022 88
2.2.1 Introduction 88
2.2.2 Authentication verification 89
2.2.3 Authorization of requests for evidence relating to represented persons 90
2.3 Representation - June 2022 91

3 Chapter 3: Common Services - June 2022 92
3.1 Data Service Directory (DSD) - June 2022 93
3.1.1 Overview 93
3.1.2 Functionality 94
3.1.3 Information Data Model 94
3.1.4 Query Interface Specification 100
3.1.5 LCM Interface Specification 148
3.2 Evidence Broker (EB) - June 2022 158
3.2.1 Overview 158
3.2.2 Information Model 159

3.2.3 Criterion to Evidence Type Mapping Mechanism 161
3.2.4 Query Interface Specification 161
3.2.5 LCM Interface Specification 185
3.3 Semantic Repository (SR) - June 2022 189
3.3.1 Overview 190
3.3.2 High-level structure of the semantic repository 190
3.4 Common Services Distribution - June 2022 191
3.4.1 Introduction 191
3.4.2 Common Services Configuration 192
3.4.3 Discovery of Common Services 192
3.4.4 Proxy Caching 194
3.4.5 References 194
3.5 Code Lists - June 2022 194
3.5.1 Code lists used by the OOTS Exchange Data Models 194
3.6 Common Services API Specification - June 2022 196
3.6.1 Introduction 196
3.6.2 Query Interface Specification 196
3.6.3 The Lifecycle Management Specification 198

4 Chapter 4: Evidence Exchange - June 2022 205
4.1 Introduction to Exchange Data Model and Protocol - June 2022 205
4.2 Scope and Goals - June 2022 207
4.2.1 Scope & Goals 207
4.2.2 Architecture Requirements 208
4.3 Business Requirements - June 2022 209
4.3.1 Evidence Request Business Requirements 209
4.3.2 Evidence Response Business Requirements 212
4.3.3 Error Response Business Requirements 213
4.4 Query Model - June 2022 214
4.4.1 Overview 214
4.4.2 Common Query Attributes 215
4.4.3 Document Query 216
4.5 Syntax Mapping - June 2022 219
4.5.1 Overview 219
4.5.2 Evidence Request Syntax Mapping - June 2022 219
4.5.3 Evidence Response Syntax Mapping - June 2022 267
4.5.4 Evidence Error Response Syntax Mapping - June 2022 292
4.5.5 OOTS-EDM XML Examples of the Evidence Exchange- June 2022 308
4.6 Business Rules - June 2022 335
4.7 eDelivery Configuration - June 2022 385

4.7.1 Four Corner Topology in OOTS 385
4.7.2 Routing Metadata 386
4.7.3 Access Point Interconnectivity 389
4.8 Evidence Exchange Logging - June 2022 390
4.8.1 Introduction 390
4.8.2 Objectives 390
4.8.3 Log data correlation 391
4.8.4 Message Acknowledgment, Error or Fault 394
4.8.5 Non-Repudiation 394
4.8.6 Log System Security and Privacy 395
4.8.7 Log System Interchange Format (Informative) 396
4.9 Evidence Preview - June 2022 396
4.9.1 Introduction 396
4.9.2 Evidence Preview Service Flow 397
4.9.3 Coordination of Evidence Preview Service and Data Service 402
4.9.4 Preview Location Metadata 402
4.9.5 Coordination of Evidence Preview Service and Online Procedure Portal 403
4.9.6 Multiple Evidence Requests (Informative) 404

5 Chapter 5: Data Models - June 2022 405
5.1 Methodology for Data Model Development - June 2022 406
5.1.1 Methodology 406
5.1.2 Phase 1: Identify and analyse existing standardisation efforts, evidences and data models 409
5.1.3 Phase 2: Draft data model 414
5.1.4 Phase 3: Select controlled vocabularies 422
5.1.5 Phase 4: Review data model and incorporate comments 426
5.1.6 Phase 5: Finalise data model 435
5.1.7 Phase 6: Create distributions and publish documentation 442
5.1.8 Quality 445
5.1.9 Review cycles and consensus 445
5.1.10 Stakeholders 446
5.1.11 Terminologies 448
5.2 Education Domain - June 2022 449
5.2.1 Education Domain OOTS Data Models - June 2022 450
5.2.2 Education Domain Code Lists - June 2022 481
5.3 Vehicle Domain - June 2022 483
5.3.1 Vehicle Domain Data Models - June 2022 484
5.3.2 Vehicle Domain Code Lists - June 2022 493
5.3.3 EUCARIS 494
5.4 Public Documents - June 2022 495

5.4.1 Public Documents Data Models - June 2022 496
5.4.2 Public Documents Code Lists - June 2022 512

6 Chapter 6: OOTS Guidance & UX Recommendations - June 2022 514
6.1 Summary 514
6.2 OOTS Guidance document 514
6.3 OOTS UX Recommendations 514
6.3.1 Get involved 515
6.3.2 discover OOTS 516
6.3.3 authenticate 518
6.3.4 locate evidence 520
6.3.5 request evidence 521
6.3.6 redirect 523
6.3.7 Preview 524
6.3.8 evidence response 525
6.3.9 submit 526

Change log

The following table lists changes made to the technical design documents after the Q1 2022 release, based on:

- Update of the draft Implementing Act. This version of the technical design documents is aligned with the version released for vote by the Member States in June 2002.
- Feedback on the previous release provided by some Member States.
- Feedback and other requests from the team developing the OOTS test service.
- Many other improvements from close scrutiny of the existing text by the editors.

Description	Area / Change	Comments	Location (Chapter, Section)
General	Editorial	Improved naming and spelling consistency for some OOTS terms.	1
		References for eID and eDelivery updated from former CEF to DEP and for Interoperable Europe from the completed ISA² action.	1
HLA	Misc. maintenance	Removed Wallet references	1
		Updated diagram to align with eID chapter updates, removed features.	1.10
		Updated figure 1, decoupled Preview Service and eIDAS Node via Identification Service	1.3.3
		Updated Acronyms section	1
	Consistency	Cross-references to Implementing Act adapted for current version	1
	Consistency	Aligned section on Intermediary Platform with Implementing Act (MS comment)	1.7.7
Identification and authentication	OOTS attributes and type of person	Updated text and diagrams for removal of DSD OOTS attributes (user-supplied user identity attributes).	1.8, 2, 2.1, 2.1.5, 3.1, 3.2.
		Clarified that only mandatory attributes of the MDS of (natural and/or legal) person are included in the request, with the possible exception of the unique identifier.	1.4.1, 2., 2.1.2.1, 2.1.2.2, 2.1.2.3, 2.1.2.5, 2.1.4.1

		Clarified that optional and sector/additional specific attributes for Natural Person may be requested but are not included in the request.	2.1.2.4
		Removed the ability of DSD to express the eIDAS type of person that can request evidence.	1.2, 1.6.3, 3.1
		Added a new short description of representative minimum data set for eIDAS attributes for Natural Person representing Legal Person.	2.1.2.6
		In authentication section, removed reference to Wallet and clarified which attributes are used in the request.	2.1.4.1
		In re-authentication section, clarified the attributes to be matched and the handling of the unique identifier (if present).	2.1.4.2
		Moved the examples from the 2.1.2.3. in a separate section labelled as Informative.	2.1.6
Common Services	Syntax & Semantics	Updated models , reviewed cardinalities, major increase in detail on documentation of Evidence Broker and Data Service Directory	3.1, 3.2
		Aligned all snippets with latest version of XSD	3.1, 3.2
		Code lists updated, aligned with content of other chapters	3.5
Common Service - LCM	LCM	Defined use of eDelivery and its profiling	3.6.3.4
Evidence Exchange	Facilitate detection of related requests for preview	Extend eDelivery profiling of conversation identifier to cover multiple requests, so they can be correlated.	4.7.2.5
		Explain how Data Service and Preview Space can use the conversation identifier to detect requests relating to a single session. (MS review comment).	4.9.6
	Ordering of Preview Space and Data Service processing	Explained that there is no timing dependency between transmission of the second evidence request and the user redirection.	4.9.2

Evidence Exchange	Syntax & Semantics	Major increase in detail on documentation of evidence exchange messages	4.5
		Updated the introductory sections	4.1 4.2 4.3
		Aligned all snippets with latest version of XSD	4.5
		Business rules update, aligned with content of other chapters	4.6
		Rewrite of EDM example section	4.5.4
Evidence Exchange	Logging	Added logging of preview location	4.8
UX Guidance	Documentation	UX Guidance included	6
Various related artifacts	Schemas	SDG XSD updated to reflect changes to the models.	OOTS GIT repository
		A driver XSD created to allow validation of messages containing RegRep and SDG structures (test service team request).	OOTS GIT repository
		Schematron rules created for Slot cardinality and data types (test service team request).	OOTS GIT repository
	Examples	Examples updated to reflect the above (test service team request).	OOTS GIT repository

1 Chapter 1: Introduction - High Level Architecture - June 2022

1.1 Introduction - High Level Architecture - June 2022

Summary
This chapter provides a high level overview of the architecture of the Once-Only Technical System (OOTS) of the Single Digital Gateway (SDG) and serves as an introduction to all technical design documents.
The overview starts by stating the requirements that the technical system addresses. It then introduces and defines all architectural elements. These elements include elements located with evidence requesters and evidence providers and some common services that support them. Following this, the way evidences are exchanged using eDelivery, the use of identification and authentication, and the role of the log system are explained. Finally, some sample flows illustrating the functionality of the system are provided.
Together, this document and the other technical design documents and the interface specifications they describe complement and provide additional technical detail to the OOTS Implementing Act.
Please find the content of the chapter, including sub-chapters, by clicking on the link below:

- Once-Only Technical System High Level Architecture

Change log
For this release, the changes for all chapters are combined at the top level.

1.2 Once-Only Technical System High Level Architecture - June 2022

Single Digital Gateway (SDG) High Level Architecture Version 1.00

- Purpose of the document
- Acronyms
- References
- 1. Introduction
  - 1.1. Once-Only Technical System
  - 1.2. Context
  - 1.3. Input
  - 1.4. Scope
  - 1.5. Extensibility
  - 1.6 Structure of this document
- 2. Requirements
- 3. Once-Only Technical System Architecture
  - 3.1. Context
  - 3.2. Approach
  - 3.3. Overview
  - 3.4. Core and Extension Architectural Elements
  - 3.5. Governance
  - 3.6. Roles and Responsibilities
- 4. Evidence Requester Architecture Elements
  - 4.1. Introduction
  - 4.2. Online Procedure Portal
  - 4.3. Online Procedure Portal Access Point
  - 4.4. eIDAS Node of Evidence Requesting Member State
- 5. Evidence Provider Architecture Elements
  - 5.1. Introduction
  - 5.2. Data Service
  - 5.3. Preview Space

    - 5.4. Data Service Access Point
    - 5.5. eIDAS Node of Evidence Issuing Member State
- 6. Once-Only Common Services
    - 6.1. Introduction
    - 6.2. Evidence Broker
    - 6.3. Data Service Directory
    - 6.4. Semantic Repository
    - 6.5. Life Cycle Management
    - 6.6. Deployment Options
- 7. Evidence Exchange and eDelivery
    - 7.1. Introduction
    - 7.3. Evidence Request Response
    - 7.4. eDelivery
    - 7.5. Configuration of eDelivery
    - 7.6. Use in complex scenarios
    - 7.7. Intermediary Platform
    - 7.8 Evidence Exchange Logging
    - 7.9 Evidence Exchange integration in Member States
- 8. Identification and Authentication
    - 8.1. Introduction
    - 8.2. eIDAS Node
    - 8.3. Identification and authentication
    - 8.4 Identity Matching
    - 8.6. Representation
    - 8.7. Additional OOTS eID security services
- 9. System Operation
    - 9.1 Introduction
    - 9.2 Log System
- 10. Sample Once-Only Flows
    - 10.1. Sample Flow

Purpose of the document
The following table summarises the objectives, target audience and main outputs of this document:

Objective(s)	• Introduce and position the Once-Only Technical System in the context of the SDG Regulation and OOTS Implementing Act. • Provide a high-level overview of the main components in the system and the functionality they provide. • Provide a description of the evidence exchange process.
Audience	• Member State representatives in SDG Coordination Group and other designated experts. • Participants in Once-Only Large-Scale Pilots. • European Commission DG CNECT and GROW policy units in the area of the "once-only" principle (OOP) and of the Single Digital Gateway (SDG). • European Commission Digital Building Blocks team.
Output	• Functional description of components in Once-Only Technical System. • Identification of roles and responsibilities of the European Commission and the Member States in Once-Only. • Sample OOP flows.

Acronyms

Acronym	Description
AP	Access Point
AS4	Applicability Statement 4
CEF	Connecting Europe Facility
CBV	Core Business Vocabulary
CCCEV	Core Criterion and Core Evidence Vocabulary
CPV	Core Person Vocabulary
DCAT	Data Catalog Vocabulary

DSM	Digital Single Market
DE4A	Digital Europe for All
DS	Data Service
DSD	Data Service Directory
EB	Evidence Broker
EBMS3	OASIS ebXML Messaging Services 3 Version 3.0
EC	European Commission
EDM	Exchange Data Model
eID	Electronic Identification
eIDAS	Electronic Identification, Authentication and Trust Services
EIF	European Interoperability Framework
EP	Evidence Provider
ER	Evidence Requester
Eucaris	EUropean CAR and driving licence Information System
HLA	High Level Architecture
ISA²	Interoperability solutions for public administrations, businesses and citizens
ISO	International Organization for Standardization
LSP	Large Scale Pilot
LOA	Level of Assurance
MDS	Minimum Data Set

MS	Member State
OASIS	Organization for the Advancement of Structured Information Standards
OOP	Once-Only Principle
OOTS	Once-Only Technical System
OPP	Online Procedure Portal
SDG	Single Digital Gateway
SR	Semantic Repository
TOOP	The Once-Only Principle Project
URI	Uniform Resource Identifier
URL	Uniform Resource Locator

References

Ref.	Document	Content outline
[REF1]	ebXML Messaging Protocol Binding for RegRep Version 1.0	The OASIS ebXML Messaging Protocol Binding for RegRep Version 1.0 specifies a messaging protocol binding for the Registry Services of the OASIS ebXML RegRep Version 4.0 OASIS Standard. This binding is compatible with both the versions 2.0 and 3.0 of ebMS as well as the AS4 profile and complements the existing protocol bindings specified in OASIS RegRep Version 4.0. It is compatible with eDelivery AS4 [REF13].
[REF2]	Breg-DCAT-AP	A draft of registry of registries (RoR) specification, definition of the main aspects and elements to be served for the creation of potential Registry of Registries at the European level in the future. The specification elaborates the Registry of Registries specification, namely BRegDCAT-AP, an extension of the DCAT application profile for data portals in Europe (DCAT-AP), aiming to facilitate MS work on creating their own Registry of Registries.
[REF3]	Digital Europe	Digital Europe including the eID and eDelivery Building Blocks.
[REF7]	DE4A	Digital Europe for All (DE4A) Large Scale Pilot

[REF8]	3.1 - Data Service Directory (DSD) - June 2022	Data Service Directory design documentation
[REF9]	3.2 - Evidence Broker (EB) - June 2022	Evidence Broker design documentation
[REF10]	EDCI Data Model	The European Commission is developing the Europass Digital Credentials Infrastructure (EDCI) – a set of tools, services and software to support the issuance of authentic, tamper-proof digital credentials (such as qualifications and other learning achievements) across Europe. The EDCI is being developed as part of ongoing work to implement the new Europass Framework for supporting transparency of skills and qualifications in Europe.
[REF11]	eDelivery	eDelivery is a building block that provides technical specifications and standards, software and ancillary services to allow projects to create a network of nodes for secure digital data exchange. By building with eDelivery, public and private organisations from different sectors can easily create a safe and interoperable channel to transfer documents and data among each other over a public or private network.
[REF12]	eDelivery Access Point	The eDelivery Access Point (AP) implements a standardized message exchange protocol that ensures interoperable, secure and reliable data exchange. An eDelivery AP is an implementation of the eDelivery AS4 Profile.
[REF13]	eDelivery AS4	eDelivery AS4 Specification, profiling the ISO 15000 international standards ebMS3 [REF26] and AS4 [REF25].
[REF14]	eDelivery Security Controls	The Digital Europe 'Security Controls' guidance document addresses the security controls and recommendations applicable to Digital Europe's eDelivery's message exchange Use Case. As the message exchange Use Case is closely linked to the Electronic Registered Delivery Service (ERDS), a trust service under the eIDAS regulation, this document maps the Qualified ERDS (QERDS) requirements to the security controls of eDelivery.
[REF15]	eGovernment Action Plan 2016-2020	COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS EU eGovernment Action Plan 2016-2020 Accelerating the digital transformation of government COM/2016/0179 final.
[REF16]	eIDAS Regulation	REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[REF17]	eID Homepage	eID is a set of services provided by the European Commission to enable the mutual recognition of national electronic identification schemes (eID) across borders. It allows European citizens to use their national eIDs when accessing online services from other European countries.
[REF18]	Enterprise Integration Patterns	A pattern language consisting of 65 integration patterns to establish a technology-independent vocabulary and a visual notation to design and document integration solutions.
[REF19]	European Interoperability Framework	The European Interoperability Framework (EIF) is part of the Communication (COM(2017)134) from the European Commission adopted on 23 March 2017. The framework gives specific guidance on how to set up interoperable digital public services.
[REF20]	Chapter 4: Evidence Exchange - June 2022	Draft design document describing use of open technical specifications and ISA vocabularies for evidence requests and responses.
[REF21]	General Data Protection Regulation	REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
[REF22]	IMI	Internal Market Information system (IMI).
[REF23]	Interoperable Europe	Interoperable Europe. Interoperability solutions for public administrations, businesses and citizens. (Success for ISA²).
[REF24]	eGovernment Core Vocabularies	The e-Government Core Vocabularies are simplified, re-usable and extensible data models that capture the fundamental characteristics of a data entity in a context-neutral fashion.
[REF25]	ISO 15000-2:2021	ISO 15000-2:2021. Electronic business eXtensible Markup Language (ebXML) — Part 2: Applicability Statement (AS) profile of ebXML messaging service
[REF26]	ISO 15000-1:2021	ISO 15000-1:2021. Electronic business eXtensible Markup Language (ebXML) — Part 1: Messaging service core specification
[REF27]	OASIS ebXML registry and repository version 4.0	Electronic business eXtensible Markup Language (ebXML). Registry and repository. Under submission to ISO TC 154 for inclusion in the ISO 15000 series of International Standards as ISO 15000-3.
[REF28]	3.3 - Semantic Repository (SR) - June 2022	OOP Semantic Repository design documentation

[REF29]	SEMIC	Semantic Interoperability Community (SEMIC).
[REF30]	Single Digital Gateway Regulation	Regulation (EU) 2018/1724 of the European Parliament and of the Council of 2 October 2018 establishing a single digital gateway to provide access to information, to procedures and to assistance and problem-solving services and amending Regulation (EU) No 1024/2012 (Text with EEA relevance.).
[REF31]	Single Digital Gateway Coordination Group	The Single Digital Gateway Coordination Group is based on the SDG Regulation [REF30]. The coordination group will have approximately 6 meetings per year and has a high need of exchange of information and content in between.
[REF32]	Single Digital Gateway Regulation Implementation Guidelines	Guidelines for the implementation of the single digital gateway Regulation 2019-2020 work programme. Commission notice. (2019/C 257/01).
[REF33]	TOGAF	TOGAF Standard, a specification of The Open Group, is a proven Enterprise Architecture methodology and framework used by the world's leading organizations to improve business efficiency.
[REF34]	TOOP	The Once-Only Principle Project (TOOP) is a Large Scale Pilot (LSP) that was launched by the European Commission in January 2017 as an initiative of about 51 organisations from 21 EU Member States and Associated Countries.
[REF35]	TOOP D23	The Once-Only Principle Project (TOOP) Generic Federated OOP Architecture (3rd version).
[REF36]	ISO 25010	ISO/IEC 25010:2011. Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — System and software quality models
[REF37]	Archive: UX Guidance	Once-Only User Experience.
[REF38]	OOTS Implementing Act	Draft Commission Implementing Regulation EU ... XXX on the technical and operational specifications of the technical system for the cross-border exchange of evidence and application of the "once-only" principle in accordance with Regulation (EU) 2018/1724 of the European Parliament and of the Council. LAST VERSION: version0206_1415315304 Ares(2022)4144391 02 June 2022. NOTE: references to this draft will be replaced by the references to the IR once it is adopted by the Commission and published in the Official Journal.
[REF39]	SIP	Barros, Alistair P. and Dumas, Marlon and ter Hofstede, Arthur H.M. (2005) Service Interaction Patterns. In Proceedings 3rd International Conference on Business Process Management, pages pp. 302-318, Nancy, France.

[REF40]	CCCEV	Core Criterion and Core Evidence Vocabulary (CCCEV) - Version 2.00.
[REF41]	3.4 - Common Services Distribution - June 2022	Hybrid Deployment Model of the OOTS Common Services.

1.2.1 Introduction

1.2.1.1 Once-Only Technical System

Article 14 of the Single Digital Gateway Regulation [REF30] states that the Commission, in cooperation with the Member States, shall establish a technical system for the cross-border automated exchange of evidences between competent authorities in different Member States. The draft "once-only" Implementing Act [REF38] further sets out the technical and operational specifications of the technical system necessary for the implementation of this Article. (References to this draft will be replaced by the references to the IR once it is adopted by the Commission and published in the Official Journal). This document complements the Implementing Act by providing a high-level architecture. This high level architecture is complemented by, and serves as an introduction to, further technical and operational design documents. References to current versions of this documentation are provided in this document. Together, these documents and the interface documentation they provide deliver the interoperability necessary to support the implementation and interconnection of the distributed components that constitute the Once-Only Technical System (OOTS).

1.2.1.2 Context

Initial preparatory work for the entry into force of the Once-Only Technical System, which is set to be in place and ready for use by 12 December 2023 was organized into a number of Work Packages, operating under the SDG Coordination Group. This document is an output of:

- Work Package 7, “Technical Design”.
- The "Evidence Exchange" topic in Work Package 6, "Functionality".
- The "User Identification" topic in Work Package 6, "Functionality".

The Once-Only technical system serves primarily as an integration mechanism for existing systems in Member States and is therefore primarily concerned with establishing interoperability by providing interface documentation. Interoperability is defined in the European Interoperability Framework (EIF, [REF19]).
This document also provides an initial introduction to outputs from the following Work Packages and topic:

- WP2, “User Centricity”, which addresses user journeys and use cases for "once-only". This Work Package adds a User perspective.
- WP4, “Data Semantics, Formats and Quality”, which covers content aspects of evidence exchange. Its main focus is Semantic Interoperability

1.2.1.3 Input

This document is based on the following main inputs:

- Single Digital Gateway Regulation, in particular Art 14 [REF30];
- OOTS Implementing Act [REF38].

Other inputs include:

- Deliverables and other input from the TOOP Large Scale Pilot [REF34];
- Deliverables and information from the DE4A Large Scale Pilot [REF7];
- The “OOP Blueprint” [REF1] created by the preparatory action on "once-only". That action, which was started in 2019, intends to pave the way for the creation of a dedicated ‘Once-Only Principle' (OOP) Building Block and the identification of potential new building blocks supporting cross-border interoperability;
- Input from Member State representatives in the SDG Coordination Group, provided during its periodic SDG plenary meetings;
- Input from Member State experts, provided during bilateral meetings scheduled with their representatives in the SDG Coordination Group, but also involving a broader range of experts;
- Input from Member State experts participating in the meetings and discussion item section of WP7, "Technical Design"; WP2, "User Centricity"; WP4, "Semantics", and WP6, "Functionality";
- Input from policy and subject matter experts in the Commission and from other Commission actions, in particular the ISA² and Interoperable Europe actions and the Building Blocks at DIGIT and the relevant units at DG GROW and DG CNECT.

1.2.1.4 Scope

This document covers the Once-Only Technical System specified in Article 14 of the SDG Regulation [REF30] and the draft Implementing Act [REF38]. This system will come as an addition to several existing systems for cooperation between Member States mentioned in recital (50) of the regulation, which are used to exchange evidence for exchanges that are in the scope of the SDG Regulation.

Other types of evidence handling, not in the scope of this document, include:

- Once-Only functionality that does not involve any cross-border border exchange;
- Cross-border exchange involving private sector sources;
- Evidences directly uploaded by the user;
- Once-Only functionality that uses different mechanisms for the exchange of evidences, as stated in Art 14.10.

Requirements of the SDG Regulation other than functionality covered by Article 14 are also out of scope.

1.2.1.5 Extensibility

While Article 14 of the SDG Regulation [REF30] and the Implementing Act [REF38] set a clear functional scope, the intended applicability of the OOP Technical System is broader. The system, or selected subsets of it, support and enable other data sharing requirements. In particular, the system is intended to not be limited to the procedures described in Article 14.1 but to also support other electronic procedures.
A key consideration is to make sure that additional functionality, if needed in the future, can be added in an incremental way to avoid a major redesign of the initial system. Incremental extensions in the future are made easier by defining the OOP system, as much as possible, using profiled subsets of more comprehensive open standards. This will allow functionality to be added relatively easily by extending the profiled subsets beyond the requirements in Article 14 of the SDG Regulation. This approach of using profiled subsets of standards was used successfully in the eDelivery Building Block, which has been extended in response to new needs without disrupting existing users and deployments.
A future version of the OOTS may also incorporate, at design level, other implementation technologies to implement existing elements, or add additional optional elements.

1.2.1.6 Structure of this document

The remainder of this document is structured as follows:

- Section 2, Requirements: gives an overview of the requirements on which the architecture is based.
- Section 3, Once-Only Technical System Architecture: provides a high level overview of Business Layer and Application Layer views. It partitions the elements in the architecture in four groups, which are discussed in the four next sections;
- Section 4, Evidence Requester Side Architecture Elements: covers Requester-side systems;
- Section 5, Evidence Providing Side Architecture Elements: covers Provider-side elements;
- Section 6, Once-Only Common Services that support the system;
- Section 7, Evidence Exchange and eDelivery: explains evidence exchange protocol supported by the eDelivery Building Block;
- Section 8, Identification and Representation: covers identification of natural and legal persons as well as representation;
- Section 9, System Operation: covers general operational constraints for the technical system;
- Section 10, Sample Once-Only Flows: describes in some detail a sample flow involving the Once-Only Technical System.

1.2.2 Requirements

The High Level Architecture is closely aligned with the activities and outputs of the User Centricity Work Package. That Work Package is in the process of defining a set of Functional Requirements that the Once-Only Technical System must support [REF37].
The following table complements these functional requirements by providing a more general overview of the key architectural requirements that the Once-Only Technical System addresses. The table classifies these requirements using the ISO 25010 quality attributes framework [REF36]. It also provides the source, in most cases the relevant section of the SDG Regulation (label "SDG.*"), the Implementing Act (label "IA.*"), and/or the applicable principle from

the European Interoperability Framework (label "EIF.*") [REF19]. To support traceability, the table indicates the architectural element (or elements) in which each requirement is addressed.

ID	Quality Attribute	Quality Sub-Attribute	Requirement	Source	Applies to Architectural Element(s)	Comments
1	Functional Suitability	Completeness, correctness and appropriateness of coverage of tasks and user objectives	Member States shall ensure that, where a procedure [..] can be accessed and completed online by non-cross-border users, it can also be accessed and completed online by cross-border users [..].	SDG.Art.13.1	Portal	Context, not about Once-Only per se.
2	Functional Suitability		Users are able to access the instructions for completing the procedure in an official language of the Union [..].	SDG.Art.13.2.a; EIF.P.9	Portal	Context, not about Once-Only per se.
3	Functional Suitability		Cross-border users are able to submit the required information, including where the structure of such information differs from similar information in the Member State where the user is undertaking the procedure.	SDG.Art.13.2.b	Portal, Evidence Broker	The Evidence Broker helps find evidence types that have "the required information" even if "the structure of such information" is different.
4	Functional Suitability		Cross-border users shall identify and authenticate themselves electronically.	SDG.Art.13.2.c; eIDAS	Portal, eID	SDG does not mandate eID (it says users "are able to") . But for OOP it is essential (an uploaded scanned identity document does not provide any validated identity attributes). So Art 13.3 seems not to be sufficient/relevant for OOP.

5	Functional Suitability		Cross-border users are able to provide evidence of compliance with applicable requirements in all cases where this is also possible for non-crossborder users.	SDG.Art.13.2.d	Portal	Article also mentions "to receive the outcome of the procedures in electronic format" but that is out of scope for OOP.
6	Functional Suitability		A technical system for the automated exchange of evidence between competent authorities in different Member States ('the Technical System') shall be established by the Commission in cooperation with the Member States.	SDG.Art.14.1; EIF.P.6	All	
7	Functional Suitability		The system supports the exchange of evidence for the online procedures listed in Annex II to the SDG Regulation and the procedures provided for in Directives 2005/36/EC, 2006/123/EC, 2014/24/EU and 2014/25/EU.	SDG.Art.14.1; EIF.P.6	All	
8	Functional Suitability		Where competent authorities lawfully issue, in their own Member State and in an electronic format that allows automated exchange, evidence that is relevant for the online procedures referred to in SDG.Art.14.1, they shall also make such evidence available to requesting competent authorities from other Member States in an electronic format that allows automated exchange.	SDG.Art.14.2; EIF.P.6	Data Service	Allowing for automated exchange means that the data in electronic format must be structured in such a way that it allows for machine-to-machine exchange of the data, or automated processing, based on a request from a user, through a competent authority in another Member State. This includes both structured and unstructured evidence. Evidence issued in paper format only falls outside

						the scope of the Article 14 exchange.
9	Performance Efficiency	Time behaviour	If the requested evidence is available, the issuing authority shall return it instantly to the requesting authority so that the procedure can be completed without making the user wait. If this is not possible (e.g. because the evidence is not yet in a digital format or otherwise needs more time to be created), the provider shall return a response informing the requester of this.	EIF.P.6	Data Service	If the evidence exists but can be (made to be) available in a very near future, this allows the user to decide to resume the procedure at a later stage.
10	Performance Efficiency	Resource Utilization	A requesting competent authority shall only request evidences lawfully that are relevant for the user in the context of the procedure, and shall only request these from issuing competent authorities in the specified Member State that issue that type of evidence.		Portal; Data Service Directory	The evidence requester is responsible for lawfulness of the request.
11	Compatibility	Co-Existence	The user shall be permitted to submit evidence by means other than the technical system and directly to the requesting competent authority.	SDG.Art.14.4; EIF.P.6	N/A	Context, scope.
12	Compatibility	Co-Existence	The system shall not apply to procedures established at Union level which provide for different mechanisms for the exchange of evidence, unless the technical	SDG.Art.14.10	Related Systems	

			system necessary for the implementation of this Article is integrated into those procedures in accordance with the rules of the Union acts that establish those procedures.			
13	Compatibility	Co-Existence	Where the technical system, or other systems for the exchange or verification of evidence between Member States, are not available or are not applicable, or where the user does not request the use of the technical system, competent authorities shall cooperate through the Internal Market Information System (IMI).	SDG.Art.15; EIF.P.4	Related Systems	Context, scope.
14	Compatibility	Interoperability	Components in the system interact following common interface specifications that are based on open standards and technical specifications.	EIF.P.2	All	
15	Compatibility	Interoperability	The technical system shall reuse existing standards.	EIF.P.4	Portal, Data Service, Evidence Broker	
16	Compatibility	Interoperability	Evidence exchange shall be enabled for evidences that are in a format that allows for automated exchange.	SDG.Art.14.2; EIF.P.4	Portal, Data Service, Evidence Broker	
17	Compatibility	Interoperability	Evidence formats and metadata structures shall be based on	EIF.P.2	Portal, Data Service, Evidence Broker	

			agreed standards and technical specifications.			
18	Compatibility	Interoperability	Competent authorities shall be identified using an agreed party-identifier format.	EIF.P.4.	eDelivery, Data Service Directory, Evidence Broker	
19	Compatibility	Co-Existence	The identifier format shall be able to leverage existing identifier systems in Member States.	EIF.P.1	eDelivery, Data Service Directory, Evidence Broker	
20	Compatibility	Interoperability	The message packaging format for evidence exchange shall be based on open standards and technical specifications.	EIF.P.2	eDelivery Message Exchange	
21	Compatibility	Interoperability	The interfaces of common services shall be based on open standards and technical specifications.	EIF.P.2	Data Service Directory, Evidence Broker, Semantic Repository	
24	Usability	Operability	The system makes it easy for the user to determine what (kind of) evidence is needed, and where to get it.	EIF.P.6; SDG.Art.14.3.a; SDG.Art.14.3.f; IA.Art.5; IA.Art.6; IA.Art.9; IA.Art.10; IA.Art.10;	Portal, Evidence Broker, Data Service Directory	
25	Usability	User error protection	Evidence requesters shall ensure that their procedure portals contain an explanation about the possibility to use the OOTS and its features.	EIF.P.6; IA.Art.9	Portal	

26	Usability	User error protection	Evidence requesters shall give users the possibility to select and request the types of evidence.	EIF.P.6; IA.Art.10	Portal, Evidence Broker, Data Service Directory, eDelivery	
27	Usability	User error protection	The user is provided with information about name of evidence provider and evidence type for confirmation, before any request is made.	EIF.P.6; IA.Art.12	Portal	The user does not have to provide the name him/herself.
28	Usability	User error protection	The user has the ability to preview evidence and can control whether or not it is used.	EIF.P.6; SDG.Art.14.3.f; IA.15	Preview Space	In case an evidence was selected by mistake, or an evidence has some issue, it can be discarded.
29	Usability	Accessibility	Accessibility refers to the degree to which a product or system can be used by people with the widest range of characteristics and capabilities to achieve a specified goal in a specified context of use.	EIF.P.7	Portal	
30	Reliability	Maturity	The solution reuses mature, proven eID and eDelivery Building Blocks developed under the Connecting Europe Facility.	EIF.P.4	eDelivery, eID	
31	Reliability	Availability	Member States and the European Commission shall ensure the availability of components up to agreed Service Levels.	EIF.P.6	All	
32	Reliability	Fault Tolerance	Exchange of evidence shall provide mechanisms to recover	EIF.P.6	eDelivery Message Exchange	

			from temporary transmission failures.			
33	Security	Confidentiality	The system shall ensure the confidentiality of the evidence. Evidences cannot be read/viewed while in transit between requester and provider.	SDG.Art.14.3.e; EIF.P.8	eDelivery Message Exchange	
34	Security	Integrity	The system shall ensure the integrity of the evidence. Evidences cannot be modified while in transit between requester and provider.	SDG.Art.14.3.e; EIF.P.8	eDelivery Message Exchange	
35	Security	Integrity	The Evidence Provider shall ensure the integrity of the evidence between the Data Source (Base Registry) and its Access Point.	EIF.P.8; IA.18	Data Service, Access Point	See section 5.3. Same security requirements on messaging within a Member State as on eDelivery messaging.
36	Security	Integrity	The evidence requester shall ensure the integrity of the evidence request between Portal and its Access Point,	EIF.P.8	Portal, Access Point.	See section 4.3. Same security requirements on messaging within a Member State as on eDelivery messaging.
37	Security	Non-Repudiation of Receipt	A competent authority cannot repudiate its receipt of an evidence through the technical system, as it sends a signed eDelivery receipt that includes the digest of the received message.	EIF.P.8	eDelivery Message Exchange	
38	Security	Non-Repudiation of Origin	A competent authority cannot repudiate its issuing of an evidence through the technical	EIF.P.8	eDelivery Message Exchange	

			system, as evidences are exchanged in signed messages.			
39	Security	Non-Repudiation of Origin	A competent authority cannot repudiate having requested an evidence through the technical system, as evidence requests are exchanged in signed messages.	EIF.P.8	eDelivery Message Exchange	
40	Security	Authenticity	The evidence exchanged through the technical system shall, for the purposes of the requesting competent authority, be deemed to be authentic.	SDG.Art.14.8; EIF.P.8	eDelivery Message Exchange, Data Service.	
41	Security	User Identification	The identification of users, the provision of information and supporting evidence, signature and final submission can all be carried out electronically at a distance, through a service channel which enables users to fulfil the requirements related to the procedure in a user-friendly and structured way.	SDG.Art.6.2.a; EIF.P.6;EIF.P.8	Portal, eID	
42	Security	User Identification	Evidence Providers may ask the user to re-authenticate.	IA.Art.16	eID, Data Service Directory	
43	Security	User Identification	Evidence Requesters shall ensure that users are authenticated when they use the OOTS.	IA.Art.11	eID, Portal	
46	Security	User Identification	Evidence Providers shall not return an evidence if there is no unique match for the user based	IA.Art.16	Data Service	

			on his or her attributes but instead return an error			
47	Security	Accountability	Requesting and issuing competent authorities shall log all exchanges of (requests for) evidence and associated metadata and non-repudiation data.	EIF.P.3; EIF.P.8	Portal, Data Service, eDelivery	
48	Maintainability	Modularity	The technical system is a distributed system consisting of systems supporting the evidence requester, the evidence provider and supporting common services.	EIF.P.1	All	
49	Maintainability	Modularity	Components are placed where possible and, if preferred by a MS, in the MS rather than at central EU level.	EIF.P.1	All	
50	Maintainability	Modularity	The components in the system communicate based on agreed interfaces. Beyond these interfaces and SLAs, no implementation constraints apply.	EIF.P.2; EIF.P.5	All	Components can be implemented in any programming language or framework, run on any operating system, hardware or cloud, as long as the interfaces are correctly implemented.
51	Maintainability	Modifiability	The system will not be hard-wired to particular types of evidence requirements and evidence types. Evidence Requesters may use a registry to dynamically discover evidence types to use. Evidence Providers may register evidence types in the registry.	EIF.P.2; EIF.P.4; EIF.P.12	Evidence Broker	

52	Maintainability	Modifiability	The system will not be hard-wired to particular data services for particular evidence types. Evidence requester may use a registry to dynamically discover data services that can be used. Evidence Providers may register (and change registrations for) Data Services.	EIF.P.2; EIF.P.4; EIF.P.12	Data Service Directory	
53	Maintainability	Modifiability	The system is designed to enable future enhancements to support types of exchange beyond Article 14 requirements, such as subscriptions or deferred responses.	EIF.P.2;EIF.P.4; EIF.P.12	Portal, Data Service, Data Service Directory	
54	Maintainability	Reusability	Elements of the system should be reusable for data sharing beyond the scope of the SDG Regulation.	EIF.P.2;EIF.P.4	All	
55	Portability	Adaptability, Replaceability	Elements in the system can be transferred from one hardware, software or other operational or usage environment to another.	EIF.P.5	All	The focus of the architecture is on interfaces; implementations can be changed.

1.2.3 Once-Only Technical System Architecture

1.2.3.1 Context

The Single Digital Gateway Regulation [REF30] aims to make it easier for a user to initiate and execute, subject to specified constraints, a set of procedures online where:

- the user is using an Online Procedure Portal of a public administration in a Member State;
- the procedure requires evidence from a different Member State than the Member State hosting the Online Procedure Portal.

While carrying out a cross-border online procedure, evidence relating to a citizen (of the Union), a natural person (residing in a Member State) or a legal person (having its registered office in a Member State) may be required. The Once-Only Technical System allows the governmental Portal to request, following the explicit request of the user (unless exemptions apply), the exchange of evidences from one or several competent authorities in (a) different Member State(s), for use in the context of the procedure. This means that this system aims at enabling cross-border data-sharing between competent authorities at all administrative levels (local, regional and national).
Note that:

- Under ECJ case law competent authorities can also be non-governmental entities with a formal task in the public remit.
- The competent authority that *issues* the evidence acts, in terms commonly used in other contexts (including the former TOOP large scale pilot [REF34]), as a Data Provider. The competent authority that *requests* the provided evidence acts as a Data Consumer.

This document provides a high-level architecture for the Once-Only Technical System. Its aim is to link the SDG Regulation [REF30] and Implementing Act [REF38] to the more detailed technical design documents and to provide a summary overview.

1.2.3.2 Approach

The OOP Technical System establishes a general purpose data exchange ecosystem for the public sector in Europe. The system enables trusted cross-border data sharing between competent authorities in a distributed environment involving many evidence providers and many evidence requesters.
The Once-Only Technical System is not a single monolithic system. Instead, it is a distributed collection of systems that, once interacting with one another, form a Once-Only technical “ecosystem”. Rather than assuming a shared, single, central information system, the architecture takes a decentralized approach based on integration and interconnection of independent systems. Most of the systems that will be part of the Once-Only Technical System are independently operated by Member States, and many of them are likely to be (evolutions of) existing systems that are already in use today, rather than new systems designed specifically for Once-Only in the context of the SDG Regulation.

To allow the interconnection of existing systems in use in Member States, the architecture uses a loosely coupled interoperability layer based on the concept of common reusable “Building Blocks”. Building Blocks provide agreed, common interfaces. They are designed to minimise the impact on existing systems in Member States and to maximise opportunities for reuse. The architecture includes interoperability-enabling elements provided by existing Building Blocks developed under the former Connecting Europe Facility (CEF) such as eID and eDelivery [REF3] and adds additional Once-Only common services to provide comprehensive support for Once-Only. The interfaces may be implemented in multiple independent software implementations or services, including software products or services from third party solution providers.

1.2.3.3 Overview

Figure 1 provides a High Level view of the Once-Only Technical System.[1] and it is provided as an illustrative example only. The system as shown includes a “Once-Only Evidence Exchange” business process that establishes a transition between two business events, associated to a cross-border administrative procedure:

1. A “Cross-Border Evidence Required” input event that indicates that (an action in) a procedure requires one or more evidences to be retrieved from one or more other Member States (this will most likely be based on information supplied by the user).
2. An “Exchange Completed” output event that occurs when, in case of success, the required evidence(s) has/have been exchanged, where “exchange” implies not just the transmission of the evidence, but also the request of the user and the acceptance for use in the procedure. Note that the exchange may also be unsuccessful, if no evidence was available or the user decided not to use it in the procedure.

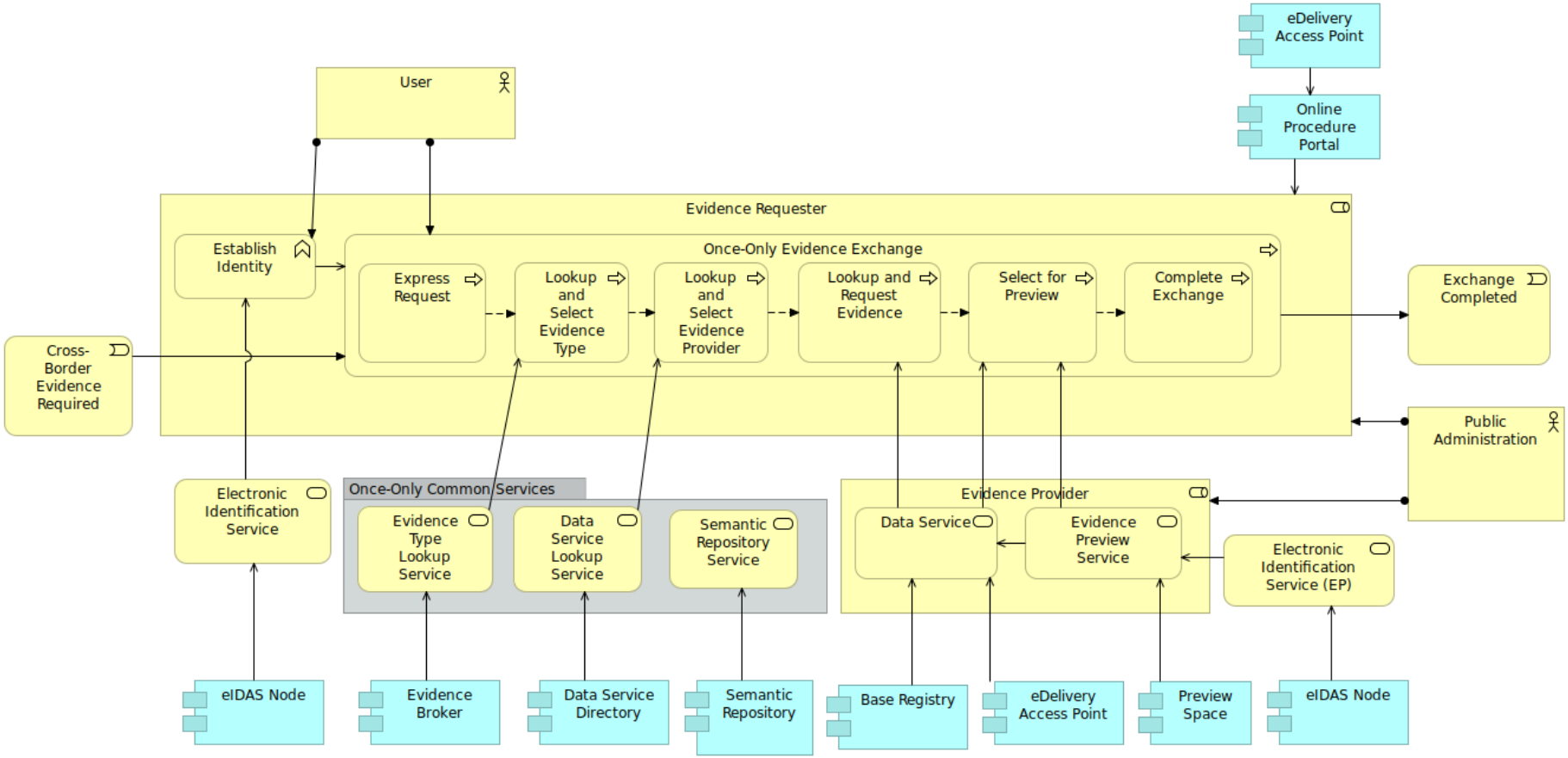


Figure 1 High Level View of the Once-Only Technical System

Both of these events relate to the competent authority that requests the evidence(s). They are connected by the business process that involves interactions with:

- the user;
- the Data Service of the competent authority that provides the evidence, acting as Evidence Provider;
- Once-Only common services that support the operational uses of the Once-Only Technical System.

The flow of the business process follows the steps described in Article 14(3) of the SDG Regulation [REF30].

As Article 14(7) of the SDG Regulation and Article 12 of the Implementing Act explain, an evidence request is issued by a competent authority but is subject to an explicit request given by the user, unless otherwise provided under Union or national law. It therefore relies on authentication of the user. This is provided by the “Establish Identity” business function that is served by an “Electronic Identification Service”. This service may be provided by the eIDAS Node component from the eID Building Block [REF17] or by other components (not shown in the diagram), such as a notified electronic identification service of the Member State in which the requesting authority is based. Since identification is typically a general requirement for electronic procedures and not only for evidence exchange, it is not modelled as a step in the exchange business process but as a business function that serves it.

The “Once-Only evidence exchange” process consists of the following steps, all initiated from an Online Procedure Portal (see section 4.2):

1. "Express Request" is a step in which the user is asked to express explicitly whether he or she wants to use the Once-Only Technical System.
2. “Lookup and Select Evidence Type” is an optional step in which an “Evidence Type Lookup Service” is used to determine the type of evidence to be retrieved. This service is implemented in an Evidence Broker component (see section 6.2).
3. “Lookup and Select Evidence Provider” is a step in which a “Data Service Lookup Service” is used to determine the competent authority to which the evidence request is made. This service is provided by a Data Service Directory component (see section 6.3).
4. “Lookup and Request Evidence” is a step in which a request for available evidences is made to a “Data Service” (see section 5.2) using eDelivery messaging. This service is provided by a “Base Registry” component owned by a competent authority that is an “Evidence Provider”. If any evidences may be available from the contacted Data Services, the response will include hyperlinks that link to a separate "Evidence Preview Service" offered by (or on behalf of) the Evidence Provider.
5. "Select for Preview" is a step in which the user selects one or more available pieces of evidence for consideration. At this stage, the user will be provided the option to follow the hyperlinks to preview and decide on the use of the evidence, and return to the Online Procedure Portal. In parallel, any confirmed pieces of evidences are returned to the Portal using secure eDelivery messaging.
6. After returning from the Preview Space, the “Complete Exchange” is a step in which the user continues the procedure.

Of these six steps, all but the first and last involve interaction between IT systems in different Member States. The Once-Only Technical System is based on detailed technical design documentation that provide interoperability between these systems.

The three services “Evidence Type Lookup Service”, “Data Service Lookup Service” and “Semantic Repository Service” together comprise a group of Once-Only common services. These platforms do not handle requests for evidences and their issuance directly but provides supporting services.

Section 4 will discuss the architectural elements relating to the competent authority that requests the evidence. Section 5 will do the same for the evidence-issuing competent authority. Section 6 discusses the Once-Only common services. Section 7 and 8 cover eDelivery, evidence change and identification and authentication in the Once-Only Technical System.

1.2.3.4 Core and Extension Architectural Elements

The following elements are core elements as they are used for all "once-only" exchanges:

- Online Procedure Portal;
- Data Service;
- Data Service Directory;
- eDelivery Access Points.

Other elements of the architecture are extension elements, as their functionality is not always needed. For example:

- The user may authenticate to the Online Procedure Portal of a public administration in a Member State using a notified national eID of that Member State, thus obviating the need to use eIDAS nodes.
- In procedures in which Member States have agreed to all use the same evidence types, there is no need for Evidence Broker functionality to determine evidence types to select. In that case, an Online Procedure Portal can directly look up Data Services in the Data Service Directory without having to first look up a rule for a particular requirement.

1.2.3.5 Governance

Section VI of the Implementing Act [REF38] addresses some governance aspects of the Once-Only Technical System. It covers:

- The role of the Gateway Coordination Group established under the SDG regulation and its subgroups.
- Technical support.
- Cooperation with other governance structures.

1.2.3.6 Roles and Responsibilities

The Once-Only Technical System is a collection of interacting technical systems of the Member States and the Commission. According to Article 14(11) of the SDG Regulation, the Commission and each of the Member States shall be responsible for the development, availability, maintenance, supervision, monitoring and security management of their respective parts of the technical system.
Section VII of the Implementing Act [REF38] covers responsibility for the maintenance and operation of the components of the OOTS.

1.2.4 Evidence Requester Architecture Elements

1.2.4.1 Introduction

The interaction in the Once-Only Technical System is an interaction between competent authorities. This section covers architecture elements involving systems of competent authorities that request evidences.
As an example, a university, or another public administration in the education domain, could provide an Online Procedure Portal to help candidates apply online for a tertiary education study financing. A prospective student that previously studied in a different Member State, or even in multiple different

Member States, could use this portal to apply. Using the Once-Only Technical System, the candidate can provide the university or public administration with proof of any relevant existing qualifications he or she obtained from institutions in other Member State(s), and other relevant documentation such as information on social situation and level of income.

1.2.4.2 Online Procedure Portal

An **Online Procedure Portal** is an online system of a public administration in a Member State that allows users, including cross-border users from other Member States, to execute a procedure of the public administration. The Once-Only Technical System is concerned with the subset of functionality of an Online Procedure Portal that relates to the cross-border automated exchange of evidence between competent authorities in different Member States and application of the 'once-only' principle as defined in Article 14 of the SDG Regulation. This functionality is provided by the "Once-Only evidence exchange" business process as shown in Figure 1.
The functionality of an Online Procedure Portal can be considered along two dimensions, which relate to the two axes in Figure 2:

- Front end functionality versus back end functionality. This is reflected in the vertical axis of the diagram. Front end components can be implemented, for example, as a website that supports access using a Web browser or as a mobile application.
- Different types of functionality. This is reflected in the horizontal axis of the diagram. Seven components and related sets of functions are defined.

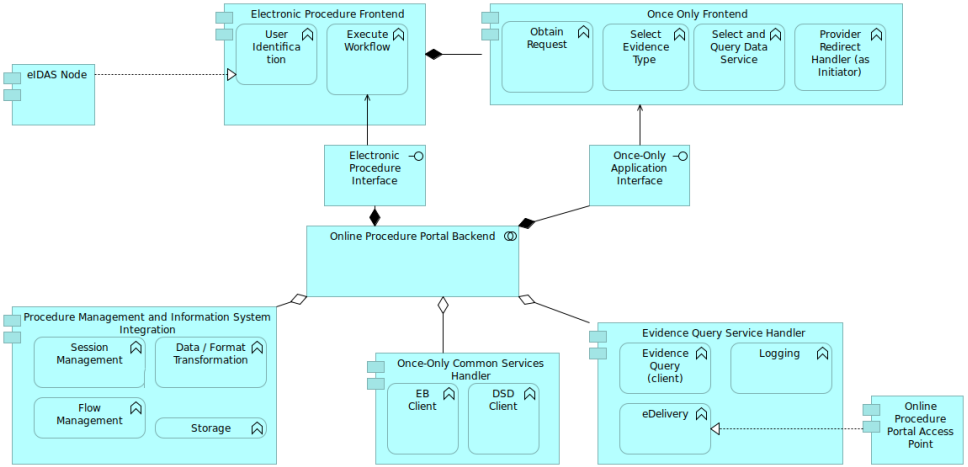


Figure 2 Online Procedure Portal Application View

Together, the front end components and the back end components include functions to allow the user to execute the actions in the "Once-Only evidence exchange" business process, as well as any preceding actions that are preconditions:

- Identify himself/herself ("Establish Identity");
- Explicitly request to use the system for exchange of evidence ("Express Request");
- Select evidence types ("Lookup and Select Evidence Type");
- Select data services ("Lookup and Select Evidence Provider");
- Look up available pieces of evidence ("Lookup and Request Evidence");
- Consider some or all pieces of evidences for preview and use in the procedure ("Select for Preview");
- Complete the process and continue back to the procedure ("Approve and Complete Exchange");

This architecture only specifies at a high level the interfaces provided by back-end components to front-end components. It does not constrain them at more detailed technical level because they are only used internally in Member State systems.
In this version of the OOTS, following article 15 of the Implementing Act, it is assumed that the user executes the preview of and decision to use a piece of evidence using an Evidence Preview Service located in the Member State of the Evidence Provider. Any interaction with this service is therefore a temporary interruption of the business process of the Evidence Provider. The Online Procedure Portal needs to provide a Provider Redirect Handler function that:

- allows a user to choose to navigate to the Evidence Provider for preview and confirmation purposes.
- provides a return address that the user can be directed back to in order to continue its procedure.

The Once-Only Technical System is about exchange of "read-only" evidences. The user can decide to not use the evidence but cannot modify its content in any way. User confirmation to use evidence in the context of a particular procedure does not constitute an authorization to use the provided evidence in other contexts or for other purposes.
Figure 2 classifies back end functions in three groups:

- Procedure management and information systems integration. This is common functionality that is needed in an Online Procedure Portal that does not relate to Once-Only Technical System. It is mentioned for context.
- Once-Only Common Services handler functions that interface to the Once-Only common services described in section 6. These functions include client interfaces to the **Evidence Broker** and the **Data Service Directory**.
- Evidence query service handler functions that control the exchange of evidence requests and correlated evidence responses (or error messages) from a **Data Service** using the functionality described in section 7.

Article 9 of the Implementing Act [REF38] requires the Online Procedure Portal to explain the possibility to use the Once-Only Technical System and its features to users. Article 10(1) requires involving the user in the selection of evidence types and data services. Article 11, user authentication, is addressed in section 8. Article 12 shows information that must be provided to the user before evidence is requested.
An Online Procedure Portal Back-end needs to cover general electronic procedure functionality, such as procedure management functionality, to manage a user's session and flow through the procedure, and information system integration, which includes any permanent storage of procedure data and submitted evidences. These functionalities include:

- Procedure and session state management: at a particular point in time, multiple users may be interacting with the system and using the Once-Only Technical System. Any evidences that are returned in response are made available to the specific procedure end-user that issued the query for

those evidences. In addition, user input to the procedure, and evidences retrieved to support it, may be provided over time, and possibly interrupted/resumed;
- Integration with information systems and/or databases and any required data or format transformation. This may involve transformation between different structured formats, or from structured (data-oriented) to unstructured (presentation-oriented) formats.

Since the Once-Only Common Services Handler and Evidence Query Service Handler relate to systems in different Member States, and to systems provided by the European Commission, their external interfaces are specified in design documentation of the Once-Only Technical System in order to achieve interoperability. Their internal interfaces to the front end components are not standardized as they are used within a Member State.
The functionality for evidence exchange includes functionality to:

- Create evidence requests and submit them to the **Online Procedure Portal Access Point** for transmission to a **Data Service**;
- Receive responses, delivered to the Online Procedure Portal by the Online Procedure Portal eDelivery Access Point;
- Logging of evidence exchange information including date and time and unique identifiers of evidence request, evidence response, user, data service and evidence type.

Article 13, content of evidence request, and Article 15, the response to evidence requests, are addressed in section 7.3.

1.2.4.3 Online Procedure Portal Access Point

The Evidence Query Service Handler application component of an Online Procedure Portal uses an eDelivery **Access Point** to request the evidence from the evidence provider and receive the evidence in response. This may be a dedicated Access Point for that specific Portal, or a more general communication component that is also used by other portals and systems. By sharing an Access Point, competent authorities can reduce the cost and complexity of implementation. For further discussion and references, see section 7.2.
Since this Access Point is the entry point into the Once-Only Technical System, it is essential that the competent authority on behalf of which the Access Point makes such a request has an appropriate legal basis to make such a request, such as Directive 2005/36/EC, 2006/123/EC, 2014/24/EU or 2014/25/EU or, for the procedures listed in Annex II of the SDG Regulation, other applicable Union or national law as stated in recital 45 of the SDG Regulation. According to Article 35 of the Implementing Regulation, the Evidence Requester is responsible for lawfulness of the evidence request. Member States are responsible for securing the evidence request as it is transmitted from an Online Procedure Portal to the Access Point, as required in Article 28 of the Implementing Act. For more information on requirements, see section 7.9.

1.2.4.4 eIDAS Node of Evidence Requesting Member State

To use the Once-Only system, the user needs to be identified and authenticated. If the user is registered in the Evidence Requesting Member State, a notified eID system of the Member State may be used. If the user is from a different Member State and has an eID from that Member State, the **eIDAS Nodes** of the two Member States can be used for cross-border authentication. The mandatory attributes of the eIDAS minimum data set obtained from the user using either of these identifications methods are included in evidence requests to the Data Services. If the Unique Identifier is Member State specific, this attribute should not be included as it was issued for a specific context of the Online Procedure Portal. The eID functionality will be accessed from the front-end part of the Online Procedure Portal and/or the Evidence Provider as it involves interaction with the user. For more on eIDAS nodes, see section 7.

1.2.5 Evidence Provider Architecture Elements

1.2.5.1 Introduction

The interaction in the Once-Only Technical System is an interaction between competent authorities. A competent authority that *issues* evidences in response to evidence requests provides a **Data Service** as specified in section 5.2. The transmission of requests and evidences uses an **eDelivery Access Point** as specified in section 5.3. This section covers architectural elements involving systems of competent authorities that issue evidences.

1.2.5.2 Data Service

Competent authorities in Member States operate **Data Services** to issue evidences, in response to requests from requesting competent authorities and users executing procedures in Online Procedure Portals. The legal base for this service is provided in article 15 of the Implementing Act.
For example, the Ministry of Education in one Member State may offer a service that provides evidences concerning diplomas, certificates or other proof of studies or courses obtained in that Member State that can be shared with other Member States through the OOP system.
A Data Service must implement a common “Evidence Query Service”. In support of this services, a Data Service includes functionality to:

- Receive evidence requests, delivered by an eDelivery Access Point, and interpret them. These requests are the input to the “Evidence Query Service”;
- Perform evidence request validation;
- Perform identity matching, to determine which (if any) evidences in storage relate to the user (see section 8.5);
- Apply, if requested, a transformation on the evidence, from a predefined set of transformations;
- Coordinate its processing with the Preview Space;
- Return evidence responses (including possibly errors) and submit them to an eDelivery Access Point for transmission to the requesting Online Procedure Portal.

This exchange of pieces of evidence is subject to user preview and approval. The user performs these actions using the Preview Space (see section 5.3 below). Therefore, two request-response loops are required:

- A first request-response loop in which the Data Service, if pieces of evidence may be available, returns hyperlink information that allows the Online Procedure Portal to direct the user to the Preview Space.
- A second request-response loop, executed in the background and in parallel to the user's interaction with the preview space, that returns any selected pieces of evidences.

The Data Service implements functions to coordinate the second request-response loop and the user's actions in the Preview Space and to make sure that:

- User identity attributes in the evidence request match the user's identity as established by authentication to the Preview Space.

- Only pieces of evidence are made available to the user that are of the requested type and that relate to the identified data subject.
- Only pieces of evidence selected by the user for use in the procedure (if any) are included in the second loop evidence response.
- The interactive user activity relates to the same procedure execution on the side of the Evidence Requester.

A Data Service may respond to requests by providing pre-existing evidences or by creating or assembling evidences from data dynamically. Such assembling may involve operations such as selection, filtering or transformation.
The generic format for evidence requests and responses is based on exchange data model design documentation based on open standards and technical specifications introduced in section 7.
A data service may not be directly connected to an information system. Instead, middleware or other integration solutions may be used. A data service may also connect to a national OOP layer, rather than integrate directly to an information system. This is not reflected in the following diagram.

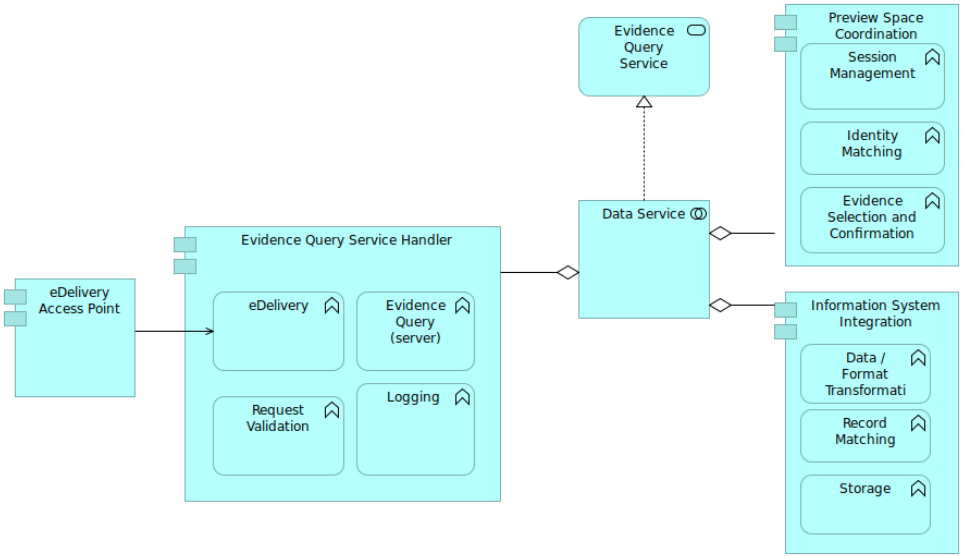


Figure 3 Data Service Application View

1.2.5.3 Preview Space

In this version of the OOTS, the Evidence Preview Service is offered by (or on behalf of) the evidence issuing competent authority. The service may be an integral part of the Data Service or it may be a separate component, called **Preview Space**, as defined in article 15 of the IA. Subject to the conditions specified in that article, a single Preview Space component may offer an Evidence Preview Service to multiple Evidence Providers and their Data Services. The preview space provides user-interface related functions supporting the once-only user interaction. These allow the user to:

- Enter the space using a hyperlink that was communicated to the Online Procedure Portal using the response message in the first request-response loop.
- Return to the Online Procedure Portal using a return address provided by the Online Procedure Portal.
- Authenticate himself or herself, if deemed necessary.
- Preview pieces of evidences of the selected evidence type.
- Decide whether or not to transmit any piece of evidence to the Online Procedure Portal so that it can be used in the procedure.

Mirroring the coordination functions of the Data Service, the Preview Space needs to make sure:

- All and only pieces of evidence matching an evidence request for the procedure the user is executing can be previewed and selected.
- Decisions by the user whether or not to use a piece of evidence are reflected in the evidence response by the Data Service.
- The identity attributes for the user in the evidence request match the attributes established by electronic identification of the user.

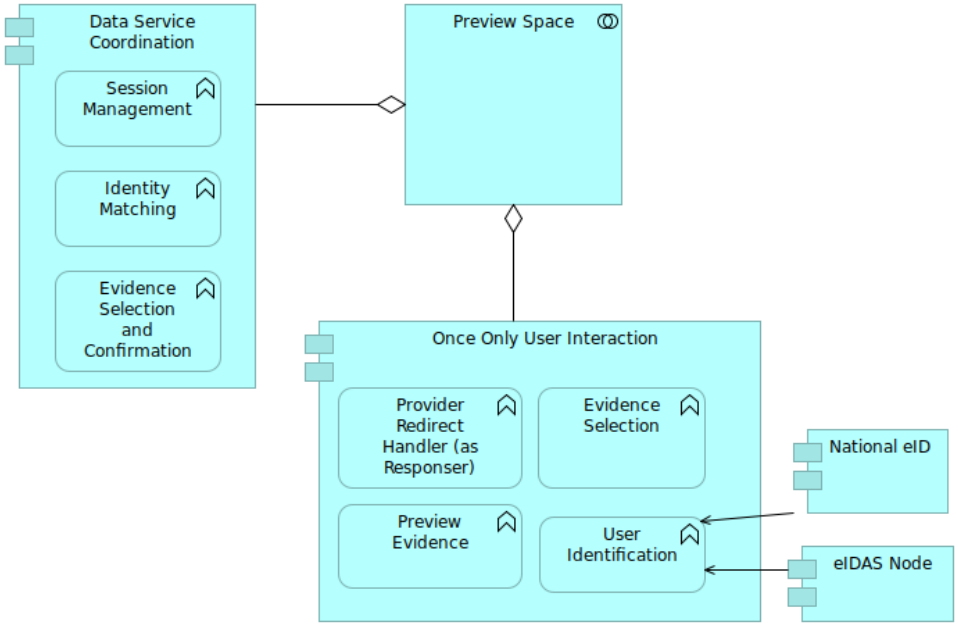


Figure 4 Preview Space Application View

1.2.5.4 Data Service Access Point

The requests to a Data Service and the responses to those requests are exchanged securely and reliably using eDelivery. The Data Service must therefore also be accessible via an eDelivery **Access Point**. This may be a dedicated Access Point for that specific Data Service. It can also be a more general communication component that is also used by other applications. An Access Point may be shared by multiple competent authorities, to reduce the cost and complexity of implementation. For further discussion and references, see section 7.2.
Member States are responsible for securing the evidence as it is transmitted from a Data Service to the Access Point, as required in Article 29 of the Implementing Act. For more information on requirements, see section 7.9.

1.2.5.5 eIDAS Node of Evidence Issuing Member State

As mentioned in section 4.4, the eIDAS Node of the Member States from which evidences are requested may be used to authenticate the user to the online procedure. This is initiated via the eIDAS Node and Online Procedure Portal from which the evidence is requested. For more on eIDAS nodes, see section 6.3.
When the user follows a link to the Preview Space, he or she may be requested to re-authenticate. If the user is not authenticating using an eID from the Issuing Member State, he or she shall use the eIDAS Node system to authenticate using a notified eID from another Member State.

1.2.6 Once-Only Common Services

1.2.6.1 Introduction

To support the exchange of evidences between **Data Services** and **Online Procedure Portals**, the Once-Only Technical System uses Once-Only supporting services. Article 4 of the draft Implementing Act [REF38] refers to these services as the Common Services. The Common Services do not process data about citizens or businesses. Instead they contain and serve operational data parameters that support the operation of the Once-Only technical system. The Common Services are:

- Evidence Broker (see section 6.2);
- Data Service Directory (see section 6.3);
- Semantic Repository (see section 6.4).

Each of these services will provide a life-cycle management interface (see section 6.5) to maintain the data it serves as this data is subject to change over time. The Once-Only Technical System follows a hybrid deployment model (see section 6.6).

1.2.6.2 Evidence Broker

The Once-Only Technical System supports situations in which an Online Procedure Portal, when performing an online procedure, requests an evidence from a data service in a different Member State. The evidence relates to a requirement to obtain information on a citizen or business or to prove that certain claims about the citizen or business are true. Its legal base is Article 6 of the Implementing Act.
If for a particular procedure, for a particular requirement, a harmonized evidence type (and associated schema) is defined and agreed by the Member States, all Member States know in advance which evidence type needs to be requested. However, the Once-Only Technical System also supports situations in which there is no single agreed evidence type that is harmonized across the EU and that all Member States can provide. The type of evidence that is used in the Member State that requests the evidence may not exist in another Member State. However, that Member State may be able to provide an "equivalent" evidence type, or even multiple "equivalent" types. Here, "equivalence" is used in the informal sense that the other type(s) can be used to prove the same claim about the citizen or business, or that the evidence type provides the same required information as the evidence type used in the Member State from which the request is made. In this case, the procedure can be executed using the alternative evidence type(s).
It is impractical to assume that an Online Procedure Portal in a Member State knows in advance which type of evidence to request, not just because this may differ for each of the many other source Member States, but also because the rules underlying the equivalence may change over time. Therefore, the Once-Only Technical System provides a common service, the **Evidence Broker**, which allows an Online Procedure Portal in a Member State to determine which evidence type it may request from another Member State for a particular purpose in a particular context.

The Evidence Broker has a defined interface. It responds to requests that contain the following information:

- The Member State from which evidence is to be retrieved;
- An identifier of the requirement for which evidence is requested (information needed, criteria that need to be met);
- The context in which the request is made (life event, procedure, applicable Directive);
- Optionally, the geographic area code for the Member State in which the competent authority that lawfully issues the evidence is based.

It will return, in response, the following information:

- A (possibly empty) list of the following information item pairs:
    - An identifier of an evidence type that satisfies the information requirement;
    - Optionally, for structured evidences, an identifier of a transformation that may be applied, if requested, to the evidence by the Evidence Provider.

The ability to specify transformations that may be applied to evidences supports the data minimization requirement of the GDPR [REF21]. The provider can use a transformation to provide an evidence that more narrowly matches the relevant requirement, by removing unnecessary substructures and/or aggregating information. However, this functionality is optional. If the competent authority providing the requested evidence can only provide digitalised documents, instead of data, it is possible that the requesting authority receives more personal data than strictly needed. However, this situation is no different from those in which such evidence is submitted by the user. The SDGR does not aim to harmonise the format in which evidence is provided by the different competent authorities in the Member States. Until all administrations move to a system based on data instead of documents, the Once-Only Technical System will be able to accommodate both.

This Evidence Broker service is based on rule content, provided by the Member States themselves. It provides an online mechanism for Member States to align and query their evidence requirements and evidence type sets. This obviates the need for full EU-level harmonisation of evidences types. The Evidence Broker allows Member States to manage and share information about rules relating to evidence types. As noted, for any evidence type, equivalence is relative to the purpose for which, and context in which, it is used.
The data model and concepts used in the Evidence Broker are defined in the Core Criterion and Core Evidence Vocabulary (CCCEV, [REF40]), provided by Interoperable Europe [REF29]. Additional design documentation is available for the Evidence Broker [REF9].

In case where there are multiple options (multiple evidence types) for a particular requirement, the Online Procedure Portal may ask the User to select which (if any) option will be used, putting the user in control of the execution of the procedure.
Note that use of the Evidence Broker is not needed and its use is not required in situations where the evidence requester already has obtained the response information mentioned above.

1.2.6.3 Data Service Directory

To request electronically available evidence from a Data Service in a different Member State, the portal of a public administration in a Member State needs data about the Data Service (such as the relevant eDelivery routing identifier) in the other Member State that may provide the evidence. The OOP Technical System includes a **Data Service Directory** which allows Member States to manage and share this information in a structured format. Its legal base is Article 5 of the Implementing Act.
The Data Service Directory has a defined interface. It responds to requests that contain the following information:

- An identifier of the Evidence Type;
- The Member State in which Data Services for the identified Evidence Type are being looked up;
- Optionally, the geographic area code for the Member State in which the competent authority that lawfully issues the evidence is based.

It will return, in response, the following information:

- A (possibly empty) list of tuples providing the following information:
    - The identifier code and identifier code type of the Evidence Provider served by the Data Service;
    - The identifier code and identifier code type of the authority that operates the Data Service Access Point used by the Data Service;
    - The required Levels of Assurance of the eID means notified in accordance with Regulation (EU) 910/2014
    - A list of additional attributes (if any) used to facilitate the identification of the relevant evidence provider, their formats and optionality.

The Once-Only Technical System supports situations in which there is more than one Evidence Provider for an Evidence Type in a Member State. In these cases, the user may help decide which (if any) of them will be queried, as he or she may know from which Data Service(s) relevant evidence(s) can be obtained. For example, in an educational procedure the user could select the university that he or she knows issued an educational evidence type for him/her from a list of universities, if universities in the relevant Member State use different Data Services.
Additional design documentation is available for the Data Service Directory [REF8]. This work is based on open technical specifications and Interoperable Europe (formerly ISA^2) specifications.

On the support of the Data Service Directory for identification and authentication, see section 8 below.

1.2.6.4 Semantic Repository

In order to achieve semantic interoperability, Member States need to make detailed agreements on the semantics of evidence types that are to be exchanged using the OOP Technical System. The **Semantic Repository** supports this by storing and sharing definitions of names, definitions and data types of data elements associated with specific evidence types. Its legal base is Article 7 of the Implementing Act. This Repository is not used in the run-time exchange of evidences. Its purpose is only to support the Member States as they design and implement systems consuming or providing evidences. The Semantic Repository contains:

- Visual class diagrams;
- Data models and definitions;
- Data elements and definitions;
- Distributions in XML schema (XSD) or equivalent formats;
- Code lists of information requirements;
- Code lists of evidence types;
- Other code lists, or references to code lists, used in the system;
- A methodology for developing new data models for structured evidence types.

Additional design documentation is available for the semantic repository [REF28].
The Semantic Repository includes a generic metamodel that can be used for the exchange of arbitrary unstructured evidences. It provides a light-weight generic mechanism to support the exchange of any type of evidences. It facilitates the automated exchange of either unstructured or structured types of evidence. This metadata model is in line with the Exchange Data Model used in Evidence Exchange. The data models for specific evidence types complement the generic metadata model and provide structured data models developed for a particular evidence type.

1.2.6.5 Life Cycle Management

The instances of the Evidence Broker and the Data Service Directory provided by the European Commission will provide interfaces that allows Member States to maintain (add, change, delete) content regarding evidence types available from them and data services that provide them. Two interfaces will be provided:

- A user-interface that can be used by Member State representatives to interactively manage content;
- An automated bulk load interface that allows Member States to replace their partition of the content in the EC provided instances by an updated version.

While the lookup query interfaces of Evidence Broker and Data Service Directory use a lightweight REST interface, the bulk load interface will use the existing Life Cycle Management service interface of OASIS RegRep [REF27] using eDelivery [REF13] in order to benefit from its advanced security and reliability.

1.2.6.6 Deployment Options

As a reflection of the different implementation preferences of Member States, the deployment of the Once-Only common services Data Service Directory and Evidence Broker follows a hybrid model, in which:

- The European Commission will operate an optional EU-wide central service instance for the Member States. This instance contains metadata for those Member States that want to use this service instance. This instance allows metadata from these Member States to be searched by all participants in the Once-Only Technical System. Member States using this instance still need to provide and help maintain the metadata in the central service as discussed in section 6.5.
- A Member State that wants to do so can operate and provide access to its own instance of the service. To retrieve data related to this Member State, this instance is used and there is no need to provide data to the EU-wide central service instance.

The legal base for this deployment model is Article 8 of the Implementing Act.
The European Commission will provide a central registry in which connectivity information for each of the evidence broker and data service directory instances is published and provide a mechanism supporting dynamic discovery of these directory instances. More information on this registry discovery functionality is provided in [REF41].

The model is illustrated for the Data Service Directory in the following diagram. It shows a situation in which Member State 1 uses the EC central Data Service Directory and uses the LCM interface mentioned in section 6.5 above to upload its data (step 1 in the diagram). Member State 2 provides its own data and does not upload it to the EU Central DSD instance. To discover which DSD to retrieve data from, Evidence Requesters may query the EU DSD Registry (step 2). This Registry will indicate that DSD queries for Member State 1 should be addressed to the EU Central DSD (step 3a), whereas DSD queries for Member State 2 should be addressed directly to its national DSD (step 3b).

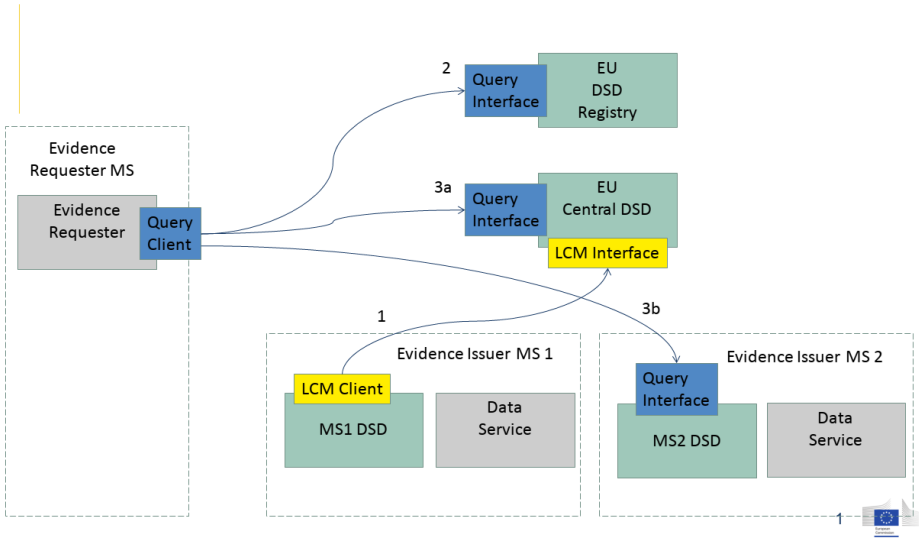


Figure 5 Hybrid deployment model for common services

Note that there shall be no more than one instance of a common service for a given Member State. Therefore, a given Member State either has no service instance of its own, like MS 1 in Figure 4, or a single service instance, as is the case for MS 2. No Member State shall have two or more instances.
The lookup interface design documentation to be used for a service instance shall be the same for the European Commission-operated service instance and for any service instance operated by a Member State, following Article 8 of the Implementing Act [REF38]. The life cycle management interface is covered in section 6.5 above and in Chapter 3.

1.2.7 Evidence Exchange and eDelivery

1.2.7.1 Introduction

Evidence exchange in the Once-Only Technical System is based on bilateral exchange between competent authorities. An exchange is always a pair of two correlated messages:

- An evidence request message generated by an Online Procedure Portal in a Member State, supporting a competent authority in the “Evidence Requester” role;
- A corresponding evidence response message generated by a Data Service in one or several other Member States, supporting a competent authority in the “Evidence Provider” role.

For interoperability, the Once-Only Technical System defines in detail the structure and content and message exchange parameters.
This version of the OOTS architecture maps any exchange of a piece of evidence involving preview to a sequence of up to two request-response message loops and an interactive redirect/return user flow.

- In the first message loop:
  - The request message expresses evidence query parameters including the requested type of evidence, the user and the data subject. It does not contain any hyperlink to the Preview Space.
  - If a piece of evidence relating to the user may be available and preview is offered, the response message includes a hyperlink that the user may follow for the Evidence Preview Service. In this case, no piece of evidence is included in the response.
- The second message loop is triggered by the user's decision to follow the presented link:
  - The request message has the same query parameters as the first request message but, in addition, includes the hyperlink provided in the first loop response. This signals to the Data Service that the user is engaging with the Evidence Preview Service and allows the Data Service to coordinate its processing with that service.
  - The response message in this loop includes all and only those pieces of evidence that match the query parameters, identity and any other parameters established in the interactive flow, reflecting user decisions on whether or not to use any matching available pieces of evidence.

The response message in the first message loop can and must be returned instantly to ensure a smooth user experience. By contract, the response in the second message is only returned when the user completes his or her interaction with the Evidence Preview Service.

1.2.7.2 Integration and Service Interaction Patterns

The Once-Only Technical System is based on a number of common patterns identified in technical literature such as Enterprise Integration Patterns [REF18] and Service Interaction Patterns [REF39].
The OOP Technical System uses the **Request-Reply** integration pattern, also known as the **Single-Transmission**, **Round-Trip** service interaction pattern.
The exchange of evidences takes place between competent authorities, but never in isolation or spontaneously, always in response to explicit requests:

- Evidence requests are made by Online Procedure Portals in a Member State in the “Evidence Requester” role;
- Corresponding evidence responses are provided by Data Services in one or several other Member States in the “Evidence Provider” role.

The use of message-based communication components called Access Points in eDelivery is an instance of the **Messaging Gateway** pattern. A gateway is a component that is responsible for the implementation of messaging functionality according to the agreed interoperability design. Reusable Access Points make it easy to enable the use of eDelivery in Online Procedure Portals and Data Services by competent authorities and their service providers.
Access Points also instantiate the **Messaging Bridge** integration. The communication between the Online Procedure Portal and its Access Point and the communication between the Data Service and its Access Point may use different communication protocols and formats, which the Access Point helps bridge.
In a particular step in a procedure, an Online Procedure Portal may issue multiple requests to different Data Services and collect the responses in parallel. In this case, the interaction follows the **Scatter-Gather** with **Distribution List** pattern. The service pattern is also known as the **One-to-many send/receive** service integration pattern and is **Multilateral** rather than **Bilateral**.

1.2.7.3 Evidence Request Response

The evidence request response exchange legs use generic structures based on a specified profile of the RegRep4 open technical specifications [REF27] and Interoperable Europe eGovernment vocabularies. The structures support transport, routing, packaging and correlation.
The request structure includes, following Article 13 of the Implementing Act:

- a unique identification of the evidence request;
- the evidence type that is requested;
- date and time when the request was made;
- identification of the procedure for which the evidence is required;
- name and metadata that uniquely identifies the evidence requester and intermediary platform, where applicable;
- the personal identification data of the user;
- the level of assurance of the electronic identification means used by the user;
- additional attributes used for selection of the evidence provider;
- metadata that identifies the evidence provider;
- an indicator whether or not the user has provided explicit confirmation to request the evidence;
- an indicator whether or not the user is required (by law applicable to the evidence requester) to offer preview that needs to be implemented on the EP side;
- in the second loop, the request also includes the hyperlink of the corresponding Evidence Preview Service.

Optionally, for structured evidences, an identifier of a transformation operation to be applied by the Data Service to the evidence before it is issued to the evidence requester may be included.
In response to a request message, an error message may be returned and no piece of evidence is included, following Article 15(4) of the Implementing Act. This shall include:

- a unique identifier of the error;
- the identifier of the evidence request to which the response relates, to support correlation;
- date and time at which the error was generated;
- a description of the error that occurred.

As a special category of error, in the first request-response loop, in case evidence may be available and is ready for preview, the response includes:

- A hyperlink that the user may follow to interact with the Evidence Preview Service.

The Online Procedure Portal shall recognize this situation and use the provided information to allow the user to navigate to the Evidence Preview Service in the Evidence Provider Member State. This hyperlink shall never be included in errors returned in the second loop, i.e. in response to requests that contain the hyperlink.
In the second request-response message loop, any response that is not an error shall include the following elements:

- a unique identification of the evidence response;
- the identifier of the evidence request to which the response relates, to support correlation;

- date and time at which the response is created;
- identifier code of the evidence requester and intermediary platform, where applicable;
- identifier code of the evidence provider and intermediary platform, where applicable.
- For each evidence included in the response, the response includes:
    - evidence metadata as defined in CCCEV [REF40]:
        - Title; distribution; issuer; issue date; language; validity period.
    - an indication of the transformation applied, if any;
    - the evidence in electronic form;

NB: if the evidence request requested application of a transformation, the attached evidence is the output of the application of the transformation to the evidence. The optional requested transformation allows the requester to receive a more tailored version of the evidence, as explained above in section 6.2. Since this transformation is applied by the Data Service of the Evidence Provider, it is the output of the transformation that is exchanged as the authentic evidence in the Once-Only Technical System. It is protected by the integration and non-repudiation features of eDelivery.
The syntax and semantic of evidence requests and evidence response is covered in the technical design documents [REF20].
Optionally, a Data Service may inform the requester that evidence may exist for the request, but is not yet available.

1.2.7.4 eDelivery

The Once-Only Technical System reuses the eDelivery Building Blocking [REF11] and uses its Acccess Point [REF12] specification. See Figure 5 for an overview of its functions.

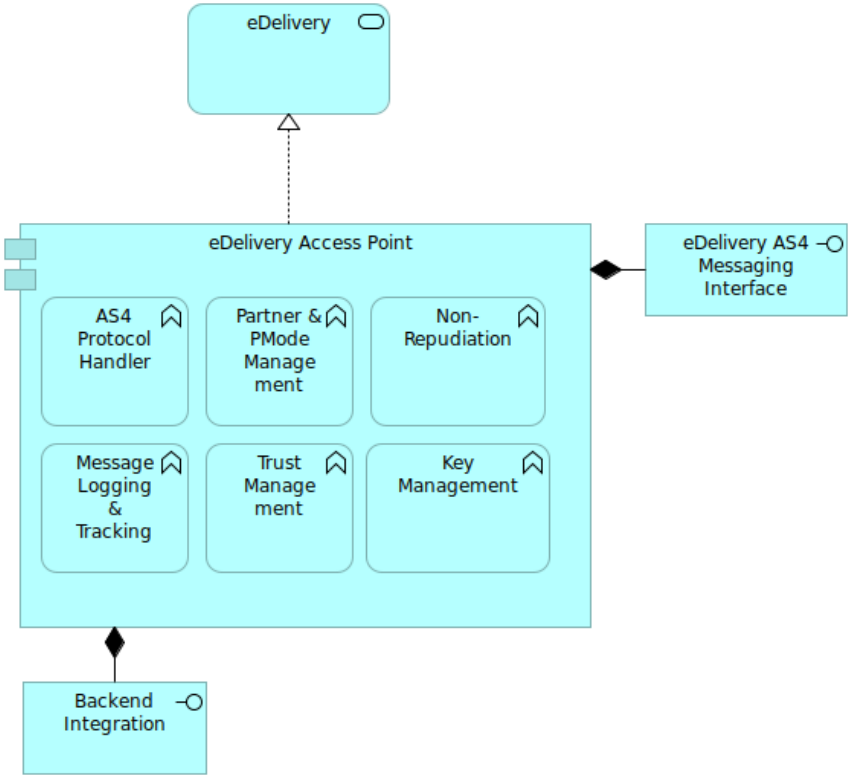


Figure 6 Access Point Application View

An Access Point in the Once-Only Technical System performs key security and reliability functions. It signs and encrypts messages and, in a delegated role, provides integrity, confidentiality, authenticity and non-repudiation of origin and receipt as explained in the Security Controls guidance document [REF14].
As noted above in section 4.3, the competent authority that operates an Online Procedure Portal Access Point has a responsibility to make sure that it only issues evidence requests on behalf of requesting competent authorities that have an appropriate legal basis to make such requests, as required in recital 45 of the SDG Regulation [REF30].

1.2.7.5 Configuration of eDelivery

Evidence exchange uses eDelivery Access Points as provided by the DEP eDelivery Building Block. It uses the ISO 15000 ebMS3 [REF26] and AS4 [REF25] standards profiled as eDelivery AS4 using the so-called four-corner topology profile enhancement [REF13]. The packaging of RegRep4 in AS4 and the values of key AS4 processing mode parameters and associated headers are specified in a separate open technical specification [REF1]. The four-corner topology applies to both the flow of the request from the Online Procedure Portal to the Data Service and the reverse flow from the Data Service to the Online Procedure Portal.

As the four corner topology profile enhancement is used, for an evidence request:

1. The competent authority on whose behalf the evidence request is made is identified as *original sender* (Corner 1).
2. The competent authority that operates the Access point is identified as the sender (the "From" party) of the AS4 message (Corner 2).
3. The competent authority that operates the Access Point for the Data Service is the receiver (the "To" party) of the AS4 message (Corner 3).
4. The competent authority that provides the evidence is the *final recipient* of the message (Corner 4).

Routing of eDelivery messages is handled as follows:

- The Data Service Directory provides both the identifiers of the evidence provider and of its Access Point provider. Therefore, any evidence request message can be routed appropriately, for any identified Data Service.
- Evidence response messages shall be routed in reverse order, i.e. the final recipient value of the response is set to the value of the original sender in the request (*C1 → C4*), the response original sender value is set to the request final recipient value (*C4 → C1*), and the sender and receiver values are swapped *(C2 → C3*; *C3 → C2*).

A single Access Point may serve any number of evidence requesters and/or evidence providers. If a competent authority operates its own Access Point, then:

- Corner 1 and 2 are the same for outbound messages. The value of the AS4 sender header ("*eb:From"*) shall be the same as the value of the *original sender* message property.
- Corner 3 and 4 are the same for inbound messages. The value of the AS4 receiver *("eb:To")* shall be the same as the value *final recipient* message property.

All Access Points that are part of the Once-Only Technical System are statically configured to make evidence requests to, and respond to evidence requests from, all other Access Points. This configuration includes networking (e.g. firewall settings), transport layer security, message layer security (including certificates used for signing and encryption) and all AS4 processing mode configurations including endpoint URIs.

Detailed information on the use of eDelivery in OOTS is provided in 4.7 - eDelivery Configuration - June 2022.

The following diagram shows the integration of eDelivery in the exchange between an Online Procedure Portal and a Data Service. The Data Service Directory provides corner 3 and 4 routing identifier information for the request message. The Data Service reverse routes the response message to the Online Procedure Portal.

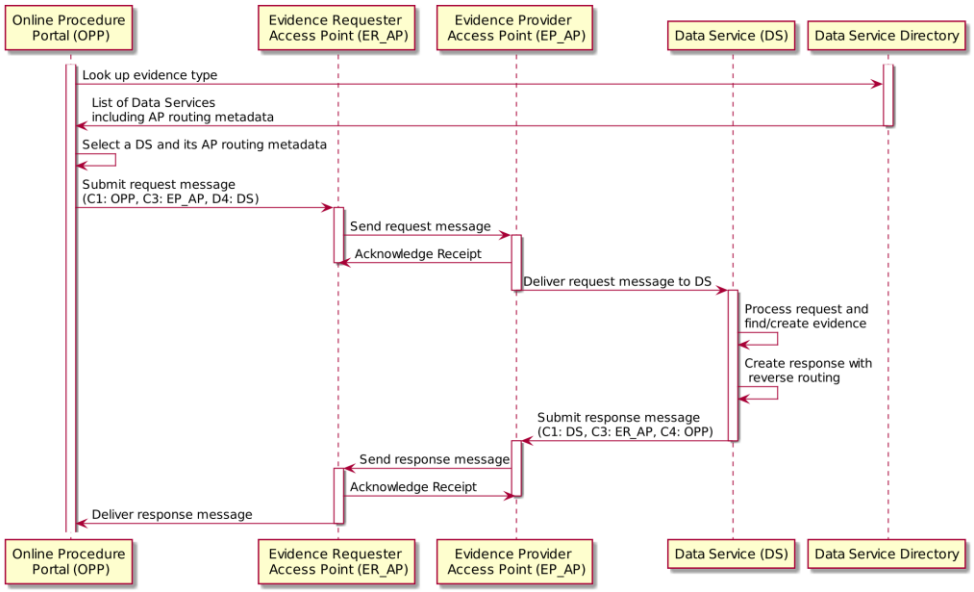


Figure 7 Message exchange and routing using eDelivery Access Points and Data Service Directory

The Once-Only Technical System does not provide end-to-end security:

- Evidence requests and evidence responses are trusted based on the message signature applied by the sending Access Point. The OPP (for requests) and the DS (for responses) do not sign the content that they submit to the Access Point with an expectation that the DS (for requests) and the OPP (for responses) verify the signature. This obviates the need for sharing of signing certificates and agreement on trusted Certification Authorities between competent authorities that use the Once-Only Technical System.
- Evidence requests and responses are encrypted when they packaged and transmitted as eDelivery messages. The OPP (for requests) and the DS (for responses) do not encrypt the content that they submit to the Access Point with an expectation that the DS (for requests) and the OPP (for responses) decrypt the content. This obviates the need for sharing of encryption certificates and agreement on trusted Certification Authorities between competent authorities that use the Once-only Technical System.

Member States are responsible for providing equivalent or better protection of evidence requests and responses in the exchange between Online Procedure Portals, Preview Areas, Data Services, any other intermediary components and their respective Access Points (i.e. between C1 and C2 and between C3 and C4).

Exchange of eDelivery messages between Access Points shall use the public Internet. As specified in the eDelivery AS4 specification, eDelivery is secured at both the transport layer and the message layer. This provides integrity, authentication, confidentiality and non-repudiation of origin and non-repudiation of receipt at a level of protection comparable to the use of a private network.

A Member State may deploy a single Access Point covering all OOP-related eDelivery messaging. Alternatively, it may deploy multiple Access Points at any hierarchical or geographic level of the public administration, in addition to potentially having specialised Access Points for specific domains.
Since the Once-Only Technical System supports interactive use cases, the integration of Access Points to the national systems on the Evidence Requester and Evidence Provider sides must be configured to minimize the latency, for example by avoiding polling interfaces or setting the any polling intervals to sub-second values.

1.2.7.6 Use in complex scenarios

The Once-Only Technical System does not provide any specific functionality beyond the exchange of pairs of evidence requests and responses. There are no mechanisms to link different subsequent uses of the system by the same user. This does not mean that it is not possible or useful to use the system in situations where one procedure is dependent on another procedure.
For example, the system can be used for procedures involving registration and related de-registration. An example of this is shown in the following figure. Here, the user performs a registration procedure in Member State A. The output of this procedure is created as an output of this procedure in a registry in Member State A. The Once-Only Technical System can be used as an input in a separate de-registration procedure in Member State B. (For simplification, the diagram does not include interaction with the Preview Space).

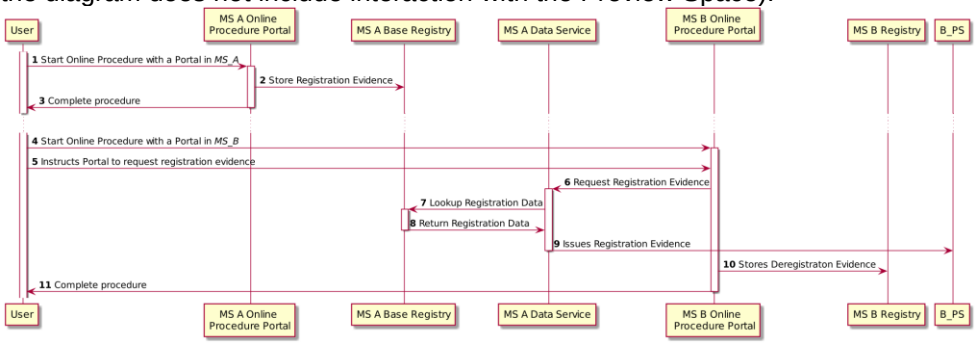


Figure 8 Once-only Technical System supporting registration and Deregistration

Note that this example assumes that the registration evidence is input to the subsequent de-registration procedure. In other situations, the registration procedure may use output from a prior de-registration procedure.

1.2.7.7 Intermediary Platform

In some Member States, some evidences are not provided directly by individual competent authorities but by entities that the Implementing Act calls "intermediary platforms". An intermediary platform is a technical solution acting in its own capacity or on behalf of other entities such as evidence providers or evidence requesters, depending on the administrative organisation of Member States in which the intermediary platform operates, and through which evidence providers or evidence requesters connect to the common services referred to in Article 4(1) or to evidence providers or evidence requesters from

other Member States provide such evidences in a delegated capacity. For example, there may be a dedicated service organisation in a Member State that stores and makes available, on request, educational evidences on behalf of many educational institutions, such as universities. The Implementing Act, Article 1(6), refers to these organisations as Intermediary Platforms.
Use of such a platform may simplify the use of the Once-Only Technical System on the Evidence Provider side:

- Only the Intermediary Platform needs to implement a Data Service for the type of evidences that it makes available;
- Only the Intermediary Platform needs to implement (or connect to) an Access Point and needs to be integrated in the Once-Only Technical System;
- The evidence providing competent authorities that use the Intermediary Platform do not have to join the Once-Only Technical System directly themselves;
- Evidence requesters that look up the provided evidence type in the Data Service Directory will find only one Data Service in the Member State. This means that there is no need to determine which Data Service(s) (potentially among many) to send the evidence request(s) to, and therefore no need to consult the user to select a Data Service.
- Implementation, testing, configuration, maintenance, etc. are all simplified.

An Intermediary Platform may also simplify the use of the Once-Only Technical System on the Evidence Requester side:

- It could provide the functionality of the Once-Only Staging Area to Online Procedure Portals and the competent authorities served by those portals;
- Online Procedure Portals that use the platform do not need to operate client interfaces to the Common Services themselves;
- The platform could implement eDelivery for the Online Procedure Portals by providing (or connecting to) an Access Point.

Whether or not a Member State uses a (or some) Intermediary Platform(s), and which competent authorities should use the (or a particular) Intermediary Platform, is at the Member State's discretion.
An Intermediary Platform also instantiates the **Messaging Gateway** and **Messaging Bridge** integration patterns. In addition to bridging messaging protocols (e.g. eDelivery AS4 to other protocols used within the Member State), functionality provided may include:

- Mapping between national party identifier code systems and cross-border identifier code systems;
- Mapping between data formats, schemas, code lists;
- Mapping between synchronous and asynchronous communication;
- Service Bus connections;
- Aggregation services (e.g. combine information from multiple Data Services).

The concept of an Intermediary Platform is also sometimes known as a "Single Window" or as a "Data Aggregator".

1.2.7.8 Evidence Exchange Logging

To support the OOTS, events related to the use of the system need to be logged. Legal requirements for logging are defined in Article 17 of the draft Implementing Act, with the specifics for evidence exchange being covered in Article 17(1). Due to the OOTS being a distributed system, evidence exchange events occur and are logged in the various components involved in the execution of the evidence request and response flows. The design section on 4.8 - Evidence Exchange Logging - June 2022 further describes the correlation identifiers that are generated and processed in the various components and how they allow end-to-end tracking and tracing.

In OOTS, evidence exchange event logging supports audits and security checks, but also the usual tasks of deployment, integration, testing and operation of parts of the system. The logging of eDelivery event data serves the important additional purpose of non-repudiation of origin and receipt for OOTS evidence exchange.

1.2.7.9 Evidence Exchange integration in Member States

The OOTS uses the four-corner topology model for eDelivery. The profiling of eDelivery AS4 as defined in section 7.5 and in 4.7 - eDelivery Configuration - June 2022 only applies to the cross-border eDelivery message exchange, not to the communication between components within the Member States. Member States have a wide variety of existing national eDelivery systems or other intermediary components based on national standards and infrastructure that may be re-used for OOTS. The details of these national evidence transmission infrastructure are out-of-scope for OOTS, except for the following general requirements:

- The confidentiality, integrity and authenticity of the communication of evidence requests and responses in the exchange between Online Procedure Portals, Preview Are as, Data Services or other intermediary components and their respective Access Points (i.e. between C1 and C2 and between C3 and C4) must be protected at a level that is equivalent to or better than that provided by eDelivery Message Exchange.
- The communication of evidence requests and responses must include all data elements required for enabling logging for end-to-end correlation, tracking and tracing of data flows, in order to support end-to-end tracking and tracing as specified in 4.8 - Evidence Exchange Logging - June 2022.

On the Evidence Requester side, the following additional requirements apply:

- Mechanisms must be in place to ensure that Online Procedure Portals may only request pieces of evidence that are lawful in the context of the electronic procedure that the user is executing.
- Unless the exemption of Article 14(5) of the SDG regulation applies, the Data Service shall not make available any pieces of evidence without preview and approval by the user that the evidence may be used in the procedure.

1.2.8 Identification and Authentication

1.2.8.1 Introduction

The architecture of the Once-Only Technical System reuses the eID building block as it is today. Should the eID building block change, the technical specifications would be adapted to support the changes.

1.2.8.2 eIDAS Node

The use of eIDAS nodes is discussed in sections 4.4 and 5.5. The purpose, use and specifications of eIDAS Nodes are specified in the existing, separate eID Building Block [REF17]. They are reused in the Once-Only context.

Note that in some procedures, for some users, a national eID that has been notified may be used without the need to use the eIDAS Node. This is the case for a user that executes a procedure in Member State A, has a national eID issued by MS A but wants to use evidence from MS B. This is an option irrespective of the nationality of the user as Member States may notify eID schemes that issue eID means also to foreigners. In order to be used the eID means from MS A must be issued under an eID scheme notified according to Article 11(1) of the Implementing Act .
Note that eID means issued under notified eID schemes may differ in level of assurance and that the Online Procedure Portal and Evidence Provider define which level they expect.
The Once-Only Technical System distinguishes the identity and authentication of natural persons and legal persons, if supported by the eID service used.

1.2.8.3 Identification and authentication

In the execution of an electronic procedure, there are two situations in which the user can be identified and authenticated:

- to use the procedure;
- to use the Once-Only Technical System to retrieve a particular evidence.

Identification and authentication performed by the Evidence Requester must use electronic identification schemes that have been notified by a Member State in accordance to Regulation (EU) No 910/2014. If the access to the procedure has been granted without the fulfilment of this requirement, the Evidence Requester must ask the user to re-authenticate taking into account the previously mentioned requirements before using OOTS.
The mandatory attributes of the eIDAS minimum data set obtained as a result of a successful authentication at the Evidence Requester side, as described above, are added to the evidence request.

The mandatory attributes of the eIDAS minimum data set, with the exception of the Unique Identifier, must always be provided in the evidence request, together with the Level of Assurance. When the Unique Identifier is derived receiving-MS-specific, it means that the Unique Identifier changes for each Member State. Therefore the Unique Identifier obtained by the Online Procedural Portal is specific to the Member State of the Online Procedure Portal and should not be used in another Member State. The information about the Unique Identifier is communicated during the notification process and more information is available here. Additionally, this information could be provided by the eIDAS Cooperation Network. The Data Service may rely on person identification data received or choose to ask the user to re-authenticate. If the user is re-authenticated, the Data Service must ensure that the attributes received match the ones that ones held by them. More details on this can be found in 2.1 - Identity and Record Matching - June 2022.

1.2.8.4 Identity Matching

As part of user identification and authentication, a relying party commonly wants to know whether the claimed identity can be found in their records as an identity who is authorised to access that service or data. In the use of electronic procedures, such identity matching may be needed at two points in time:

1. When the user authenticates in order to interact with the Online Procedure Portal. This authentication involves the use of notified eID and depending on the issuing Member State the use of eIDAS nodes. This step is typically needed for any interaction with an electronic procedure, including interactions that do not involve the use of the Once-Only Technical System.
2. As part of the processing of an evidence request by a Data Service in the context of the Once-Only Technical System. This could be done using the identity attributes received in the evidence request or by requiring the user to re-authenticate.

Note that the eIDAS minimum data set may not be enough to properly identify a foreign user according to national rules. Therefore, the ability to request additional attributes should be used to make sure sufficient disambiguating information is available.
The identity matching functionality needed for authenticating the user to an online service may be part of the functionality of an interactive service or it may be provided by a dedicated (typically centralised) **Matching Service**. How this is implemented for a Data Service is up to the Data Service, taking into account the national set-up.

1.2.8.5 Representation

Several of the procedures listed in Annex II of the SDG regulation are procedures about legal persons. In these procedures, Evidence Requesters typically need to be able to authenticate a legal person (legal person as defined in Article 3(3) of Regulation EU No 910/2014) or establish that the user has the power to represent the legal person (natural person representing a legal person as defined in Article 3(3) of Regulation EU No 910/2014) in the electronic procedure in order to be able to proceed with the application. This requirement applies whether or not any evidences are exchanged in the electronic procedure and is therefore independent and separate from the Once-Only Technical System.
The Online Procedure portal shall rely on electronic identification means defined in Article 3(2) of Regulation (EU) 910/2014 issued under the electronic identification schemes notified in accordance with that Regulation. The identity attributes obtained as a result of eIDAS authentication of legal person or natural person representing a legal person will be included in the evidence request. The Data Service may use these identity attributes for the identity and record matching or it may choose to re-authenticate. In case of the latter, the Data Service must ensure that the identity attributes received match the identity attributes retrieved during the re-authentication.

1.2.8.6 Additional OOTS eID security services

Once-only toolbox offers the competent authorities in a Member State to use in their implementation of the Once-Only Technical System opt-in elements, amongst which there are eID additional security services:

- An authentication verification service that a Data Service can use to verify that the user identity attributes in the evidence request link to a recent eIDAS authentication transaction.
- Authorization of requests for evidence relating to represented persons.

Data Services may benefit from an **authentication verification service** that allows them to verify that an eIDAS authentication took place for a user. The verification shall match the provided identity attribute values and indicated level of assurance in the evidence request, make sure that this authentication took place sufficiently recently to be plausibly related to a single user session and was made by the user for the execution of an electronic procedure in the scope of the SDG. This opt-in feature could be used in the case where the Data Service would like to rely on the person identification data received from the Online Procedure Portal, without re-authentication.
A Data Service, should the national set-up allows it, may benefit from a service (for example, a Mandate Management Service) that can validate whether the representative is authorized to obtain evidence for the represented person.

1.2.9 System Operation

1.2.9.1 Introduction

To support the operation of the technical system, additional constraints need to be adhered to.

1.2.9.2 Log System

The legal base for logging in the technical system is provided in Article 17 of the draft Implementing Act.
The approach to logging in the technical system reflects its distributed nature.
The actors performing logging are:

- Member States as evidence requesters and providers
- Commission (and some Member States) as provider of common services

The information to be logged is:

- Evidence request metadata
- Evidence response or error metadata
- eDelivery event data (message sent, received, acknowledged, acknowledgment received, any errors)
- Use of common services

Confidentiality, integrity and availability of the logs need to be applied. Note, however, only evidence request metadata includes personal information.

1.2.10 Sample Once-Only Flows

1.2.10.1 Sample Flow

The sequence diagram in Figure 10 shows a sample execution flow of a procedure where the user involved uses the Once-Only Technical System. It is provided as an illustrative example only.[2] The diagram assumes "Once-Only"-specific functionality on the Evidence Requester side is handled by a separate **Once-Only Staging Area** sub-portal. The diagram shows a single successful flow. At many stages there is more than one potential next step, including error situations, which are not shown in the diagram - the diagram shows only ideal user progress through the system. Furthermore, the use of eDelivery (using Access Points) is omitted from the diagram. Refer to chapter 7 to see how use of eDelivery Access Points can be represented.

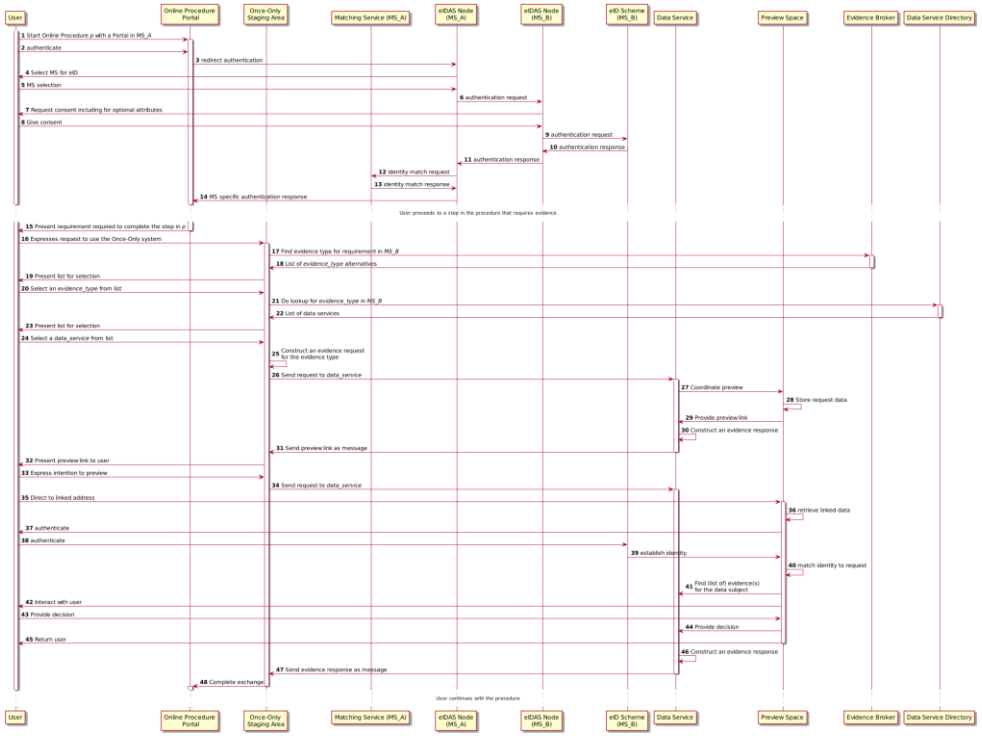


Figure 10 Once-Only Technical System Flow

The diagram shows an approach that maximises interaction with the User. This goes beyond the strict requirements of Article 14, which only mandates the preview feature, but it follows the principle of giving the user full control of their evidence when interacting with the Once-Only Technical System.
The following table provides more in-depth explanations of each step in the sequence.

Step	Description	Notes
1	Unless otherwise provided for under Union or national law, any Once-Only operation only starts when a user initiates an electronic procedure provided by an Online Procedure Portal in a Member State. The procedure may involve many different steps and a complex logic, potentially involving conditional branching, loops, etc.	The User may have found the Portal via the “Your Europe” portal, or some other way. It is not important for the functioning of the Once-Only Technical System.
2-14	The User is authenticated, as such authentication is a pre-condition to the use of the Once-Only Technical System. In this example, the User uses an eID from another Member State, Member State B, and is authenticated using the eIDAS nodes.	If the user has a notified eID from Member State A, in which the requesting competent authority is based, the user could also use that eID. In that case, the eIDAS nodes are not used. The Member State selection functionality, step (4)- (5), in this example is offered by the eIDAS Node in Member State A. As stated in section 4 of the eIDAS Interoperability Architecture V1.2., the eIDAS connector SHALL offer this functionality if this was not already pre-selected by the relying party (Online Procedure Portal). The user consent, set (7) - (8), concerning the identification attributes to be exchanged, is MS specific and not described by the eIDAS interoperability framework. Therefore, it is up to each Member State to decide how this is implemented. To be noted that in order to support the identity matching process for both the Online Procedure Portal and Data Service, the user may be asked to give consent for the exchange of the optional attributes of the eIDAS minimum data set, attributes that are made available by MS B, provided this is allowed by national law. For simplicity purposes , the following simplifications have been made to the diagram: • Steps 12-13: the eIDAS node encompasses together the different roles/functionalities of eIDAS connector, eIDAS Proxy-Service and the Member State specific part, depending on the case it is used. Therefore, it is the Member State specific part of the eIDAS node that is connected to the Matching Service in Member State A. It should not be understood that the standard eIDAS node provides an interface with the Matching Service nor does it exclude the existence

		of other components that may be connected in-between , like a national authentication service. • Step14: it is the Member State Specific interface that sends back the response and it does not preclude the existence of other components that may be connected in-between , like a national authentication service. The identity matching functionality needed to authenticate the user to the online service may be part of the functionality provided by the relying party (the Online Procedure Portal) or it may be provided by a dedicated (typically centralized) **Matching Service**. Therefore, this example presents separately the "Matching Service" which is integrated with the Member State specific interface of the eIDAS node of Member State A. The eIDAS authentication response is used by the Member State specific part in the eIDAS Node in Member State A to create the reply, step (14), for the Online Procedure Portal.
15	In the execution of the procedure, the User may arrive at a point where evidences need to be provided to fulfil certain information requirements or to prove that certain conditions have been met. For example, the procedure "*apply on-line for a tertiary education study financing*" may require "*proof of any existing qualifications for tertiary education*". At this point, the portal may interact with the User to obtain evidence that proves the requirement. The Portal may support multiple ways to provide this evidence. For evidence that is available using the Once-Only Technical System, the Portal may ask the User to indicate in which (if any) other Member State(s) such evidence can be found.	Step (15) – (48) could be repeated for each of the points in the procedure at which evidence is to be provided.
16	The User indicates that he or she wants to use the Once-Only Technical System to have evidence retrieved from Member State B.	This flow assumes the interaction of the user with the Once-Only Technical System on the Evidence Requester side is handled by a separate Once-Only Staging Area sub-portal. The user is directed to this sub-portal to complete the evidence exchange. This is an implementation choice, not a requirement of OOTS.

		The sample Portal asks the user to specify from which Member State the evidence is to be requested. Alternatively, the Portal may query all Member States, but this is not recommended as it would result in a large amount of unnecessary queries.
17	The Once-Only Staging Area, with this User-provided information, proceeds to consult the Evidence Broker to check which types of evidence should be selected from the specified Member State.	The sample flow assumes the portal is designed to use the Evidence Broker. For some procedures and/or evidence types, Member States may have agreed on a predefined set of harmonized evidence types, or the Portal may know from other sources which specific evidence types it accepts from the other Member State. In that case, no interaction is needed with the Evidence Broker.
18	In response, the Evidence Broker indicates that in Member State B, from which evidence is being requested, the information requirement can be met using either evidence type *ET1* or evidence type *ET2.* For example, a structured electronic diploma based on the EDCI data model [REF10] or another evidence type.	
19	The Once-Only Staging Area displays the results of its interaction with the Evidence Broker and asks which (if any) of the evidence types should be requested.	The portal takes advantage of the fact that the User may know which evidences are or aren't available. This may avoid some unnecessary queries. The Portal may also simply query *ET1* and/or *ET2,* without asking for user input, skipping steps (19) and (20).
20	In this sample flow, the User knows that only type *ET2* is available and therefore indicates that evidence type *ET1* does not have to be requested.	Note that the user may still select more than one option.
21	Now that the evidence type to be requested and the Member State holding it have been identified, the Portal can consult the Data Service Directory to determine which competent authorities in the Member State provide this type of evidence.	If the Member State is not known, the Portal may also search for Data Services in any Member State. However, in practice the number of Member States where a User may have relevant evidence is likely to be small, so this would create a large amount of unnecessary message traffic and system load.
22	The Data Service Directory returns a list of Providers of the selected evidence type.	

23-24	Similarly to (17)-(18), the Portal may allow the User to select one or a subset of items from the list. For example, if individual educational institutions in a Member State are separate Data Services, the list could be quite long, and the User could indicate which of them may hold evidence.	If there is only one Data Service for the evidence type in the Member State, the check with the User should most likely be omitted. It is still possible to query all Data Services, but, as before, it could result in many unnecessary requests.
25	For the selected Data Service(s) in the selected Member State(s), a request is constructed using the evidence exchange data model and format [REF20]. This request is subsequently sent to the Data Service.	Steps (25)-(48) need to be repeated for each selected provider of each selected evidence type. Due to the preview functionality, there are two separate request-response loops.
26, 31, 34, 47	The request and response messages are exchanged using eDelivery.	The diagram omits the use of Access Points and the details of the use of eDelivery.
26-29	The Data Service and the Preview Space coordinate to create a link to be communicated to the user in order to initiate his or her evidence preview and selections.	The syntax and semantics of the link are out of scope for this specification and left to Member State implementations. The Preview Space shall generate a unique, time-limited URL that is linked to the specific data subject and a specific unique electronic procedure session, so that, when the user visits the link, the user's decisions and the evidence request are linked unambiguously and securely to the corresponding evidence request and response.
28	Request parameters including the requesting competent authority, the requested evidence type, the requested evidence provider, and identity attributes of the user are recorded.	This is a preparatory step for steps (40) and (41). Note that this is an internal implementation step at Member State discretion.
31-33	The link and associated information are transmitted back to the Online Procedure Portal using an eDelivery response message and presented to the user.	At this stage, the user still remains under no obligation to follow the link to the Preview Space.
33-35	The user expresses her intention to preview the piece of evidence. This triggers two actions: 1. The user is directed to the Preview Space (step 37). 2. In the background, a second follow-on eDelivery request message is sent to the Data Service (step 38).	This diagram assumes that the Preview Space is a dedicated component, linked to but separate from the Data Service. This is an internal implementation step at Member State discretion. The functionality could be integrated in the Data Service. The evidence request sent in the eDelivery message in step 37 differs from the earlier request in step 28 in that it includes the hyperlink to the Preview

		Space. This signals to the Data Service that the user may, in parallel, be visiting the Preview Space and that the content of the response to be generated depends on the user's actions. To prepare for the user's return (step 47), the Once-Only Staging Area should append a return address URL as a parameter to the request. This parameter is to be recorded by the Preview Space for the duration of the session.
36	When the user accesses the Preview Space using the selected link, the Preview space retrieves data previously stored in step 31.	This allows the Preview Space to determine which type of evidence the user requests, from which Provider, for which Requester, and the identity attributes included in the earlier evidence request.
37	The Preview Space requests the user to re-authenticate.	Even if the link is unique for a specific user, time-limited and exchanged using a secure TLS connection, the Preview Space is likely to want to securely determine the identity of the user. Note, however, that this is an internal implementation decision of the Member State. In case the identity attributes were not unique for a specific person, re-authentication also serves disambiguation. Re-authentication may provide additional identity attributes that were not shared using eIDAS but are necessary for record matching.
38-39	The user re-authenticates.	In this sample flow, the user has an eID for Member State B. There is therefore no use of the eIDAS nodes.
40	Match identity to request	By comparing the identity attributes for the user established through re-authentication to the identity attributes included in the request (stored in step 30), the Preview Space prevents (potentially erroneous or even fraudulent) situations in which the user uses a different identity on the Evidence Provider side than one the Evidence Requester.
41	In conjunction with the Data Service, the Preview space finds a (list of) piece of evidence for the data subject of the requested type.	The identity information from the Preview Space is used to make sure only pieces of evidence for the data subject are retrieved.
42-43	Interact with user	This interaction includes, for each piece of evidence: • Giving the user the option to previewing the piece of evidence.

		• Determining whether or not to use the piece of evidence.
44	Provide decision	The decision of the user, made in the preview space, is to be shared with the Data Service, so that the Data Service knows which if any piece(s) of evidence to return.
45	Return user	The return URL parameter appended to the URL used in step 37 is used. This URL should allow the user to resume his or her activity from where she left off.
46-47	Construct evidence response and send the evidence response as a message	The Data Service, taking into account the user's decisions, constructs the evidence response and returns it via the secure eDelivery channel.
48	Complete exchange	At this stage, the user has finished his or her OOTS interaction, the evidence is transferred and the user can return to the procedure. Following the common practice of showing a final "shopping cart check out" page that users know from electronic commerce, the Once-Only Staging Area may present the results of all OOTS interactions, for possibly multiple pieces of evidences, before returning the user. This is an implementation choice at Member State discretion.

[1] The sources of all Archimate models in this document are publicly available at https://ec.europa.eu/digital-building-blocks/code/projects/OOP/repos/hla/browse.
[2] The sources of all UML models in this document are publicly available at https://ec.europa.eu/digital-building-blocks/code/projects/OOP/repos/hla/browse.

2 Chapter 2: User Identification, Authentication and Record Matching - June 2022

User Identification, Authentication and Record Matching - June 2022

Summary
In the execution of an electronic procedure, there are two situations in which the user has to be identified and authenticated:

- to use the procedure and;
- to use the Once-Only Technical System to retrieve a particular evidence for use in that procedure.

The Once-Only Technical System uses the eID Building Block, as it is today, to identify and authenticate the user. Should the eID building block change, the technical specifications would be adapted to support the changes. Specifically, it uses the assured eIDAS user identity attributes obtained from the user authentication in evidence requests. It may also be used by the Data Service if the user is asked to re-authenticate.
Besides the eIDAS attributes, additional attributes may be requested from the user for the purpose of identification of the relevant Evidence Provider. These attributes, should they be needed, are listed in the DSD and would be included in the evidence request. Both the DSD and the evidence request must make a clear distinction between the two different types of attributes.
The eIDAS attributes that are included in the evidence request are the mandatory attributes of the minimum data set, with the exception of the Unique Identifier when it is receiving Member State specific.
The Preview Space may choose to re-authenticate the user but would need to ensure that the person identification data received matches the one held by them.
The Data Service could rely on the person identification data received in combination with additional security features:

- An authentication verification service that a Data Service can use to verify that the user identity attributes in the evidence request link to a recent eIDAS authentication transaction.
- Authorisation of requests for evidence relating to represented persons.

Note that given the constraints of the current eIDAS regulation and its implementation, there are situations in which a user cannot be granted access to a service immediately. For example, some Member States have manual processes to match users that have not previously accessed their services using eIDAS. These Member States may be unable to process evidence requests dynamically in similar situations.
The chapter includes the following sub-chapters:

Change log
For this release, the changes for all chapters are combined at the top level

2.1 Identity and Record Matching - June 2022

2.1.1 Introduction

As a general rule, only users authorised to access data should be able to access that data. When a user requests access to data, the Data Service and other services on the Evidence Provider side need to identify a user that was authenticated by the requesting Online Procedure Portal. This can be done by comparing the claimed identity to the identities that are authorised to access that particular data or by requesting the user to re-authenticate. The re-authentication will be performed following the same principles as described in article 6 of Regulation (EU) No 910/2014. In both cases, if a unique successful match is identified, access can be granted, if not, access is not granted.

Where users wish to use OOTS for exchanging evidences, the access to these evidences should be restricted to evidences for the identified and authenticated user, who is acting either on their own behalf or through a representative, and who is interacting with the Online Procedure Portal and made the evidence request. Therefore, when processing evidence requests, the Data Service needs to make sure that the user, acting directly or through a representative, has access only to evidences related to that specific user. Identity and record matching on the Data Service side can be performed based based on:

- mandatory attributes of the eIDAS minimum data set as defined by Commission Implementing Regulation (EU) 2015/1501 : a matching service will use person identification data that is retrieved using eIDAS authentication on the Online Procedure Portal side OR,
- re-authentication of the user taking into account the Data Service requirements for authentication.

When using an eID means issued under an eID scheme notified under eIDAS for user identification, the eIDAS attributes that can be used are the attributes of natural, natural representing legal or legal person. The eIDAS attributes included in the notification process will have the same level of assurance as the eID means used by the user in eIDAS authentication. If these attributes are not sufficient for identity and record matching, the Data Service may require the user to re-authenticate. If the user is re-authenticated, the Data Service must ensure that the mandatory attributes of the eIDAS minimum data set included in the evidence request match the attributes held by them.

2.1.2 Use of eIDAS

2.1.2.1 Use of eIDAS attributes in OOTS

The Annex of the Commission Implementing Regulation (EU) 2015/1501 lists the attributes of the eIDAS minimum data set. The list is comprised of **mandatory attributes,** attributes which must always be requested and provided, and **optional attributes** ("additional attributes") which may be provided if available. Other attributes beyond the minimum data set, referred to as "sector specific" in section **2.7. Sector specific attributes** of eIDAS Attribute Profile - Version 1.2, may be described by Member State and domain experts and further included in the eIDAS Node metadata.

In addition to the *mandatory attributes* of the eIDAS minimum data set, the Online Procedure Portal may request optional attributes of the eIDAS minimum data set, together with the available sector specific attributes, if it is allowed by the national law and the user gives their consent. This is usually done in order to increase the success rate of identity and record matching. Only the *mandatory attributes* of the eIDAS minimum data set shall be included in the evidence request, with the exception of the Unique Identifier if it is derived receiving Member State specific.

The eIDAS means used in the eIDAS authentication has a Level of Assurance which will be linked to the eIDAS assertion.This Level of Assurance will be included in the evidence request.

Neither the evidence requester nor the evidence provider shall store or use the person identification data, beyond the scope expressed in the consent for the purposes of the evidence request.

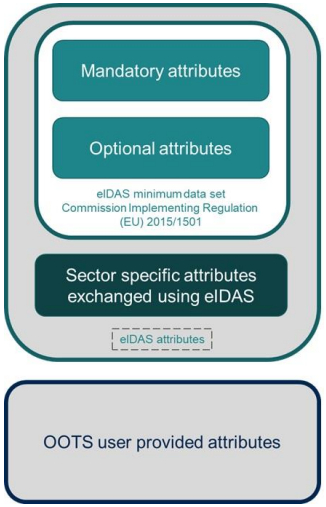


Figure 1. Person identification data used in OOTS

2.1.2.2 Mandatory attributes of eIDAS minimal data set for Natural Persons

Mandatory attributes of the eIDAS minimum data set must always be requested and provided during the eIDAS authentication.

Attribute (Friendly) Name	eIDAS MDS Attribute	ISA Core Vocab Equivalent	Notes
FamilyName	Current Family Name	cbc:FamilyName	Encoded as xsd:string
FirstName	Current First Names	cvb:GivenName	Encoded as xsd:string

Attribute (Friendly) Name	eIDAS MDS Attribute	ISA Core Vocab Equivalent	Notes
DateOfBirth	Date of Birth	cvb:BirthDate	Encoded as xsd:date
PersonIdentifier	Unique Identifier	cva:Cvidentifier	Encoded as xsd:string

Mandatory attributes of the eIDAS minimum data set for Natural Persons, eIDAS SAML Attribute Profile V1.2. , 31 August 2019

These attributes will be further included in the evidence request, with the exception of the Unique Identifier if it is derived receiving Member State specific. For more information on the Unique Identifier see the next section.

2.1.2.3 eIDAS Unique Identifier

Identity matching is typically done by looking up and matching the identity received with the identities registered. For this purpose, the eIDAS Unique Identifier (eIDAS UID) can only be directly used if it is already known by the Evidence Provider. This may be true in cases where the Evidence Provider has already linked the eIDAS UID to a known identifier or has access to such record.

The eIDAS UID is a mandatory attribute, and its definition is defined in the **eIDAS SAML Attribute Profile.**

Extract from eIDAS SAML Attribute Profile v1.2., 31 August 2019
"*The unique identifier consists of:*
1. The first part is the Nationality Code of the identifier
- *This is one of the ISO 3166-1 alpha-2 codes, followed by a slash (“/“))*

2. The second part is the Nationality Code of the destination country or international organization
- *This is one of the ISO 3166-1 alpha-2 codes, followed by a slash (“/“)*

3. The third part a combination of readable characters
- *This uniquely identifies the identity asserted in the country of origin but does not necessarily reveal any discernible correspondence with the subject's actual identifier (for example, username, fiscal number etc)*

Example: ES/AT/02635542Y (Spanish eIDNumber for an Austrian SP)"

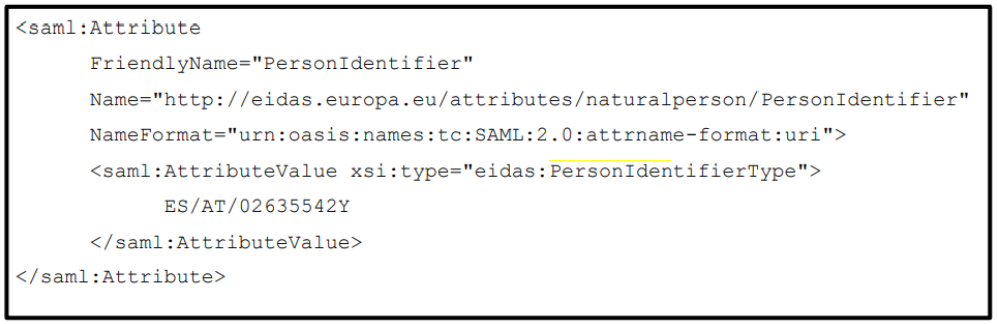


Figure 2: example PersonIdentifier attribute value

Figure 2 from eIDAS SAML Attribute Profile v1.2., 31 August 2019

Some Member States issue an outbound identifier for each Member State, which is also usually derived. This means that the third part of the Unique Identifier, the combination of readable characters, may not have the same value for all requesting Member States. Taking the above example, the identifier for the user authenticating in Austria can be "*ES/AT/02635542Y*", however, when authenticating in Belgium, it would not only have a different Nationality Code of the destination country, but also a different third part, resulting in, for example: "*ES/BE/03835542X".*

This means that in such cases, the eIDAS UID (PersonIdentifier) was issued for the specific context of the Online Procedure Portal and it cannot be used by the Data Service. In this case the Online Procedure Portal should not send the Unique Identifier to the Data Service.

How these outbound identifiers are generated, is specific to each Member State and/or eID means. The derivation process could potentially make it challenging even for a matching function from the issuing Member State to identify the user based only on this identifier. Additional attributes may be needed.

The information on the Unique Identifier, if it is derived and/or receiving Member State specific is communicated during the notification procedure and in the following resource. This information could be requested to the eIDAS Cooperation Network and configured accordingly. More examples on how Unique Identifier could be used by a Data Service and its matching service can be found in section *6. Examples Unique Identifier and Data Service identity matching (Informative).*

2.1.3 eIDAS optional and sector/additional specific attributes for Natural Person

In cases where the mandatory attributes of the eIDAS minimum data are not sufficient to identify a unique user, identity matching may need to rely on other attributes.

Users can reduce the ambiguity and therefore increase the likelihood of unambiguous record matches by agreeing to exchange more attributes.

Optional attributes of the eIDAS minimum data set if they are available, may be requested by the Online Procedure Portal in order to increase the success rate of identity and record matching. The decision to request these attributes belongs to the Online Procedure Portal and may be based on the national identity matching requirements.

These optional attributes would not be further sent as part of the evidence request to the Evidence Provider.

Attribute (Friendly) Name	eIDAS MDS Attribute	ISA Core Vocab Equivalent	Notes
BirthName	First Names at Birth	cvb:BirthName	Encoded as xsd:string
BirthName	Family Name at Birth	cvb:BirthName	See above re birth names
PlaceOfBirth	Place of Birth	cva:BirthPlaceCvlocation	See above re birth names
CurrentAddress	Current Address	cva:Cvaddress	Encoded as multiple xsd:string elements
Gender	Gender	cvb:GenderCode	Encoded as xsd:string with a restriction of selection: Male, Female, Unspecified

Optional attributes of the eIDAS minimum data set for Natural Person, eIDAS SAML Attribute Profile V1.2., 31 August 2019

(eIDAS-provided) Sector specific/additional attributes (non eIDAS minimum data set) that can be provided via eIDAS could similarly be requested in order to increase the success rate of identity and record matching provided that the user has given her/his consent. The Online Procedure Portal could request these attributes but they would not be sent further to the Evidence Provider as part of the evidence request.

The sector specific attribute schema must be defined and published in-line with section *2.7. Sector Specific Attributes* of ***eIDAS SAML Attribute Profile***, currently at version 1.2. More information on all eIDAS available attributes of pre-notified and notified eID schemes can be found here.

2.1.3.1 eIDAS attributes for Legal Persons

Mandatory attributes of the eIDAS minimum data set must always be requested and provided during the eIDAS authentication.

Attribute (Friendly) Name	eIDAS MDS Attribute	ISA Core Vocab Equivalent	Notes
LegalName	Current Legal Name	cvb:LegalName	Encoded as xs:string
LegalPersonIdentifier	Uniqueness Identifier	cvb:Cvidentifier	Encoded as xs:string

Mandatory attributes of the eIDAS minimum data set for Legal Person, eIDAS SAML Attribute Profile V1.2., 31 August 2019

In addition to these mandatory attributes, section 2.3.1 of the eIDAS SAML Attribute Profile v1.2 lists eight optional attributes that MAY be supplied by a MS if available and acceptable to national law.

Attribute (Friendly) Name	eIDAS MDS Attribute	ISA Core Vocab Equivalent	Notes
LegalAddress	Current Address	cva:Cvaddress	Encoded as multiple xsd:string elements
VATRegistration	VAT Registration Number	cva:CvbusinessCode	Encoded as xsd:string
TaxReference	Tax Reference Number	cva:CvbusinessCode	Encoded as xsd:string
BusinessCodes	Directive 2012/17/EU Identifier	cva:CvbusinessCode	Encoded as xsd:string
LEI	Legal Entity Identifier (LEI)	cva:CvbusinessCode	Encoded as xsd:string
EORI	Economic Operator Registration and Identification (EORI)	cva:CvbusinessCode	Encoded as xsd:string
SEED	System for Exchange of Excise Data (SEED)	cva:CvbusinessCode	Encoded as xsd:string
SIC	Standard Industrial Classification (SIC)	cva:CvbusinessCode	Encoded as xsd:string

Optional attributes of the eIDAS minimum data set for Legal Person, eIDAS SAML Attribute Profile V1.2., 31 August 2019

The processing of mandatory and optional attributes for legal persons is done analogously to the processing of mandatory and optional attributes for natural persons.

Only the mandatory attributes of the eIDAS minimum data set are sent in the evidence request.

For more information on using the OOTS for evidences related to legal persons, see 2.3 - Representation - June 2022.

2.1.3.2 2.6 eIDAS attributes for Natural Person representing Legal Person

Article 3(1) of the Regulation (EU) No 910/2014 allows the case of representation, in particular "natural person representing a legal person". Because in reality there are more cases of representation, the eIDAS Technical subgroup has been requested by the eIDAS Cooperation Network to amend the technical specifications to include all the cases of representation.

2.8. NATURAL AND LEGAL PERSON REPRESENTATIVE

The eIDAS Regulation allows for representation of persons as described in Article 3 (1), which explicitly states this as "a natural person representing a legal person". In practice this representation is not limited to this scenario but may also include other representation such as a natural person representing another natural person. This has been elaborated on in the eIDAS Cooperation Network where the European Commission presented "*... the idea of covering all scenarios of representation.*" The Cooperation Network discussed whether the scope and limitations of representation, like limited powers of representation or restriction to certain actions, should already be covered. The conclusion was that such limitations should not yet be included in the attributes and that "*... the scope and limitation should be covered by separate documents or processes*". The European Commission "*... confirmed there was a legal basis stemming from the implementing decision.*" (quotes taken from the minutes of the 3rd eIDAS Cooperation Network meeting June 20th, 2016) and the technical subgroup was asked to amend the specification to cover all scenarios of a natural persons or a legal persons representing another natural person or a legal person.

Figure 4. Section 2.8. NATURAL AND LEGAL PERSON REPRESENTATIVE from eIDAS SAML Attribute Profile V1.2., 31 August 2019

Even if the representative attributes MUST not be explicitly requested, the eIDAS response MAY however return one representative attribute set in case of representation.

The representative attributes follow the specifications of natural person (*2.2 Mandatory attributes of eIDAS minimal data set for Natural Persons*) and legal person (*2.5 eIDAS attributes for Legal Persons*) as described in the *eIDAS SAML Attribute Profile V1.2., 31 August 2019* and they need to be pre-fixed with "**Representative**".

2.1.4 Authentication and re-authentication

2.1.4.1 Authentication

In the context of the SDG, identification and authentication of the user serve two separate purposes:

- to use the procedure;
- to use the once-only technical system to retrieve a particular piece of evidence.

Identification and authentication performed by the Online Procedure Portal must use electronic identification schemes that have been notified by a Member State in accordance to Regulation (EU) No 910/2014. If the access to the procedure has been granted without the fulfillment of this requirement, the Online Procedure Portal must ask the user to authenticate taking into account the previously mentioned requirements before using OOTS.

The Online Procedure Portal includes the mandatory attributes of the eIDAS minimum data set retrieved during the eIDAS authentication at the Online Procedure Portal side in the evidence request to be sent to the Evidence Provider. This information should be accompanied by the level of assurance of electronic identification means used. The Unique Identifier shall not be sent if it is Member State specific as explained in section 2.3. Unique Identifier.

2.1.4.2 Re-authentication

This version of the OOTS provides a 4.9 - Evidence Preview - June 2022 feature in which the user interacts, using redirection, with a service provided by, or on behalf of, the Data Service, and therefore a service offered from the Member State of the Evidence Provider. The component offering the service is called Preview Space. As the operation of the Preview Space is coordinated with the operation of the Data Service, the Preview Space has access to all identity attributes provided by the user that are included in the evidence request. At this stage, the Preview Space and Data Service need to determine if the personal identification data provided is sufficient for the purposes of identification and authentication or if there is the need to re-authenticate. When re-authentication is required, the principles set by article 6 of Regulation (EU) No 910/2014 must be enforced. This means that the user would be asked to re-authenticate using one of the below options:

- eID schemes from the Member State of the Evidence Provider, which are deemed adequate for the access to the Evidence Providers' services. This includes both notified and non-notified eID schemes.
- eID schemes notified by other Member States in accordance to Regulation (EU) No 910/2014.

When re-authentication occurs, the Data Service must ensure that the person identification data received match the attributes held by them as follows:

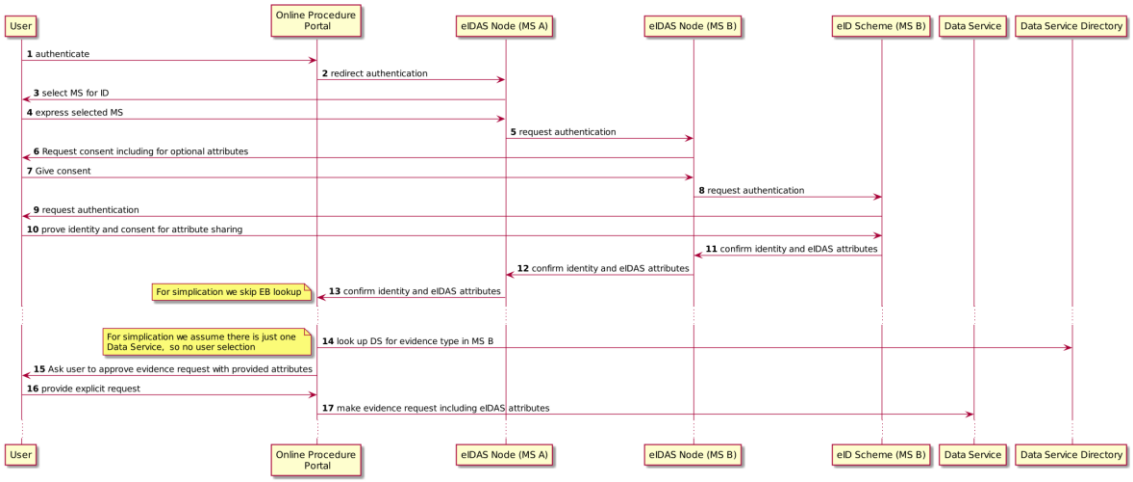
Type of person	Checks performed
Natural person	MUST ensure that the identity and record matching, was done based on the same value of the First Name, Last Name and DoB;

Type of person	Checks performed
	If the Unique identifier is sent and if the Data Service has the information about the account used by the user (e.g. the account corresponds to an eID means issued by the same Member State), it MAY perform additional checks in the process or following the re-authentication and identity matching on the Data Service side.
Legal person	MUST ensure that the identity and record matching, was done based on the same value of the LegalName, LegalPersonIdentifier (if sent);
Natural person representing legal person	MUST ensure that the identity and record matching, was done based on the same value of LegalName, LegalPersonIdentifier (if sent) of the represented
	MAY perform additional checks on the attributes of the representative (First Name, Last Name and DoB) if the Data Service hold this information and the access policy requires it.
	If the Unique identifier of the representative (natural person) is sent and if the Data Service has the information about the account used by the user (e.g. the account corresponds to an eID means issued by the same Member State), it MAY perform additional checks in the process or following the re-authentication and identity matching on the Data Service side.

If the process of identity matching does not result in a match, an error message MUST be generated and an error report is sent back to the Evidence Requester.

2.1.5 Sample attribute collection and evidence exchange flow

The following diagram shows the ways in which the eIDAS attributes are collected. It covers all steps that prepare to collect attributes on the side of MS A. These attributes are made available for further processing steps (not shown in this diagram) by the Data Service and Preview Space.



The following table describes the various steps.

Step	Description
1-2	User chooses to authenticate with eIDAS in order to get access to the Online Procedure Portal.
3-4	The user is requested to select the Member States who issued the electronic identification means he/she would like to use for authentication. The user makes a choice. NOTE: The Member States selection is for the case when the electronic identification means is issued by another Member State, a Member State other than the one of the Online Procedure Portal.
5	Based on the requested attributes and LoA, the user is presented the option(s) for electronic identification schemes and/or electronic identification means.
6-8	The user is asked to consent the exchange of requested attributes and the user confirms. The user selects one of the electronic identification means issued by an eID scheme notified in accordance with Regulation (EU) 910/2014. The Online Procedure Portal MAY request all available attributes that can be made available by the eID scheme that issued the eID means that the user selected. The available attributes are listed in the Proxy-Service metadata, and it should be requested provided that it is allowed by the national law and that the user has given her/his consent.

Step	Description
9-10	The user is requested by the eID scheme to authenticate. The authentication process depends on the eID means selected.
11-13	The user is successfully authenticated using electronic identification means notified in accordance with Regulation (EU) 910/2014 and the Online Procedure Portal receives (natural or legal) person identification data. This MUST include the **mandatory attributes of the eIDAS minimum data set** and, if available and approved by the user for exchange, optional and/or sector specific attributes. Depending on the national implementation of the eIDAS node and identity matching service, the Online Procedure Portal may receive additional national specific person identification data, e.g. a national registration number. NOTE: For simplicity reasons, the identity matching service and the eIDAS node Member State specific part have been depicted as a single component - eIDAS Node (MS A). The additional attributes beyond the mandatory attributes of the minimum data set are not sent in the evidence request.
14	The Online Procedure Portal consults the Data Service Directory to find if there are additional attributes beyond the the minimum data set laid down in accordance with Commission Implementing Regulation (EU) 2015/1501, that need to be specified in order to facilitate the identification of the relevant evidence provider. The Online Procedure Portal received the list of additional attributes which have to be provided by the user for the purpose of the identification of the evidence provider.
15	If there are any additional attributes beyond the mandatory attributes that are needed for the identification of the evidence provider, ask the user to provide them. The user provides the additional attributes. NOTE: All **mandatory attributes of the eIDAS minimum data set** must be provided. Therefore if any of these attributes are not available, the user must be re-authenticate with an eID means issued by an eID scheme notified under eIDAS.
16-17	With the user's input and consent, the Online Procedure Portal adds all the person identification data to the evidence request and sends this request to the Data Service.

2.1.6 Examples Unique Identifier and Data Service identity matching (Informative)

A Data Service may be faced with some of the following cases when performing the identity and record matching:

NOTE
In the below scenarios and examples, where referring to the Unique Identifier being derived or not, known or unknown, it should be understood as the "*the third part a combination of readable characters"* of the PersonIdentifier, and it is based on the information provided during notification process and summarised here: https://ec.europa.eu/digital-building-blocks/wikis/x/pSQIBQ
When the Unique Identifier is referred to as *receiving Member State specific*, it means that the identifier changes for each country.
The list of examples is not exhaustive and other cases may exist.

NOTE
In the below examples, the Unique Identifier has been retrieved during the eIDAS authentication on the Online Procedure Portal side.
The Online Procedure Portal is from Member State B and the Data Service is from Member State A.
The eID used by the user may be issued by Member State A, Member State B or Member State C, depending on each example.

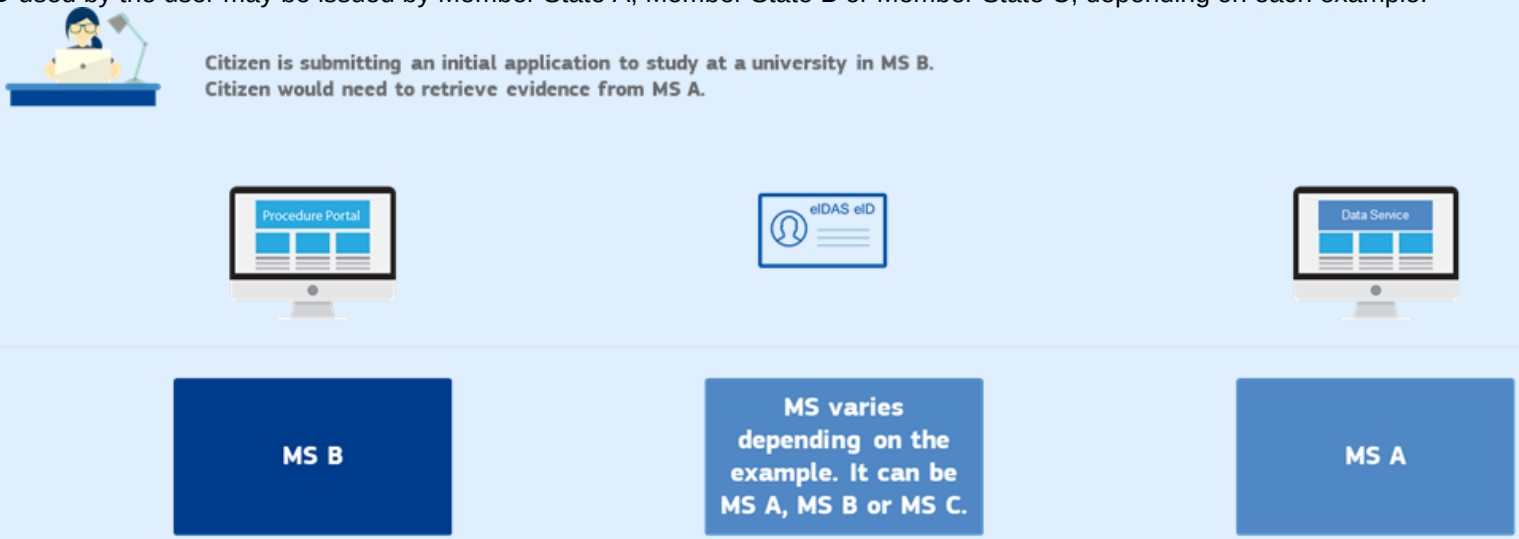
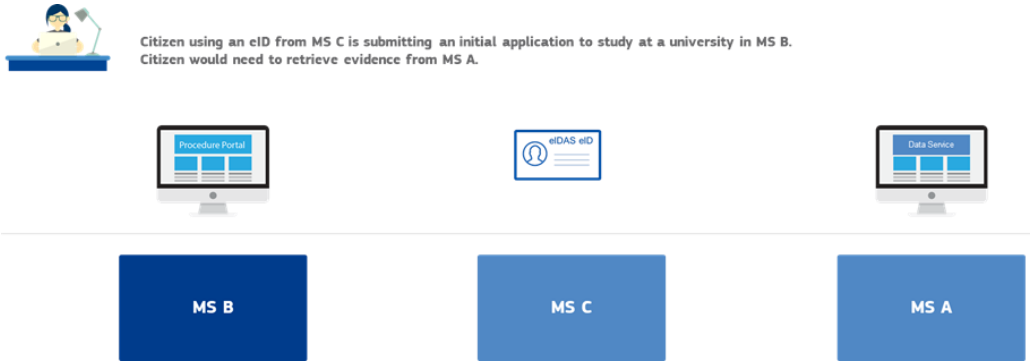
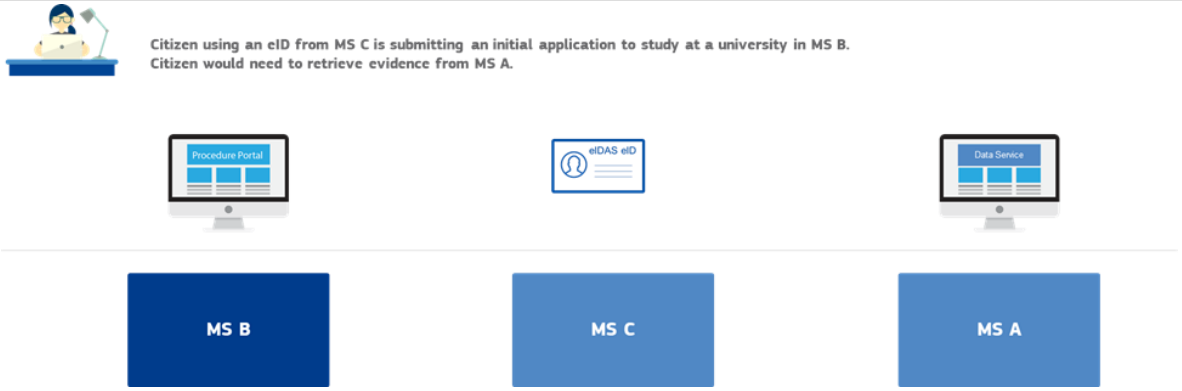
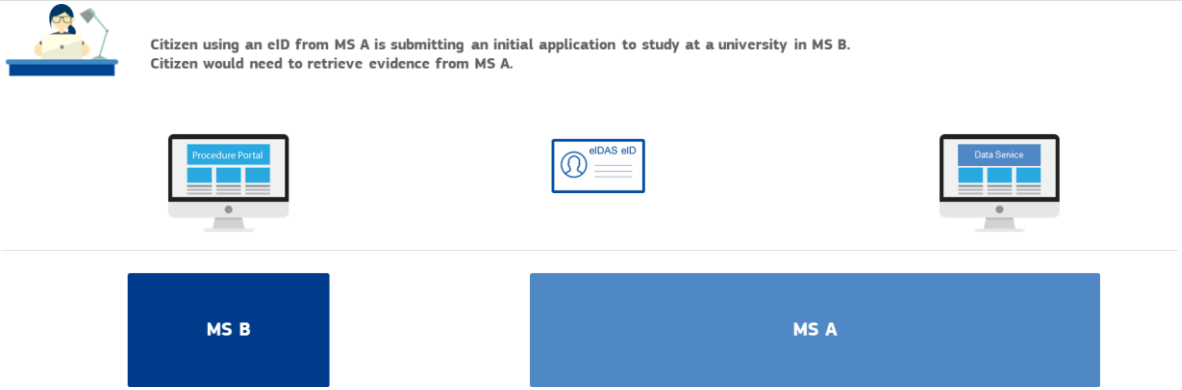
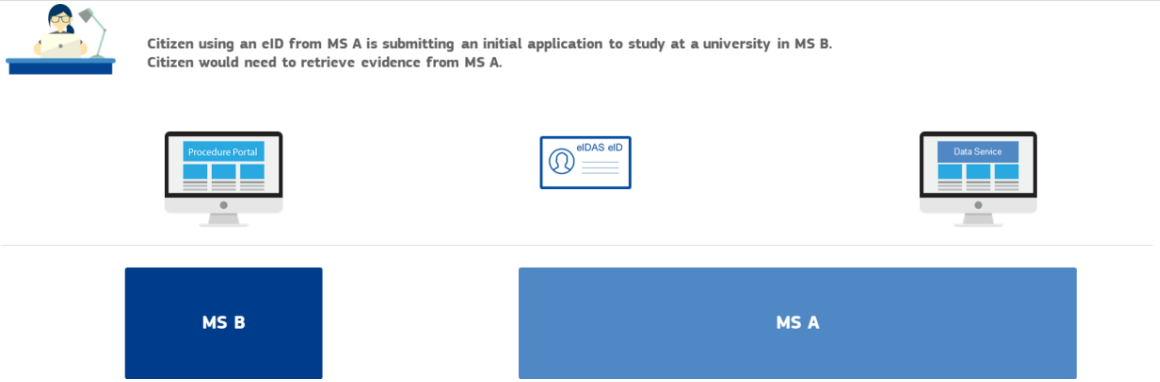


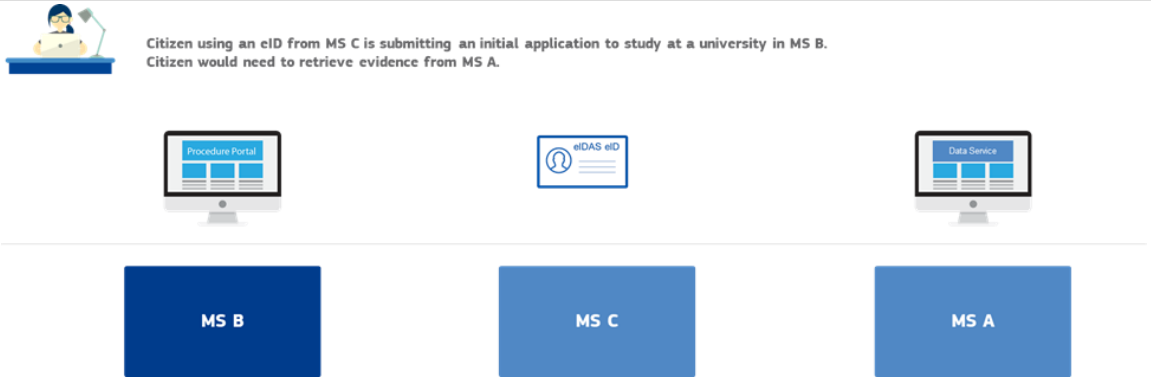
Figure 3. Unique Identifier various examples

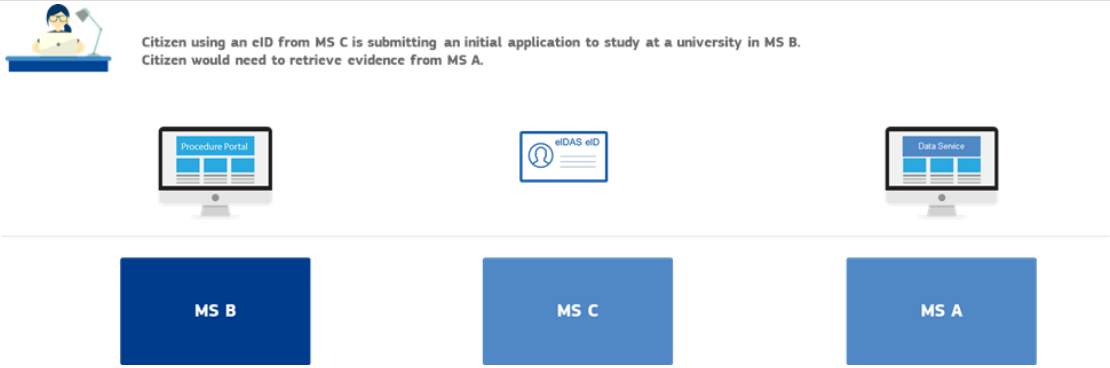
#	Derived Unique Identifier (YES/NO)	Unique Identifier known by Data Service (YES/NO)	Member State specific derived Identifier (YES/NO)	eID means issued by	Description
1	NO	YES	NO	Member State different from the Member State of the Data Service	**Unique Identifier is non-derived and it is known by the Data Service** Example: User is using an eID means issued by Member State C which uses as Unique Identifier a national personal identification code, without derivation.  Following a previous interaction of the user with the Data Service or its matching function, this identifier is known by the Data Service. Therefore, it doesn't matter in which Member State the Online Procedure Portal is, the eIDAS authentication request will retrieve the Unique Identifier which is known by the Data Service or it's matching function.
2	NO	NO	NO	Member State different from the Member State of the Data Service	**Unique Identifier is non-derived but it is not known by the Data Service** Example: User is using an eID means issued by Member State C which uses as Unique Identifier a national personal identification code, without derivation.

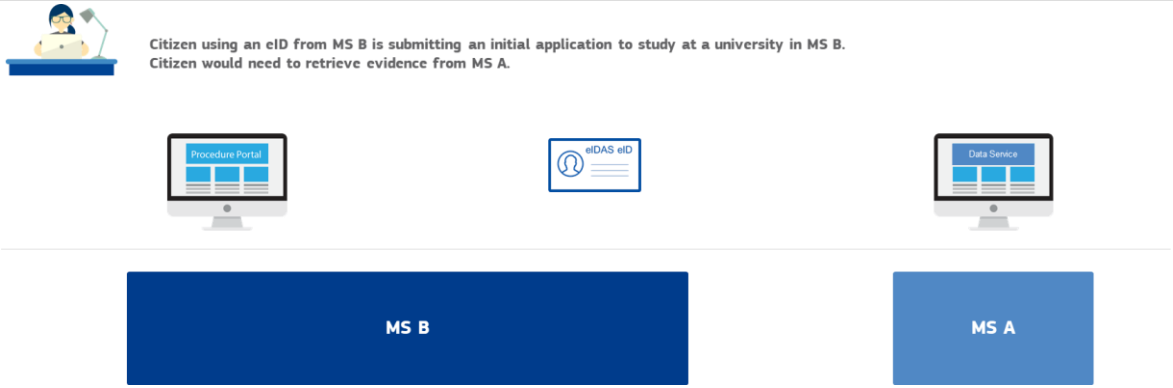
#	Derived Unique Identifier (YES/NO)	Unique Identifier known by Data Service (YES/NO)	Member State specific derived Identifier (YES/NO)	eID means issued by	Description
					 However, as the user has never linked this identity to his/her records in the Member State of the Data Service, the Unique Identifier is not known by the Data Service or its matching function. Therefore, even if the Data Service receives the non-derived Unique Identifier, simply by using this identifier and the other mandatory attributes of the minimum data set , it would not be able to do the identity match. Additional attributes would be needed, similar to the process used nationally for linking the different identities.
3	YES	YES or NO	NO	Member State of the Data Service	**Unique Identifier is derived, not receiving Member State specific and it has been issued by the Member State of the Data Service** Example: User is using an eID means issued by Member State A, which has a derived identifier but which is not receiving Member State specific.

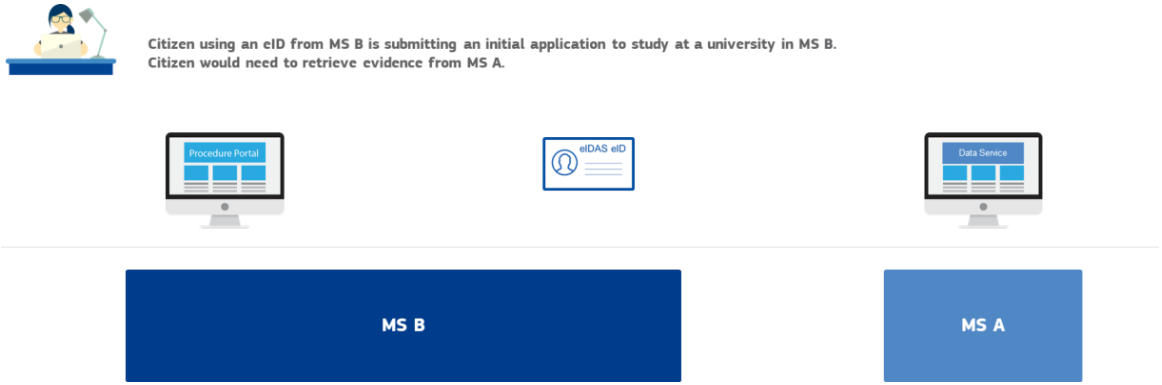
#	Derived Unique Identifier (YES/NO)	Unique Identifier known by Data Service (YES/NO)	Member State specific derived Identifier (YES/NO)	eID means issued by	Description
					 The Data Service is also in Member State A, but as the Unique Identifier is not receiving Member State specific, it does not matter from where the request for evidence is made, as the same Unique Identifier would be returned. Depending on the derivation methodology, the Data Service or its matching function may be able to directly perform the identity match or it may require additional person identification data beyond the mandatory minimum data set. The eIDAS Unique Identifier may or may not be known by the Data Service Provider, depending on the national implementation of the management of Unique Identifiers and if the user is registered with the Data Service.
4	YES	YES or NO	YES	Member State of the Data Service	**Unique Identifier is derived, receiving Member State specific and it has been issued by the Member State of the Data Service** Example: User is using an eID means issued by Member State A, which is a derived identifier and which is receiving Member State specific.

#	Derived Unique Identifier (YES/NO)	Unique Identifier known by Data Service (YES/NO)	Member State specific derived Identifier (YES/NO)	eID means issued by	Description
					 The Data Service is also in Member State A, but unlike case 3, the Unique Identifier received would depend on the Member State of the Online Procedure Portal. Depending on the derivation methodology, the Data Service or its matching function may be able to directly perform the identity match or it may require additional person identification data beyond the mandatory minimum data set. The eIDAS Unique Identifier may or may not be known by the Data Service Provider, depending on the national implementation of the management of Unique Identifiers and if the user is registered with the Data Service.
5	YES	YES or NO	NO	Other Member State than Member State of the Data Service and Online	**Unique Identifier is derived, not receiving Member State specific and not issued by the Member State of the Data Service or Online Procedure Portal** Example: Data Service is in Member State A, Online Procedure Portal is from Member State B and eID means is issued by Member State C.

#	Derived Unique Identifier (YES/NO)	Unique Identifier known by Data Service (YES/NO)	Member State specific derived Identifier (YES/NO)	eID means issued by	Description
				Procedure Portal	 The Unique Identifier is derived, but since it is not receiving Member State specific, the same Unique Identifier would be issued for requests made from Member State A and B. Therefore, if the user has in the past linked her/his identity at the Data Service or its matching function, when receiving the evidence request, the Data Service should be able to perform the identity match. If she/he has not linked her/his identity, this identifier is not known and additional attributes would be needed, similar to the process used nationally for linking the different identities.
6	YES	YES or NO	YES	Other Member State than Member State of the Data Service and Online Procedure Portal	**Unique Identifier is derived, receiving Member State specific and not issued by the Member State of the Data Service or Online Procedure Portal** Example: Data Service is in Member State A, Online Procedure Portal is from Member State B and eID means is issued by Member State C.

#	Derived Unique Identifier (YES/NO)	Unique Identifier known by Data Service (YES/NO)	Member State specific derived Identifier (YES/NO)	eID means issued by	Description
					 Unlike the previous case, the Unique Identifier is derived and receiving Member State specific, therefore the Unique Identifier received by the Online Procedure Portal, is specific to Member State B and cannot be used in Member State A of the Data Service. Therefore, even if the user has in the past linked her/his identity at the Data Service or its matching function, the Unique Identifier cannot be used and additional attributes would be needed, similar to the process used nationally for linking the different identities.
7	YES	YES or NO	NO	Member State of the Online Procedure Portal	**Unique Identifier is derived, not receiving Member State specific and is issued by the Member State of the Online Procedure Portal** Example: Data Service is in Member State A, Online Procedure Portal is in Member State B, eID means is issued by Member State B.

#	Derived Unique Identifier (YES/NO)	Unique Identifier known by Data Service (YES/NO)	Member State specific derived Identifier (YES/NO)	eID means issued by	Description
					 When authenticating at the Online Procedure Portal, since the authentication is using a national eID means, even if in the context of OOTS it has to be an eID means notified under eIDAS, the eIDAS infrastructure and its components are most likely not used. The Online Procedure Portal may receive a Unique Identifier that is nationally specific and therefore, when creating the evidence request it should ideally send the identifier that it is meant to be used for the context of the Data Service. In this case, it is a derived identifier but which is not receiving Member State specific, so it would be the same value no matter the Member State of the Data Service. If the identifier sent by the Online Procedure Portal is the same as the one issued when making an eIDAS request from Member State A, and the user has linked her/his identity, the Data Service should be able to perform the identity match. If this identifier sent by the Online Procedure Portal is the same as the one issued when making an eIDAS request from Member State A, but the user has not linker her/his identity, the Data Service would need additional attributes, similar to the process used nationally for linking the different identities.

#	Derived Unique Identifier (YES/NO)	Unique Identifier known by Data Service (YES/NO)	Member State specific derived Identifier (YES/NO)	eID means issued by	Description
8	YES	YES or NO	YES	Member State of the Online Procedure Portal	**Unique Identifier is derived, receiving Member State specific and it is issued by the Member State of the Online Procedure Portal** Example: Data Service is in Member State A, Online Procedure Portal is in Member State B, eID means is issued by Member State B.  When authenticating at the Online Procedure Portal, since the authentication is using a national eID means, even if in the context of OOTS it has to be an eID means notified under eIDAS, the eIDAS infrastructure and its components are most likely not used. The Online Procedure Portal may receive a Unique Identifier that is nationally specific and therefore, when creating the evidence request it should ideally send the identifier that it is meant to be used for the context of the Data Service. In this case, it is a derived identifier which is also receving Member State specific, so it should provide a different identifier depending on context of the Data Service.

#	Derived Unique Identifier (YES/NO)	Unique Identifier known by Data Service (YES/NO)	Member State specific derived Identifier (YES/NO)	eID means issued by	Description
					If this identifier sent by the Online Procedure Portal is the same as the one issued when making an eIDAS request from Member State A, and the user has linked her/his identity, the Data Service should be able to perform the identity match. If this identifier sent by the Online Procedure Portal is the same as the one issued when making an eIDAS request from Member State A but the user has not linker her/his identity, the Data Service would need additional attributes, similar to the process used nationally for linking the different identities.

For the last two cases, where the eID means is issued by the Member State of the Online Procedure Portal, the Online Procedure Portal should have available the possibility to retrieve and provide a UniqueIdentifier, to the Data Service. This should cover also the cases where the eIDAS UniqueIdentifier is derived and receiving Member State specific.

2.2 OOTS eID additional security services - June 2022

2.2.1 Introduction

The Once-Only Technical System relies of the use of eIDAS and the existing infrastructure of eIDAS nodes to authenticate the user and to obtain assured identity attributes. A Data Service can use these identity attributes to match evidence requests to any relevant evidences. The identity attributes are received from the Online Procedure Portal or as a result of re-authentication. However, the use of eIDAS does not preclude the use of other mechanisms to provide complementary or additional security measures. This section describes two such mechanisms.

- An authentication verification service that a Data Service can use to verify that the user identity attributes in the evidence request link to a recent eIDAS authentication transaction.
- Authorization of requests for evidence relating to represented persons.

These features should be viewed as opt-in elements of the Once Only toolbox that competent authorities in a Member State may use in their implementation of the Once Only technical system. A Member State that does not want, or is not able, to use the service does not need to take any action.

In the current version of the technical design documents, the authentication verification and authorization of requests for evidence relating to represented persons features rely on national services that only involve communication between components within a single Member State. There is no cross-border interoperabilty dimension and therefore no technical design information that needs to be shared between Member States.

2.2.2 Authentication verification

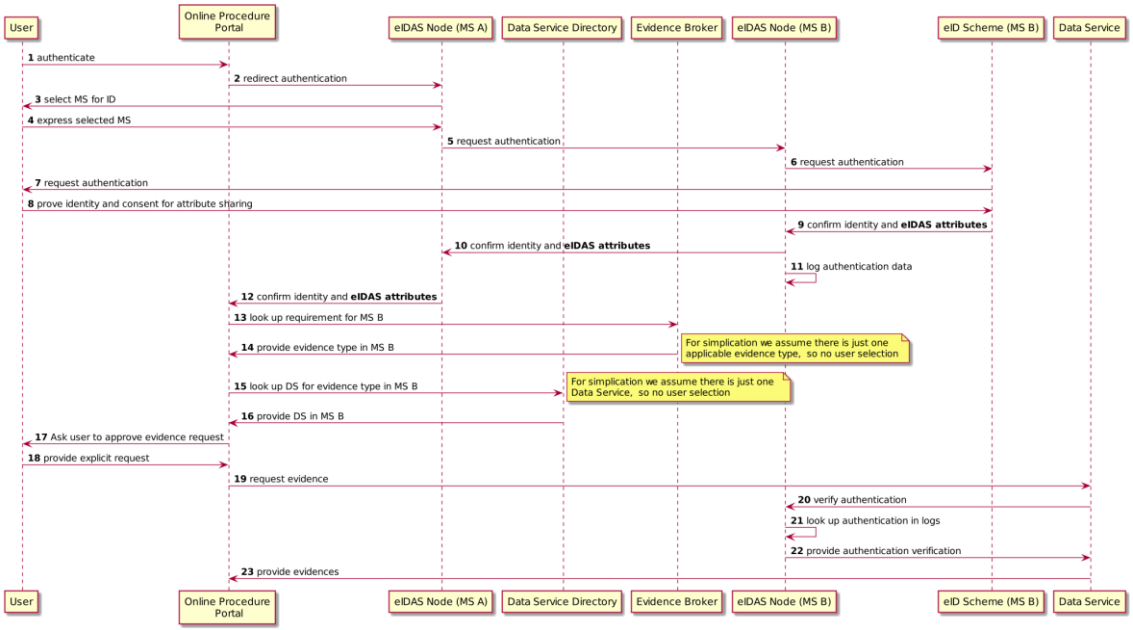
Once-Only evidence requests are requests from evidence requesters to evidence providers for evidence relating to identified users acting either directly or through a representative. The syntax and semantics of evidence requests is defined in Chapter 4, which specifies how person identity attribute information is expressed. Attributes whose values are obtained following an eIDAS authentication and delivered as part of an eIDAS assertion are marked with the level of assurance of the eIDAS identification means.

It is the responsibility of the Online Procedure Portal (or of a Once-Only Staging Area, if used) to make sure the assured identity data that is included in the request matches the information provided using the eID means issued by an eID scheme notified under eIDAS. Based on the the identity data received, the Data Service decides if the user, once re-directed, needs to re-authenticate.

Data Services could use a combination of identity matching based on the attributes received with an authentication verification service. This would allow them to verify that an eIDAS authentication took place for a user whose identity attribute values and indicated level of assurance, match the data in the evidence request, that this authentication took place sufficiently recently to be plausibly related to a single user session and that the authentication was made by the user for the execution of an electronic procedure in the scope of the SDG.

The following diagram shows a situation in which this service is provided by the eIDAS Node Member State specific module of a Member State in which a Data Service is requested to provide evidence on a user. For ease of understanding, this diagram is simplified and does not include the use of 4.9 - Evidence Preview - June 2022.

In step 11, it is shown that the service node would need to log data about the authentication, including the time at which it took place. In step 20, it is shown that the service node accepts requests from a Data Service to verify that a related authentication took place. The service determines, in step 21, whether the claimed identity data matches the data that was provided in prior authentications and how much time expired since the last such authentication and the context in which the authentication was made. Based on this, the service provides, in step 22, either confirmation or denial that the request matches a recent authentication. If authentication is verified, the Data Service may proceed to making the evidence available. If not, it should reject the request.



If limited to use by Data Services in the same Member State in which the user authenticated, the authentication verification service is a national service. As per subsidiarity, it is up to a Member State and its competent authorities to deploy and use such service. If such a service is available, Data Services should use it as it provides an important additional security layer to the use of the Once-Only Technical System.

2.2.3 Authorization of requests for evidence relating to represented persons

For evidence relating to legal persons for use in business-oriented procedures, evidence requests may include identity attributes of both the represented legal entity and the representative. These attributes are described in section 2.1. and may be assured using eIDAS as explained in that section and in section 2.8 of the eIDAS SAML Attribute profile, v1.2.

A Data Service may be integrated into a service (for example, a Mandate Management Service) that can validate whether the representative is authorized to obtain evidence for the represented person. If access is not authorized, the Data Service must return an error message containing a RegRep AuthorizationException.

This additional service is internal to the Member State and therefore any further details are out-of-scope for these technical design documents.

2.3 Representation - June 2022

Several of the procedures listed in Annex II of the SDG regulation are procedures about legal persons. In these procedures, Evidence Requesters typically need to establish that the user (a natural person) has the power to represent the legal person in the electronic procedure in order to be able to proceed with the application. This requirement applies whether or not any evidences are exchanged in the electronic procedure and is therefore independent and separate from the Once-Only Technical System. This section is about requirements on the OOTS for the exchange of evidences about legal persons.

When processing requests for evidence about legal persons, the Online Procedure Portal must authenticate users acting either directly or through a representative using electronic identification means defined in Article 3(2) of Regulation (EU) 910/2014 issued under the electronic identification schemes notified in accordance with that Regulation. Even if the representative attributes MUST NOT be explicitly requested in the eIDAS Authentication request, the Online Procedure Portal MAY receive from the eIDAS service one representative attribute set in case of representation. (see 2.8 of the eIDAS SAML Attribute Profile 1.2). This means that the Online Procedure Portal may receive in case of representation two attribute sets, one for the representative and one for the represented person. The attributes for representative must follow the same specifications as defined in sections 2.2, 2.3 of the eIDAS SAML Attribute Profile 1.2 and must have the attribute's FriendlyName prefixed with "Representative".

When making evidence requests, the evidence requester shall include all the attribute sets obtained using eIDAS. A Data Service, when processing an evidence request, shall use all identity attributes of the user that are included in the request. The Data Service may choose to re-authenticate the user, or use the attributes sets in combination with additional security services as defined in 2.2 - OOTS eID additional security services - June 2022 to determine if pieces of evidence can be returned. In both cases, the Data Service must ensure that the attributes of the user and of the representative where applicable match the attributes held by it.

Please note that the current eIDAS technical specifications do not consider any constraints of representation. The scope of powers or mandates may be described in the notification process of eID schemes that concern either legal persons or natural persons representing legal persons, but this information is not available to the evidence requester and there is no agreed syntax to encode it.

3 Chapter 3: Common Services - June 2022

Common Services - June 2022

Summary

In this chapter, the identified Common Services, necessary for the proper execution of the Evidence Exchange process, are described in detail, providing the information model and their technical design documentation. To achieve organisational interoperability, several functions have been identified that need to be available either centrally or at MS level as described in section 6.6 of the OOTS HLA, to execute the business processes of discovering and getting the required evidence. The identified Common Services are:

- The **Data Service Directory (DSD)**, which is a common service that acts as a catalogue of Evidence types that the EPs can provide upon request. It is used in the Evidence Exchange process by the Evidence Requesters to discover the Evidence Providers that can provide the evidence they require.
- The **Evidence Broker (EB)**, which is an authoritative system that maps specific data sets as Evidence types that prove specific requirements. The ER consults the EB to find which types of evidence can be requested as evidence for a specific Evidence Subject, taking into account the Subject's location and/or jurisdiction.
- The **Semantic Repository (SR)** is a common service that acts as a data portal for OOTS, storing commonly agreed information models grouped by domain, providing them under multiple representation techniques.

The chapter includes the following sub-chapters:

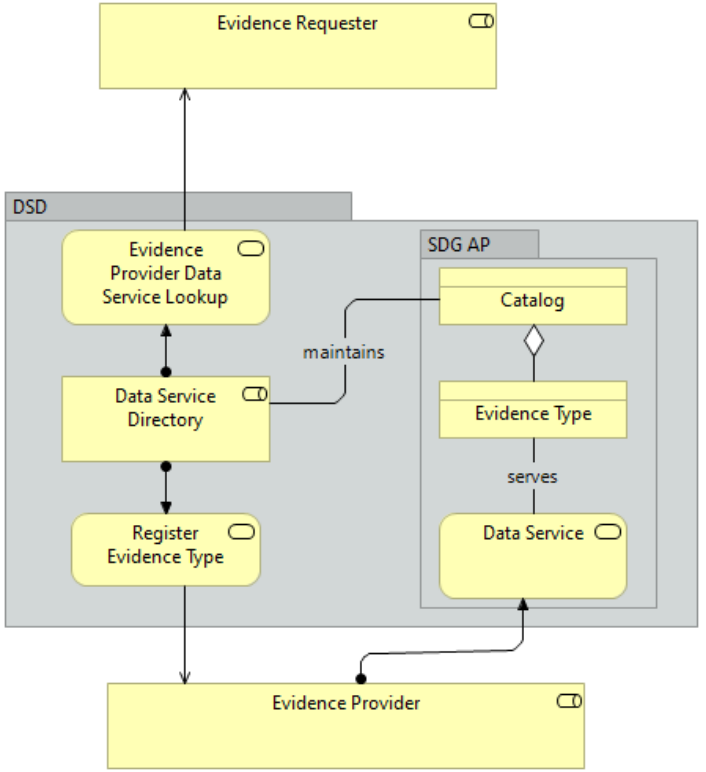
Change log

For this release, the changes for all chapters are combined at the top level

3.1 Data Service Directory (DSD) - June 2022

3.1.1 Overview

The Data Service Directory is a Common Service defined in the OOTS HLA. It maintains a catalog of Evidence Providers with the Evidence Types they are able to provide upon request using their Data Services. It is used in the Evidence Exchange process by the Evidence Requesters to discover the Evidence Providers that can provide the evidences they require, together with the required metadata and attributes imposed by the Data Services, like the classifications and context determinations of the Evidence Providers.
The information data model is based on the SDGR Application Profile for the DSD. The Service API is implemented using the OASIS RegRep v4 Query Protocol with the REST API Binding.
In the following sections, a detailed analysis of the internal data model and the Service API specification are provided.



3.1.2 Functionality

The main functionality of the DSD is to publish Data Services of Evidence Providers that provide distributions of Evidence Types and make them discoverable through queries. The functionality requires four main classes of Information:

- The `DataServiceEvidenceType`, providing the semantic information and requirements for retrieving an evidence type from a Data Service.
- The `Distribution` of the `DataServiceEvidenceType`, describing the format, the semantic and syntactic conformance, under which the Evidence Type can be distributed.
- The `DataService`, describing the technical endpoint from which an Evidence Requester can request the Evidence distributions.
- the `EvidenceProvider`, describing the details of the Provider of the Evidence.

An Evidence Provider that wants to serve an Evidence of a specific evidence type MUST register this capability in the DSD. To do that, it needs to be registered as an Evidence Provider with its Data Service. Each Data Service MUST be linked with at least one Evidence Type Distribution expressed using the `DataServiceEvidenceType` class. A `DataServiceEvidenceType`, if it does not already exist, must also be registered in the DSD containing all the attributes required for informing the Evidence Requester of the requirements for requesting the Evidence, like any additional attributes required for Evidence Provider discovery, the level of assurance of the identification required, together with its available distributions. When all three information classes have been properly registered, the Evidence Provider links its Data Service with the `DataServiceEvidence t`ype to publish its capability of providing the specific evidence type through its Data Service.
The following section describes the Information Data Model used for the registration and the queries of the DSD Service.

3.1.3 Information Data Model

3.1.3.1 Introduction

The DSD information Data Model is based on the SDGR Application Profile for the DSD. It is based on the semantic classes of Evidence Type derived from the CCCEV v2.0, the DataService from DCAT and the Organization Class from the Core Public Organisation Vocabularies. It provides all the information aspects of the model, including the data types, use of Identifiers and code lists for every element used in this profile. The serialization of the model is done using XML according to the guidelines below. Below is an example of the XML representation of a Data Service serving an Evidence Type as it is contained in the DSD.

```
<?xml version="1.0" encoding="UTF-8"?>
<DataServiceEvidenceType xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                         xmlns="http://data.europa.eu/p4s">
```

```
    <!-- - - Evidence Type Metadata - - -->
    <!-- The Data Service assigned Unique Identifier of the Evidence Type. Must be used in the Evidence Exchange Request --
>
    <sdg:Identifier>RE238918378</sdg:Identifier>

    <!-- Classification Information - Used for linking with the Evidence Broker -->
    <EvidenceTypeClassification>CertificateOfBirth</EvidenceTypeClassification>
    <Title>Certificate of Birth</Title>

    <!-- Distribution Information - Multiple Distributions per Data Service Evidence Type -->
    <!-- XML Distribution, conforming to the common data model on Birth Certificate -->
    <DistributedAs>
        <Format>http://publications.europa.eu/resource/authority/file-type/XML</Format>
        <ConformsTo>https://semic.org/sa/common/birthcert-1.0.0</ConformsTo>
    </DistributedAs>

    <!-- PDF Distribution. PDF is unstructured data so there is no conformance to a data model -->
    <DistributedAs>
        <Format>application/pdf</Format>
    </DistributedAs>


    <!-- - - Evidence Provider and Data Service Metadata - - -->

    <!-- Access Service represents the Data Service serving the piece of Evidence on behalf of an Evidence Provider -->
    <!-- Multiple Access Services, one per Evidence Provider -->
    <AccessService>

        <!-- The identifier of the Access Service, using ebcore Party ID Type. Used in eDelivery Evidence Exchange for
PMode Mapping -->
        <Identifier schemeID="urn:oasis:names:tc:ebcore:partyid-type:iso6523:0060">8889909098</Identifier>
        <!-- The Evidence Exchange profile version to which this access service expects / serves -->
        <ConformsTo>oots:edm-v1.0</ConformsTo>

        <!-- The Evidence Provider Information of this access service -->
        <Publisher>
            <Identifier schemeID="VAT">DE73524311</Identifier>
            <Name>Civil Registration Office Hamburg</Name>
```

```
            <Address>
                <FullAddress>Street ABC</FullAddress>
                <AdminUnitLevel1>DE</AdminUnitLevel1>
                <!-- NUTS Code -->
                <AdminUnitLevel2>DE12</AdminUnitLevel2>
            </Address>

            <Jurisdiction>
                <AdminUnitLevel1>DE</AdminUnitLevel1>
                <AdminUnitLevel2>DE12</AdminUnitLevel2>
            </Jurisdiction>
        </Publisher>
    </AccessService>
    <!-- Additional Access Service representing a different Evidence Provider -->
    <AccessService>
        <Identifier schemeID="urn:oasis:names:tc:ebcore:partyid-type:iso6523:0060">8889909099</Identifier>
        <ConformsTo>oots:edm-v1.0</ConformsTo>
        <Publisher>
            <!-- The Evidence Provider Information -->
            <Identifier schemeID="122">SK11231112313</Identifier>
            <Name>Example Organization </Name>

            <Address>
                <FullAddress>Prince Street 15</FullAddress>
                <AdminUnitLevel1>SK</AdminUnitLevel1>
                <!-- NUTS Code -->
                <AdminUnitLevel2>SK77</AdminUnitLevel2>
            </Address>

            <Jurisdiction>
                <AdminUnitLevel1>SK</AdminUnitLevel1>
                <AdminUnitLevel2>SK77</AdminUnitLevel2>
            </Jurisdiction>
        </Publisher>
    </AccessService>

    <EvidenceProviderClassification>
        <Identifier>TypeOfInsurance</Identifier>
        <Type>Codelist</Type>
```

```
        <!-- Value from a Codelist required. Must be published in the Semantic Repository -->
        <ValueExpression>http://sr.europa.eu/codelists/insuranceType</ValueExpression>
        <Description lang="en">Type of Insurance</Description>
    </EvidenceProviderClassification>
</DataServiceEvidenceType>
```

The `DataServiceEvidenceType` consists of specific groups of elements covering different contextual metadata required for a successful Evidence Exchange:

- **Evidence Type Metadata**, providing information on the qualities of the Evidence Type.
- **Data Service Metadata,** providing information on the identification, distinction, location and jurisdiction of the Evidence Providers and its Data Services.

The following sub-sections provide an overview of the use of elements and attributes found in this class with a detailed explanation.

3.1.3.2 Evidence Type Metadata

The Evidence type metadata describes specific aspects of the evidence type such as:

- The Identifier, using the `Identifier` element, provided by the Data Services to uniquely identify an Evidence Type with its required metadata. This identifier is used by the Evidence Requester in the Evidence Exchange Request, to identify the Evidence Type to be retrieved by the Data Service.
- The available distributions, using the `DistributedAs` element. The distributions provide the available formats for the Evidence Type, such as PDF, XML, JSON etc, using code values from the IANA Media Types registry. For the file types that provide structured content like XML, JSON, RDF, etc., the Data Service can provide a conformance statement, using the `conformsTo` sub-element of the `DistributedAs` element, for denoting the semantic and technical conformance profile. The element's value is a persistent URL, pointing to an entry of the OOTS Semantic Repository that contains all the relevant information of such a profile.

3.1.3.3 Data Service Metadata

The Data Service metadata provides the necessary information needed for selecting the proper Evidence Provider and its relevant Data Service. It consists of:

- The Data Service Identifier, using the `AccessService/Identifier` element that is used by the eDelivery infrastructure to extract and use the proper pre-configured PMode for the submission of the Evidence Request. This identifier is profiled as a CEF eDelivery ebcore Party Identifier.
- The Evidence Exchange Message Data Model Profile and version, denoted in the `AccessService/ConformsTo` element. Currently, the only value allowed is the `oots:edm-1.0.`

- The Publisher element, providing the Name, Location and Jurisdiction of the Evidence Provider, used by the Evidence Requester for filtering and selection of the correct Evidence Provider.
- The Evidence Provider Determination Context, defining the location context of the Evidence provider. For example, if the determination context is "Place of Birth", it means that the jurisdiction of the Evidence provider must match the place of birth of the user.

3.1.3.4 Evidence Provider Discovery Metadata

3.1.3.4.1 Introduction

There could be occasions where the proper discovery of the Evidence Provider requires more data to be provided by the User or Evidence Requester. For example, there might be situations where the jurisdiction of the Evidence Provider MUST map to a specific location attribute of the user like the Place of Birth or the Evidence Provider serves evidence of specific contexts like the type of insurance, the type of company, etc. The DSD provides the following mechanisms for discovering the Evidence Provider based on additional attributes

3.1.3.4.2 Evidence Provider Jurisdiction mapping to user attribute

The jurisdiction of the Evidence Provider is usually contextualized with a specific property of the user and the issued evidence type. A birth certificate registry's jurisdiction for example must match the user's place of birth at a specific level of jurisdiction. The DSD contains the `EvidenceProviderJurisdictionDetermination` attribute that defines the required mapping of the Evidence Provider's jurisdiction, in the `DataServiceEvidenceType` element. The attribute consists of the following sub-attributes:

- The Jurisdiction Context Identifier that is used as part of the query API for providing the response to the DSD by the User
- The Jurisdiction Context itself, which is a multilingual string describing the context as it should be displayed by the Evidence Requester's UI
- The Jurisdiction Level required, defining the required granularity of the jurisdiction.

The following example describes an entry in the DSD:

```
<sdg:EvidenceProviderJurisdictionDetermination>
    <sdg:JurisdictionContextId>PlaceOfBirthIdentifier</sdg:JurisdictionContextId>
    <sdg:JurisdictionContext lang="en">Place Of Birth</sdg:JurisdictionContext>
    <sdg:JurisdictionContext lang="de">Geburtsort</sdg:JurisdictionContext>
    <!-- Codelist defining the jurisdiction levels, registered in the semantic repository -->
    <sdg:JurisdictionLevel>https://sr.ec.europa.eu/codelist/locationLevel/LAU</sdg:JurisdictionLevel>
</sdg:EvidenceProviderJurisdictionDetermination>
```

3.1.3.4.3 Provider Context Determination

Although the jurisdiction mapping can be the main attribute for discovering the Evidence Provider, there are situations where the Evidence Provider must be further classified, depending on domain-specific quality attributes. For example, a registry containing social security and/or insurance contracts covers only specific kinds of insurance (Private, Public, Mixed) or could cover only specific kinds of subjects, (e.g. SMEs, very large companies, construction companies, etc.). These domain-specific quality attributes must be declared in the Evidence Provider's DSD information and also in the `DataServiceEvidenceType` structure as a mandatory classification filter that needs to be provided by the Evidence Requester. The DSD represents these attributes using the CCCEV 2.0 Information Concept structure. The Evidence Provider declares the qualities supported together with the supported values, as shown in the example below:

```
<sdg:AccessService>
    <sdg:Identifier schemeID="urn:oasis:names:tc:ebcore:partyid-type:iso6523:0060">8889909099</Identifier>
    <sdg:ConformsTo>oots:edm-v1.0</ConformsTo>
    <sdg:Publisher>
         /* Omitted ... */
        <sdg:ClassificationConcept>
            <sdg:Identifier>TypeOfInsurance</sdg:Identifier>
            <sdg:SupportedValue>
                <sdg:StringValue>Private</sdg:StringValue>
            </sdg:SupportedValue>
        </sdg:ClassificationConcept>
    /* Omitted ... */
    </sdg:Publisher>
</sdg:AccessService>
```

Classification concepts must be present in the `DataServiceEvidenceType` for supporting a filtering mechanism at the Evidence Requester side. The classification concepts are listed, using CCCEV 2.0 at the `DataServiceEvidenceType` as the following example:

```
<sdg:EvidenceProviderClassification>
    <sdg:Identifier>CertificateOfBirth</sdg:Identifier>
    <sdg:Type>Codelist</sdg:Type>
    <!-- Value from a Codelist required. Must be published in the Semantic Repository -->
    <sdg:ValueExpression>http://sr.europa.eu/codelists/birthCertificate</sdg:ValueExpression>
    <sdg:Description lang="en">Certificate of Birth</sdg:Description>
</sdg:EvidenceProviderClassification>
```

The complete use of the Evidence Provider Discovery metadata is described in the query interface specification.

3.1.4 Query Interface Specification

3.1.4.1 Introduction

The query interface specification for the Data Service Directory is based on the OASIS ebXML RegRep V4 standard. This standard has multiple protocol bindings that can be used to execute queries. Since the DSD queries have only simple, single-value parameters, the REST binding is used to implement the DSD query interface. This implies that the query transaction is executed as an HTTP GET request with the URL representing the query to execute and the HTTP response carrying the query response as an XML document. This section further profiles the REST binding as specified in the OASIS RegRep standard for use by the DSD.

3.1.4.2 Query: Find Data Services of Evidence Providers for a specific Evidence Type Classification

3.1.4.2.1 Introduction

This query allows the Evidence Requester to find all the Data Services of the Evidence Providers that can provide the required type of Evidence Type and are based in a specific geographic area.

3.1.4.2.2 Parameter Details

Parameter	Requirement	Description
queryId	MANDATORY	This parameter MUST have value **urn:fdc:oots:dsd:ebxml-regrep:queries:dataservices-by-evidencetype-and-jurisdiction**.
evidence-type-classification	MANDATORY	The Evidence Type classification code.
country-code	MANDATORY	Two-letter ISO 3166-1 alpha-2 country code.
jurisdiction-admin-l2	OPTIONAL	3 to 5 letter NUTS code.

jurisdiction-admin-l3	OPTIONAL	LAU Code.
jurisdiction-context-id	OPTIONAL	Used to provide the jurisdiction context id used for the query. The parameter MUST be used when responding to a DSD exception received, by providing the Jurisdiction Context Id found in the exception.
evidence-type-id	OPTIONAL	Used to provide the selected Data Service Evidence Type from a set of multiple. The parameter MUST be used when responding to a DSD exception received, by providing the Identifier of the selected DataServiceEvidenceType found in the exception

3.1.4.2.3 Result set specification

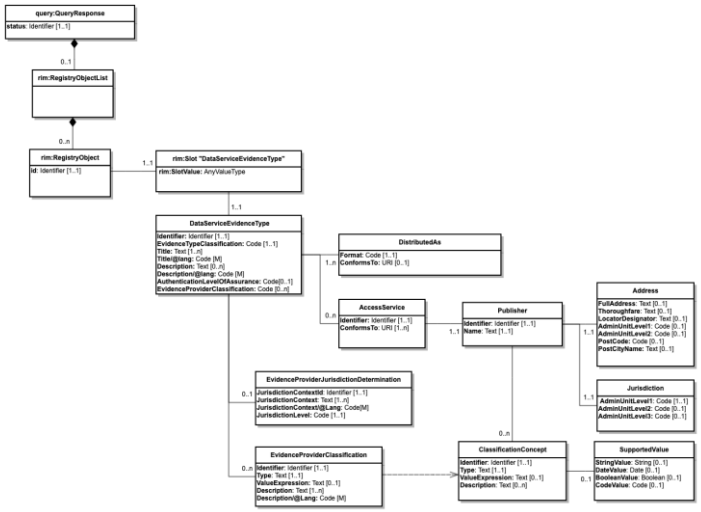
The result set of this query is specified as follows:

```
{d ∈ dsd.DataServiceEvidenceType: d.EvidenceTypeClassification == evidence-type-classification ∧
(d.AccessService.EvidenceProvider.Jurisdiction.adminUnitLevel1 == country-code) ∧ (adminUnitL2= "" ∨
d.AccessService.EvidenceProvider.Jurisdiction.adminUnit2 == jurisdiction-admin-l2) ∧ (adminUnitL3 = "" ∨
d.AccessService.EvidenceProvider.Jurisdiction.adminUnitLevel3 == jurisdiction-admin-l3) }
```

3.1.4.3 Query Response of the DSD

3.1.4.3.1 Data Model of the Query Response of the DSD

The Query Response of the DSD returns a RegRep QueryResponse document which MUST either contain an `Exception` or `RegistryObjectList` element with zero or more `RegistryObjects`. Each `RegistryObject` in the result MUST include one `Slot` element with a `SlotValue` of type *rim:AnyValueType* and a single `sdg:DataServiceEvidenceType` child element, following the SDGR Application Profile of the DSD. The SDGR application profile of the DSD describes how the SDG-Generic-Metadata Profile (SDG-syntax) is profiled in ebRIM in order to compose a valid QueryResponse. It, therefore, contains a mapping to the underlying SDG-syntax elements and necessary parameters to compose a QueryResponse. The namespace of the SDG-syntax is http://data.europa.eu/p4s.
The following data model illustrates the RegRep QueryResponse returned by the DSD.



3.1.4.3.2 Implementation Guideline of the Query Response of the DSD

The table below defines the elements of the data model illustrated above according to the core ebRIM elements and the `DataServiceEvidenceType` slot which is adapted by the SDGR-Application Profile of the DSD.

	Name	Definition	Cardinality	Type	Data Type	Rules	Core Vocabulary / Domain	Element of Core Vocabulary
	query:QueryResponse	**root element**		ComplexType			ebRIM	
+	status	This attribute contains the status of the response. If the DSD provides at least	1..1	Attribute	Identifier	Must be "Success" if the DSD	ebRIM	-

		one RegistryObject, the value "urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Success" is used.				provides a RegistryObject.		
++	**rim:RegistryObjectList**	**Element to list the Registry Objects of the QueryResponse.**	0..1	ComplexType			ebRIM	-
+++	**rim:RegistryObject**	**Element to control the type and structure of Registry Object within the QueryResponse.**	0..n	ExtrinsicObjectType			ebRIM	-
++++	id	Unique UUID for each RegistryObject.	1..1	Attribute	Identifier	Must be unique UUID for each Registry Object.	ebRIM	-
++++	rim:slot "DataServiceEvidenceType"	The slot is a container to describe the specific aspects and metadata of the Data Service and Evidence Type.	1..1	SlotType	AnyValueType		ebRIM	-
++++	rim:slot "DataServiceEvidenceType"	The slot is a container to describe the specific aspects and metadata of the Data Service and Evidence Type.	1..1	SlotType	AnyValueType		ebRIM	-
+++++	DataServiceEvidenceType	The element describes specific aspects and	1..1	DataServiceEvidenceTypeType			SDGR Applicat	-

		metadata of the Data Service and Evidence Type.					ion Profile	
+++++	DataServiceEvidenceType	The element describes specific aspects and metadata of the Data Service and Evidence Type.	1..1	DataServiceEvidenceTypeType			SDGR Application Profile	-
++++++	Identifier	The unique identifier of the Evidence Type of the Data Service. Must be used in the Evidence Request.	1..1	Attribute	Identifier		DCAT-AP	dct:identifier
++++++	EvidenceTypeClassification	A URI pointing to the Evidence Type that this Data Service is supporting. The classification is linked with the Evidence Type of the Semantic Repository (Evidence Broker).	1..1	Attribute	Code		Core Criterion Core Evidence Vocabulary	cccev:evidenceTypeClassification
++++++	Title	A name to identify in natural language the Evidence Type. Unbounded cardinality to support multiple languages.	1..n	Attribute	Text		DCAT-AP	dct:title
++++++	Title/@lang	The language of the title encoded as ISO 639-1 two-letter code. Default value "en"	M	Attribute	Code	ISO 639-1 two-letter code	DCAT-AP	dct:title

++++++	Description	A description of the Evidence Type. Unbounded cardinality to support multiple languages.	0..n	Attribute	Text		DCAT-AP	dct:description
++++++	Description/@lang	The language of the description encoded as ISO 639-1 two-letter code. Default value "en"	M	Attribute	Code	ISO 639-1 two-letter code	DCAT-AP	dct:description
++++++	AuthenticationLevelOfAssurance	The Minimum eIDAS Level Of Assurance Required for this Evidence Type, so that the Evidence can be released	0..1	Attribute	Code		SDGR Application Profile	
++++++	DistributedAs	The representations that are supported by the Data Service Evidence Type.	1..n	EvidenceTypeDistributionType			DCAT Application Profile	dcat:distribution
++++++	AccessService	The details of the Data Service serving the Evidence Type on behalf of an Evidence Provider. The Access Service enables to express that for one Data Service Evidence Type, the Data Service A is providing the distribution XML and Data Service B is providing the distribution JSON.	0..n	DataServiceType			DCAT Application Profile	dcat:servesDataset

++++++	EvidenceProviderJurisdictionDetermination	Contextual Information required for the jurisdiction determination of the correct Evidence Provider	0..1	JurisdictionDeterminationType			SDGR Application Profile	
++++++	EvidenceProviderClassification	The Evidence Provider required classifications mapped to this Evidence Type that need to be mapped to an EvidenceProvider Classification Concept for proper Evidence Provider Discovery	0..n	InformationConcept			Core Criterion Core Evidence Vocabulary	cccev:InformationConcept
++++++	DistributedAs	The representations that are supported by the Evidence Type Dataset.	1..n	EvidenceTypeDistributionType			DCAT Application Profile	dcat:distribution
++++++	Format	The technical representation of the Evidence Type. Declaration of the file types that provide structured content like PDF, XML, JSON, RDF etc	1..1	Attribute	Code		DCAT-AP	dct:format
++++++	ConformsTo	A registered schema or conformance profile in the OOTS semantic repository to which the described Distribution conforms.	0..1	Attribute	URI		DCAT-AP	dct:conformsTo
++++++	AccessService	The details of the Data Service serving the	0..n	DataServiceType			DCAT Applicat	dcat:servesDataset

		Evidence Type It enables to express that for one Data Service Evidence Type, the Data Service A is providing the Distribution XML and Data Service B is providing the Distribution JSON.					ion Profile	
++++++	Identifier	The identifier of the Access Service, using ebcore Party ID Type. Used in eDelivery Evidence Exchange for PMode Mapping.	1..1	Attribute	Identifier		DCAT-AP	dct:identifier
++++++	ConformsTo	The registered version(s) of the eDelivery profile used by the access service	1..n	Attribute	URI		DCAT-AP	dct:conformsTo
++++++	EvidenceProviderJurisdictionDetermination	Contextual Information required for the jurisdiction determination of the correct Evidence Provider	0..1	JurisdictionDeterminationType			SDGR Application Profile	
++++++	JurisdictionContextId	A codified, mappable value of the Jurisdiction Determination Context of an Evidence Provider	1..1	Attribute	Identifier		SDGR Application Profile	
++++++	JurisdictionContext	The Jurisdiction Determination Context of an Evidence Provider in natural language	1..n	Attribute	Text		SDGR Application Profile	

++++++	JurisdictionContext/@Lang	The Language used for the Jurisdiction Context	M	Attribute	Code	ISO 639-1 two-letter code	SDGR Application Profile	
++++++	JurisdictionLevel	The minimum level of the jurisdiction Granularity Required for proper discovery of the Evidence Provider (MS, NUTS1-3, LAU)	1..1	Attribute	Code		SDGR Application Profile	
++++++	EvidenceProviderClassification	An Evidence Provider Classification is a structured piece of information that is used to provide the context on the classification concepts defined the Data Service Evidence Type an Evidence Provider needs to provide	0..n	InformationConcept			Core Criterion Core Evidence Vocabulary	cccev:InformationConcept
++++++	Identifier	Unambiguous reference to the Information Concept.	1..1	Attribute	Identifier		CCCEV	cccev:identifier
++++++	Type	Category to which the Information Concept belongs.	1..1	Attribute	Code		CCCEV	cccev:type
++++++	ValueExpression	Formulation in a formal language of the expected value(s) for the Classification Concept which is aligned with the concepts from the Requirements defined and	0..1	Attribute	Text		CCCEV	cccev:expressionOfExpected Value

		must be respected by the supplied Supported Values. Currently, the Regular Expression language is supported for strings.						
++++++	Description	Short explanation supporting the understanding of the Classification Concept.	1..n	Attribute	Text		CCCEV	cccev:description
++++++	Publisher	The organisation responsible for issuing Evidences via this Data Service.	1..1	EvidenceProviderType			Core Public Service Vocabulary Application Profile (CPSV-AP)	dct:Agent
++++++	Publisher	The organisation responsible for issuing Evidences via this Data Service.	1..1	EvidenceProviderType			CPSV-AP	dct:Agent
++++++	Identifier	A unique identification for the Publisher or agent.	1..1	Attribute	Identifier		CPSV-AP	dct:identifier
++++++	Name	A short label for the agent.	1..1	Attribute	Text		CPSV-AP	dct:title
++++++	Address	A location of the Publisher in the form of an address.	1..1	AddressType			Core Location	ocn:Address

							Vocabulary (CLV)	
++++++++	Jurisdiction	The jurisdiction to which this Evidence Provider applies.	1..1	JurisdictionType			Core Location Vocabulary (CLV)	ocn:Address
++++++++	Address	A location of the Publisher in the form of an address.	1..1	AddressType			CLV	locn:Address
+++++++++	FullAddress	The complete address written as a string.	0..1	Attribute	Text		CLV	locn:fullAddress
+++++++++	Thoroughfare	The name of a street, passage or way through from one location to another.	0..1	Attribute	Text		CLV	locn:thoroughfare
+++++++++	LocatorDesignator	A number or sequence of characters that uniquely identifies the locator (building number, apartment number, etc.) within the relevant scope.	0..1	Attribute	Text		CLV	locn:locatorDesignator
+++++++++	AdminUnitLevel1	The name of the uppermost level of the address, almost always a country.	0..1	Attribute	Code		CLV	locn:adminUnitL1
+++++++++	AdminUnitLevel2	The name of a secondary level/region of the address, usually a county,	0..1	Attribute	Code		CLV	locn:adminUnitL2

		state or other such area that typically encompasses several localities.						
++++++++	AdminUnitLevel3	The name of a secondary level/region of the address, usually a municipality or other such area that typically encompasses several localities.	0..1	Attribute	Code		CLV	locn:adminUnitL3
++++++++	PostCode	The code created and maintained for postal purposes to identify a subdivision of addresses and postal delivery points.	0..1	Attribute	Code		CLV	locn:postCode
++++++++	PostCityName	The key postal division of the address, usually the city.	0..1	Attribute	Code		CLV	locn:postName
+++++++	Jurisdiction	The Jurisdiction to which this Data Service Evidence Type applies.	1..1	JurisdictionType			Core Criterion Core Evidence Vocabulary	cccev:evidenceTypeJurisdiction
++++++++	AdminUnitLevel1	The name of the uppermost level of the address, almost always a country.	1..1	Attribute	Code		CLV	locn:adminUnitL1

++++++++	AdminUnitLevel2	The name of a secondary level/region of the address, usually a county, state or other such area that typically encompasses several localities.	0..1	Attribute	Code		CLV	locn:adminUnitL2
++++++++	AdminUnitLevel3	The name of a secondary level/region of the address, usually a municipality or other such area that typically encompasses several localities.	0..1	Attribute	Code		CLV	locn:adminUnitL3
++++++	ClassificationConcept	A Classification Concept is a structured piece of information that is used to provide the supported values on the classification concepts defined the Data Service Evidence Type	0..n	InformationConcept			Core Criterion Core Evidence Vocabulary	cccev:InformationConcept
++++++++	Identifier	Unambiguous reference to the Information Concept.	1..1	Attribute	Identifier		CCCEV	cccev:identifier
++++++++	Type	Category to which the Information Concept belongs.	1..1	Attribute	Code		CCCEV	cccev:type
++++++++	ValueExpression	Formulation in a formal language of the expected value(s) for the Classification Concept which is aligned with the concepts from the	0..1	Attribute	Text		CCCEV	cccev:expressionOfExpected Value

		Requirements defined and must be respected by the supplied Supported Values. Currently only Regular Expression is supported.						
++++++++	Description	Short explanation supporting the understanding of the Classification Concept.	1..n	Attribute	Text		CCCEV	cccev:description
++++++++	SupportedValue	The value that is supported by the response	0..1	SupportedValue			XML Schema	
++++++++++	SupportedValue	The value that is supported by the response	0..1	SupportedValue			XML Schema	
++++++++++++	StringValue	Textual field	0..1	Attribute	String		XML	XML Schema data types
++++++++++++	DateValue	Date values (format YYYY-DD-MM)	0..1	Attribute	Date		XML	XML Schema data types
++++++++++++	BooleanValue	"true" or 1 Representing "Yes" affirmative answers "false" or 0 representing "No" negative answers	0..1	Attribute	Boolean		XML	XML Schema data types
++++++++++++	CodeValue	A code for a concept.	0..1	Attribute	Code		XML	XML Schema data types
++++++++++++	DateTimeValue	Date values that include a time (format YYYY-DD-MM hh:mm:ss zzzzzz)	0..1	Attribute	DataTime		XML	XML Schema data types

++++++++++	Identifier	An identifier of a concept, including a schemeID	0..1	Attribute	Identifier		XML	XML Schema data types
++++++++++	URI	A URI, including e-mail addresses	0..1	Attribute	anyURI		XML	XML Schema data types
++++++++++	Time	Time values (format hh:mm:ss)	0..1	Attribute			XML	XML Schema data types
++++++++++	Duration	A duration expressed as Year, Month, Day, Hour and Minutes (format PnYn MnDTnH nMnS)	0..1	Attribute	duration		XML	XML Schema data types
++++++++++	Decimal	A number represented with decimal notation	0..1	Attribute	Decimal		XML	XML Schema data types
++++++++++	Amount	An Amount, and currency, as defined in UN/CEFACT's CCTS	0..1	Attribute	Amount		XML	XML Schema data types

3.1.4.3.3 Example of a sucessful Query Response of the DSD

An example of a successful QueryResponse of the DSD providing a collection of Data Services of Service Providers for a specific Evidence Type is shown below:

```
<?xml version="1.0" encoding="UTF-8"?>
<query:QueryResponse
    xmlns:query="urn:oasis:names:tc:ebxml-regrep:xsd:query:4.0"
    xmlns:rim="urn:oasis:names:tc:ebxml-regrep:xsd:rim:4.0"
    xmlns:rs="urn:oasis:names:tc:ebxml-regrep:xsd:rs:4.0"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns:sdg="http://data.europa.eu/p4s"
    startIndex="0"
    status="urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Success" totalResultCount="1">
    <!-- depending on the count of datasets returned, the totalResultCount attribute should reflect the number of the
datasets returned -->
    <rim:RegistryObjectList>
        <!-- One registry object per dataset -->
        <rim:RegistryObject id="RE238912378">
            <rim:Slot name="DataServiceEvidenceType">
                <rim:SlotValue xsi:type="rim:AnyValueType">
                    <sdg:DataServiceEvidenceType>

                        <!-- - - Evidence Type Metadata - - -->

                        <!-- The Data Service assigned Unique Identifier of the Evidence Type. Must be used in the Evidence
Exchange Request -->
                        <sdg:Identifier>RE238918378</sdg:Identifier>

                        <!-- Classification Information - Used for linking with the Semantic Repository and Evidence Broker
-->

<sdg:EvidenceTypeClassification>http://oots.eu/evidencetypes/germany/geburtsurkunde</sdg:EvidenceTypeClassification>
                        <sdg:Title lang="en">Certificate of Birth</sdg:Title>
                        <sdg:Title lang="de">Geburtsurkunde</sdg:Title>
                        <sdg:Description lang="en">An official certificate of birth of a person - with first name, surname,
sex, date and place of birth, which is obtained from the birth register of the place of birth.</sdg:Description>
                        <sdg:Description lang="de">Eine amtliche Bescheinigung über die Geburt einer Person – mit Vorname,
Familienname, Geschlecht, Datum und Ort der Geburt, welche aus dem Geburtsregister des Geburtsortes erstellt
wird.</sdg:Description>

                        <!-- Distribution Information - Multiple Distributions per Data Service Evidence Type -->
                        <!-- XML Distribution, conforming to the common data model on Birth Certificate -->
                        <sdg:DistributedAs>
```

```
                            <sdg:Format>http://publications.europa.eu/resource/authority/file-type/XML</sdg:Format>
                            <sdg:ConformsTo>https://semic.org/sa/common/birthcert-1.0.0</sdg:ConformsTo>
                        </sdg:DistributedAs>
                        <!-- PDF Distribution. PDF is unstructured data so there is no conformance to a data model -->
                        <sdg:DistributedAs>
                            <sdg:Format>application/pdf</sdg:Format>
                        </sdg:DistributedAs>

                        <!-- - - Evidence Provider and Data Service Metadata - - -->

                        <!-- Access Service represents the Data Service serving the piece of Evidence on behalf of an
Evidence Provider -->
                        <!-- Multiple Access Services, one per Evidence Provider -->
                        <sdg:AccessService>
                            <!-- The Evidence Exchange profile version to which this access service expects / serves -->
                            <sdg:Identifier schemeID="urn:oasis:names:tc:ebcore:partyid-
type:iso6523:0060">8889909098</sdg:Identifier>
                            <!-- The identifier of the Access Service, using ebcore Party ID Type. Used in eDelivery
Evidence Exchange for PMode Mapping -->
                            <sdg:ConformsTo>oots:edm-v1.0</sdg:ConformsTo>

                            <!-- The Evidence Provider Information of this access service -->
                            <sdg:Publisher>
                                <sdg:Identifier schemeID="VAT">DE73524311</sdg:Identifier>
                                <sdg:Name>Civil Registration Office Hamburg</sdg:Name>
                                <sdg:Address>
                                    <sdg:FullAddress>Street ABC</sdg:FullAddress>
                                    <sdg:AdminUnitLevel1>DE</sdg:AdminUnitLevel1>
                                    <!-- NUTS Code -->
                                    <sdg:AdminUnitLevel2>DE12</sdg:AdminUnitLevel2>
                                </sdg:Address>
                                <sdg:Jurisdiction>
                                    <sdg:AdminUnitLevel1>DE</sdg:AdminUnitLevel1>
                                    <sdg:AdminUnitLevel2>DE12</sdg:AdminUnitLevel2>
                                </sdg:Jurisdiction>
                                <!-- - - An Example of an Information Concept that can be provided by the Access Service in
a structured format - - -->
                                <sdg:ClassificationConcept>
                                    <sdg:Identifier>BirthDate</sdg:Identifier>
```

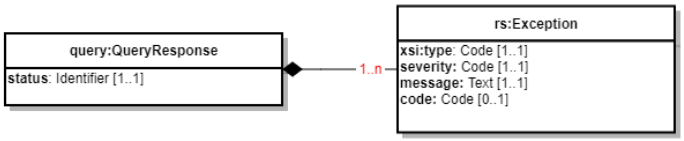
```
                                    <sdg:Type>CertificateOfBirth</sdg:Type>
                                    <sdg:Description>The month, day, and year a person was born</sdg:Description>
                                    <sdg:SupportedValue>
                                        <sdg:DateValue>2022-05-05</sdg:DateValue>
                                    </sdg:SupportedValue>
                                </sdg:ClassificationConcept>
                            </sdg:Publisher>
                        </sdg:AccessService>

                        <!-- Classification Information - Used for linking with the Evidence Broker -->
                        <sdg:AccessService>
                            <sdg:Identifier schemeID="urn:oasis:names:tc:ebcore:partyid-
type:iso6523:0060">8889909099</sdg:Identifier>
                            <sdg:ConformsTo>oots:edm-v1.0</sdg:ConformsTo>
                            <sdg:Publisher>
                                <!-- The Evidence Provider Information -->
                                <sdg:Identifier schemeID="VAT">DE73524311</sdg:Identifier>
                                <sdg:Name>Civil Registration Office Hamburg</sdg:Name>

                                <sdg:Address>
                                    <sdg:FullAddress>Street ABC</sdg:FullAddress>
                                    <sdg:AdminUnitLevel1>DE</sdg:AdminUnitLevel1>
                                    <!-- NUTS Code -->
                                    <sdg:AdminUnitLevel2>DE12</sdg:AdminUnitLevel2>
                                </sdg:Address>

                                <sdg:Jurisdiction>
                                    <sdg:AdminUnitLevel1>DE</sdg:AdminUnitLevel1>
                                    <sdg:AdminUnitLevel2>DE12</sdg:AdminUnitLevel2>
                                </sdg:Jurisdiction>
                            </sdg:Publisher>
                        </sdg:AccessService>
                        <sdg:EvidenceProviderClassification>
                            <sdg:Identifier>CertificateOfBirth</sdg:Identifier>
                            <sdg:Type>Codelist</sdg:Type>
                            <!-- Value from a Codelist required. Must be publised in the Semantic Repository -->
                            <sdg:ValueExpression>http://sr.europa.eu/codelists/birthCertificate</sdg:ValueExpression>
                            <sdg:Description lang="en">Certificate of Birth</sdg:Description>
                        </sdg:EvidenceProviderClassification>
```

```
                    </sdg:DataServiceEvidenceType>
                </rim:SlotValue>
            </rim:Slot>
        </rim:RegistryObject>
    </rim:RegistryObjectList>
</query:QueryResponse>
```

3.1.4.4 Query Error Response of the DSD

3.1.4.4.1 Data Model of the Query Error Responses of the DSD

The Query Error Response of the DSD is syntactically expressed inside an ebRS QueryResponse using the ebRS RegistryExceptionType as shown in data model below:



3.1.4.4.2 Implementation Guideline of the Query Error Response of the DSD

The following table below defines the elements of the data model illustrated above according to the core ebRIM elements of the ebRS RegistryExceptionType .

	Name	Definition	Cardinality	ebRIM type	Data Type	Rules	Domain
	query:QueryResponse	**Query Error Response root element**		RegistryResponseType			ebRIM
+	status	Element used to define the status of the Query Request.	1..1	Attribute	Identifier	Must always be "urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Failure"	ebRIM

						when an EDM Error Response is generated.	
++	**rs:Exception**	**The rs:exeption describes an error which occurs during the processing of a Query Request.**	1..n	RegistryExceptionType			ebRIM
+++	xsi:type	Describes the nature of the error that occurred.	1..1	Attribute	string	Must be one of the exception types listed in the table below describing the DSDErrorResponseCodes.	ebRIM
+++	severity	Is used to show the impact of the error with regard to the business process. Use the severity codes WARNING or FAILURE to scope the impact of the error.	1..1	Attribute	objectReferenceType	default="urn:oasis:names:tc:ebxml-regrep:ErrorSeverityType:Error"	ebRIM
+++	message	Is used to add an error message that can be shown and understood by the user of the system.	1..1	Attribute	string		ebRIM

+++	code	A code that corresponds to the status of the system with regard to the processing of a request. If the specific error codes do not cover the reason for failure use the generic error code "other".	0..1	Attribute	string	Must contain an appropriate value for the code of the expections according to the table below describing the DSDErrorResponseCodes.	ebRIM

3.1.4.4.3 Example of the Query Error Response of the DSD

An example of Query Error Responses of the DSD due to an empty result set of the Data Service is shown in the following XML snippet:

```
<?xml version="1.0" encoding="UTF-8"?>
<query:QueryResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                     xmlns:rs="urn:oasis:names:tc:ebxml-regrep:xsd:rs:4.0"
                     xmlns:rim="urn:oasis:names:tc:ebxml-regrep:xsd:rim:4.0"
                     xmlns:query="urn:oasis:names:tc:ebxml-regrep:xsd:query:4.0"
                     xmlns:xlink="http://www.w3.org/1999/xlink"
                     status="urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Failure">

  <rs:Exception
      xsi:type="rs:ObjectNotFoundExceptionType"
      severity="urn:oasis:names:tc:ebxml-regrep:ErrorSeverityType:Error"
      message="No Data services were found based on the given parameters"
      code="DSD:ERR:0001">
  </rs:Exception>
</query:QueryResponse>
```

3.1.4.4.4 Error Response Codes of the DSD

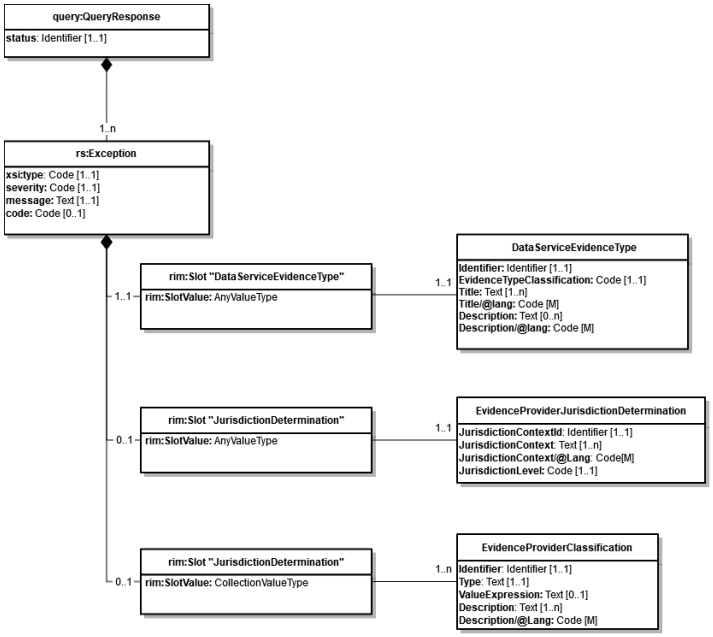
The following table provides the list of QueryErrorResponseCodes for the expections defined in the Query Error Response:
DSDErrorResponseCodes

#	Error Title	Type	code	Message
1	Data Services Not Found	rs:ObjectNotFoundExceptionType	DSD:ERR:0001	No Data Services were found based on the given parameters
2	Evidence Type Not Found	rs:ObjectNotFoundExceptionType	DSD:ERR:0002	The Evidence requested cannot be found
3	Bad Query Parameters	rs:InvalidRequestExceptionType	DSD:ERR:0003	The query parameters do not follow the query specification
4	Unknown Query	rs:InvalidRequestExceptionType	DSD:ERR:0004	The requested Query does not exist
5	Additional Parameters Required	rs:ObjectNotFoundExceptionType	DSD:ERR:0005	The query requires the included extra attributes to be provided by the user
6	Incorrect Parameter Value	rs:InvalidRequestExceptionType	DSD:ERR:0006	Incorrect provided value for requested parameters

3.1.4.5 DSD Response Requesting Additional User Provided Attributes

3.1.4.5.1 Introduction

When a `DataServiceEvidenceType` contains required Evidence Provider Discovery Metadata, the DSD will respond initially with an exception containing the required Discovery Metadata. The exception used is the `DSD:ERR:0005` with type `rs:ObjectNotFoundExceptionType` and uses an extension of the Query Error Response for the DSD Model. The following diagram summarizes the extension of the data model for the DSD:ERR:0005 exception:



The following table below defines the elements of the data model illustrated above according to the core ebRIM elements of the ebRS RegistryExceptionType .

	Name	Definition	Cardinality	ebRIM type	Data Type	Rules	Domain
	query:QueryResponse	**Query Error Response root element**		RegistryResponseType			ebRIM

+	status	Element used to define the status of the Query Request.	1..1	Attribute	Identifier	Must always be "urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Failure" when an EDM Error Response is generated.	ebRIM
++	**rs:Exception**	**The rs:exception describes an error which occurs during the processing of a Query Request.**	1..n	RegistryExceptionType			ebRIM
+++	xsi:type	Describes the nature of the error that occurred.	1..1	Attribute	string	MUST be rs:ObjectNotFoundExceptionType	ebRIM
+++	severity	Is used to show the impact of the error with regard to the business process.	1..1	Attribute	objectReferenceType	default="urn:oasis:names:tc:ebxml-regrep:ErrorSeverityType:Error"	ebRIM

		Use the severity codes WARNING or FAILURE to scope the impact of the error.					
+++	message	Is used to add an error message that can be shown and understood by the user of the system.	1..1	Attribute	string	MUST be equal to the following String: "The query requires the incuded extra attributes to be provided by the user."	ebRIM
+++	code	A code that corresponds to the status of the system with regard to the processing of a request. If	0..1	Attribute	string	MUST be equal to "DSD:ERR:0005"	ebRIM

		the specific error codes do not cover the reason for failure use the generic error code "other".					
++++	rim:slot "DataServiceEvidenceType"	The slot is a container to describe the specific aspects and metadata of the Data Service and Evidence Type.	1..1	SlotType	AnyValueType		ebRIM
++++	rim:slot "DataServiceEvidenceType"	The slot is a container to describe the specific	1..1	SlotType	AnyValueType		ebRIM

		aspects and metadata of the Data Service and Evidence Type.					
+++++	DataServiceEvidenceType	The element describes specific aspects and metadata of the Data Service and Evidence Type.	1..1	DataServiceEvidenceTypeType			SDGR Application Profile
+++++	DataServiceEvidenceType	The element describes specific aspects and metadata of the Data Service and	1..1	DataServiceEvidenceTypeType			SDGR Application Profile

		Evidence Type.					
+++++	Identifier	The unique identifier of the Evidence Type of the Data Service. Must be used in the Evidence Request.	1..1	Attribute	Identifier		DCAT-AP
+++++	EvidenceTypeClassification	A URI pointing to the Evidence Type that this Data Service is supporting. The classification is linked with the Evidence Type of the Semantic Repository	1..1	Attribute	Code		Core Criterion Core Evidence Vocabulary

		(Evidence Broker).					
+++++	Title	A name to identify in natural language the Evidence Type. Unbounded cardinality to support multiple languages.	1..n	Attribute	Text		DCAT-AP
++++++	Title/@lang	The language of the title encoded as ISO 639-1 two-letter code. Default value "en"	M	Attribute	Code	ISO 639-1 two-letter code	DCAT-AP
+++++	Description	A description of the Evidence Type. Unbound	0..n	Attribute	Text		DCAT-AP

		ed cardinality to support multiple languages.					
++++++	Description/@lang	The language of the description encoded as ISO 639-1 two-letter code. Default value "en"	M	Attribute	Code	ISO 639-1 two-letter code	DCAT-AP
++++	rim:slot "JurisdictionDetermination"	The slot is a container to describe the specific aspects and metadata of the Data Service and	0..1	SlotType	AnyValueType		ebRIM

		Evidence Type.					
+++++	EvidenceProviderJurisdictionDetermination	The element describes specific aspects and metadata of the Data Service and Evidence Type.	0..1	DataServiceEvidenceTypeType		Follows the DSD Data Model specification of the EvidenceProviderJurisdictionDetermination	SDGR Application Profile
++++	rim:slot "UserRequestedClassificationConcepts"	The slot is a container to describe the specific aspects and metadata of the Data Service and Evidence Type.	0..1	SlotType	CollectionValueType		ebRIM

+++++	EvidenceProviderClassification	The element describes specific aspects and metadata of the Data Service and Evidence Type.	1..n	EvidenceProviderClassificationType		Follows the DSD Data Model specification of the EvidenceProviderClassification	SDGR Application Profile

3.1.4.5.2 Jurisdiction Context

When the `DataServiceEvidenceType` class contains the `EvidenceProviderJursidictionDetermination`, the returned exception MUST contain:

- One slot with name `DataServiceEvidenceType` with a slot value of type `rim:AnyValueType`. The contents of the slot value MUST be mandatory elements of the `DataServiceEvidenceType` with the descriptions included. When responding to the exception, if the specific DataServiceEvidenceType is the one selected by the user, the Evidence Requester MUST add a new query parameter with name `evidence-type-id` and value the identifier of the `DataServiceEvidenceType`.
- One slot with name `JurisdictionDetermination` with a slot value of type `rim:AnyValueType`. The contents of the slot value MUST be the complete structure of the `EvidenceProviderJursidictionDetermination`. When responding to the exception, the Evidence Requester MUST add a new query parameter with name `jurisdiction-context-id` with a value equal to the JurisdictionContextId element's value of the `JurisdictionDerermination` slot.
- Additionally, the query must now provide the extra level of jurisdiction level values required, as declared in the `JurisdictionLevel` element of the `JurisdictionDetermination` slot, by using the pre-defined parameters `jurisdiction-admin-l3` and/or `jurisdiction-admin-l2`

The following example shows an exception sent back to the Evidence Requester containing a `JurisdictionDetermination` slot, stating that the user should provide his place of birth using LAU codes:

```
<query:QueryResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns:rs="urn:oasis:names:tc:ebxml-regrep:xsd:rs:4.0"
    xmlns:rim="urn:oasis:names:tc:ebxml-regrep:xsd:rim:4.0"
    xmlns:query="urn:oasis:names:tc:ebxml-regrep:xsd:query:4.0"
    xmlns:sdg="http://data.europa.eu/p4s"
    requestId="c4369c4d-740e-4b64-80f0-7b209a66d629"
    status="urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Failure">

    <!-- Additional elements describing the response -->

    <rs:Exception xsi:type="rs:ObjectNotFoundExceptionType" severity="FAILURE"
        message="The query requires the incuded extra attributes to be provided by the user."
        code="DSD:ERR:0005">
        <rim:Slot name="DataServiceEvidenceType">
            <rim:SlotValue xsi:type="rim:AnyValueType">
                <sdg:DataServiceEvidenceType xmlns:sdg="http://data.europa.eu/p4s">
                    <sdg:Identifier>DSEV-ID1</sdg:Identifier>
                    <sdg:EvidenceTypeClassification>CertificateOfBirth</sdg:EvidenceTypeClassification>
                    <sdg:Title>Certificate Of Birth</sdg:Title>
                    <sdg:Description>
                        Certificate Of Birth provided by the regional service providers of Region A of country MS.
                        Evidence Provider Jurisdiction is resolved at Municipality level, where the natural person has its
place of birth.
                    </sdg:Description>
                </sdg:DataServiceEvidenceType>
            </rim:SlotValue>
        </rim:Slot>
        <!-- Jurisdiction Mapping Requests -->
        <rim:Slot name="JurisdictionDetermination">
            <rim:SlotValue xsi:type="rim:AnyValueType">
                <sdg:EvidenceProviderJurisdictionDetermination>
                    <sdg:JurisdictionContextId>PlaceOfBirth</sdg:JurisdictionContextId>
                    <sdg:JurisdictionContext lang="en">Place Of Birth</sdg:JurisdictionContext>
                    <sdg:JurisdictionLevel>https://sr.ec.europa.eu/codelist/locationLevel/LAU</sdg:JurisdictionLevel>
                </sdg:EvidenceProviderJurisdictionDetermination>
            </rim:SlotValue>
        </rim:Slot>
    </rs:Exception>
</query:QueryResponse>
```

When responding to the example above, the Evidence Requester MUST add the JurisdictionContextId parameter with the value of the JurisdictionContextId found in the exception, accompanied by the proper jurisdiction level (in the example the LAU code) provided by the user as follows: *«server base url»*/rest/search?queryId=urn:oots:dsd:ebxml-regrep:queries:dataservices-by-evidencetype-and-jurisdiction&evidence-type-classification=CertificateOfBirth&country-code=MS**&evidence-type-id=DSEV-ID1&jurisdiction-context-id=PlaceOfBirth&jurisdiction-admin-l2=MS202&jurisdiction-admin-l3=02200334**

3.1.4.5.3 Evidence Provider Classification

When the `DataServiceEvidenceType` class contains the `EvidenceProviderClassification` elements, the returned exception MUST contain:

- One slot with name `DataServiceEvidenceType` with a slot value of type `rim:AnyValueType`. The contents of the slot value MUST be mandatory elements of the `DataServiceEvidenceType` with the descriptions included. When responding to the exception, if the specific DataServiceEvidenceType is the one selected by the user, the Evidence Requester MUST add a new query parameter with name `evidence-type-id` and value the identifier of the `DataServiceEvidenceType`.
- one slot with name `UserRequestedClassificationConcepts` with a slot value of type `rim:CollectionValueType` with `collectionType="urn:oasis:names:tc:ebxml-regrep:CollectionType:Set"`. The contents of the slot value MUST be the complete structure of the `EvidenceProviderClassification`, with each `EvidenceProviderClassification` placed inside a `rim:element` of type `rim:AnyValyeType`. When responding to the exception, the Evidence Requester MUST add a new query parameter for every Classification Concept existing in the `EvidenceProviderClassification` element, using the `ClassificationConcept` Identifier as its name and providing as a value one that complies with the `Type`, `ValueExpression` and `Description` of the `Classification Concept`.

The following example shows an exception sent back to the Evidence Requester containing a `UserRequestedClassificationConcepts` slot, stating that the user should provide his type of insurance using a string value:

```
<query:QueryResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns:rs="urn:oasis:names:tc:ebxml-regrep:xsd:rs:4.0"
    xmlns:rim="urn:oasis:names:tc:ebxml-regrep:xsd:rim:4.0"
    xmlns:query="urn:oasis:names:tc:ebxml-regrep:xsd:query:4.0"
    xmlns:sdg="http://data.europa.eu/p4s"
    xmlns:xlink="http://www.w3.org/1999/xlink"
    requestId="c4369c4d-740e-4b64-80f0-7b209a66d629"
    status="urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Failure">
```

```
    <!-- Additional elements describing the response -->

    <rs:Exception xsi:type="rs:ObjectNotFoundExceptionType" severity="FAILURE"
        message="The query requires the incuded extra attributes to be provided by the user."
        code="DSD:ERR:0005">
        <rim:Slot name="DataServiceEvidenceType">
            <rim:SlotValue xsi:type="rim:AnyValueType">
                <sdg:DataServiceEvidenceType xmlns:sdg="http://data.europa.eu/p4s">
                    <sdg:Identifier>DSEV-ID1</sdg:Identifier>
                    <sdg:EvidenceTypeClassification>CertificateOfInsurance</sdg:EvidenceTypeClassification>
                    <sdg:Title>Certificate Of Insurance</sdg:Title>
                    <sdg:Description>
                        Certificate Of Insurance provided by the regional service providers of Region A of country MS.
                        Evidence providers are classified according to the type of insurance the Evidence Subject has.
                    </sdg:Description>
                </sdg:DataServiceEvidenceType>
            </rim:SlotValue>
        </rim:Slot>

        <rim:Slot name="UserRequestedClassificationConcepts">
            <rim:SlotValue xsi:type="rim:CollectionValueType"
                collectionType="urn:oasis:names:tc:ebxml-regrep:CollectionType:Set">
                <rim:Element xsi:type="rim:AnyValueType">
                    <sdg:EvidenceProviderClassification>
                        <sdg:Identifier>TypeOfInsurance</sdg:Identifier>
                        <sdg:Type>String</sdg:Type>
                        <!-- Value from a Codelist required. Must be publised in the Semantic Repository -->
                        <sdg:ValueExpression>http://sr.europa.eu/codelists/birthCertificate</sdg:ValueExpression>
                        <sdg:Description lang="en">Type of insurance</sdg:Description>
                    </sdg:EvidenceProviderClassification>
                </rim:Element>
            </rim:SlotValue>
        </rim:Slot>
    </rs:Exception>
</query:QueryResponse>
```

When responding to the example above, the Evidence Requester MUST add the *TypeOfInsurance* parameter with the proper string value provided by the user as follows:
«server base url»/rest/search?queryId=urn:fdc:oots:dsd:ebxml-regrep:queries:dataservices-by-evidencetype-and-jurisdiction&evidence-type-classification=CertificateOfInsurance&country-code=MS**&evidence-type-id=DSEV-ID1&TypeOfInsurance=public**. Since the evidence provider classification identifier values are used as query parameters, they MUST be different from any of the predefined query parameters.

3.1.4.6 Response Signature

The DSD Service signs the query responses using JWS detached signature following the HttpHeaders Mechanism of the ETSI ESI JAdES specification. In accordance with ENISA's Good Practises in Cryptography – Primitives and Schemes, the following algorithms found in [RFC7518] are selected to be used in the following form:

- The EdDSA Algorithm [RFC8032] using one of the curves defined in RFC7748 shall be used. The value "EdDSA" for the "alg" parameter MUST be used and the curve shall be encoded in the "crv" parameter as defined in RFC8037.

The following sets of rules shall apply in the application of the HttpHeaders mechanism ETSI ESI Jades compliant signature:

- The JWS content (Data to be Signed) MUST be detached from the signatures as defined in RFC7515 Appendix F.
- The signed `SigD` parameter object MUST be present in the JWS headers, denoting the use of the JAdES detached header profile.
- The value of the `mId` parameter MUST be set to `"http://uri.etsi.org/19182/HttpHeaders"`.
- The `pars` array of the `SigD` MUST contain only the element "digest", denoting that for the calculation of the signature only the digest of the HTTP payload must be taken into account, according to [RFC3230].
- The `alg` parameter is set to `"EdDSA"` and the `crv` parameter MUST be set.

The JWS structure shall be carried in the HTTP header field named `"oots-response-sig"`.

3.1.4.7 Transport Security

DSD clients shall connect to a Data Service Directory using secure HTTP (HTTP over Transport Layer Security).

3.1.4.8 A DSD Interaction Example Flow (Informative)

3.1.4.8.1 Introduction

To make it clearer on how the exception-based flow can work as a dialog-based interaction, we provide the following example flow.

3.1.4.8.2 Registration by the MS

In this example flow, a MS needs to register an **Insurance Certificate for Companies** evidence type. For this specific MS, the evidence type is issued by Evidence Providers that are located in the same region as the **company's headquarters** and thus the Jurisdiction Determination context is "Company's headquarters location", **with the response required to be a NUTS2 based code**. The following snippet shows how this jurisdiction context is defined in the DSD DataServiceEvidenceType element:

```
<?xml version="1.0" encoding="UTF-8"?>
<sdg:DataServiceEvidenceType>

    <!-- - - Evidence Type Metadata - - -->
    <sdg:Identifier>RE238918378</sdg:Identifier>

    <!-- Classification Information - Used for linking with the Evidence Broker -->
    <sdg:EvidenceTypeClassification>CertificateOfInsurance</sdg:EvidenceTypeClassification>
    <sdg:Title>Certificate of Insurance</sdg:Title>

    <!-- Distribution Information - Multiple Distributions per Data Service Evidence Type -->
    <!-- XML Distribution, conforming to the common data model on Birth Certificate -->
    <sdg:DistributedAs>
        <sdg:Format>http://publications.europa.eu/resource/authority/file-type/XML</sdg:Format>
        <sdg:ConformsTo>https://semic.org/sa/common/insurancecert-1.0.0</sdg:ConformsTo>
    </sdg:DistributedAs>
    <!-- PDF Distribution. PDF is unstructured data so there is no conformance to a data model -->
    <sdg:DistributedAs>
        <sdg:Format>application/pdf</sdg:Format>
    </sdg:DistributedAs>

    <!-- - - Evidence Provider and Data Service Metadata - - -->
    <!-- Access Service represents the Data Service serving the piece of Evidence on behalf of an Evidence Provider -->
    <!-- Multiple Access Services, one per Evidence Provider -->
    <!-- Declaration of the possible classifications of the Evidence provider ... Omitted in this snippet -->

    <!-- Determination of the Jurisdiction Mapping to the User's attributes. NUTS2 is required -->
    <sdg:EvidenceProviderJurisdictionDetermination>
        <sdg:JurisdictionContextId>CompanyHq</sdg:JurisdictionContextId>
```

```
        <sdg:JurisdictionContext>Company's Headquarters Location</sdg:JurisdictionContext>
        <sdg:JurisdictionLevel>https://sr.ec.europa.eu/codelist/locationLevel/NUTS2</sdg:JurisdictionLevel>
    </sdg:EvidenceProviderJurisdictionDetermination>

    <!-- - - - Data Service Identity Matching Requirements - - - -->
    <!-- Level Of Assurance Required for the Evidence Type by the Evidence Provider ... Omitted in this snippet -->
    <sdg:EvidenceProviderClassification>
        <sdg:Identifier>TypeOfInsurance</sdg:Identifier>
        <sdg:Type>Codelist</sdg:Type>
        <!-- Value from a Codelist required. Must be published in the Semantic Repository -->
        <sdg:ValueExpression>http://sr.europa.eu/codelists/insuranceType</sdg:ValueExpression>
        <sdg:Description lang="en">Type Of Insurance</sdg:Description>
    </sdg:EvidenceProviderClassification>
</sdg:DataServiceEvidenceType>
```

This specific evidence type also depends on Evidence Provider classifications. Although several Evidence Providers can issue the specific evidence type, the Evidence Providers can issue the evidence type only for a specific kind of insurance the company endorses. Thus a classification scheme of the Evidence Providers must be declared in the DataServiceEvidenceType using the Evidence Provider Classification Mechanism. The following snippet describes the declaration of the classification scheme required for this evidence type:

```
<?xml version="1.0" encoding="UTF-8"?>
<sdg:DataServiceEvidenceType>
    <!-- - - Evidence Type Metadata - - -->
    <sdg:Identifier>RE238918378</sdg:Identifier>

    <!-- Classification Information - Used for linking with the Evidence Broker -->
    <sdg:EvidenceTypeClassification>CertificateOfInsurance</sdg:EvidenceTypeClassification>
    <sdg:Title>Certificate of Insurance</sdg:Title>

    <!-- Distribution Information - Multiple Distributions per Data Service Evidence Type -->
    <!-- XML Distribution, conforming to the common data model on Birth Certificate -->
    <sdg:DistributedAs>
        <sdg:Format>http://publications.europa.eu/resource/authority/file-type/XML</sdg:Format>
        <sdg:ConformsTo>https://semic.org/sa/common/insurancecert-1.0.0</sdg:ConformsTo>
    </sdg:DistributedAs>
    <!-- PDF Distribution. PDF is unstructured data so there is no conformance to a data model -->
```

```
    <sdg:DistributedAs>
        <sdg:Format>application/pdf</sdg:Format>
    </sdg:DistributedAs>

    <!-- - - Evidence Provider and Data Service Metadata - - -->
    <!-- Access Service represents the Data Service serving the piece of Evidence on behalf of an Evidence Provider -->
    <!-- Multiple Access Services, one per Evidence Provider -->
    <!-- Declaration of the possible classifications of the Evidence Provider ... Omitted in this snippet -->

    <!-- Declaration of the possible classifications of the Evidence Provider -->
    <sdg:EvidenceProviderClassification>
        <sdg:Identifier>TypeOfInsurance</sdg:Identifier>
        <sdg:Type>Codelist</sdg:Type>
        <!-- Value from a Codelist required. Must be publised in the Semantic Repository -->
        <sdg:ValueExpression>http://sr.europa.eu/codelists/insuranceType</sdg:ValueExpression>
        <sdg:Description lang="en">Type Of Insurance</sdg:Description>
    </sdg:EvidenceProviderClassification>

    <!-- Determination of the Jurisdiction Mapping to the User's attributes. -->
    <!-- - - - Data Service Identity Matching Requirements - - - -->
    <!-- Level Of Assurance Required for the Evidence Type by the Evidence Provider ... Omitted in this snippet -->
</sdg:DataServiceEvidenceType>
```

3.1.4.8.3 Registration of Data Services and Evidence Providers

The Evidence Providers of the specific MS must now register their capability on providing the Insurance certificate, but associating themselves to the specific `DataServiceEvidenceType` registered by the MS. For the example, two Evidence Providers are able to issue this evidence type for the MS, but are assigned different types of classifications. Evidence Provider 1 supports public insurance policies, while evidence provider 2 supports only private ones. The following snippet shows how the data services will be properly declared to contain also these classifications:

```
<!-- Multiple Access Services, one per Evidence Provider -->
<sdg:AccessService>
    <!-- The identifier of the Access Service, using ebcore Party ID Type. Used in eDelivery Evidence Exchange for PMode
Mapping -->
    <sdg:Identifier schemeID="urn:oasis:names:tc:ebcore:partyid-type:iso6523:0060">8889909098</sdg:Identifier>
```

```
    <!-- The Evidence Exchange profile version to which this access service expects / serves -->
    <sdg:ConformsTo>oots:edm-v1.0</sdg:ConformsTo>

    <!-- Access Service of an Evidence Provider supporting only Private Insurance Types -->
    <sdg:Publisher>
        <sdg:Identifier schemeID="1204">11231112313</sdg:Identifier>
        <sdg:Name>Example Organization</sdg:Name>
        <sdg:Address>
            <sdg:AdminUnitLevel1>MS</sdg:AdminUnitLevel1>
        </sdg:Address>
        <sdg:Jurisdiction>
            <sdg:AdminUnitLevel1>MS12</sdg:AdminUnitLevel1>
        </sdg:Jurisdiction>

        <!-- Information Concepts that Classify the Evidence Provider -->
        <sdg:ClassificationConcept>
            <sdg:Identifier>TypeOfInsurance</sdg:Identifier>
            <sdg:SupportedValue>
                <sdg:StringValue>private</sdg:StringValue>
            </sdg:SupportedValue>
        </sdg:ClassificationConcept>
    </sdg:Publisher>
</sdg:AccessService>

<sdg:AccessService>
<!-- The identifier of the Access Service, using ebcore Party ID Type. Used in eDelivery Evidence Exchange for PMode
Mapping -->
    <sdg:Identifier schemeID="urn:oasis:names:tc:ebcore:partyid-type:iso6523:0060">8889909098</sdg:Identifier>
    <!-- The Evidence Exchange profile version to which this access service expects / serves -->
    <sdg:ConformsTo>oots:edm-v1.0</sdg:ConformsTo>

    <!-- Access Service of an Evidence Provider supporting only Private Insurance Types -->
    <sdg:Publisher>
        <sdg:Identifier schemeID="1204">Ev-1</sdg:Identifier>
        <sdg:Name>Evidence Provider 1</sdg:Name>
        <sdg:Address>
            <sdg:AdminUnitLevel1>MS</sdg:AdminUnitLevel1>
        </sdg:Address>
```

```
        <sdg:Jurisdiction>
        <!-- NUTS Code -->
            <sdg:AdminUnitLevel1>MS12</sdg:AdminUnitLevel1>
        </sdg:Jurisdiction>

        <!-- Information Concepts that Classify the Evidence Provider -->
        <sdg:ClassificationConcept>
            <sdg:Identifier>TypeOfInsurance</sdg:Identifier>
            <sdg:SupportedValue>
                <sdg:StringValue>public</sdg:StringValue>
            </sdg:SupportedValue>
        </sdg:ClassificationConcept>
    </sdg:Publisher>
</sdg:AccessService>
```

These two registration are then integrated into the complete record in the DSD as follows:

```
<?xml version="1.0" encoding="UTF-8"?>
<query:QueryResponse
    xmlns:query="urn:oasis:names:tc:ebxml-regrep:xsd:query:4.0"
    xmlns:rim="urn:oasis:names:tc:ebxml-regrep:xsd:rim:4.0"
    xmlns:rs="urn:oasis:names:tc:ebxml-regrep:xsd:rs:4.0"
    startIndex="0"
    status="urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Success" totalResultCount="1"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns:sdg="http://data.europa.eu/p4s"
    xmlns:xmime="http://www.w3.org/2005/05/xmlmime"
    xmlns:xlink="http://www.w3.org/1999/xlink"
    xmlns:xml="http://www.w3.org/XML/1998/namespace">
    <!-- depending on the count of datasets returned, the totalResultCount attribute should
reflect the number of the datasets returned -->
    <rim:RegistryObjectList>
        <!-- One registry object per dataset -->
        <rim:RegistryObject id="RE238912378">
            <rim:Slot name="DataServiceEvidenceType">
                <rim:SlotValue xsi:type="rim:AnyValueType">
```

```
                    <sdg:DataServiceEvidenceType>

                        <!-- - - Evidence Type Metadata - - -->
                        <sdg:Identifier>RE238918378</sdg:Identifier>
                        <!-- Classification Information - Used for linking with the Evidence Broker -->
                        <sdg:EvidenceTypeClassification>CertificateOfInsurance</sdg:EvidenceTypeClassification>
                        <sdg:Title>Certificate of Insurance</sdg:Title>

                        <!-- Distribution Information - Multiple Distributions per Data Service Evidence Type -->
                        <!-- XML Distribution, conforming to the common data model on Birth Certificate -->
                        <sdg:DistributedAs>
                            <sdg:Format>http://publications.europa.eu/resource/authority/file-type/XML</sdg:Format>
                            <sdg:ConformsTo>https://semic.org/sa/common/insurancecert-1.0.0</sdg:ConformsTo>
                        </sdg:DistributedAs>
                        <!-- PDF Distribution. PDF is unstructured data so there is no conformance to a data model -->
                        <sdg:DistributedAs>
                            <sdg:Format>application/pdf</sdg:Format>
                        </sdg:DistributedAs>

                        <!-- - - Evidence Provider and Data Service Metadata - - -->
                        <!-- Access Service represents the Data Service serving the piece of Evidence on behalf of an
Evidence Provider -->
                        <!-- Multiple Access Services, one per Evidence Provider -->
                        <sdg:AccessService>
                            <!-- The identifier of the Access Service, using ebcore Party ID Type. Used in eDelivery
Evidence Exchange for PMode Mapping -->
                            <sdg:Identifier schemeID="urn:oasis:names:tc:ebcore:partyid-
type:iso6523:0060">8889909098</sdg:Identifier>
                            <!-- The Evidence Exchange profile version to which this access service expects / serves -->
                            <sdg:ConformsTo>oots:edm-v1.0</sdg:ConformsTo>

                            <!-- Access Service of an Evidence Provider supporting only Private Insurance Types -->
                            <sdg:Publisher>
                                <sdg:Identifier schemeID="1204">Ev-1</sdg:Identifier>
                                <sdg:Name>Evidence Provider 1</sdg:Name>

                                <sdg:Address>
                                    <sdg:AdminUnitLevel1>MS</sdg:AdminUnitLevel1>
```

```
                                </sdg:Address>

                                <sdg:Jurisdiction>
                                    <sdg:AdminUnitLevel1>MS12</sdg:AdminUnitLevel1>
                                </sdg:Jurisdiction>

                                <!-- Information Concepts that Classify the Evidence Provider -->

                                <sdg:ClassificationConcept>
                                    <sdg:Identifier>TypeOfInsurance</sdg:Identifier>
                                    <sdg:SupportedValue>
                                        <sdg:StringValue>public</sdg:StringValue>
                                    </sdg:SupportedValue>
                                </sdg:ClassificationConcept>

                            </sdg:Publisher>
                        </sdg:AccessService>

                        <!-- Access Service of an Evidence Provider supporting only Public Insurance Types -->
                        <sdg:AccessService>
                            <sdg:Identifier schemeID="urn:oasis:names:tc:ebcore:partyid-
type:iso6523:0060">8889909099</sdg:Identifier>
                            <sdg:ConformsTo>oots:edm-v1.0</sdg:ConformsTo>
                            <sdg:Publisher>
                                <!-- The Evidence Provider Information -->
                                <sdg:Identifier schemeID="1204">Ev-2</sdg:Identifier>
                                <sdg:Name>Evidence Provider 2</sdg:Name>

                                <sdg:Address>
                                    <!-- NUTS Code -->
                                    <sdg:AdminUnitLevel1>MS</sdg:AdminUnitLevel1>
                                    <sdg:AdminUnitLevel2>MS77</sdg:AdminUnitLevel2>
                                </sdg:Address>

                                <sdg:Jurisdiction>
                                    <sdg:AdminUnitLevel1>MS</sdg:AdminUnitLevel1>
                                    <!-- NUTS Code -->
                                    <sdg:AdminUnitLevel2>MS77</sdg:AdminUnitLevel2>
                                </sdg:Jurisdiction>
```

```
                                <sdg:ClassificationConcept>
                                    <sdg:Identifier>TypeOfInsurance</sdg:Identifier>
                                    <sdg:SupportedValue>
                                        <sdg:StringValue>public</sdg:StringValue>
                                    </sdg:SupportedValue>
                                </sdg:ClassificationConcept>


                            </sdg:Publisher>
                        </sdg:AccessService>

                        <!-- - - - Data Service Identity Matching Requirements - - - -->
                        <!-- Level Of Assurance Required for the Evidence Type by the Evidence Provider -->

<sdg:AuthenticationLevelOfAssurance>http://eidas.europa.eu/LoA/High</sdg:AuthenticationLevelOfAssurance>
                        <!-- Determination of the Jurisdiction Mapping to the User's attributes. NUTS2 is required -->
                        <sdg:EvidenceProviderJurisdictionDetermination>
                            <sdg:JurisdictionContextId>CompanyHq</sdg:JurisdictionContextId>
                            <sdg:JurisdictionContext>Company's Headquarters Location</sdg:JurisdictionContext>

<sdg:JurisdictionLevel>https://sr.ec.europa.eu/codelist/locationLevel/NUTS2</sdg:JurisdictionLevel>
                        </sdg:EvidenceProviderJurisdictionDetermination>
                        <!-- Determination of the Jurisdiction Mapping to the User's attributes. NUTS2 is required -->
                        <!-- Declaration of the possible classifications of the Evidence Provider -->
                        <sdg:EvidenceProviderClassification>
                            <sdg:Identifier>TypeOfInsurance</sdg:Identifier>
                            <sdg:Type>Codelist</sdg:Type>
                            <!-- Value from a Codelist required. Must be publised in the Semantic Repository -->
                            <sdg:ValueExpression>http://sr.europa.eu/codelists/insuranceType</sdg:ValueExpression>
                            <sdg:Description lang="en">Type Of Insurance</sdg:Description>
                        </sdg:EvidenceProviderClassification>
                    </sdg:DataServiceEvidenceType>
                </rim:SlotValue>
            </rim:Slot>
        </rim:RegistryObject>
    </rim:RegistryObjectList>
</query:QueryResponse>
```

3.1.4.8.4 Evidence Requester Query

The Evidence Requester needs to fetch the Evidence Providers that can provide an evidence type with Evidence Type Classification `CertificateOfInsurance`, as it was extracted from the Evidence Broker. To do this, it executes the following HTTP REST Call to the DSD:
«server base url»/rest/search?queryId=urn:fdc:oots:dsd:ebxml-regrep:queries:dataservices-by-evidencetype-and-jurisdiction&**evidence-type-classification=CertificateOfInsurance&country-code=MS**
The DSD receives the requests and checks whether the specific evidenceType for country MS has a `DataServiceEvidenceType` contains either a Jurisdiction Context or a classification scheme. In our example, both exists and thus it must return an exception requesting information on both the Jurisdiction Context and the Classification Scheme, as follows:

```
<?xml version="1.0" encoding="UTF-8" ?>
<query:QueryResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:rs="urn:oasis:names:tc:ebxml-regrep:xsd:rs:4.0"
  xmlns:rim="urn:oasis:names:tc:ebxml-regrep:xsd:rim:4.0"
  xmlns:query="urn:oasis:names:tc:ebxml-regrep:xsd:query:4.0"
  xmlns:sdg="http://data.europa.eu/p4s"
  xmlns:xlink="http://www.w3.org/1999/xlink"
  requestId="c4369c4d-740e-4b64-80f0-7b209a66d629"
  status="urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Failure">

  <!-- Additional elements describing the response -->

  <rs:Exception xsi:type="rs:ObjectNotFoundExceptionType" severity="FAILURE"
    message="The query requires the included extra attributes to be provided by the user."
    code="DSD:ERR:0005">
    <rim:Slot name="DataServiceEvidenceType">
      <rim:SlotValue xsi:type="rim:AnyValueType">
        <sdg:DataServiceEvidenceType xmlns:sdg="http://data.europa.eu/p4s">
          <sdg:Identifier>DSEV-ID1</sdg:Identifier>
          <sdg:EvidenceTypeClassification>CertificateOfInsurance</sdg:EvidenceTypeClassification>
          <sdg:Title>Certificate Of Insurance</sdg:Title>
```

```
          <sdg:Description>
            Certificate Of Insurance provided by the regional service providers of Region A of MS C.
            Evidence Provider Jurisdiction is resolved at Municipality level, where the company has its office
headquarters.
            Evidence providers are classified according to the type of insurance the Evidence Subject has.
          </sdg:Description>
        </sdg:DataServiceEvidenceType>
      </rim:SlotValue>
    </rim:Slot>
    <!-- Jurisdiction Mapping Requests -->
    <rim:Slot name="JurisdictionDetermination">
      <rim:SlotValue xsi:type="rim:AnyValueType">
        <sdg:EvidenceProviderJurisdictionDetermination>
          <sdg:JurisdictionContextId>CompanyHq</sdg:JurisdictionContextId>
          <sdg:JurisdictionContext>Company Headquarters location</sdg:JurisdictionContext>
          <sdg:JurisdictionLevel>https://sr.ec.europa.eu/codelist/locationLevel/NUTS2</sdg:JurisdictionLevel>
        </sdg:EvidenceProviderJurisdictionDetermination>
      </rim:SlotValue>
    </rim:Slot>

    <!-- Evidence Provider Classification Scheme -->
    <rim:Slot name="UserRequestedClassificationConcepts">
      <rim:SlotValue xsi:type="rim:CollectionValueType">
        <rim:Element xsi:type="rim:AnyValueType">
          <sdg:EvidenceProviderClassification>
            <sdg:Identifier>TypeOfInsurance</sdg:Identifier>
            <sdg:Type>Codelist</sdg:Type>
            <sdg:ValueExpression>http://sr.europa.eu/codelists/insuranceType</sdg:ValueExpression>
            <sdg:Description lang="en">Type of insurance</sdg:Description>
          </sdg:EvidenceProviderClassification>
        </rim:Element>
      </rim:SlotValue>

    </rim:Slot>
  </rs:Exception>
</query:QueryResponse>
```

The Evidence Requester will then request the company's headquarters location, using the NUTS2 codes of country MS and will also ask the type of insurance the company supports from the user and then create a new HTTP as follows:
«server base url»/rest/search?queryId=urn:fdc:oots:dsd:ebxml-regrep:queries:dataservices-by-evidencetype-and-jurisdiction&**evidence-type-classification=CertificationOfInsurance&country-code=MS&evidence-type-id=DSEV-ID1&jurisdiction-context-id=CompanyHq&jurisdiction-admin-l2=MS77&TypeOfInsurance=public**
where "DSEV-ID1", "MS77" and "public" are values provided by the user.
The DSD is now able to properly provide a `DataServiceEvidenceType` with the appropriate Data Services and Evidence Providers. for our example, the following response will be returned:

```
<?xml version="1.0" encoding="UTF-8"?>
<sdg:DataServiceEvidenceType>

    <!-- - - Evidence Type Metadata - - -->
    <sdg:Identifier>RE238918378</sdg:Identifier>

    <!-- Classification Information - Used for linking with the Evidence Broker -->
    <sdg:EvidenceTypeClassification>CertificateOfInsurance</sdg:EvidenceTypeClassification>
    <sdg:Title>Certificate of Insurance</sdg:Title>

    <!-- Distribution Information - Multiple Distributions per Data Service Evidence Type -->
    <!-- XML Distribution, conforming to the common data model on Birth Certificate -->
    <sdg:DistributedAs>
         <sdg:Format>http://publications.europa.eu/resource/authority/file-type/XML</sdg:Format>
         <sdg:ConformsTo>https://semic.org/sa/common/insurancecert-1.0.0</sdg:ConformsTo>
    </sdg:DistributedAs>
     <!-- PDF Distribution. PDF is unstructured data so there is no conformance to a data model -->
    <sdg:DistributedAs>
         <sdg:Format>application/pdf</sdg:Format>
    </sdg:DistributedAs>

        <!-- - - Evidence Provider and Data Service Metadata - - -->
        <!-- Access Service represents the Data Service serving the piece of Evidence on behalf of an Evidence Provider -->
        <!-- Access Service of an Evidence Provider supporting only Public Insurance Types -->
    <sdg:AccessService>
        <sdg:Identifier schemeID="urn:oasis:names:tc:ebcore:partyid-type:iso6523:0060">8889909099</sdg:Identifier>
        <sdg:ConformsTo>oots:edm-v1.0</sdg:ConformsTo>
        <sdg:Publisher>
        <!-- The Evidence Provider Information -->
            <sdg:Identifier schemeID="1204">Ev-2</sdg:Identifier>
            <sdg:Name>Evidence Provider 2</sdg:Name>

            <sdg:Address>
                <sdg:AdminUnitLevel1>MS</sdg:AdminUnitLevel1>
                    <!-- NUTS Code -->
                    <sdg:AdminUnitLevel2>MS77</sdg:AdminUnitLevel2>
            </sdg:Address>

            <sdg:Jurisdiction>
```

```
                <sdg:AdminUnitLevel1>MS</sdg:AdminUnitLevel1>
                  <!-- NUTS Code -->
                <sdg:AdminUnitLevel2>MS77</sdg:AdminUnitLevel2>
            </sdg:Jurisdiction>
            <sdg:ClassificationConcept>
                <sdg:Identifier>TypeOfInsurance</sdg:Identifier>
                <sdg:SupportedValue>
                    <sdg:StringValue>public</sdg:StringValue>
                </sdg:SupportedValue>
                </sdg:ClassificationConcept>

        </sdg:Publisher>
    </sdg:AccessService>

        <!-- Determination of the Jurisdiction Mapping to the User's attributes. NUTS2 is required -->
    <sdg:EvidenceProviderJurisdictionDetermination>
            <sdg:JurisdictionContextId>CompanyHq</sdg:JurisdictionContextId>
            <sdg:JurisdictionContext>Company's Headquarters Location</sdg:JurisdictionContext>
            <sdg:JurisdictionLevel>https://sr.ec.europa.eu/codelist/locationLevel/NUTS2</sdg:JurisdictionLevel>
    </sdg:EvidenceProviderJurisdictionDetermination>
        <!-- Declaration of the possible classifications of the Evidence Provider -->
    <sdg:EvidenceProviderClassification>
        <sdg:Identifier>TypeOfInsurance</sdg:Identifier>
        <sdg:Type>Codelist</sdg:Type>
        <!-- Value from a Codelist required. Must be published in the Semantic Repository -->
        <sdg:ValueExpression>http://sr.europa.eu/codelists/insuranceType</sdg:ValueExpression>
        <sdg:Description lang="en">Type Of Insurance</sdg:Description>
    </sdg:EvidenceProviderClassification>
</sdg:DataServiceEvidenceType>
```

3.1.5 LCM Interface Specification

The DSD Service provides an Regrep 4.0 based LCM API, following the Regrep 4.0 LCM SubmitObjects Profile of the OOTS Common Services. This section defines the Classification Scheme, Classification Nodes, Associations and Registry Objects of the SubmitObjects Request Message.

3.1.5.1 Classification Scheme and Nodes

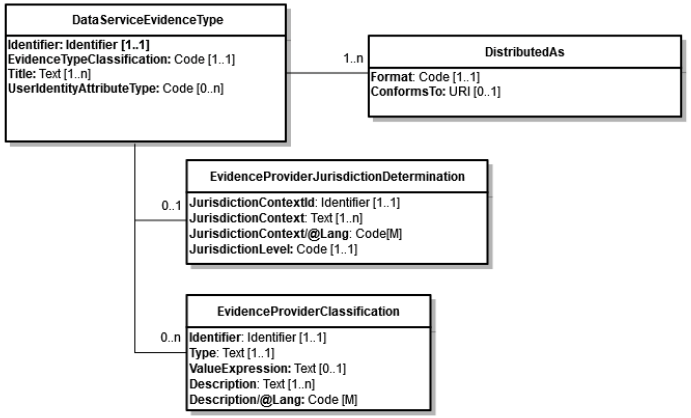
Definition Type	Value	Description
Classification Scheme	`urn:fdc:oots:classification:dsd`	The classification scheme under which the specific classification nodes reside for the DSD Service
Classification Node	`EvidenceProvider`	A Node defining the registry object as an Evidence Provider Entity
Classification Node	`DataServiceEvidenceType`	A classification node defining the registry object as Data Service Evidence Type
Association	`urn:oasis:names:tc:ebxml-regrep:AssociationType:ServesEvidence`	The association linking the EvidenceProvider Registry objects with the Data Service Evidence Types

3.1.5.2 Registry Objects

The DSD LCM Interface accepts two different registry objects in the SubmitObjectsRequest Message which are defined in the sections below:

3.1.5.2.1 DataServiceEvidenceType

This Registry Object provides the information on the Data Service Evidence Type. It MUST NOT contain the Access Service and the Evidence Provider details, as these are provided through the use of associations with EvidenceProvider Registry Objects. The classification node used MUST be `DataServiceEvidenceType` under the DSD Classification Scheme `urn:fdc:oots:classification:dsd`.
The following diagram shows the structure of the registry object:

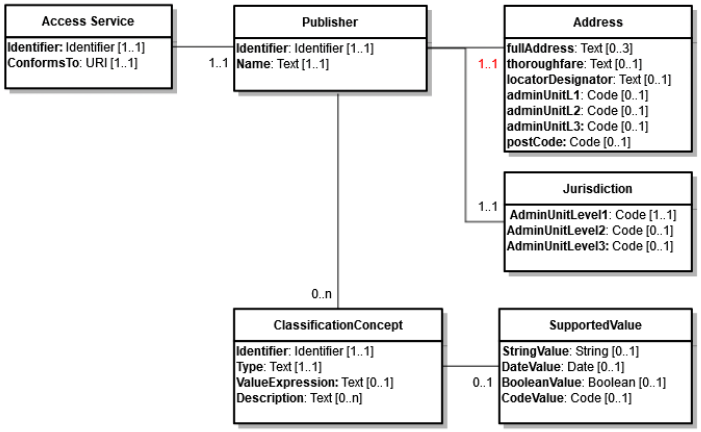


An example DataServiceEvidenceType Registry Object in XML format is shown below:

```
<rim:RegistryObject id="urn:uuid:61165d22-657b-45fa-9240-f1ed35837c23">
  <rim:Classification id="urn:uuid:a1be6e74-efgh-5678-aaaa-0376f367b8fd" classificationScheme="urn:oots:classification:dsd"
classificationNode="DataServiceEvidenceType"/>
  <rim:Slot name="DataServiceEvidenceType">
  <rim:SlotValue xsi:type="rim:AnyValueType">

    <sdg:DataServiceEvidenceType>
      <sdg:Identifier>ID-123</sdg:Identifier>
      <sdg:EvidenceTypeClassification>CertificateOfInsurance</sdg:EvidenceTypeClassification>
      <sdg:Title>Certificate Of Insurance</sdg:Title>
      <sdg:DistributedAs>
        <sdg:Format>application/pdf</sdg:Format>
      </sdg:DistributedAs>

      <sdg:EvidenceProviderClassification>

        <sdg:Identifier>TypeOfInsurance</sdg:Identifier>
        <sdg:Type>Codelist</sdg:Type>
        <!-- Value from a Codelist required. Must be published in the Semantic Repository -->
        <sdg:ValueExpression>http://sr.europa.eu/codelists/insuranceType</sdg:ValueExpression>
        <sdg:Description lang="en">Type Of Insurance</sdg:Description>
      </sdg:EvidenceProviderClassification>

      <sdg:EvidenceProviderJurisdictionDetermination>
        <sdg:JurisdictionContextId>CompanyHq</sdg:JurisdictionContextId>
        <sdg:JurisdictionContext>Company Headquarters</sdg:JurisdictionContext>
        <sdg:JurisdictionLevel>https://sr.ec.europa.eu/codelist/locationLevel/LAU</sdg:JurisdictionLevel>
      </sdg:EvidenceProviderJurisdictionDetermination>

    </sdg:DataServiceEvidenceType>
  </rim:SlotValue>
  </rim:Slot>

</rim:RegistryObject>
```

3.1.5.2.2 Evidence Provider

This Registry Object provides the information of the Evidence Provider. The classification node used MUST be `EvidenceProvider` under the DSD Classification Scheme `urn:fdc:oots:classification:dsd`.
The following diagram shows the structure of the registry object:



An example Evidence Provider Registry Object in XML format is shown below:

```
<rim:RegistryObject  id="urn:uuid:a1be6e74-bbbb-4444-b04c-0376f367b8fd">
  <rim:Classification id="urn:uuid:a1be6e74-abcd-1234-b04c-0376f367b8fd"
classificationScheme="urn:fdc:oots:classification:dsd" classificationNode="EvidenceProvider"/>

  <!-- The actual Evidence Provider Structure -->
  <rim:Slot name="EvidenceProvider">
    <rim:SlotValue xsi:type="rim:AnyValueType">
    <sdg:AccessService>
      <sdg:Identifier schemeID="urn:oasis:names:tc:ebcore:partyid-type:iso6523:0060">8889909099</sdg:Identifier>
      <sdg:ConformsTo>oots:edm-v1.0</sdg:ConformsTo>

      <sdg:Publisher>
        <!-- The Evidence Provider Information -->
        <sdg:Identifier schemeID="1204">11231112313</sdg:Identifier>
        <sdg:Name>Example Organization</sdg:Name>

        <sdg:Address>
          <sdg:AdminUnitLevel1>MS</sdg:AdminUnitLevel1>
          <!-- NUTS Code -->
          <sdg:AdminUnitLevel2>MS77</sdg:AdminUnitLevel2>
        </sdg:Address>

        <sdg:Jurisdiction>
          <sdg:AdminUnitLevel1>MS</sdg:AdminUnitLevel1>
          <!-- NUTS Code -->
          <sdg:AdminUnitLevel2>MS77</sdg:AdminUnitLevel2>
        </sdg:Jurisdiction>

        <sdg:ClassificationConcept>
          <sdg:Identifier>TypeOfInsurance</sdg:Identifier>
          <sdg:SupportedValue>
            <sdg:StringValue>private</sdg:StringValue>
          </sdg:SupportedValue>
        </sdg:ClassificationConcept>

      </sdg:Publisher>
    </sdg:AccessService>
    </rim:SlotValue>
  </rim:Slot>
```

```
</rim:RegistryObject>
```

3.1.5.3 Associations

The DSD LCM Interface accepts a single association that links a DataServiceEvidenceType with an Evidence Provider in the SubmitObjectsRequest Message which is defined in the sections below:

3.1.5.3.1 ServesEvidenceType

This Association provides the link between an Evidence Provider and a Data Service Evidence Type . The type attribute MUST be `urn:oasis:names:tc:ebxml-regrep:AssociationType:ServesEvidenceType`, with the source object pointing to an EvidenceProvider RegistryObject through the use of its id and the targetObject pointing to a DataserviceEvidenceType object through the id.

3.1.5.4 A complete SubmitObjects Request Example (Informative)

The following example shows a complete example of a possible bulk upload for a member state MS, submitting an evidence provider, a DataserviceEvidenceType and an association that links them together:

```
<lcm:SubmitObjectsRequest xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                          xmlns:rs="urn:oasis:names:tc:ebxml-regrep:xsd:rs:4.0"
                          xmlns:rim="urn:oasis:names:tc:ebxml-regrep:xsd:rim:4.0"
                          xmlns:query="urn:oasis:names:tc:ebxml-regrep:xsd:query:4.0"
                          xmlns:lcm="urn:oasis:names:tc:ebxml-regrep:xsd:lcm:4.0"
                          xmlns:sdg="http://data.europa.eu/p4s"
                          id="urn:uuid:ccbe6e99-abcd-1234-b04c-0376f367b8ff">

    <rim:RegistryObjectList>
        <!-- This is the registry object for Evidence Provider A -->
        <rim:RegistryObject id="urn:uuid:a1be6e74-bbbb-4444-b04c-0376f367b8fd">
            <rim:Classification id="urn:uuid:a1be6e74-abcd-1234-b04c-0376f367b8fd"
                                classificationScheme="urn:fdc:oots:classification:dsd"
                                classificationNode="EvidenceProvider"/>
```

```
        <!-- The actual Evidence Provider Structure -->
        <rim:Slot name="EvidenceProvider">
            <rim:SlotValue xsi:type="rim:AnyValueType">
                <sdg:AccessService xmlns:sdg="http://data.europa.eu/p4s">
                    <sdg:Identifier schemeID="urn:oasis:names:tc:ebcore:partyid-type:iso6523:0060">8889909099
                    </sdg:Identifier>
                    <sdg:ConformsTo>oots:edm-v1.0</sdg:ConformsTo>

                    <sdg:Publisher>
                        <!-- The Evidence Provider Information -->
                        <sdg:Identifier schemeID="1204">11231112313</sdg:Identifier>
                        <sdg:Name>Example Organization</sdg:Name>

                        <sdg:Address>
                            <sdg:AdminUnitLevel1>MS</sdg:AdminUnitLevel1>
                            <!-- NUTS Code -->
                            <sdg:AdminUnitLevel2>MS77</sdg:AdminUnitLevel2>
                        </sdg:Address>

                        <sdg:Jurisdiction>
                            <sdg:AdminUnitLevel1>MS</sdg:AdminUnitLevel1>
                            <!-- NUTS Code -->
                            <sdg:AdminUnitLevel2>MS77</sdg:AdminUnitLevel2>
                        </sdg:Jurisdiction>

                        <sdg:ClassificationConcept>
                            <sdg:Identifier>TypeOfInsurance</sdg:Identifier>
                            <sdg:SupportedValue>
                                <sdg:StringValue>private</sdg:StringValue>
                            </sdg:SupportedValue>
                        </sdg:ClassificationConcept>

                    </sdg:Publisher>
                </sdg:AccessService>
            </rim:SlotValue>
        </rim:Slot>
    </rim:RegistryObject>
```

```
<rim:RegistryObject id="urn:uuid:61165d22-657b-45fa-9240-f1ed35837c23">
    <rim:Classification id="urn:uuid:a1be6e74-efgh-5678-aaaa-0376f367b8fd"
                        classificationScheme="urn:oots:classification:dsd"
                        classificationNode="DataServiceEvidenceType"/>
    <rim:Slot name="DataServiceEvidenceType">
        <rim:SlotValue xsi:type="rim:AnyValueType">

            <sdg:DataServiceEvidenceType>
                <sdg:Identifier>ID-123</sdg:Identifier>
                <sdg:EvidenceTypeClassification>CertificateOfInsurance</sdg:EvidenceTypeClassification>
                <sdg:Title>Certificate Of Insurance</sdg:Title>
                <sdg:DistributedAs>
                    <sdg:Format>application/pdf</sdg:Format>
                </sdg:DistributedAs>

                <sdg:EvidenceProviderClassification>

                    <sdg:Identifier>TypeOfInsurance</sdg:Identifier>
                    <sdg:Type>Codelist</sdg:Type>
                    <!-- Value from a Codelist required. Must be publised in the Semantic Repository -->
                    <sdg:ValueExpression>http://sr.europa.eu/codelists/insuranceType</sdg:ValueExpression>
                    <sdg:Description lang="en">Type Of Insurance</sdg:Description>
                </sdg:EvidenceProviderClassification>

                <sdg:EvidenceProviderJurisdictionDetermination>
                    <sdg:JurisdictionContextId>CompanyHq</sdg:JurisdictionContextId>
                    <sdg:JurisdictionContext>Company Headquarters</sdg:JurisdictionContext>
                    <sdg:JurisdictionLevel>https://sr.ec.europa.eu/codelist/locationLevel/LAU
                    </sdg:JurisdictionLevel>
                </sdg:EvidenceProviderJurisdictionDetermination>

            </sdg:DataServiceEvidenceType>
        </rim:SlotValue>
    </rim:Slot>

</rim:RegistryObject>

<!-- Associate Evidence Provider A with Evidence Type 1-->
<rim:RegistryObject xsi:type="rim:AssociationType" id="urn:uuid:f6458bc0-bdaa-489a-84bd-451d1dbf800b"
```

```
                            sourceObject="urn:uuid:a1be6e74-bbbb-4444-b04c-0376f367b8fd"
                            targetObject="urn:uuid:61165d22-657b-45fa-9240-f1ed35837c23"
                            type="urn:oasis:names:tc:ebxml-regrep:AssociationType:ServesEvidenceType"/>

    </rim:RegistryObjectList>

</lcm:SubmitObjectsRequest>
```

3.2 Evidence Broker (EB) - June 2022

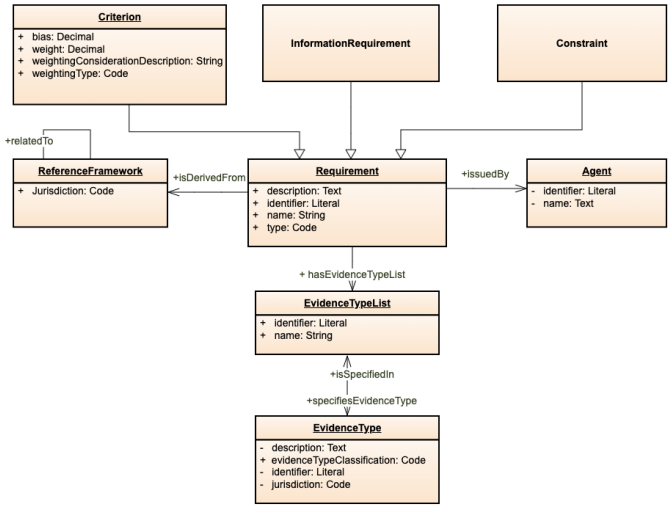
3.2.1 Overview

The Evidence Broker is one of the Common Services of the OOTS HLA. It is a service that publishes which types of evidence Member States can provide to prove a particular requirement of a procedure. It provides metadata on the requirements applicable in a procedure and which type of evidence can be used by the User to prove fulfilment. Using the mapping from criteria or information requirements to possible evidence types, the Evidence Requester can find the evidence types that can prove that the User fulfills the requirements of the procedure.

3.2.2 Information Model

The EB Information Model is based on the ISA^2 SEMIC Core Criterion and Core Evidence Vocabulary (CCCEV) v2.0. The CCCEV is designed to support the exchange of information between organisations defining requirements and organisations responding to these requirements by means of evidence types.
The CCCEV contains two basic and complementary core concepts:

- The Requirement, which is used as the basis for making a judgment or decision, e.g. a requirement set in a public tender or a condition that has to be fulfilled for a public service to be executed;
- The Evidence Type, which proves that something else exists or is true. In particular, an evidence is used to prove that a specific requirement is met by someone or by something.



3.2.2.1 Requirement Model

One of the central concepts of the Evidence Broker is the '*Requirement*'. It is a condition or prerequisite that someone requests and someone else has to meet.
The requirement is realised by three concrete types of requirements: The Information Requirement, the Criterion and the Constraint.

- ***The Information Requirement*** is to be seen as a request for data that proves one or more facts of the real world, or that leads to the source of such a proof.
- ***The Criterion*** is to be seen as a condition that will be evaluated.
- ***The Constraint*** is a limitation imposed on any type of requirement or on an element defined inside a requirement.

3.2.2.2 Evidence Type Model

Each requirement is linked with one or more lists of Evidence Types. Each list contains one or more evidence types that can prove the specific requirement. The following behavior is supported by the EB Mechanism:

- The respondent to a ***Requirement*** must provide at least one evidence per each type of evidence specified in one list; the respondent can select the list amongst the ones proposed by the requester. This amounts to say that the content of a list is combined via the logic operator 'AND', and the lists are combined via the logic operator 'OR'.
- The types of evidences can be described in detail with respect to their jurisdiction level.
- The class **'*Evidence*'** provides the means to support responses to *Criteria* or in response to a concrete *Information Requirements*.

The EB keeps a mapping between the requirements and the evidence types, either national or harmonized, that are able to fulfil these requirements.

3.2.3 Criterion to Evidence Type Mapping Mechanism

The EB mapping mechanism is a requirement-oriented one. It assumes that each procedure has one or more specific requirements that need to be fulfilled by the User that executes the procedure. Conceptually, the mapping process follows the steps below:

1. A Member State implementing a procedure, has identified a requirement that must be fulfilled by the user executing the procedure.
2. It initially checks whether this requirement already exists and has been addressed within the scope of this or another procedure, by scanning the list of available requirements.
3. If the requirement does not already exist, the Member State requests a requirement addition for the specific procedure. If it exists, then it maps this requirement as part of the implementation of the procedure in the Member State.
4. Member States providing evidence need to map the specific new requirement with list of evidence types that prove the requirement added, by adding evidence types. These evidence types MUST be registered in the codelist of evidence type classifications, published by the semantic repository.

For the pivoting mechanism to work, each requirement MUST have a EU-wide scope so that is visible and mappable to evidence types issued by all the MSs.

3.2.4 Query Interface Specification

The query interface specification for the Evidence Broker is based on the OASIS ebXML RegRep V4 standard. This standard has multiple protocol bindings that can be used to execute queries. Since the EB queries have only simple, single-value parameters, the REST binding is used to implement the EB query interface. This implies that the query transaction is executed as an HTTP GET request with the URL representing the query to execute and the HTTP response carrying the query response as an XML document. This section further profiles the REST binding as specified in the OASIS RegRep standard for use by the EB.

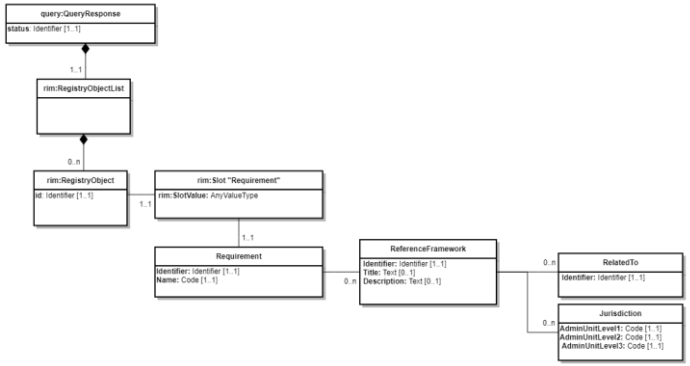
3.2.4.1 Get List of Requirements Query

The initial top-level query returns a list of available requirements. The supported parameters and query filters, are listed in the following table:

Parameter	Requirement	Description
queryId	MUST	This parameter MUST have value **urn:fdc:oots:eb:ebxml-regrep:queries:requirements-by-procedure-and-jurisdiction**.
procedure-id	OPTIONAL	The identifier of the procedure at the EU level, used to filter only the requirements that are used under the specific procedure
country-code	OPTIONAL	The jurisdiction of the procedure, expressed as a ISO 3166-2 country code, used to filter only the requirements that are used under the specific member state for procedure implementation
jurisdiction-admin-l2	OPTIONAL	The level two administration level code for the jurisdiction of the evidence type, expressed using NUTS code. It MUST be combined with `country-code`
jurisdiction-admin-l3	OPTIONAL	The level three administration level code for the jurisdiction of the evidence type, expressed using LAU code. It MUST be combined with `country-code`

3.2.4.1.1 Data Model of the Query Response of the EB for the "Requirement Query"

The Query Response of the EB of an Requirement Query returns a RegRep QueryResponse document which MUST either contain an `Exception` or `RegistryObjectList` element with zero or more `RegistryObjects`. Each `RegistryObject` in the result MUST include one `Slot` element with a `SlotValue` of type *rim:AnyValueType* and a single `Requirement` child element, following the SDGR Application Profile of the EB. The SDGR application profile of the EB describes how the SDG-Generic-Metadata Profile (SDG-syntax) is profiled in ebRIM in order to compose a valid QueryResponse. It therefore contains a mapping to the underlying SDG-syntax elements and necessary parameters to compose a QueryResponse. The namespace of the SDG-syntax is http://data.europa.eu/p4s.
The following data model illustrates the RegRep QueryResponse returned by the EB for a Requirements Query. It shows the case of a successful response, therefore the `RegistryObjectList` element is present and the `Exception` element is not present.



3.2.4.1.2 Implementation Guideline of the Query Response of the EB for the "Requirement Query"

The table below defines the elements of the SDG Application Profile for the Query Response of the EB (for Requirements) according to the core ebRIM elements and the `Requirement` slot.

	Name	Definition	Cardinality	Type	Data Type	Rules	Core Vocabulary / Domain	Element of Core Vocabulary
	query:QueryResponse	**root element**		ComplexType			ebRIM	
+	status	This attribute contains the status of the response. If the EB provides at least one RegistryObject, the value "urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Success" is used.	1..1	Attribute	Identifier		ebRIM	-

++	**rim:RegistryObjectList**	**Element to list the Registry Objects of the QueryResponse.**	1..1	ComplexType			ebRIM	-
+++	**rim:RegistryObject**	**Element to control the type and structure of Registry Object within the QueryResponse.**	0..n	ExtrinsicObjectType			ebRIM	-
++++	id	Unique UUID for each RegistryObject.	1..1	Attribute	Identifier	Must be unique UUID for each Registry Object.	ebRIM	-
++++	rim:slot "Requirement"	The slot is a container to describe the specific aspects and metadata of the Requirement	1..1	SlotType	AnyValueType		ebRIM	-
++++	rim:slot "Requirement"	The slot is a container to describe the specific aspects and metadata of the Requirement	1..1	SlotType	AnyValueType		ebRIM	-
+++++	Requirement	The element describes specific aspects and metadata of the Requirement	1..1	RequirementType			Core Criterion and Core Evidence Vocabulary	cccev:Requirement

+++++	Requirement	The element describes specific aspects and metadata of the Requirement	1..1	RequirementType			Core Criterion and Core Evidence Vocabulary	cccev:Requirement
++++++	Identifier	The unique identifier of the Requirement	1..1	Attribute	Identifier		CCCEV	cccev:identifier
++++++	Name	A name to identify in common language the Requirement	1..1	Attribute	Text		CCCEV	cccev:name
++++++	ReferenceFramework	The Reference Framework that is responsible for the creation/initiation of the Requirement.	0..n	ReferenceFrameworkType			Core Criterion and Core Evidence Vocabulary	cccev:ReferenceFramework
++++++	ReferenceFramework	The Reference Framework that is responsible for the creation/initiation of the Requirement.	0..n	ReferenceFrameworkType			Core Criterion and Core Evidence Vocabulary	cccev:ReferenceFramework
+++++++	Identifier	The Identifier of the Procedure	1..1	Attribute	Identfier		CCCEV	cccev:identifier
+++++++	Title	The title of the Procedure	0..1	Attribute	Text		-	-
+++++++	Description	The description of the Procedure	0..1	Attribute	Text		-	-
+++++++	RelatedTo	The Identifier of the SDGR Procedure which this procedure relates to	0..n	ReferenceFrameworkType			Core Criterion and Core Evidence	cccev:ReferenceFramework

							Vocabulary	
+++++++	Jurisdiction	The administrative level in which this reference framework applies. It can apply to multiple jurisdictions	0..n	JurisdictionType			Core Location Vocabulary (CLV)	locn:Address
+++++++	RelatedTo	The Identifier of the SDGR Procedure which this procedure relates to	0..n	ReferenceFrameworkType			Core Criterion and Core Evidence Vocabulary	cccev:ReferenceFramework
+++++++	Identifier	The Identifier of the Procedure	1..1	Attribute	Identfier		CCCEV	cccev:identifier
+++++++	Jurisdiction	The Jurisdiction to which this Data Service Evidence Type applies.	0..n	JurisdictionType			Core Location Vocabulary (CLV)	locn:Address
+++++++	AdminUnitLevel1	The name of the uppermost level of the address, almost always a country.	1..1	Attribute	Code		Core Location Vocabulary	locn:adminUnitL1
+++++++	AdminUnitLevel2	The name of a secondary level/region of the address, usually a county, state or other such area that typically encompasses several localities.	0..1	Attribute	Code		Core Location Vocabulary (CLV)	locn:adminUnitL2
+++++++	AdminUnitLevel3	The name of a secondary level/region of the address, usually a municipality or other	0..1	Attribute	Code		Core Location	locn:adminUnitL3

		such area that typically encompasses several localities.					Vocabulary (CLV)	

3.2.4.1.3 Example of the Query Response of the EB for the "Requirement Query"

The query response contains the list of requirements, with each requirement correlated to one or more procedure national implementations. The following example shows a response using the SDG Application Profile XML Representation.

```
<?xml version="1.0" encoding="UTF-8"?>
<query:QueryResponse xmlns="urn:oasis:names:tc:ebxml-regrep:xsd:lcm:4.0"
    xmlns:lcm="urn:oasis:names:tc:ebxml-regrep:xsd:lcm:4.0"
    xmlns:query="urn:oasis:names:tc:ebxml-regrep:xsd:query:4.0"
    xmlns:rim="urn:oasis:names:tc:ebxml-regrep:xsd:rim:4.0"
    xmlns:rs="urn:oasis:names:tc:ebxml-regrep:xsd:rs:4.0"
    xmlns:sdg="http://data.europa.eu/p4s"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" totalResultCount="1" startIndex="0"
       status="urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Success">

    <rim:RegistryObjectList>
        <rim:RegistryObject id="315cfd75-6605-49c4-b0fe-799833b41099">
            <rim:Slot name="Requirement">
                <rim:SlotValue xsi:type="rim:AnyValueType">
                    <sdg:Requirement>
                        <sdg:Identifier>315cfd75-6605-49c4-b0fe-799833b41099</sdg:Identifier>
                        <sdg:Name>Proof of Birth</sdg:Name>

                        <sdg:ReferenceFramework>

                            <!-- Procedure Identifier -->
                            <sdg:Identifier>118fd444-6443-42be-a084-c9fbfd1f674d</sdg:Identifier>
                            <sdg:Title>Procedure 5 - Annex II of SDG as Implemented in the Spanish Portal</sdg:Title>
                            <sdg:Description> Procedure 5 of Annex II of the Regulation (EU) 2018/1724
                                of the European Parliament and of the Council of 2 October 2018 establishing a single
digital gateway
                                to provide access to information, to procedures and to assistance and problem-solving
services and amending Regulation (EU) No 1024/2012
                            </sdg:Description>

                            <!-- The Identifier of the SDGR Procedure which this procedure relates to -->
                            <sdg:RelatedTo>
                                <sdg:Identifier>http://data.europa.eu/eli/reg/2018/1724/oj#AnnexII-5</sdg:Identifier>
                            </sdg:RelatedTo>

                            <!-- Requirement is used in the implementation of Procedure 5 in Spain -->
                            <sdg:Jurisdiction>
                                <sdg:AdminUnitLevel1>ES</sdg:AdminUnitLevel1>
                            </sdg:Jurisdiction>
```

```
                        </sdg:ReferenceFramework>

                        <sdg:ReferenceFramework>

                            <!-- Procedure Identifier -->
                            <sdg:Identifier>03b82e6a-3227-4751-a815-b570a9c0aeb4</sdg:Identifier>
                            <sdg:Title>Procedure 5 - Annex II of SDG as Implemented in Belgian Portal</sdg:Title>
                            <sdg:Description> Procedure 5 of Annex II of the Regulation (EU) 2018/1724
                                of the European Parliament and of the Council of 2 October 2018 establishing a single
digital gateway
                                to provide access to information, to procedures and to assistance and problem-solving
services and amending Regulation (EU) No 1024/2012
                            </sdg:Description>

                            <!-- The Identifier of the SDGR Procedure which this procedure relates to -->
                            <sdg:RelatedTo>
                                <sdg:Identifier>http://data.europa.eu/eli/reg/2018/1724/oj#AnnexII-5</sdg:Identifier>
                            </sdg:RelatedTo>

                            <!-- Requirement is used in the implementation of Procedure 5 in Belgium -->
                            <sdg:Jurisdiction>
                                <sdg:AdminUnitLevel1>BE</sdg:AdminUnitLevel1>
                            </sdg:Jurisdiction>
                        </sdg:ReferenceFramework>
                    </sdg:Requirement>
                </rim:SlotValue>
            </rim:Slot>

        </rim:RegistryObject>

    </rim:RegistryObjectList>
</query:QueryResponse>
```

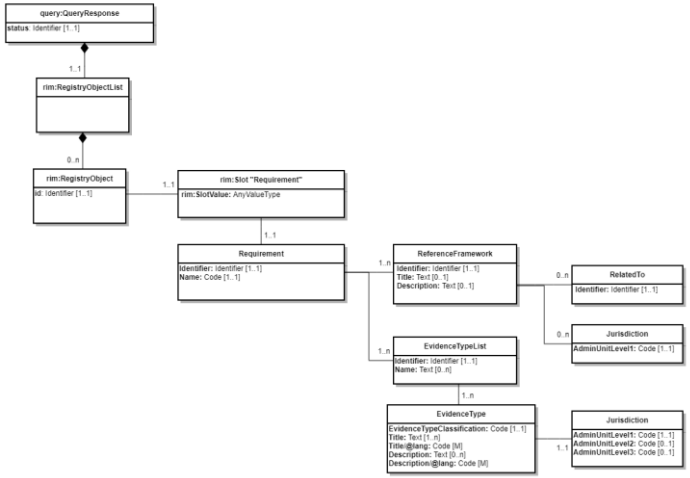
3.2.4.2 Get Evidence Types for Requirement Query

This query returns the list of evidence types that prove a specific requirement. It must contain the Identifier of the requirement, that can be extracted using the "Get List of Requirements" query if not known. The supported parameters and query filters, are listed in the following table:

Parameter	Requirement	Description
queryId	MANDATORY	**urn:fdc:oots:eb:ebxml-regrep:queries:evidence-types-by-requirement-and-jurisdiction**
requirement-id	MANDATORY	The id of the requirement we request the evidence types for
country-code	OPTIONAL	The country code of the mapped evidence under request
jurisdiction-admin-l2	OPTIONAL	The level two administration level code for the jurisdiction of the evidence type, expressed using NUTS code. It MUST be combined with `country-code`
jurisdiction-admin-l3	OPTIONAL	The level three administration level code for the jurisdiction of the evidence type, expressed using LAU code. It MUST be combined with `country-code`

3.2.4.2.1 Data Model of the Query Response of the EB for the "Get Evidence Types for Requirement Query"

The Query Response of the EB for Evidence Types that prove a specific requirement returns a RegRep QueryResponse document which MUST either contain an `Exception` or `RegistryObjectList` element with zero or more `RegistryObjects`. Each `RegistryObject` in the result MUST include one `Slot` element with a `SlotValue` of type *rim:AnyValueType* and a single `Requirement` child element, following the SDGR Application Profile of the EB. The SDGR application profile of the EB describes how the SDG-Generic-Metadata Profile (SDG-syntax) is profiled in ebRIM in order to compose a valid QueryResponse. It therefore contains a mapping to the underlying SDG-syntax elements and necessary parameters to compose a QueryResponse. The namespace of the SDG-syntax is http://data.europa.eu/p4s.
The following data model illustrates the RegRep QueryResponse returned by the EB when requesting Evidence Types that prove a specific requirement. It shows the case of a successful response, therefore the `RegistryObjectList` element is present and the `Exception` element is not present.



3.2.4.2.2 Implementation Guideline of the Query Response of the EB for the "Get Evidence Types for Requirement Query"

The table below defines the elements of the SDG Application Profile for the Query Response of the EB (for Evidence Types) according to the core ebRIM elements and the `Requirement` slot including among other element the Evidence Types.

	Name	Definition	Cardinality	Type	Data Type	Rules	Core Vocabulary / Domain	Element of Core Vocabulary
	query:QueryResponse	**root element**		ComplexType			ebRIM	
+	status	This attribute contains the status of the response. If the EB provides at least one RegistryObject, the value "urn:oasis:names:tc:ebxml-	1..1	Attribute	Identifier		ebRIM	-

		regrep:ResponseStatusType :Success" is used.						
++	**rim:RegistryObject List**	**Element to list the Registry Objects of the QueryResponse.**	1..1	ComplexType			ebRIM	-
+++	**rim:RegistryObject**	**Element to control the type and structure of Registry Object within the QueryResponse.**	0..n	ExtrinsicObjectType			ebRIM	-
++++	id	Unique UUID for each RegistryObject.	1..1	Attribute	Identifier	Must be unique UUID for each Registry Object.	ebRIM	-
++++	rim:slot "Requirement"	The slot is a container to describe the specific aspects and metadata of the Requirement.	1..1	SlotType	AnyValueType		ebRIM	-
++++	rim:slot "Requirement"	The slot is a container to describe the specific aspects and metadata of the Requirement.	1..1	SlotType	AnyValueType		ebRIM	-
+++++	Requirement	The element describes specific aspects and metadata of the Requirement.	1..1	RequirementType			Core Criterion and Core Evidence Vocabulary	cccev:Requirement

+++++	Requirement	The element describes specific aspects and metadata of the Requirement.	1..1	RequirementType			Core Criterion and Core Evidence Vocabulary	cccev:Requirement
++++++	Identifier	The unique identifier of the Requirement.	1..1	Attribute	Identifier		CCCEV	cccev:identifier
++++++	Title	A name to identify in common language the Requirement.	1..1	Attribute	Text		CCCEV	cccev:name
++++++	ReferenceFramework	The Reference Framework that is responsible for the creation/initiation of the Requirement.	0..n	ReferenceFrameworkType			Core Criterion and Core Evidence Vocabulary	cccev:ReferenceFramework
++++++	EvidenceTypeList	A list of Evidence Types, that can be provided to meet a requirement, within a certain jurisdiction.	1..n	EvidenceTypeListType			Core Criterion and Core Evidence Vocabulary	cccev:EvidenceTypeList
++++++	ReferenceFramework	The Reference Framework that is responsible for the creation/initiation of the Requirement.	0..n	ReferenceFrameworkType			Core Criterion and Core Evidence Vocabulary (CCCEV)	cccev:ReferenceFramework
++++++ +	Identifier	The Identifier of the Procedure.	1..1	Attribute	Identfier		CCCEV	cccev:identifier
++++++ +	Title	The title of the Procedure.	0..1	Attribute	Text		-	-
++++++ +	Description	The description of the Procedure.	0..1	Attribute	Text		-	-

++++++	RelatedTo	The Identifier of the SDGR Procedure which this procedure relates to.	0..n	ReferenceFrameworkType			Core Criterion and Core Evidence Vocabulary (CCCEV)	cccev:ReferenceFramework
++++++	Jurisdiction	The administrative level in which this reference framework applies. It can apply to multiple jurisdictions.	0..n	JurisdictionType			Core Criterion Core Evidence Vocabulary (CCCEV)	cccev:evidenceTypeJurisdiction
++++++	RelatedTo	The Identifier of the SDGR Procedure which this procedure relates to.	0..n	ReferenceFrameworkType			Core Criterion and Core Evidence Vocabulary (CCCEV)	cccev:ReferenceFramework
++++++	Identifier	The Identifier of the Procedure.	1..1	Attribute	Identfier		CCCEV	cccev:identifier
++++++	Jurisdiction	The Jurisdiction to which this Data Service Evidence Type applies.	0..n	JurisdictionType			Core Location Vocabulary (CLV)	locn:Address
++++++	AdminUnitLevel1	The name of the uppermost level of the address, almost always a country.	1..1	Attribute	Code		Core Location Vocabulary (CLV)	locn:adminUnitL1
++++++	EvidenceTypeList	A list of Evidence Types, that can be provided to meet a requirement, within a certain jurisdiction.	1..n	EvidenceTypeListType			Core Criterion Core Evidence Vocabulary (CCCEV)	cccev:EvidenceTypeList
++++++	Identifier	The identifier of the Evidence Type List.	1..1	Attribute	Identifier		CCCEV	cccev:identifier

++++++	Name	The name of the Evidence Type List. Unbounded cardinality to support multiple languages.	0..n	Attribute	Text			cccev:name
++++++	EvidenceType	An Evidence Type is a type of evidence that can be provided to meet a requirement, within a certain jurisdiction.	1..n	EvidenceTypeType			Core Criterion Core Evidence Vocabulary (CCCEV)	cccev:EvidenceType
++++++	EvidenceType	An Evidence Type is a type of evidence that can be provided to meet a requirement, within a certain jurisdiction.	1..n	EvidenceTypeType			Core Criterion Core Evidence Vocabulary (CCCEV)	cccev:EvidenceType
++++++++	EvidenceTypeClassification	An URI pointing to the Evidence Type. The classification is linking with the Evidence Type of the Semantic Repository (Evidence Broker).	1..1	Attribute	Code		Core Criterion Core Evidence Vocabulary	cccev:evidenceTypeClassification
++++++++	Title	A name to identify in common language the Evidence Type. Unbounded cardinality to support multiple languages.	1..n	Attribute	Text		DCAT-AP	dct:title
+++++++++	Title/@lang	The language of the title encoded as ISO 639-1 two-letter code. Default value "en"	M	Attribute	Code	ISO 639-1 two-letter code	DCAT-AP	dct:title

++++++++	Description	A description of the Evidence Type. Unbounded cardinality to support multiple languages.	0..n	Attribute	Text		DCAT-AP	dct:description
+++++++++	Description/@lang	The language of the description encoded as ISO 639-1 two-letter code. Default value "en"	M	Attribute	Code	ISO 639-1 two-letter code	DCAT-AP	dct:description
++++++++	Jurisdiction	The administrative level in which this reference framework applies. It can apply to multiple jurisdictions.	1..1	JurisdictionType			Core Criterion Core Evidence Vocabulary	cccev:evidenceTypeJurisdiction
++++++++	Jurisdiction	The Jurisdiction to which this Data Service Evidence Type applies.	1..1	JurisdictionType			Core Location Vocabulary (CLV)	locn:Address
+++++++++	AdminUnitLevel1	The name of the uppermost level of the address, almost always a country.	1..1	Attribute	Code		Core Location Vocabulary (CLV)	locn:adminUnitL1
+++++++++	AdminUnitLevel2	The name of a secondary level/region of the address, usually a county, state or other such area that typically encompasses several localities.	0..1	Attribute	Code		Core Location Vocabulary (CLV)	locn:adminUnitL2
+++++++++	AdminUnitLevel3	The name of a secondary level/region of the address, usually a municipality or other such area that typically	0..1	Attribute	Code		Core Location Vocabulary (CLV)	locn:adminUnitL3

		encompasses several localities.						

3.2.4.2.3 Example of the Query Response of the EB for the "Get Evidence Types for Requirement Query"

The query response contains the list of evidence types that fulfil the specific requirement of the query, filtered by the jurisdiction level code. The following example shows a response using the SDG Application Profile XML Representation

```
<?xml version="1.0" encoding="UTF-8"?>
<query:QueryResponse
    xmlns:lcm="urn:oasis:names:tc:ebxml-regrep:xsd:lcm:4.0"
    xmlns:query="urn:oasis:names:tc:ebxml-regrep:xsd:query:4.0"
    xmlns:rim="urn:oasis:names:tc:ebxml-regrep:xsd:rim:4.0"
    xmlns:rs="urn:oasis:names:tc:ebxml-regrep:xsd:rs:4.0"
    xmlns:sdg="http://data.europa.eu/p4s"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        status="urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Success">

    <rim:RegistryObjectList>
        <!-- One registry object per dataset -->
        <rim:RegistryObject id="315cfd75-6605-49c4-b0fe-799833b41099">
            <rim:Slot name="Requirement">
                <rim:SlotValue xsi:type="rim:AnyValueType">
                    <sdg:Requirement >

                        <sdg:Identifier>315cfd75-6605-49c4-b0fe-799833b41099</sdg:Identifier>
                        <sdg:Name>Proof of Birth</sdg:Name>

                        <sdg:ReferenceFramework>

                            <!-- Procedure Identifier -->
                            <sdg:Identifier>118fd444-6443-42be-a084-c9fbfd1f674d</sdg:Identifier>
                            <sdg:Title>Procedure 5 - Annex II of SDG as Implemented in the Spanish Portal</sdg:Title>
                            <sdg:Description> Procedure 5 of Annex II of the Regulation (EU) 2018/1724
                                of the European Parliament and of the Council of 2 October 2018 establishing a single
digital gateway
                                to provide access to information, to procedures and to assistance and problem-solving
services and amending Regulation (EU) No 1024/2012
                            </sdg:Description>

                            <!-- The Identifier of the SDGR Procedure which this procedure relates to -->
                            <sdg:RelatedTo>
                                <sdg:Identifier>http://data.europa.eu/eli/reg/2018/1724/oj#AnnexII-5</sdg:Identifier>
                            </sdg:RelatedTo>

                            <!-- Requirement is used in the implementation of Procedure 5 in Spain -->
                            <sdg:Jurisdiction>
```

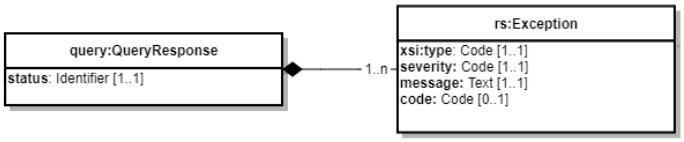
```
                            <sdg:AdminUnitLevel1>ES</sdg:AdminUnitLevel1>
                        </sdg:Jurisdiction>

                    </sdg:ReferenceFramework>

                    <sdg:ReferenceFramework>

                        <!-- Procedure Identifier -->
                        <sdg:Identifier>03b82e6a-3227-4751-a815-b570a9c0aeb4</sdg:Identifier>
                        <sdg:Title>Procedure 5 - Annex II of SDG as Implemented in Belgian Portal</sdg:Title>
                        <sdg:Description> Procedure 5 of Annex II of the Regulation (EU) 2018/1724
                            of the European Parliament and of the Council of 2 October 2018 establishing a single
digital gateway
                            to provide access to information, to procedures and to assistance and problem-solving
services and amending Regulation (EU) No 1024/2012
                        </sdg:Description>

                        <!-- The Identifier of the SDGR Procedure which this procedure relates to -->
                        <sdg:RelatedTo>
                            <sdg:Identifier>http://data.europa.eu/eli/reg/2018/1724/oj#AnnexII-5</sdg:Identifier>
                        </sdg:RelatedTo>

                        <!-- Requirement is used in the implementation of Procedure 5 in Belgium -->
                        <sdg:Jurisdiction>
                            <sdg:AdminUnitLevel1>BE</sdg:AdminUnitLevel1>
                        </sdg:Jurisdiction>
                    </sdg:ReferenceFramework>

                    <sdg:EvidenceTypeList>
                        <!-- Example structure of an evidence type having national coverage area / jurisdiction -->
                        <sdg:Identifier>EV-List-1</sdg:Identifier>
                        <sdg:EvidenceType>
                            <sdg:EvidenceTypeClassification>Classification Code</sdg:EvidenceTypeClassification>
                            <sdg:Title lang="en">Title of the Evidence Type</sdg:Title>
                            <sdg:Description>certificado de nacimiento</sdg:Description>
                            <sdg:Jurisdiction>
                                <!-- ISO code -->
                                <sdg:AdminUnitLevel1>ES</sdg:AdminUnitLevel1>
                                <!-- NUTS Code -->
```

```
                                    <sdg:AdminUnitLevel2>ES211</sdg:AdminUnitLevel2>
                                    <!-- LAU Code -->
                                    <sdg:AdminUnitLevel3>01001</sdg:AdminUnitLevel3>
                                </sdg:Jurisdiction>
                            </sdg:EvidenceType>
                        </sdg:EvidenceTypeList>

                        <!-- Example structure of an evidence type having national coverage area / jurisdiction -->
                        <sdg:EvidenceTypeList>
                            <sdg:Identifier>EV-List-2</sdg:Identifier>

                            <!-- Classification Information - Provided by the Evidence Broker on the basis of the Semantic
Repository -->
                            <sdg:EvidenceType>
                                <sdg:EvidenceTypeClassification>Classification Code</sdg:EvidenceTypeClassification>
                                <sdg:Title lang="en">Certificate of Birth</sdg:Title>
                                <sdg:Title lang="de">Geburtsurkunde</sdg:Title>
                                <sdg:Description lang="en">An official certificate of birth of a person - with first name,
surname, sex, date and place of birth, which is obtained from the birth register of the place of birth.</sdg:Description>
                                <sdg:Description lang="de">Eine amtliche Bescheinigung über die Geburt einer Person – mit
Vorname, Familienname, Geschlecht, Datum und Ort der Geburt, welche aus dem Geburtsregister des Geburtsortes erstellt
wird.</sdg:Description>
                                <sdg:Jurisdiction>
                                    <!-- Country - Mandatory -->
                                    <sdg:AdminUnitLevel1>DE</sdg:AdminUnitLevel1>
                                    <!-- Regional Code not applicable for DE (Common Evidence for all country) -->
                                </sdg:Jurisdiction>
                            </sdg:EvidenceType>
                        </sdg:EvidenceTypeList>
                    </sdg:Requirement>
                </rim:SlotValue>
            </rim:Slot>
        </rim:RegistryObject>
    </rim:RegistryObjectList>
</query:QueryResponse>
```

3.2.4.3 API Error Response

3.2.4.3.1 Data Model of the Query Error Response of the Evidence Broker

The Query Error Response of the EB is syntactically expressed inside an ebRS QueryResponse using the ebRS RegistryExceptionType as shown in data model below. It shows the case of an usuccessful response, therefore the `RegistryObjectList` element is notpresent and the `Exception` element is present.



3.2.4.3.2 Implementation Guideline of the Query Error Response of the Evidence Broker

The following table below defines the elements of the data model illustrated above according to the core ebRIM elements of the ebRS RegistryExceptionType .

	Name	Definition	Cardinality	ebRIM type	Data Type	Rules	Domain
	query:QueryResponse	**Query Error Response root element**		RegistryResponseType			ebRIM
+	status	Element used to define the status of the Query Request.	1..1	Attribute	Identifier	Must always be "urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Failure" when an EDM Error Response is generated.	ebRIM
++	**rs:Exception**	**The rs:exeption describes an error which occurs during the processing**	1..n	RegistryExceptionType			ebRIM

		of a Query Request.					
+++	xsi:type	Describes the nature of the error that occurred.	1..1	Attribute	string	Must be one of the exception types listed in the table below describing the EBErrorResponseCodes.	ebRIM
+++	severity	Is used to show the impact of the error with regard to the business process. Use the severity codes WARNING or FAILURE to scope the impact of the error.	1..1	Attribute	objectReferenceType	default="urn:oasis:names:tc:ebxml-regrep:ErrorSeverityType:Error"	ebRIM
+++	message	Is used to add an error message that can be shown and understood by the user of the system.	1..1	Attribute	string		ebRIM
+++	code	A code that corresponds to the status of the system with regard to the processing of a request. If the specific error codes do not	0..1	Attribute	string	Must contain an appropriate value for the code of the expections according to the table below describing the EBErrorResponseCodes.	ebRIM

		cover the reason for failure use the generic error code "other".					

3.2.4.3.3 Example of the Query Error Response of the Evidence Broker

An example of Query Error Responses of the Evidence Broker due to an empty list of requirements is shown in the following XML snippet:

```
<?xml version="1.0" encoding="UTF-8"?>
<query:QueryResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                     xmlns:rs="urn:oasis:names:tc:ebxml-regrep:xsd:rs:4.0"
                     xmlns:rim="urn:oasis:names:tc:ebxml-regrep:xsd:rim:4.0"
                     xmlns:query="urn:oasis:names:tc:ebxml-regrep:xsd:query:4.0"
                     status="urn:oasis:nammes:tc:ebxml-regrep:ResponseStatusType:Failure">

  <rs:Exception
      xsi:type="rs:ObjectNotFoundExceptionType"
      severity="urn:oasis:names:tc:ebxml-regrep:ErrorSeverityType:Error"
      message="List of requirements requested is empty"
      code="EB:ERR:0001">
  </rs:Exception>
</query:QueryResponse>
```

3.2.4.3.4 Error Response Codes of the Evidence Broker

The following table provides the list of EBErrorResponseCodes for the expections defined in the Query Error Response:

#	Error Title	Type	code	Message
1	Resultset is empty	rs:ObjectNotFoundExceptionType	EB:ERR:0001	The result set is empty
2	Requirement not found	rs:ObjectNotFoundExceptionType	EB:ERR:0002	The requirement requested, represented by the requirement id, does not exist

3	Bad Query Parameters	rs:InvalidRequestExceptionType	EB:ERR:0003	The query parameters do not follow the query specification
4	Unknown Jurisdiction Level Code	rs:InvalidRequestExceptionType	EB:ERR:0004	The jurisdiction level code query parameter is invalid or unknown
5	Unknown procedure	rs:InvalidRequestExceptionType	EB:ERR:0005	The value of the procedure-id query parameter is invalid or unknown
6	Unknown procedure implementation country	rs:InvalidRequestExceptionType	EB:ERR:0006	The value of the procedure implementation country query parameter is invalid or unknown
7	Unknown Query	rs:InvalidRequestExceptionType	EB:ERR:0007	The requested Query does not exist

3.2.4.4 Response Signature

The EB Service signs the query responses using JWS detached signature following the HttpHeaders Mechanism of the ETSI ESI JAdES specification. In accordance with ENISA's Good Practises in Cryptography – Primitives and Schemes, the following algorithms found in [RFC7518] are selected to be used in the following form:

- The EdDSA Algorithm [RFC8032] using one of the curves defined in RFC7748 shall be used. The value "EdDSA" for the "alg" parameter MUST be used and the curve shall be encoded in the "crv" parameter as defined in RFC8037.

The following sets of rules shall apply in the application of the HttpHeaders mechanism ETSI ESI Jades compliant signature:

- The JWS content (Data to be Signed) MUST be detached from the signatures as defined in RFC7515 Appendix F.
- The signed `SigD` parameter object MUST be present in the JWS headers, denoting the use of the JAdES detached header profile.
- The value of the `mId` parameter MUST be set to `"http://uri.etsi.org/19182/HttpHeaders"`.
- The `pars` array of the `SigD` MUST contain only the element "digest", denoting that for the calculation of the signature only the digest of the HTTP payload must be taken into account, according to [RFC3230].
- The `alg` parameter is set to `"EdDSA"` and the `crv` parameter MUST be set.

The JWS structure shall be carried in the HTTP header field named `"oots-response-sig"`.

3.2.4.5 Transport Security

EB clients shall connect to an Evidence Broker using secure HTTP (HTTP over Transport Layer Security).

3.2.5 LCM Interface Specification

The EB Service provides a Regrep 4.0 based LCM API, following the Regrep 4.0 LCM SubmitObjects Profile of the OOTS Common Services. This section defines the Classification Scheme, Classification Nodes, Associations and Registry Objects of the SubmitObjects Request Message.

3.2.5.1 Classification Scheme and Nodes

Definition Type	Value	Description
Classification Scheme	`urn:fdc:oots:classification:eb`	The classification scheme under which the specific classification nodes reside for the EBService
Classification Node	`EvidenceType`	A Node defining the registry object as an Evidence Provider Entity
Classification Node	`EvidenceTypeList`	A classification node defining the registry object as an Evidence Type List
Classification Node	`Requirement`	A classification node defining the registry object as a Requirement
Classification Node	`Procedure`	A classification node defining the registry object as a Procedure
Association	`urn:oasis:names:tc:ebxml-regrep:AssociationType:containsEvidence`	The association linking EvidenceTypes with EvidenceTypeLists Registry objects
Association	`urn:oasis:names:tc:ebxml-regrep:AssociationType:fulfillsRequirement`	The association linking EvidenceTypeList Registry objects with Requirements
Association	`urn:oasis:names:tc:ebxml-regrep:AssociationType:derivesFromProcedure`	The association linking Requirements Registry objects with Procedures

3.2.5.2 Registry Objects

The DSD LCM Interface accepts two different registry objects in the SubmitObjectsRequest Message which are defined the sections below:

3.2.5.2.1 EvidenceType

This Registry Object provides the information of the Evidence Type. The classification node used MUST be `EvidenceType`under the EB Classification Scheme `urn:fdc:oots:classification:eb.`
An example EvidenceType Registry Object in XML format is shown below

```
<rim:RegistryObject id="urn:uuid:a1be6e74-e9ba-4d44-b04c-0376f367b8fd"
   xmlns:rim="urn:oasis:names:tc:ebxml-regrep:xsd:rim:4.0"
   xmlns:sdg="http://data.europa.eu/p4s"
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
   <rim:Slot name="EvidenceType">
       <rim:SlotValue xsi:type="rim:AnyValueType">
           <sdg:EvidenceType >
               <sdg:EvidenceTypeClassification>Classification Code</sdg:EvidenceTypeClassification>
               <sdg:Title lang="en">Certificate of Birth</sdg:Title>
               <sdg:Title lang="de">Geburtsurkunde</sdg:Title>
               <sdg:Description>certificado de nacimiento</sdg:Description>
               <sdg:Jurisdiction>
                   <!-- ISO code -->
                   <sdg:AdminUnitLevel1>ES</sdg:AdminUnitLevel1>
                   <!-- NUTS Code -->
                   <sdg:AdminUnitLevel2>ES211</sdg:AdminUnitLevel2>
                   <!-- LAU Code -->
                   <sdg:AdminUnitLevel3>01001</sdg:AdminUnitLevel3>
               </sdg:Jurisdiction>
           </sdg:EvidenceType>
       </rim:SlotValue>
   </rim:Slot>
   <rim:Classification id="urn:uuid:d45aa619-2d90-4d6c-ae59-b9ca4e6a5873"
       classificationScheme="urn:fdc:oots:classification:eb" classificationNode="EvidenceType"/>
</rim:RegistryObject>
```

3.2.5.2.2 EvidenceTypeList

This Registry Object provides the information of the Evidence Type List. It works as an intermediate class linking multiple evidence types as an atomic proof to requirements and thus it MUST NOT contain any evidence types in its structure. The classification node used MUST be `EvidenceTypeList` under the EB Classification Scheme `urn:fdc:oots:classification:eb.`
An example EvidenceTypeList Registry Object in XML format is shown below

```
<rim:RegistryObject id="urn:uuid:a1be6e74-e9ba-4d44-b04c-0376f367b8fd"
    xmlns:rim="urn:oasis:names:tc:ebxml-regrep:xsd:rim:4.0"
    xmlns:sdg="http://data.europa.eu/p4s"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

    <rim:Slot name="EvidenceTypeList">
        <rim:SlotValue xsi:type="rim:AnyValueType">
            <sdg:EvidenceTypeList>
                <sdg:Identifier>a1be6e74-e9ba-4d44-b04c-0376f367b8fd</sdg:Identifier>
            </sdg:EvidenceTypeList>
        </rim:SlotValue>
    </rim:Slot>
    <rim:Classification id="urn:uuid:d45aa619-2d90-4d6c-ae59-b9ca4e6a5873"
        classificationScheme="urn:fdc:oots:classification:eb" classificationNode="EvidenceTypeList"/>

</rim:RegistryObject>
```

3.2.5.2.3 Requirement

This Registry Object provides the information of a Requirement in any of its derivative forms (Critertion, Information Requirement). It MUST NOT contain any Evidence Type or Reference Frameworks (Procedures) as this are provided dynamically by the use of associations. The classification node used MUST be Requirement under the EB Classification Scheme `urn:fdc:oots:classification:eb.`
An example Requirement Registry Object in XML format is shown below

```
<rim:RegistryObject id="urn:uuid:315cfd75-6605-49c4-b0fe-799833b41099"
    xmlns:rim="urn:oasis:names:tc:ebxml-regrep:xsd:rim:4.0" xmlns:sdg="http://data.europa.eu/p4s"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

    <rim:Slot name="Requirement">
        <rim:SlotValue xsi:type="rim:AnyValueType">
            <sdg:Requirement>
                <sdg:Identifier>315cfd75-6605-49c4-b0fe-799833b41099</sdg:Identifier>
                <sdg:Name>Proof of Birth</sdg:Name>
            </sdg:Requirement>
        </rim:SlotValue>
    </rim:Slot>
    <rim:Classification id="urn:uuid:d45aa619-2d90-4d6c-ae59-b9ca4e6a5876"
        classificationScheme="urn:fdc:oots:classification:eb" classificationNode="Procedure"/>

</rim:RegistryObject>
```

3.2.5.2.4 Procedure

This Registry Object provides the information of a Procedure. It MUST NOT contain any relations to other Reference Frameworks (Procedures) as this are provided dynamically by the use of associations. The classification node used MUST be `Procedure` under the EB Classification Scheme `urn:fdc:oots:classification:eb.`
An example Procedure Registry Object in XML Format is shown below:

```
<rim:RegistryObject id="urn:uuid:315cfd75-6605-49c4-b0fe-799833b41099"
    xmlns:rim="urn:oasis:names:tc:ebxml-regrep:xsd:rim:4.0"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

    <rim:Slot name="Procedure">
        <rim:SlotValue xsi:type="rim:AnyValueType">
            <Requirement xmlns="http://data.europa.eu/p4s">
                <Identifier>315cfd75-6605-49c4-b0fe-799833b41099</Identifier>
                <Name>Proof of Birth</Name>
            </Requirement>
        </rim:SlotValue>
    </rim:Slot>
```

```
    <rim:Classification id="urn:uuid:d45aa619-2d90-4d6c-ae59-b9ca4e6a5876"
        classificationScheme="urn:fdc:oots:classification:eb" classificationNode="Procedure"/>

</rim:RegistryObject>
```

3.2.5.3 Associations

The EB LCM Interface accepts three distict associations linking the Registry Objects together the SubmitObjectsRequest Message which are defined the sections below

3.2.5.3.1 ContainsEvidence

This Association provides the link between an Evidence Type List and an Evidence Type. The type attribute MUST be `urn:oasis:names:tc:ebxml-regrep:AssociationType:ContainsEvidence`, with the source object pointing to an EvidenceTypeList RegistryObject through the use of its lid and the targetObject pointing to an EvidenceType object.

3.2.5.3.2 FulfillsRequirement

This Association provides the link between an Evidence Type List and a Requirement. The type attribute MUST be `urn:oasis:names:tc:ebxml-regrep:AssociationType:FulfillsRequirement`, with the source object pointing to an EvidenceTypeList RegistryObject through the use of its lid and the targetObject pointing to an Requirement object.

3.2.5.3.3 DerivesFromProcedure

This Association provides the link between a Requirement and a Procedure. The type attribute MUST be `urn:oasis:names:tc:ebxml-regrep:AssociationType:DerivesFromProcedure`, with the source object pointing to a Requirement RegistryObject through the use of its lid and the targetObject pointing to a Procedure object.

3.3 Semantic Repository (SR) - June 2022

NOTE
This section has not been updated since the release of July 2021.

3.3.1 Overview

The Semantic Repository is a central service, providing commonly agreed semantic specifications for the exchange of evidences.

The service should provide the following functionalities:

- Ability to externally reference data models from other components;
- Ability to define and extract subsets of models;
- Provision of documentation.

In order to implement these functionalities, the following components will be included:

- Evidence types: for both the generic metadata model and each specific evidence type, a repository is created which contains the following elements per data model:

  1) A visual class diagram;

  2) A textual description of all the entities of the data model, consisting of a definition and the list of the attributes of the entity. For each attribute, the expected type (Boolean, Identifier, Date, etc), a definition, the cardinality and the optional usage of a code list is indicated. The repository of each evidence will also offer version control and keep track of a change log in between different versions.

  3) Distributions in .XSD, complemented by other widely used serialisation formats if there are operational reasons to do so.

- Code lists: to ensure the automated processing of evidences, certain properties of data models will be populated based on code lists. The code lists will be made available in XML.
- Methodology: to formalise the process of developing new data models for evidence types exchanged in cross-border administrative procedures, a methodology has been designed. This methodology also comprises examples and learning materials.

3.3.2 High-level structure of the semantic repository

The structure below gives an outline of how users will be able to navigate across the various resources and specifications published through the semantic repository. All specifications will allow version control and to embed comments and change requests from the user community.

- Data models
    - Generic metadata model
        - Data model
        - Distributions
        - Documentation
            - Instantiated dummy examples
            - Sources
    - Data models for specific evidence types
        - Data model
        - Distributions
            - Formats
            - Conformance
            - Transformation
        - Documentation
            - Instantiated dummy examples
            - Sources
- Code lists
- Methodology

3.4 Common Services Distribution - June 2022

3.4.1 Introduction

As explained in Chapter 1, section 6.6, the OOTS architecture uses a hybrid deployment model for the Common Services. This section provides more information on distribution of these services, their configuration, discovery, and use of proxy servers.

3.4.2 Common Services Configuration

The data provided by Evidence Broker and Data Service Directory services is logically partitioned in subsets corresponding to the participating Member States. Each of the defined lookup functions includes a parameter to indicate the Member State to which the lookup applies. The OOTS architecture also allows the partition to be reflected in a distribution of the data across multiple component instances. The architecture uses a hybrid deployment model in which:

- The European Commission will provide an instance into which Member States may upload their data.
- Member States may also provide their own instance of the service.

These options are exclusive, meaning that data for a given Member State can, depending on configuration based on the Member State decision, be looked up either in the Commission instance or in an instance provided by the Member State.

The OOTS has the Member State level as its fixed granularity level, meaning that a Member State has either no instance of the Common Service (if it uses the Commission provided instance) or one (if it provides its own instance), but never more than one. It is therefore not possible to, for example, have multiple Data Service Directories for different regions of a Member State.

Note that, over time, a Member State may decide to move the management of its Common Services data from the Commission provided instance to an instance it provides itself, or vice versa. Also, a Member State may also decide to provide one service itself but not the other. For example, a Member State could provide its own Data Service Directory but use the Commission instance of the Evidence Broker.

In addition to being partitioned geographically, common service data and instances are further partitioned according to other criteria. This version of the OOTS supports two such other criteria: production use versus test use and the technical interface version. The latter is intended to support potential migration to future incompatible versions.

3.4.3 Discovery of Common Services

Depending on the option selected by the Member State, lookups must be directed to either the instance provided by the Commission or by the instance provided by the Member State, and similar routing decisions apply for the production/test environment or interface version use. A clear, unambiguous and up to date overview of all instances of the Common Services, for all Member States, for all environments and for technical interface versions is needed and will be provided using the following two mechanisms:

1. Overview tables on a restricted area (to be created) of the OOTS Collaborative Space.
2. An online DNS-based discovery service.

The DNS-based discovery service is similar to and inspired by the OASIS BDXL specification which is used in combination with eDelivery. It uses the mechanism of URI-enabled Naming Authority Pointer (NAPTR) DNS resource records as defined in IETF RFC 4848. For use in OOTS, the Commission shall provide a DNS name template. The template shall include placeholders that are to be substituted for the following parameters:

- The type of common service. Values are “eb” for Evidence Broker service) or “dsd” for Data Service Directory service.
- The geography area. Values are ISO 3166 ALPHA-2 country codes for EU Member States.
- The major version number of the interface of the service instance preceded by the letter “v”. The initial major version number shall be indicated using the string “1”.
- The environment that the instance supports. The string value “prod” shall be used for the production use.

Available service instances shall be mapped to DNS names that instantiate the template with appropriate substitutions for the four above-mentioned parameters. The Commission will communicate the exact format of the template as part of the rollout of the OOTS common services.

For the created names, the Commission will provide NAPTR resource records as follows:

- Record type: “NAPTR”
- Flag: “u”
- Service parameter: “”
- Value: the HTTPS URI of the service encoded using the restricted regular expression syntax defined in section 2.2 of RFC 4848.

The registered HTTPS URI shall be the base server URL of the common service as defined in section12.2 of OASIS ebRS, i.e. the HTTPS URI including the domain root name, without the “/rest/search?q..” part.

The following example is hypothetical record content that could be associated with DNS query strings for all the Member States that use the instance provided by the European Commission.

```
IN NAPTR 100 10 "U" "" "!.*!https://dsd.prod.v1.oots.ec.europa.eu!" .
```

The following equally hypothetical example shows a sample record for the situation in which Germany would operate its own test DSD.

```
IN NAPTR 100 10 "U" "" "!.*!https://test.dsd.once-only.bund.de!" .
```

When requesting data, Common Service clients shall substitute the placeholders in the template by the requested values prior to making DNS requests. They shall then extract the service root (i.e. for the example "https://dsd.prod.v1.oots.ec.europa.eu") and append the predefined path components (i.e. "/rest/search?q.. ") to construct the HTTP client request.

3.4.4 Proxy Caching

Data served by the OOTS common services is expected to be highly static and very suited to use in combination with caching proxy servers.

Member States are strongly recommended to route requests to the OOTS Common Services via caching proxy servers in order to:

- Reduce the load on common services.
- Reduce the latency on OOTS client applications.
- Add fault tolerance in case the origin server is not accessible.

Server implementation of common services shall be configured to set the caching related HTTP headers as described in RFC 7234 to enable caching and to ensure that responses retain their considered freshness sufficiently.

To enable caching, the proxy should terminate TLS connections from its clients and establish its own TLS connections to the origin servers. This is not problematic as the data is not sensitive and its integrity is protected using the response signatures, which the clients shall validate.

3.4.5 References

OASIS Business Document Metadata Service Location Version 1.0. http://docs.oasis-open.org/bdxr/BDX-Location/v1.0/os/BDX-Location-v1.0-os.pdf

OASIS ebXML RegRep Version 4.0 Part 2: Services and Protocols (ebRS). https://docs.oasis-open.org/regrep/regrep-core/v4.0/os/

RFC 4848. Domain-Based Application Service Location Using URIs and the Dynamic Delegation Discovery Service (DDDS) https://datatracker.ietf.org/doc/html/rfc4848

RFC 7234. Hypertext Transfer Protocol (HTTP/1.1): Caching. https://datatracker.ietf.org/doc/html/rfc7234.

3.5 Code Lists - June 2022

3.5.1 Code lists used by the OOTS Exchange Data Models

The following table presents the code lists used by the transactions associated to the EB, DSD, LCM and Evidence Exchange. For each code list, a ShortName, LongName, Version, Agency and FileName is provided. Where applicable the listID and LocationURI is provided. The corresponding code list files can be found in the GIT Repository.

ShortName	LongName @xml:lang="en"	LongName @Identifier="listID"	Version	LocationURI	Agency	FileName
LanguageCode	Language Code	ISO 639	2018-02-14	Language Code	International Organization for Standardization	LanguageCode-2.3
EAS	Electronic Address Scheme		2022-03-04	Electronic Address Scheme	Digital Europe Programme (DIGITAL)	EAS.gc
CountryIdentificationCode	Country Identification Code	ISO 3166	2020-04-17	Country Identification Code	International Organization for Standardization	CountryIdentificationCode-2.3
BinaryObjectMimeCode	Binary Object Mime Code	IANA Media Types	2020-04-14	Binary Object Mime Code	Internet Assigned Numbers Authority	BinaryObjectMimeCode-2.3.gc
LevelsOfAssuranceCode	Levels Of Assurance Code		2018-12-19		The Once-Only Principle Project	LevelsOfAssuranceCode-CodeList.gc
Nuts	Nomenclature of Territorial Units for Statistics	http://publications.europa.eu/resource/authority/nuts	2016	Nomenclature of Territorial Units for Statistics	Publications Office	NutsCodes.gc

IdentifierTypeCode	Identifier Type Code		2020-05-28		The Once-Only Principle Project	IdentifierType-CodeList.gc
ProtocolExceptionCode	Protocol Exception Code		2020-05-28		The Once-Only Principle Project	ProcotolException-CodeList.gc
ErrorSeverity	Error Severity		2018-10-01		The Once-Only Principle Project	ErrorSeverity-CodeList.gc

3.6 Common Services API Specification - June 2022

3.6.1 Introduction

The Common Services of the OOTS provide machine-to-machine APIs both for querying and data lifecycle management. This section specifies the normative common part of these APIs using the OASIS Regrep 4.0 standard. Services implementing these interfaces MUST adhere to the following interface specifications.

3.6.2 Query Interface Specification

3.6.2.1 Introduction

The query interface specification for the Common Services is based on the OASIS ebXML RegRep V4 standard. This standard has multiple protocol bindings that can be used to execute queries. Since the Common Services queries have only simple, single-value parameters, the REST binding is used to implement the DSD query interface. This implies that the query transaction is executed as an HTTP GET request with the URL representing the query to execute and the HTTP response carrying the query response as an XML document. This section profiles the REST binding as specified in the OASIS RegRep standard for use by the Common Services.

3.6.2.2 The RegRep Query Request

The URL pattern for parameterised query invocation is defined as follows in the OASIS RegRep REST binding:

*«server base url»***/rest/search?queryId=***{the query id}*(**&***{param-name}*=*{param-value}*)*

The query interface consists of a simple predefined parameterised query detailed below. In addition, the RegRep standard defines a set of canonical queries and query parameters that can be used. As the Data Service Directory is not a complete implementation of a RegRep server, it is NOT REQUIRED to support these canonical queries and query parameters. Clients, therefore, SHOULD only use the queries and query parameters specified by this specification. When the canonical queries or parameters are used, the Common Service implementation MAY return an error.

3.6.2.3 The RegRep Successful Response

As specified by the RegRep REST binding, the implemented Common Service MUST always return a RegRep QueryResponse document which MUST either contain an `Exception` or `RegistryObjectList` element with zero or more `RegistryObject`s .

An example response, with response-specific details omitted, is provided in the following table:

```
<query:QueryResponse xmlns="urn:oasis:names:tc:ebxml-regrep:xsd:lcm:4.0"
    xmlns:lcm="urn:oasis:names:tc:ebxml-regrep:xsd:lcm:4.0"
    xmlns:query="urn:oasis:names:tc:ebxml-regrep:xsd:query:4.0"
    xmlns:rim="urn:oasis:names:tc:ebxml-regrep:xsd:rim:4.0"
    xmlns:rs="urn:oasis:names:tc:ebxml-regrep:xsd:rs:4.0"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="urn:oasis:names:tc:ebxml-regrep:xsd:lcm:4.0"
totalResultCount="1" startIndex="0" status="urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Success">
    <!-- depending on the count of datasets returned, the totalResultCount attribute should
  reflect the number of the datasets returned -->
    <rim:RegistryObjectList>
        <!-- One registry object per dataset -->
        <rim:RegistryObject id="urn:uuid:a1be6e74-e9ba-4d44-b04c-0376f367b8fd">
            <rim:Slot name="DataServiceEvidenceType">
                <rim:SlotValue xsi:type="rim:AnyValueType">
                    <DataServiceEvidenceType xmlns="http://data.europa.eu/sdg#">
                      <!-- Omitted for clarity -->
                    </DataServiceEvidenceType>
                </rim:SlotValue>
            </rim:Slot>
        </rim:RegistryObject>
    </rim:RegistryObjectList>
</query:QueryResponse>
```

3.6.2.4 The RegRep Error Response

When an error occurs during the execution of the query, the Common Service returns an exception as defined in the Common Service Query Interface Specification. The exception has the following properties that are profiled for each expected error of the query.

- **xsi:type:** The type of the error, selectable from a predefined set of error classes of the Query Interface of the Common Service.
- **severity:** The severity of the error, selectable from a predefined set of error classes of the Query Interface of the Common Service.
- **message:** A string describing the error in Human Readable form.
- **code:** A code for the error, specified by the Common Service Technical Design documents.

An Example of an empty result set is provided below:

```
<?xml version="1.0" encoding="UTF-8"?>
<query:QueryResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                     xmlns:rs="urn:oasis:names:tc:ebxml-regrep:xsd:rs:4.0"
                     xmlns:rim="urn:oasis:names:tc:ebxml-regrep:xsd:rim:4.0"
                     xmlns:query="urn:oasis:names:tc:ebxml-regrep:xsd:query:4.0"
                     status="urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Failure">

  <rs:Exception
      xsi:type="rs:ObjectNotFoundExceptionType"
      severity="urn:oasis:names:tc:ebxml-regrep:ErrorSeverityType:Error"
      message="No Evidence Providers were found based on the given parameters"
      code="DSD:ERR:0001">
  </rs:Exception>
</query:QueryResponse>
```

Depending on the exception raised, the message response may contain information on how to properly recover from the exception. For example, a common service may send back an exception when more attributes are needed to be provided in order for the Common Service to properly respond. These details are further specified in their respective specifications.

3.6.3 The Lifecycle Management Specification

3.6.3.1 Introduction

A Common Service MAY provide a Lifecycle Management (LCM) Interface for a bulk update of the information stored in the Common Services of a Member State. This section provides the technical specification of this interface as it will be implemented by the European Commission to implement its Common Services. This LCM interface is a highly constrained profile based on the RegRep 4.0 LCM Manager Interface Specification that has the following limitations:

- Only the SubmitObjects protocol is supported.
- Each Member State shall authorize at most one authorized competent authority to make submissions.
- A submission is linked to a single Member State and made on behalf of that Member State.
- Submission linked to a single Member State do not affect data related to other Member States.
- A submission contains a complete, internally consistent set of data. It is not possible to incrementally submit objects using a series of submissions.
- In case of a successful submission made for a Member State to a Common Service, any existing data previously submitted to the Common Service for that Member State is replaced. This obviates the need for the RemoveObjects protocol.
- In case of an unsuccessful submission made for a Member State to a Common Service, the existing data held by the Common Service is retained.

Since object submission updates data, this profile use eDelivery for secure and reliable messaging as described below.

A service implementing the LCM specification MUST define a Classification Scheme using a unique `urn`. The Classification Scheme MUST contain all the Classification Nodes that properly characterize the registry objects and associations under submission.

The SubmitsObjects Protocol defines a `SubmitsObjectsRequest` message for sending the objects to be added together with successful and error responses. The following subsections define these messages in detail.

3.6.3.2 The Regrep LCM Submission

For the LCM submission, the profile uses the SubmitObjectsRequest message, as defined by the RegRep 4.0 LCM Manager Interface Specification SubmitObjects Protocol. The message MUST contain a unique id and one `Registry Object List` containing the `Registry Objects` under submission.

The attribute “checkReferences” on SubmitObjectsRequest MUST be set to “true” to express that a server MUST check submitted objects and make sure that all references via reference attributes and slots to other RegistryObjects are resolvable. If a reference does not resolve then the server MUST return UnresolvedReferenceException.

Each contained `Registry Object` MUST contain:

- A `Classification` with a `Classification Node` that is part of the `Classification Scheme` as defined by the service implementing the profile.

- An `lid` attribute that must be unique using a UUID version 4 urn. This logical id MUST be used in the contained `association`s, for associating source and target registry objects.
- A Slot with a name that is identical with the `Classification`'s `Classification Node.` The slot MUST contain the information of the Registry Object according to the service profiled specification

Each contained `Registry Object` that is an `Association` MUST Contain:

- the xsi:type which MUST be of value `rim:AssociationType`
- An `lid` attribute that must be unique using a UUID version 4.
- the sourceObject attribute that denotes the starting point of the association. The attribute value MUST be the UUID v4 urn lid of a `Registry Object`
- the targetObject attribute that denotes the ending point of the association. The attribute value MUST be the UUID v4 urn lid of a `Registry Object`
- The type attribute which MUST use Classification Nodes, defined as extensions to the canonical `AssociationType Classification Scheme` of RegRep v4.0

```
<lcm:SubmitObjectsRequest xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:rs="urn:oasis:names:tc:ebxml-regrep:xsd:rs:4.0"
  xmlns:rim="urn:oasis:names:tc:ebxml-regrep:xsd:rim:4.0"
  xmlns:query="urn:oasis:names:tc:ebxml-regrep:xsd:query:4.0"
  xmlns:lcm="urn:oasis:names:tc:ebxml-regrep:xsd:lcm:4.0"
  xmlns:sdg="http://data.europa.eu/sdg#"
  xmlns:xlink="http://www.w3.org/1999/xlink"
  id="urn:uuid:4dd63731-1b16-484e-af7c-baaf492f9073">

  <rim:RegistryObjectList>
    <rim:RegistryObject lid="urn:uuid:a1be6e74-e9ba-4d44-b04c-0376f367b8fd">
      <rim:Classification id="urn:uuid:e8cd682c-08f2-4f90-a310-dc2c4d785fdb"
           classificationScheme="urn:fdc:oots:classification:example"
           classificationNode="ExampleNode"/>

      <rim:Slot name="ExampleNode">
        <rim:SlotValue xsi:type="rim:AnyValueType">
         <!-- Registry Object Data -->
        </rim:SlotValue>
      </rim:Slot>
    </rim:RegistryObject>

    <rim:RegistryObject lid="urn:uuid:9d72ced7-638e-4023-9712-d7e871bf7d3d">
       <rim:Classification id="urn:uuid:e8cd682c-08f2-4f90-a310-dc2c4d785fdb"
           classificationScheme="urn:fdc:oots:classification:example"
           classificationNode="ExampleNode"/>

     <rim:Slot name="ExampleNode">
         <rim:SlotValue xsi:type="rim:AnyValueType">
         <!-- Registry Object Data -->
        </rim:SlotValue>
      </rim:Slot>

    </rim:RegistryObject>

    <!-- Association -->
    <rim:RegistryObject xsi:type="rim:AssociationType"
         id="urn:uuid:ac720bc9-b967-4858-b3f7-83d26020dab7"
         sourceObject="urn:uuid:a1be6e74-e9ba-4d44-b04c-0376f367b8fd"
```

```
            targetObject="urn:uuid:9d72ced7-638e-4023-9712-d7e871bf7d3d"
            type="urn:oasis:names:tc:ebxml-regrep:AssociationType:Serves"/>
    </rim:RegistryObjectList>
</lcm:SubmitObjectsRequest>
```

3.6.3.3 The Regrep LCM Successful Response

Upon a successful SubmitObjectsRequest message submission, the service MUST return a `RegistryResponse` message that MUST contain:

- A `requestId` attribute with the value of the id of the `submitObjectsRequest` that this message responds to.
- A `status` attribute with the value "`Success`"

The following example shows a successful response to the SubmitObjectsRequest of section 3.1

```
<RegistryResponse xmlns="urn:oasis:names:tc:ebxml-regrep:xsd:rs:4.0"
                  status="urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Success"
                  requestId="urn:uuid:4dd63731-1b16-484e-af7c-baaf492f9073"/>
```

3.6.3.4 The Regrep LCM Error Response

When an error occurs during the execution of the SubmitObjectsRequest, the Common Service returns an exception. The exception has the following properties that are profiled for each expected error of the submission request.

- **xsi:type:** The type of the error, selectable from a predefined set of error classes of the LCM Interface of the Common Service.
- **severity:** The severity of the error, selectable from a predefined set of error classes of the LCM Interface of the Common Service.
- **message:** A string describing the error in Human Readable form.
- **code:** A code for the error, specified by the Common Service Technical Design documents.

An Example of an empty result set is provided below:

```
<?xml version="1.0" encoding="UTF-8"?>
<rs:RegistryResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                     xmlns:rs="urn:oasis:names:tc:ebxml-regrep:xsd:rs:4.0"
                     xmlns:rim="urn:oasis:names:tc:ebxml-regrep:xsd:rim:4.0"
                     xmlns:query="urn:oasis:names:tc:ebxml-regrep:xsd:query:4.0"
                     status="urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Failure"
                     requestId="urn:uuid:4dd63731-1b16-484e-af7c-baaf492f9073">

  <rs:Exception
      xsi:type="rs:ObjectNotFoundExceptionType"
      severity="urn:oasis:names:tc:ebxml-regrep:ErrorSeverityType:Error"
      message="Generic Error"
      code="SERVICE:ERR:0001">
  </rs:Exception>
</rs:RegistryResponse>
```

3.6.3.4.1 Common Error Codes

#	Error Title	Type	code	Message
1	Invalid Registry Object	rs:InvalidRequestExceptionType	LCM:ERR:0001	A registry object in the Request does not comply with the specification
2	Invalid Association	rs:InvalidRequestExceptionType	LCM:ERR:0002	An association in the Request does not comply with the specification
3	Inconsistent Dataset	rs:InvalidRequestExceptionType	LCM:ERR:0003	The dataset provided failed to pass the validation and integrity check

3.6.3.5 eDelivery Configuration

Since object submission updates data, the LCM interface uses eDelivery for secure and reliable messaging.

Use of eDelivery MUST follow the OASIS ebXML Messaging Protocol Binding for RegRep Version 1.0. That specification provides details needed for proper eDelivery configuration, including the values for the AS4 *Service*, *Action* and *Role* message headers and for packaging.

Use of eDelivery MUST also follow the OOTS eDelivery configuration as specified in chapter 4.7. This means that the Access Point of the authorized competent authority is pre-configured for message exchange with the Access Point of the Common Service and that the four corner topology profile enhancement is used.

At most one competent authority per Member State will be allowed to send object submission requests to the Common Service. The party identifier for this authority will be used as *originalSender* in LCM requests and as *finalRecipient* in LCM responses. The Common Service MUST reject requests from parties other than authorized parties using exceptions of type AuthorizationException.

4 Chapter 4: Evidence Exchange - June 2022

Evidence Exchange - June 2022

Summary
Evidence exchange in the OOTS is based on bilateral exchange between competent authorities. An exchange is always a combination of two correlated messages:

- An Evidence Request message generated by an Online Procedure Portal in a Member State, supporting a competent authority in the “Evidence Requester” role;
- A corresponding Evidence Response message generated by a Data Service in one or several other Member States, supporting a competent authority in the “Evidence Provider” role.
- Alternatively to the Evidence Response message, an Evidence Error message may be returned.

For interoperability, the OOTS specifications in this chapter define in detail the structure and content and message exchange parameters.
The chapter includes the following sub-chapters:

Change log
For this release, the changes for all chapters are combined at the top level

4.1 Introduction to Exchange Data Model and Protocol - June 2022

The **Evidence Exchange** section describes the scope and goals of the **Exchange Data Models (EDM)** that support the communication between two competent authorities. It provides the business requirements for the Evidence Request (Request from Evidence Requester to Evidence Provider to request certain evidence data or documents) and the Evidence Response (Response from Evidence Provider to Evidence Requester to deliver the requested evidence data or documents). The Query Model is always based on these request-response pattern and supports the execution of document queries including eventual Error Responses that may occur during the execution. The syntax mapping for the Exchange Data Models to form XML-based messages is also provided, including examples.

In this chapter, the Exchange Data Models are being detailed. Three main messages are defined:

- Evidence Request;
- Evidence Response;
- Error Response.

The **Evidence Request** is the message created by the Evidence Requester, containing all the necessary information for requesting an Evidence. Depending on the preference and availability, the Evidence Request can be used to query documents, that are either structured and unstructured pieces of evidence. In preparation to the request, the Evidence Broker helps to determine which evidence types can be accepted for a particular procedure. A list of Evidence Providers that issue the required Evidence Type together with associated metadata can be looked up in the Data Service Directory. The Evidence Requests is then addressed to a specific Evidence Provider that has been identified in the Data Service Directory (DSD).

The **Evidence Response** is the answer to an Evidence Request created by the Evidence Provider and sent to the Evidence Requester. It contains necessary information of the Evidence Provider and data for the correlation of the Evidence Response with the respective Evidence Request. The response messages distinguish between three different status:

- Success: The Evidence Response message is delivered together with the requested Evidence and its associated Metadata.
- Unavailable: The Evidence Response message points to a date when the requested Evidence will be available. The Evidence Requester then can define a new Evidence Request at the time of availability.
- Failure: The response message is defined as Error Response that points to an exception that occurred during the processing of an Evidence Request such as a missing authorization, an object that cannot be found or the need for preview on the side of the Evidence Provider. The Evidence Requester then can define a new Evidence Request who fulfills the requirements.

The **Evidence Exchange specification** firstly illustrates the scope, goals and architecture requirements of the Exchange Data Models, and the underlying business requirements for Evidence Requests, Evidence Responses and Error Responses.

The Exchange Data Models make use of the functional capabilities of the OASIS RegRep V4 Query Protocol, and therefore the request and response messages are being modeled in the form of query models. The query models are illustrated together with a mapping to the appropriate syntax elements of the OASIS RegRep V4 Query Protocol and the syntax elements of the SDG metadata profile, a generic metadata model for the OOTS that is used to enhance the capability of the OASIS RegRep V4 Query Protocol (Syntax Mapping). In this way, for each Exchange Data Model, a specific SDGR Application Profile is defined that consists of syntax mappings to all necessary information entities for Evidence Requests, Evidence Responses and Error Responses. Class diagrams, tables and XML examples of the Evidence Exchange illustrate the shape of the Exchange Data Models.

In the further course of the document, business rules formalize the constraints associated to the Exchange Data Models and their information entities. Business rules therewith control the correct structure and use of information entities and are in the process of being implemented as executable Schematron rules that can be used for testing and validation.

At the end of the document, additional components such as eDelivery configuration, Evidence Exchange Logging and Evidence Preview are specified.

4.2 Scope and Goals - June 2022

4.2.1 Scope & Goals

The OOTS Exchange Data Model design describes a process providing electronic messaging support for requesting Evidence documents. The specification, therefore, differentiates between the Evidence Request transaction and the Evidence Response transaction. Differences between these two transactions are found on the conceptual and process level. While the Evidence Request enables Evidence Requesters (ER) to initiate document queries to the Evidence Providers (EP), the Evidence Response provides the possibility to return the requested Evidence and its associated Evidence metadata. Thus:

- The Evidence Request describes the transaction from ER to EP to request certain structured or unstructured pieces of evidence.
- The Evidence Response describes the transaction from EP to ER to deliver the requested evidence and its accompanying metadata or to inform the ER about exceptions or unavailability of the evidence until a given time.

The OOTS Exchange Data Model structure is generic in its design, meaning that the structure itself is independent of specific Evidence Types. However, the OOTS Exchange Data Model's abstract structure must be filled with concrete information established in certain business domains. The Evidence Request then enables ERs to ask for certain Evidence Types (e.g. Birth Certificates), formats and to adress particular data services in the business domains. The Evidence Response then enables the EPs of that business domain to deliver the corresponding Evidence Type as evidence document (positive case) or to inform the ER about excpetions that occured (negtive case).

To ensure a high level of interoperability, comprehension and reusability, the OOTS Exchange Data Model is based on several core vocabularies and metadata profiles such as CCCEV, DCAT, CBV and CPV that are captured within the OOTS Generic Metadata Profile. These standards are integrated and combined with the overarching standard OASIS ebXML RegRep Version 4.0 to form a generic query model for the OOTS. The combination of these standards enables the OOTS Exchange Data Model to address information entities raised by other OOTS High-Level Architecture components (e.g. eDelivery, eID, DSD, Evidence Broker) and to facilitate their interaction.

Thus, the main goals to be gained by implementing the OOTS Exchange Data Model are:

ID	Description
G-001	The OOTS Exchange Data Model allows an evidence exchange between the ER and the EP.
G-003	An EP can automatically generate an Evidence Response according to the Evidence Request of an ER.
G-004	The OOTS Exchange Data Model structure must be abstract to allow the request for evidence types for any electronic procedure.

G-005	The OOTS Exchange Data Model is based on existing architecture components and standards and facilitates their interaction (e.g. eDelivery, eID, DSD, Evidence Broker)

4.2.2 Architecture Requirements

To enable this evidence exchange, the OOTS Exchange Data Model requires several information elements. It needs to describe and identify the Evidence Subject (ES) uniquely, being either a legal person or a natural person (taking into account whether authorized representatives have appropriate authorization to act on behalf of the ES). The ES or its authorized representative (denoted as user in the architecture requirements) must then provide its explicit request to an ER to initiate an Evidence Request for a piece of evidence. On the other hand, an ER needs to identify the requested evidence type required for a procedure (capability provided the Evidence Broker), identify an appropriate evidence provider and/or data service to deliver/issue the evidence (capability provided through the Data Service Directory) and authorize the ES through eIDAS.

When the Evidence Request has been send it needs to enable the EP to identify the ES through record matching using appropriate ES identity attributes of the Evidence Request. In order to initiate the evidence provision, the EP may require from the ER that the ES (or user) is redirected from the ER procedure portal to the preview space of the EP (indicated through an Error Response with information about the preview space) in order to perform an EP-side authorization and to preview and select the evidence. Throughout the preview process the EP may ask the ES (or user) to provide further information (e.g. jurisdiction information or other classification values) to address the correct data service and find the evidence. When compiling the Evidence Response, an EP needs to place the requested evidence and evidence metadata inside the response. In cases where evidences are not available yet, the EP needs to signal a date of availability to the ER in the Evidence Response that indicates when the evidence can be retrieved through another Evidence Request. If an EP cannot answer an Evidence Request, it must provide notification back to the ER by sending an appropriate Error Response with the reasons for failure.

The following architecture requirements describe the architecture requirements connected to the EDM which are further detailed in the business requirements section.

ID	Description	Category	Reference to Business Requirement
AR-01	The Evidence Requester must be able to send an Evidence Request to the Evidence Provider.	General Processing	REQ01-RESP09
AR-02	The Evidence Requester must describe the procedure and requirements that are the basis for the issued Evidence Request.	Procedural Requirements	REQ10-RESP11
AR-03	The Evidence Requester must include information about the Evidence Requester and Evidence Provider to the Evidence Request.	Evidence Requester and Evidence Provider	REQ12-RESP13

ID	Description	Category	Reference to Business Requirement
AR-04	The Evidence Requester must identify the Evidence Subject associated with the user.	Evidence Subject	REQ15-RESP18
AR-05	Evidence Requester must be able to identify and describe the evidence about the Evidence Subject that is requested from the Evidence Provider.	Evidence Request	REQ19-RESP21
AR-06	The Evidence Provider must be able to sent the requested Evidence or a date of availability to the Evidence Requester.	General Processing	RESP01-RESP06
AR-07	The Evidence Provider must include information about the Evidence Requester and Evidence Provider to the Evidence Response.	Evidence Requester and Evidence Provider	RESP07-RESP08
AR-08	The Evidence Provider must include the evidence and associated evidence metadata to the Evidence Response.	Evidence and Evidence Metadata	RESP09-RESP15
AR-09	The Error Provider must be able to sent and Error Response to the Evidence Requester.	General Processing	ERR01-ERR04
AR-10	The Error Provider must include information about the Evidence Requester and Evidence Provider to the error response.	Evidence Requester and Evidence Provider	ERR05-ERR06
AR-11	The Error Provider must describe the exception that occurred and may, as a particular exception, indicate requirements related to an Evidence Provider side preview.	Exception	ERR07-ERR10

4.3 Business Requirements - June 2022

In this section, the business requirements of the Evidence Request, the Evidence Response and the Error Response are identified in a structured format.

4.3.1 Evidence Request Business Requirements

The following tables structure the business requirements identified for the Evidence Request. In the **information entity** column, we map the information entity that covers the requirement.

4.3.1.1 General Processing

ID	Requirement	Information Entity
REQ01	The Evidence Request must be identified.	query:QueryRequest
REQ02	The Evidence Request must be timestamped.	rim:Slot "IssueDateTime"
REQ03	The Evidence Request must point to its underlying specification.	rim:Slot "SpecificationIdentifier"
REQ04	The Evidence Request may point to a preview location if required by the evidence provider.	rim:Slot "PreviewLocation"
REQ05	The Evidence Request must indicate if the Evidence Requester requires a preview to be done.	rim:Slot "PossibilityForPreview"
REQ06	The Evidence Request must indicate if an explicit request was given by the Evidence Subject.	rim:Slot "ExplicitRequest"
REQ07	The Evidence Request must indicate the query type which is associated to the Evidence Request.	query:Query
REQ08	The Evidence Request must be addressable to a specific Evidence Provider via electronic address.	eDelivery Configruation Profile
REQ09	The Evidence Request must indicate response type which is expected by the Evidence Response.	query:ResponseOption

4.3.1.2 Procedural Requirements

ID	Requirement	Information Entity
REQ10	An Evidence Request should describe the procedure in which it was created and initiated.	rim:Slot "Procedure"
REQ11	An Evidence Request should name the requirement for which it was created and initiated.	rim:Slot "Requirements"

4.3.1.3 Evidence Requester and Evidence Provider

ID	Requirement	Information Entity
REQ12	The Evidence Request must contain the identifier, name, address and classification of the Evidence Requester.	rim:Slot "EvidenceRequester"
REQ13	The Evidence Request must contain the identifier, name of the Evidence Provider.	rim:Slot "EvidenceProvider"

ID	Requirement	Information Entity
REQ14	The Evidence Request may indicate additional Evidence Provider specific classification values provided by the user which are required by the Evidence Provider to discover the evidence.	rim:Slot "EvidenceProviderClassificationValues"

4.3.1.4 Evidence Subject

ID	Requirement	Information Entity
REQ15	The Evidence Request must determine if the request is related to a legal person or a natural person.	rim:Slot "NaturalPerson" rim:Slot "LegalPerson"
REQ16	The Evidence Request shall use the minimum data set (mandatory elements) of the eIDAS SAML Attribute Profile v.1.2 to uniquely describe the legal person reflecting the Evidence Subject. Additionally, optional elements and sector specific attributes may be used where appropriate.	rim:Slot "LegalPerson"
REQ17	The Evidence Request shall use the minimum data set (mandatory elements) of the eIDAS SAML Attribute Profile v.1.2 to uniquely describe the natural person reflecting the Evidence Subject. Additionally, optional elements and sector specific attributes may be used where appropriate.	rim:Slot "NaturalPerson"
REQ18	The Evidence Request should describe a natural person with the authorisation and power to act on behalf of a legal entity or natural person. The Evidence Request shall therefore use the minimum data set (mandatory elements) of the eIDAS SAML Attribute Profile v.1.2 to uniquely describe the authorized natural person associated to the request as Evidence Subject. Additionally, optional elements and sector specific attributes may be used where appropriate.	rim:Slot "AuthorizedRepresentative"

4.3.1.5 Evidence Request

ID	Requirement	Information Entity
REQ19	The Evidence Request must identify the evidence type and its associated data service and contain the title and description of the evidence requested from the Evidence Provider.	rim:Slot "EvidenceRequest"
REQ20	The Evidence Request must specify the preferred format of the Evidence and shall indicate a desired conformance and transformation profile if applicable.	rim:Slot "EvidenceRequest"
REQ21	The Evidence Request should be enabled to indicate a desired conformance and transformation profile to retrieve pieces of evidence conforming to the common data models available in the semantic repository.	rim:Slot "EvidenceRequest"

4.3.2 Evidence Response Business Requirements

The following tables structure the business requirements identified for the Evidence Response.

4.3.2.1 General Processing

ID	Requirement	Information Entity
RESP01	The Evidence Response must point to the Evidence Request for which the Evidence Response was created.	query:QueryResponse
RESP02	The Evidence Response must indicate if the Evidence is available or unavailable	query:QueryResponse
RESP03	If the Evidence is unavailable, the Evidence Request must indicate the date and time when the evidence will be available.	rim:Slot "ResponseAvailableDateTime"
RESP04	The Evidence Response must point to its underlying specification.	rim:Slot "SpecificationIdentifier"
RESP05	The Evidence Response must be identified.	rim:Slot "EvidenceResponseIdentifier"
RESP06	The Evidence Response must be timestamped.	rim:Slot "IssueDateTime"

4.3.2.2 Evidence Provider and Evidence Requester

ID	Requirement	Information Entity
RESP07	The Evidence Response must contain the identifier, name, address and classification of the Evidence Provider.	rim:Slot "EvidenceProvider"
RESP08	The Evidence Response must contain the identifier, name of the Evidence Requester.	rim:Slot "EvidenceRequester"

4.3.2.3 Evidence and Evidence Metadata

ID	Requirement	Information Entity
RESP09	The Evidence Response must identify the evidence and indicate its issuing date.	rim:Slot "EvidenceMetadata"
RESP10	The Evidence Response must declare the Evidence Subject associated to the evidence being either a natural person or a legal person.	rim:Slot "EvidenceMetadata"

ID	Requirement	Information Entity
RESP11	The Evidence Response must describe the authority that issued the evidence.	rim:Slot "EvidenceMetadata"
RESP12	The Evidence Response must contain the evidence type and title which is associated to the evidence.	rim:Slot "EvidenceMetadata"
RESP13	The Evidence Response must describe the distribution of the evidence. The distribution must at least contain the format of the evidence. The evidence may be further specified through other distribution elements such such as packaging format, compression format, language and the underlying conformance profile.	rim:Slot "EvidenceMetadata"
RESP14	The Evidence Response may indicate a period of validity of the evidence.	rim:Slot "EvidenceMetadata"
RESP15	The Evidence Response must contain an identifier that points to the internal location and filename of the evidence document.	rim:RespositoryItemRef

4.3.3 Error Response Business Requirements

The following tables structure the business requirements identified for the Evidence Response.

4.3.3.1 General Processing

ERR01	**The Error Response must point to the Evidence Request for which the Error Response was created.**	**query:QueryResponse**
ERR02	The Error Response must indicate that the Evidence Request has failed.	query:QueryResponse
ID	**Requirement**	Information Entity
ERR03	The Error Error Response must point to its underlying specification.	rim:Slot "SpecificationIdentifier"
ERR04	The Error Response must be identified.	rim:Slot "EvidenceResponseIdentifier"

4.3.3.2 Error Provider and Evidence Requester

ID	Requirement	Information Entity
ERR05	The Error Response must contain the identifier, name, address and classification of the Error Provider.	rim:Slot "ErrorProvider"
ERR06	The Error Response must contain the identifier, name of the Evidence Requester.	rim:Slot "EvidenceRequester"

4.3.3.3 Exception

ID	Requirement	Information Entity
ERR07	The Error Response must indicate the error type, the severity and provide and error message.	rs:Exception
ERR08	The Error Response may provide further details and code value to describe the exception.	rs:Exception
ERR09	The Error Response must link each error to a timestamp indicating when the error was created.	rim:Slot "Timestamp"
ERR10	The Error Response may indicate a preview location, preview description and preview method if the error occurred due to the need to authenticate the user and to execute a preview of the evidence on the side of the Evidence Provider.	rim:Slot "PreviewLocation" rim:Slot "PreviewDescription" rim:Slot "PreviewMethod"

4.4 Query Model - June 2022

4.4.1 Overview

The Exchange Data Model makes use of the functional capabilities that are provided by the RegRep V4 Query Protocol. In the following section, we describe the query that is supported by the OOTS.

4.4.2 Common Query Attributes

4.4.2.1 Common Query Attributes

The following table depicts the attributes that are common between all the types of requests and are expressed as Top-Level Slots and specific Query Slots of the RegRep Information Model.

SLOT NAME	TYPE	VOCABULARIES	CARDINALITY
Top-Level Slots			
SpecificationIdentifier	StringValueType	SDGR Application Profile	1..1
IssueDateTime	DateTimeValueType	SDGR Application Profile	1..1
Procedure	InternationalStringValueType	SDGR Application Profile	0..1
PreviewLocation	StringValueType	SDGR Application Profile	0..1
PossibilityForPreview	BooleanValueType	SDGR Application Profile	1..1
ExplicitRequestGiven	BooleanValueType	SDGR Application Profile	1..1
Requirements	CollectionValueType	Core Criterion and Core Evidence Vocabulary	0..1
EvidenceRequester	CollectionValueType	Core Public Service Vocabulary Application Profile	1..1
EvidenceProvider	AnyValueType	Core Public Service Vocabulary Application Profile	1..1
EvidenceProviderClassificationValues	CollectionValueType	SDGR Application Profile	0..1
Query Slots			
EvidenceRequest	AnyValueType	DCAT Application Profile	1..1
LegalPerson	AnyValueType	Core Business	0..1 → Must contain either a Legal or a Natural Person but **NOT** both.

SLOT NAME	TYPE	VOCABULARIES	CARDINALITY
NaturalPerson	AnyValueType	Core Person	0..1 → Must contain either a Legal or a Natural Person but **NOT** both.
AuthorizedRepresentative	AnyValueType	Core Person	0..1

4.4.2.2 Evidence Request Subject

The Evidence Subject is either a Natural Person or a Legal Person. The Query Slots contain the required information to identify the Evidence Subject.

A Query Request may either contain a NaturalPerson **OR** a LegalPerson depending on the subject of the query, but **NOT** both. An additional Authorized Representative may be specified.

In order to describe the Natural Person and the Legal Representative, the eGovernment Core Person Vocabulary is used. For the Legal Person, the eGovernment Core Business Vocabulary is used. The vocabularies are maintained by Interoperable Europe which succeeds the ISA^2 action.

The Document-Based Query defines a structure for requesting unstructured or structured pieces of evidence that will be used in a specific procedure. The Query Response contains the evidence and evidence metadata with a reference to the document itself.

4.4.3 Document Query

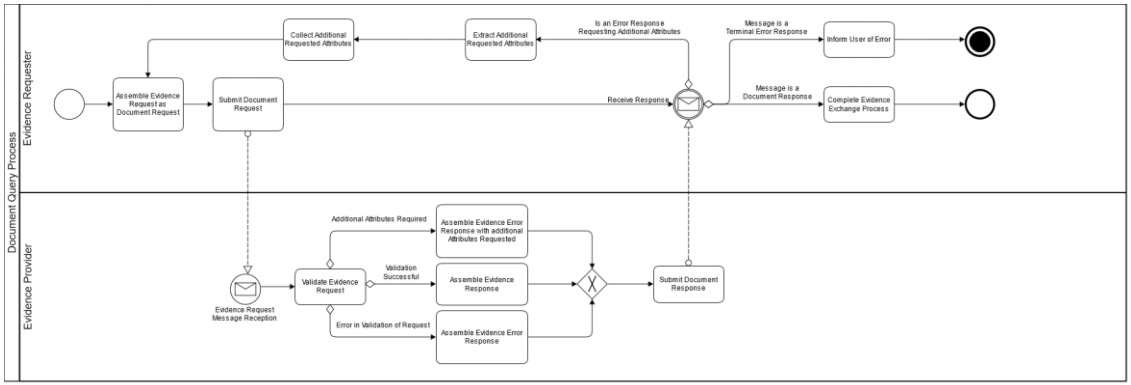
4.4.3.1 Document Query attributes and Process Model

The Evidence Exchange is always based on a document query. The ER requests for the evidence document and its metadata to be provided in the response. The table below shows the query attributes and their value/structure.

Query Attribute	Value / Structure
Query Definition	DocumentQuery
Response Option Attribute	LeafClassWithRepositoryItem
Request Parameters	Elements to identify the Evidence Type issued by a Data Service like identifer, evidence type and title. Distribution attributes of the document, like the format, transformation or conformance profile. Optional EvidenceProviderClassificationValues that help the evidence provider to identify the evidence or data service.
Response Values	Success: Evidence Metadata and attached Evidence document indicated though a RepositoryItemRef

Query Attribute	Value / Structure
	OR Unavailable: ResponseAvailableDataTime OR Failure: Error Response

The following process model provides an overview of the One Step Document-Based Query. The process model depicts the specific query attributes of a Document Query as transaction notes. These attributes are required to formulate a valid query for the desired query type. The common query attributes are not illustrated in the process model but the next section provides a brief overview.



4.4.3.2 Query Request

The ER needs to provide an Evidence Request that contains several evidence-related request parameters. The details contain the following attributes which act as a filtering mechanism to the EP:

- The Identifier of the Data Service Evidence Type received from the Data Service Directory
- The Evidence Type Classification and Title of the evidence received from the Evidence Broker and/or Data Service Directory

- The Format and Conformance Profile of the selected Distribution retrieved from the Data Service Directory.
- A desired Transformation of the Evidence described in the Semantic Repository.
- Optional Classification Values indicated in the Data Service Directory for the EP that help the EP to identify the evidence or data service.

The response option attribute 'returnType' is set to "LeafClassWithRepositoryItem" in order to explicitly state that the requested document MUST be inside Query Response from the EP.

The Evidence Request is expressed along the Evidence Request Syntax Mapping.

4.4.3.3 Query Responses

The Query Response can be either an Evidence Response or an Error Response whereas the status of the Evidence Response can be success of unavailable.

Success: The Evidence Response is sent after a successful validation of the request received and it contains the Evidence Metadata of the attached Evidence together with the Evidence documents themselves. The status of the Evidence Response is set to 'Success'. The Evidence Response with the status 'success' is specified along the Evidence Response Syntax Mapping. The Evidence Metadata described in the Evidence Request is expressed using DCAT Application Profile.

Unavailable: In situations where evidences may exist that are not immediately available, a Data Service may notify the user and start a process to make these evidences available at a later point in time in the Evidence Response. The status of the Evidence Response is set to 'Unavailable'. The status may be used by a Data Service that generates evidences using a process that cannot be completed within the duration of an interactive user session. Based on this response, the Online Procedure Portal has an obligation to inform the user accordingly. It is up to the user to decide whether to proceed with the procedure without the unavailable evidences, or to stop (or, if supported by the Online Procedure Portal, pause) the procedure and re-start (or, if supported, continue) it at a later point in time and re-request the evidences at that later time. This mechanism is opt-in for Data Services. A Data Service that supports the mechanism may, optionally, indicate at which date and time any evidences may be made available, helping the user decide whether and when to return to the Online Procedure Portal and continue the procedure. The Evidence Response with the status 'unavailble' is specified along the Evidence Response Syntax Mapping.

Failure: The Error Response contains the exception raised by the EP. The exception can be either a handled one, which means that the ER SHOULD retry the submission of the Evidence Request fulfilling the requirements present in the exception or an unhandled one which the ER must accept and inform the user of the unsuccessful transaction. The Query Model caters for both handled and unhandled exceptions. A typical example for a managable exception is the need for an Evidence Provider side preview which is declared in the Error response. The Error Request is expressed along the Error Response Syntax Mapping.

4.5 Syntax Mapping - June 2022

4.5.1 Overview

The OOTS uses OASIS Regrep v4 for the syntax mapping of the EDM. It provides a standardised way of expressing messaging transactions, like queries, data creation and data updates. RegRep v4 uses the Slot mechanism for data provision, and it is extensively used in the EDM profile.

In the EDM, there are two main messages defined: The Evidence Request and the Evidence Response. The Evidence Request is the message created by the Evidence Requester, containing all the necessary information requirements for requesting datasets, whether they are structured or unstructured datasets. The Evidence Response responds to an Evidence Request with the necessary information for the correlation of the Evidence Response with the respective Evidence Request, the actual data provided and the metadata of the Evidence Provider who is the responder.

Each message defines its own information requirements that are expressed as slots. Depending on the type of request, the information requirements can vary. In the following sections, we describe the messages, the common information requirements and the specific information requirements.

4.5.2 Evidence Request Syntax Mapping - June 2022

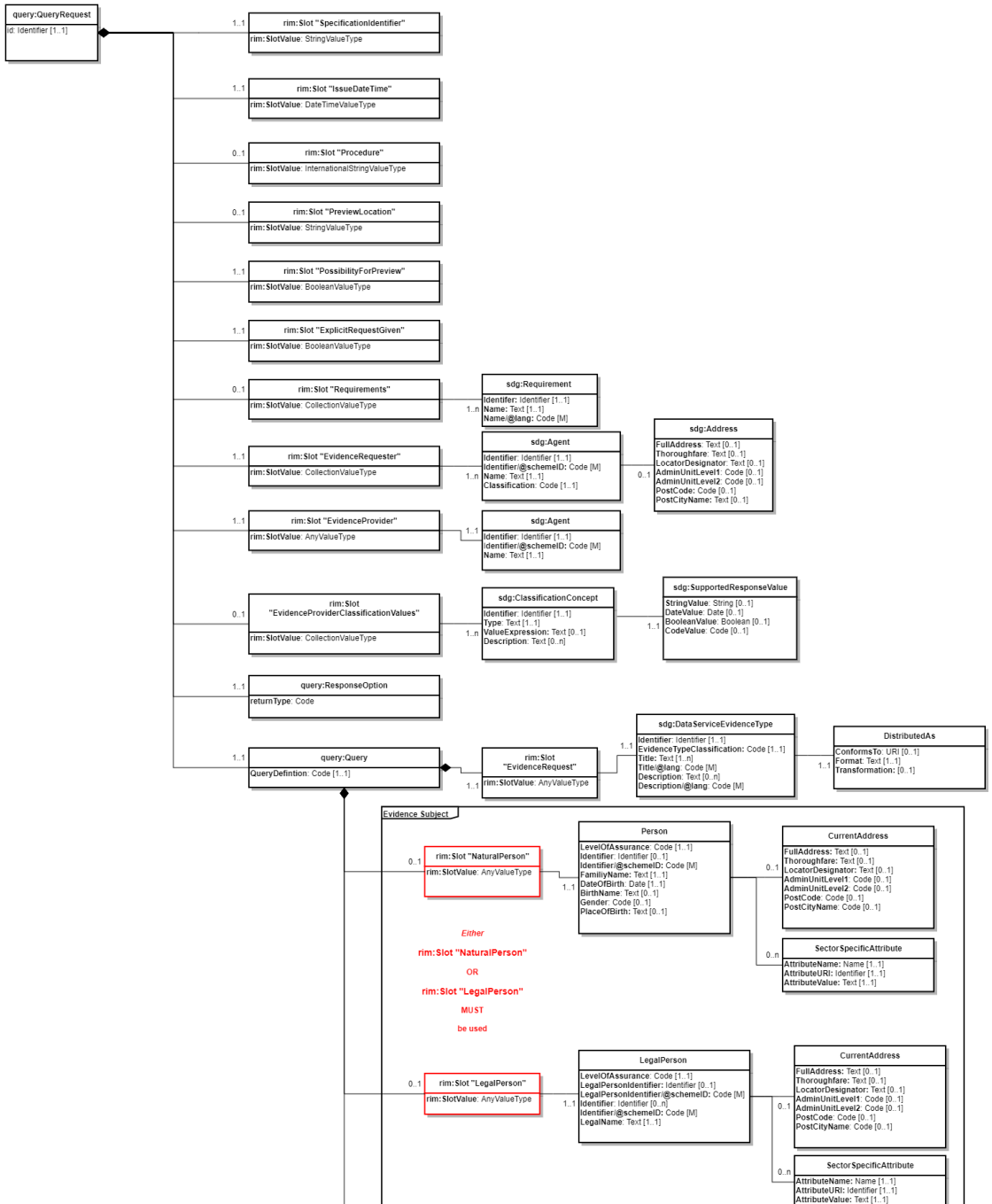
- Exchange Data Model: QueryRequest (Evidence Request)
- ebRIM Definitions of the QueryRequest (Evidence Request)
    - ebRIM QueryRequest example
    - Specification Identifier example
    - Issue Date and Time example
    - Procedure example
    - Preview Location example
    - PossibilityForPreview example
    - Explicit Request Given example
- SDGR Application Profile for the ebRIM QueryRequest (Evidence Request)
    - Requirements slot and example
    - Evidence Requester slot and example

- Evidence Provider slot and example
- Evidence Provider Classification Values slot and example
- Evidence Request slot and example
- Evidence Subject and Authorized Representative slots and example
  - Natural Person slot and example
  - Legal Person slot and example
  - Authorized Representative slot and example

4.5.2.1 Exchange Data Model: QueryRequest (Evidence Request)

This guideline explains how to use the ebRS QueryRequest syntax to implement the Business Requirements (Req ID) described for the Evidence Request. The guideline provides specific details for each class and information element including the underlying standards, data types and cardinalities to produce conformant XML documents. In the following sections, we describe the XML serialization of the Evidence Request in the same hierarchical order of the corresponding Exchange Data Model.

The Exchange Data Model in the figure below provides an overview of the information elements and their associations contained in the Evidence Request. An Evidence Request is a message created by the Evidence Requester (ER) containing all the necessary parameters for requesting evidences.


query:QueryRequest
Id: Identifier [1..1]
rim:Slot "SpecificationIdentifier"
rim:SlotValue: StringValueType
rim:Slot "IssueDateTime"
rim:SlotValue: DateTimeValueType
rim:Slot "Procedure"
rim:SlotValue: InternationalStringValueType
rim:Slot "PreviewLocation"
rim:SlotValue: StringValueType
rim:Slot "PossibilityForPreview"
rim:SlotValue: BooleanValueType
rim:Slot "ExplicitRequestGiven"
rim:SlotValue: BooleanValueType
rim:Slot "Requirements"
rim:SlotValue: CollectionValueType
sdg:Requirement
Identifier: Identifier [1..1]
Name: Text [1..1]
Name/@lang: Code [M]
rim:Slot "EvidenceRequester"
rim:SlotValue: CollectionValueType
sdg:Agent
Identifier: Identifier [1..1]
Identifier/@schemeID: Code [M]
Name: Text [1..1]
Classification: Code [1..1]
sdg:Address
FullAddress: Text [0..1]
Thoroughfare: Text [0..1]
LocatorDesignator: Text [0..1]
AdminUnitLevel1: Code [0..1]
AdminUnitLevel2: Code [0..1]
PostCode: Code [0..1]
PostCityName: Text [0..1]
rim:Slot "EvidenceProvider"
rim:SlotValue: AnyValueType
sdg:Agent
Identifier: Identifier [1..1]
Identifier/@schemeID: Code [M]
Name: Text [1..1]
rim:Slot "EvidenceProviderClassificationValues"
rim:SlotValue: CollectionValueType
sdg:ClassificationConcept
Identifier: Identifier [1..1]
Type: Text [1..1]
ValueExpression: Text [0..1]
Description: Text [0..n]
sdg:SupportedResponseValue
StringValue: String [0..1]
DateValue: Date [0..1]
BooleanValue: Boolean [0..1]
CodeValue: Code [0..1]
query:ResponseOption
returnType: Code
query:Query
QueryDefintion: Code [1..1]
rim:Slot "EvidenceRequest"
rim:SlotValue: AnyValueType
sdg:DataServiceEvidenceType
Identifier: Identifier [1..1]
EvidenceTypeClassification: Code [1..1]
Title: Text [1..n]
Title/@lang: Code [M]
Description: Text [0..n]
Description/@lang: Code [M]
DistributedAs
ConformsTo: URI [0..1]
Format: Text [1..1]
Transformation: [0..1]
Evidence Subject
rim:Slot "NaturalPerson"
rim:SlotValue: AnyValueType
Person
LevelOfAssurance: Code [1..1]
Identifier: Identifier [0..1]
Identifier/@schemeID: Code [M]
FamilyName: Text [1..1]
DateOfBirth: Date [1..1]
BirthName: Text [0..1]
Gender: Code [0..1]
PlaceOfBirth: Text [0..1]
CurrentAddress
FullAddress: Text [0..1]
Thoroughfare: Text [0..1]
LocatorDesignator: Text [0..1]
AdminUnitLevel1: Code [0..1]
AdminUnitLevel2: Code [0..1]
PostCode: Code [0..1]
PostCityName: Code [0..1]
SectorSpecificAttribute
AttributeName: Name [1..1]
AttributeURI: Identifier [1..1]
AttributeValue: Text [1..1]
Either
rim:Slot "NaturalPerson"
OR
rim:Slot "LegalPerson"
MUST
be used
rim:Slot "LegalPerson"
rim:SlotValue: AnyValueType
LegalPerson
LevelOfAssurance: Code [1..1]
LegalPersonIdentifier: Identifier [0..1]
LegalPersonIdentifier/@schemeID: Code [M]
Identifier: Identifier [0..n]
Identifier/@schemeID: Code [M]
LegalName: Text [1..1]
CurrentAddress
FullAddress: Text [0..1]
Thoroughfare: Text [0..1]
LocatorDesignator: Text [0..1]
AdminUnitLevel1: Code [0..1]
AdminUnitLevel2: Code [0..1]
PostCode: Code [0..1]
PostCityName: Code [0..1]
SectorSpecificAttribute
AttributeName: Name [1..1]
AttributeURI: Identifier [1..1]
AttributeValue: Text [1..1]

To form a valid QueryRequest (Evidence Request), at least the following elements are required:

- the "id" of the QueryRequest;
- the "SpecificationIdentifier" to identify the version of this specification. Please use the value "oots-edm:v1.0";
- the "IssueDateTime" to describe the time of the request;
- the "PossibilityForPreview" to declare the intention of the Evidence Requester to allow the user to preview the Evidence to be received from the Evidence Provider;
- the "ExplicitRequestGiven" to indicate the user consent to request the evidence;
- the "EvidenceRequester" to identify the one or more entities that are technically executing the request on behalf of the User;
- the "EvidenceProvider" to identify the entity that the Evidence Request is sent to;
- the "queryResponse" option "LeafClassWithRepositoryItem".
- the "queryDefinition" expressed through the information entity "DataServiceEvidenceType" in the "EvidenceRequest" slot, which is used to form the "DocumentQuery".
- the highlighted information entities "LegalPerson" and "NaturalPerson" to identify the Evidence Subject (or User) for which the query is done. The business rules do not permit the use of both information entities at the same time;

4.5.2.2 ebRIM Definitions of the QueryRequest (Evidence Request)

This section defines the core ebRIM elements that are used to compose a Query Request (Evidence Request). It thereby distinguishes between attributes and slots to define the Evidence Request:

Attribute Definition: The table provides an overview of the mandatory attributes and the information they contain for each QueryRequest according to ebRIM.

Slot definition: The elements provide an overview about the defined ebRIM SlotType instances, which have a name and a value. The value is of type ValueType. Most rim:Slots do not contain sub-properties other than the SlotValue itself, except if they are collections. Collections refer to other sources of information such as Core Vocabularies and a corresponding class defined in the SDGR Application Profile (see section 3).

Legend
The tables below represent the tree structure of the EDM. Light grey rows open classes and define ther properties and attributes. Light green rows soley illustrate the classes that are subordinated to a class and illustrate the tree structure. Light green rows are then repeated as light grey rows to describe properties and attributes of the class. The hierarchy of the tree structure is also indicated in the first column via the '+' symbol.

	Name	Definition	Cardinality	ebRIM type	Data Type	BusinessRules	Mapping to class of SDGR Application Profile	Mapping to Core Vocabulary
	query:QueryRequest	**Evidence Request root element**		ComplexType		Structure: BR-OOTS-REQ-ebRIM-014		
+	id	The unique identifier of the Evidence Request.	1..1	Attribute	Identifier	Use: BR-OOTS-REQ-001		
++	SpecificationIdentifier	An identification of the specification for the Evidence Request containing the total set of rules regarding semantic content, cardinalities and business rules to which the data contained in the instance document conforms.	1..1	SlotType	StringValueType	Structure: BR-OOTS-REQ-ebRIM-001, BR-OOTS-REQ-ebRIM-015, Use: BR-OOTS-REQ-002	-	-
++	IssueDateTime	The issue date and time when the request is issued. The issue date time must have a granularity of seconds	1..1	SlotType	DateTimeValueType	Structure: BR-OOTS-REQ-ebRIM-002, BR-OOTS-REQ-ebRIM-016,	-	-

	Name	Definition	Cardinality	ebRIM type	Data Type	BusinessRules	Mapping to class of SDGR Application Profile	Mapping to Core Vocabulary
		and include time zone information.				Use: BR-OOTS-REQ-003		
++	Procedure	A definition of the procedure which defines the context under which a QueryRequest was initiated.	0..1	SlotType	InternationalStringValueType	Structure: BR-OOTS-REQ-ebRIM-003, BR-OOTS-REQ-ebRIM-017, Use: BR-OOTS-REQ-004, BR-OOTS-REQ-005	-	-
++	PreviewLocation	The URL of the server on which the Preview Space is available for preview related to the Evidence Request.	0..1	SlotType	StringValueType	Structure: BR-OOTS-REQ-ebRIM-004, BR-OOTS-REQ-ebRIM-018, Use: BR-OOTS-REQ-006 Note: Must not be present in the first	-	-

	Name	Definition	Cardinality	ebRIM type	Data Type	BusinessRules	Mapping to class of SDGR Application Profile	Mapping to Core Vocabulary
						request. Must be present in the second request. The presence and absence of the Slot are described in 4.9 - Evidence Preview - June 2022.		
++	PossibilityForPreview	Element to declare the intention of the Evidence Requester to allow the user to preview the Evidence to be received from the Evidence Provider.	1..1	SlotType	BooleanValueType	Structure: BR-OOTS-REQ-ebRIM-005, BR-OOTS-REQ-ebRIM-019, Use: BR-OOTS-REQ-007 Note: "true" or 1 representing "Yes" affirmative answers; "false" or 0	-	-

	Name	Definition	Cardinality	ebRIM type	Data Type	BusinessRules	Mapping to class of SDGR Application Profile	Mapping to Core Vocabulary
						representing "No" negative answers		
++	ExplicitRequestGiven	Element to declare that the Evidence Requester has received the user's explicit consent to request the evidence from the specific Evidence Provider.	1..1	SlotType	BooleanValueType	Structure: BR-OOTS-REQ-ebRIM-006, BR-OOTS-REQ-ebRIM-020, Use: BR-OOTS-REQ-008 Note: "true" or 1 representing "Yes" affirmative answers; "false" or 0 representing "No" negative answers	-	-
++	Requirement	A requirement is a named set of requests for information that may be made for making a judgment or	0..1	SlotType	CollectionValueType	Structure: BR-OOTS-REQ-ebRIM-007, BR-OOTS-REQ-	Requirement	Core Criterion and Core Evidence

	Name	Definition	Cardinality	ebRIM type	Data Type	BusinessRules	Mapping to class of SDGR Application Profile	Mapping to Core Vocabulary
		decision, see draft implementing act.				ebRIM-021, BR-OOTS-REQ-ebRIM-030, BR-OOTS-REQ-ebRIM-031, BR-OOTS-REQ-ebRIM-022		Vocabulary
++	EvidenceRequester	The Agent or organisation that is requesting the evidence.	1..n	SlotType	CollectionValueType	Structure: BR-OOTS-REQ-ebRIM-008, BR-OOTS-REQ-ebRIM-023, BR-OOTS-REQ-ebRIM-032, BR-OOTS-REQ-ebRIM-033, BR-OOTS-REQ-ebRIM-024	Agent	Core Public Service Vocabulary Application Profile
++	EvidenceProvider	The Agent or organisation that operates the data service providing the evidence.	1..1	SlotType	AnyValueType	Structure: BR-OOTS-REQ-ebRIM-009, BR-OOTS-REQ-ebRIM-034, BR-OOTS-	Agent	Core Public Service Vocabulary

	Name	Definition	Cardinality	ebRIM type	Data Type	BusinessRules	Mapping to class of SDGR Application Profile	Mapping to Core Vocabulary
						REQ-ebRIM-035, BR-OOTS-REQ-ebRIM-025		Application Profile
++	EvidenceProviderClassificationValues	The Classification Values that were selected by the User for the Evidence Provider Discovery	0..n	SlotType	CollectionValueType	Structure: BR-OOTS-REQ-ebRIM-042, BR-OOTS-REQ-ebRIM-043, BR-OOTS-REQ-ebRIM-044	EvidenceProviderClassification	SDGR Application Profile
++	**query:ResponseOption**	**Element to control the type and structure of results within the corresponding QueryResponse.**		ComplexType				
+++	returnType	Specifies whether the RegistryObjects returned should include composed objects. Fixed value: "LeafClassWithRepositoryItem"	1..1	Attribute	Code	Use: BR-OOTS-REQ-022	-	-
++	**query:Query**	**Element to specify the parametrized query as**		ComplexType				

	Name	Definition	Cardinality	ebRIM type	Data Type	BusinessRules	Mapping to class of SDGR Application Profile	Mapping to Core Vocabulary
		well as the values for its parameters.						
+++	queryDefinition	Used to control the parameterized query. Fixed value "DocumentQuery"	1..1	Attribute	Code	Use: BR-OOTS-REQ-023	-	-
+++	EvidenceRequest	A request for a piece of evidence to the data service of an Evidence Provider.	1..1	SlotType	AnyValueType	Struture: BR-OOTS-REQ-ebRIM-010, BR-OOTS-REQ-ebRIM-036, BR-OOTS-REQ-ebRIM-037, BR-OOTS-REQ-ebRIM-026	DataServiceEvidenceType	DCAT Application Profile
+++	LegalPerson	The Evidence Subject, being a natural person, whose evidence is requested from the Data Service.	0..1	SlotType	AnyValueType	Struture: BR-OOTS-REQ-ebRIM-011, BR-OOTS-REQ-ebRIM-039, BR-OOTS-REQ-ebRIM-027	LegalPerson	Core Business
+++	NaturalPerson	The Evidence Subject, being a legal person,	0..1	SlotType	AnyValueType	Struture: BR-OOTS-	Person	Core Person

	Name	Definition	Cardinality	ebRIM type	Data Type	BusinessRules	Mapping to class of SDGR Application Profile	Mapping to Core Vocabulary
		whose evidence is requested from the Data Service.				REQ-ebRIM-012, BR-OOTS-REQ-ebRIM-038, BR-OOTS-REQ-ebRIM-028		
+++	AuthorizedRepresentative	The representative of the Evidence Subject who makes the Evidence Request on their behalf.	0..1	SlotType	AnyValueType	Struture: BR-OOTS-REQ-ebRIM-013, BR-OOTS-REQ-ebRIM-040, BR-OOTS-REQ-ebRIM-029	Person	Core Person

4.5.2.2.1 ebRIM QueryRequest example

The Evidence Request is syntactically expressed using the ebRS QueryRequest, as shown in the example below.

The element "id" is used to assign a unique identifier to the Evidence Request.

The element "ResponseOption" is used to control the type and structure of results within the corresponding QueryResponse. It specifies whether the RegistryObjects returned should include composed objects. Must be fixed value "LeafClassWithRepositoryItem" to ensure that the response include the RepositoryItems, if any, for every rim:RegistryObject in the rim:RegistryObjectList element of the QueryResponse.

In order to specify a Query, the ebXML Element Query is used. The attribute queryDefinition can be used to specify the type of Query to be done. The value of this attribute must come from the appropriate codelist. The value of the queryDefinition attribute in the Query element must always be "DocumentQuery" when requesting Document Evidence.

```
<?xml version="1.0" encoding="UTF-8"?>
<query:QueryRequest xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns:rs="urn:oasis:names:tc:ebxml-regrep:xsd:rs:4.0"
    xmlns:sdg="http://data.europa.eu/p4s"
    xmlns:xmime="http://www.w3.org/2005/05/xmlmime"
    xmlns:rim="urn:oasis:names:tc:ebxml-regrep:xsd:rim:4.0"
    xmlns:query="urn:oasis:names:tc:ebxml-regrep:xsd:query:4.0"
    xmlns:xlink="http://www.w3.org/1999/xlink"
    id="c4369c4d-740e-4b64-80f0-7b209a66d629">

    <!-- Slots are omitted for clarity -->

    <!-- Default Response Option -->
    <query:ResponseOption returnType="LeafClassWithRepositoryItem"/>

    <!-- Query Definition -->
    <query:Query queryDefinition="DocumentQuery">

    <!-- Further slots are omitted for clarity. -->

    </query:Query>
</query:QueryRequest>
```

4.5.2.2.2 Specification Identifier example

The SpecificationIdentifier slot is used for expressing the version of the specification used for creating the referred message. A Slot with the name "SpecificationIdentifier" is used with the ValueType of StringValueType. In this version of the design documentation, this MUST be set to the value “oots-edm:v1.0”

```
<!-- SpecificationIdentifier Slot -->
    <rim:Slot name="SpecificationIdentifier">
        <rim:SlotValue xsi:type="rim:StringValueType">
            <rim:Value>oots-edm:v1.0</rim:Value>
        </rim:SlotValue>
    </rim:Slot>
```

4.5.2.2.3 Issue Date and Time example

The IssueDateTime slot is used for expressing the creation date and time of the referred document.

A Slot with the name "IssueDateTime" is used with the ValueType of DateTimeValueType which has an ISO timestamp value.

```
   <!-- IssueDateTime Slot -->
    <rim:Slot name="IssueDateTime">
        <rim:SlotValue xsi:type="rim:DateTimeValueType">
            <rim:Value>2021-02-14T19:20:30+01:00</rim:Value>
        </rim:SlotValue>
    </rim:Slot>
```

4.5.2.2.4 Procedure example

A slot with the name Procedure and ValueType of InternationalStringValueType is used to represent the information contained in one or more local languages and has a sequence of LocalizedString instances. Each LocalizedString instance is specific to a particular locale. The language must be specified using ISO 639-1 two-letter code. The value represents the procedure under which the Evidence Requester requests the specific evidence.

```
<!-- Procedure SLOT -->
<rim:Slot name="Procedure">
    <rim:SlotValue xsi:type="rim:InternationalStringValueType">
        <rim:Value>
            <rim:LocalizedString
                value="Requesting a birth certificate"
                xml:lang="en"/>
        </rim:Value>
    </rim:SlotValue>
</rim:Slot>
```

4.5.2.2.5 Preview Location example

The PreviewLocation element is used for expressing the location of the Preview Space for the Evidence Request.

A Slot with the name of "PreviewLocation" is used with the ValueType of StringValueType which has the value of a URI.

```
   <!-- PreviewLocation Slot -->
    <rim:Slot name="PreviewLocation">
        <rim:SlotValue xsi:type="rim:StringValueType">
            <rim:Value>https://preview.space.example.com/requests/d36af8bc-fea6-4ee5-a32d-5bef82cdb071</rim:Value>
        </rim:SlotValue>
    </rim:Slot>
```

4.5.2.2.6 PossibilityForPreview example

The `PossibilityForPreview` is the slot used to declare the intention of the Evidence Requester to allow the user to preview the Evidence to be received from the Evidence Provider. When its value is `true`, then the user will be able to preview, if desired, the provided evidence. When its value is `false`, then the user will not be able to preview the evidence to be received. The flag is set by the ER, when such an exemption is required for the execution of the specific procedure. The following example depicts the use of the slot.

```
<!-- PossibilityForPreview Slot  -->
 <rim:Slot name="PossibilityForPreview">
     <rim:SlotValue xsi:type="rim:BooleanValueType">
         <rim:Value>true</rim:Value>
     </rim:SlotValue>
 </rim:Slot>
```

4.5.2.2.7 Explicit Request Given example

The `ExplicitRequestGiven` is the slot used to declare that the Evidence Requester has received the user's explicit confirmation to request the evidence from the specific Evidence Provider. When its value is `true`, then the user has provided his explicit request, while when its value is `false`, then the user has not provided his explicit confirmation to request the evidence. The flag is set by the ER, when such an exemption is required for the execution of the specific procedure. The following example depicts the use of the slot.

```
<!-- ExplicitRequestGiven Slot  -->
 <rim:Slot name="ExplicitRequestGiven">
     <rim:SlotValue xsi:type="rim:BooleanValueType">
         <rim:Value>true</rim:Value>
     </rim:SlotValue>
 </rim:Slot>
```

4.5.2.3 SDGR Application Profile for the ebRIM QueryRequest (Evidence Request)

The SDGR application profile for the Evidence Request defines the semantics of the previously introduced rim:Slots defined as a collection (green components) of the Evidence Request Message. The SDGR application profile for the Evidence Request describes how the SDG XML Schema is profiled in ebRIM in order to compose a valid QueryRequest. It therefore contains a mapping to the underlying SDG-syntax elements and the necessary parameters for requesting evidences based on information retrieved from eIDAS, the Evidence Broker and the Data Service Directory. Thus, the values for several parameters are obtained from the queries made to eIDAS, the Evidence Broker and the Data Service Directory in order to initiate the Query Request. The namespace of the SDG-syntax is http://data.europa.eu/p4s. In the following samples, the prefix "sdg" is assumed to be linked to the namespace http://data.europa.eu/p4s.

4.5.2.3.1 Requirements slot and example

The requirement in the Evidence Request is contextual information that can be used to perform logging in compliance with the regulatory framework of the SDGR. It is not (yet) expected to be required to determine the evidence for the evidence subject. The value is obtained by the Evidence Requester from the Evidence Broker while executing an SDG procedure.

	Name	Definition	Cardinality	Type	BusinessRules	Core Vocabulary	Notes
	Requirement	A requirement is a named set of requests for information that may be made for making a judgment or decision, see draft implementing act.	1..n	Requirement		cccev:Requirement	Core Criterion and Core Evidence Vocabulary
+	Identifier	The identifier for the requirement.	1..1	Identifier	BR-OOTS-REQ-009	cccev:identifier	CCCEV
+	Name	The name of the requirement	1..1	Text		cccev:name	CCCEV
++	Name/@lang	The language of the name encoded as ISO 639-1 two-letter code. Default value "en"	M	Code	BR-OOTS-REQ-010, BR-OOTS-REQ-011	cccev:name	CCCEV

A slot with the name Requirement and ValueType of CollectionValueType is used by the Evidence Requester to provide the Requirements that will be proven using the requested evidence. It is represented as a list of `Requirement` elements, expressed using the CCCEV 2.0 Vocabulary and typically extracted from the Evidence Broker.

```
 <!-- Requirements Slot  -->
<rim:Slot name="Requirements">
    <rim:SlotValue xsi:type="rim:CollectionValueType" collectionType="urn:oasis:names:tc:ebxml-regrep:CollectionType:Set">
        <rim:Element xsi:type="rim:AnyValueType">
            <sdg:Requirement>
                <!--  cccev requirement -->
                <Identifier>315cfd75-6605-49c4-b0fe-799833b41099</Identifier>
                <Name lang="en">Proof of Birth</Name>
            </sdg:Requirement>
        </rim:Element>

            <!--  another cccev requirement may be added as rim:Element-->

    </rim:SlotValue>
</rim:Slot>
```

4.5.2.3.2 Evidence Requester slot and example

The Evidence Requester element is used to describe an organisation that requests data or documents from Evidence Providers. The agent requests the evidence, by sending an Evidence Request to the Evidence Provider, on behalf of the evidence subject. In several cases it might be a portal/organisation or intermediary that initiates the evidence request. If there are multiple agents involved, they can be classified. No central registry of Evidence Requesters is required, only the minimal details required to enable legal logging of requests or facilitate the processing of the evidence request.

	Name	Definition	Cardinality	Type	BusinessRules	Core Vocabulary	Notes
	Agent	The Agent or organisation that is requesting the evidence.	1..n	Agent		dct:Agent	Core Public Service Vocabulary Application Profile
+	Identifier	A unique identification for the agent.	1..1	Identifier		dct:identifier	
++	Identifier/@schemeID	Scheme identifier for the agent identification	M	Code	BR-OOTS-REQ-012, BR-OOTS-REQ-013	dct:identifier	
+	Name	A short label for the agent.	1..1	Text		dct:title	

	Name	Definition	Cardinality	Type	BusinessRules	Core Vocabulary	Notes
+	Address	A location of the Evidence Requester in the form of an address.	0..1	Address		locn:Address	Core Location Vocabulary
+	Classification	A code to classify the agents associated to the communication. In case there are multiple agents the codes must be used to distinguish between the actual Evidence Requester and Intermediary Platforms that are involved in the transaction. Default value: Evidence Requester	1..1	Code	BR-OOTS-REQ-014, BR-OOTS-REQ-015	cv:role	
++	Address	A location of the Evidence Requester in the form of an address.		Address		locn:Address	Core Location Vocabulary
+++	FullAddress	The complete address written as a string.	0..1	Text		locn:fullAddress	
+++	Thoroughfare	The name of a street, passage or way through from one location to another.	0..1	Text		locn:thoroughfare	
+++	LocatorDesignator	A number or sequence of characters that uniquely identifies the locator (building number, apartment number, etc.) within the relevant scope.	0..1	Text		locn:locatorDesignator	
+++	AdminUnitLevel1	The name of the uppermost level of the address, almost always a country.	0..1	Code	BR-OOTS-REQ-016	locn:adminUnitL1	
+++	AdminUnitLevel2	The name of a secondary level/region of the address, usually a county, state or other such area that typically encompasses several localities.	0..1	Code	BR-OOTS-REQ-017	locn:adminUnitL2	
+++	PostCode	The code created and maintained for postal purposes to identify a subdivision of addresses and postal delivery points.	0..1	Code		locn:postCode	

	Name	Definition	Cardinality	Type	BusinessRules	Core Vocabulary	Notes
+++	PostCityName	The key postal division of the address, usually the city.	0..1	Code		locn:postName	

A Slot with the name of "EvidenceRequester" is used with the ValueType of CollectionValueType which is a container for a collection of values. It may be used to represent a SlotValue that is a collection of values where each value is represented by a AnyValueType instance which accepts any xml representation. In this particular case, the Agent class is used for the expression of the Evidence Requester information inside the AnyValueType Slot and more specifically the Agent Class. The CollectionValueType Slot as a container can hold information about EvidenceRequester and Intermediaries.

```
<!-- EvidenceRequester Slot  -->
<rim:Slot name="EvidenceRequester">
        <rim:SlotValue xsi:type="rim:CollectionValueType">
            <rim:Element xsi:type="rim:AnyValueType">
                <sdg:Agent>
                    <sdg:Identifier schemeID="0096">DK22233223</sdg:Identifier>
                    <sdg:Name lang="en">Denmark University Portal</sdg:Name>
                    <sdg:Address>
                        <sdg:FullAddress>Prince Street 15</sdg:FullAddress>
                        <sdg:LocatorDesignator>15</sdg:LocatorDesignator>
                        <sdg:PostCode>1050</sdg:PostCode>
                        <sdg:PostCityName>Copenhagen</sdg:PostCityName>
                        <sdg:AdminUnitLevel1>Denmark</sdg:AdminUnitLevel1>
                        <sdg:AdminUnitLevel2>DK011</sdg:AdminUnitLevel2>
                    </sdg:Address>
                    <sdg:Classification>IntermediaryPlatform</sdg:Classification>
                </sdg:Agent>
            </rim:Element>
        </rim:SlotValue>
    </rim:Slot>lue>
</rim:Slot>
```

4.5.2.3.3 Evidence Provider slot and example

The Evidence Provider element is used to describe an organisation that receives the Evidence Request from the Evidence Requester. In most cases, the agent is a public organisation, however in some MSs, for some evidence types, businesses have been accredited to supply them.

An evidence provider must be registered in the Data Service Directory in order to be activated in the SDG OOTS.

	Name	Definition	Cardinality	Type	BusinessRules	Core Vocabulary	Notes
	Agent	The Agent or organisation that is providing the evidence.	1..1	Agent		dct:Agent	Core Public Service Vocabulary Application Profile
+	Identifier	A unique identification for the agent.	1..1	Identifier		dct:identifier	
++	Identifier/@schemeID	Scheme identifier for the agent identification	M	Code	BR-OOTS-REQ-018, BR-OOTS-REQ-019	dct:identifier	
+	Name	A short label for the agent.	1..1	Text		dct:title	

A Slot with the name of "EvidenceProvider" is used with the ValueType of AnyValueType which accepts any xml representation. In this particular case, the Agent class is used for the expression of the Evidence Provider information inside the AnyValueType Slot and more specifically the Agent Class.

```
<!-- EvidenceProvider Slot  -->
<rim:Slot name="EvidenceProvider">
        <rim:SlotValue xsi:type="rim:AnyValueType">
            <sdg:Agent>
                <sdg:Identifier schemeID="9930">DE73524311</sdg:Identifier>
                <sdg:Name>Civil Registration Office Berlin I</sdg:Name>
            </sdg:Agent>
        </rim:SlotValue>
    </rim:Slot>
```

4.5.2.3.4 Evidence Provider Classification Values slot and example

The Evidence Provider Classification Values are used to collect the required information selected by the user during the Data Services Directory queries for the proper discovery of the Evidence Provider.

	Name	Definition	Cardinality	Type	BusinessRules	Core Vocabulary	Notes
+	**EvidenceProviderClassification**	A Classification Concept is a structured piece of information that is used to provide the supported values required for evidence discovery along the definition of the Data Service Evidence Type	0..n	InformationConcept		cccev:InformationConcept	Core Criterion Core Evidence Vocabulary
+	Identifier	Unambiguous reference to the Information Concept.	1..1	Identifier		cccev:identifier	CCCEV
+	Type	Category to which the Information Concept belongs.	1..1	Code		cccev:type	CCCEV
+	ValueExpression	Formulation in a formal language of the expected value(s) for the Classification Concept which is aligned with the concepts from the Requirements defined and must be respected by the supplied Supported Values. Currently only Regular Expression is supported.	0..1	Text		cccev:expressionOfExpectedValue	CCCEV
+	Description	Short explanation supporting the	1..n	Text		cccev:description	CCCEV

	Name	Definition	Cardinality	Type	BusinessRules	Core Vocabulary	Notes
		understanding of the Classification Concept.					
++	Description/@lang	The language of the description encoded as ISO 639-1 two-letter code. Default value "en"	M	Code	BR-OOTS-REQ-020, BR-OOTS-REQ-021	cccev:description	CCCEV
++	SupportedValue	The value that is supported by the response	1..1	SupportedValue			XML Schema
++	SupportedValue	The value that is supported by the response	1..1	SupportedValue			XML Schema
+++	StringValue	Textual field	0..1	String	Value MUST be xs:string	XML Schema data types	XML
+++	DateValue	Date values (format YYYY-DD-MM)	0..1	Date	Value MUST be xs:date	XML Schema data types	XML
+++	BooleanValue	"true" or 1 representing "Yes" affirmative answers "false" or 0 representing "No" negative answers	0..1	Boolean	Value MUST be xs:boolean	XML Schema data types	XML
+++	CodeValue	A code for a concept.	0..1	Code		XML Schema data types	XML
+++	DateTimeValue	Date values that include a time (format	0..1	DateTime	Value MUST be xs:dateTime	XML Schema data types	XML

	Name	Definition	Cardinality	Type	BusinessRules	Core Vocabulary	Notes
		YYYY-DD-MM hh:mm:ss zzzzzz)					
+++	Identifier	An identifier of a concept, including a schemeID	0..1	Identifier		XML Schema data types	XML
+++	URI	A URI, including e-mail addresses	0..1	anyURI	Value MUST be xs:anyURI	XML Schema data types	XML
+++	Duration	A duration expressed as Year, Month, Day, Hour and Minutes (format PnYn MnDTnH nMnS)	0..1	Duration	Value MUST be xs:duaration	XML Schema data types	XML
+++	Decimal	A number represented with decimal notation	0..1	Decimal	Value MUST be xs:decimal	XML Schema data types	XML
+++	Amount	An Amount, and currency, as defined in UN/CEFACT's CCTS	0..1	Amount		XML Schema data types	XML

The ClassificationConcept class is used for the expression of these values inside the AnyValueType slot.

```
<!-- EvidenceProviderClassificationValues Slot  -->
<rim:Slot name="EvidenceProviderClassificationValues">
    <rim:SlotValue xsi:type="rim:CollectionValueType">

        <!-- Classification Information - Used for finding the evidence -->
        <rim:Element xsi:type="rim:AnyValueType">
            <sdg:EvidenceProviderClassification>
                <sdg:Identifier>SecondarySchool</sdg:Identifier>
                <sdg:SupportedValue>
                    <sdg:StringValue>Wilhelm Gymnasium</sdg:StringValue>
                </sdg:SupportedValue>
            </sdg:EvidenceProviderClassification>
        </rim:Element>

        <!-- Classification Information - Used for finding the evidence -->
        <rim:Element xsi:type="rim:AnyValueType">
            <sdg:EvidenceProviderClassification>
                <sdg:Identifier>YearOfGraduation</sdg:Identifier>
                <sdg:SupportedValue>
                    <sdg:StringValue>1988</sdg:StringValue>
                </sdg:SupportedValue>
            </sdg:EvidenceProviderClassification>
        </rim:Element>
    </rim:SlotValue>
</rim:Slot>
```

4.5.2.3.5 Evidence Request slot and example

Element to request for a piece of evidence to the Data Service of an Evidence Provider. The elements provide a complete semantic description required to point to the correct evidence type and format.

	Name	Definition	Cardinality	Type	BusinessRules	Core Vocabulary	Notes
	DataServiceEvidenceType	Provides the semantic information and requirements for retrieving	1..1	DataServiceEvidenceType		dcat:Dataset	DCAT Application Profile

	Name	Definition	Cardinality	Type	BusinessRules	Core Vocabulary	Notes
		an evidence type from a Data Service.					
+	Identifier	The Identifier, provided by the Data Services to uniquely identify an Evidence Type.	1..1	Identifier	BR-OOTS-REQ-024	dcat:identifier	It is assumed that every data service implementation is aware of the identifiers that are used to describe the evidence types in the Data Service Directory.
+	EvidenceTypeClassification	An URI pointing to the Evidence Type that this Data Service is supporting. The classification is linking with the Evidence Type of the Semantic Repository (Evidence Broker).	1..1	Code	BR-OOTS-REQ-025	cccev:evidenceTypeClassification	Core Criterion Core Evidence Vocabulary
+	Title	A name to identify in	1..n	Text		dct:title	

	Name	Definition	Cardinality	Type	BusinessRules	Core Vocabulary	Notes
		common language the Evidence Type. Unbounded cardinality to support multiple languages.					
++	Title/@lang	The language of the title encoded as ISO 639-1 two-letter code. Default value "en"	M	Code	BR-OOTS-REQ-026, BR-OOTS-REQ-027	dct:title	
+	Description	A description of the Evidence Type. Unbounded cardinality to support multiple languages.	0..n	Text		dct:description	
++	Description/@lang	The language of the description encoded as ISO 639-1 two-letter code.	M	Code	BR-OOTS-REQ-028, BR-OOTS-REQ-029	dct:description	

	Name	Definition	Cardinality	Type	BusinessRules	Core Vocabulary	Notes
		Default value "en"					
+	DistributedAs	The kind of distributions that are expected as response to this request.	1..1	EvidenceTypeDistribution		dcat:distribution	
++	DistributedAs	A description of the format and the semantic and syntactic conformance, under which the Evidence Type can be distributed.	1..1	EvidenceTypeDistribution	BR-OOTS-REQ-030	dcat:distribution	Each distribution describes a format and scheme in which the evidence type can be provided. The allowed schemes are expressed in the Data Service Directory. Thus, only distributions which the data service is able to provide can be requested.
+++	Format	The technical representation of the	1..1	Code	BR-OOTS-REQ-031	dct:format	

	Name	Definition	Cardinality	Type	BusinessRules	Core Vocabulary	Notes
		evidence. Declaration of the file types that provide structured content like PDF, XML, JSON, RDF etc					
+++	ConformsTo	A registered schema or conformance profile in the OOTS semantic repository to which the described Distribution conforms.	0..1	URI	BR-OOTS-REQ-032	dct:conformsTo	The element's value is a persistent URL, pointing to an entry of the OOTS Semantic Repository that contains all the relevant information of such a profile.
+++	Transformation	The element points to a known and structured evidence type subset that would suffice the request. Evidence type subsets fulfil the principle of data	0..1	URI	BR-OOTS-REQ-033	dct:conformsTo	

	Name	Definition	Cardinality	Type	BusinessRules	Core Vocabulary	Notes
		minimization and can limit the collection to those information required for the execution of a procedure.					

The EvidenceRequest Slot has a SlotValue of type AnyValueType. It contains a **DataServiceEvidenceType**, containing one Distribution class as defined by the SDG AP. This class must specify the Identifier of the Evidence type requested together with one distribution containing the format and the conformance profile requested when applicable (e.g. when evidence is structured), as it comes from the Data Services Directory.

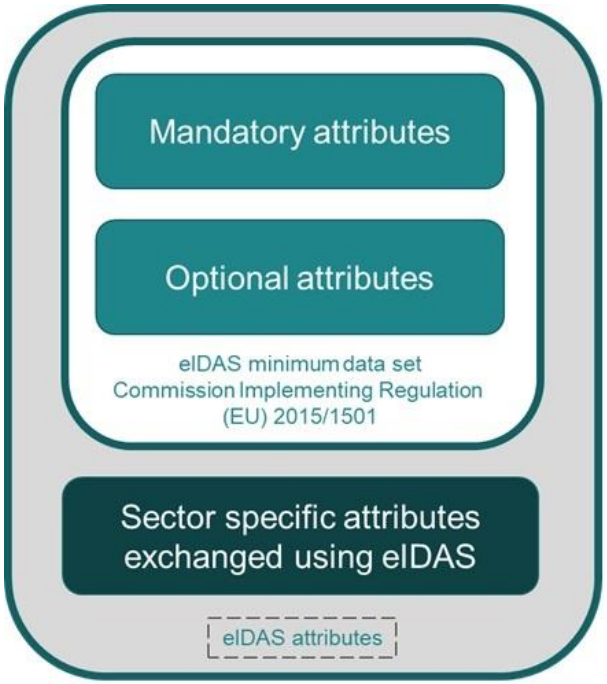
Optionally, the requester may indicate that a specific identified transformation is to be applied to the evidence by the Data Service. The format of a transformation identifier must be a URI. The transformation itself is defined in the Semantic Repository. A transformation could be used to minimize the information in the evidence to a specific information requirement. For example, to prove that a particular person has become an adult and acquired full legal capacity, the person identification and age-related information in a birth certificate is sufficient. Information on place of birth or about parents is not relevant and could therefore be omitted.

The DCAT Application profile is used for representing each XML element. The Evidence Request uses the ValueType of AnyValueType which accepts any xml representation as the slot's value.

```
<!-- EvidenceRequest Slot  -->
<rim:Slot name="EvidenceRequest">
    <rim:SlotValue xsi:type="rim:AnyValueType">
        <sdg:DataServiceEvidenceType>
            <!-- This is the ID that is fetched from the Data Services Directory -->
            <Identifier>2af27699-f131-4411-8fdb-9e8cd4e8bded</Identifier>

            <!-- Classification Information - Used for linking with the Semantic Repository and Evidence Broker -->
            <EvidenceTypeClassification>CertificateOfBirth</EvidenceTypeClassification>
            <Title lang="en">Certificate of Birth</Title>
            <Title lang="de">Geburtsurkunde</Title>
            <Description lang="en">An official certificate of birth of a person - with first name, surname, sex, date and
place of birth, which is obtained from the birth register of the place of birth.</Description>
            <Description lang="de">Eine amtliche Bescheinigung über die Geburt einer Person – mit Vorname, Familienname,
Geschlecht, Datum und Ort der Geburt, welche aus dem Geburtsregister des Geburtsortes erstellt wird.</Description>

            <!-- This is the selected distribution requested.
            It must be one of the distributions provided by the DSD for this specific Data Service Evidence Type-->
            <DistributedAs>
                <Format>application/pdf</Format>
                <ConformsTo>https://semic.org/sa/common/birthcert-1.0.0</ConformsTo>
                <Transformation>https://semic.org/sa/transformations/birthcert-1.0.0/age-of-majority</Transformation>
            </DistributedAs>
        </sdg:DataServiceEvidenceType>
    </rim:SlotValue>
</rim:Slot>
```

4.5.2.3.6 Evidence Subject and Authorized Representative slots and example

The Evidence Subject is the entity whose evidence is requested from the Data Service. The Evidence Subject can be a natural person or a legal person. This can be expressed either by a NaturalPerson **OR** a LegalPerson slot. A request may contain one of the two but **NOT** both. The Evidence Subject has a complexity dependent on the nature of the subject and the agreements made in the context of identity record matching. An optional Authorized Representative may also be defined. The Authorized Representative is a Person acting on behalf of the Evidence Subject being either a legally registered business or a natural person to trigger the Evidence Requester's request for evidence. The provided values for Evidence Subjects and Authorized Representatives are primarily bound to the eIDAS agreements. The figure below illustrates the eIDAS attributes covered by the slots "NaturalPerson", "LegalPerson" and "AuthorizedRepresentative":



eIDAS Minimum Data Set and Level of Assurance

Once-Only Evidence Requests relate to Evidence Subject, the identified users, acting either directly or through a representative. The syntax and semantics of Evidence Subject specifies how person identity attribute information is expressed. The NaturalPerson Slot and Legal Person Slot are obtained using eIDAS Minimum Data Set (MDS). Both slots contain the level of assurance of the eIDAS identification scheme. It is the responsibility of the Evidence Requester to make sure that the Level of Assurance of the identity data that is included to the request matches the previous authentication via eID means issued by an eID scheme notified under eIDAS.

Based on the the identity data received from eIDAS and included to the Evidence Request, the Data Service may decide if the user, once re-directed, needs to re-authenticate. Data Services could use identity matching based on the attributes received in the Evidence Request with an authentication verification service. The re-authentication on the side of the Data Service will allow the Data Service to verify that an eIDAS authentication took place for a user-session before which resulted in an Evidence Request with the included identity data and the indicated Level of Assurance . Thus, the Data Service could assume that the authentication was made by the user for the execution of an electronic procedure in the scope of the SDG.

Sector specific attributes

Within the Evidence Subject slots LegalPerson and NaturalPerson, it is possible to add further attributes that relate to sector-specific application contexts. These SectorSpecificAttributes can be also retrieved via eIDAS. They are embedded in the slots LegalPerson and NaturalPerson of the Evidence Request message via key-value pairs. Sector specific attributes are developed by Member States and domain experts to create additional attribute schema describing the type and usage of these attributes for inclusion in Member State eIDAS Node metadata. However, SectorSpecificAttributes are not part of the eIDAS Minimum Data Set (MDS) and identification scheme.

4.5.2.3.6.1 Natural Person slot and example

A natural person that is alive, dead or real acting as Evidence Subject described along the Core Person Vocabulary (https://semiceu.github.io/Core-Person-Vocabulary/releases/2.00/#Person).

	Name	Definition	Cardinality	Data Type	BusinessRules	Core Vocabulary	Notes
	Person	A natural person that is alive, dead or real acting as Evidence Subject.	0..1	Person		cpv:Person	Core Person Vocabulary
+	LevelOfAssurance	The Level of Assurance assured by the Evidence Requester for a specific concept of the eIDAS Minimum Data Set provided for the Natural Person.	1..1	Code	BR-OOTS-REQ-034, BR-OOTS-REQ-035	-	Reflect the Level of Assurance for the Minimum Data Set of the eIDAS identification scheme. The Level of Assurance is not applied for SectorSpecificAttributes.
+	Identifier	The unique identifier provided by eIDAS to identify the Natural Person. Example: ES/AT/02635542Y	0..1	Identifier	BR-OOTS-REQ-036, BR-OOTS-REQ-037, BR-OOTS-REQ-038	cpv:identifier	
++	Identifier/@schemeID	The schemeID of this identifier. Fixed value: eidas	M	Code	BR-OOTS-REQ-039, BR-OOTS-REQ-040	cpv:identifier	

	Name	Definition	Cardinality	Data Type	BusinessRules	Core Vocabulary	Notes
+	FamilyName	The hereditary surname of a family. Is part of the MDS.	1..1	Text		cpv:familyName	
+	GivenName	The name(s) that identify the Person within a family with a common surname. Is part of the MDS.	1..1	Text		cpv:givenName	
+	DateOfBirth	The point in time on which the Person was born. Is part of the MDS.	1..1	Date	BR-OOTS-REQ-041	cpv:dateOfBirth	
+	BirthName	Full name of the Person given upon their birth. Is part of the MDS.	0..1	Text		cpv:birthName	
+	PlaceOfBirth	The Location where the Person was born. Is part of the MDS.	0..1	Text		locn:placeOfBirth	Core Location Vocabulary
+	CurrentAddress	The place that the Person treats as permanent home. Is part of the MDS.	0..1	Address		locn:Address	Core Location Vocabulary
+	Gender	The identities, expressions and societal roles of the Person. Is part of the MDS.	0..1	Text	BR-OOTS-REQ-042	cpv:gender	
+	SectorSpecificAttribute	SectorSpecificAttributes could similarly be requested via eIDAS in order to increase the success rate of identity and record matching.	0..n	AttributeKeyValuePair		-	SectorSpecificAttributes are not part of the MDS.

	Name	Definition	Cardinality	Data Type	BusinessRules	Core Vocabulary	Notes
		They are expressed via key-value pairs.					
++	CurrentAddress	The place that the Person treats as permanent home. Is part of the MDS.	0..1	Address		locn:Address	Core Location Vocabulary
+++	FullAddress	The complete address written as a string. Is part of the MDS.	0..1	Text		locn:fullAddress	
+++	Thoroughfare	The name of a street, passage or way through from one location to another. Is part of the MDS.	0..1	Text		locn:thoroughfare	
+++	LocatorDesignator	A number or sequence of characters that uniquely identifies the locator (building number, apartment number, etc.) within the relevant scope. Is part of the MDS.	0..1	Text		locn:locatorDesignator	
+++	AdminUnitLevel1	The name of the uppermost level of the address, almost always a country. Is part of the MDS.	0..1	Code	BR-OOTS-REQ-043	locn:adminUnitL1	
+++	AdminUnitLevel2	The name of a secondary level/region of the address, usually a county, state or other such area that typically	0..1	Code	BR-OOTS-REQ-044	locn:adminUnitL2	

	Name	Definition	Cardinality	Data Type	BusinessRules	Core Vocabulary	Notes
		encompasses several localities. Is part of the MDS.					
+++	PostCode	The code created and maintained for postal purposes to identify a subdivision of addresses and postal delivery points. Is part of the MDS.	0..1	Code		locn:postCode	
+++	PostCityName	The key postal division of the address, usually the city.	0..1	Code		locn:postName	
++	SectorSpecificAttribute	SectorSpecificAttributes could similarly be requested via eIDAS in order to increase the success rate of identity and record matching. They are expressed via key-value pairs.	0..n	AttributeKeyValuePair		-	SectorSpecificAttributes are not part of the MDS.
+++	AttributeName	The name of the SectorSpecificAttribute. Is **not** part of the MDS.	1..1	Text		-	
+++	AttributeURI	A unique identifier of the SectorSpecificAttribute. Is **not** part of the MDS.	1..1	Identifier		-	

	Name	Definition	Cardinality	Data Type	BusinessRules	Core Vocabulary	Notes
+++	AttributeValue	The Value of the SectorSpecificAttribute. Is **not** part of the MDS.	1..1	Text		-	

The NaturalPerson slot contains data that describes a Natural Person. When using an ISA Core Person Vocabulary for representing the value of a slot, AnyValueType is used as its type since it allows data in XML format to be used as the slot's value.

```
<!-- NaturalPerson Slot  -->
<rim:Slot name="NaturalPerson">
    <rim:SlotValue xsi:type="rim:AnyValueType">
        <sdg:Person>
            <!-- Level of Assurance for the Minimum Data Set (MDS) -->
            <LevelOfAssurance>High</LevelOfAssurance>

            <!-- eIDAS Identifier -->
            <Identifier schemeID="eidas">EL/BE/12313132</Identifier>

            <!-- eIDAS Mandatory Attributes of the Minimum Data Set -->
            <FamilyName>Doe</FamilyName>
            <GivenName>John</GivenName>
            <DateOfBirth>1978-09-09</DateOfBirth>

            <!-- eIDAS Optional Attributes of the Minimum Data Set -->
            <BirthName>Jonathan Doepidis</BirthName>
            <PlaceOfBirth>Athens</PlaceOfBirth>
            <CurrentAddress >
                <FullAddress>Panepistimou 5, 85101, Athens</FullAddress>
                <AdminUnitLevel1>GR</AdminUnitLevel1>
            </CurrentAddress>
            <Gender>Male</Gender>

            <!-- Optional Sector Specific Attributes not belonging to the Minimum Data Set -->
            <SectorSpecificAttribute>
                <AttributeName>IBAN</AttributeName>
                <AttributeURI>http://eidas.europa.eu/attributes/naturalperson/banking/IBAN</AttributeURI>
                <AttributeValue>DE02500105170137075032</AttributeValue>
            </SectorSpecificAttribute>
            <SectorSpecificAttribute>
                <AttributeName>BIC</AttributeName>
                <AttributeURI>http://eidas.europa.eu/attributes/naturalperson/banking/BIC</AttributeURI>
                <AttributeValue>INGDDEFFYYY</AttributeValue>
            </SectorSpecificAttribute>
        </sdg:Person>
    </rim:SlotValue>
</rim:Slot>
```

4.5.2.3.6.2 Legal Person slot and example

A business that is legally registered acting as Data Subject described along the Core Business Vocabulary (https://semiceu.github.io/Core-Business-Vocabulary/releases/2.00/)

	Name	Definition	Cardinality	Type	BusinessRules	Core Vocabulary	Notes
	LegalPerson			Identifier		cbv:LegalEntity	Core Business Vocabulary
+	LevelOfAssurance	The Level of Assurance assured by the Evidence Requester for a specific concept of the eIDAS Minimum Data Set provided for the Natural Person.	1..1	Code	BR-OOTS-REQ-045, BR-OOTS-REQ-046	-	Reflect the Level of Assurance for the Minium Data Set of the eIDAS identification scheme. The Level of Assurance is not applied for SectorSpecificAttributes.
+	LegalPersonIdentifier	The unique identifier provided by eIDAS to identify the Legal Entity. Example: ES/AT/02635542Y	0..1	Identifier	BR-OOTS-REQ-047, BR-OOTS-REQ-048, BR-OOTS-REQ-049	cbv:legalIdentifier	
++	LegalPersonIdentifier/@schemeID	The schemeID of this identifier. Fixed value: eidas	M	Code	BR-OOTS-REQ-050, BR-OOTS-REQ-051	cbv:legalIdentifier	
+	Identifier	The unambiguous structured reference assigned to the Legal Entity by the legal	0..n	Identifier		cbv:identifier	

	Name	Definition	Cardinality	Type	BusinessRules	Core Vocabulary	Notes
		authority that registered it.					
++	Identifier/@schemeID	The schemeID of this identifier.	M	Code	BR-OOTS-REQ-052, BR-OOTS-REQ-053	cbv:identifier	
+	LegalName	The name under which the Legal Entity is legally registered.	1..1	Text		cbv:legalName	
+	RegisteredAddress	The address at which the Legal Entity is legally registered.	0..1	Address		locn:Address	
+	SectorSpecificAttribute	SectorSpecificAttributes could similarly be requested via eIDAS in order to increase the success rate of identity and record matching. They are expressed via key-value pairs.	0..n	AttributeKeyValuePair		-	SectorSpecificAttributes are not part of the MDS.
++	RegisteredAddress	The address at which the Legal Entity is legally registered.	0..1	Address		locn:Address	
+++	FullAddress	The complete address written as a string.	0..1	Text		locn:fullAddress	

	Name	Definition	Cardinality	Type	BusinessRules	Core Vocabulary	Notes
+++	Thoroughfare	The name of a street, passage or way through from one location to another.	0..1	Text		locn:thoroughfare	
+++	LocatorDesignator	A number or sequence of characters that uniquely identifies the locator (building number, apartment number, etc.) within the relevant scope.	0..1	Text		locn:locatorDesignator	
+++	AdminUnitLevel1	The name of the uppermost level of the address, almost always a country.	0..1	Code	BR-OOTS-REQ-054	locn:adminUnitL1	
+++	AdminUnitLevel2	The name of a secondary level/region of the address, usually a county, state or other such area that typically encompasses several localities.	0..1	Code	BR-OOTS-REQ-055	locn:adminUnitL2	
+++	PostCode	The code created and maintained for postal purposes to identify a subdivision of addresses and postal delivery points.	0..1	Code		locn:postCode	

	Name	Definition	Cardinality	Type	BusinessRules	Core Vocabulary	Notes
+++	PostCityName	The key postal division of the address, usually the city.	0..1	Code		locn:postName	
++	SectorSpecificAttribute	SectorSpecificAttributes could similarly be requested via eIDAS in order to increase the success rate of identity and record matching. They are expressed via key-value pairs.	0..n	AttributeKeyValuePair		-	SectorSpecificAttributes are not part of the MDS.
+++	AttributeName	The name of the SectorSpecificAttribute. Is **not** part of the MDS.	1..1	Text		-	
+++	AttributeURI	A unique identifier of the SectorSpecificAttribute. Is **not** part of the MDS.	1..1	Identifier		-	
+++	AttributeValue	The Value of the SectorSpecificAttribute. Is **not** part of the MDS.	1..1	Text		-	

The LegalPerson slot contains data that describes the Legal Person (a.k.a. a Company) that submits this request. When using an ISA Core Busines Vocabulary for representing the value of a slot, AnyValueType is used as its type since it allows data in XML form to be used as the slot's value.

```
 <!-- LegalPerson Slot  -->
<rim:Slot name="LegalPerson">
    <rim:SlotValue xsi:type="rim:AnyValueType">
        <sdg:LegalPerson>
            <!-- Level of Assurance for the Minimum Data Set (MDS) -->
            <LevelOfAssurance>High</LevelOfAssurance>

            <!-- eIDAS Mandatory Attributes of the Minimum Data Set -->
            <LegalPersonIdentifier schemeID="eidas">ES/SE/12132123Y</LegalPersonIdentifier>
            <LegalName>AnyCompanyName</LegalName>

            <!-- Optional Attributes of the Minimum Data Set -->
            <Identifier schemeID="Tax">113123123123123</Identifier>
            <Identifier schemeID="VAT">SE730757727</Identifier>
            <RegisteredAddress>
                <FullAddress>Prince Street 15</FullAddress>
                <LocatorDesignator>15</LocatorDesignator>
                <PostCode>11221</PostCode>
                <PostCityName>Malmo</PostCityName>
                <Thoroughfare>PrinceStreet</Thoroughfare>
                <AdminUnitLevel1>SE</AdminUnitLevel1>
            </RegisteredAddress>

            <!-- Optional Sector Specific Attributes not belonging to the Minimum Data Set -->
            <SectorSpecificAttribute>
                <AttributeName>IBAN</AttributeName>
                <AttributeURI>http://eidas.europa.eu/attributes/legalperson/banking/IBAN</AttributeURI>
                <AttributeValue>SE0250010517013707503 2</AttributeValue>
            </SectorSpecificAttribute>
            <SectorSpecificAttribute>
                <AttributeName>BIC</AttributeName>
                <AttributeURI>http://eidas.europa.eu/attributes/legalperson/banking/BIC</AttributeURI>
                <AttributeValue>INGDDEFFYYY</AttributeValue>
            </SectorSpecificAttribute>
        </sdg:LegalPerson>
    </rim:SlotValue>
</rim:Slot>
```

4.5.2.3.6.3 Authorized Representative slot and example

An optional Authorized Representative may also be defined. The Authorized Representative is a Person acting on behalf of the Evidence Subject being either a legaly registered business or a natural person to trigger the evidence requester's request for evidence. The profile is dependent on the SDG OOTS record matching agreements. The Authorized Representative is described along the Core Person Vocabulary (https://semiceu.github.io/Core-Person-Vocabulary/releases/2.00/#Person).

	Name	Definition	Cardinality	Data Type	BusinessRules	Core Vocabulary	Notes
	Person	A natural person acting on behalf of a legally registered business or natural person.	0..1	Person		cpv:Person	Core Person Vocabulary
+	LevelOfAssurance	The Level of Assurance assured by the Evidence Requester for a specific concept of the eIDAS Minimum Data Set provided for the Natural Person.	1..1	Code	BR-OOTS-REQ-056, BR-OOTS-REQ-057	-	Reflect the Level of Assurance for the Minium Data Set of the eIDAS identification scheme. The Level of Assurance is not applied for SectorSpecificAttributes.
+	Identifier	The unambiguous structured reference to the Person. Is part of the MDS.	1..n	Identifier	BR-OOTS-REQ-058, BR-OOTS-REQ-059, BR-OOTS-REQ-060	cpv:identifier	
++	Identifier/@schemeID	The schemeID of this identifier. Fixed value: eidas	M	Code	BR-OOTS-REQ-061, BR-OOTS-REQ-062	cpv:identifier	
+	FamilyName	The hereditary surname of a family. Is part of the MDS.	1..1	Text		cpv:familyName	
+	GivenName	The name(s) that identify the Person within a family with a common surname. Is part of the MDS.	1..1	Text		cpv:givenName	

	Name	Definition	Cardinality	Data Type	BusinessRules	Core Vocabulary	Notes
+	DateOfBirth	The point in time on which the Person was born. Is part of the MDS.	1..1	Text	BR-OOTS-REQ-063	cpv:dateOfBirth	
+	BirthName	Full name of the Person given upon their birth. Is part of the MDS.	0..1	Text		cpv:birthName	
+	Gender	The identities, expressions and societal roles of the Person. Is part of the MDS.	0..1	Code	BR-OOTS-REQ-064	cpv:gender	
+	PlaceOfBirth	The Location where the Person was born. Is part of the MDS.	0..1	Text		locn:placeOfBirth	Core Location Vocabulary
+	CurrentAddress	The place that the Person treats as permanent home. Is part of the MDS.	0..1	Address		locn:Address	Core Location Vocabulary
+	SectorSpecificAttribute	SectorSpecificAttributes could similarly be requested via eIDAS in order to increase the success rate of identity and record matching. They are expressed via key-value pairs. SectorSpecificAttributes are **not part** of the MDS. Thus no level of assurance is provided by eIDAS.	0..n				SectorSpecificAttributes are not part of the MDS.
++	CurrentAddress	The place that the Person treats as permanent home. Is part of the MDS.	0..1	Address		locn:Address	Core Location Vocabulary

	Name	Definition	Cardinality	Data Type	BusinessRules	Core Vocabulary	Notes
+++	FullAddress	The complete address written as a string. Is part of the MDS.	0..1	Text		locn:fullAddress	
+++	Thoroughfare	The name of a street, passage or way through from one location to another. Is part of the MDS.	0..1	Text		locn:thoroughfare	
+++	LocatorDesignator	A number or sequence of characters that uniquely identifies the locator (building number, apartment number, etc.) within the relevant scope. Is part of the MDS.	0..1	Text		locn:locatorDesignator	
+++	AdminUnitLevel1	The name of the uppermost level of the address, almost always a country. Is part of the MDS.	0..1	Code	BR-OOTS-REQ-065	locn:adminUnitL1	
+++	AdminUnitLevel2	The name of a secondary level/region of the address, usually a county, state or other such area that typically encompasses several localities. Is part of the MDS.	0..1	Code	BR-OOTS-REQ-066	locn:adminUnitL2	
+++	PostCode	The code created and maintained for postal purposes to identify a subdivision of addresses and postal delivery points. Is part of the MDS.	0..1	Code		locn:postCode	
+++	PostCityName	The key postal division of the address, usually the city.	0..1	Code		locn:postName	

	Name	Definition	Cardinality	Data Type	BusinessRules	Core Vocabulary	Notes
++	SectorSpecificAttribute	SectorSpecificAttributes could similarly be requested via eIDAS in order to increase the success rate of identity and record matching. They are expressed via key-value pairs.	0..n				SectorSpecificAttributes are not part of the MDS.
+++	AttributeName	The name of the SectorSpecificAttribute. Is **not** part of the MDS.	1..1	Text		-	
+++	AttributeURI	A unique identifier of the SectorSpecificAttribute. Is **not** part of the MDS.	1..1	Identifier		-	
+++	AttributeValue	The Value of the SectorSpecificAttribute. Is **not** part of the MDS.	1..1	Text		-	

The AuthorizedRepresentative slot contains data that describes the Legal Representative of a company. This slot is optional and may be used for expressing the representative of either a LegalPerson or a NaturalPerson slot. When using an ISA Core Vocabulary for representing the value of a slot, AnyValueType is used as its type since it allows data in XML format to be used as the slot's value.

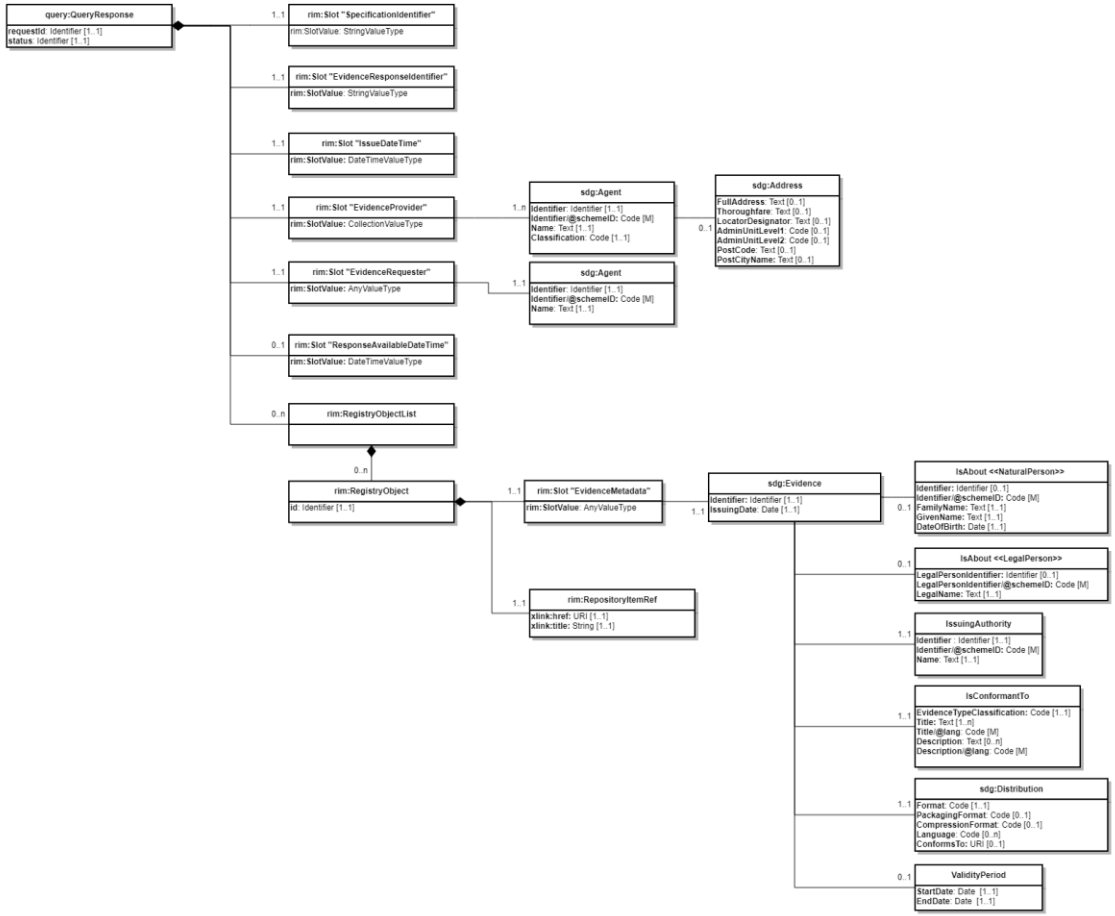
```
<!--  AuthorizedRepresentative Slot. Both LegalPerson and NaturalPerson can have an AuthorizedRepresentative (optional 0..1)-
->
<rim:Slot name="AuthorizedRepresentative">
    <rim:SlotValue xsi:type="rim:AnyValueType">
        <!--     Core Person Vocabulary (CPV) Expression of the LegalRepresentative -->
        <sdg:Person>

            <!-- Level of Assurance for the Minimum Data Set (MDS) -->
            <LevelOfAssurance>High</LevelOfAssurance>

            <!-- eIDAS Mandatory Attributes of the Minimum Data Set -->
            <Identifier>GR/BE/12313132</Identifier>
            <FamilyName>Doe</FamilyName>
            <GivenName>John</GivenName>
            <DateOfBirth>1978-09-09</DateOfBirth>

            <!-- eIDAS Optional Attributes of the Minimum Data Set -->
            <BirthName>Jonathan Doepidis</BirthName>
            <PlaceOfBirth>Athens</PlaceOfBirth>
            <CurrentAddress >
                <FullAddress>Panepistimou 5, 85101, Athens</FullAddress>
                <AdminUnitLevel1>GR</AdminUnitLevel1>
            </CurrentAddress>
            <Gender>Male</Gender>

            <!-- Optional Sector Specific Attributes not belonging to the Minimum Data Set -->
            <SectorSpecificAttribute>
                <AttributeName>IBAN</AttributeName>
                <AttributeURI>http://eidas.europa.eu/attributes/naturalperson/banking/IBAN</AttributeURI>
                <AttributeValue>DE02500105170137075032</AttributeValue>
            </SectorSpecificAttribute>
            <SectorSpecificAttribute>
                <AttributeName>BIC</AttributeName>
                <AttributeURI>http://eidas.europa.eu/attributes/naturalperson/banking/BIC</AttributeURI>
                <AttributeValue>INGDDEFFYYY</AttributeValue>
            </SectorSpecificAttribute>
        </sdg:Person>
    </rim:SlotValue>
</rim:Slot>
```

4.5.3 Evidence Response Syntax Mapping - June 2022

4.5.3.1 Exchange Data Model: QueryResponse (Evidence Response)

This guideline explains how to use the ebRS QueryResponse syntax to implement the Business Requirements (Req ID) described for the Evidence Response. The guideline provides specific details for each class and information elements including the underlying standards, data types and cardinalities to produce conformant XML documents. In the following sections, we describe the XML serialization of the Evidence Response in the same hierarchical order of the corresponding Exchange Data Model.

The Exchange Data Model in the figure below provides an overview of the information elements and their associations contained in the Evidence Response. An Evidence Response is a message created by the Evidence Provider (EP) containing all the necessary parameters for positively responding to an evidence request including the evidence itself.



To form a valid QueryResponse, at least the following elements are required:

- the "requestID" of the QueryRequest;

- the "status" of the QueryResponse;
- the "SpecificationIdentifier" to identify the version of this specification.
- the "EvidenceResponseIdentifier" provides a unique identifier of the Response Message.
- the "IssueDateTime" to describe the time of the response;
- the "EvidenceProvider" to describe the entity that is technically responsible for creating the QueryResponse;
- the "EvidenceRequester" to describe the entity that is technically responsible for receiving the QueryResponse;
- the QueryResponse must include a "rim:RegistryObjectList" which returns the requested information. A "DocumentQuery" triggers a response with the rim:Slot "EvidenceMetadata" and rim:RepositoryItemRef.

4.5.3.2 ebRIM Definition of the QueryResponse (Evidence Response)

This section defines the core ebRIM elements that are used to compose a Query Response (Evidence Response). It thereby distinguishes between attributes and slots to define the Evidence Response:

Attribute Definition: The table provides an overview of the mandatory attributes and the information they contain for each QueryResponse according to ebRIM.

Slot definition: The elements provide an overview of the defined ebRIM SlotType instances, which have a name and a value. The value is of type ValueType. Most rim:Slots do not contain sub-properties other than the SlotValue itself, except if they are collections. Collections refer to sources such as Core Vocabularies and a corresponding class defined in the SDGR Application Profile (see section 3).

Legend
The tables below represent the tree structure of the EDM. Light grey rows open classes and define ther properties and attributes. Light green rows soley illustrate the classes that are subordinated to a class and illustrate the tree structure. Light green rows are then repeated as light grey rows to describe properties and attributes of the class. The hierarchy of the tree structure is also indicated in the first column via the '+' symbol.

	Name	Definition	Cardinality	ebRIM type	Data Type	Rules	Mapping to a class of SDGR Application Profile	Mapping to Core Vocabulary
	query:QueryResponse	**Evidence Response root element**		ComplexType		Structure: BR-		

	Name	Definition	Cardinality	ebRIM type	Data Type	Rules	Mapping to a class of SDGR Application Profile	Mapping to Core Vocabulary
						OOTS-RESP-ebRIM-008		
+	requestId	The unique identifier of the Evidence request. Must be the same as the id attribute of the QueryRequest that generated this QueryResponse.	1..1	Attribute	Identifier	Use: BR-OOTS-RESP-001		
+	status	This attribute contains the status of the response. If the evidence is provided the value "urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Success" is used.	1..1	Attribute	Identifier	Use: BR-OOTS-RESP-002		
++	SpecificationIdentifier	An identification of the specification for the Evidence Response containing the total set of rules regarding semantic content, cardinalities and business rules to which the data contained in the instance document conforms.	1..1	SlotType	StringValueType	Structure: BR-OOTS-RESP-ebRIM-001, BR-OOTS-RESP-ebRIM-009 Use: BR-OOTS-	-	-

	Name	Definition	Cardinality	ebRIM type	Data Type	Rules	Mapping to a class of SDGR Application Profile	Mapping to Core Vocabulary
						RESP-003		
++	EvidenceResponseIdentifier	The unique identifier of the Evidence Response.	1..1	SlotType	StringValueType	Structure: BR-OOTS-RESP-ebRIM-002, BR-OOTS-RESP-ebRIM-010 Use: BR-OOTS-RESP-004		
++	IssueDateTime	The issue date and time when the Evidence Response is issued. The issue date time must have a granularity of seconds and include time zone information.	1..1	SlotType	DateTimeValueType	Structure: BR-OOTS-RESP-ebRIM-003, BR-OOTS-RESP-ebRIM-011 Use: BR-OOTS-	-	-

	Name	Definition	Cardinality	ebRIM type	Data Type	Rules	Mapping to a class of SDGR Application Profile	Mapping to Core Vocabulary
						RESP-005		
++	ResponseAvailableDateTime	The date and time when the Evidence Response will be issued in case of asynchronous evidence distribution.	0..1	SlotType	DateTimeValueType	Structure: BR-OOTS-RESP-ebRIM-006, BR-OOTS-RESP-ebRIM-014 Use: BR-OOTS-RESP-006	-	-
++	EvidenceProvider	The Agent or organisation that operates the data service providing the evidence.	1..n	SlotType	CollectionValueType	Structure: BR-OOTS-RESP-ebRIM-004, BR-OOTS-RESP-ebRIM-012, BR-OOTS-RESP-	Agent	Core Public Service Vocabulary Application Profile

	Name	Definition	Cardinality	ebRIM type	Data Type	Rules	Mapping to a class of SDGR Application Profile	Mapping to Core Vocabulary
						ebRIM-016, BR-OOTS-RESP-ebRIM-017		
++	EvidenceRequester	The Agent or organisation that is requesting the evidence.	1..1	SlotType	AnyValueType	Structure: BR-OOTS-RESP-ebRIM-005, BR-OOTS-RESP-ebRIM-013, BR-OOTS-RESP-ebRIM-018, BR-OOTS-RESP-ebRIM-019	Agent	Core Public Service Vocabulary Application Profile
++	**rim:RegistryObjectList**	**Element to list the Registry Objects of the QueryResponse.**	0..n	ComplexType	-			

	Name	Definition	Cardinality	ebRIM type	Data Type	Rules	Mapping to a class of SDGR Application Profile	Mapping to Core Vocabulary
+++	**RegistryObject**	**Element to control the type and structure of Registry Object within the QueryResponse.**	0..n	ComplexType	ExtrinsicObjectType			
++++	id	Unique UUID for each RegistryObject. This value is defined by the Evidence Provider.	1..1	Attribute	Identifier	Use: BR-OOTS-RESP-015	-	-
++++	EvidenceMetadata		1..1	SlotType	AnyValueType	Structure: BR-OOTS-RESP-ebRIM-007, BR-OOTS-RESP-ebRIM-015, BR-OOTS-RESP-ebRIM-020, BR-OOTS-RESP-ebRIM-021	Evidence	DCAT Application Profile
++++	RepositoryItemRef	The RepositoryItemRef locates the Evidence file within the repository. It provides a precise reference to the	1..1	ComplexType				

	Name	Definition	Cardinality	ebRIM type	Data Type	Rules	Mapping to a class of SDGR Application Profile	Mapping to Core Vocabulary
		repository item provided by the Evidence Provider.						
++++	xlink:href	An internal reference to the repository in which the requested Evidence file is located. The reference thereby may point to a specific distribution of the Evidence.	1..1	Attribute	URI	Use: BR-OOTS-RESP-043		
++++	xlink:title	The title of the document instance that is provided by the Data Provider.	1..1	Attribute	string			

4.5.3.2.1 ebRIM QueryResponse example

The Evidence Response is expressed using the ebRS Query Response Message. It contains a reference to the query it is responding to, and thus there is no need to include any information already present in the request. This reference is in the form of a **requestID attribute**.

The **status attribute** is used to distinguish between a successful response using the value "urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Success" and a response that is available at a later time "urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Unavailable".

The Evidence Response is contained in the `RegistryObjectList` element of the QueryResponse. Each Registry Object in the registry object list represents an Evidence Distribution. It is noted that the Registry Object list may contain more than one responding pieces of evidence, each represented in the distribution requested. Each `RegistryObject` element contains one EvidenceMetadata slot and one `repositoryItemRef` element.

The `RepositoryItemRef` element contains the link to the AS4 Attachment containing the distribution described in the EvidenceMetadata Slot.

```
<?xml version="1.0" encoding="UTF-8"?>

<query:QueryResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns:rs="urn:oasis:names:tc:ebxml-regrep:xsd:rs:4.0"
    xmlns:rim="urn:oasis:names:tc:ebxml-regrep:xsd:rim:4.0"
    xmlns:query="urn:oasis:names:tc:ebxml-regrep:xsd:query:4.0"
    xmlns:sdg="http://data.europa.eu/p4s"
    xmlns:xlink="http://www.w3.org/1999/xlink"
    xmlns:xml="http://www.w3.org/XML/1998/namespace"

    requestId="c4369c4d-740e-4b64-80f0-7b209a66d629"
    status="urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Success">

    <!-- Slots are omitted for clarity  -->
    <rim:RegistryObjectList>

        <!-- First Object -->
        <rim:RegistryObject xsi:type="rim:ExtrinsicObjectType" id="555555-740e-4b64-80f0-2462462462">

            <!-- The slot "EvidenceMetadata" is included here -->

            <!-- The attached Document Provided as Evidence. Points to an AS4 attachment -->
            <rim:RepositoryItemRef xlink:href="cid:attachment100001@example.oots.eu"
xlink:title="SecondaryEducationCompletion"/>
        </rim:RegistryObject>

        <!-- Second Object -->
        <rim:RegistryObject xsi:type="rim:ExtrinsicObjectType" id="60bc1cbb-2f6c-4eef-9479-b4ce3684572c">

            <!-- The slot "EvidenceMetadata" is included here -->

            <!-- The attached Document Provided as Evidence. Points to an AS4 attachment -->
            <rim:RepositoryItemRef xlink:href="cid:attachment100002@example.oots.eu" xlink:title="Secondary Education
Completion Evidence Supplement"/>
        </rim:RegistryObject>
    </rim:RegistryObjectList>
</query:QueryResponse>
```

4.5.3.2.2 Specification Identifier example

The `SpecificationIdentifier` element is used for expressing the version of the specification used for creating the referred document.

A Slot with the name of "SpecificationIdentifier" is used with the ValueType of StringValueType.

```
<!-- SpecificationIdentifier Slot -->
    <rim:Slot name="SpecificationIdentifier">
        <rim:SlotValue xsi:type="rim:StringValueType">
            <rim:Value>oots-edm:v1.0</rim:Value>
        </rim:SlotValue>
    </rim:Slot>
```

4.5.3.2.3 Evidence Response Identifier example

The `EvidenceResponseIdentifier` element is used for expressing the Unique Identifier of the response generated by the evidence provider.

A Slot with the name of "EvidenceResponseIdentifier" is used with the ValueType of StringValueType.

```
<!-- EvidenceResponseIdentifier Slot -->
    <rim:Slot name="EvidenceResponseIdentifier">
        <rim:SlotValue xsi:type="rim:StringValueType">
            <rim:Value>5af62cce-debe-11ec-9d64-0242ac120002</rim:Value>
        </rim:SlotValue>
    </rim:Slot>
```

4.5.3.2.4 Issue Date and Time example

The IssueDateTime element is used for expressing the creation date and time of the referenced document.

A Slot with the name of "IssueDateTime" is used with the ValueType of DateTimeValueType which has the value of ISO timestamp.

```
<!-- IssueDateTime Slot -->
 <rim:Slot name="IssueDateTime">
     <rim:SlotValue xsi:type="rim:DateTimeValueType">
         <rim:Value>2022-05-19T17:10:10.872Z</rim:Value>
     </rim:SlotValue>
 </rim:Slot>
```

4.5.3.2.5 Response Available Date Time example

In situations where pieces of evidence may exist that are not immediately available, the ResponseAvailableDateTime slot may be used to express the latest point in time by which any such late pieces of evidence may be made available. As an example, this may be used by Data Services that generate evidence using a process that cannot complete within the duration of an interactive user session, but which have a predictable availability date and time. For example, a process that involves scheduled batch jobs. Depending on implementation, the Online Procedure Portal may use this information to inform the user to pause the procedure and to return at a later point by which time the evidence will be available.

If multiple pieces of evidence may be available, with possibly different dates and times at which they are available, the value to be used in the Slot should be the latest of these values.

This Slot must only be used with Query Response status set to the “Unavailable” response status. In that case, the content of the QueryResponse element must contain a (possibly empty) RegistryObjectList.

The Slot must be omitted if the Data Service is not willing or able to provide the date and time by which pieces of evidence may be available.

A Slot with the name of "ResponseAvailableDateTime" is optionally used with the ValueType of DateTimeValueType which has the value of ISO timestamp.

```
<!-- ResponseAvailableDateTime Slot  -->
 <rim:Slot name="ResponseAvailableDateTime">
     <rim:SlotValue xsi:type="rim:DateTimeValueType">
         <rim:Value>2022-05-30T15:00:00.000Z</rim:Value>
     </rim:SlotValue>
 </rim:Slot>
```

4.5.3.3 SDGR Application Profile for the Evidence Response

The SDGR application profile for the Evidence Response defines the semantics of the previously introduced rim:Slots defined as a collection (green components) of the Evidence Response Message. The SDGR application profile for the Evidence Response describes how the SDG-Generic-Metadata Profile (SDG-syntax) is profiled in ebRIM in order to compose a valid QueryResponse. It therefore contains a mapping to the underlying SDG-syntax elements and necessary parameters for providing the evidence that was requested by an Evidence Request. Thus, the values for several parameters are

obtained from the Evidence Provider that is responding to the Evidence Request. The namespace of the SDG-syntax is http://data.europa.eu/p4s. In the following samples, the prefix "sdg" is assumed to be linked to the namespace http://data.europa.eu/p4s.

4.5.3.3.1 Evidence Provider slot and example

The Evidence Provider element is used to describe an organisation that provides data or documents requested by an Evidence Requester. In most cases, the agent is a public organisation, however in some MSs, for some evidence types, businesses have been accredited to supply them.

An evidence provider must be registered in the Data Service Directory in order to be activated in the SDG OOTS.

	Name	Definition	Cardinality	Type	Rules	Core Vocabulary	Notes
	Agent	The Agent or organisation that is providing the evidence.	1..n	Agent		dct:Agent	Core Public Service Vocabulary Application Profile
+	Identifier	A unique identification for the agent.	1..1	Identifier		dct:identifier	
++	Identifier/@schemeID	Scheme identifier for the agent identification	M	Code	BR-OOTS-RESP-007, BR-OOTS-RESP-008	dct:identifier	
+	Name	A short label for the agent.	1..1	Text		dct:title	
+	Address	A location of the Evidence Provider in the form of an address.	0..1	Address		locn:Address	Core Location Vocabulary
+	Classification	A code to classify the agents associated to the communication. In case there are multiple agents the codes must be used to distinguish between the actual Evidence Provider and Intermediary Platforms that are involved in the transaction. Default value: EvidenceProvider	1..1	Code	BR-OOTS-RESP-011, BR-OOTS-RESP-012	cv:role	
++	Address	A location of the Evidence Provider in the form of an address.		Address		locn:Address	Core Location Vocabulary

	Name	Definition	Cardinality	Type	Rules	Core Vocabulary	Notes
+++	FullAddress	The complete address written as a string.	0..3	Text		locn:fullAddress	
+++	Thoroughfare	The name of a street, passage or way through from one location to another.	0..1	Text		locn:thoroughfare	
+++	LocatorDesignator	A number or sequence of characters that uniquely identifies the locator (building number, apartment number, etc.) within the relevant scope.	0..1	Text		locn:locatorDesignator	
+++	AdminUnitLevel1	The name of the uppermost level of the address, almost always a country.	0..1	Code	BR-OOTS-RESP-009	locn:adminUnitL1	
+++	AdminUnitLevel2	The name of a secondary level/region of the address, usually a county, state or other such area that typically encompasses several localities.	0..1	Code	BR-OOTS-RESP-010	locn:adminUnitL2	
+++	PostCode	The code created and maintained for postal purposes to identify a subdivision of addresses and postal delivery points.	0..1	Code		locn:postCode	
+++	PostCityName	The key postal division of the address, usually the city.	0..1	Code		locn:postName	

The Evidence Provider element is expressed using a Slot with the name of "EvidenceProvider" and ValueType of AnyValueType in order to express the information using the Core Public Service Vocabulary Application Profile. The Evidence Provider information inside the AnyValueType Slot is expressed using the Agent Class.

```
<!--   EvidenceProvider Slot -->
    <rim:Slot name="EvidenceProvider">
        <rim:SlotValue xsi:type="rim:AnyValueType">
            <sdg:Agent>
                <sdg:Identifier schemeID="9930">DE73524311</sdg:Identifier>
                <sdg:Name lang="en">Civil Registration Office Berlin I</sdg:Name>
                <sdg:Address>
                        <sdg:FullAddress>Schönstedtstraße 5</sdg:FullAddress>
                        <sdg:LocatorDesignator>5</sdg:LocatorDesignator>
                        <sdg:PostCode>13357</sdg:PostCode>
                        <sdg:PostCityName>Berlin</sdg:PostCityName>
                        <sdg:AdminUnitLevel1>DE</sdg:AdminUnitLevel1>
                </sdg:Address>
                <sdg:Classification>EvidenceProvider</sdg:Classification>
            </sdg:Agent>
        </rim:SlotValue>
    </rim:Slot>
```

4.5.3.3.2 Evidence Requester slot and example

The Evidence Requester element is used to describe an organisation that requests data or documents from Evidence Providers. The agent requests the evidence, by sending an evidence request to the evidence provider, on behalf of the evidence subject. In several cases it might be a portal/organisation that initiates the evidence request. However, the evidence response must be returned to the Evidence Requester that initiated the evidence request and not to the portal/intermediary in case there are more than one Evidence Requesters named in the evidence request.

No central registry of evidence requesters is required, only the minimal details required to enable legal logging of requests or facilitate the processing of the evidence request.

	Name	Definition	Cardinality	Type	Rules	Core Vocabulary	Notes
	Agent	The Agent or organisation that is requesting the evidence.	1..1	Agent		dct:Agent	Core Public Service Vocabulary Application Profile
+	Identifier	A unique identification for the agent.	1..1	Identifier		dct:identifier	

	Name	Definition	Cardinality	Type	Rules	Core Vocabulary	Notes
++	Identifier/@schemeID	Scheme identifier for the agent identification	M	Code	BR-OOTS-RESP-013, BR-OOTS-RESP-014	dct:identifier	
+	Name	A short label for the agent.	1..1	Text		dct:title	

A Slot with the name of "EvidenceRequester" is used with the ValueType of AnyValueType which accepts any xml representation. In this particular case, the Core Public Service Vocabulary Application Profile and its Agent class is used for the expression of the Evidence Requester information inside the AnyValueType Slot.

```
<!--   EvidenceRequester Slot  -->
    <rim:Slot name="EvidenceRequester">
        <rim:SlotValue xsi:type="rim:AnyValueType">
            <sdg:Agent>
                <sdg:Identifier schemeID="0096">DK22233223</sdg:Identifier>
                <sdg:Name>Denmark University Portal</sdg:Name>
            </sdg:Agent>
        </rim:SlotValue>
    </rim:Slot>
```

4.5.3.3.3 Evidence Metadata slot and example

Element to provide the metadata about an evidence that is provided from the Data Service of an Evidence Provider (EP). Is described along the DCAT Application Profile.

	Name	Definition	Cardinality	Type	Rules	Core Vocabulary	Notes
	Evidence	Provides the semantic information and requirements for retrieving an evidence type from a Data Service.	1..1	Evidence		dcat:Dataset	DCAT Application Profile

	Name	Definition	Cardinality	Type	Rules	Core Vocabulary	Notes
+	Identifier	The identifier of an evidence.	1..1	Identifier	BR-OOTS-RESP-016	dcat:identifier	
+	IsAbout <<NaturalPerson>>	The evidence subject, namly the natural person which the evidence is about.	0..1	Person	Must contain either a IsAbout <<NaturalPerson>> or <<LegalPerson>> but **NOT** both.	cpv:Person	
+	IsAbout <<LegalPerson>>	The evidence subject, namly the legal entity which the evidence is about.	0..1	Legal Person	Must contain either a IsAbout <<NaturalPerson>> or <<LegalPerson>> but **NOT** both.	cbv:LegalEntity	
+	IssuingAuthority	The evidence provider, namely the agent that is issuing the evidence.	1..1	Agent		dct:Agent	
+	IsConformantTo	Relation to an Evidence Type. An Evidence Type is a type of evidence that can be provided to meet a requirement, within a certain jurisdiction.	1..1	EvidenceType		cccev:EvidenceType	
+	IssuingDate	The date and time the evidence has	1..1	Date	BR-OOTS-RESP-017	dct:issued	

	Name	Definition	Cardinality	Type	Rules	Core Vocabulary	Notes
		been issued by the Evidence Provider.					
+	Distribution	The kind of distributions that are expected as response to this request.	1..1	Distribution		dcat:distribution	
+	ValidityPeriod	The validity period of the evidence ensured by the Evidence Provider.	0..1	Period		dct:PeriodOfTime	
++	IsAbout <<NaturalPerson>>	The evidence subject, namly the natural person or legal entity which the evidence is about.	0..1	Person	Must contain either a IsAbout <<NaturalPerson>> or <<LegalPerson>> but **NOT** both.	cpv:Person	
+++	Identifier	The unique identifier provided by eIDAS to identify the Natural Person. Example: ES/AT/02635542Y	0..1	Identifier	BR-OOTS-RESP-028, BR-OOTS-RESP-029, BR-OOTS-RESP-030,	cpv:identifer	
++++	Identifier/@schemeID	The schemeID of this identifier. Fixed value: eidas	M	Code	BR-OOTS-RESP-031, BR-OOTS-RESP-032	cpv:identifier	
+++	FamilyName	The hereditary surname of a family.	1..1	Text		cpv:familyName	

	Name	Definition	Cardinality	Type	Rules	Core Vocabulary	Notes
+++	GivenName	The name(s) that identify the Person within a family with a common surname.	1..1	Text		cpv:givenName	
+++	DateOfBirth	The point in time on which the Person was born.	1..1	Date	BR-OOTS-RESP-033	cpv:dateOfBirth	
++	IsAbout <<LegalPerson>>	The evidence subject, namly the natural person or legal entity which the evidence is about.	0..1	Legal Person	Must contain either a IsAbout <<NaturalPerson>> or <<LegalPerson>> but **NOT** both.	cbv:LegalEntity	
+++	LegalPersonIdentifier	The unique identifier provided by eIDAS to identify the Legal Entity. Example: ES/AT/02635542Y	0..1	Identifier	BR-OOTS-RESP-034, BR-OOTS-RESP-035, BR-OOTS-RESP-036	cbv:identifier	
++++	LegalPersonIdentifier/@schemeID	The schemeID of this identifier. Fixed value: eidas	M	Code	BR-OOTS-RESP-037, BR-OOTS-RESP-038	cbv:identifier	
+++	LegalName	The name under which the Legal Entity is legally registered.	1..1	Text		cbv:legalName	
++	IssuingAuthority	The evidence provider, namely the agent that is	1..1	Agent		dct:Agent	

	Name	Definition	Cardinality	Type	Rules	Core Vocabulary	Notes
		issuing the evidence.					
+++	Identifier	The identifier of the Issuing Authority.	1..1	Identifier		dct:identifier	
++++	Identifier/@schemeID	Scheme identifier for the agent identification.	M	Code	BR-OOTS-RESP-039, BR-OOTS-RESP-040	dct:identifier	
+++	Name	The name of the Issuing Authority	1..1	Text		dct:title	
++	IsConformantTo	Relation to an Evidence Type. An Evidence Type is a type of evidence that can be provided to meet a requirement, within a certain jurisdiction.	1..1	EvidenceType		cccev:EvidenceType	
+++	EvidenceTypeClassification	An URI pointing to the Evidence Type that has been provided. The classification is linking with the Evidence Type of the Semantic Repository (Evidence Broker).	1..1	Code	BR-OOTS-RESP-018	cccev:evidenceTypeClassification	Core Criterion Core Evidence Vocabulary
+++	Title	A name to identify in common	1..n	Text		dct:title	

	Name	Definition	Cardinality	Type	Rules	Core Vocabulary	Notes
		language the Evidence Type. Unbounded cardinality to support multiple languages.					
++++	Title/@lang	The language of the title encoded as ISO 639-1 two-letter code. Default value "en"	M	Code	BR-OOTS-RESP-019, BR-OOTS-RESP-020	dct:title	
+++	Description	A description of the Evidence Type. Unbounded cardinality to support multiple languages.	0..n	Text		dct:description	
++++	Description/@lang	The language of the description encoded as ISO 639-1 two-letter code. Default value "en"	M	Code	BR-OOTS-RESP-021, BR-OOTS-RESP-022	dct:description	
++	Distribution	A concrete representation of the Evidence that is transported through the OOP Technical System as part of	1..1	Distribution		dcat:distribution	

	Name	Definition	Cardinality	Type	Rules	Core Vocabulary	Notes
		the response to the request.					
+++	ConformsTo	A registered schema or conformance profile in the OOTS semantic repository to which the distributed evidence conforms.	0..1	URI	BR-OOTS-RESP-023	dct:conformsTo	The element's value is a persistent URL, pointing to an entry of the OOTS Semantic Repository that contains all the relevant information of such a profile.
+++	Format	The technical representation of the evidence. Declaration of the file types that provide structured content like PDF, XML, JSON, RDF etc	1..1	Code	BR-OOTS-RESP-024	dct:format	
+++	PackagingFormat	The format that is used to group the content of the evidence together.	0..1	Code	BR-OOTS-RESP-025	dct:MediaType	

	Name	Definition	Cardinality	Type	Rules	Core Vocabulary	Notes
+++	CompressionFormat	The format that is used to compress the content of the evidence.	0..1	Code	BR-OOTS-RESP-026	dct:MediaType	
+++	Language	The language(s) in which the evidence is provided.	0..n	Code	BR-OOTS-RESP-027	dct:LinguisticSystem	
++	ValidityPeriod	The validity period of the evidence ensured by the Evidence Provider.	0..1	Period		dct:PeriodOfTime	
+++	StartDate	The start date of the validity period. The start date time must have granularity of seconds, and include time zone information.	1..1	Date	BR-OOTS-RESP-041	schema:startDate	
+++	EndDate	The start date of the validity period. The start date time must have granularity of seconds, and include time zone information.	1..1	Date	BR-OOTS-RESP-042	schema:endDate	

The `EvidenceMetadata` Slot has a SlotValue of type AnyValueType containing an Evidence class. The DCAT Application profile is used for representing each XML element.
The Evidence class contains:

- The Unique Identifier of the issued evidence

- A reference to the EvidenceType to which the Evidence is conformant to
- The Evidence Subject in the "IsAbout" element, either a natural or a legal person;
- The Distribution class, which includes:
    - The Format, conformance and locale code as defined in the SDG Application Profile.
    - The Transformation applied to the evidence, if any.
- The Issuing Body which uses the Agent class from the SDG Application Profile using the Vocabulary's Agent class:
    - This includes an identifier, the name and an address.
- The document's issue date;
- Language(s) used in the specific included evidence;
- Optionally, a validity period, specified in the temporal element with a start and end date.

When using a Core Vocabulary for representing the value of each element, AnyValueType is used as its type since it allows data in XML format to be used as the slot's value.

```
 <!--   EvidenceMetadata Slot  -->
 <rim:Slot name="EvidenceMetadata">
    <rim:SlotValue xsi:type="rim:AnyValueType">
        <sdg:Evidence>
            <Identifier>37a169f1-9cf6-4aa8-ac24-b083fa569173</Identifier>
            <IsAbout>
            <!--
                Must contain at least the Minimum Data Set part of the
                evidence Subject attributes to confirm identity matching
                Must contain either a IsAbout <<NaturalPerson>> or <<LegalPerson>> but NOT both.
            -->
                <NaturalPerson>
                    <!-- The identifier of the user retrieved through the EvidenceRequest from eIDAS -->
                    <Identifier schemeID="eidas">DK/DE/123456</Identifier>
                    <!-- Mandatory Minimum Data Set -->
                    <FamilyName>Smith</FamilyName>
                    <GivenName>John</GivenName>
                    <DateOfBirth>1985-09-09</DateOfBirth>
                </NaturalPerson>
            </IsAbout>

            <!-- The issuing authority which might be different from the evidence provider e.g. if the evidence provider acts
as intermediary platform for data services -->
            <IssuingAuthority>
                <Identifier schemeID="9930">DE73524311</Identifier>
                <Name lang="en">Civil Registration Office Berlin I</Name>
            </IssuingAuthority>

            <!-- Classification Information - Used for linking with the Semantic Repository and Evidence Broker -->
            <IsConformantTo>
                <EvidenceTypeClassification>CertificateOfBirth</EvidenceTypeClassification>
                <Title lang="en">Certificate of Birth</Title>
                <Title lang="de">Geburtsurkunde</Title>
                <Description lang="en">An official certificate of birth of a person - with first name, surname, sex, date and
place of birth, which is obtained from the birth register of the place of birth.</Description>
                <Description lang="de">Eine amtliche Bescheinigung über die Geburt einer Person – mit Vorname, Familienname,
Geschlecht, Datum und Ort der Geburt, welche aus dem Geburtsregister des Geburtsortes erstellt wird.</Description>
            </IsConformantTo>
```

```
            <!-- The issuing date, distribution and validity period of the evidence -->
            <IssuingDate>1985-09-11</IssuingDate>
            <Distribution>
                <Format>application/pdf</Format>
            </Distribution>
            <ValidityPeriod>
                <StartDate>2022-05-20</StartDate>
                <EndDate>2023-05-20</EndDate>
            </ValidityPeriod>
        </sdg:Evidence>
    </rim:SlotValue>
</rim:Slot>
```

4.5.4 Evidence Error Response Syntax Mapping - June 2022

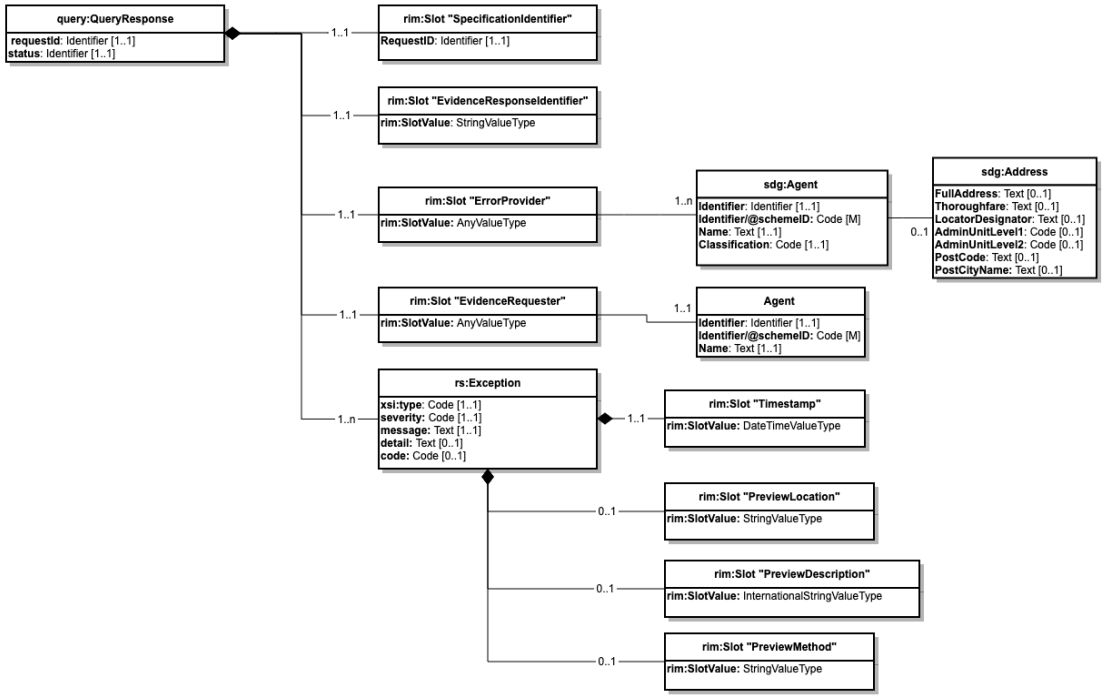
4.5.4.1 Exchange Data Model: QueryResponseError (EDM Error Response)

The following exchange data model provides an overview of the information entities and information elements contained in the EDM Error Response.

This guideline explains how to use the ebRS QueryResponse using the ebRS RegistryExceptionType syntax to implement the Business Requirements (Req ID) described for the EDM Error Response. The guideline provides specific details for each class and information elements including the underlying standards, data types and cardinalities to produce conformant XML documents. In the following sections, we describe the XML serialization of the EDM Error Response in the same hierarchical order of the corresponding Exchange Data Model.

The Exchange Data Model in the figure below provides an overview of the information elements and their associations contained in the EDM Error Response. An EDM Error Response is a message created by the Evidence Provider (EP) containing all the necessary parameters to perform the following actions:

- to either negatively respond to an Evidence Request due to an exception arising at the Error Provider (e.g. Evidence Provider or Gateway) or
- to return information about the preview location and to pause an "Evidence Response" until the data subject has agreed, in that preview location, to the use evidence.



To form a valid EDM Error Response at least the following elements are required:

- the "requestID" of the QueryRequest;
- the "status" of the QueryResponse;
- the "EvidenceResponseIdentifier" providing a unique identifier of the Response Message;
- the "SpecificationIdentifier" to identify the version of this specification;
- the "ErrorProvider" to describe the entity that is technically responsible for creating the QueryResponse;
- the "EvidenceRequester" to describe the entity that is technically responsible for receiving the QueryResponse;

- the "Exception" is described through several mandatory codes and error messages. Each "Exception" must contain:
    - the "Timestamp" of the exception.

4.5.4.2 ebRIM Definition of the QueryResponseError (EDM Error Response)

This section defines the core ebRIM elements of the ebRS RegistryExceptionType that are used to compose a QueryResponseError (EDM Error Response). It thereby distinguishes between attributes and slots to define the Evidence Response:

Attribute Definition: The table provides an overview of the mandatory attributes and the information they contain for each QueryResponse according to the ebRIM element.

Slot definition: The elements provide an overview of the defined ebRIM SlotType instances, which have a name and a value. The value is of type ValueType. Most rim:Slots do not contain sub-properties other than the SlotValue itself, except if they are collections. Collections refer to sources such as Core Vocabularies and a corresponding class defined in the SDGR Application Profile (see section 3).

Legend
The tables below represent the tree structure of the EDM. Light grey rows open classes and define ther properties and attributes. Light green rows soley illustrate the classes that are subordinated to a class and illustrate the tree structure. Light green rows are then repeated as light grey rows to describe properties and attributes of the class. The hierarchy of the tree structure is also indicated in the first column via the '+' symbol.

	Name	Definition	Cardinality	ebRIM type	Data Type	BusinessRules	Mapping to the class of SDGR Application Profile	Mapping to Core Vocabulary
	query:QueryResponse	**EDM Error Response root element**		RegistryResponseType		Structure: BR-OOTS-ERR-ebRIM-009		
+	requestId	The unique identifier of the Evidence Request. Must be the same as the id attribute of the	1..1	Attribute	Identifier	Use: BR-OOTS-ERR-001	-	-

	Name	Definition	Cardinality	ebRIM type	Data Type	BusinessRules	Mapping to the class of SDGR Application Profile	Mapping to Core Vocabulary
		QueryRequest that generated this QueryResponse.						
+	status	Element used to define the status of the Evidence Response.	1..1	Attribute	Identifier	Use: BR-OOTS-ERR-002	-	-
++	SpecificationIdentifier	An identification of the specification for the EDM Error Response containing the total set of rules regarding semantic content, cardinalities and business rules to which the data contained in the instance document conforms.	1..1	SlotType	StringValueType	Structure: BR-OOTS-ERR-ebRIM-001, BR-OOTS-ERR-ebRIM-010 Use: BR-OOTS-ERR-003	-	-
++	EvidenceResponseIdentifier	The unique identifier of the Evidence Response error message.	1..1	SlotType	StringValueType	Structure: BR-OOTS-ERR-ebRIM-002, BR-OOTS-	-	-

	Name	Definition	Cardinality	ebRIM type	Data Type	BusinessRules	Mapping to the class of SDGR Application Profile	Mapping to Core Vocabulary
						ERR-ebRIM-011 Use: BR-OOTS-ERR-004		
++	ErrorProvider	The Agent or organisation that returns the error message. In most cases the Error Provider is the Evidence Provider informing the Evidence Requester about a failed response or additional information or to perform a preview. However, in the case of multiple national routings, an error might be created by an intermediate as well.	1..n	SlotType	AnyValueType	Structure: BR-OOTS-ERR-ebRIM-003, BR-OOTS-ERR-ebRIM-012	Agent	Core Public Service Vocabulary Application Profile

	Name	Definition	Cardinality	ebRIM type	Data Type	BusinessRules	Mapping to the class of SDGR Application Profile	Mapping to Core Vocabulary
++	EvidenceRequester	The Agent or organisation that is requesting the evidence.	1..1	SlotType	AnyValueTpye	Structure: BR-OOTS-ERR-ebRIM-004, BR-OOTS-ERR-ebRIM-013	Agent	Core Public Service Vocabulary Application Profile
++	**rs:Exception**	**The rs:exception describes an error which occurs during the processing of an EvidenceRequest.**	1..n	RegistryExceptionType		Use: BR-OOTS-ERR-013		
+++	xsi:type	Describes the nature of the error that occurred.	1..1	Attribute	string	Use: BR-OOTS-ERR-014, BR-OOTS-ERR-015	-	-
+++	severity	Is used to show the impact of the error with regard to the business process. Use the severity codes WARNING or	1..1	Attribute	objectReferenceType	Use: BR-OOTS-ERR-016, BR-OOTS-ERR-017	-	-

	Name	Definition	Cardinality	ebRIM type	Data Type	BusinessRules	Mapping to the class of SDGR Application Profile	Mapping to Core Vocabulary
		FAILURE to scope the impact of the error.						
+++	message	Is used to add an error message that can be shown and understood by the user of the system. The element is particularly important when you return a generic error code.	1..1	Attribute	string	Use: BR-OOTS-ERR-018	-	-
+++	detail	Is used to describe technical details of the error that might be needed to identify and debug the error.	0..1	Attribute	string		-	-
+++	code	A code that corresponds to the status of the system with regard to the processing of a request. If the specific error codes do not cover	0..1	Attribute	string	Use: BR-OOTS-ERR-019	-	-

	Name	Definition	Cardinality	ebRIM type	Data Type	BusinessRules	Mapping to the class of SDGR Application Profile	Mapping to Core Vocabulary
		the reason for failure use the generic error code "other".						
++ +	rim:Slot "Timestamp"	The timestamp shows when this error has been generated.	1..1	SlotType	DateTimeValueType	Structure: BR-OOTS-ERR-ebRIM-005, BR-OOTS-ERR-ebRIM-014 Use: BR-OOTS-ERR-020	-	-
++ +	rim:Slot "PreviewLocation"	The PreviewLocation element is used for expressing the location of the Preview Space for the evidence request.	0..1	SlotType	StringValueType	Structure: BR-OOTS-ERR-ebRIM-006, BR-OOTS-ERR-ebRIM-015 Use: BR-OOTS-ERR-021	-	-
++ +	rim:Slot "PreviewDescription"	The PreviewDescription element is used to provide additional	0..1	SlotType	InternationalStringValueType	Structure: BR-OOTS-ERR-ebRIM-007, BR-OOTS-	-	-

	Name	Definition	Cardinality	ebRIM type	Data Type	BusinessRules	Mapping to the class of SDGR Application Profile	Mapping to Core Vocabulary
		explanatory information for the use of Preview Space.				ERR-ebRIM-016 Use: BR-OOTS-ERR-022		
++ +	rim:Slot "PreviewMethod"	The PreviewMethod element is used for expressing the HTTP verb to access the Preview Space.	0..1	SlotType	StringValueType	Structure: BR-OOTS-ERR-ebRIM-008, BR-OOTS-ERR-ebRIM-017 Use: BR-OOTS-ERR-023	-	-

4.5.4.2.1 ebRIM QueryResponseError example

The EDM Error Responses are syntactically expressed inside an ebRS QueryResponse using the ebRS RegistryExceptionType as shown in the example below:

```
<?xml version="1.0" encoding="UTF-8"?>
<query:QueryResponse xmlns:rim="urn:oasis:names:tc:ebxml-regrep:xsd:rim:4.0"
    xmlns:query="urn:oasis:names:tc:ebxml-regrep:xsd:query:4.0"
    xmlns:sdg="http://data.europa.eu/p4s"
    xmlns:rs="urn:oasis:names:tc:ebxml-regrep:xsd:rs:4.0"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns:xlink="http://www.w3.org/1999/xlink"
    requestId="4ffb5281-179d-4578-adf2-39fd13ccc797"
    status="urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Failure">

    <!-- Additional slots describing the response are omitted for clarity -->

    <rs:Exception xsi:type="rs:ObjectNotFoundExceptionType" severity="FAILURE"
        message="No data found." detail="No data could be found for the Legal Person with ID 1234."
        code="GEN">

        <!-- Additional slots describing the exception and the preview if required -->

    </rs:Exception>

</query:QueryResponse>
```

Code Block 1 EDM Error Example

One or more **rs:Exception** elements **(1..n)** can be put inside a QueryResponse.

In the following table, the list of all available ebRS Protocol Exceptions is provided that must be returned as xsi:type of the rs:Exception.

EXCEPTION TYPE	DESCRIPTION
AuthenticationExceptionType	Generated when a client sends a request with authentication credentials and the authentication fails for any reason.
AuthorizationExceptionType	Generated when a client sends a request to the server for which it is not authorized.
InvalidRequestExceptionType	Generated when a client sends a request that is syntactically or semantically invalid.
ObjectExistsExceptionType	Generated when a SubmitObjectsRequest attempts to create an object with the same id as an existing object and the mode is “CreateOnly”.

EXCEPTION TYPE	DESCRIPTION
ObjectNotFoundExceptionType	Generated when a QueryRequest expects an object but it is not found in the server.
QuotaExceededExceptionType	Generated when a request exceeds a server-specific quota for the client.
ReferencesExistExceptionType	Generated when a RemoveObjectRequest attempts to remove a RegistryObject while references to it still exist.
TimeoutExceptionType	Generated when the processing of a request exceeds a server-specific timeout period.
UnresolvedReferenceExceptionType	Generated when a request references an object that cannot be resolved within the request or to an existing object in the server.
UnsupportedCapabilityExceptionType	Generated when a request attempts to use an optional feature or capability that the server does not support.
QueryExceptionType	Generated when the query syntax or semantics were invalid. The client must fix the query syntax or semantic error and re-submit the query.

4.5.4.2.2 Specification Identifier example

The SpecificationIdentifier element is used for expressing the version of the specification used for creating the referred document.

A Slot with the name of "SpecificationIdentifier" is used with the ValueType of StringValueType.

```
<!-- SpecificationIdentifier Slot -->
<rim:Slot name="SpecificationIdentifier">
    <rim:SlotValue xsi:type="rim:StringValueType">
        <rim:Value>oots-edm:v1.0</rim:Value>
    </rim:SlotValue>
</rim:Slot>
```

4.5.4.2.3 Evidence Response Identifier example

The `EvidenceResponseIdentifier` element is used for expressing the Unique Identifier of the response generated by the evidence provider.

A Slot with the name of "EvidenceResponseIdentifier" is used with the ValueType of StringValueType.

```
<!-- EvidenceResponseIdentifier Slot -->
 <rim:Slot name="EvidenceResponseIdentifier">
     <rim:SlotValue xsi:type="rim:StringValueType">
         <rim:Value>530ad1e2-5eaf-4a9a-8192-227432eea95d</rim:Value>
     </rim:SlotValue>
 </rim:Slot>
```

4.5.4.2.4 Timestamp example

The Timestamp element is used for expressing the creation date and time of the referenced error.

A Slot with the name of "Timestamp" is used with the ValueType of DateTimeValueType which has the value of ISO timestamp.

```
<!-- TimeStamp -->
 <rim:Slot name="Timestamp">
     <rim:SlotValue xsi:type="rim:DateTimeValueType">
         <rim:Value>2020-02-14T19:20:30+01:00</rim:Value>
     </rim:SlotValue>
 </rim:Slot>
```

4.5.4.2.5 PreviewLocation example

The PreviewLocation element is used for expressing the location of the Preview Space for the evidence request.

A Slot with the name of "PreviewLocation" is used with the ValueType of StringValueType which has the value of a URI.

```
<!-- Preview Location -->
 <rim:Slot name="PreviewLocation">
     <rim:SlotValue xsi:type="rim:StringValueType">
         <rim:Value>https://preview.space.example.com/requests?session=d36af8bc-fea6-4ee5-a32d-5bef82cdb071</rim:Value>
     </rim:SlotValue>
 </rim:Slot>
```

4.5.4.2.6 PreviewDescription example

The PreviewDescription element is used to provide additional explanatory information for the use of Preview Space. It provides text in possibly multiple natural languages that can be displayed to the user by the Online Procedure Portal.

A Slot with the name of "PreviewDescription" is used with the ValueType of InternationalStringValueType.

```
<!-- Preview Description -->
 <rim:Slot name="PreviewDescription">
     <rim:SlotValue xsi:type="rim:InternationalStringValueType">
         <rim:Value>
             <rim:LocalizedString xml:lang="nl" value="Kies uw diploma."/>
             <rim:LocalizedString xml:lang="ro" value="Vă rugăm să selectaţi diploma dvs."/>
             <rim:LocalizedString xml:lang="en" value="Please select your diploma."/>
             <rim:LocalizedString xml:lang="en" value="Bitte wählen Sie Ihr Diplom aus."/>
          </rim:Value>
     </rim:SlotValue>
 </rim:Slot>
```

4.5.4.2.7 PreviewMethod example

The PreviewMethod element is used for expressing the HTTP verb to access the Preview Space.

A Slot with the name of "PreviewMethod" is used with the ValueType of StringValueType which has the value of a either "GET" or "POST".

```
<!-- Preview Method -->
 <rim:Slot name="PreviewMethod">
     <rim:SlotValue xsi:type="rim:StringValueType">
         <rim:Value>GET</rim:Value>
     </rim:SlotValue>
 </rim:Slot>
```

4.5.4.3 SDGR Application Profile for the EDM Error Response

The SDGR application profile for the EDM Error Response defines the semantics of the previously introduced rim:Slots defined as a collection (green components) of the Evidence Response Message. The SDGR application profile for the EDM Error Response describes how the SDG-Generic-Metadata Profile (SDG-syntax) is profiled in ebRIM in order to compose a valid QueryResponse. It therefore contains a mapping to the underlying SDG-syntax elements and necessary parameters for providing the EDM Error Response on the basis of an earlier Evidence Request. Thus, the values for several parameters are obtained from the Evidence Provider that is responding to the Evidence Request. The namespace of the SDG-syntax is https://data.europa.eu/p4s. In the following samples, the prefix "sdg" is assumed to be linked to the namespace http://data.europa.eu/p4s.

4.5.4.3.1 Error Provider slot and example

Element to describe the organisation or agent that is providing the error. In most cases the Error Provider is the Evidence Provider informing the Evidence Requester about a failed response or additional information or to preform a preview. However, in case of multiple national routings an error might be created by an intermediate as well or by a businesses that has been accredited to supply the evidence.

	Name	Definition	Cardinality	Type	BusinessRules	Core Vocabulary	Notes
	Agent	The Agent or organisation that is providing the evidence.	1..n	Agent		dct:Agent	Core Public Service Vocabulary Application Profile
+	Identifier	A unique identification for the agent.	1..1	Identifier		dct:identifier	
++	Identifier/@schemeID	Scheme identifier for the agent identification	M	Code	BR-OOTS-ERR-005, BR-OOTS-ERR-006	dct:identifier	
+	Name	A short label for the agent.	1..1	Text		dct:title	
+	Classification	A code to classify the agents associated to the communication. In case there are multiple agents the codes must be used to distinguish between the actual Error Provider and Intermediary Platforms that are involved in the transaction. Default value: ErrorProvider	1..1	Code	BR-OOTS-ERR-009	cv:role	
+	Address	A location of the Evidence Provider in the form of an address.	0..1	Address		locn:Address	Core Location Vocabulary
++	Address	A location of the Evidence Provider in the form of an address.	0..1	Address		locn:Address	Core Location Vocabulary
+++	fullAddress	The complete address written as a string.	0..3	Text		locn:fullAddress	
+++	thoroughfare	The name of a street, passage or way through from one location to another.	0..1	Text		locn:thoroughfare	

	Name	Definition	Cardinality	Type	BusinessRules	Core Vocabulary	Notes
+++	locatorDesignator	A number or sequence of characters that uniquely identifies the locator (building number, apartment number, etc.) within the relevant scope.	0..1	Text		locn:locatorDesignator	
+++	adminUnitL1	The name of the uppermost level of the address, almost always a country.	0..1	Code	BR-OOTS-ERR-007	locn:adminUnitL1	
+++	adminUnitL2	The name of a secondary level/region of the address, usually a county, state or other such area that typically encompasses several localities.	0..1	Code	BR-OOTS-ERR-008	locn:adminUnitL2	
+++	postCode	The code created and maintained for postal purposes to identify a subdivision of addresses and postal delivery points.	0..1	Code		locn:postCode	

The Error Provider element is expressed using a Slot with the name of "ErrorProvider" and ValueType of AnyValueType in order to express the information using the Core Public Service Vocabulary Application Profile. The Error Provider information inside the AnyValueType Slot is expressed using the Agent Class elements.

```
<!--   ErrorProvider Slot -->
<rim:Slot name="ErrorProvider">
    <rim:SlotValue xsi:type="rim:AnyValueType">
            <sdg:Agent >
                <Identifier schemeID="0204">DE7657587001</Identifier>
                <Name>Authority for school and occupational training</Name>
                <Address>
                    <sdg:FullAddress>Hamburger Str. 31</sdg:FullAddress>
                    <sdg:LocatorDesignator>31</sdg:LocatorDesignator>
                    <sdg:PostCode>22083</sdg:PostCode>
                    <sdg:PostCityName>Hamburg</sdg:PostCityName>
                    <sdg:AdminUnitLevel1>DE</sdg:AdminUnitLevel1>
                    <sdg:AdminUnitLevel2>DE60</sdg:AdminUnitLevel2>
                </Address>
                <Classification>ErrorProvider</Classification>
            </sdg:Agent>
    </rim:SlotValue>
</rim:Slot>
```

4.5.4.3.2 Evidence Requester

Element to describe the organisation or agent that has requested the evidence. The agent requests the evidence, by sending an evidence request to the evidence provider, on behalf of the evidence subject. In several cases it might be a portal/organisation that initiates the evidence request. However, the response must be returned to the Evidence Requester that initiated the evidence request and not to the portal /intermediary in case there are more than one Evidence Requesters named in the evidence request.

No central registry of evidence requesters is required, only the minimal details required to enable legal logging of requests or facilitate the processing of the evidence request.

	Name	Definition	Cardinality	Type	BusinessRules	Core Vocabulary	Notes
	Agent	The Agent or organisation that is requesting the evidence.	1..1	Agent		dct:Agent	Core Public Service Vocabulary Application Profile

	Name	Definition	Cardinality	Type	BusinessRules	Core Vocabulary	Notes
+	Identifier	A unique identification for the agent.	1..1	Identifier	BR-OOTS-ERR-011, BR-OOTS-ERR-012	dct:identifier	
++	Identifier/@schemeID	Scheme identifier for the agent identification	M	Code	BR-OOTS-ERR-011, BR-OOTS-ERR-012	dct:identifier	
+	Name	A short label for the agent.	1..1	Text		dct:title	

The Evidence Requester element is used to describe an organisation that requests data or documents from Evidence Providers.

A Slot with the name of "EvidenceRequester" is used with the ValueType of AnyValueType which accepts any xml representation. In this particular case, the Agent class of the Core Public Service Vocabulary Application Profile is used for the expression of the Evidence Requester information inside the AnyValueType Slot.

```
<!--   Evidence Requester  -->
<rim:Slot name="EvidenceRequester">
    <rim:SlotValue xsi:type="rim:AnyValueType">
        <sdg:Agent>
            <Identifier schemeID="0190">NL22233223</Identifier>
            <Name>Dutch University Portal</Name>
        </sdg:Agent>
    </rim:SlotValue>
</rim:Slot>
```

4.5.5 OOTS-EDM XML Examples of the Evidence Exchange- June 2022

4.5.5.1 Introduction

In this section, some examples for the evidence exchange using the OOTS Exchange Data Model are provided. The Request-Response samples can be found in the OOTS-EDM/XML folder of the tdd_chapters git repository.

4.5.5.2 Example for requesting a birth certificate

In this example, we consider the case of a natural person that needs to provide a prove of birth. Therefore an Evidence Requester is requesting a birth certificate on behalf of the natural person. To do this, an Evidence Request is sent, which contains information about who is participating in this data

exchange and which DataServiceEvidenceType is required. The information about the required DataServiceEvidenceType has been received from the DSD. The request is sent to a service that can provide the evidence (Evidence Provider). The Evidence Provider then sends back to the Evidence Requester an Evidence Response that contains the certificates that has been requested. The example can be also found in the git repository.

4.5.5.2.1 Step 1: Evidence Request Header and Evidence Request

The sender of the Evidence Request uses an ebMS message header that contains the Access Point identifiers as sender and receiver. Using an eDelivery AS4 profile enhancement, however, the outer corners, i.e. the Evidence Requester (originalSender) and Evidence Provider (finalRecipient), can be included in the ebMS message header. For the identification of the Access Points in the ebMS message header, i.e. the values to be used in the `/PartyInfo/To/PartyId` element are extracted from the DSD Response. The Evidence Request itself is referenced in the `/PayloadInfo` element. More information about the ebMS message header can be found at in the eDelivery Configuration.

```xml
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Messaging mustUnderstand="false" xmlns="http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/">
    <UserMessage>
        <PartyInfo>
            <From>
                <PartyId type="urn:oasis:names:tc:ebcore:partyid-type:unregistered:oots-simulator"
                    >urn:oasis:names:tc:ebcore:partyid-type:unregistered:C2</PartyId>
                <Role>http://sdg.europa.eu/edelivery/gateway</Role>
            </From>
            <To>
                <PartyId type="urn:oasis:names:tc:ebcore:partyid-type:unregistered:oots-simulator"
                    >urn:oasis:names:tc:ebcore:partyid-type:unregistered:C3</PartyId>
                <Role>http://sdg.europa.eu/edelivery/gateway</Role>
            </To>
        </PartyInfo>
        <CollaborationInfo>
            <Service type="urn:oasis:names:tc:ebcore:ebrs:ebms:binding:1.0">QueryManager</Service>
            <Action>ExecuteQueryRequest</Action>
            <ConversationId>c73b7fdc-1ab0-4b1e-b295-ac9e4a35d764</ConversationId>
        </CollaborationInfo>
        <MessageProperties>
            <Property name="originalSender">urn:oasis:names:tc:ebcore:partyid-type:unregistered:C1</Property>
            <Property name="finalRecipient">urn:oasis:names:tc:ebcore:partyid-type:unregistered:C4</Property>
        </MessageProperties>
        <PayloadInfo>
            <PartInfo href="cid:regreprequest@example.oots.eu">
                <Schema/>
                <PartProperties>
                    <Property name="MimeType">application/x-ebrs+xml</Property>
                    <Property name="PayloadName">request.xml</Property>
                </PartProperties>
            </PartInfo>
        </PayloadInfo>
    </UserMessage>
</Messaging>
```

Code Block 2 Step 1: XML example of the ebMS message header for the Evidence Request

The Evidence Request itself contains information about the Evidence Requester who is requesting the birth certificate for a natural person from the Evidence Provider based on the underlying procedure and requirements. More information about how this information is represented within the XML document can be found in the Evidence Request Syntax Mapping.

```
<?xml version="1.0" encoding="UTF-8"?>
<query:QueryRequest xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                    xmlns:rs="urn:oasis:names:tc:ebxml-regrep:xsd:rs:4.0"
                    xmlns:sdg="http://data.europa.eu/p4s"
                    xmlns:xmime="http://www.w3.org/2005/05/xmlmime"
                    xmlns:rim="urn:oasis:names:tc:ebxml-regrep:xsd:rim:4.0"
                    xmlns:query="urn:oasis:names:tc:ebxml-regrep:xsd:query:4.0"
                    xmlns:xlink="http://www.w3.org/1999/xlink"
                    xmlns:xml="http://www.w3.org/XML/1998/namespace"
                    id="4ffb5281-179d-4578-adf2-39fd13ccc797">

    <rim:Slot name="SpecificationIdentifier">
        <rim:SlotValue xsi:type="rim:StringValueType">
            <rim:Value>oots-edm:v1.0</rim:Value>
        </rim:SlotValue>
    </rim:Slot>
    <rim:Slot name="IssueDateTime">
        <rim:SlotValue xsi:type="rim:DateTimeValueType">
            <rim:Value>2022-05-19T17:08:10.872Z</rim:Value>
        </rim:SlotValue>
    </rim:Slot>
    <rim:Slot name="Procedure">
        <rim:SlotValue xsi:type="rim:InternationalStringValueType">
            <rim:Value>
                <rim:LocalizedString xml:lang="en"
                                     value="Requesting a birth certificate"/>
            </rim:Value>
        </rim:SlotValue>
    </rim:Slot>
    <rim:Slot name="PossibilityForPreview">
        <rim:SlotValue xsi:type="rim:BooleanValueType">
            <rim:Value>false</rim:Value>
        </rim:SlotValue>
    </rim:Slot>
    <rim:Slot name="ExplicitRequestGiven">
        <rim:SlotValue xsi:type="rim:BooleanValueType">
            <rim:Value>true</rim:Value>
        </rim:SlotValue>
    </rim:Slot>
```

```
<rim:Slot name="Requirements">
    <rim:SlotValue xsi:type="rim:CollectionValueType"
                   collectionType="urn:oasis:names:tc:ebxml-regrep:CollectionType:Set">
    <rim:Element xsi:type="rim:AnyValueType">
        <rim:Requirement>
           <Identifier>315cfd75-6605-49c4-b0fe-799833b41099</Identifier>
           <Name lang="en">Proof of Birth</Name>
        </rim:Requirement>
    </rim:Element>
    </rim:SlotValue>
</rim:Slot>
<rim:Slot name="EvidenceRequester">
    <rim:SlotValue xsi:type="rim:CollectionValueType">
        <rim:Element xsi:type="rim:AnyValueType">
            <sdg:Agent>
                <sdg:Identifier schemeID="0096">DK22233223</sdg:Identifier>
                <sdg:Name lang="en">Denmark University Portal</sdg:Name>
                <sdg:Classification>IntermediaryPlatform</sdg:Classification>
                <sdg:Address>
                    <sdg:FullAddress>Prince Street 15</sdg:FullAddress>
                    <sdg:LocatorDesignator>15</sdg:LocatorDesignator>
                    <sdg:PostCode>1050</sdg:PostCode>
                    <sdg:PostCityName>Copenhagen</sdg:PostCityName>
                    <sdg:AdminUnitLevel1>Denmark</sdg:AdminUnitLevel1>
                    <sdg:AdminUnitLevel2>DK011</sdg:AdminUnitLevel2>
                </sdg:Address>
            </sdg:Agent>
        </rim:Element>
    </rim:SlotValue>
</rim:Slot>
<rim:Slot name="EvidenceProvider">
    <rim:SlotValue xsi:type="rim:AnyValueType">
        <sdg:Agent>
            <sdg:Identifier schemeID="9930">DE73524311</sdg:Identifier>
            <sdg:Name>Civil Registration Office Berlin I</sdg:Name>
        </sdg:Agent>
    </rim:SlotValue>
</rim:Slot>
<query:ResponseOption returnType="LeafClassWithRepositoryItem"/>
```

```
    <query:Query queryDefinition="DocumentQuery">
        <rim:Slot name="NaturalPerson">
            <rim:SlotValue xsi:type="rim:AnyValueType">
                <sdg:Person>
                    <sdg:LevelOfAssurance>High</sdg:LevelOfAssurance>
                    <sdg:Identifier schemeID="eidas">DK/DE/123456</sdg:Identifier>
                    <sdg:FamilyName>Smith</sdg:FamilyName>
                    <sdg:GivenName>John</sdg:GivenName>
                    <sdg:DateOfBirth>1970-03-01</sdg:DateOfBirth>
                    <sdg:Gender>Male</sdg:Gender>
                    <sdg:PlaceOfBirth>Hamburg, Germany</sdg:PlaceOfBirth>
                    <sdg:CurrentAddress>
                        <sdg:FullAddress>Dieter Wellhausen 71</sdg:FullAddress>
                        <sdg:AdminUnitLevel1>DE</sdg:AdminUnitLevel1>
                    </sdg:CurrentAddress>
                </sdg:Person>
            </rim:SlotValue>
        </rim:Slot>
        <rim:Slot name="EvidenceRequest">
            <rim:SlotValue xsi:type="rim:AnyValueType">
                <sdg:DataServiceEvidenceType xmlns="urn:oasis:names:tc:ebxml-regrep:xsd:rim:4.0">
                    <sdg:Identifier>2af27699-f131-4411-8fdb-9e8cd4e8bded</sdg:Identifier>
                    <sdg:EvidenceTypeClassification>CertificateOfBirth</sdg:EvidenceTypeClassification>
                    <sdg:Title lang="en">Certificate of Birth</sdg:Title>
                    <sdg:Title lang="de">Geburtsurkunde</sdg:Title>
                    <sdg:DistributedAs>
                        <sdg:Format>application/pdf</sdg:Format>
                        <sdg:ConformsTo>https://semic.org/sa/common/birthcert-1.0.0</sdg:ConformsTo>
                    </sdg:DistributedAs>
                </sdg:DataServiceEvidenceType>
            </rim:SlotValue>
        </rim:Slot>
    </query:Query>
</query:QueryRequest>
```

Code Block 3 Step 1: XML example of Evidence Request for a birth certificate

4.5.5.2.2 Step 2: Evidence Response Header and Evidence Response

Similar to the request, the sender of the Evidence Response uses an ebMS message header that contains the Access Point identifiers as sender and receiver. Next to the Evidence Request itself the requested evidence object is additionally included to the `/PayloadInfo` element of the ebMS message header. More information about the ebMS message header can be found at in the eDelivery Configuration.

```xml
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Messaging mustUnderstand="false" xmlns="http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/">
    <UserMessage>
        <PartyInfo>
            <From>
                <PartyId type="urn:oasis:names:tc:ebcore:partyid-type:unregistered:oots-simulator"
                    >urn:oasis:names:tc:ebcore:partyid-type:unregistered:C3</PartyId>
                <Role>http://sdg.europa.eu/edelivery/gateway</Role>
            </From>
            <To>
                <PartyId type="urn:oasis:names:tc:ebcore:partyid-type:unregistered:oots-simulator"
                    >urn:oasis:names:tc:ebcore:partyid-type:unregistered:C2</PartyId>
                <Role>http://sdg.europa.eu/edelivery/gateway</Role>
            </To>
        </PartyInfo>
        <CollaborationInfo>
            <Service type="urn:oasis:names:tc:ebcore:ebrs:ebms:binding:1.0">QueryManager</Service>
            <Action>ExecuteQueryResponse</Action>
            <ConversationId>c73b7fdc-1ab0-4b1e-b295-ac9e4a35d764</ConversationId>
        </CollaborationInfo>
        <MessageProperties>
            <Property name="originalSender">urn:oasis:names:tc:ebcore:partyid-type:unregistered:C4</Property>
            <Property name="finalRecipient">urn:oasis:names:tc:ebcore:partyid-type:unregistered:C1</Property>
        </MessageProperties>
        <PayloadInfo>
            <PartInfo href="cid:regrepresponse@example.oots.eu">
                <PartProperties>
                    <Property name="MimeType">application/x-ebrs+xml</Property>
                    <Property name="PayloadName">response.xml</Property>
                </PartProperties>
            </PartInfo>
            <PartInfo href="cid:attachment100001@example.oots.eu">
                <PartProperties>
                    <Property name="MimeType">application/pdf</Property>
                    <Property name="PayloadName">BirthCertificate.pdf</Property>
                </PartProperties>
            </PartInfo>
        </PayloadInfo>
    </UserMessage>
```

```
</Messaging>
```

Code Block 4 Step 2: XML example of ebMS message header for the Evidence Response

The Evidence Response itself contains information about the Evidence Provider who is providing the birth certificate and its associated Evidence Metadata for a natural person based on the Evidence Request issued by the Evidence Requester. The /rim:RepositoryItemRef provides a references to the evidence object in the ebMS message header. More information about how this information is represented within the XML document can be found in the Evidence Response Syntax Mapping.

XML sample of Evidence Response for a birth certificate

```
<?xml version="1.0" encoding="UTF-8"?>

<query:QueryResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns:rs="urn:oasis:names:tc:ebxml-regrep:xsd:rs:4.0"
    xmlns:rim="urn:oasis:names:tc:ebxml-regrep:xsd:rim:4.0"
    xmlns:sdg="http://data.europa.eu/p4s"
    xmlns:query="urn:oasis:names:tc:ebxml-regrep:xsd:query:4.0"
    xmlns:xlink="http://www.w3.org/1999/xlink"
    status="urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Success"
    xmlns:xml="http://www.w3.org/XML/1998/namespace"
    requestId="4ffb5281-179d-4578-adf2-39fd13ccc797">


    <!-- Top Level Slots, providing metadata about the Response and the Evidence Provider -->
    <rim:Slot name="SpecificationIdentifier">
        <rim:SlotValue xsi:type="rim:StringValueType"
                       xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
            <rim:Value>oots-edm:v1.0</rim:Value>
        </rim:SlotValue>
    </rim:Slot>
    <rim:Slot name="EvidenceResponseIdentifier">
        <rim:SlotValue xsi:type="rim:StringValueType"
                       xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
            <rim:Value>166155eb-d7a7-4cac-9086-8a85f0116462</rim:Value>
        </rim:SlotValue>
    </rim:Slot>
    <rim:Slot name="IssueDateTime">
        <rim:SlotValue xsi:type="rim:DateTimeValueType"
                       xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
            <rim:Value>2022-05-19T17:10:10.872Z</rim:Value>
        </rim:SlotValue>
    </rim:Slot>
    <rim:Slot name="EvidenceProvider">
        <rim:SlotValue xsi:type="rim:AnyValueType">
            <sdg:Agent>
                <sdg:Identifier schemeID="9930">DE73524311</sdg:Identifier>
                <sdg:Name lang="en">Civil Registration Office Berlin I</sdg:Name>
                <sdg:Classification>EvidenceProvider</sdg:Classification>
                <sdg:Address>
```

```
                    <sdg:FullAddress>Schönstedtstraße 5</sdg:FullAddress>
                    <sdg:LocatorDesignator>5</sdg:LocatorDesignator>
                    <sdg:PostCode>13357</sdg:PostCode>
                    <sdg:PostCityName>Berlin</sdg:PostCityName>
                    <sdg:AdminUnitLevel1>DE</sdg:AdminUnitLevel1>
                </sdg:Address>
            </sdg:Agent>
        </rim:SlotValue>
    </rim:Slot>
    <rim:Slot name="EvidenceRequester">
        <rim:SlotValue xsi:type="rim:AnyValueType">
            <sdg:Agent>
                <sdg:Identifier schemeID="0096">DK22233223</sdg:Identifier>
                <sdg:Name>Denmark University Portal</sdg:Name>
            </sdg:Agent>
        </rim:SlotValue>
    </rim:Slot>
    <rim:RegistryObjectList>
    <rim:RegistryObject xsi:type="rim:ExtrinsicObjectType" id="555555-740e-4b64-80f0-2462462462">
        <rim:Slot name="EvidenceMetadata">
            <rim:SlotValue xsi:type="rim:AnyValueType">
                <sdg:Evidence>
                    <sdg:Identifier>37a169f1-9cf6-4aa8-ac24-b083fa569173 </sdg:Identifier>
                    <sdg:IsAbout>
                        <sdg:NaturalPerson>
                            <sdg:Identifier schemeID="eidas">DK/DE/123456</sdg:Identifier>
                            <sdg:FamilyName>Smith</sdg:FamilyName>
                            <sdg:GivenName>John</sdg:GivenName>
                            <sdg:DateOfBirth>1970-03-01</sdg:DateOfBirth>
                        </sdg:NaturalPerson>
                    </sdg:IsAbout>
                    <sdg:IssuingAuthority>
                        <sdg:Identifier schemeID="9930">DE73524311</sdg:Identifier>
                        <sdg:Name lang="en">Civil Registration Office Berlin I</sdg:Name>
                    </sdg:IssuingAuthority>
                    <sdg:IsConformantTo>
                        <sdg:EvidenceTypeClassification>CertificateOfBirth</sdg:EvidenceTypeClassification>
                        <sdg:Title lang="en">Certificate of Birth</sdg:Title>
                        <sdg:Title lang="de">Geburtsurkunde</sdg:Title>
```

```
                        <sdg:Description lang="en">Civil status certificate created from the birth register</sdg:Description>
                        <sdg:Description lang="de">Personenstandsurkunde, die aus dem Geburtenregister erstellt
wird</sdg:Description>
                    </sdg:IsConformantTo>
                    <sdg:IssuingDate>1970-03-03</sdg:IssuingDate>
                    <sdg:Distribution>
                        <sdg:Format>application/pdf</sdg:Format>
                    </sdg:Distribution>
                </sdg:Evidence>
            </rim:SlotValue>
        </rim:Slot>
        <!-- The attached Document Provided as Evidence. Points to an AS4 attachment -->
        <rim:RepositoryItemRef xlink:href="cid:attachment100001@example.oots.eu" xlink:title="BirthCertificate"/>
    </rim:RegistryObject>
</rim:RegistryObjectList>
</query:QueryResponse>
```

Code Block 5 Step 2: XML example of Evidence Response for a birth certificate

4.5.5.3 Example for requesting Secondary Education Completition Evidence with Error Response requesting an Evidence Provider side Preview

In this example, we consider the case of a natural person that needs to prove secondary education completition. Therefore an Evidence Requester is requesting a Secondary Education Completition Evidence and its supplement on behalf of the natural person. To do this, an Evidence Request is sent, which contains information about who is participating in this data exchange and which DataServiceEvidenceType is required. The information about the required DataServiceEvidenceType has been received from the DSD. The request is sent to a service that can provide the evidence (Evidence Provider).

Since for this evidence type a preview on the side of the Evidence Provider is required, the Evidence Provider responds with an Error Response who rejects a direct evidence provision and informs the Evidence Requester about the required preview location, location and method provided for the Evidence Provider. The Evidence Requester than redirects the user (natural person) to the corresponding preview location and sends a second Evidence Request after the preview. The Evidence Provider matches the second Evidence Request with the preview results and sends an Evidence Response with the the Secondary Education Completition Evidence and its supplement to the Evidence Requester.

As the ebMS message header has been already introduced in the preview example illustrating the request for a birth certificate it is not repeated here even though it is needed for the message exchange. The complete example can be found in the git repository.

4.5.5.3.1 Step1: Initiating Evidence Request

The initating Evidence Request contains information about the Evidence Requester who is requesting the Secondary Education Completition Evidence for a natural person from the Evidence Provider based on the underlying procedure and requirements. More information about how this information is represented within the XML document can be found in the Evidence Request Syntax Mapping.

```
<?xml version="1.0" encoding="UTF-8"?><query:QueryRequest xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                  xmlns:rs="urn:oasis:names:tc:ebxml-regrep:xsd:rs:4.0"
                  xmlns:sdg="http://data.europa.eu/p4s"
                  xmlns:xmime="http://www.w3.org/2005/05/xmlmime"
                  xmlns:rim="urn:oasis:names:tc:ebxml-regrep:xsd:rim:4.0"
                  xmlns:query="urn:oasis:names:tc:ebxml-regrep:xsd:query:4.0"
                  xmlns:xlink="http://www.w3.org/1999/xlink"
                  xmlns:xml="http://www.w3.org/XML/1998/namespace"
                  id="4ffb5281-179d-4578-adf2-39fd13ccc797">

    <rim:Slot name="SpecificationIdentifier">
        <rim:SlotValue xsi:type="rim:StringValueType">
            <rim:Value>oots-edm:v1.0</rim:Value>
        </rim:SlotValue>
    </rim:Slot>
    <rim:Slot name="IssueDateTime">
        <rim:SlotValue xsi:type="rim:DateTimeValueType">
            <rim:Value>2022-02-14T19:20:30+01:00</rim:Value>
        </rim:SlotValue>
    </rim:Slot>
    <rim:Slot name="Procedure">
        <rim:SlotValue xsi:type="rim:InternationalStringValueType">
            <rim:Value>
                <rim:LocalizedString xml:lang="en"
                                     value="Requesting recognition of diploma"/>
            </rim:Value>
        </rim:SlotValue>
    </rim:Slot>
    <rim:Slot name="PossibilityForPreview">
        <rim:SlotValue xsi:type="rim:BooleanValueType">
            <rim:Value>true</rim:Value>
        </rim:SlotValue>
    </rim:Slot>
    <rim:Slot name="ExplicitRequestGiven">
        <rim:SlotValue xsi:type="rim:BooleanValueType">
            <rim:Value>true</rim:Value>
        </rim:SlotValue>
    </rim:Slot>
    <rim:Slot name="Requirements">
```

```
        <rim:SlotValue xsi:type="rim:CollectionValueType"
                       collectionType="urn:oasis:names:tc:ebxml-regrep:CollectionType:Set">
        <rim:Element xsi:type="rim:AnyValueType">
            <rim:Requirement>
               <Identifier>315cfd75-6605-49c4-b0fe-799833b41099</Identifier>
               <Name lang="en">Proof of Secondary Education Completion</Name>
            </rim:Requirement>
        </rim:Element>
        <rim:Element xsi:type="rim:AnyValueType">
            <rim:Requirement>
               <Identifier>543-cfd75-6605-49c4-b0fe-799833b41111</Identifier>
               <Name lang="en">Proof of Secondary Education Completion Supplemenent Evidence</Name>
            </rim:Requirement>
        </rim:Element>
        </rim:SlotValue>
    </rim:Slot>
    <rim:Slot name="EvidenceRequester">
        <rim:SlotValue xsi:type="rim:CollectionValueType">
            <rim:Element xsi:type="rim:AnyValueType">
                <sdg:Agent>
                    <sdg:Identifier schemeID="0190">NL22233223</sdg:Identifier>
                    <sdg:Name lang="en">University of Amsterdam</sdg:Name>
                    <sdg:Classification>EvidenceRequester</sdg:Classification>
                        <sdg:Address>
                            <sdg:FullAddress>Binnengasthuisstraat 9</sdg:FullAddress>
                            <sdg:LocatorDesignator>9</sdg:LocatorDesignator>
                            <sdg:PostCode>1012</sdg:PostCode>
                            <sdg:PostCityName>Amsterdam</sdg:PostCityName>
                            <sdg:AdminUnitLevel1>NL</sdg:AdminUnitLevel1>
                            <sdg:AdminUnitLevel2>NL329</sdg:AdminUnitLevel2>
                        </sdg:Address>
                </sdg:Agent>
            </rim:Element>
        </rim:SlotValue>
    </rim:Slot>
    <rim:Slot name="EvidenceProvider">
        <rim:SlotValue xsi:type="rim:AnyValueType">
            <sdg:Agent>
                <sdg:Identifier schemeID="0204">DE7657587001</sdg:Identifier>
```

```
            <sdg:Name>Authority for school and occupational training</sdg:Name>
        </sdg:Agent>
    </rim:SlotValue>
</rim:Slot>
<rim:Slot name="EvidenceProviderClassificationValues">
    <rim:SlotValue xsi:type="rim:CollectionValueType">
        <rim:Element xsi:type="rim:AnyValueType">
            <sdg:ClassificationConcept>
                <sdg:Identifier>SecondarySchool</sdg:Identifier>
                <sdg:SupportedValue>
                    <sdg:StringValue>Wilhelm Gymnasium</sdg:StringValue>
                </sdg:SupportedValue>
            </sdg:ClassificationConcept>
        </rim:Element>
        <rim:Element xsi:type="rim:AnyValueType">
            <sdg:ClassificationConcept>
                <sdg:Identifier>YearOfGraduation</sdg:Identifier>
                <sdg:SupportedValue>
                    <sdg:StringValue>1988</sdg:StringValue>
                </sdg:SupportedValue>
            </sdg:ClassificationConcept>
        </rim:Element>
    </rim:SlotValue>
</rim:Slot>
<query:ResponseOption returnType="LeafClassWithRepositoryItem"/>
<query:Query queryDefinition="DocumentQuery">
    <rim:Slot name="NaturalPerson">
        <rim:SlotValue xsi:type="rim:AnyValueType">
            <sdg:Person>
                <sdg:LevelOfAssurance>High</sdg:LevelOfAssurance>
                <sdg:Identifier schemeID="eidas">DK/DE/123456</sdg:Identifier>
                <sdg:FamilyName>Smith</sdg:FamilyName>
                <sdg:GivenName>Jack</sdg:GivenName>
                <sdg:DateOfBirth>1970-03-01</sdg:DateOfBirth>
                <sdg:PlaceOfBirth>Dusseldorf</sdg:PlaceOfBirth>
                <sdg:CurrentAddress>
                    <sdg:FullAddress>Lansstraße 81</sdg:FullAddress>
                    <sdg:AdminUnitLevel1>DE</sdg:AdminUnitLevel1>
                </sdg:CurrentAddress>
```

```
                </sdg:Person>
            </rim:SlotValue>
        </rim:Slot>
        <rim:Slot name="EvidenceRequest">
            <rim:SlotValue xsi:type="rim:AnyValueType">
                <sdg:DataServiceEvidenceType>
                    <sdg:Identifier>487fdfdc-7f92-42bb-a690-dcbd3d65f435</sdg:Identifier>
                    <sdg:EvidenceTypeClassification>SecondaryEducationCompletion</sdg:EvidenceTypeClassification>
                    <sdg:Title lang="en">Secondary Education Completion Evidence</sdg:Title>
                    <sdg:Title lang="de">Nachweis des Sekundarschulabschlusses</sdg:Title>
                    <sdg:DistributedAs>
                        <sdg:Format>application/pdf</sdg:Format>
                        <sdg:ConformsTo>https://semic.org/sa/common/secondary-education-evidence-1.0.0</sdg:ConformsTo>
                    </sdg:DistributedAs>
                </sdg:DataServiceEvidenceType>
            </rim:SlotValue>
        </rim:Slot>
    </query:Query>
</query:QueryRequest>
```

Code Block 6 Step 1: XML example of the initiating Evidence Request for a Secondary Education Completition Evidence

4.5.5.3.2 Step 2: Error Response

The response status provided by the Evidence Provider is declared as failure. The rs:Exception type provided by the Evidence Provider references to an authorization problem which requires a user redirection to a preview location where the user can preview, select and give his consent to use the evidence. Therefore the Evidence provider informs the Evdience Requester about the required preview location, location and method. More information about how this information is represented within the XML document can be found in the Error Response Syntax Mapping.

```
<?xml version="1.0" encoding="UTF-8"?>
<query:QueryResponse xmlns:rim="urn:oasis:names:tc:ebxml-regrep:xsd:rim:4.0"
    xmlns:query="urn:oasis:names:tc:ebxml-regrep:xsd:query:4.0"
    xmlns:sdg="http://data.europa.eu/p4s"
    xmlns:rs="urn:oasis:names:tc:ebxml-regrep:xsd:rs:4.0"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns:xlink="http://www.w3.org/1999/xlink"
    requestId="4ffb5281-179d-4578-adf2-39fd13ccc797"
    status="urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Failure">
    <rim:Slot name="SpecificationIdentifier">
        <rim:SlotValue xsi:type="rim:StringValueType">
            <rim:Value>oots-edm:v1.0</rim:Value>
        </rim:SlotValue>
    </rim:Slot>
    <rim:Slot name="EvidenceResponseIdentifier">
        <rim:SlotValue xsi:type="rim:StringValueType">
            <rim:Value>530ad1e2-5eaf-4a9a-8192-227432eea95d</rim:Value>
        </rim:SlotValue>
    </rim:Slot>
    <rim:Slot name="ErrorProvider">
        <rim:SlotValue xsi:type="rim:AnyValueType">
            <sdg:Agent>
                <sdg:Identifier schemeID="0204">DE7657587001</sdg:Identifier>
                <sdg:Name>Authority for school and occupational training</sdg:Name>
                <sdg:Classification>IntermediaryPlatform</sdg:Classification>
                <sdg:Address>
                    <sdg:FullAddress>Hamburger Str. 31</sdg:FullAddress>
                    <sdg:LocatorDesignator>31</sdg:LocatorDesignator>
                    <sdg:PostCode>22083</sdg:PostCode>
                    <sdg:PostCityName>Hamburg</sdg:PostCityName>
                    <sdg:AdminUnitLevel1>DE</sdg:AdminUnitLevel1>
                    <sdg:AdminUnitLevel2>DE60</sdg:AdminUnitLevel2>
                </sdg:Address>
            </sdg:Agent>
        </rim:SlotValue>
    </rim:Slot>
    <rim:Slot name="EvidenceRequester">
        <rim:SlotValue xsi:type="rim:AnyValueType">
            <sdg:Agent>
```

```
                <sdg:Identifier schemeID="0190">NL22233223</sdg:Identifier>
                <sdg:Name lang="en">University of Amsterdam</sdg:Name>
            </sdg:Agent>
        </rim:SlotValue>
    </rim:Slot>
    <rs:Exception xsi:type="rs:AuthorizationExceptionType"   severity="FAILURE"
        message="User redirection required"  >
        <rim:Slot name="Timestamp">
            <rim:SlotValue xsi:type="rim:DateTimeValueType">
                <rim:Value>2020-02-14T19:21:30+01:00</rim:Value>
            </rim:SlotValue>
        </rim:Slot>
        <rim:Slot name="PreviewLocation">
            <rim:SlotValue xsi:type="rim:StringValueType">
                <rim:Value>https://preview.space.example.com/requests?session=d36af8bc-fea6-4ee5-a32d-
5bef82cdb071</rim:Value>
            </rim:SlotValue>
        </rim:Slot>
        <rim:Slot name="PreviewDescription">
            <rim:SlotValue xsi:type="rim:InternationalStringValueType">
                <rim:Value>
                    <rim:LocalizedString xml:lang="nl" value="Kies uw diploma."/>
                    <rim:LocalizedString xml:lang="ro" value="Vă rugăm să selectaţi diploma dvs."/>
                    <rim:LocalizedString xml:lang="en" value="Please select your diploma."/>
                </rim:Value>
            </rim:SlotValue>
        </rim:Slot>
        <rim:Slot name="PreviewMethod">
            <rim:SlotValue xsi:type="rim:StringValueType">
                <rim:Value>GET</rim:Value>
            </rim:SlotValue>
        </rim:Slot>
    </rs:Exception>
</query:QueryResponse>
```

Code Block 7 Step 2: XML example of the Error Response returned by the Evidence Provider

4.5.5.3.3 Step 3: Second Evidence Request

The Evidence Requester redirects the user (natural person) to the corresponding preview location. After the execution of the preview the Evidence Requester sends a second Evidence Request to the Evidence Provider containing the preview location. More information about how this information is represented within the XML document can be found in the Evidence Request Syntax Mapping.

```
<?xml version="1.0" encoding="UTF-8"?>
<query:QueryRequest xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                    xmlns:rs="urn:oasis:names:tc:ebxml-regrep:xsd:rs:4.0"
                    xmlns:sdg="http://data.europa.eu/p4s"
                    xmlns:xmime="http://www.w3.org/2005/05/xmlmime"
                    xmlns:rim="urn:oasis:names:tc:ebxml-regrep:xsd:rim:4.0"
                    xmlns:query="urn:oasis:names:tc:ebxml-regrep:xsd:query:4.0"
                    xmlns:xlink="http://www.w3.org/1999/xlink"
                    xmlns:xml="http://www.w3.org/XML/1998/namespace"
                    id="bc2842c1-6625-450d-a7c6-7d692230b753">

    <rim:Slot name="SpecificationIdentifier">
        <rim:SlotValue xsi:type="rim:StringValueType">
            <rim:Value>oots-edm:v1.0</rim:Value>
        </rim:SlotValue>
    </rim:Slot>
    <rim:Slot name="IssueDateTime">
        <rim:SlotValue xsi:type="rim:DateTimeValueType">
            <rim:Value>2022-02-15T19:20:30+01:00</rim:Value>
        </rim:SlotValue>
    </rim:Slot>
    <rim:Slot name="Procedure">
        <rim:SlotValue xsi:type="rim:InternationalStringValueType">
            <rim:Value>
                <rim:LocalizedString xml:lang="en"
                                     value="Requesting recognition of diploma"/>
            </rim:Value>
        </rim:SlotValue>
    </rim:Slot>
    <rim:Slot name="PreviewLocation">
        <rim:SlotValue xsi:type="rim:StringValueType">
            <rim:Value>https://preview.space.example.com/requests?session=d36af8bc-fea6-4ee5-a32d-5bef82cdb071</rim:Value>
        </rim:SlotValue>
    </rim:Slot>
    <rim:Slot name="PossibilityForPreview">
        <rim:SlotValue xsi:type="rim:BooleanValueType">
            <rim:Value>true</rim:Value>
        </rim:SlotValue>
    </rim:Slot>
```

```
<rim:Slot name="ExplicitRequestGiven">
    <rim:SlotValue xsi:type="rim:BooleanValueType">
        <rim:Value>true</rim:Value>
    </rim:SlotValue>
</rim:Slot>
<rim:Slot name="Requirements">
    <rim:SlotValue xsi:type="rim:CollectionValueType"
                   collectionType="urn:oasis:names:tc:ebxml-regrep:CollectionType:Set">
        <rim:Element xsi:type="rim:AnyValueType">
            <rim:Requirement>
                <Identifier>315cfd75-6605-49c4-b0fe-799833b41099</Identifier>
                <Name lang="en">Proof of Secondary Education Completion</Name>
            </rim:Requirement>
        </rim:Element>
        <rim:Element xsi:type="rim:AnyValueType">
            <rim:Requirement>
                <Identifier>543-cfd75-6605-49c4-b0fe-799833b41111</Identifier>
                <Name lang="en">Proof of Secondary Education Completion Supplemenent Evidence</Name>
            </rim:Requirement>
        </rim:Element>
    </rim:SlotValue>
</rim:Slot>
<rim:Slot name="EvidenceRequester">
    <rim:SlotValue xsi:type="rim:CollectionValueType">
        <rim:Element xsi:type="rim:AnyValueType">
            <sdg:Agent>
                <sdg:Identifier schemeID="0190">NL22233223</sdg:Identifier>
                <sdg:Name lang="en">University of Amsterdam</sdg:Name>
                <sdg:Classification>EvidenceRequester</sdg:Classification>
                <sdg:Address>
                    <sdg:FullAddress>Binnengasthuisstraat 9</sdg:FullAddress>
                    <sdg:LocatorDesignator>9</sdg:LocatorDesignator>
                    <sdg:PostCode>1012</sdg:PostCode>
                    <sdg:PostCityName>Amsterdam</sdg:PostCityName>
                    <sdg:AdminUnitLevel1>NL</sdg:AdminUnitLevel1>
                    <sdg:AdminUnitLevel2>NL329</sdg:AdminUnitLevel2>
                </sdg:Address>
            </sdg:Agent>
        </rim:Element>
```

```
        </rim:SlotValue>
    </rim:Slot>
    <rim:Slot name="EvidenceProvider">
        <rim:SlotValue xsi:type="rim:AnyValueType">
            <sdg:Agent>
                <sdg:Identifier schemeID="0204">DE7657587001</sdg:Identifier>
                <sdg:Name>Authority for school and occupational training</sdg:Name>
            </sdg:Agent>
        </rim:SlotValue>
    </rim:Slot>
    <rim:Slot name="EvidenceProviderClassificationValues">
        <rim:SlotValue xsi:type="rim:CollectionValueType">
            <rim:Element xsi:type="rim:AnyValueType">
                <sdg:ClassificationConcept>
                    <sdg:Identifier>SecondarySchool</sdg:Identifier>
                    <sdg:SupportedValue>
                        <sdg:StringValue>Wilhelm Gymnasium</sdg:StringValue>
                    </sdg:SupportedValue>
                </sdg:ClassificationConcept>
            </rim:Element>
            <rim:Element xsi:type="rim:AnyValueType">
                <sdg:ClassificationConcept>
                    <sdg:Identifier>YearOfGraduation</sdg:Identifier>
                    <sdg:SupportedValue>
                        <sdg:StringValue>1988</sdg:StringValue>
                    </sdg:SupportedValue>
                </sdg:ClassificationConcept>
            </rim:Element>
        </rim:SlotValue>
    </rim:Slot>
    <query:ResponseOption returnType="LeafClassWithRepositoryItem"/>
    <query:Query queryDefinition="DocumentQuery">
        <rim:Slot name="NaturalPerson">
            <rim:SlotValue xsi:type="rim:AnyValueType">
                <sdg:Person>
                    <sdg:LevelOfAssurance>High</sdg:LevelOfAssurance>
                    <sdg:Identifier schemeID="eidas">DK/DE/123456</sdg:Identifier>
                    <sdg:FamilyName>Smith</sdg:FamilyName>
                    <sdg:GivenName>Jack</sdg:GivenName>
```

```
                    <sdg:DateOfBirth>1970-03-01</sdg:DateOfBirth>
                    <sdg:PlaceOfBirth>Dusseldorf</sdg:PlaceOfBirth>
                    <sdg:CurrentAddress>
                        <sdg:FullAddress>Lansstraße 81</sdg:FullAddress>
                        <sdg:AdminUnitLevel1>DE</sdg:AdminUnitLevel1>
                    </sdg:CurrentAddress>
                </sdg:Person>
            </rim:SlotValue>
        </rim:Slot>
        <rim:Slot name="EvidenceRequest">
            <rim:SlotValue xsi:type="rim:AnyValueType">
                <sdg:DataServiceEvidenceType>
                    <sdg:Identifier>487fdfdc-7f92-42bb-a690-dcbd3d65f435</sdg:Identifier>
                    <sdg:EvidenceTypeClassification>SecondaryEducationCompletion</sdg:EvidenceTypeClassification>
                    <sdg:Title lang="en">Secondary Education Completion Evidence</sdg:Title>
                    <sdg:Title lang="de">Nachweis des Sekundarschulabschlusses</sdg:Title>
                    <sdg:DistributedAs>
                        <sdg:Format>application/pdf</sdg:Format>
                        <sdg:ConformsTo>https://semic.org/sa/common/secondary-education-evidence-1.0.0</sdg:ConformsTo>
                    </sdg:DistributedAs>
                </sdg:DataServiceEvidenceType>
            </rim:SlotValue>
        </rim:Slot>
    </query:Query>
</query:QueryRequest>
```

Code Block 8 Step 3: XML example of the second Evidence Request for a Secondary Education Completition Evidence

4.5.5.3.4 Step 4: Evidence Response

After the execution of the preview and a matching of the preview results with the second Evidence Request, the Evidence Provider sends an Evidence Response with the Secondary Education Completition Evidence and its supplement to the Evidence Requester. More information about how this information is represented within the XML document can be found in the Evidence Response Syntax Mapping.

```xml
<?xml version="1.0" encoding="UTF-8"?>

<query:QueryResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns:rs="urn:oasis:names:tc:ebxml-regrep:xsd:rs:4.0"
    xmlns:rim="urn:oasis:names:tc:ebxml-regrep:xsd:rim:4.0"
    xmlns:sdg="http://data.europa.eu/p4s"
    xmlns:query="urn:oasis:names:tc:ebxml-regrep:xsd:query:4.0"
    xmlns:xlink="http://www.w3.org/1999/xlink"
    status="urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Success"
    xmlns:xml="http://www.w3.org/XML/1998/namespace"
    requestId="bc2842c1-6625-450d-a7c6-7d692230b753">


    <!-- Top Level Slots, providing metadata about the Response and the Evidence Provider -->
    <rim:Slot name="SpecificationIdentifier">
        <rim:SlotValue xsi:type="rim:StringValueType"
                       xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
            <rim:Value>oots-edm:v1.0</rim:Value>
        </rim:SlotValue>
    </rim:Slot>
    <rim:Slot name="EvidenceResponseIdentifier">
        <rim:SlotValue xsi:type="rim:StringValueType">
            <rim:Value>5af62cce-debe-11ec-9d64-0242ac120002</rim:Value>
        </rim:SlotValue>
    </rim:Slot>
    <rim:Slot name="IssueDateTime">
        <rim:SlotValue xsi:type="rim:DateTimeValueType">
            <rim:Value>2022-02-14T19:20:30+02:00</rim:Value>
        </rim:SlotValue>
    </rim:Slot>
    <rim:Slot name="EvidenceProvider">
        <rim:SlotValue xsi:type="rim:AnyValueType">
            <sdg:Agent>
                <sdg:Identifier schemeID="0204">DE7657587001</sdg:Identifier>
                <sdg:Name>Authority for school and occupational training</sdg:Name>
                <sdg:Classification>IntermediaryPlatform</sdg:Classification>
                <sdg:Address>
                    <sdg:FullAddress>Hamburger Str. 31</sdg:FullAddress>
                    <sdg:LocatorDesignator>31</sdg:LocatorDesignator>
```

```
                <sdg:PostCode>22083</sdg:PostCode>
                <sdg:PostCityName>Hamburg</sdg:PostCityName>
                <sdg:AdminUnitLevel1>DE</sdg:AdminUnitLevel1>
                <sdg:AdminUnitLevel2>DE60</sdg:AdminUnitLevel2>
            </sdg:Address>
        </sdg:Agent>
    </rim:SlotValue>
</rim:Slot>
<rim:Slot name="EvidenceRequester">
    <rim:SlotValue xsi:type="rim:AnyValueType">
        <sdg:Agent>
            <sdg:Identifier schemeID="0190">NL22233223</sdg:Identifier>
            <sdg:Name lang="en">University of Amsterdam</sdg:Name>
        </sdg:Agent>
    </rim:SlotValue>
</rim:Slot>
<rim:RegistryObjectList>
<rim:RegistryObject xsi:type="rim:ExtrinsicObjectType" id="555555-740e-4b64-80f0-2462462462">
    <rim:Slot name="EvidenceMetadata">
        <rim:SlotValue xsi:type="rim:AnyValueType">
            <sdg:Evidence>
                <sdg:Identifier>7c2e04cf-7d20-4363-908d-827817746725</sdg:Identifier>
                <sdg:IsAbout>
                    <sdg:NaturalPerson>
                        <sdg:Identifier schemeID="eidas">DK/DE/123456</sdg:Identifier>
                        <sdg:FamilyName>Smith</sdg:FamilyName>
                        <sdg:GivenName>Jack</sdg:GivenName>
                        <sdg:DateOfBirth>1970-03-01</sdg:DateOfBirth>
                        <sdg:PlaceOfBirth>Dusseldorf</sdg:PlaceOfBirth>
                    </sdg:NaturalPerson>
                </sdg:IsAbout>
                <sdg:IssuingAuthority>
                    <sdg:Identifier schemeID="9930">DE7657587001</sdg:Identifier>
                    <sdg:Name>Wilhelm Gymnasium</sdg:Name>
                </sdg:IssuingAuthority>
                <sdg:IsConformantTo>
                    <sdg:EvidenceTypeClassification>SecondaryEducationCompletion</sdg:EvidenceTypeClassification>
                    <sdg:Title lang="en">Secondary Education Completion Evidence</sdg:Title>
                    <sdg:Title lang="de">Nachweis des Sekundarschulabschlusses</sdg:Title>
```

```
                        <sdg:Description lang="de">Nachweis über den Abschluss der Sekundarstufe II</sdg:Description>
                        <sdg:Description lang="en">Proof of completion of secondary education second stage</sdg:Description>
                    </sdg:IsConformantTo>
                    <sdg:IssuingDate>1988-05-10</sdg:IssuingDate>
                    <sdg:Distribution>
                        <sdg:Format>application/pdf</sdg:Format>
                    </sdg:Distribution>
                </sdg:Evidence>
            </rim:SlotValue>
        </rim:Slot>
        <!-- The attached Document Provided as Evidence. Points to an AS4 attachment -->
        <rim:RepositoryItemRef xlink:href="cid:attachment100001@example.oots.eu" xlink:title="SecondaryEducationCompletion"/>
    </rim:RegistryObject>
    <rim:RegistryObject xsi:type="rim:ExtrinsicObjectType" id="555555-740e-4b64-80f0-2462462462">
        <rim:Slot name="EvidenceMetadata">
            <rim:SlotValue xsi:type="rim:AnyValueType">
                <sdg:Evidence>
                    <sdg:Identifier>5ee5c0de-c066-4637-bea3-6e3511ada970</sdg:Identifier>
                    <sdg:IsAbout>
                        <sdg:NaturalPerson>
                            <sdg:Identifier schemeID="eidas">DK/DE/123456</sdg:Identifier>
                            <sdg:FamilyName>Smith</sdg:FamilyName>
                            <sdg:GivenName>Jack</sdg:GivenName>
                            <sdg:DateOfBirth>1970-03-01</sdg:DateOfBirth>
                            <sdg:PlaceOfBirth>Dusseldorf</sdg:PlaceOfBirth>
                        </sdg:NaturalPerson>
                    </sdg:IsAbout>
                    <sdg:IssuingAuthority>
                        <sdg:Identifier schemeID="9930">DE7657587001</sdg:Identifier>
                        <sdg:Name>Wilhelm Gymnasium</sdg:Name>
                    </sdg:IssuingAuthority>
                    <sdg:IsConformantTo>
                        <sdg:EvidenceTypeClassification>SecondaryEducationCompletion</sdg:EvidenceTypeClassification>
                        <sdg:Title lang="en">Secondary Education Completion Evidence Supplement</sdg:Title>
                        <sdg:Title lang="de">Anhang zum Nachweis des Sekundarschulabschlusses</sdg:Title>
                        <sdg:Description lang="en">The Supplement of the Secondary Education Completion Evidence Supplement
to understand the qualification.</sdg:Description>
                        <sdg:Description lang="de">Die Anlage zum Nachweis des Sekundarschulabschlusses, um die Qualifikation
zu verstehen.</sdg:Description>
```

```
                    </sdg:IsConformantTo>
                    <sdg:IssuingDate>1988-05-10</sdg:IssuingDate>
                    <sdg:Distribution>
                        <sdg:Format>application/pdf</sdg:Format>
                    </sdg:Distribution>
                </sdg:Evidence>
            </rim:SlotValue>
        </rim:Slot>
        <!-- The attached Document Provided as Evidence. Points to an AS4 attachment -->
        <rim:RepositoryItemRef xlink:href="cid:attachment100002@example.oots.eu"
xlink:title="SecondaryEducationCompletionSupplement"/>
    </rim:RegistryObject>
</rim:RegistryObjectList>
</query:QueryResponse>
```

Code Block 9 Step 4: XML example of Evidence Response for a Secondary Education Completition Evidence

4.6 Business Rules - June 2022

4.6.1 Introduction

In order to facilitate interoperability for the Evidence Exchange, a set of business rules is defined which must be applied in each transaction (Evidence Request, Evidence Reponse, Error Response). For each business rule, a corresponding schematron rule is defined that references the same rule ID. The business rules are sets of rules that guarantee the correct structure of the transactions and they clarify the content of instances by stating mandatory fields, fixed values (like code lists), the dependency between fields in the same object and dependency between different objects. The business rules are grouped into two main sections depending on their scope:

- Business rules that guarantee the correct structure of the message:
    - Check information constraints related to the use of different components such as namespaces, root elements, slots, data types including "multidimensional" checks crossing the barrier between the different XSD schemes (XSD-Binding and XSD-Restriction).
- Business rules that ensure the correct use of information objects:
    - Check cardinalities, identifiers, formats, fixed values, mandatory set of values on specific fields (code lists) and dependencies between fields;

Each business rule is associated with an error level (flag) that expresses a validation result when an XML instance is proven against the rules through schematron validation:

- *note:* a hint that an additional object is mandatory in some cases;
- *warning*: offering recommendations to improve the quality of the instance or regain full validity;
- *fatal*: the rule point to a major issue of consistency or data correctness.

The rule type classifies the principle goal of a business rule. The rule ID is used to identify the rule and can be used as an error code next to the rule description. Rule descriptions containing "MUST" correspond to an error level that is flagged as *fatal*, while "SHOULD" rules correspond to an error level that is flagged as a *warning*. "MAY" rules point to error level *note*. The Element and Location points to the correct information object that is affected by the rule.

4.6.2 Business rules associated to the Evidence Request

The tables below collect the set of business rules affecting the creation of Evidence Request instances.

4.6.2.1 Business rules that prove the correct structure of Evidence Requests

Rule Type	Rule ID	Element	Location	Rule	Flag
Slot	BR-OOTS-REQ-ebRIM-001	SpecificationIdentifier	query:QueryRequest/rim:Slot[@name='SpecificationIdentifier']	The <rim:Slot name="SpecificationIdentifier"> MUST be present in the QueryRequest.	Fatal
Slot	BR-OOTS-REQ-ebR	IssueDateTime	query:QueryRequest/rim:Slot[@name='IssueDateTime']	The <rim:Slot name="IssueDateTime"> MUST be present in the QueryRequest.	Fatal

Rule Type	Rule ID	Element	Location	Rule	Flag
	IM-002				
Slot	BR-OOTS-REQ-ebRIM-003	Procedure	query:QueryRequest/rim:Slot[@name='Procedure']	The <rim:Slot name="Procedure"> SHOULD be present in the QueryRequest.	Warning
Slot	BR-OOTS-REQ-ebRIM-004	PreviewLocation	query:QueryRequest/rim:Slot[@name='PreviewLocation']	The <rim:Slot name="PreviewLocation"> MAY be present in the QueryRequest.	Note
Slot	BR-OOTS-REQ-ebRIM-005	PossibilityForPreview	query:QueryRequest/rim:Slot[@name='PossibilityForPreview']	The <rim:Slot name="PossibilityForPreview"> MUST be present in the QueryRequest.	Fatal
Slot	BR-OOTS-RE	ExplicitRequestGiven	query:QueryRequest/rim:Slot[@name='ExplicitRequestGiven']	The <rim:Slot name="ExplicitRequestGiven"> MUST be present in the QueryRequest.	Fatal

Rule Type	Rule ID	Element	Location	Rule	Flag
	Q-ebRIM-006				
Slot	BR-OOTS-REQ-ebRIM-007	Requirement	query:QueryRequest/rim:Slot[@name='Requirement']	The <rim:Slot name="Requirement"> SHOULD be present in the QueryRequest.	Warning
Slot	BR-OOTS-REQ-ebRIM-008	EvidenceRequester	query:QueryRequeste/rim:Slot[@name='EvidenceRequester']	The <rim:Slot name="EvidenceRequester"> MUST be present in the QueryRequest.	Fatal
Slot	BR-OOTS-REQ-ebRIM-009	EvidenceProvider	query:QueryRequest/rim:Slot[@name='EvidenceProvider']	The <rim:Slot name="EvidenceProvider"> MUST be present in the QueryRequest.	Fatal

Rule Type	Rule ID	Element	Location	Rule	Flag
Slot	BR-OOTS-REQ-ebRIM-042	EvidenceProviderClassificationValues	query:QueryRequest/rim:Slot[@name='EvidenceProviderClassificationValues']	The <rim:Slot name="EvidenceProviderClassificationValues"> MAY be present in the QueryRequest.	Note
Slot	BR-OOTS-REQ-ebRIM-010	EvidenceRequest	query:QueryRequest/query:Query/rim:Slot[@name='EvidenceRequest']	The <rim:Slot name="EvidenceRequest"> MUST be present in the Query.	Fatal
Slot	BR-OOTS-REQ-ebRIM-011	LegalPerson	query:QueryRequest/query:Query/rim:Slot[@name='LegalPerson']	A Query MUST contain either a <rim:Slot name="LegalPerson"> or a <rim:Slot name="NaturalPerson"> but NOT both.	Fatal
Slot	BR-OOTS-REQ-ebR	NaturalPerson	query:QueryRequest/query:Query/rim:Slot[@name='NaturalPerson']	A Query MUST contain either a <rim:Slot name="LegalPerson"> or a <rim:Slot name="NaturalPerson"> but NOT both.	Fatal

Rule Type	Rule ID	Element	Location	Rule	Flag
	IM-012				
Slot	BR-OOTS-REQ-ebRIM-013	AuthorizedRepresentative	query:QueryRequest/query:Query/rim:Slot[@name='AuthorizedRepresentative']	The <rim:Slot name="AuthorizedRepresentative"> MAY be present in the Query.	Note
Slot	BR-OOTS-REQ-ebRIM-014	QueryRequest	query:QueryRequest	A 'query:QueryRequest' MUST not contain any other rim:Slots.	Fatal
DataType	BR-OOTS-REQ-ebRIM-015	SpecificationIdentifier	query:QueryRequest/rim:Slot[@name='SpecificationIdentifier']/rim:SlotValue	The <rim:SlotValue> of <rim:Slot name="SpecificationIdentifier"> MUST be of "rim:StringValueType"	Fatal
DataType	BR-OOTS-RE	IssueDateTime	query:QueryRequest/rim:Slot[@name='IssueDateTime']/rim:SlotValue	The <rim:SlotValue> of <rim:Slot name="IssueDateTime"> MUST be of "rim:DateTimeValueType"	Fatal

Rule Type	Rule ID	Element	Location	Rule	Flag
	Q-ebRIM-016				
DataType	BR-OOTS-REQ-ebRIM-017	Procedure	query:QueryRequest/rim:Slot[@name='Procedure']/rim:SlotValue	The <rim:SlotValue> of <rim:Slot name="Procedure"> MUST be of "rim:InternationalStringValueType"	Fatal
DataType	BR-OOTS-REQ-ebRIM-018	PreviewLocation	query:QueryRequest/rim:Slot[@name='PreviewLocation']/rim:SlotValue	The <rim:SlotValue> of <rim:Slot name="PreviewLocation"> MUST be of "rim:StringValueType"	Fatal
DataType	BR-OOTS-REQ-ebRIM-019	PossibilityForPreview	query:QueryRequest/rim:Slot[@name='PossibilityForPreview']/rim:SlotValue	The <rim:SlotValue> of <rim:Slot name="PossibilityForPreview"> MUST be of "rim:BooleanValueType"	Fatal

Rule Type	Rule ID	Element	Location	Rule	Flag
DataType	BR-OOTS-REQ-ebRIM-020	ExplicitRequestGiven	query:QueryRequest/rim:Slot[@name='ExplicitRequestGiven']/rim:SlotValue	The <rim:SlotValue> of <rim:Slot name="ExplicitRequestGiven"> MUST be of "rim:BooleanValueType"	Fatal
DataType	BR-OOTS-REQ-ebRIM-021	Requirement	query:QueryRequest/rim:Slot[@name='Requirement']/rim:SlotValue	The <rim:SlotValue> of <rim:Slot name="Requirement> MUST be of "rim:CollectionValueType"	Fatal
DataType	BR-OOTS-REQ-ebRIM-022	Requirement	query:QueryRequest/rim:Slot[@name='Requirement']/rim:SlotValue/rim:Element	The <rim:Element> of <rim:SlotValue> of <rim:Slot name="Requirement"> MUST be of "rim:AnyValueType"	Fatal
DataType	BR-OOTS-REQ-ebR	EvidenceRequester	query:QueryRequeste/rim:Slot[@name='EvidenceRequester']/rim:SlotValue	The <rim:SlotValue> of <rim:Slot name="EvidenceRequester"> MUST be of "rim:CollectionValueType"	Fatal

Rule Type	Rule ID	Element	Location	Rule	Flag
	IM-023				
DataType	BR-OOTS-REQ-ebRIM-024	EvidenceRequester	query:QueryRequeste/rim:Slot[@name='EvidenceRequester']/rim:SlotValue/rim:Element	The <rim:Element> of <rim:SlotValue> of <rim:Slot name="EvidenceRequester"> MUST be of "rim:AnyValueType"	Fatal
DataType	BR-OOTS-REQ-ebRIM-025	EvidenceProvider	query:QueryRequest/rim:Slot[@name='EvidenceProvider']/rim:SlotValue	The <rim:SlotValue> of <rim:Slot name="EvidenceProvider"> MUST be of "rim:AnyValueType"	Fatal
DataType	BR-OOTS-REQ-ebRIM-044	EvidenceProviderClassificationValues	query:QueryRequest/rim:Slot[@name='EvidenceProviderClassificationValues']/rim:SlotValue	The <rim:SlotValue>of <rim:Slot name="EvidenceProviderClassificationValues"> MUST be of "rim:CollectionValueType"	Fatal
DataType	BR-OOTS-RE	EvidenceRequest	query:QueryRequest/query:Query/rim:Slot[@name='EvidenceRequest']/rim:SlotValue	The <rim:SlotValue> of <rim:Slot name="EvidenceRequest"> MUST be of "rim:AnyValueType"	Fatal

Rule Type	Rule ID	Element	Location	Rule	Flag
	Q-ebRIM-026				
DataType	BR-OOTS-REQ-ebRIM-027	LegalPerson	query:QueryRequest/query:Query/rim:Slot[@name='LegalPerson']/rim:SlotValue	The <rim:SlotValue> of <rim:Slot name="LegalPerson"> MUST be of "rim:AnyValueType"	Fatal
DataType	BR-OOTS-REQ-ebRIM-028	NaturalPerson	query:QueryRequest/query:Query/rim:Slot[@name='NaturalPerson']/rim:SlotValue	The <rim:SlotValue> of <rim:Slot name="NaturalPerson"> MUST be of "rim:AnyValueType"	Fatal
DataType	BR-OOTS-REQ-ebRIM-029	AuthorizedRepresentative	query:QueryRequest/query:Query/rim:Slot[@name='AuthorizedRepresentative']/rim:SlotValue	The <rim:SlotValue> of <rim:Slot name="AuthorizedRepresentative"> MUST be of "rim:AnyValueType"	Fatal

Rule Type	Rule ID	Element	Location	Rule	Flag
XSD-Binding	BR-OOTS-REQ-ebRIM-030	Requirement	query:QueryRequest/rim:Slot[@name='Requirement']/rim:SlotValue/rim:Element	The 'query:QueryRequest/rim:Slot[@name='Requirement']/rim:SlotValue/rim:Element' MUST use the '<xs:element name="Requirement" type="sdg:RequirementType"/>' of the targetNamespace="http://data.europa.eu/p4s"	Fatal
XSD-Restriction	BR-OOTS-REQ-ebRIM-031	Requirement	query:QueryRequest/rim:Slot[@name='Requirement']/rim:SlotValue/rim:Element/Requirement	A Requirement 'rim:Element/Requirement' MUST not contain any other elements than 'sdg:Identifier' and 'sdg:Name'.	Fatal
XSD-Binding	BR-OOTS-REQ-ebRIM-032	EvidenceRequester	query:QueryRequest/rim:Slot[@name='EvidenceRequester']/rim:SlotValue/rim:Element	The 'query:QueryRequest/rim:Slot[@name='EvidenceRequester']/rim:SlotValue/rim:Element' MUST use the '<xs:element name="Agent" type="sdg:AgentType" />' of the targetNamespace="http://data.europa.eu/p4s"	Fatal
XSD-Restriction	BR-OOTS-REQ-ebR	EvidenceRequester	query:QueryRequest/rim:Slot[@name='EvidenceRequester']/rim:SlotValue/rim:Element/Agent	An EvidenceRequester "rim:Element/Agent' MUST not contain any other elements than 'sdg:Identifier' and 'sdg:Name', 'Address' and 'Classification'.	Fatal

Rule Type	Rule ID	Element	Location	Rule	Flag
	IM-033				
XSD-Binding	BR-OOTS-REQ-ebRIM-043	EvidenceProviderClassificationValues	query:QueryRequest/rim:Slot[@name='EvidenceProviderClassificationValues']/rim:SlotValue	The 'query:QueryRequest/rim:Slot[@name='EvidenceProviderClassificationValues']/rim:SlotValue' MUST use the '<xs:element name="EvidenceProviderClassification" type="sdg:InformationConceptType" />' of the targetNamespace="http://data.europa.eu/p4s"	Fatal
XSD-Binding	BR-OOTS-REQ-ebRIM-034	EvidenceProvider	query:QueryRequest/rim:Slot[@name='EvidenceProvider']/rim:SlotValue	The 'query:QueryRequest/rim:Slot[@name='EvidenceProvider']/rim:SlotValue' MUST use the '<xs:element name="Agent" type="sdg:AgentType" />' of the targetNamespace="http://data.europa.eu/p4s"	Fatal
XSD-Restriction	BR-OOTS-REQ-ebRIM-035	EvidenceProvider	query:QueryRequest/rim:Slot[@name='EvidenceProvider']/rim:SlotValue/Agent	An EvidenceProvider 'rim:SlotValue/Agent' MUST not contain any other elements than 'sdg:Identifier' and 'sdg:Name'.	Fatal
XSD-Binding	BR-OOTS-RE	EvidenceRequest	query:QueryRequest/query:Query/rim:Slot[@name='EvidenceRequest']/rim:SlotValue	The 'query:QueryRequest/rim:Slot[@name='EvidenceRequest']/rim:SlotValue' MUST use the '<xs:element name="DataServiceEvidenceType"	Fatal

Rule Type	Rule ID	Element	Location	Rule	Flag
	Q-ebRIM-036			type="sdg:DataServiceEvidenceTypeType"/>' of the targetNamespace="http://data.europa.eu/p4s"	
XSD-Restriction	BR-OOTS-REQ-ebRIM-037	EvidenceRequest	query:QueryRequest/query:Query/rim:Slot[@name='EvidenceRequest']/rim:SlotValue/ DataServiceEvidenceType	An EvidenceRequest 'rim:SlotValue/DataServiceEvidenceType' MUST not contain any other elements than 'sdg:Identifier', 'EvidenceTypeClassification', 'Title', 'Description' and 'DistributedAs'.	Fatal
XSD-Binding	BR-OOTS-REQ-ebRIM-038	NaturalPerson	query:QueryRequest/query:Query/rim:Slot[@name='NaturalPerson']/rim:SlotValue	The 'query:QueryRequest/query:Query/rim:Slot[@name='NaturalPerson']/rim:SlotValue' MUST use the '<xs:element name="Person" type="sdg:PersonType"/>' of the targetNamespace="http://data.europa.eu/p4s"	Fatal
XSD-Binding	BR-OOTS-REQ-ebRIM-039	LegalPerson	query:QueryRequest/query:Query/rim:Slot[@name='LegalPerson']/rim:SlotValue	The 'query:QueryRequest/query:Query/rim:Slot[@name='LegalPerson']/rim:SlotValue' MUST use the '<xs:element name="LegalPerson" type="sdg:LegalPersonType"/>' of the targetNamespace="http://data.europa.eu/p4s"	Fatal

Rule Type	Rule ID	Element	Location	Rule	Flag
XSD-Binding	BR-OOTS-REQ-ebRIM-040	AuthorizedRepresentative	query:QueryRequest/query:Query/rim:Slot[@name='AuthorizedRepresentative']/rim:SlotValue	The 'query:QueryRequest/query:Query/rim:Slot[@name='AuthorizedRepresentative']/rim:SlotValue' MUST use the '<xs:element name="Person" type="sdg:PersonType"/>' of the targetNamespace="http://data.europa.eu/p4s"	Fatal

4.6.2.2 Business rules that prove the correct use of information objects in Evidence Requests

Rule Type	Rule ID	Element	Location	Rule	Flag
Identifier	BR-OOTS-REQ-001	query:QueryRequest	query:QueryRequest/@id	The 'id' attribute of a 'QueryRequest' MUST be unique UUID (RFC 4122) for each request.	Fatal
Identifier	BR-OOTS-REQ-002	SpecificationIdentifier	query:QueryRequest/rim:Slot[@name='SpecificationIdentifier']/rim:SlotValue/rim:Value	The 'rim:Value' of the 'SpecificationIdentifier' MUST be the fixed value "oots-edm:v1.0".	Fatal
Format	BR-OOTS-REQ-003	IssueDateTime	query:QueryRequest/rim:Slot[@name='IssueDateTime']/rim:SlotValue/rim:Value	The 'rim:Value' of 'IssueDateTime' MUST be according to xsd:dateTime.	Fatal

Rule Type	Rule ID	Element	Location	Rule	Flag
CodeList	BR-OOTS-REQ-004	Procedure	query:QueryRequest/rim:Slot[@name='Procedure']/rim:SlotValue/rim:Value/rim:LocalizedString/@value	The 'value' attribute of 'Procedure' MUST be part of the code list 'Procedure Types'	Fatal
CodeList	BR-OOTS-REQ-005	Procedure	query:QueryRequest/rim:Slot[@name='Procedure']/rim:SlotValue/rim:Value/rim:LocalizedString/@xml:lang	The 'language' attribute of 'Procedure' MUST be specified using the code list 'LanguageCode' (ISO 639-1 two-letter code).	Fatal
Identifier	BR-OOTS-REQ-006	PreviewLocation	query:QueryRequest/rim:Slot[@name='PreviewLocation']/rim:SlotValue/rim:Value	The 'rim:Value' of a 'PreviewLocation' MUST be a URI starting with 'https://'.	Fatal
CodeList	BR-OOTS-REQ-007	PossibilityForPreview	query:QueryRequest/rim:Slot[@name='PossibilityForPreview']/rim:SlotValue/rim:Value	The 'rim:Value' of 'PossibilityForPreview' MUST be according to xsd:boolean.	Fatal
CodeList	BR-OOTS-REQ-008	ExplicitRequestGiven	query:QueryRequest/rim:Slot[@name='ExplicitRequestGiven']/rim:SlotValue/rim:Value	The 'rim:Value' of 'ExplicitRequestGiven' MUST be xsd:boolean.	Fatal
Identifier	BR-OOTS-	Requirement	query:QueryRequest/rim:Slot[@name='Requirement']/rim:SlotValue/rim:Element/Identifier	The value of 'Identifier' of a 'Requirement' MUST be unique UUID (RFC 4122) provided by the EvidenceBroker.	Fatal

Rule Type	Rule ID	Element	Location	Rule	Flag
	REQ-009				
CodeList	BR-OOTS-REQ-010	Requirement	query:QueryRequest/rim:Slot[@name='Requirement']/rim:SlotValue/rim:Element/Name/@lang	The value of 'lang' attribute MUST be part of the code list 'LanguageCode' (ISO 639-1 two-letter code).	Fatal
Cardinality	BR-OOTS-REQ-011	Requirement	query:QueryRequest/rim:Slot[@name='Requirement']/rim:SlotValue/rim:Element/Name/@lang	The value of 'lang' attribute MUST be be provided. Default value: 'en'.	Fatal
Cardinality	BR-OOTS-REQ-012	EvidenceRequester	query:QueryRequest/rim:Slot[@name='EvidenceRequester']/rim:SlotValue/rim:Element/Agent/ Identifier/@schemeID	The 'schemeID' attribute of 'Identifier' MUST be present.	Fatal
CodeList	BR-OOTS-REQ-013	EvidenceRequester	query:QueryRequest/rim:Slot[@name='EvidenceRequester']/rim:SlotValue/rim:Element/Agent/ Identifier/@schemeID	The value of the 'schemeID' attribute of the 'Identifier' MUST be part of the code list 'EAS' (Electronic Address Scheme).	Fatal
Cardinality	BR-OOTS-REQ-014	EvidenceRequester	query:QueryRequest/rim:Slot[@name='EvidenceRequester']/rim:SlotValue/rim:Element/Agent/ Classification	The value for 'Agent/Classification' MUST be provided.	Fatal

Rule Type	Rule ID	Element	Location	Rule	Flag
CodeList	BR-OOTS-REQ-015	EvidenceRequester	query:QueryRequest/rim:Slot[@name='EvidenceRequester']/rim:SlotValue/rim:Element/Agent/ Classification	The value MUST be part of the code list 'AgentClassification'. Default value: EvidenceRequester	Fatal
CodeList	BR-OOTS-REQ-016	EvidenceRequester	query:QueryRequest/rim:Slot[@name='EvidenceRequester']/rim:SlotValue/rim:Element/Agent/ Address/AdminUnitLevel1	The value of the 'AdminUnitLevel1' MUST be coded using the code list 'CountryIdentificationCode' (ISO 3166-1' alpha-2 codes).	Fatal
CodeList	BR-OOTS-REQ-017	EvidenceRequester	query:QueryRequest/rim:Slot[@name='EvidenceRequester']/rim:SlotValue/rim:Element/Agent/ Address/AdminUnitLevel2	The value of the 'AdminUnitLevel2' MUST be coded using the code list 'Nomenclature of Territorial Units for Statistics' (NUTS)	Fatal
Cardinality	BR-OOTS-REQ-018	EvidenceProvider	query:QueryRequest/rim:Slot[@name='EvidenceProvider']/rim:SlotValue/Agent/Identifier/@schemeID	The 'schemeID' attribute of 'Identifier' MUST be present.	Fatal
CodeList	BR-OOTS-REQ-019	EvidenceProvider	query:QueryRequest/rim:Slot[@name='EvidenceProvider']/rim:SlotValue/Agent/Identifier/@schemeID	The value of the 'schemeID' attribute of the 'Identifier' MUST be part of the code list 'EAS' (Electronic Address Scheme).	Fatal
FixedValue	BR-OOTS-	query:ResponseOption	query:QueryRequest/query:ResponseOption/@returnType	The 'returnType' attribute of 'ResponseOption' MUST be the fixed value "LeafClassWithRepositoryItem".	Fatal

Rule Type	Rule ID	Element	Location	Rule	Flag
	REQ-020				
FixedValue	BR-OOTS-REQ-021	query:Query	query:QueryRequest/query:Query/@queryDefinition	The 'queryDefinition' attribute of 'Query' MUST be the fixed value "DocumentQuery".	Fatal
Identifier	BR-OOTS-REQ-022	EvidenceRequest	query:QueryRequest/query:Query/rim:Slot[@name='EvidenceRequest']/rim:SlotValue/ DataServiceEvidenceType/Identifier	The value of 'Identifier' of an 'DataServiceEvidenceType' MUST be unique UUID (RFC 4122) retrieved from the Data Service Directory.	Fatal
CodeList	BR-OOTS-REQ-023	EvidenceRequest	query:QueryRequest/query:Query/rim:Slot[@name='EvidenceRequest']/rim:SlotValue/ DataServiceEvidenceType/EvidenceTypeClassification	The value of 'EvidenceTypeClassification' of a 'DataServiceEvidenceType' MUST be a URI with the following format 'http::////……' pointing to the Semantic Repository encoded in the EvidenceBroker.	Fatal
CodeList	BR-OOTS-REQ-024	EvidenceRequest	query:QueryRequest/query:Query/rim:Slot[@name='EvidenceRequest']/rim:SlotValue/ DataServiceEvidenceType/Title/@lang	The value of 'lang' attribute MUST be part of the code list 'LanguageCode' (ISO 639-1 two-letter code).	Fatal
Cardinality	BR-OOTS-	EvidenceRequest	query:QueryRequest/query:Query/rim:Slot[@name='EvidenceRequest']/rim:SlotValue/ DataServiceEvidenceType/Title/@lang	The value of 'lang' attribute MUST be be provided. Default value: 'en'.	Fatal

Rule Type	Rule ID	Element	Location	Rule	Flag
	REQ-025				
CodeList	BR-OOTS-REQ-026	EvidenceRequest	query:QueryRequest/query:Query/rim:Slot[@name='EvidenceRequest']/rim:SlotValue/ DataServiceEvidenceType/Description/@lang	The value of 'lang' attribute MUST be part of the code list 'LanguageCode' (ISO 639-1 two-letter code).	Fatal
Cardinality	BR-OOTS-REQ-027	EvidenceRequest	query:QueryRequest/query:Query/rim:Slot[@name='EvidenceRequest']/rim:SlotValue/ DataServiceEvidenceType/Description/@lang	The value of 'lang' attribute MUST be be provided. Default value: 'en'.	Fatal
Cardinality	BR-OOTS-REQ-028	EvidenceRequest	query:QueryRequest/query:Query/rim:Slot[@name='EvidenceRequest']/rim:SlotValue/ DataServiceEvidenceType/DistributedAs	The Element 'DistributedAs' must occur not more than once (maxOccurs="1)' in the EvidenceRequest.	Fatal
CodeList	BR-OOTS-REQ-029	EvidenceRequest	query:QueryRequest/query:Query/rim:Slot[@name='EvidenceRequest']/rim:SlotValue/ DataServiceEvidenceType/DistributedAs/Format	The value of 'Format' of the requested distribution MUST be be part of the code list 'BinaryObjectMimeCode'.	Fatal
Identifier	BR-OOTS-REQ-030	EvidenceRequest	query:QueryRequest/query:Query/rim:Slot[@name='EvidenceRequest']/rim:SlotValue/ DataServiceEvidenceType/DistributedAs/ConformsTo	The value of 'ConformsTo' of the requested distribution MUST be a persistent URL pointing to the Data Service Directory (Semantic Respository).	Fatal

Rule Type	Rule ID	Element	Location	Rule	Flag
Identifier	BR-OOTS-REQ-031	EvidenceRequest	query:QueryRequest/query:Query/rim:Slot[@name='EvidenceRequest']/rim:SlotValue/ DataServiceEvidenceType/DistributedAs/Transformation	The value of 'Transformation' of an requested distribution MUST be a persistent URL pointing to the Data Service Directory (Semantic Respository).	Fatal
Cardinality	BR-OOTS-REQ-032	NaturalPerson	query:QueryRequest/query:Query/rim:Slot[@name='NaturalPerson']/rim:SlotValue/Person/ LevelOfAssurance	The Element 'LevelOfAssurance' must be provided (minOccurs="1)' in the EvidenceRequest when rim:Slot[@name='NaturalPerson'] is used.	Fatal
CodeLIst	BR-OOTS-REQ-033	NaturalPerson	query:QueryRequest/query:Query/rim:Slot[@name='NaturalPerson']/rim:SlotValue/Person/ LevelOfAssurance	The value of 'LevelOfAssurance' must be part of the code list 'LevelsOfAssuranceCode'	Fatal
Cardinality	BR-OOTS-REQ-034	NaturalPerson	query:QueryRequest/query:Query/rim:Slot[@name='NaturalPerson']/rim:SlotValue/Person/ Identifier	The value of a Person 'Identifier' SHOULD be provided.	Warning
Format	BR-OOTS-REQ-035	NaturalPerson	query:QueryRequest/query:Query/rim:Slot[@name='NaturalPerson']/rim:SlotValue/Person/ Identifier	The value of a Person 'Identifier' MUST have the format XX/YY/ZZZZZZZ where XX is the Nationality Code of the identifier and YY is the Nationality Code of the destination country and ZZZZZZZ is an undefined combination of characters which uniquely identifies the identity	Fatal

Rule Type	Rule ID	Element	Location	Rule	Flag
				asserted in the country of origin. Example: ES/AT/02635542Y	
CodeList	BR-OOTS-REQ-036	NaturalPerson	query:QueryRequest/query:Query/rim:Slot[@name='NaturalPerson']/rim:SlotValue/Person/ Identifier	The value of Person 'Identifier' MUST have the format XX/YY/ZZZZZZZ where the values of XX and YY MUST be part of the code list 'CountryIdentificationCode' (ISO 3166-1' alpha-2 codes). Example: ES/AT/02635542Y	Fatal
Cardinality	BR-OOTS-REQ-037	NaturalPerson	query:QueryRequest/query:Query/rim:Slot[@name='NaturalPerson']/rim:SlotValue/Person/ Identifier/@schemeID	The 'schemeID' attribute of 'Identifier' MUST be present.	Fatal
FixedValue	BR-OOTS-REQ-038	NaturalPerson	query:QueryRequest/query:Query/rim:Slot[@name='NaturalPerson']/rim:SlotValue/Person/ Identifier/@schemeID	The 'schemeID' attribute of the 'Identifier' MUST have the fixed value 'eidas'.	Fatal
Format	BR-OOTS-REQ-039	NaturalPerson	query:QueryRequest/query:Query/rim:Slot[@name='NaturalPerson']/rim:SlotValue/Person/ DateOfBirth	The value of 'DateOfBirth' MUST use the following format YYYY + “-“ + MM + “-“ + DD (as defined for xsd:date)	Fatal
CodeList	BR-OOTS-	NaturalPerson	query:QueryRequest/query:Query/rim:Slot[@name='NaturalPerson']/rim:SlotValue/Person/ Gender	The value of 'Gender' MUST be 'Male', 'Female' or 'Unspecified'.	Fatal

Rule Type	Rule ID	Element	Location	Rule	Flag
	REQ-040				
CodeList	BR-OOTS-REQ-041	NaturalPerson	query:QueryRequest/query:Query/rim:Slot[@name='NaturalPerson']/rim:SlotValue/Person/ CurrentAddress/AdminUnitLevel1	The value of the 'AdminUnitLevel1' SHOULD be part of the code list the code list 'CountryIdentificationCode' (ISO 3166-1' alpha-2 codes).	Warning
CodeList	BR-OOTS-REQ-042	NaturalPerson	query:QueryRequest/query:Query/rim:Slot[@name='NaturalPerson']/rim:SlotValue/Person/ CurrentAddress/AdminUnitLevel2	The value of the 'AdminUnitLevel2' SHOULD be coded using the code list 'Nomenclature of Territorial Units for Statistics' (NUTS)	Warning
Cardinality	BR-OOTS-REQ-043	LegalPerson	query:QueryRequest/query:Query/rim:Slot[@name='LegalPerson']/rim:SlotValue/LegalPerson/ LevelOfAssurance	The Element 'LevelOfAssurance' must be provided (minOccurs="1)' in the EvidenceRequest when rim:Slot[@name='LegalPerson'] is used.	Fatal
CodeList	BR-OOTS-REQ-044	LegalPerson	query:QueryRequest/query:Query/rim:Slot[@name='LegalPerson']/rim:SlotValue/LegalPerson/ LevelOfAssurance	The value of 'LevelOfAssurance' must be part of the code list 'LevelsOfAssuranceCode'	Fatal
Cardinality	BR-OOTS-REQ-045	LegalPerson	query:QueryRequest/query:Query/rim:Slot[@name='LegalPerson']/rim:SlotValue/LegalPerson/ LegalPersonIdentifier	The value of a Legal Person 'LegalPersonIdentifier' SHOULD be provided.	Warning

Rule Type	Rule ID	Element	Location	Rule	Flag
Format	BR-OOTS-REQ-046	LegalPerson	query:QueryRequest/query:Query/rim:Slot[@name='LegalPerson']/rim:SlotValue/LegalPerson/ LegalPersonIdentifier	The value of a 'LegalPersonIdentifier' MUST have the format XX/YY/ZZZZZZZ where XX is the Nationality Code of the identifier and YY is the Nationality Code of the destination country and ZZZZZZZ is an undefined combination of characters which uniquely identifies the identity asserted in the country of origin. Example: ES/AT/02635542Y	Fatal
CodeList	BR-OOTS-REQ-047	LegalPerson	query:QueryRequest/query:Query/rim:Slot[@name='LegalPerson']/rim:SlotValue/LegalPerson/ LegalPersonIdentifier	The value of a 'LegalPersonIdentifier' MUST have the format XX/YY/ZZZZZZZ where the values of XX and YY MUST be part of the code list 'CountryIdentificationCode' (ISO 3166-1' alpha-2 codes). Example: ES/AT/02635542Y	Fatal
Cardinality	BR-OOTS-REQ-048	LegalPerson	query:QueryRequest/query:Query/rim:Slot[@name='LegalPerson']/rim:SlotValue/LegalPerson/ LegalPersonIdentifier/@schemeID	The 'schemeID' attribute of 'LegalPersonIdentifier' MUST be present.	Fatal
FixedValue	BR-OOTS-	LegalPerson	query:QueryRequest/query:Query/rim:Slot[@name='LegalPerson']/rim:SlotValue/LegalPerson/ LegalPersonIdentifier/@schemeID	The 'schemeID' attribute of the 'LegalPersonIdentifier' MUST have the fixed value 'eidas'.	Fatal

Rule Type	Rule ID	Element	Location	Rule	Flag
	REQ-049				
Cardinality	BR-OOTS-REQ-050	LegalPerson	query:QueryRequest/query:Query/rim:Slot[@name='LegalPerson']/rim:SlotValue/LegalPerson/ Identifier/@schemeID	The 'schemeID' attribute of 'Identifier' MUST be present.	Fatal
CodeList	BR-OOTS-REQ-051	LegalPerson	query:QueryRequest/query:Query/rim:Slot[@name='LegalPerson']/rim:SlotValue/LegalPerson/ Identifier/@schemeID	The 'schemeID' attribute of the 'Identifier' MUST have be part of the code list 'IdentifierTypeCodes'.	Fatal
CodeList	BR-OOTS-REQ-052	LegalPerson	query:QueryRequest/query:Query/rim:Slot[@name='LegalPerson']/rim:SlotValue/LegalPerson/ RegisteredAddress/AdminUnitLevel1	The value of the 'AdminUnitLevel1' SHOULD be part of the code list the code list 'CountryIdentificationCode' (ISO 3166-1' alpha-2 codes).	Warning
CodeList	BR-OOTS-REQ-053	LegalPerson	query:QueryRequest/query:Query/rim:Slot[@name='LegalPerson']/rim:SlotValue/LegalPerson/ RegisteredAddress/AdminUnitLevel2	The value of the 'AdminUnitLevel2' SHOULD be part of the code list 'Nuts' (Nomenclature of Territorial Units for Statistics).	Warning
Cardinality	BR-OOTS-REQ-054	AuthorizedRepresentative	query:QueryRequest/query:Query/rim:Slot[@name='AuthorizedRepresentative']/rim:SlotValue/ Person/LevelOfAssurance	The Element 'LevelOfAssurance' must be provided (minOccurs="1)' in the EvidenceRequest when rim:Slot[@name='AuthorizedRepresentative'] is used.	Fatal

Rule Type	Rule ID	Element	Location	Rule	Flag
CodeList	BR-OOTS-REQ-055	AuthorizedRepresentative	query:QueryRequest/query:Query/rim:Slot[@name='AuthorizedRepresentative']/rim:SlotValue/ Person/LevelOfAssurance	The value of 'LevelOfAssurance' must be part of the code list 'LevelsOfAssuranceCode'	Fatal
Cardinality	BR-OOTS-REQ-056	AuthorizedRepresentative	query:QueryRequest/query:Query/rim:Slot[@name='AuthorizedRepresentative']/rim:SlotValue/ Person/Identifier	The value of a Person 'Identifier' SHOULD be provided.	Warning
Format	BR-OOTS-REQ-057	AuthorizedRepresentative	query:QueryRequest/query:Query/rim:Slot[@name='AuthorizedRepresentative']/rim:SlotValue/ Person/Identifier	The value of a Person 'Identifier' MUST have the format XX/YY/ZZZZZZZ where XX is the Nationality Code of the identifier and YY is the Nationality Code of the destination country and ZZZZZZZ is an undefined combination of characters which uniquely identifies the identity asserted in the country of origin. Example: ES/AT/02635542Y	Fatal
CodeList	BR-OOTS-REQ-058	AuthorizedRepresentative	query:QueryRequest/query:Query/rim:Slot[@name='AuthorizedRepresentative']/rim:SlotValue/ Person/Identifier	The value of Person 'Identifier' MUST have the format XX/YY/ZZZZZZZ where the values of XX and YY MUST be part of the code list 'CountryIdentificationCode' (ISO 3166-1' alpha-2 codes). Example: ES/AT/02635542Y	Fatal

Rule Type	Rule ID	Element	Location	Rule	Flag
Cardinality	BR-OOTS-REQ-059	AuthorizedRepresentative	query:QueryRequest/query:Query/rim:Slot[@name='AuthorizedRepresentative']/rim:SlotValue/ Person/Identifier/@schemeID	The 'schemeID' attribute of 'Identifier' MUST be present.	Fatal
FixedValue	BR-OOTS-REQ-060	AuthorizedRepresentative	query:QueryRequest/query:Query/rim:Slot[@name='AuthorizedRepresentative']/rim:SlotValue/ Person/Identifier/@schemeID	The 'schemeID' attribute of the 'Identifier' MUST have the fixed value 'eidas'.	Fatal
Format	BR-OOTS-REQ-061	AuthorizedRepresentative	query:QueryRequest/query:Query/rim:Slot[@name='AuthorizedRepresentative']/rim:SlotValue/ Person/DateOfBirth	The value of 'DateOfBirth' MUST use the following format YYYY + “-“ + MM + “-“ + DD (as defined for xsd:date)	Fatal
CodeList	BR-OOTS-REQ-062	AuthorizedRepresentative	query:QueryRequest/query:Query/rim:Slot[@name='AuthorizedRepresentative']/rim:SlotValue/ Person/Gender	The value of 'Gender' MUST be 'Male', 'Female' or 'Unspecified'.	Fatal
CodeList	BR-OOTS-REQ-063	AuthorizedRepresentative	query:QueryRequest/query:Query/rim:Slot[@name='AuthorizedRepresentative']/rim:SlotValue/ Person/CurrentAddress/AdminUnitLevel1	The value of the 'AdminUnitLevel1' SHOULD be part of the code list the code list 'CountryIdentificationCode' (ISO 3166-1' alpha-2 codes).	Warning
CodeList	BR-OOTS-	AuthorizedRepresentative	query:QueryRequest/query:Query/rim:Slot[@name='AuthorizedRepresentative']/rim:SlotValue/ Person/CurrentAddress/AdminUnitLevel2	The value of the 'AdminUnitLevel2' SHOULD be part of the code list 'Nuts'	Warning

Rule Type	Rule ID	Element	Location	Rule	Flag
	REQ-064			(Nomenclature of Territorial Units for Statistics).	

4.6.3 Business rules associated to the Evidence Response

The tables below collect the set of business rules affecting the creation of Evidence Response instances.

4.6.3.1 Business rules that prove the correct structure of Evidence Responses

Rule Type	Rule ID	Element	Location	Rule	Flag
Slot	BR-OOTS-RESP-ebRIM-001	SpecificationIdentifier	query:QueryResponse/rim:Slot[@name='SpecificationIdentifier']	The <rim:Slot name="SpecificationIdentifier"> MUST be present in the QueryResponse.	Fatal
Slot	BR-OOTS-RESP-ebRIM-002	EvidenceResponseIdentifier	query:QueryResponse/rim:Slot[@name='EvidenceResponseIdentifier']	The <rim:Slot name="EvidenceResponseIdentifier"> MUST be present in the QueryResponse.	Fatal
Slot	BR-OOTS-	IssueDateTime	query:QueryResponse/rim:Slot[@name='IssueDateTime']	The <rim:Slot name="IssueDateTime"> MUST be present in the QueryResponse.	Fatal

Rule Type	Rule ID	Element	Location	Rule	Flag
	RESP-ebRIM-003				
Slot	BR-OOTS-RESP-ebRIM-004	EvidenceProvider	query:QueryResponse/rim:Slot[@name='EvidenceProvider']	The <rim:Slot name="EvidenceProvider"> MUST be present in the QueryResponse.	Fatal
Slot	BR-OOTS-RESP-ebRIM-005	EvidenceRequester	query:QueryResponsee/rim:Slot[@name='EvidenceRequester']	The <rim:Slot name="EvidenceRequester"> MUST be present in the QueryResponse.	Fatal
Slot	BR-OOTS-RESP-ebRIM-006	ResponseAvailableDateTime	query:QueryResponse/rim:Slot[@name='ResponseAvailableDateTime']	The <rim:Slot name="ResponseAvailableDateTime"> MAY be present in the QueryResponse.	Note

Rule Type	Rule ID	Element	Location	Rule	Flag
Slot	BR-OOTS-RESP-ebRIM-007	EvidenceMetadata	query:QueryResponse/rim:RegistryObjectList/rim:RegistryObject/rim:Slot[@name='EvidenceMetadata']	The <rim:Slot name="EvidenceMetadata"> MUST be present in the RegistryObject.	Fatal
Slot	BR-OOTS-RESP-ebRIM-008	QueryResponse	query:QueryResponse	A 'query:QueryResponse' MUST not contain any other rim:Slots.	Fatal
DataType	BR-OOTS-RESP-ebRIM-009	SpecificationIdentifier	query:QueryResponse/rim:Slot[@name='SpecificationIdentifier']/rim:SlotValue	The <rim:SlotValue> of <rim:Slot name="SpecificationIdentifier"> MUST be of "rim:StringValueType"	Fatal
DataType	BR-OOTS-RESP-ebRI	EvidenceResponseIdentifier	query:QueryResponse/rim:Slot[@name='EvidenceResponseIdentifier']/rim:SlotValue	The <rim:SlotValue> of <rim:Slot name="EvidenceResponseIdentifier"> MUST be of "rim:StringValueType"	Fatal

Rule Type	Rule ID	Element	Location	Rule	Flag
	M-010				
DataType	BR-OOTS-RESP-ebRIM-011	IssueDateTime	query:QueryResponse/rim:Slot[@name='IssueDateTime']/rim:SlotValue	The <rim:SlotValue> of <rim:Slot name="IssueDateTime"> MUST be of "rim:DateTimeValueType"	Fatal
DataType	BR-OOTS-RESP-ebRIM-012	EvidenceProvider	query:QueryResponse/rim:Slot[@name='EvidenceProvider']/rim:SlotValue	The <rim:SlotValue> of <rim:Slot name="EvidenceProvider"> MUST be of "rim:CollectionValueType"	Fatal
DataType	BR-OOTS-RESP-ebRIM-013	EvidenceRequester	query:QueryResponsee/rim:Slot[@name='EvidenceRequester']/rim:SlotValue	The <rim:SlotValue> of <rim:Slot name="EvidenceRequester"> MUST be of "rim:AnyValueType"	Fatal
DataType	BR-OOTS-RES	ResponseAvailableDateTime	query:QueryResponse/rim:Slot[@name='ResponseAvailableDateTime']/rim:SlotValue	The <rim:SlotValue> of <rim:Slot name="ResponseAvailableDateTime"> MUST be of "rim:DateTimeValueType"	Fatal

Rule Type	Rule ID	Element	Location	Rule	Flag
	P-ebRIM-014				
DataType	BR-OOTS-RESP-ebRIM-015	EvidenceMetadata	query:QueryResponse/rim:RegistryObjectList/rim:RegistryObject/rim:Slot[@name='EvidenceMetadata']/ rim:SlotValue	The <rim:SlotValue> of <rim:Slot name="EvidenceMetadata> MUST be of "rim:AnyValueType"	Fatal
XSD-Binding	BR-OOTS-RESP-ebRIM-016	EvidenceProvider	query:QueryResponse/rim:Slot[@name='EvidenceProvider']/rim:SlotValue	The 'query:QueryResponse/rim:Slot[@name='EvidenceProvider']/rim:SlotValue' MUST use the '<xs:element name="Agent" type="sdg:AgentType" />' of the targetNamespace="http://data.europa.eu/p4s"	Fatal
XSD-Restriction	BR-OOTS-RESP-ebRIM-017	EvidenceProvider	query:QueryResponse/rim:Slot[@name='EvidenceProvider']/rim:SlotValue/Agent	An EvidenceProvider 'rim:SlotValue/Agent' MUST not contain any other elements than 'sdg:Identifier' and 'sdg:Name', 'Address'.	Fatal

Rule Type	Rule ID	Element	Location	Rule	Flag
XSD-Binding	BR-OOTS-RESP-ebRIM-018	EvidenceRequester	query:QueryResponse/rim:Slot[@name='EvidenceRequester']/rim:SlotValue/rim:Element	The 'query:QueryResponse/rim:Slot[@name='EvidenceRequester']/rim:SlotValue' MUST use the '<xs:element name="Agent" type="sdg:AgentType" />' of the targetNamespace="http://data.europa.eu/p4s"	Fatal
XSD-Restriction	BR-OOTS-RESP-ebRIM-019	EvidenceRequester	query:QueryResponse/rim:Slot[@name='EvidenceRequester']/rim:SlotValue/rim:Element/Agent	An EvidenceRequester "rim:SlotValue/Agent' MUST not contain any other elements than 'sdg:Identifier' and 'sdg:Name'.	Fatal
XSD-Binding	BR-OOTS-RESP-ebRIM-020	EvidenceMetadata	query:QueryResponse/rim:RegistryObjectList/rim:RegistryObject/rim:Slot[@name='EvidenceMetadata']/ rim:SlotValue	The 'query:QueryResponse/rim:RegistryObjectList/rim:RegistryObject/ rim:Slot[@name='EvidenceMetadata']/rim:SlotValue' MUST use the '<xs:element name="Evidence" type="sdg:EvidenceType" />' of the targetNamespace="http://data.europa.eu/p4s"	Fatal
XSD-Restriction	BR-OOTS-RESP-ebRI	EvidenceMetadata	query:QueryResponse/rim:RegistryObjectList/rim:RegistryObject/rim:Slot[@name='EvidenceMetadata']/ rim:SlotValue/Evidence/IsConformantTo	The class 'IsConformantTo' of 'Evidence' MUST not contain any other elements than 'sdg:Identifier' and 'sdg:Description'.	

Rule Type	Rule ID	Element	Location	Rule	Flag
	M-021				

4.6.3.2 Business rules that prove the correct use of information objects in Evidence Responses

Rule Type	Nr	Element	Location	Rule	Flag
Identifier	BR-OOTS-RESP-001	query:QueryResponse	query:QueryResponse/@requestID	The 'requestID' attribute of a 'QueryResponse' MUST be unique UUID (RFC 4122) and match the corresponding request.	Fatal
CodeList	BR-OOTS-RESP-002	query:QueryResponse	query:QueryResponse/@status	The 'status attribute of a 'QueryResponse' MUST be encoded as "urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Success" for successful responses or as "urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Unavailable" for responses that will be available at a later time .	Fatal
Identifier	BR-OOTS-RESP-003	SpecificationIdentifier	query:QueryResponse/rim:Slot[@name='SpecificationIdentifier']/rim:SlotValue/rim:Value	The 'rim:Value' of the 'SpecificationIdentifier' MUST be the fixed value "oots-edm:v1.0".	Fatal

Rule Type	Nr	Element	Location	Rule	Flag
Identifier	BR-OOTS-RESP-004	EvidenceResponseIdentifier	query:QueryResponse/rim:Slot[@name='EvidenceResponseIdentifier']/rim:SlotValue/rim:Value	The 'rim:Value' of the 'EvidenceResponseIdentifier' MUST be unique UUID (RFC 4122) for each response.	Fatal
Format	BR-OOTS-RESP-005	IssueDateTime	query:QueryResponse/rim:Slot[@name='IssueDateTime']/rim:SlotValue/rim:Value	The 'rim:Value' of 'IssueDateTime' MUST be according to xsd:dateTime.	Fatal
Format	BR-OOTS-RESP-006	ResponseAvailableDateTime	query:QueryResponse/rim:Slot[@name='IssueDateTime']/rim:SlotValue/rim:Value	The 'rim:Value' of 'ResponseAvailableDateTime' MUST be according to xsd:dateTime.	Fatal
Cardinality	BR-OOTS-RESP-007	EvidenceProvider	query:QueryResponse/rim:Slot[@name='EvidenceProvider']/rim:SlotValue/rim:Element/Agent/Identifier/@schemeID	The 'schemeID' attribute of 'Identifier' MUST be present.	Fatal
CodeList	BR-OOTS-RESP-008	EvidenceProvider	query:QueryResponse/rim:Slot[@name='EvidenceProvider']/rim:SlotValue/rim:Element/Agent/Identifier/@schemeID	The value of the 'schemeID' attribute of the 'Identifier' MUST be part of the code list 'EAS' (Electronic Address Scheme).	Fatal

Rule Type	Nr	Element	Location	Rule	Flag
CodeList	BR-OOTS-RESP-009	EvidenceProvider	query:QueryResponse/rim:Slot[@name='EvidenceProvider']/rim:SlotValue/rim:Element/Agent/Address/AdminUnitLevel1	The value of the 'AdminUnitLevel1' MUST be part of the code list 'CountryIdentificationCode' (ISO 3166-1 alpha-2 codes).	Fatal
CodeList	BR-OOTS-RESP-010	EvidenceProvider	query:QueryResponse/rim:Slot[@name='EvidenceProvider']/rim:SlotValue/rim:Element/Agent/Address/AdminUnitLevel2	The value of the 'AdminUnitLevel2' MUST be coded using the code list 'Nuts' (Nomenclature of Territorial Units for Statistics).	Fatal
Cardinality	BR-OOTS-RESP-011	EvidenceProvider	query:QueryResponse/rim:Slot[@name='EvidenceProvider']/rim:SlotValue/rim:Element/Agent/Classification	The value for 'Agent/Classification' MUST be provided.	Fatal
CodeList	BR-OOTS-RESP-012	EvidenceProvider	query:QueryResponse/rim:Slot[@name='EvidenceProvider']/rim:SlotValue/rim:Element/Agent/Classification	The value MUST be part of the code list 'AgentClassification'. Default value: Evidence Provider	Fatal
Cardinality	BR-OOTS-RESP-013	EvidenceRequester	query:QueryResponse/rim:Slot[@name='EvidenceRequester']/rim:SlotValue/Agent/Identifier/@schemeID	The 'schemeID' attribute of 'Identifier' MUST be present.	Fatal

Rule Type	Nr	Element	Location	Rule	Flag
CodeList	BR-OOTS-RESP-014	EvidenceRequester	query:QueryResponse/rim:Slot[@name='EvidenceRequester']/rim:SlotValue/Agent/Identifier/@schemeID	The value of the 'schemeID' attribute of the 'Identifier' MUST be part of the code list 'EAS' (Electronic Address Scheme).	Fatal
Identifier	BR-OOTS-RESP-015	RegistryObject	query:QueryResponse/rim:RegistryObjectList/rim:RegistryObject/@id	The 'id' attribute of a 'RegistryObject' MUST be unique UUID (RFC 4122).	Fatal
Identifier	BR-OOTS-RESP-016	Evidence	query:QueryResponse/rim:RegistryObjectList/rim:RegistryObject/rim:Slot[@name='EvidenceMetadata']/rim:SlotValue/ Evidence/ Identifier	The value of 'Identifier' of an 'Evidence' MUST be unique UUID (RFC 4122).	Fatal
Format	BR-OOTS-RESP-017	Evidence	query:QueryResponse/rim:RegistryObjectList/rim:RegistryObject/rim:Slot[@name='EvidenceMetadata']/rim:SlotValue/ Evidence/ IssuingDate	The value of 'IssuingDate' of an 'Evidence' MUST be be according to xsd:date.	Fatal
Codelist	BR-OOTS-RESP-018	Evidence	query:QueryResponse/rim:RegistryObjectList/rim:RegistryObject/rim:Slot[@name='EvidenceMetadata']/rim:SlotValue/ Evidence/ IsConformantTo/EvidenceTypeClassification	The value of 'EvidenceTypeClassification' of 'IsConformantTo' MUST be a URI with the following format 'http:://……' pointing to the Semantic Repository	Fatal

Rule Type	Nr	Element	Location	Rule	Flag
				encoded in the EvidenceBroker.	
CodeList	BR-OOTS-RESP-019	Evidence	query:QueryResponse/rim:RegistryObjectList/rim:RegistryObject/rim:Slot[@name='EvidenceMetadata']/rim:SlotValue/ Evidence/ IsConformantTo/Title/@lang	The value of 'lang' attribute MUST be part of the code list 'LanguageCode' (ISO 639-1 two-letter code).	Fatal
Cardinality	BR-OOTS-RESP-020	Evidence	query:QueryResponse/rim:RegistryObjectList/rim:RegistryObject/rim:Slot[@name='EvidenceMetadata']/rim:SlotValue/ Evidence/ IsConformantTo/Title/@lang	The value of 'lang' attribute MUST be be provided. Default value: 'en'.	Fatal
CodeList	BR-OOTS-RESP-021	Evidence	query:QueryResponse/rim:RegistryObjectList/rim:RegistryObject/rim:Slot[@name='EvidenceMetadata']/rim:SlotValue/ Evidence/ IsConformantTo/Description/@lang	The value of 'lang' attribute MUST be part of the code list 'LanguageCode' (ISO 639-1 two-letter code).	Fatal
Cardinality	BR-OOTS-RESP-022	Evidence	query:QueryResponse/rim:RegistryObjectList/rim:RegistryObject/rim:Slot[@name='EvidenceMetadata']/rim:SlotValue/ Evidence/ IsConformantTo/Description/@lang	The value of 'lang' attribute MUST be be provided. Default value: 'en'.	Fatal
Identifier	BR-OOTS-	Evidence	query:QueryResponse/rim:RegistryObjectList/rim:RegistryObject/rim:Slot[@name='EvidenceMetadata']/rim:SlotValue/ Evidence/ Distribution/ConformsTo	The value of 'ConformsTo' of the 'Distribution' MUST be a persistent URL pointing to	Fatal

Rule Type	Nr	Element	Location	Rule	Flag
	RESP-023			the Data Service Directory (Semantic Respository).	
CodeList	BR-OOTS-RESP-024	Evidence	query:QueryResponse/rim:RegistryObjectList/rim:RegistryObject/rim:Slot[@name='EvidenceMetadata']/rim:SlotValue/ Evidence/ Distribution/Format	The value of 'Format' of the 'Distribution' MUST be be part of the code list 'BinaryObjectMimeCode'.	Fatal
CodeList	BR-OOTS-RESP-025	Evidence	query:QueryResponse/rim:RegistryObjectList/rim:RegistryObject/rim:Slot[@name='EvidenceMetadata']/rim:SlotValue/ Evidence/ Distribution/PackagingFormat	The value of 'PackagingFormat' of the 'Distribution' MUST be be part of the code list 'BinaryObjectMimeCode'.	Fatal
CodeList	BR-OOTS-RESP-026	Evidence	query:QueryResponse/rim:RegistryObjectList/rim:RegistryObject/rim:Slot[@name='EvidenceMetadata']/rim:SlotValue/ Evidence/ Distribution/CompressionFormat	The value of 'CompressionFormat' of the 'Distribution' MUST be be part of the code list 'BinaryObjectMimeCode'.	Fatal
CodeList	BR-OOTS-RESP-027	Evidence	query:QueryResponse/rim:RegistryObjectList/rim:RegistryObject/rim:Slot[@name='EvidenceMetadata']/rim:SlotValue/ Evidence/ Distribution/Language	The value of 'Language' MUST be part of the code list 'Language Code' (two-letter ISO 639-1).	Fatal

Rule Type	Nr	Element	Location	Rule	Flag
Cardinality	BR-OOTS-RESP-028	Evidence	query:QueryResponse/rim:RegistryObjectList/rim:RegistryObject/rim:Slot[@name='EvidenceMetadata']/rim:SlotValue/ Evidence/ IsAboutNaturalPerson/Identifier	The value of a Person 'Identifier' SHOULD be provided.	Warning
Format	BR-OOTS-RESP-029	Evidence	query:QueryResponse/rim:RegistryObjectList/rim:RegistryObject/rim:Slot[@name='EvidenceMetadata']/rim:SlotValue/ Evidence/ IsAboutNaturalPerson/Identifier	The value of a Person 'Identifier' MUST have the format XX/YY/ZZZZZZZ where XX is the Nationality Code of the identifier and YY is the Nationality Code of the destination country and ZZZZZZZ is an undefined combination of characters which uniquely identifies the identity asserted in the country of origin. Example: ES/AT/02635542Y	Fatal
CodeList	BR-OOTS-RESP-030	Evidence	query:QueryResponse/rim:RegistryObjectList/rim:RegistryObject/rim:Slot[@name='EvidenceMetadata']/rim:SlotValue/ Evidence/ IsAboutNaturalPerson/Identifier	The value of Person 'Identifier' MUST have the format XX/YY/ZZZZZZZ where the values of XX and YY MUST be part of the code list 'CountryIdentificationCode' (ISO 3166-1 alpha-2 codes). Example: ES/AT/02635542Y	Fatal

Rule Type	Nr	Element	Location	Rule	Flag
Cardinality	BR-OOTS-RESP-031	Evidence	query:QueryResponse/rim:RegistryObjectList/rim:RegistryObject/rim:Slot[@name='EvidenceMetadata']/rim:SlotValue/ Evidence/ IsAboutNaturalPerson/Identifier/@schemeID	The 'schemeID' attribute of 'Identifier' MUST be present.	Fatal
FixedValue	BR-OOTS-RESP-032	Evidence	query:QueryResponse/rim:RegistryObjectList/rim:RegistryObject/rim:Slot[@name='EvidenceMetadata']/rim:SlotValue/ Evidence/ IsAboutNaturalPerson/Identifier@schemeID	The 'schemeID' attribute of the 'Identifier' MUST have the fixed value 'eidas'.	Fatal
Format	BR-OOTS-RESP-033	Evidence	query:QueryResponse/rim:RegistryObjectList/rim:RegistryObject/rim:Slot[@name='EvidenceMetadata']/rim:SlotValue/ Evidence/ IsAboutNaturalPerson/DateOfBirth	The value of 'DateOfBirth' MUST use the following format YYYY + “-“ + MM + “-“ + DD (as defined for xsd:date)	Fatal
Cardinality	BR-OOTS-RESP-034	Evidence	query:QueryResponse/rim:RegistryObjectList/rim:RegistryObject/rim:Slot[@name='EvidenceMetadata']/rim:SlotValue/ Evidence/ IsAboutLegalPerson/LegalIdentifier	The value of a Legal Person 'LegalPersonIdentifier' SHOULD be provided.	Fatal
Format	BR-OOTS-RESP-035	Evidence	query:QueryResponse/rim:RegistryObjectList/rim:RegistryObject/rim:Slot[@name='EvidenceMetadata']/rim:SlotValue/ Evidence/ IsAboutLegalPerson/LegalIdentifier	The value of a 'LegalIdentifier' MUST have the format XX/YY/ZZZZZZZ where XX is the Nationality Code of the identifier and YY is the Nationality Code of the	Fatal

Rule Type	Nr	Element	Location	Rule	Flag
				destination country and ZZZZZZZ is an undefined combination of characters which uniquely identifies the identity asserted in the country of origin. Example: ES/AT/02635542Y	
CodeList	BR-OOTS-RESP-036	Evidence	query:QueryResponse/rim:RegistryObjectList/rim:RegistryObject/rim:Slot[@name='EvidenceMetadata']/rim:SlotValue/ Evidence/ IsAboutLegalPerson/LegalIdentifier	The value of a 'LegalIdentifier' MUST have the format XX/YY/ZZZZZZZ where the values of XX and YY MUST be part of the code list 'CountryIdentificationCode' (ISO 3166-1 alpha-2 codes). Example: ES/AT/02635542Y	Fatal
Cardinality	BR-OOTS-RESP-037	Evidence	query:QueryResponse/rim:RegistryObjectList/rim:RegistryObject/rim:Slot[@name='EvidenceMetadata']/rim:SlotValue/ Evidence/ IsAboutLegalPerson/LegalIdentifier/@schemeID	The 'schemeID' attribute of 'LegalIdentifier' MUST be present.	Fatal
FixedValue	BR-OOTS-RESP-038	Evidence	query:QueryResponse/rim:RegistryObjectList/rim:RegistryObject/rim:Slot[@name='EvidenceMetadata']/rim:SlotValue/ Evidence/ IsAboutLegalPerson/LegalIdentifier/@schemeID	The 'schemeID' attribute of the 'LegalIdentifier' MUST have the fixed value 'eidas'.	Fatal

Rule Type	Nr	Element	Location	Rule	Flag
Cardinality	BR-OOTS-RESP-039	Evidence	query:QueryResponse/rim:RegistryObjectList/rim:RegistryObject/rim:Slot[@name='EvidenceMetadata']/rim:SlotValue/ Evidence/IssuingAuthority/Identifier/@schemeID	The 'schemeID' attribute of 'Identifier' MUST be present.	Fatal
CodeList	BR-OOTS-RESP-040	Evidence	query:QueryResponse/rim:RegistryObjectList/rim:RegistryObject/rim:Slot[@name='EvidenceMetadata']/rim:SlotValue/ Evidence/IssuingAuthority/Identifier/@schemeID	The value of the 'schemeID' attribute of the 'Identifier' MUST be part of the code list 'EAS' (Electronic Address Scheme).	Fatal
Format	BR-OOTS-RESP-041	Evidence	query:QueryResponse/rim:RegistryObjectList/rim:RegistryObject/rim:Slot[@name='EvidenceMetadata']/rim:SlotValue/ Evidence/ValidityPeriod/StartDate	The value of 'StartDate' of an 'ValidityPeriod' MUST be be according to xsd:dateTime.	Fatal
Format	BR-OOTS-RESP-042	Evidence	query:QueryResponse/rim:RegistryObjectList/rim:RegistryObject/rim:Slot[@name='EvidenceMetadata']/rim:SlotValue/ Evidence/ValidityPeriod/EndDate	The value of 'EndDate' of an 'ValidityPeriod' MUST be be according to xsd:dateTime.	Fatal
Format	BR-OOTS-RESP-043	RepositoryItemRef	query:QueryResponse/rim:RegistryObjectList/rim:RegistryObject/rim:RepositoryItemRef/@xlink:href	The value of the attribute "xlink:href" of "rim:RepositoryItemRef" MUST follow the URI scheme cid and start with 'cid:……'	Fatal

4.6.4 **Business r**ules associated to the Error Response

The tables below collect the set of business rules affecting the creation of Error Response instances.

4.6.4.1 Business rules that prove the correct structure of Error Responses

RuleType	Nr.	Element	Location	Rule	Flag
Slot	BR-OOTS-ERR-ebRIM-001	SpecificationIdentifier	query:QueryResponse/rim:Slot[@name='SpecificationIdentifier']	The <rim:Slot name="SpecificationIdentifier"> MUST be present in the QueryResponse.	Fatal
Slot	BR-OOTS-ERR-ebRIM-002	EvidenceResponseIdentifier	query:QueryResponse/rim:Slot[@name='EvidenceResponseIdentifier']	The <rim:Slot name="EvidenceResponseIdentifier"> MUST be present in the QueryResponse.	Fatal
Slot	BR-OOTS-ERR-ebRIM-003	ErrorProvider	query:QueryResponse/rim:Slot[@name='ErrorProvider']	The <rim:Slot name="ErrorProvider"> MUST be present in the QueryResponse.	Fatal
Slot	BR-OOTS-ERR-ebRI	EvidenceRequester	query:QueryResponsee/rim:Slot[@name='EvidenceRequester']	The <rim:Slot name="EvidenceRequester"> MUST be present in the QueryResponse.	Fatal

RuleType	Nr.	Element	Location	Rule	Flag
	M-004				
Slot	BR-OOTS-ERR-ebRIM-005	Timestamp	query:QueryResponse/rs:Exception/rim:Slot[@name='Timestamp']	The <rim:Slot name="Timestamp"> MUST be present in the rs:Exception.	Fatal
Slot	BR-OOTS-ERR-ebRIM-006	PreviewLocation	query:QueryResponse/rs:Exception/rim:Slot[@name='PreviewLocation']	The <rim:Slot name="PreviewLocation"> MAY be present in the rs:Exception.	Note
Slot	BR-OOTS-ERR-ebRIM-007	PreviewDescription	query:QueryResponse/rs:Exception/rim:Slot[@name='PreviewDescription']	The <rim:Slot name="PreviewDescription"> MAY be present in the rs:Exception.	Note
Slot	BR-OOTS-ERR-ebRIM-008	PreviewMethod	query:QueryResponse/rs:Exception/rim:Slot[@name='PreviewMethod']	The <rim:Slot name="PreviewMethod"> MAY be present in the rs:Exception.	Note

RuleType	Nr.	Element	Location	Rule	Flag
Slot	BR-OOTS-ERR-ebRIM-009	QueryResponse	query:QueryResponse	A 'query:QueryResponse' MUST not contain any other rim:Slots.	Fatal
Datatype	BR-OOTS-ERR-ebRIM-010	SpecificationIdentifier	query:QueryResponse/rim:Slot[@name='SpecificationIdentifier']/rim:SlotValue	The <rim:SlotValue> of <rim:Slot name="SpecificationIdentifier"> MUST be of "rim:StringValueType"	Fatal
Datatype	BR-OOTS-ERR-ebRIM-011	EvidenceResponseIdentifier	query:QueryResponse/rim:Slot[@name='EvidenceResponseIdentifier']/rim:SlotValue	The <rim:SlotValue> of <rim:Slot name="EvidenceResponseIdentifier"> MUST be of "rim:StringValueType"	Fatal
Datatype	BR-OOTS-ERR-ebRIM-012	ErrorProvider	query:QueryResponse/rim:Slot[@name='ErrorProvider']/rim:SlotValue	The <rim:SlotValue> of <rim:Slot name="ErrorProvider"> MUST be of "rim:CollectionValueType"	Fatal

RuleType	Nr.	Element	Location	Rule	Flag
Datatype	BR-OOTS-ERR-ebRIM-013	EvidenceRequester	query:QueryResponsee/rim:Slot[@name='EvidenceRequester']/rim:SlotValue	The <rim:SlotValue> of <rim:Slot name="EvidenceRequester"> MUST be of "rim:AnyValueType"	Fatal
Datatype	BR-OOTS-ERR-ebRIM-014	Timestamp	query:QueryResponse/rs:Exception/rim:Slot[@name='Timestamp']/rim:SlotValue	The <rim:SlotValue> of <rim:Slot name="Timestamp"> MUST be of "rim:DateTimeValueType"	Fatal
Datatype	BR-OOTS-ERR-ebRIM-015	PreviewLocation	query:QueryResponse/rs:Exception/rim:Slot[@name='PreviewLocation']/rim:SlotValue	The <rim:SlotValue> of <rim:Slot name="PreviewLocation"> MUST be of "rim:StringValueType"	Fatal
Datatype	BR-OOTS-ERR-ebRIM-016	PreviewDescription	query:QueryResponse/rs:Exception/rim:Slot[@name='PreviewDescription']/rim:SlotValue	The <rim:SlotValue> of <rim:Slot name="PreviewDescription"> MUST be of "rim:InternationalStringValueType"	Fatal

RuleType	Nr.	Element	Location	Rule	Flag
Datatype	BR-OOTS-ERR-ebRIM-017	PreviewMethod	query:QueryResponse/rs:Exception/rim:Slot[@name='PreviewMethod']/rim:SlotValue	The <rim:SlotValue> of <rim:Slot name="PreviewMethod"> MUST be of "rim:StringValueType"	Fatal

4.6.4.2 Business rules that prove the correct use of information objects in Error Responses

Rule Type	Nr	Element	Location	Rule	Flag
Identifier	BR-OOTS-ERR-001	query:QueryResponse	query:QueryResponse/@requestID	The 'requestID' attribute of a 'QueryResponse' MUST be unique UUID (RFC 4122) and match the corresponding request.	Fatal
CodeList	BR-OOTS-ERR-002	query:QueryResponse	query:QueryResponse/@status	The 'status' attribute of a 'QueryResponse' that is not successful MUST be encoded as "urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Failure".	Fatal
Identifier	BR-OOTS-ERR-003	SpecificationIdentifier	query:QueryResponse/rim:Slot[@name='SpecificationIdentifier']/rim:SlotValue/rim:Value	The 'rim:Value' of the 'SpecificationIdentifier' MUST be the fixed value "oots-edm:v1.0".	Fatal
Identifier	BR-OOT	EvidenceResponseIdentifier	query:QueryResponse/rim:Slot[@name='EvidenceResponseIdentifier']/rim:SlotValue/rim:Value	The 'rim:Value' of the 'EvidenceResponseIdentifier'	Fatal

Rule Type	Nr	Element	Location	Rule	Flag
	S-ERR-004			MUST be unique UUID (RFC 4122) for each response.	
Cardinality	BR-OOTS-ERR-005	ErrorProvider	query:QueryResponse/rim:Slot[@name='ErrorProvider']/rim:SlotValue/rim:Element/Agent/ Identifier/@schemeID	The 'schemeID' attribute of 'Identifier' MUST be present.	Fatal
CodeList	BR-OOTS-ERR-006	ErrorProvider	query:QueryResponse/rim:Slot[@name='ErrorProvider']/rim:SlotValue/rim:Element/Agent/ Identifier/@schemeID	The value of the 'schemeID' attribute of the 'Identifier' MUST be part of the code list 'EAS' (Electronic Address Scheme).	Fatal
CodeList	BR-OOTS-ERR-007	ErrorProvider	query:QueryResponse/rim:Slot[@name='ErrorProvider']/rim:SlotValue/rim:Element/Agent/ Address/AdminUnitLevel1	The value of the 'AdminUnitLevel1' MUST be part of the code list 'CountryIdentificationCode' (ISO 3166-1 alpha-2 codes).	Fatal
CodeList	BR-OOTS-ERR-008	ErrorProvider	query:QueryResponse/rim:Slot[@name='ErrorProvider']/rim:SlotValue/rim:Element/Agent/ Address/AdminUnitLevel2	The value of the 'AdminUnitLevel2' MUST be coded using the code list 'Nuts' (Nomenclature of Territorial Units for Statistics).	Fatal
Cardinality	BR-OOTS-ERR-009	ErrorProvider	query:QueryResponse/rim:Slot[@name='ErrorProvider']/rim:SlotValue/rim:Element/Agent/ Classification	The value for 'Agent/Classification' MUST be provided.	Fatal

Rule Type	Nr	Element	Location	Rule	Flag
CodeList	BR-OOTS-ERR-010	ErrorProvider	query:QueryResponse/rim:Slot[@name='ErrorProvider']/rim:SlotValue/rim:Element/Agent/ Classification	The value MUST be part of the code list 'AgentClassification'. Default value: Error Provider	Fatal
Cardinality	BR-OOTS-ERR-011	EvidenceRequester	query:QueryResponse/rim:Slot[@name='EvidenceRequester']/rim:SlotValue/Agent/ Identifier/@schemeID	The 'schemeID' attribute of 'Identifier' MUST be present.	Fatal
CodeList	BR-OOTS-ERR-012	EvidenceRequester	query:QueryResponse/rim:Slot[@name='EvidenceRequester']/rim:SlotValue/Agent/ Identifier/@schemeID	The value of the 'schemeID' attribute of the 'Identifier' MUST be part of the code list 'EAS' (Electronic Address Scheme).	Fatal
Cardinality	BR-OOTS-ERR-013	rs:Exception	query:QueryResponse/rs:Exception	The 'rs:Exception' class of a 'QueryResponse' MUST be present if 'status' attribute of a 'QueryResponse' is "urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Failure".	Fatal
Cardinality	BR-OOTS-ERR-014	rs:Exception	query:QueryResponse/rs:Exception/@xsi:type	The 'xsi:type' attribute of a 'rs:Exception' MUST be present.	Fatal
CodeList	BR-OOT	rs:Exception	query:QueryResponse/rs:Exception/@xsi:type	The value of 'xsi:type' attribute of a 'rs:Exception' MUST be	Fatal

Rule Type	Nr	Element	Location	Rule	Flag
	S-ERR-015			part of the code list 'ProtocolExceptionCode'.	
Cardinality	BR-OOTS-ERR-016	rs:Exception	query:QueryResponse/rs:Exception/@severity	The 'severity' attribute of a 'rs:Exception' MUST be present.	Fatal
CodeList	BR-OOTS-ERR-017	rs:Exception	query:QueryResponse/rs:Exception/@severity	The value of 'severity' attribute of a 'rs:Exception' MUST be part of the code list 'ErrorSeverity'.	Fatal
Cardinality	BR-OOTS-ERR-018	rs:Exception	query:QueryResponse/rs:Exception/@message	The 'message' attribute of a 'rs:Exception' MUST be present.	Fatal
CodeList	BR-OOTS-ERR-019	rs:Exception	query:QueryResponse/rs:Exception/@code	The value of 'code' attribute of a 'rs:Exception' MUST be part of the code list 'Error Codes'.	Fatal
Format	BR-OOTS-ERR-020	Timestamp	query:QueryResponse/rs:Exception/rim:Slot[@name='Timestamp']/rim:SlotValue/rim:Value	The 'rim:Value' of 'Timestamp' MUST be according to xsd:dateTime.	Fatal

Rule Type	Nr	Element	Location	Rule	Flag
Identifier	BR-OOTS-ERR-021	PreviewLocation	query:QueryResponse/rs:Exception/rim:Slot[@name='PreviewLocation']/rim:SlotValue/rim:Value	The 'rim:Value' of a 'PreviewLocation' MUST be a URI starting with 'https://'.	Fatal
CodeList	BR-OOTS-ERR-022	PreviewDescription	query:QueryResponse/rs:Exception/rim:Slot[@name='PreviewDescription']/rim:SlotValue/rim:Value	The 'language' attribute of 'PreviewDescription' MUST be specified using the code list 'LanguageCode' (ISO 639-1 two-letter code).	Fatal
CodeList	BR-OOTS-ERR-023	PreviewMethod	query:QueryResponse/rs:Exception/rim:Slot[@name='PreviewMethod']/rim:SlotValue/rim:Value	The 'rim:Value' of a 'PreviewMethod' MUST be either the HTTP verb 'GET' or 'POST'.	Fatal

4.7 eDelivery Configuration - June 2022

4.7.1 Four Corner Topology in OOTS

The OASIS ebMS3 and AS4 specifications are specifications for point-to-point message exchange between two Message Service Handlers. However, eDelivery AS4 is also used in situations where Access Points exchange messages on behalf of other parties. This message exchange pattern is also followed in OOTS. The four parties are conventionally referred to using *Cn* labels, where *C* stands for "corner", and the *n* is one of the digits 1 to 4:

- *C1* is the original sender party, which can be:
  - The Evidence Requester that submits an Evidence Request Query;
  - The Evidence Provider submitting an Evidence Response asynchronously to an Evidence Request Query.

- *C2* is an Access Point that sends messages on behalf of *C1*.
- *C3* is an Access Point that receives messages on behalf of *C4.*
- *C4* is the final recipient party, which can be:
    - the Evidence Provider that receives the Evidence Request Query;
    - the Evidence Requester receiving an Evidence Response asynchronously to an Evidence Request Query.

4.7.2 Routing Metadata

4.7.2.1 Party Identification

When used in a Four Corner topology, the sender and receiver of the ebMS messages are the Access Points that act on behalf of the Evidence Requester and Provider. This implies that the ebMS message header by default contains the Access Point identifiers as sender and receiver. Using an eDelivery AS4 profile enhancement, however, the outer corners, i.e. the *Evidence Requester* and *Provider*, can be included in the ebMS message header. In these enhancements, the ebMS3 message property mechanism includes the identifiers of C1 and C4. This allows the use of arbitrary property-value pairs in an AS4 message and is independent of payload format or structure.

When used in a Four Corner typology:

- A property named **originalSender** MUST be added to the message that identifies the original sender (C1) Party;
- A property named **finalRecipient** MUST be added to the message that identifies the final recipient (C4) Party.

For the identification of the Access Points in the ebMS message header, i.e. the values to be used in the `//To/PartyId` element are extracted from the DSD Response as shown in the table below. As the sender of the message in a Four Corner architecture, needs to "find" the Access Point used by the receiving party, the receiving AP's identifier is determined on runtime.
As specified in section 5.2.2.4 of [EBMS3], the `type` attribute is required if the party identifier is not a URI. Unless otherwise specified for specific domain profiles, the value *urn:oasis:names:tc:ebcore:partyid-type:unregistered* SHOULD be used.

4.7.2.2 DSD Derived Routing Metadata

The OOTS eDelivery architecture consists of multiple statically pre-configured Access Points. Although the configuration of the APs is static, the receiving endpoint is dynamically provided using the DSD Response. So although the list of APs and their configurations is static, a Data Service can dynamically change between existing APs by updating the AP identifier in the DSD. Using a DSD lookup, the Evidence Requester is able to extract the necessary metadata to match with a pre-existing PMode. The following table specifies the PMode parameters that are mapped from specific DSD Access Service Metadata Elements.

AS4 PMode Parameter	Corresponding Structure in DSD XML	Implementation Notes
PMode[].BusinessInfo.Properties[finalRecipient]	`//DataServiceEvidenceType/AccessService/EvidenceProvider/Identifier`	URL encoding MUST NOT be used.
PMode[].Responder.Party	`//DataServiceEvidenceType/AccessService/Identifier`	

Table 1 Pmode Attribute Mappings

4.7.2.3 Static Routing Metadata

The above section defines how the sender should configure its AS4 gateway's PMode parameters related to the receiver to set up the message exchange with the receiver. Besides these dynamically set parameters, there are also PMode parameters on both the sender and receiver side, which relate to the parties themselves or which values are predefined by the eDelivery profile and independent of the counterparty. These parameters can, therefore, be statically configured. The next two paragraphs specify the statically configured PMode parameters, which are profiled specifically for the OOTS eDelivery architecture.

Sender

For the Sender, the following PMode parameters can be statically configured:

- **PMode[].Initiator.Party** : TBD.
- **PMode[].Initiator.Party/@type**: fixed value: *urn:oasis:names:tc:ebcore:partyid-type:unregistered* unless specified otherwise by a domain.
- **PMode[].Initiator.Role** : MUST be set to fixed value *http://sdg.europa.eu/edelivery/gateway.*
- **PMode[].BusinessInfo.Properties[originalSender]**: the identifier of the competent authority that is sending the message. Note: When the AP services multiple competent authorities, this parameter can also be set dynamically to prevent that, for each competent authority, a separate P-Mode is needed (which only differs for this parameter).
- **PMode[].BusinessInfo.Properties[originalSender]/@type** : not used.
- **PMode[].BusinessInfo.Service:** Follows the rules of the ebXML Messaging Protocol Binding for RegRep Version 1.0
- **PMode[].BusinessInfo.Action:** Follows the rules of ebXML Messaging Protocol Binding for RegRep Version 1.0
- **PMode.MEP**: fixed value : http://www.oasis-open.org/committees/ebxml-msg/one-way.

Receiver

For the Receiver, the following PMode parameters can be statically configured:

- **PMode[].Responder.Party** : TBD.
- **PMode[].Responder.Party/@type:** fixed value: *urn:oasis:names:tc:ebcore:partyid-type:unregistered* unless specified otherwise by a domain.
- **PMode[].Responder.Role** : MUST be set to fixed value *http://sdg.europa.eu/edelivery/gateway.*
- **PMode[].BusinessInfo.Properties[finalRecipient]** : the identifier of the competent authority for whom the AP is receiving the message.
- **PMode[].BusinessInfo.Properties[finalRecipient]/@type** : not used.
- **PMode[].Security.X509.Encryption.Certificate** : the AP's Certificate.
- **PMode[].BusinessInfo.Service:** Follows the rules of the ebXML Messaging Protocol Binding for RegRep Version 1.0.
- **PMode[].BusinessInfo.Action:** Follows the rules of ebXML Messaging Protocol Binding for RegRep Version 1.0.
- **PMode[].Security.X509.Signature.Certificate**: the AP's Certificate. Like the sender's certificate, the AP MUST use the *Binary Security Token Reference* to include the messages' certificate.
- **PMode.MEP**: fixed value : http://www.oasis-open.org/committees/ebxml-msg/one-way.

4.7.2.4 Reverse Routing for Evidence Provider Submission to Evidence Requester

The evidence provider needs to send back the response to the Evidence Requester using eDelivery AS4. To properly route the message back to the Evidence Requester, the Evidence provider access services must apply reverse routing of the received message. Reverse routing is achieved by applying the following rules:

- The Responder Party information of the request message becomes the Initiator Party of the response message
- The originalSender of the request message becomes the finalRecipient of the response message
- The Initiator Party information of the request message becomes the Responder Party of the response message
- The finalRecipient of the request message becomes the originalSender of the response message

The rest of the PMode attributes remain unchanged.

4.7.2.5 Message Exchange Pattern

The use of eDelivery is limited to the One Way MEP. OOTS eDelivery messages shall not include a *RefToMessageId* header.

The initial request message containing an evidence request shall contain a unique, previously unused value for the *ConversationId* header. A message containing an evidence response or evidence error response shall use as value for the *ConversationId* header the value used in the corresponding evidence request.

In the sequence of two request-response exchanges used to support the Preview Service described in 4.9 - Evidence Preview - June 2022, the request message and evidence response or evidence error response messages in the second request-response pair shall reuse the conversation identifier of the first request-response pair, in order to allow correlation of the two parts of the interaction.

If, in the context of a single user session, multiple requests are issued to a Data Service, the requests shall have the same conversation identifier value. This allow the Data Service and/or its Preview Space to correlate the request and detect that they relate to the same user session. This may be used to optimize the user experience.

Interactive interactions are common in eDelivery deployments with complete round-trip conversations able to be completed in sub-second timings, as demonstrated in test environments like the OOTS Simulator, supporting a good interactive user experience.

4.7.2.6 Payload Routing Metadata

When the message exchanged between two Access Points is an EDM Response, it can contain multiple ebMS payloads, one being the main ebXML RegRep response document and the other business attachments referenced from the ebXML RegRep response. To facilitate the processing of the EDM Response by the receiving Access Point, the ebMS header should indicate which payload contains the main ebXML RegRep document and which the attachments. Therefore the sending AP MUST set a part property named *MimeType* for each payload included in the message. The value of the property MUST be the MIME type of the payload, which for the ebXML RegRep document is defined as *application/x-ebrs+xml*.

4.7.3 Access Point Interconnectivity

For OOTS, eDelivery form a point-to-point exchange network of Access Points that are fully preconfigured and interconnected such that:

- Different sub-networks exist for production and test.
- Within a sub-network:
    - Network security rules (IP whitelists, blacklists) are configured such that any Access Point accepts establishing secure HTTPS connections from any of the other Access Points.
    - Any Access Point can send eDelivery AS4 test messages to, and receive such test messages from, any other Access Point, where test message is a message related to the test service defined in section 3.2.4 of the eDelivery AS4 specification.
    - Evidence Requests can be made from any Access Point to any of the other OOTS Access Points.
    - Evidence Responses and Evidence Error Responses can be made from any Access Point to any of the other OOTS Access Points.

Member States shall deploy at least one Access Point but may deploy multiple Access Points. Each Data Service and Online Procedure Portal instance shall be configured to use at most one Access Point. For Data Services, this configuration is reflected in the Data Service Directory as described in section 2.2 above.

Pre-configuration of Access Points includes the configuration of certificates for message signing and encryption, for every pair of Access Points. As explained in the eDelivery AS4 specification, the test service can be used to verify the proper configuration of network security (firewall rules etc.) and of eDelivery configurations (trusted certificates, algorithms etc.).

4.8 Evidence Exchange Logging - June 2022

4.8.1 Introduction

To support the operation of the OOTS, events related to the use of the system need to be logged. Legal requirements for logging are defined in Article 17 of the draft Implementing Act. The article covers specifics for evidence exchange in 17(1) and also provides general requirements.

This section covers logging functionality related to evidence exchange, and more specifically specifies the logging requirements on the relevant sub-system categories involved in evidence exchange: the evidence requester systems (Online Procedure Portals and Preview Areas), evidence provider systems (Data Services) and the eDelivery Access Points.

4.8.2 Objectives

Article 17(5) states that competent authorities shall make log data available to each other on request in case of “strong suspicion of incidents and for the purposes of audits and random checks of security”. More generally, and on a voluntary basis, log data can possibly also support:

- troubleshooting of OOTS (whether in testing, acceptance, production setup and operation) by IT specialists of connected competent authorities.
- handle support requests raised by users of the OOTS.

In OOTS, as explained in Chapter 1: Introduction - High Level Architecture - June 2022 section 7.4, eDelivery provides, in a delegated role, support for integrity, confidentiality, authenticity and non-repudiation of origin and receipt as explained in the CEF Security Controls guidance document. Non-repudiation is a requirement for evidence exchange as explained in section 2 of the HLA. The logging of eDelivery event data as required by Article 18(1)(c) provides the non-repudiation feature for OOTS evidence exchange.

4.8.3 Log data correlation

Since the OOTS is not a single monolithic system, but a collection of sub-systems of different competent authorities in different Member States, the OOTS log system is similarly not a single system but an abstraction for the logging of the various sub-systems.

The flow of an evidence request, and the reverse flow of the evidence response, corresponds to a series of events in various components. Both flows also involve lower-level technical eDelivery signals that support reliable messaging, non-repudiation and error handling. To log the complete flows, events generated in different modules and related log data need to be correlated.

Different components process and have access data elements. Multiple layers in message structures and their packaging and un-packaging results in different sets of identifiers. Storage of content data (including personal data) in event logs can be avoided by using unique identifiers and identifier correlation.

In this section, Evidence Requester generalizes over Online Procedure Portal and Preview Area. Both these and Data Services can also be provided using intermediary platforms.

4.8.3.1 Evidence Request

According to article 18(1)(a), the evidence request must be logged. The following table lists identifiers in the evidence request data model that enable correlation of log data and where they are processed.

Data to be logged	Source from which data can be be captured	Evidence Requester	Access Points	Data Service	Preview Space
Party identifier for requesting competent authority	originalSender @type attribute and content (eDelivery)		*		
	Agent Identifier @schemeID attribute and content in RegRep4 EvidenceRequester slot (RegRep4)	*		*	
Party identifier for providing competent authority	finalRecipient @type attribute and content (eDelivery)		*		
	Agent Identifier @schemeID attribute and content in RegRep4 EvidenceProvider slot (RegRep4)	*		*	
Identifier for the evidence request and reverse response flows	eb:ConversationId (eDelivery)	*	*	*	
Message Identifier	eb:MessageId (eDelivery)	*	*	*	

Evidence Request identifier	query:QueryRequest/ @id (RegRep4)	*		*	
Evidence Subject	A NaturalPerson, LegalPerson or Representative Slot, filled with attributes from eIDAS or supplied by the user.	*		*	
Preview Location	Content of the PreviewLocation slot and URL visited by user	*			*
Non-Repudiation Information	eb:Messaging and wsse:Security headers from eDelivery AS4 message (eDelivery) For evidence responses, includes signed hash values of all MIME evidence content payload parts to which eDelivery compression has been applied.		*		
	Signature validation date and time and outcome (success or error; eDelivery)		*		
	MIME type and full content of first MIME part (includes query:QueryRequest metadata document).	*		*	

4.8.3.2 Evidence Response and Evidence Error

According to article 17(1)(b), for the evidence response, the information included in the evidence response, with the exception of the evidence itself, must be logged. For the error response, an error report is sent and logged. For the error that transports preview information, the preview location is logged.

For this flow, the following table lists identifiers that enable correlation of log data.

Data to be logged	Source from which data can be be captured	Evidence Requester	Access Points	Data Service	Preview Space
Party identifier for requesting competent authority	finalRecipient @type attribute and content (eDelivery)		*		
	Agent Identifier @schemeID attribute and content in RegRep4 EvidenceRequester slot (RegRep4)	*		*	
Party identifier for providing competent authority	originalSender @type attribute and content (eDelivery)		*		
	Agent Identifier @schemeID attribute and content in RegRep4 EvidenceProvider slot (RegRep4)	*		*	

Identifier for the evidence request and reverse response flows	eb:ConversationId (eDelivery)	*	*	*	
Message Identifier	eb:MessageId (eDelivery)	*	*	*	
Evidence Request identifier	query:QueryResponse/ @RequestId (RegRep4)	*		*	
Evidence Response Identifier	rim:SlotValue/ rim:Value content for EvidenceResponseIdentifier Slot (RegRep4)	*		*	
Evidence Identifier (for evidence response)	Evidence/ Identifier value in EvidenceMetadata Slot (RegRep4)	*		*	
Error report (for error response)	rs:Exception element	*		*	
Preview Location	PreviewLocation Slot content and URL visited	*		*	*

For responses, the following table summarizes log data supporting non-repudiation. Note that for non-repudiation to work, the evidence provider must have a record, for each piece of evidence it exchanged using OOTS, in an eDelivery message part referenced using a rim:RepositoryItemRef, to the actual identical evidence content for the evidence. The ds:SignedInfo in the AS4 message includes the ds:DigestValue for that content, after GZIP application.

Data to be logged	Source from which data can be be captured	Evidence Requester	Access Points	Data Service	Preview Space
Non-Repudiation Information	eb:Messaging and wsse:Security headers from eDelivery AS4 message (eDelivery) For evidence responses, includes signed hash values of all MIME evidence content payload parts to which eDelivery compression has been applied.		*		
	Signature validation date and time and outcome (success or error; eDelivery)		*		
	MIME type and full content of first MIME part (includes query:QueryResponse metadata document which, for evidence responses, includes one or more rim:RepositoryItemRef elements and, for error response, an rs:Exception)	*		*	

	For evidence content referenced using rim:RepositoryItemRef elements , MIME type, MIME content identifier and MIME part content (or mechanism to dereference mechanism to retrieve them from a separate system).	*	*	*	

4.8.4 Message Acknowledgment, Error or Fault

Any OOTS evidence exchange protocol message uses eDelivery, and therefore for both evidence request and evidence response or evidence error messages, eDelivery protocol level responses are generated. Three such responses are AS4 receipts, AS4 errors, and SOAP Faults.

All logging related to these messages and the events they report is handled at the level of eDelivery Access Points as shown:

Data to be logged	**Source from which data can be be captured**	**Evidence Requester**	**Access Points**	**Data Service**	**Preview Space**
Correlation identifier (for Acknowledgment)	eb:RefToMessageId		*		
Correlation identifier (for Error)	eb:RefToMessageInError		*		
Error information	eb:Error/ @shortDescription, eb:Description and eb:ErrorDetail		*		
Fault information	soap:Fault/ Code and Reason		*		
Non-Repudiation of Receipt (for Acknowledgments)	eb:Messaging and wsse:Security headers from eDelivery AS4 message, including the eb:Receipt		*		
Message Non-Repudiation Information	Signature data and time validation outcome (success or error)		*		

4.8.5 Non-Repudiation

The OOTS relies on eDelivery and the OOTS log system for non-repudiation. For an OOTS message:

- Non-repudiation of origin protects against the originator’s false denial of having originated the message.
- Non-repudiation of receipt protects against the recipient's false denial of having received and recognized the content of the message.

For example: an evidence requester that has received a particular piece of evidence with a particular evidence identifier from an evidence provider can use the following trace for non-repudiation of origin:

- For the evidence identifier, find the related evidence response that carried it.
- Apply GZIP (eDelivery compression algorithm) to the evidence content data and compute its digest.
- From the evidence response identifier, find the Message Identifier of the evidence response eDelivery message that carried it, and MIME content identifier in which it was packaged.
- From the eDelivery message identifier, obtain the eDelivery message non-repudiation metadata (Signed Info).
- From the non-repudiation metadata, obtain the digest value.
- Verify that the evidence content has not been altered since it was transmitted to the Evidence Requester Access Point.

For example, an evidence provider that has sent a particular piece of evidence with a particular evidence identifier to an evidence requester can use the following trace for non-repudiation of receipt.

- For the evidence identifier, find the related evidence response that carried it.
- From the evidence response identifier, find the Message Identifier of the evidence response eDelivery message that carried it, and MIME content identifier in which it was packaged.
- From the eDelivery message identifier, obtain the eDelivery message non-repudiation metadata (Signed Info).
- Verify that the compressed evidence content digest matches the value for the eDelivery MIME part that has the MIME content identifier.
- Apply GZIP (eDelivery compression algorithm) to the evidence content data and compute its digest.
- Verify that the Access Point received an AS4 non-repudiation receipt from the Access Point of the evidence requester.

4.8.6 Log System Security and Privacy

Article 17(5) requires the OOTS to ensure the confidentiality, integrity and availability of the OOTS logs through appropriate and proportionate security measures, each for the logs that is has recorded.

Evidence requests and evidence content in evidence responses hold personal data. However, any storage of this content by the eDelivery Access Points for operational message exchange is temporary. Logging for these components can be set up such that no personal data is stored in the log sub-system. For logging and non-repudiation just having the hashes of evidence content can be enough. But parties must be able to provide the full evidence content in case of a dispute.

4.8.7 Log System Interchange Format (Informative)

A future release of the Technical Design Documents will provide an interchange format for log system data to support Article 17(5) of the draft Implementing Regulation.

4.9 Evidence Preview - June 2022

4.9.1 Introduction

This version of the OOTS includes support for an updated Evidence Preview Service feature. A component that implements the service is referred to using the term Preview Space. This specification aims to define a service with the following main features:

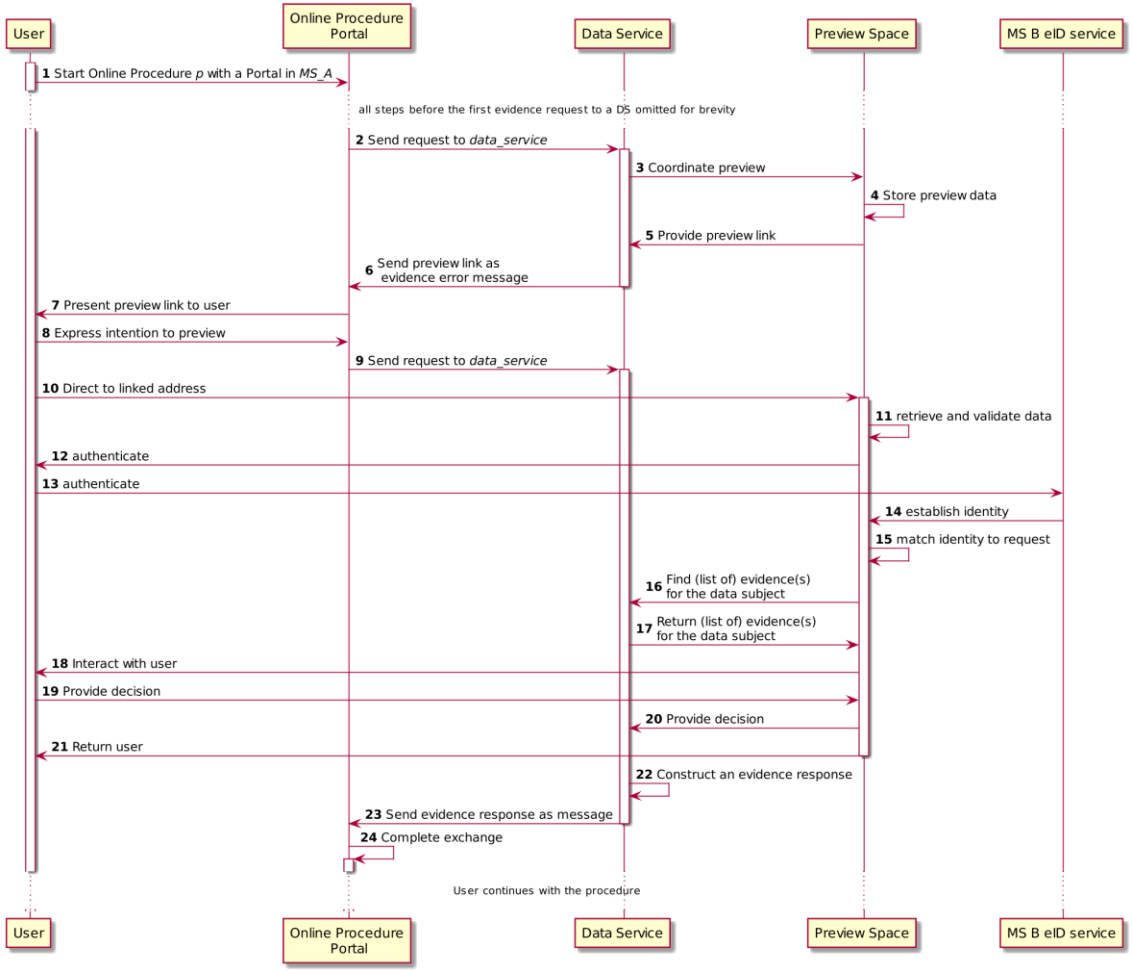
- The service is provided by or on behalf of an Evidence Provider.
- The service complements and supports the Data Service of the Evidence Provider.
- A single Preview Space may serve more than one Data Service and more than one Evidence Provider.
- A Data Service may use different Preview Spaces (for example, for different evidence types).
- The operation of the preview service is linked to the regular processing of the Data Service as further detailed in 2 and 3 below.
- The operation of the preview service is linked to the regular processing of the Online Procedure Portal as further detailed in 5 below.
- The Preview Space may be implemented as an integrated feature of a Data Service component or as a standalone component.
- Use of the service by a user for a particular evidence request is identified by a preview URL (Uniform Resource Locator). This URL is also the means for the user to access the service.
- The preview URL shall be unique to the request and therefore to the user, requested evidence type, evidence requester and evidence provider that the request relates to. However, the specific format for the URL is up to the implementation.
- The preview URL is communicated by the Data Service to the Online Procedure Portal, along with other preview metadata as described below in section 4, as a response to an initial evidence request.
- Any pieces of evidence selected for use in the procedure are returned by the Data Service to the Online Procedure Portal, as a response to a second follow-on request that includes a previously provided preview URL. This response is made after the user completes his or her interaction with the Preview Space for the specified URL.

- The Preview Space may ask the user to re-authenticate himself or herself as an additional security control, complementing and confirming the prior authentication of the user on the side of the Online Procedure Portal. This is an implementation and/or policy decision.
- The Preview Space may use re-authentication to help to uniquely identify the user, in case the identity attributes in the evidence request (based on the authentication of the user to the Online Procedure Portal) are not unique to a single person.
- The Preview Space shall allow the user to decide, for each piece of evidence matching the evidence request, whether or not to use it in the procedure.
- Before deciding whether or not to use a piece of evidence, the Preview Space shall offer the user the option to preview it. However, under the SDG regulation the user is not obliged to preview.
- The details of user experience, interaction and user interfaces are out of scope for this specification but this does not affect interoperability.
- The Preview Space shall also facilitate the smooth navigation of the user back to the Online Procedure Portal to allow him or her to continue the online procedure that he or she was executing as described in section 5 below.
- The Preview Space, like all OOTS components, may be integrated indirectly, using integration middleware.

4.9.2 Evidence Preview Service Flow

The OOTS Preview feature consists of two separate but related evidence request-response message flows, executed in sequence. The first of these flows is a machine-to-machine flow, in which the response is to be returned immediately. The second of these flows occurs in parallel to an interactive preview browsing session. The response is only sent after completion of that session, which in many cases could be minutes after the request.

The following diagram specifies an expected successful operation of preview feature and the expected processing of the Preview Space and Data Service. Variations and exceptions are explained in the summary table following the diagram.



Step	Description	Notes
1	The procedure starts when the user, while executing an electronic	This step is provided for context purposes only. The diagram omits the user authentication steps and the interaction with common services.

	procedure, is offered to use the OOTS to retrieve evidence.	
2-8	The first request-response loop is executed.	
2	The evidence request is sent to the Data Service.	As a result of the preceding steps (authentication, interaction with common services), the Online Procedure Portal constructs a an evidence request containing a *query:QueryRequest* as specified in section 4.5.1. Unlike the similar evidence request in step 9, this request does not include the "*PreviewLocation*" Slot.
3, 5	The Data Service and the Preview Service prepare and coordinate for the evidence preview.	In this step, a unique preview URL is generated and shared between the Preview Space and the Data Service. This serves to allow the two services to synchronize their operation in the second flow. Therefore the URL should be uniquely linked to the evidence request.
4	The Preview Service stores data.	Data is to be stored to prepare the Preview Space for the visiting user and to allow identity matching and request validation. Stored data should include: • The preview URL. • Subject to implementation, a validity end date time for the URL (after which the link is no longer valid). • All *rim:Slots* of *query:QueryRequest* except *IssueDateTime* and their content. • The value of the *query:QueryRequest* attribute *id*. • All *rim:Slots* of *query:QueryRequest/query:Query* element. • Attributes of the eDelivery AS4 *eb:Messaging* header including the conversation identifier. Alternatively, the data could be stored by the Data Service and retrieved (see step 11) by the Preview Space, or in a separate component.
6	The preview URL is returned to the Online Procedure Portal	The message format is that of an evidence error response message, see section 4.5.3, where: • The exception shall be of the ebRS type *rs:AuthorizationExceptionType*. • The *rs:Exception* shall contain a "*PreviewLocation*" slot. This slot provides preview location metadata structure as defined in section 3 below. This response is a response that is sent to the Online Procedure Portal in preparation of the second interaction.

		• The *rs:Exception* shall also contain a "*PreviewMethod*" slot. This allows the use of the appropriate HTTP method when directing the user. • The *rs:Exception* may contain a "*PreviewLocationDescription*" slot. Its content and purpose is explained in section 3 below.
7, 8	The Online Procedure Portal informs the user that the Data Service indicated that he or she needs to navigate to the Preview Space.	This can be done by presenting a clickable hyperlink, derived from the "*PreviewLocation*" and "*PreviewMethod*" as described in section 4 below. If provided, the content of the "*PreviewLocationDescription*" slot can used in the link. The Online Procedure Portal can filter the natural language alternatives to match its presentation language or (if known) user preference.
9-23	The second request-response flow is executed.	In parallel, the user interacts with the Preview Space.
9	The Online Procedure Portal sends a second evidence request.	For all *rim:Slots* except *IssueDateTime*, this evidence request have the same content as the first request. The eDelivery message that carries the request should have the same values for conversation identifier and other values. In addition to this, unlike the evidence request in step 2, this request does include the *rim:Slot* "*PreviewLocation*". Its content is that of the *rim:Slot* "*PreviewLocation*" in the first response exchanged in step 6. This request shall not contain any "*PreviewMethod*" or "*PreviewLocationDescription*" slots. The receiving Data Service should validate this and return an error if validation fails, and alert the Preview Space. While the diagram show this step as preceding the user redirection of step (10), the request may be delayed due to operational circumstances. However, this is not an issue as the request is only needed to allow generation of a second response (in step 22), which in practice will be many seconds if not minutes later.
10	The user follows the link to the Preview Service.	The link includes the return URL as described in section 5 below.
11	Retrieve and validate data	Using the data from the initial request, stored in step 4, the Preview Service determines that the link has not expired and obtain data from the original request, including user identity attributes.

		If the link has expired, or expires while the user is using the Preview Service (not shown), the Preview Service shall inform the user. It shall also, through the Data Service, return an evidence error message of type *rs:TimeoutExceptionType* to cancel the second request sent under step 9.
13-15	The user is identified	While the preview URL should be unique, is exchanged securely to the Online Procedure Portal and should only be known to the user, proof of knowledge of the URL may be deemed insufficiently secure. Furthermore, the identity attributes in the original request may not uniquely identify the data subject. Therefore, the Preview Space may re-authenticate the user using either a national eID of the Evidence Provider Member State, or using eIDAS nodes. If re-authentication fails, the Preview Space should: • Allow the user to return to the Online Procedure Portal using the provided return URL. • Notify the Data Service to send an evidence exception message of type *rs:AuthenticationExceptionType*. If the identity attributes of the user as expressed in the original request (steps 2, 4, 11 above) do not match the attributes obtained from the national re-authentication, the Preview Space should: • Allow the user to return to the Online Procedure Portal using the provided return URL. • Notify the Data Service to send an evidence exception message of type *rs:AuthorizationExceptionType*.
16, 17	Find (list of) piece(s) of evidence	Now that the user is successfully and uniquely authenticated, the list of pieces of evidence for the user for the selected type of evidence for the selected evidence provider can be retrieved for preview. In the diagram, this is done by using the Data Service as a back-end to the Preview Space, but this is an implementation-specific choice.
18, 19	Interact with user	The Preview Space now interacts with the user, allowing him or her to decide which if any pieces of evidence to use in the procedure, and to preview it.
20, 22, 23	Provide decision	Once the user has made his or her decision, this is relayed to the Data Service. The selected pieces of evidence (if any) are packaged in an evidence response message as defined in section 4.5.2.

21	Return user	In parallel, the Preview Space presents a return link that allows the user to return to the Online Procedure Portal. The link is constructed from the return URL as described in section 5 below.
22, 23	Construct evidence response and send using eDelivery	This step requires the second evidence request (step 9) to have been received and processed successfully. The response *query:QueryResponse/@requestId* is set to the *query:QueryRequest/@id* of the request.
25	Complete exchange	Once returned, the user can continue his or her procedure.

4.9.3 Coordination of Evidence Preview Service and Data Service

The Evidence Preview Service and the Preview Space that implements it shall coordinate their operation with the Evidence Query Service functionality of the Data Service. The details of this are up to the implementation of the two services but shall meet the following requirements:

- For the purposes of the OOTS, the Preview Service only exists to support the Data Service.
- For evidence requests that do not contain a preview URL, the Data Service and the Preview Service shall establish a preview URL. The format of the URL is described in section 4 below. The Data Service shall return the preview URL as defined under step 5 in the diagram in section 3 above.
- The Preview Space shall only allow access for preview URLs that it issued and communicated to the Online Procedure Portal and the user using an evidence error response message as described under section 2.
- The Preview Space and Data Service shall agree on any timeout values after which previously issued preview URLs are no longer valid. In particular, any time limits on access to the Preview Service for an evidence request shall not exceed the timeout intervals of the Data Service.
- Access to the Evidence Preview Service for a particular set of pieces of evidence of a specific type shall be limited to users of OOTS and shall be available only after a request for evidence of that type has been made to a Data Service.
- When the Data Service provides a response to an evidence request, the response shall include all and only those pieces of evidence that the user decided to use. This selection is made to the Preview Space and communicated to the Data Service.
- Within timeout intervals, the Data Service shall not provide an evidence response to the evidence request before the user has decided whether or not to use any matching piece of evidence.

4.9.4 Preview Location Metadata

Preview Location Metadata is provided by the Data Service (in coordination with the Preview Service) to the Online Procedure Portal, as content of the following three slots in the *rs:Exception* in the the evidence error response:

- A mandatory Slot "*PreviewLocation*" with a *rim:SlotValue* of type *rim:StringValueType*. This Slot provides the URL of the server on which the Preview Space is available for preview related to the evidence request. This slot is reused in the second evidence request message.
- An mandatory Slot "*PreviewMethod*" with a *rim:SlotValue* of type *rim:StringValueType*. It has two allowed case-insensitive values: "*PUT*" or *"POST".*
- An optional Slot "*PreviewLocationDescription*" with a *rim:SlotValue* of type *rim:InternationalStringType*. This provides additional descriptions, in possibly multiple natural languages, of the preview location. At a minimum, a description should be provided in an official language of the Union that is broadly understood by the largest possible number of cross-border users.

The specific format for the preview URL, as communicated by the Data Service to the Online Procedure Portal, is up to the implementation of the Preview Space, but shall meet the following requirements:

- The URL shall specify secure HTTP ("https://") as transport.
- The URL shall be unique to the request and therefore to the request parameters including the user identity attributes, requested evidence type, evidence requester and evidence provider that the request relates to.
- The URL shall not include query parameters with the names "*returnurl*" or "*returnmethod*". This is because parameters with those names are appended by the Online Procedure Portal as described in section 5 below.

4.9.5 Coordination of Evidence Preview Service and Online Procedure Portal

To support preview, the Online Procedure Portal needs to provide the following functionality:

- Recognize, in the first flow, evidence error response messages of type *rs:AuthorizationExceptionType* that contain a "*PreviewLocation*" slot as indications of the use of the Preview Space.
- Provide a departure page for the user to navigate to the Preview Space.
- Process the language specific information of the preview location description metadata to allow the launch page to be customized to the user's language choice (if known).
- Provide a return address to which the user can return after completing his or her interaction with the Preview Space, using GET or POST methods.
- Append the return address, in encoded form, as a value of the "*returnurl*" query parameter, to the preview URL prior to presenting the link to the user. This allows the Preview Space to return to the Online Procedure Portal, when finished previewing.
- Append the HTTP method (PUT or GET) of the return address, as a value of the "*returnmethod*" query parameter. The allows the Preview Space to return the user to the Online Procedure Portal, when finished previewing, using the appropriate method.

4.9.6 Multiple Evidence Requests (Informative)

When executing an online procedure and using the OOTS, the user may want to retrieve multiple pieces of evidence. For example, a student may want to make available two diplomas that he or she obtained from different universities. This may result in two parallel evidence requests being sent to two different Data Services, in response to which two separate preview URLs for the two requests may be returned to the Online Procedure Portal.

Following the profiling of eDelivery for OOTS in chapter 4, section 4.7.2.5, different requests for the same user session have the same conversation identifier value. The Data Service and Preview Space could make use of this in the generation of the preview URL and are required to store the identifier. This allows the Preview Space to be aware that a user that visits it for one request may have other outstanding requests and may optimize its service accordingly.

In implementing OOTS, Member States are likely to implement a shared Preview Space component that can be used by multiple Data Services. The Preview Space implementation could optimize the user experience for handling multiple evidence requests. For example, when the user has authenticated himself or herself to the Preview Space after accessing the first preview URL, the Preview Space could set a session cookie that obviates the need for the user to authenticate again when he or she follows the second preview URL.

These and other optimizations are implementation-specific and out of scope for this specification.

5 Chapter 5: Data Models - June 2022

Data Models - June 2022

Summary
This chapter of the technical design documents address the semantic interoperability challenges when designing the SDG Once-Only Technical System and ensuring its interconnection with the EU Member States' IT systems and EU level systems. Data models were developed to streamline the exchange of evidences, together with a methodology for defining new data models and code lists to ensure the quality of the evidence exchanged between the Member States.

- The **metholodogy** supports the process of creating and maintaining evidence data models. The work done in the past years under the ISA² programme and its action SEMIC served as a basis for the methodology. This methodology is based on best practices and has been tested with certain types of evidence by a working group of Member State representatives.
- Data Models for **specific evidence types** were developed using the methodology. In this release, these models and the related code lists have been regrouped under three domain categories: 2.05.2 - Education Domain - June 2022, 5.3 - Vehicle Domain - June 2022, and 5.4 - Public Documents - June 2022.

The SDG regulation does not mandate use of (only) structured evidence types and does not provide a mandate to harmonize. The evidence exchange feature documented in chapter 4 of the technical documents consists of a flow of Messages based on the Evidence Exchange Data Model (EDM), which comprises the EDM Request (Request from Evidence Requester to Evidence Provider for certain data or documents) and the EDM Response (Response from Evidence Provider to Evidence Requester to deliver the requested data or documents). The Query Model is fully documented and supports document-based queries. The Exchange Data Model of evidence exchange is a light-weight generic mechanism to support the exchange of any type of evidence. It facilitates the automated exchange of unstructured and structured types of evidence.

NOTE
The data models and code lists have not been updated since the release of July 2021.
The restructuring of the existing content of this chapter on specific evidence types and the creation of the three domain categories is a first step towards creating more detailed specifications for evidence exchanges in the various procedures in scope of the SDG regulation. In the future, these sections will also include (or reference) the deliverables of the work on procedures, requirements and evidence types and provide more detailed coverage of alignment with other initiatives, including so-called related systems.
Also note that the former Generic Data Model has been removed from this chapter. It is obsolete as this release of the technical design documents covers all of the former content in chapters 3 and 4.

The content of this chapter is structured in the following sub-chapters:

Change log
For this release, the changes for all chapters are combined at the top level

5.1 Methodology for Data Model Development - June 2022

NOTE
This section has not been updated since the release of July 2021.

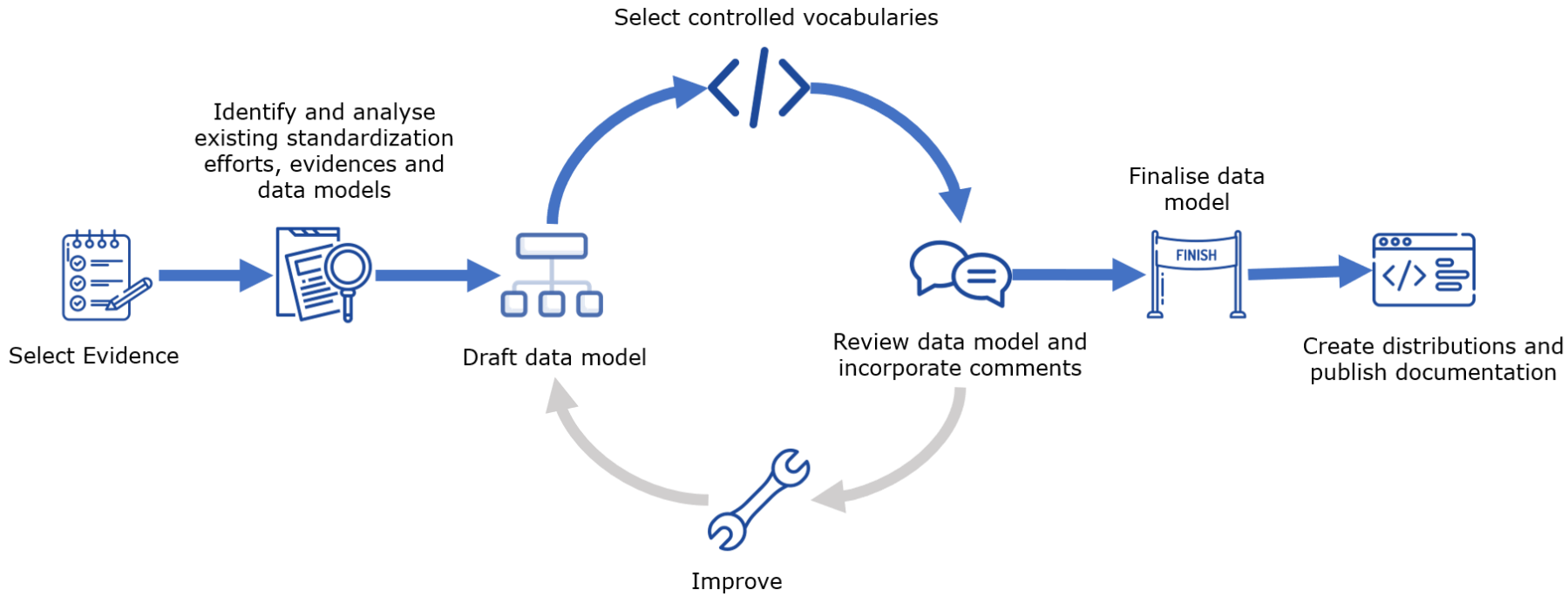
- Introduction

5.1.1 Methodology

This folder contains the various steps of a methodology to develop new data models for evidence types under the SDGR.

5.1.1.1 Process

In order to model the semantics for different types of evidence exchanged in cross-border administrative procedures, the methodology envisions the following key phases as shown below:



There are six phases, which range from the identification of existing efforts, evidences and data models to the creation of distributions and the publication of documentation. In essence, the steps focus on arriving at a consensus on semantics. In line with the European Commission's core values of democracy and transparency, this methodology provides tools and guidelines on how to reach the widest consensus possible.

This process should be placed in a broader context, in the sense that preliminary work carried out upstream, i.e. the identification of the evidence types to be modelled through the definition of use cases, is expected to take place. To define which evidences are to be modelled, there must be an evidence selection process where candidate evidences are evaluated and either selected or discarded based on whether they fulfil certain criteria or use case(s).

The involvement of domain experts (preferably from each Member State) in this kind of discussion is key to ensure collaboration between Member States. Their knowledge of the different specific features of national use cases and evidence will streamline the process of selecting the most relevant evidence to be modelled.

Once the evidence type to be modelled is defined, the methodology can be applied.

For each step, the key activities of every stakeholder group are described. If you would like to see an overview of the general roles and responsibilities of a stakeholder group, please refer to the section defining roles and responsibilities. If any key terms are unclear to you, please refer to the glossary. When relevant, additional information is provided alongside the key activities, in the form of rules and guidelines, tools or even examples. This is intended to make this methodology as easy to use as possible, helping the reader to develop common data models. Finally, for each step, three types of activities have been identified:

1. Business analysis, i.e. identifying business needs and determining solutions.
2. Technical analysis, i.e. identifying technical requirements and determining solutions.
3. Review, i.e. formal assessment potentially leading to changes.

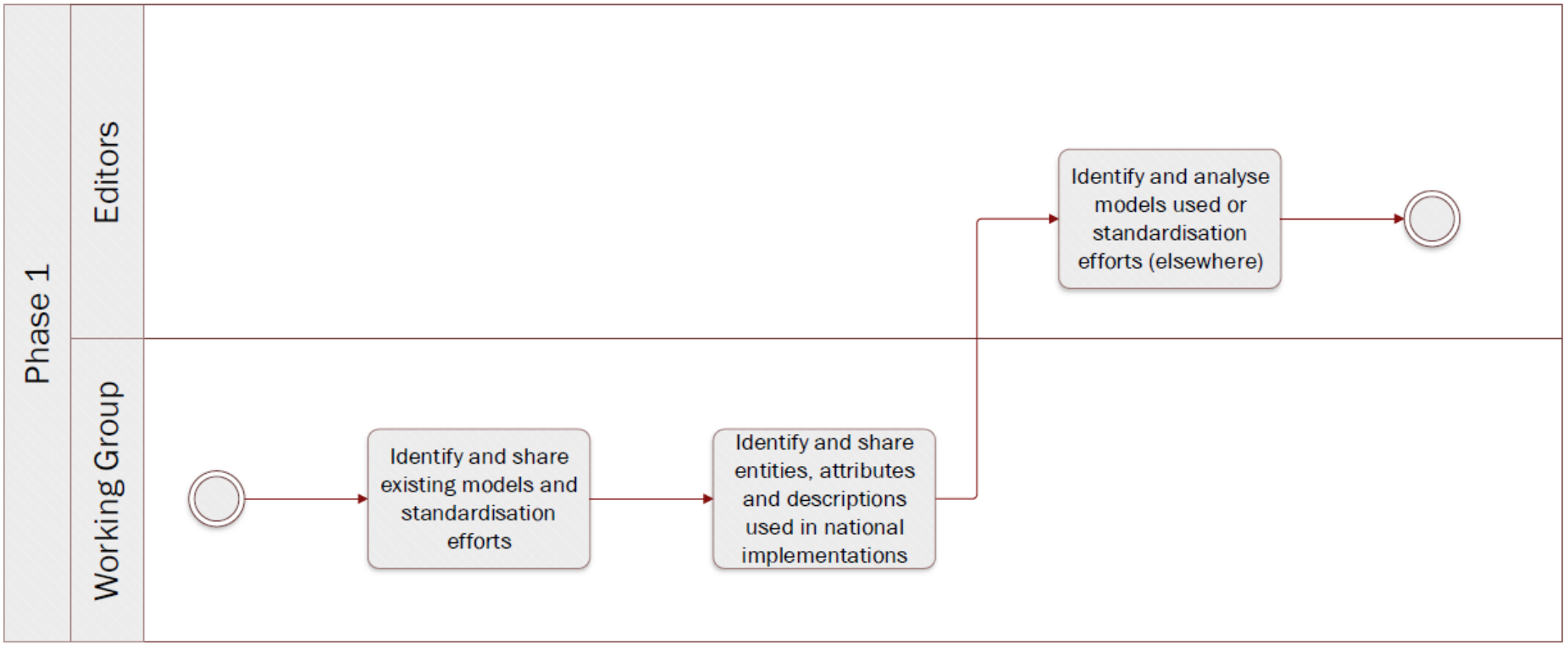
Business analysis activities are more present at the beginning of the methodology. As we advance to the latter stages of the methodology, they make way for technical activities. As in any project, business needs are defined before technical needs. Review activities occur throughout the course of the methodology.

GitHub is used as the platform for reviewing the data models as it is the de facto standard for developing technical specifications in a collaborative manner. Github offers built-in versioning control as well as other features that make it easy to propose suggestions and raise issues. (Here you can find the documentation on how to create issues on GitHub.)

Engagement is a key element to the success of the different stages of the methodology. Having a high degree of participation from MS is therefore essential to achieve quality results which are consensus-driven. Working Group members, i.e. Member States representatives, should therefore be well represented during throughout the process.

- Methodology
- Phase 1

5.1.2 Phase 1: Identify and analyse existing standardisation efforts, evidences and data models



Quick links:

- `Step 1` Identify and share existing models and standardisation efforts
- `Step 2` Identify and share entities, attributes and descriptions used in national implementations
- `Step 3` Identify and analyse models used or standardisation efforts (elsewhere)

5.1.2.1 Step 1 Identify and share existing models and standardisation efforts

Business analysis *- identification of business needs and related solutions.*

Key activities

- *The **Working Group members** and **domain experts** identify and share existing models, standardisation efforts or policies.*
- *The **responsible DG** in line with the evidence being modelled share existing models, standardisation efforts or policies.*
- *The **Editors** collect information from the Working Group members and the responsible DG.*

Description

Working Group members will share information they possess related to the OOTS data model for specific evidence types being built. Similarly, DGs with competencies in relation to the scope of the evidence being modelled, will share relevant information and existing legal pieces of work (and/or other relevant pieces of work)

The objective is to gather information in order to have a global overview of data models, and/or standardisation rules implemented and used across Europe and leverage this insight to develop a OOTS data model for specific evidence types.

This step is specifically interested in information available at global, i.e. European level, rather than at national level, which is the scope of step 2.

Rules and Guidelines

One important aspect of this step is ensuring data quality. This is ensured by the requirement that all data come from authoritative sources. Working Group members are responsible for identifying and contacting the authorities that hold the relevant information. In addition, reusing content based on intrinsic licenses may necessitate the use of a specific license for the model being developed.

Tool(s)

A collaborative tool, e.g. Confluence, GitHub.

Example(s)

For example, for social security, EESSI (Electronic Exchange of Social Security Information) is an IT system already in place. For education related matters, Europass, from DG EMPL, is in place.

5.1.2.2 Step 2 Identify and share entities, attributes and descriptions used in national implementations

***Technical analysis** - identification of technical requirements and related solutions.*

Key activities

- *The **Working Group members** share existing national data models or examples of evidences.*

- *The **Working Group members** contact relevant **domain experts** in order to identify and report features describing data models used in national implementations.*
- *The **Editors** collect information from the Working Group members.*

Description

Step 2 is about the national implementation of data models or legislative pieces. Contrary to step 1, step 2 is looking at gathering elements from national contexts.

It is possible that relevant data models (semantic or other) do not exist or were not shared in step 1. Step 2 will remediate this by gathering relevant elements from national implementations.

Working Group members will share information on:

- Examples of evidences
- Entities they judge paramount for the OOTS data model for specific evidence types being built
- Attributes they judge mandatory and optional;
- Descriptions of elements in their national implementations.

Before sending any data, the Working Group members should consider the following:

- Has the data model been validated and implemented by a competent authority?
- Has the data model been issued in a final version?

Tool(s)

A spreadsheet can be used to present and compare the different data models.

Example(s)

The table below illustrates how SKOS mapping properties can be used to compare models.

Italy data model	Spain data model	SKOS mapping value
Person	Person	exact match

Italy data model	Spain data model	SKOS mapping value
Birth		no match

If provided, the table can also include definitions and URIs to ease comparison.

Example of an implementation (Person Condition Register and Registration Register) shared by Germany: see issue #89. Example of a data model shared by Spain: issue #37.

5.1.2.3 Step 3 Identify and analyse models used or standardisation efforts (elsewhere)

Business analysis *- identification of business needs and related solutions.*

Key activities

> *The **Editors** analyse European and global initiatives to standardise the exchange of information.*

Description

In parallel with steps 1 and 2, the Editors document the information received and any European and/or global initiatives that aim at standardising data exchanges between Member States. The output of this step will serve as a basis for drafting the OOTS data model for specific evidence types.

Step 1 and 2 are the source of information for step 3. While Working Group members and competent DGs gather information, the editors will focus on documenting and analysing the information received. Editors should also do a research effort to not exclude any relevant data model and standardization effort used elsewhere.

This step supplements part of step 2, concerns existing harmonisation of information contained in the evidences at European level. The editors may reuse the necessary elements from these initiatives.

Rules and Guidelines

Reusing content based on intrinsic licenses may necessitate the use of a specific license for the model being developed.

Tool(s)

Below are some links of input sources.

- Study on Data Mapping for the cross-border application of the Once-Only technical system SDG
- Linked Open Vocabularies

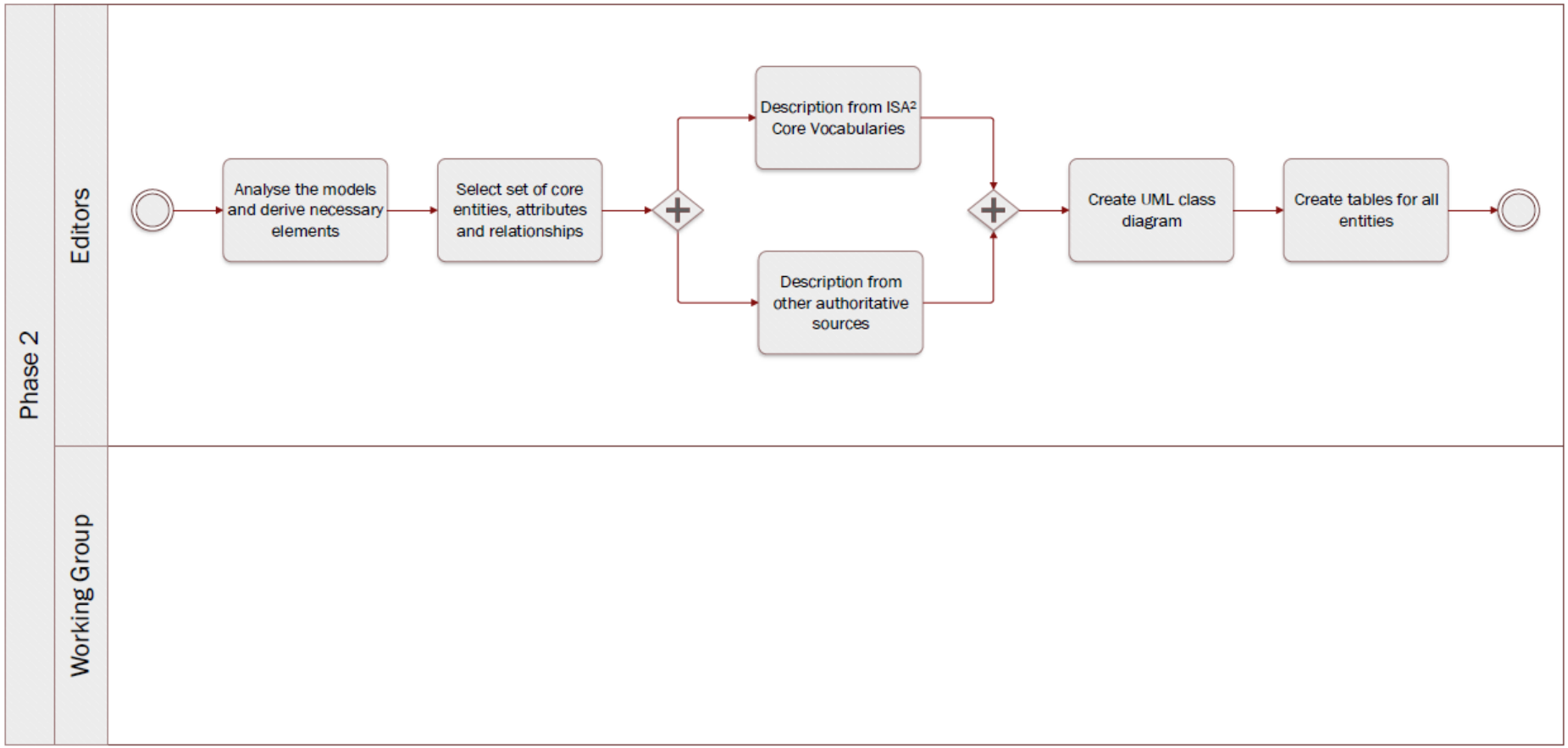
- Core Vocabularies
- Euro Vocabularies
- Ontology design patterns
- eProcurement ontology
- Public Documents forms | DG Justice

Example(s)

The Core Person Vocabulary can be used when modelling data related to people.

- Phase 2

5.1.3 Phase 2: Draft data model



Quick links:

- `Step 4` Analyse the models and derive necessary elements
- `Step 5` Select set of core entities, attributes and relationships

- `Step 6` Description from ISA² Core Vocabularies
- `Step 7` Description from other authoritative sources
- `Step 8` Create UML class diagram
- `Step 9` Create tables for all entities

5.1.3.1 Step 4 Analyse the models and derive necessary elements

Technical analysis *- identification of technical requirements and related solutions.*

Key activities

- *The **Editors** analyse the existing data models and information shared to check what is common and can be reused.*

Description

The Editors analyse the data models, concrete examples and other useful documentation received from the Working Group and the DGs in the previous steps. Specifically, they look for similarities (and dissimilarities) between the different data models and documentation in order to identify a common set of entities, attributes and relationships that are relevant for the respective evidence that is being modelled.

Considering the procedure, and thus the use case(s), for which the evidence is being modelled will also inform the analysis of models and documentation in order to derive necessary elements.

Rules and Guidelines

- The OOTS data model for specific evidence types will not be used to model paper documents but rather evidence itself, i.e., information required by competent authorities to prove a fact about a citizen or business. Therefore, when modelling evidence types, the granularity of the data should be limited to the fact the citizen or business needs to provde to complete a procedure. The Editors should look for the minimum common denominator when consolidating and analysing (fragments of) data models and information received.
- The SKOS Mapping Properties can be used to compare entities or attributes across different models.
- When selecting the core entities, attributes and relationships, the editors can define thresholds making it possible to decide which of the latter will be mandatory, optional or discarded. For instance, if no other Member State mentioned the need for an attribute it should be discarded.

Tool(s)

- Linked Open Vocabularies which is a source for predicates, i.e. existing attributes/relationships that might be candidates for reuse.
- A spreadsheet can be used to present and compare the different data models.

Example(s)

The table below illustrates how SKOS mapping properties can be used to compare models. **insert picture** If provided, the table can also include definitions and URIs to ease comparison.

5.1.3.2 Step 5 Select set of core entities, attributes and relationships

Technical analysis *- identification of technical requirements and related solutions.*

Key activities

> - *The **Editors** select the entities, attributes and relationships that are needed to model the respective evidence.*
> - *The **Editors** propose which attributes and relationships are mandatory / optional.*

Description

With the output of the previous steps, the Editors select the entities, attributes and relationships that are common to most data models and that are necessary to model the evidence. They also determine which attributes should be mandatory and which should be optional.

They do this by agreeing on thresholds with the Working Group. These thresholds might be quantifiable, e.g. “if at least five Member States have an attribute, the attribute is included” or “if one Member State is not able to provide an attribute, the attribute is made optional”.

Rules and Guidelines

Be as specific as possible, without restricting local flexibility too much.

Tool(s)

- A spreadsheet can be used to select the set of core entities, attributes and relationships of the OOTS data model for specific evidence types.
- The collaborative tool can be used to discuss on the inclusion of entities, attributes and relationships.

5.1.3.3 Step 6 Description from ISA² Core Vocabularies

Technical analysis *- identification of technical requirements and related solutions.*

Key activities

> *The **Editors** assess whether the ISA² Core Vocabularies can be reused*

Description

The Editors verify whether an ISA² Core Vocabulary can be reused. Reuse is a key objective when drafting OOTS data model for specific evidence types. In case there is no reusable ISA² Core Vocabulary, or it is not coherent with the context of the OOTS data model for specific evidence types, the editors will consider other possibilities as presented in step 7.

> *Core Vocabularies are simplified, re-usable and extensible data models that capture the fundamental characteristics of an entity in a context-neutral fashion. Public administrations can use and extend the Core Vocabularies in the following contexts:*
> - *Development of new systems*
> - *Information exchange between systems*
> - *Data integration*
> - *Open data publishing*

Tool(s)

- Core Person Vocabulary
- Core Business Vocabulary
- Core Location Vocabulary
- Core Criterion and Core Evidence Vocabulary
- Core Public Organisation Vocabulary
- Core Public Service Vocabulary Application Profile

Example(s)

- The Core Person Vocabulary describes a class/entity Person that has an attribute/property "gender" that expects a Code as data type, coming from four possible controlled vocs: ISO, Eurostat, HL7 or SDMX.
- Gender is a challenging topic due to the varying recognition of non-binary gender, issue #143.

5.1.3.4 Step 7 Description from other respected sources

Technical analysis *- identification of technical requirements and related solutions.*

Key activities

> *The **Editors** gather information elsewhere than the ISA² Core Vocabularies.*

Description

Should an entity or attribute not be (properly) defined in the ISA² Core Vocabularies, the editors will find adequate documentation elsewhere. *'Not properly defined' refers to a circular definition of a term, i.e. already containing the term that is to be defined.*

1. Other respected sources can be considered when the terms are defined in a well-known domain-specific ontology. In general, entities, attributes, relationships and definitions should be linked to existing terminologies.
2. In the event of information not being available in existing vocabularies, the editors propose definitions for new entities / attributes using respected and authoritative dictionaries (which are deemed to be of excellent quality).

A 'respected dictionary' refers to a dictionary widely regarded as an authority on the English language. **Rules and Guidelines**

Generic rules and guidelines

- Entities can be documented by using tools such as the Interoperability Platform and Data Vocabularies Tools.

Specific rules and guidelines for the table per entity

- When defining a term, it should not be included in the tentative definition.

Tool(s)

- Oxford dictionary
- Merriam-Webster

Example(s)

For instance, for the Completion of secondary education evidence the **course name** definition comes from Merriam-Webster ; i.e. "Name given to a number of lectures or other matters dealing with a subject."

5.1.3.5 Step 8 Create UML class diagram

Technical analysis *- identification of technical requirements and related solutions.*

Key activities

- *The **Editors** design an UML class diagram*

Description

The Editors will leverage the information collected in the previous phase to develop a UML class diagram. This aims to visually describe how entities of the OOTS data model for specific evidence types will interact with each other. The diagram displays thedifferent entities, the relationship between entities, and their attributes as well as the expected types.

The exclusive focus on entities, attributes and relationships will allow the Working Group members to concentrate on the semantic aspects of the model. Supplementary modelling elements are added in step 9 when entities are documented in tables.

Rules and Guidelines

- Follow the UML design rules:
- Each element and their relationships should be identified in advance;
- Attributes of each class should be clearly identified;
- Attributes should be presented in the following manner:attributeName: expected type. “Expected type” is further defined in step 11;
- Avoid as much as possible lines crossing each other;
- Ensure orthogonality of relationships;
- Parents elements are higher than the child elements, so the subclass arrows always point upwards;
- Align elements either by one of their sides or by their centers;
- Make elements of the same size, if possible;
- Diagrams should show the cardinality of attributes and relationships as well;
- Entities names should start with an uppercase;
- Attributes names should start with a lower case.

Tool(s)

Some examples of proprietary and open source tools are the following:

Proprietary tools:

- Enterprise Architect
- Microsoft Visio
- MagicDraw (No Magic)

- Visual Paradigm

Open source tools:

- Modelio
- UMLet

Example(s)

- Birth Certificate evidence

5.1.3.6 Step 9 Create tables for all entities

Technical analysis *- identification of technical requirements and related solutions.*

Key activities

- *The **Editors** create tables for all entities.*

Description

Relying on the input gathered, the editors draft tables for all the entities of the OOTS data model for specific evidence types. Per entity, the table consists of the following elements;

- Proposed attribute(s) / relationship(s)
- Proposed expected type
- Proposed definition
- Proposed cardinality

Tables are a way to provide further information and context to the OOTS data model for specific evidence types, unlike the UML class diagram which can be seen as a visual representation of the OOTS data model for specific evidence types. Both form the OOTS data model for specific evidence types referred to in the follwowing steps.

Rules and Guidelines

Generic rules and guidelines for step 9

- Multilingualism, localisation and internationalisation aspects should be considered. A language neutral identifier for every concept and additional Member State language columns in the tables facilitates Member State participation.

- The scope of the OOTS data model for specific evidence types should be described by a fact or an event that is proven by the evidence represented by the OOTS data model for specific evidence types.
- The tables should have a language-neutral identifier that, throughout the creation and review of the OOTS data model for specific evidence types, is agnostic to name changes.

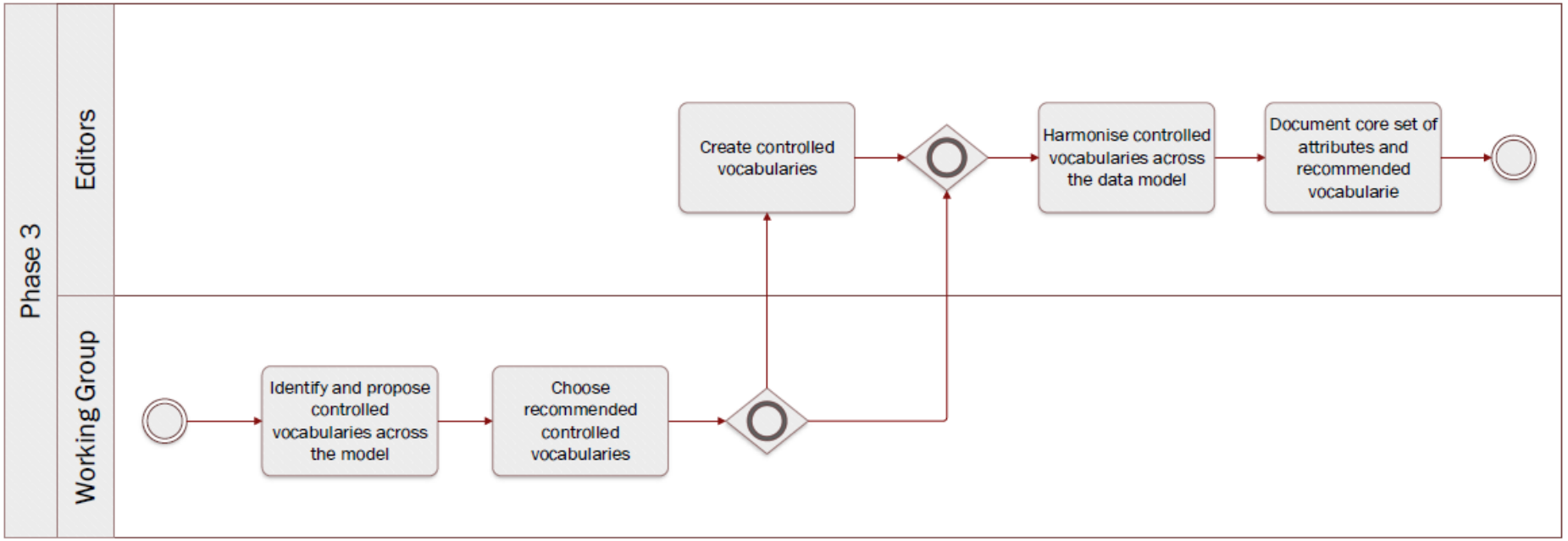
Specific rules and guidelines for the table per entity:

- Sources of the entities/attributes should be added, e.g. existing regulation, reused model, etc.
- Entities,attributes and relationships should be accompanied by a definition as well as their cardinality.
- The regulation 2016/1191 on Public Documents sets a set of fields for the production of multilingual standard forms. Each field has a code and a text label that has been officially translated into the Member States' official languages. It is essential to provide (when possible) the correspondence between the attributes of the proposed OOTS data model for specific evidence types and the fields of the multilingual standard forms of the regulation on Public Documents for evidences related to such a domain. The aforementioned approach could be reused for evidences other than public documents.

Tool(s) *The collaborative tool, e.g. Github.* **Example(s)**

- Birth evidence
- Birth
- Person
- Public Organisation
- Location
- Phase 3

5.1.4 Phase 3: Select controlled vocabularies



Quick links:

- `Step 10` Identify and propose controlled vocabularies across the model
- `Step 11` Choose recommended controlled vocabularies
- `Step 12` Create controlled vocabularies
- `Step 13` Harmonise controlled vocabularies across the data model
- `Step 14` Document core set of attributes and recommended vocabularies

5.1.4.1 Step 10 Identify and propose controlled vocabularies across the model

Technical analysis *- identification of technical requirements and related solutions.*

Key activities

- *The **Working Group members** and the **domain experts** propose controlled vocabularies for the different attributes defined in the previous phases.*
- *The **Editors** synthesise the propositions and complement with additional standard controlled vocabularies where relevant.*

Description

Once a core set of common attributes has been agreed upon and the draft OOTS data model for specific evidence types is stable enough, the set of controlled vocabularies, for those attributes where a controlled vocabulary is needed, needs to be analysed.

The editors create a table with the common attributes along one axis and the local implementations along the other, placing the controlled vocabularies suggested in the cells. Along with the controlled vocabularies, the Working Group is tasked with proposing usage notes for all the attributes agreed upon.

Rules and Guidelines

- Controlled vocabularies at the EU level are multilingual which helps in cross- border data exchange scenarios.
- (Domain-specific) Controlled vocabularies which are internationally accepted should be considered.
- Controlled vocabularies should have governance processes in place, be hosted in a sustainable manner and be provided free of charge.

Tool(s)

- EU Vocabularies
- Core Public Service Application Profile

Example(s)

For instance, for the gender attribute the Human Sex controlled vocabulary has been identified and proposed.

5.1.4.2 Step 11 Choose recommended controlled vocabularies

***Technical analysis** - identification of technical requirements and related solutions.*

Key activities

- *The **Editors** put forward the different propositions for each attribute working towards a decision.*
- *The **Working Group members** and the **domain experts** discuss - through the collaborative tool - and select the controlled vocabularies.*

Description

Based on the table of controlled vocabularies, the Working Group members discuss which controlled vocabularies are the most appropriate to be recommended. They also review whether the proposed usage notes are adequate. This may be based on the status of particular vocabularies (e.g. if they are based on an international standard) or on their usage across multiple implementations.

In the case of divergent views, a live discussion may be organised by the Editors and the moderator to arrive at a consensus on the most controversial proposed solutions.

Rules and Guidelines

It is important to agree on common official controlled vocabularies that can harmonise the way in which specific values of properties are specified accross different countries, allowing for a uniform indexing and retrieving of data based on common terms.

Example(s)

As suggested by the Working Group, the editors have used the language code list as controlled vocabulary for the language attribute of all tertiary education related evidences (see issue #120).

5.1.4.3 Step 12 Create controlled vocabularies

Technical analysis *- identification of technical requirements and related solutions.*

Key activities

- *The **Editors** create a proposition of new controlled vocabularies.*
- *The **Working Group members** review the proposition and provide comments.*
- *The **Publication Office**The Publications Office creates controlled vocabularies.*

Description

In the event of no controlled vocabularies being available, the Editors (or Working Group members) have the opportunity to propose the creation of new controlled vocabularies. Required controlled vocabularies, that do not yet exist, need to be created by the Publications Office, as part of the EU Vocabularies. If necessary, existing controlled vocabularies can be updated.

Tool(s)

- The Publication Office

5.1.4.4 Step 13 Harmonise controlled vocabularies across the data model

Technical analysis *- identification of technical requirements and related solutions.*

Key activities

> *The **Editors** harmonise the controlled vocabularies and usage notes across the OOTS data model for specific evidence types while ensuring the alignment between OOTS data models for specific evidence types.*

Description

The Editors consider all controlled vocabularies and usage notes across the OOTS data model for specific evidence types - and across all OOTS data models for specific evidence types - , checking their consistency and identifying any overlaps or gaps. Editors may propose changes to the recommendations, for example if different controlled vocabularies have been recommended for identical or similar attributes. Editors may also propose slight changes to the usage notes, for example to harmonise the writing style across the model or solve inconsistencies.

5.1.4.5 Step 14 Document core set of attributes and recommended vocabularies

Technical analysis *- identification of technical requirements and related solutions.*

Key activities

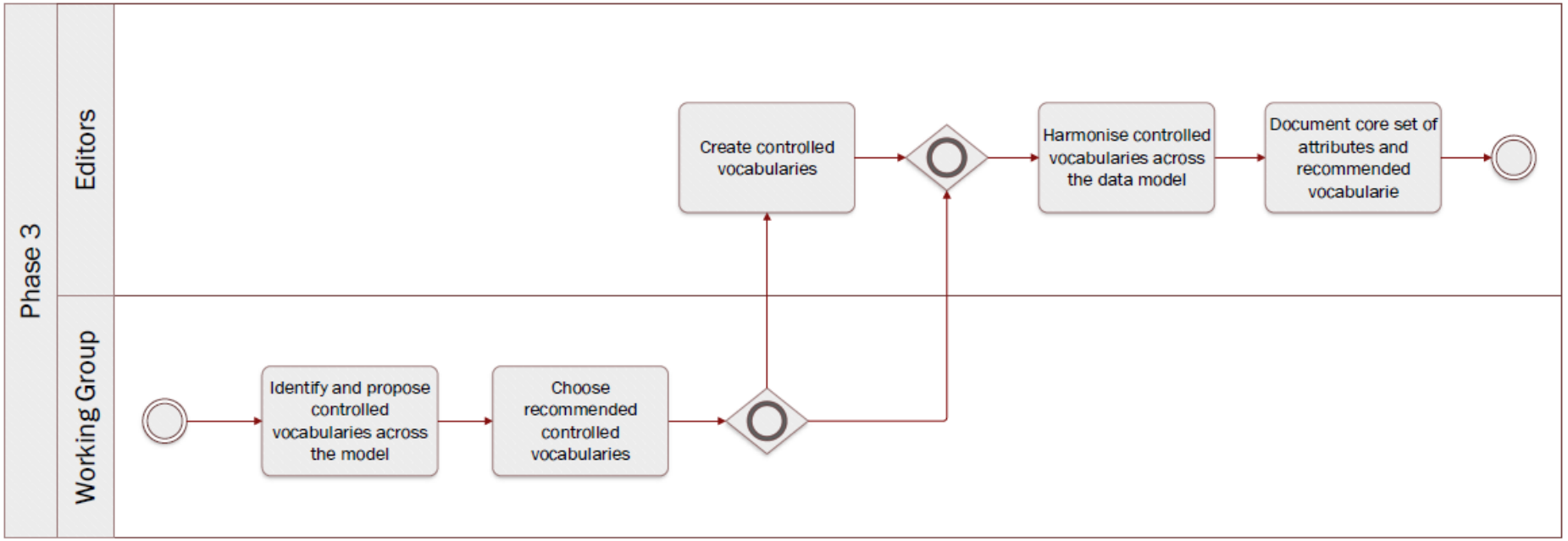
> *The **Editors** document the consensus and construct the working draft.*

Description

On the basis of discussions in phases 3 and 4, the editors will document the decisions and prepare to update the draft OOTS data model for specific evidence types.

- Phase 4

5.1.5 Phase 4: Review data model and incorporate comments



Quick links:

- `Step 15` Publish draft data model
- `Step 16` Review draft data model
- `Step 17` Propose enhancements
- `Step 18` Propose additional attributes
- `Step 19` Perform semantic mapping of attributes
- `Step 20` Harmonise entities, attributes and descriptions across the data model
- `Step 21` Update draft data model

5.1.5.1 Step 15 Publish draft data model

Technical analysis *- identification of technical requirements and related solutions.*

Key activities

- *The **Editors** finalise the OOTS data model for specific evidence types based on information collected in step 8, step 9, step 10, step 11, step 12, step 13 and step 14.*
- *The **Editors** publish the output.*

Description

The draft OOTS data model for specific evidence types expressed as a UML diagram with textual description (i.e. tables) of the entities, attributes, relationships, definitions, cardinalities, controlled vocabularies and usage notes is finalised. The Editors construct the final draft version of the OOTS data model for specific evidence types based on the changes that have been agreed upon and derived from the previous seven steps. Additionally, the model is prepared for review.

Finally, it is important for Working Group members and the Editors to agree on an Open Licence to be used. Reusing content based on intrinsic licences may oblige editors to use a specific licence. In addition, acknowledgement sections should be added specifying that the OOTS data models for specific evidence types developed rely heavily on the contributions of Working Group members, and subsequently the Member States.

Rules and Guidelines

- Publication as a Working Draft does not imply endorsement by the Working Group members or its representatives. This is a draft model and may be updated, replaced or made obsolete by another model at any time. It is inappropriate to cite this model as anything other than a work in progress. Comments on the model are invited. Further details on Step 17.
- Choose an open license, e.g. CC0, EUPL.
- Publish the OOTS data model for specific evidence types, its elements and related documentation via persistent (and ideally, dereferenceable) URIs.
- Provide machine access to the OOTS data model for specific evidence types.

Tool(s)

The collaborative tool, e.g. GitHub.

Example(s)

Based on the steps described before, diagrams and tables, in their first version, were published.

5.1.5.2 Step 16 Review draft data model

Review *- formal assessment potentially leading to changes.*

Key activities

> - *The **Working Group members** directly review the proposed model and/or contact the **domain experts** for reviewing it*
> - *The **Editors** moderate and classify the issues.*

Description

The Working Group members and the Editors agree on a tool to collaborate and capture the feedback. Using this tool, reviewers can create issues and the Editors can follow up on them thanks to an issue tracker.

The Editors then publish the draft using the collaborative tool. The published draft of the OOTS data model for specific evidence types is reviewed by the Working Group members and domain experts when relevant.

The Editors respond within an agreed timeframe to each issue made by the Working Group members, informing the reviewers that they have taken note of and will process the issue. The Editors consolidate solutions to the issue and seek additional contribution from the reviewers. This is done in collaboration with the moderator and rapporteur.

Issues can come in many different forms. For instance, an issue may deal with a modification to an existing entity or attribute, the addition or removal of an entity and/or attribute, etc. For further details about these types of issues, please check:

- `Step 17` Propose enhancements
- `Step 18` Propose additional attributes

Issues are categorised according to their type; (i) editorial (ii) minor or (iii) major.

- **Editorial issue**: issue stemming from errors in the OOTS data model for specific evidence types, which are not affecting the semantic agreement in any way. These issues may be addressed directly and do not lead to another review cycle.
- **Minor issue**: issue leading to direct changes in the deliverables. These issues may be addressed directly and do not lead to another review cycle.
- **Major issue**: issue qualified as show stopper and/or transversal issue. Either stakeholders decide together on how to address the issue directly, without leading to another review cycle, or, once the issue is addressed, the OOTS data model for specific evidence types undergoes another review round.

The moderator ensures that the agreement process is transparent and acknowledged by all reviewers.

Rules and Guidelines

- Use case descriptions should be provided along with the OOTS data model for specific evidence types.
- Model components should be translated.
- Editors organise issues as in a forum, by discussions and subjects hierachising the threads.
- Reviewers are encouraged to directly create issues on the collaborative tool.
- Reviewers are encouraged to propose a solution whenever they raise an issue.
- Reviewers are encouraged to use labelling and tagging to facilitate searchability and increase the responsiveness of contributors.
- Reviewers should consider how to present and discuss issues (e.g. technical versus business aspects).
- Reviewers are encouraged to provide context to their issues (e.g. OOTS data model for specific evidence types used).
- Reviewers are encouraged to structure their issues and especially their denomination to increase comprehension. For instance:

```
Name of the OOTS data model for specific evidence types or sub-part (e.g. relevant entity) and a short statement of the issue

+ VehicleRegistrationCertificate evidence should contain registration status
```

- Additional commenting guidelines are described in the Wiki. These guidelines are specific for the SDG OOP but generic across the Work Packages (and therefore not limited to this methodology).

Tool(s)

The collaborative tool, e.g. Confluence, GitHub.

Example(s) The following example describes the review of a draft OOTS data model for specific evidence types followed by the creation of an issue and its processing by the Editors and the Working Group members. The process is the following:

1. The **Editors** publish on GitHub the diagram and tables describing the Vehicle registration certificate.
2. While reviewing the model, the **domain experts** will try to answer the following questions:

- Can you process the evidence in your country if only the mandatory attributes are provided? If not, what other optional or missing attributes do you need?
- Are the elements and their relationships correctly used and labelled?

- Do you agree with the definition of the elements?
- Are all elements necessary for this evidence described in the model?
- Are there conflicts between the elements of the model and the elements used in your country?
- Is the element mandatory or optional in your country (cardinality)?
- Do you have specific codes or expected types (e.g. format of date, address etc.) for attributes?

1. The reviewers document their issues on GitHub. For instance, concerning the Vehicle registration certificate, the following issue was created #45.

```
  You may notice that the issue describes in practice several comments related to the vehicle registration
certificate as well as an image of the data model used within the country.
```

To simplify the contribution of other reviewers to this issue, the **Editors** will analyse the proposition, categorise it with labels, verify whether the issue should be restructured and describe the pros and cons of the issue documented.

```
 In our example, each bullet point from the general comment should represent a separate issue.
 However, the editors should avoid as much as possible overcomplicating the structure of GitHub issues by creating
complex hierarchies between the issues.
 For instance, the visual data model proposed by the issue owner does not need to be separated from the initial
issue #45 since it represents a direct source of information which may be relevant for more than one issue.
```

1. The **Editors** or the **Moderators** answer, usually within one working week, to the initial issue created by acknowledging the issue or directly giving an initial answer.
2. The **Editors** propose resolutions or ask for more details concerning the issue(s) raised to trigger discussion and comments from other Working Group members.
3. The discussion continues as reviewers comment on the issue.
4. If no agreement has been reached, the **Editors** prepare the discussions and alternatives to be tackled during a webinar to be organised following the review period.

5.1.5.3 Step 17 Propose enhancements

Review *- formal assessment potentially leading to changes.*

Key activities

> - *The **Working Group members** propose enhancements after reviewing the OOTS data model for specific evidence types, if needed.*
> - *The **Editors** consolidate the propositions and present them with resolutions to the Working Group members. If needed, the Editors seek additional contributions from the reviewers in collaboration with the moderator and rapporteur.*

Description

Working Group members create semantic issues that deal with enhancements to the draft OOTS data model for specific evidence types published. Enhancements can take the form of requests regarding the proposed draft OOTS data model for specific evidence types. This may be changes to the definitions, relationships, data types, cardinalities, etc.

In this context, it must important to note that enhancement also means restrictions, as one of the key principles of developing OOTS data models for specific evidence types is data minimisation.

As outlined in Step 16. Review draft data model, the Editors invite opinions and feedback to the issues and moderate the ensuing discussion.

After considering the proposition, the Editors assess the type of issue, whether it is minor or major, and record the resolution. After that, a response is sent to the reviewers. The response to a semantic issue usually includes a summary of the context of the proposition, the resolution agreed by the Working Group members and the justification for the resolution, particularly in cases where the proposition is rejected.

Rules and Guidelines

The Working Group members must resolve each proposition in one of three ways:

- *Accepted: This usually means that changes will be made that will be reflected in the next draft OOTS data model for specific evidence types.*
- *Rejected: No changes will be made to the draft OOTS data model for specific evidence types.*
- *Partially accepted: Part of the change is accepted, but other parts are rejected. As indicated in the previous step, resolution will either lead to phase 5 or phase 4.*

Tool(s)

There are no specific tools for this step. The GitHub issue feature can be used (or pull request feature for more advanced users) to propose enhancements.

Example(s)

As described in issue#125, a proposition was made to enhance an attribute as it was too narrow and did not encompass all the possibilities for that attribute.

5.1.5.4 Step 18 Propose additional attributes

Review *- formal assessment potentially leading to changes.*

Key activities

- *The **Working Group members** propose additional attributes after reviewing the OOTS data model for specific evidence types, if needs be.*

- *The **Editors** consolidate the propositions and present them with resolutions to the Working Group members. If needed, the editors seek additional contribution from the reviewers in collaboration with the moderator and rapporteur.*

Description

Working Group members create semantic issues which deal with attributes (and entities) that could or should be included in the draft OOTS data model for specific evidence types published. It might be that in certain cases Working Group members request the deletion of an attribute, a controlled vocabulary, and/or entity.

As outlined in Step 16. Review draft data model, the Editors invite opinions and feedback on the issue and moderate the ensuing discussion.

After considering of the proposition, the Editors assess the type of issue, whether it is minor or major, and record the resolution. After that, a response is sent to the reviewers. The response usually includes the resolution agreed on by the Working Group members and the justification for the resolution, particularly in cases where the proposed attribute(s) is (are) rejected.

Rules and Guidelines

The Working Group members must resolve each proposition in one of three ways:

- Accepted: This usually means that changes will be made that will be reflected in the next draft OOTS data model for specific evidence types.
- Rejected: No changes will be made to the draft OOTS data model for specific evidence types.
- Partially accepted: Part of the change is accepted, but other parts are rejected.

By default, attributes and entities added to the OOTS data model for specific evidence types are optional.

Tool(s)

There are no specific tools for this step. As in the previous step, we propose using the GitHub issue feature (or pull request feature for more advanced users) to propose additional attributes/entities.

Example(s)

For instance, issue #26 suggested adding the CO2 emission per KM as well as the environmental class attributes to the vehicle class. In issue#73 additional dates were added to the model.

5.1.5.5 Step 19 Perform semantic mapping of attributes

***Technical analysis** - identification of technical requirements and related solutions.*

Key activities

- *Upon receiving additional attributes from the the **Working Group members**, the **Editors** perform a semantic clustering of attributes. Afterwards, the Editors will map the 'semantic clusters' to existing attributes, if any. Should there not be an attribute to map a 'semantic cluster' to, the Editors will propose a new attribute (or entity).*
- *The **Working Group members** discuss the 'semantic clusters' - and potentially the new attribute(s) - and work towards consensus.*

Description

Wherever attributes do not convey exactly the same information, 'semantic clusters' of similar attributes should be constructed to find a common, higher-level, and more general attribute to which the more specific attributes can be mapped.

Rules and Guidelines

The relationships between different attributes (or entities) can be given a value according to the SKOS (Simple Knowledge Organization System) Mapping system. The different values outlined in this system are

- exact match;
- close match;
- related match;
- broader match;
- narrower match;
- (no match, i.e. absence of match).

Tool(s) This step can be performed using a spreadsheet tool, such as Microsoft Excel, in which related attributes are juxtaposed in two columns and given a semantic mapping value in a third column. **Example(s)**

- speed hasCloseMatch velocity
- For instance, #issue 143 reported that in the sex/gender code list from the Publication Office, the property "not applicable" related to the legal recognition of non-binary gender.

5.1.5.6 Step 20 Harmonise entities, attributes and descriptions across the data model

***Technical analysis** - identification of technical requirements and related solutions.*

Key activities

- *the **Editors** harmonise the entities, attributes and descriptions across the OOTS data model for specific evidence types.*

Description

The Editors consider all the entities, attributes and descriptions across the all OOTS data models for specific evidence types and check their consistency. The Editors may propose changes to the attributes, for example to harmonise the names and definitions across entities or solve inconsistencies.

Rules and Guidelines

In order to guarantee semantic interoperability amongst different OOTS data models for specific evidence types – that might be developed at the same time – , the same modelling patterns, especially for concepts independent of a specific domain, can be applied across OOTS data models for specific evidence types (e.g. location, person, organisation) unless specific characteristics for them are required.

Example(s)

Following a discussion on the SDG sandbox, the editors proposed to align the Location entity for all tertiary education related evidences (see issue #133).

5.1.5.7 Step 21 Update draft data model

Technical analysis *- identification of technical requirements and related solutions.*

Key activities

*the **Editors** create an updated coherent draft OOTS data model for specific evidence types based on information collected in the previous steps.*

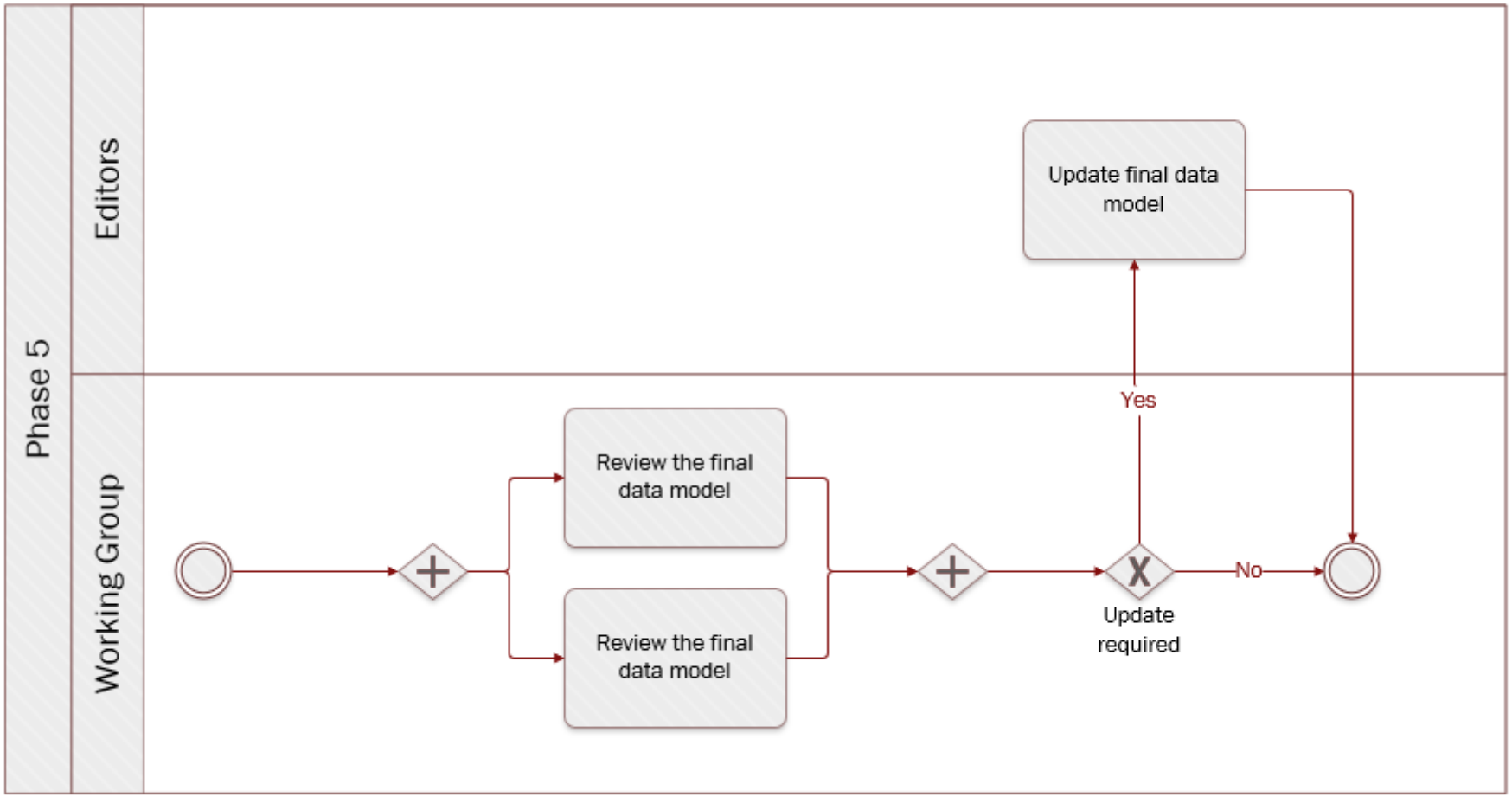
Description

The draft OOTS data model for specific evidence types expressed as a UML diagram with textual description (i.e. tables) of the entities, attributes, relationships, definitions, cardinalities and controlled vocabularies, i.e. codelists, is finalised. The Editors construct the new and final version of the OOTS data model for specific evidence types based on the changes that have been agreed upon and derived from the previous four steps.

Rules and Guidelines Publication as a last call Working Draft does not imply endorsement by the Working Group members or its representatives. This is a draft model and may be updated, replaced or made obsolete by another model at any time. Endorsement of the model will be sought in the `step 23`.

- Phase 5

5.1.6 Phase 5: Finalise data model



Quick links:

- `Step 22` Test the final data model with instance data

- `Step 23` Review the final data model
- `Step 24` Update the final data model

5.1.6.1 Step 22 Test the final data model with instance data

Review *- formal assessment potentially leading to changes.*

Key activities

- *A selected number of **Working Group members** and domain experts test the model against instance data.*
- *The **Editors** assist the Working Group members in the testing by collecting and categorising the feedback.*

Description

So far, the process of defining the elements of the OOTS data model for specific evidence types was a theoretical exercise. The objective of this step is to test the final model against instance data, i.e. actual data, in order to discover potential flaws or blind spots in the model. In this step, working group members have to provide (dummy) instance data and report on the challenges they face when:

- mapping this instance data to the model (perspective of the data provider). Working group members must answer the question: *"Can we provide this information?".*
- processing instance data that respects the OOTS data model for specific evidence types (perspective of the data consumer). Working group members must now answer the question: *"Can we process this information?"*, where the information represents the minimum data required by the model and, in this case, considering that the data was hypothetically received from another party.

Mapping instance data is, in the jargon, looking from the data provider perspective. For instance, a person needs evidence of a diploma from studying in a Member State (A) for a procedure in another Member State (B). The mapping takes the perspective of Member State (A). From the other perspective, processing the instance data would take the role of the data consumer. In the example above, Member State (B) is the data consumer.

A likely process for this step could be as follows:

1. **Initiate** – All working group members have the possibility to volunteer for the testing of the OOTS data model for specific evidence types with instance data. At the beginning of this exercise, editors will organise a meeting with the volunteers to walk them through the process and outline the expectations.
2. **Map** – Volunteers will play the role of the data provider and create instance data for the OOTS data model for specific evidence types, with as many attributes as are available in their national system, and map them to the attributes in the template provided.
3. **Process** – Volunteers will play the role of the data consumer and receive minimal evidence (mandatory fields only) data from another MS, i.e. another volunteer - as collected in the preceding step. These volunteers will then process the instance data received.

4. **Report** – Volunteers will report on (semantic) challenges arising from both the mapping and processing of instance data. This step should reveal potential flaws in the model thanks to the life-like situation of processing an evidence.
5. **Improve** – Testing is followed by reporting. Volunteers will therefore share their findings with the broader audience and discuss how to improve the models (e.g. by adding usage notes).

The feedback received during this step needs to be documented, categorised and analysed.

Rules and Guidelines

Questions to bear in mind when testing the model against instance data:

- How relevant do you think the data in the attribute is for cross-border exchange?
- For the mandatory attributes: how can you process them, and are there any specific requirements for the format of the data?
- For the optional attributes: what are the challenges for processing of data if the attribute is missing?

Tools

For this exercise, a spreadsheet is useful.

Attribute	Expected type	Definition	Cardinality	Code list	Instance data	Mapping relation	Mapping Comment	Processing comment
Identifier	Identifier	An unambiguous reference to the Tertiary Education Evidence.	[1..1]	N/A				
issuing date	Date	The date on which the Tertiary Education Evidence was issued.	[1..1]	N/A				
language	Code	The language in which the Tertiary Education Evidence is issued.	[1..*]	Language				
qualification name	Text	Full name of the qualification, at least in the original language(s) as it is styled in the original qualification, e.g. Master of Science, Kandidat nauk, Maîtrise, Diplom, etc.	[1..*]	N/A				

Attribute	Expected type	Definition	Cardinality	Code list	Instance data	Mapping relation	Mapping Comment	Processing comment
issuing place	Location	The Location where the Tertiary Education Evidence was issued.	[1..1]	N/A				
belongs to	Student	The Student that is the holder of the Tertiary Education Evidence.	[1..1]	N/A				
obtained at	Education Institution	The Education Institution that educated the Student.	[0..*]	N/A				
issuing authority	Organisation	The Organisation that issued the Tertiary Education Evidence.	[1..*]	N/A				

Several columns will be needed to describe the model:

- Attribute;
- Expected type;
- Definition;
- Cardinality;
- Code list;

Along with these elements, some input fields need to be provided:

- Instance data - Actual data to be provided. For instance, the given name for Johann Sebastian Bach is “Johann Sebastian”
- Mapping relation - e.g. exact match, no match, near match, etc. For further information on the definitions of these mappings
- Mapping comment - Comments in case there is a remark, suggestion or issue with the mapping (data provider perspective)
- Processing comment - Comments in case there is a remark, suggestion, issue with the processing, (data consumer perspective)

5.1.6.2 Step 23 Review the final data model

Review *- formal assessment potentially leading to changes.*

Key activities

- *The **Working Group members** and the **domain experts** review the final OOTS data model for specific evidence types.*

- *The **Editors** assist the Working Group members, collect and categorise the feedback.*

Description

Working Group members discuss and validate the OOTS data model for specific evidence types with the business, domain experts and share their questions and / or remarks, if any, with the editors via the relevant channel.

In parallel, the Editors collect and, again, categorise the feedback. For instance:

- Editorial issue;
- Minor issue;
- Major issue.

This step is also important to come to a final agreement on cardinalities. To facilitate this, the Editors have the possibility of proposing editable tables. The sole purpose of the tables is for the Working Group members to indicate whether they are able to provide the attributes listed in the OOTS data model for specific evidence types. But also whether a specific attribute is needed to process the evidence.

The tables should be composed of the following columns:

- Entity;
- Attribute;
- Description;
- Cardinality;
- Country abbreviation;
- multiple columns allowing Working Group members to specify whether an Attribute can be provided (Y) or not (N));
- multiple columns allowing Working Group members to specify whether an Attribute is needed (Y) or not (N));

It is important to note that the tables will not replace the collaborative tool selected. The latter will still be the main platform for designing and discussing. The tables provide a structured way to collect input on whether an attribute can be provided or not. In case further information is necessary to ascertain whether an attribute can be provided or not, the Working Group members must be redirected to the collaborative tool selected.

Ultimately, the Working Group members have to come to a semantic agreement with regards to the OOTS data model for specific evidence types reviewed. Unless there are major semantic changes, this step should be considered as a way for the Working Group members to formally approve the OOTS data model for specific evidence types

Rules and Guidelines Aspects to bear in mind while reviewing:

- Data elements and entity names
- Model appearance
- Rules of normalisation
- Definitions
- Model flexibility

Questions to bear in mind while reviewing:

- Do I agree with the proposed controlled vocabularies?
- Do I agree with the proposed changes to the OOTS data model for specific evidence types?
- Are the entities and attributes definitions clear enough?
- Does the modelling approach make sense?
- Do I agree with the proposed cardinalities (i.e. mandatory versus optional)
- With data minimisation in mind, should some of the entities and or attributes be removed?
- Will my country be able to provide all the mandatory information?
- What information does my country need to process the evidence?

Example(s) 'Editable table' as described further above:

	Attribute	**Description**	**Cardinality**	**AT**	**BE**	**BG**	**HR**	**CY**	**CZ**	**DK**	**EE**	**FI**	**FR**	**DE**	**EL**	**HU**	**IS**	**IE**	**IT**	**LV**	**LI**	**LT**	**LU**	**MT**	**NL**	**NO**	**PL**	**PT**	**RO**	**SK**	**SI**	**ES**	**SE**
Birth Evidence																																	
	BirthEvidence.identifier	[Link]	[1..1]					Y			Y															Y		Y				Y	Y
	BirthEvidence.issuingDate	[Link]	[1..1]					Y			Y															Y		Y				Y	Y

	Attribute	Description	Cardinality	AT	BE	BG	HR	CY	CZ	DK	EE	FI	FR	DE	EL	HU	IS	IE	IT	LV	LI	LT	LU	MT	NL	NO	PL	PT	RO	SK	SI	ES	SE
	BirthEvidence.certifies	[Link]	[1..1]					Y			Y															Y		Y				Y	Y
	BirthEvidence.issuingAuthority	[Link]	[1..1]					Y			Y															Y		Y				Y	Y

5.1.6.3 Step 24 Update the final model

Review *- formal assessment potentially leading to changes.*

Key activities

- *The **Editors** process any last feedback and finish the final model.*

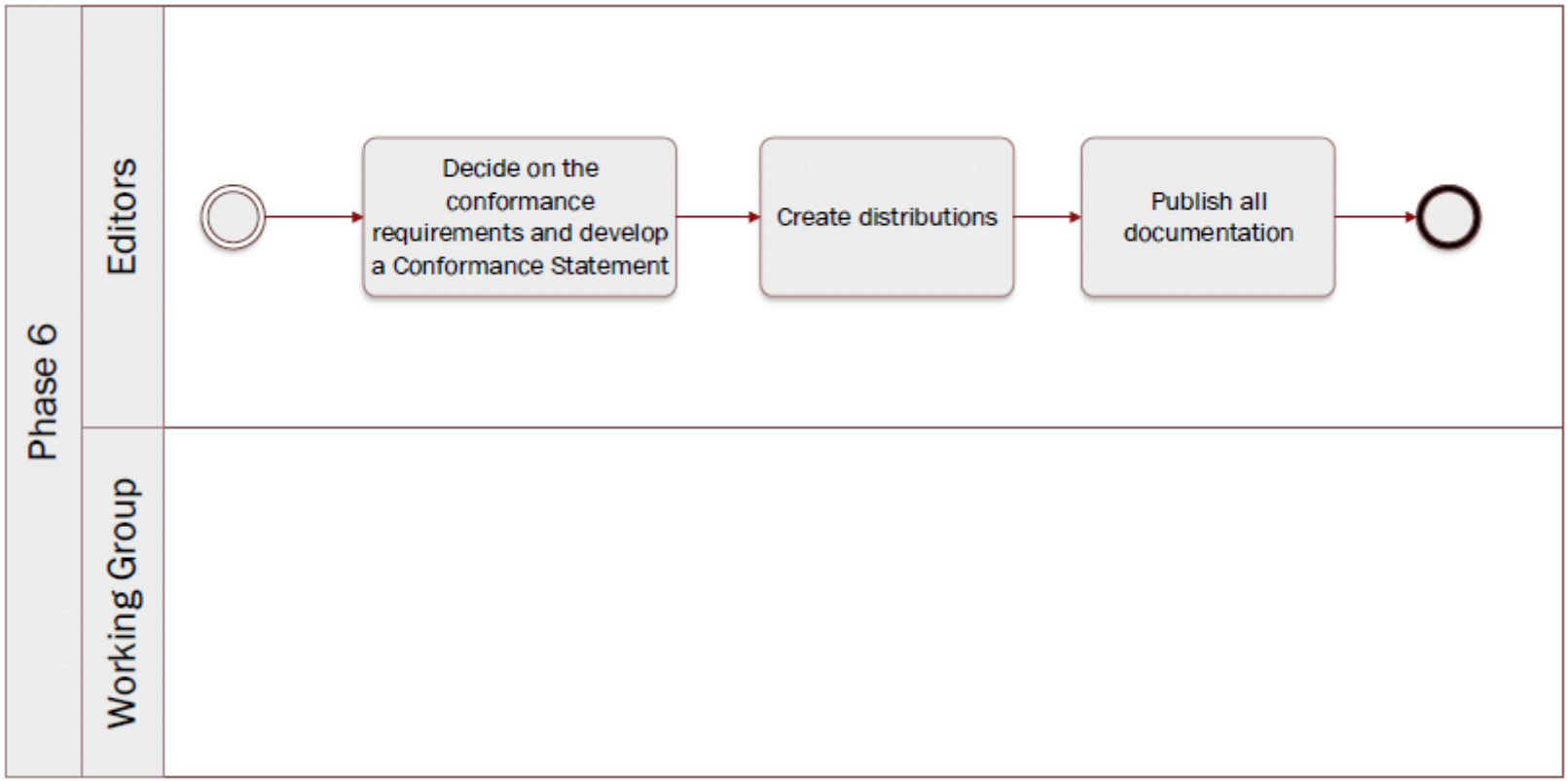
Description

As the Working Group members have given feedback in the previous two steps, the Editors process these comments and make changes to the OOTS data model for specific evidence types as agreed with the Working Group members. From this point on, the Editors can only make changes that the Working Group members have agreed on by consensus. Since there is no longer a review period, all changes that are carried out during this step should have already been discussed with the Working Group members.

Rules and Guidelines

- No change - not agreed upon by the Working Group - is made.
- The change log is updated to reflect the final changes in order to achieve full transparency towards the Working Group.
- Every element, e.g. attributes, needs to have a persistent identifier alongside labels that could be in different languages.
- Phase 6

5.1.7 Phase 6: Create distributions and publish documentation



Quick links:

- `Step 25` Decide on the conformance requirements and develop a conformance statement
- `Step 26` Create distributions
- `Step 27` Publish all documentation

5.1.7.1 Step 25 Decide on the conformance requirements and develop a conformance statement

Technical analysis *- identification of technical requirements and related solutions.*

Key activities

- *The **Editors** write a conformance statement.*
- *The **Working Group members** agree on the conformance statement.*

Description

A conformance statement declares a minimum set of requirements that an implementation must adhere to, in order to be considered conformant with the respective OOTS data model for specific evidence types. The Working Group members must agree on these conformance requirements. The Editors then include a conformance statement in the OOTS data model for specific evidence types.

The OOTS data model for specific evidence types may have natural divisions, in which case it might be appropriate to set different conformance levels. For example, a model used to describe vehicles may have a group of terms related specifically to motor vehicles that could be used in an implementation that has no need to understand the terms that relate to bicycles. This will consequently lead to the establishment of different conformance levels.

Rules and Guidelines

- Publish the conformance statement together with the OOTS data model for specific evidence types.

5.1.7.2 Step 26 Create distributions

Technical analysis *- identification of technical requirements and related solutions.*

Key activities

- *The **Editors** create the required distributions for the OOTS data model for specific evidence types.*

Description

The OOTS data model for specific evidence types can be expressed (or serialised) in various formats depending on the specific needs and context. Each distribution (format) will have its own uses and advantages, but also its own disadvantages and limitations.

Semantic data models can be expressed in different serialisation formats, such as TTL (RDF/turtle), RDF/XML, JSON-LD, SHACL, etc. Special care needs to be taken when using multiple formats, as conversion between different serialisation formats can potentially introduce inconsistencies.

Aside from these machine-readable formats, human-readable formats also need to be created. A visual representation of the entities, attributes and relationships of the OOTS data model for specific evidence types is always recommended to provide a clear overview. For example, this can be a UML-diagram, saved as a PNG-file. Alongside this, human-readable documentation is also required with all the necessary information to construct the OOTS data

models for specific evidence types, i.e. the entities and attributes with their definitions, cardinalities, proposed codelists, etc. This can be distributed as an HTML-page and a PDF-document, for example.

All these distributions can be manually created or created automatically via one or multiple tools. If possible, preference should be given to the usage of an automated toolchain, reducing the risk of introducing inconsistencies during updates.

During this step, URIs are also created (or reused when possible) for the OOTS data model for specific evidence types itself, its entities and their attributes. These identifiers need to be minted and maintained by a (European Commission) service.

Rules and Guidelines

- Create both machine-readable as well as human-readable distributions of the OOTS data model for specific evidence types.
- Automate, if possible, the creation of the distributions as much as possible in order to avoid inconsistencies.
- Use URIs under data.europa.eu which allows as to flexibility for where the URIs resolve to.
- UML diagrams can be published in machine-readable formats, e.g. XMI.

Tool(s)

- VocBench3
- Sparx Enterprise Architect
- Protégé

Example(s)

For instance, the Birth evidence was distributed in XML.

5.1.7.3 Step 27 Publish all documentation

Technical analysis *- identification of technical requirements and related solutions.*

Key activities

- *The **Editors** publish all documentation on the collaborative tool.*

Description

The Editors publish the final version of the OOTS data model for specific evidence types, in both machine-readable and human-readable formats, on the selected collaborative tool. The Editors must publish the OOTS data model for specific evidence types as open (meta)data and specify which license is

applicable.
Tool(s) The collaborative tool, e.g. Confluence, Github. Ideally, a collaborative tool allowing public access is more appropriate for transparency reasons.

- Quality

5.1.8 Quality

The quality aspect is addressed at three different levels:

5.1.8.1 data models

This is ensured by using the **proposed methodology**, which is based on the existing SEMIC methodology. In addition, we build as much as possible on **existing resources**, like the ISA² Core Vocabularies, the Public/eJustice documents, EUCARIS, EU Vocabularies of the Publications Office etc., taking into account the **feedback and suggestions of the member states**, building consensus and delivering detailed documentation.

5.1.8.2 instance data

[the actual evidences to be exchanged] in terms of **correctness of the XML data** with respect to the data models: this can be supported by tools like **the Interoperability testbed** and can be included as a post-development step after phase 7 (finalisation) of the methodology.

5.1.8.3 source of data

This is ensured by the requirement that all data comes from **authoritative sources**. Member States are responsible for identifying and connecting the relevant authorities to the system.

- Review cycles and consensus

5.1.9 Review cycles and consensus

The process by which semantic agreements can be reached among working group members in a consensus-building activity.

5.1.9.1 Consensus

Consensus is a generally accepted opinion or general agreement among a group of people.

> *Consensus is the heart of the process to develop OOTS data models for specific evidence types. It aims at developing a collective output, which is the reflection of the greatest possible number of views.*
> *Indeed, consensus involves looking for solutions that are acceptable to all. When everyone agrees with a decision, they are more likely to implement it and, in our case, ultimately use the common data models being built. Consensus is built through iterations, called review cycles.*

> *In the process defined, consensus takes the form of proposals shared, valued and debated to work towards semantic agreement. Semantic agreements aim to meet everyone's most important needs and find a balance between what different Working Group members want, while bearing in mind data minimisation and data sensitivity.*
> *Transparency and record keeping are important aspects of achieving consensus. Therefore, all proposals must be debated and documented.*
> *Once a proposal has been dealt with, stakeholders are informed of the group's decision and reasoning. However, there may be times when consensus cannot be reached on an issue or on a comment received. In such cases, one possible course of action is to seek external guidance.*

5.1.9.2 Review cycle

A review cycle occurs when a (working) draft model is shared with the Working Group so that the members can provide comments and proposals for change. It is during this activity that the consensus is built.

> *All stakeholders should bear in mind that it is important to always ensure that the broadest possible consensus is achieved when a review cycle is carried out. Once reviewed, proposals are categorised and addressed, leading to a new version of the (working) draft model.*

- Stakeholders

5.1.10 Stakeholders

This page describes the stakeholders identified in the process of developing data models along with their rolesand responsibilities.

5.1.10.1 Roles and responsibilities

This section describes the stakeholders identified in the process of developing data models along with their roles and responsibilities.

The shared goal of developing a set of OOTS data models for specific evidence types [...] that best serves the interests of the SDG regulation and the Member States (MS) is broken down into different phases. These different phases are executed by distinct groups, which are described below.

5.1.10.1.1 Authority

Final decision maker regarding the results of development of the data models in cases where no consensus could be reached.

> *In the context of the SDG Work Package 4, the European Commission is taking this role.*

5.1.10.1.2 Working Group members

The Working Group members contribute to the different deliverables and help others to meet the incremental goals and deadlines mutually agreed upon upfront. Working Group members will be responsible for achieving consensus.

Ideally, knowledge of the SDG is required and semantic awareness is recommended.

In addition to the core activities - defining data models - it is important for the Working Group to understand the wider context, i.e. how the output of this methodology will fit the technical aspect of the SDG OOP. For example, they must be aware of how the data models are going to be used in the exchange of information. This requires IT knowledge, which competency could be included as a responsibility of the Editors or by including an IT representative of the SDG OOP in all relevant activities of the methodology.

> *In the context of the SDG Work Package 4, the Working Group is composed of representatives of the Member States. Representatives attend the webinars and coordinate the work at the national level. It was recommended to have not only people with "semantic awareness" but also data modellers and data stewards.*

5.1.10.1.2.1 Domain experts

The domain experts can be divided per domain or evidence type (e.g. vital records, vehicles, etc.). They are the people who have the business experience specific to a certain domain. They know how the evidence is used, for which procedures, by whom and, most importantly, the information described within each type of evidence. Domain experts should be reachable and available throughout the development of the data model.

> *In the context of the SDG Work Package 4, one expert per domain should ideally be reachable by the representatives of Member States composing the Working Group. Alternatively, a pool of 2-5 experts per domain would be enough to provide the expected input with the Working Group ensuring that all the Member States have the possibility to monitor the quality of the work and the models proposed.*

5.1.10.1.3 Editors

The Editors lead the drafting of the deliverables and specification (i.e. data model) by integrating and consolidating the input received from the Working Group. Specifically, the role of the Editors is threefold:

- To create a formal specification which is in line with the best practices in regards to data modeling and data standards reuse.
- To motivate and explain how every information request being discussed is either adopted in the formal specification, or not.
- To initiate the consensus making process around discussion topics.

> *In the context of SDG Work Package 4, the editors are external to the European Commission and the Working Group. They are responsible for doing the groundwork, collecting and aggregating the input.*

5.1.10.1.4 Moderator

The moderator works with the rapporteur to ensure that the objectives, deliverables and deadlines of the Work Package are well defined and followed-up. The moderator communicates with other Work Packages to ensure alignment.

> *In the context of SDG Work Package 4, the moderator is an official of the Commission, who is in contact with other work packages as well as the directing bodies.*

5.1.10.1.5 Rapporteur

The rapporteur collects input from the Working Group, ensures that the Working Group is on schedule regarding the deadline of each deliverable in collaboration with the moderator. In addition, both the moderator and rapporteur communicate with other Work Packages to ensure alignment. The rapporteur is drawn from the Working Group.

> *In the context of SDG Work Package 4, the rapporteur is a member of the Working Group. At the outset, Working Members were given the possibility to take up the role of rapporteur.*

- Terminology

5.1.11 Terminologies

This pages contains the definitions (and illustrations) of the different concepts and terms used throughout the repository.

5.1.11.1 Glossary

5.1.11.1.1 Application profile

A data model defining which entities and attributes to use, what the cardinalities of the attributes are and recommendations for core vocabularies to be used, in order to support a particular application or use case(s).

5.1.11.1.2 Attribute

A characteristic of an entity in a particular dimension such as the weight of an object, the name of an organisation or the date and time that an observation was made, often representing things or events in the real world.

5.1.11.1.3 Controlled vocabulary

A controlled vocabulary is an authoritative list of terms to be used in indexing. Controlled vocabularies do not necessarily have any structure or relationship between terms within the list.

5.1.11.1.4 Data model

A data model is an abstract model that organises elements of data and standardizes how they relate to one another. It specifies the entities, their attributes and the relationships between entities.

5.1.11.1.5 Entity

A 'thing', such as a vessel, a geographic location, a sensor, a map or something more abstract like an incident, an event or an observation.

5.1.11.1.6 Evidence

An evidence means any document or data, including text or sound, visual or audiovisual recording, irrespective of the medium used, required by a competent authority to prove facts or compliance with procedural requirements

5.1.11.1.7 Procedure

Set of administrative formalities or steps to be followed in order to carry out a request.

Example

Life events	Procedures	Expected output subject to an assessment of the application by the competent authority in accordance with national law, where relevant
Birth	Requesting proof of registration of birth	Proof of registration of birth or birth certificate
Residence	Requesting proof of residence	Confirmation of registration at the current address

5.1.11.1.8 Relationship

A link between two concepts; examples are the link between an observation and the sensor that produced it, the link between a document and the organisation that published it, or the link between a map and the geographic region it depicts.

5.1.11.1.9 Semantic agreement

A specification of a data model and entities for which stakeholders reached consensus.

5.1.11.1.10 Vocabulary

A set of concepts and relationships (also referred to as “terms”) used to describe and represent an area of concern.

5.2 Education Domain - June 2022

This section contains data models and code lists for evidence related to the education domain.

NOTE

The data models and code lists have not been updated since the release of July 2021.
The restructuring of the existing content of this chapter on specific evidence types and the creation of the three domain categories is a first step towards creating more detailed specifications for evidence exchanges in the various procedures in scope of the SDG regulation. In the future, these sections will also include (or reference) the deliverables of the work on procedures, requirements and evidence types and provide more detailed coverage of alignment with other initiatives, including so-called related systems.

The content of this chapter is structured in the following sub-chapters:

5.2.1 Education Domain OOTS Data Models - June 2022

5.2.1.1 Introduction

The data models are available as **UML diagrams** and **Tables:**

- **UML Diagrams:** Models are visually represented in a diagram based on the UML (Unified Modeling Language) with the purpose of displaying the classes, their attributes and cardinalities along with the relationships between the classes.
- **Tables:** Models are represented in a tabular view with additional information not included in the UML diagram such as expected type, definition and code list.

5.2.1.2 SDG Sandbox

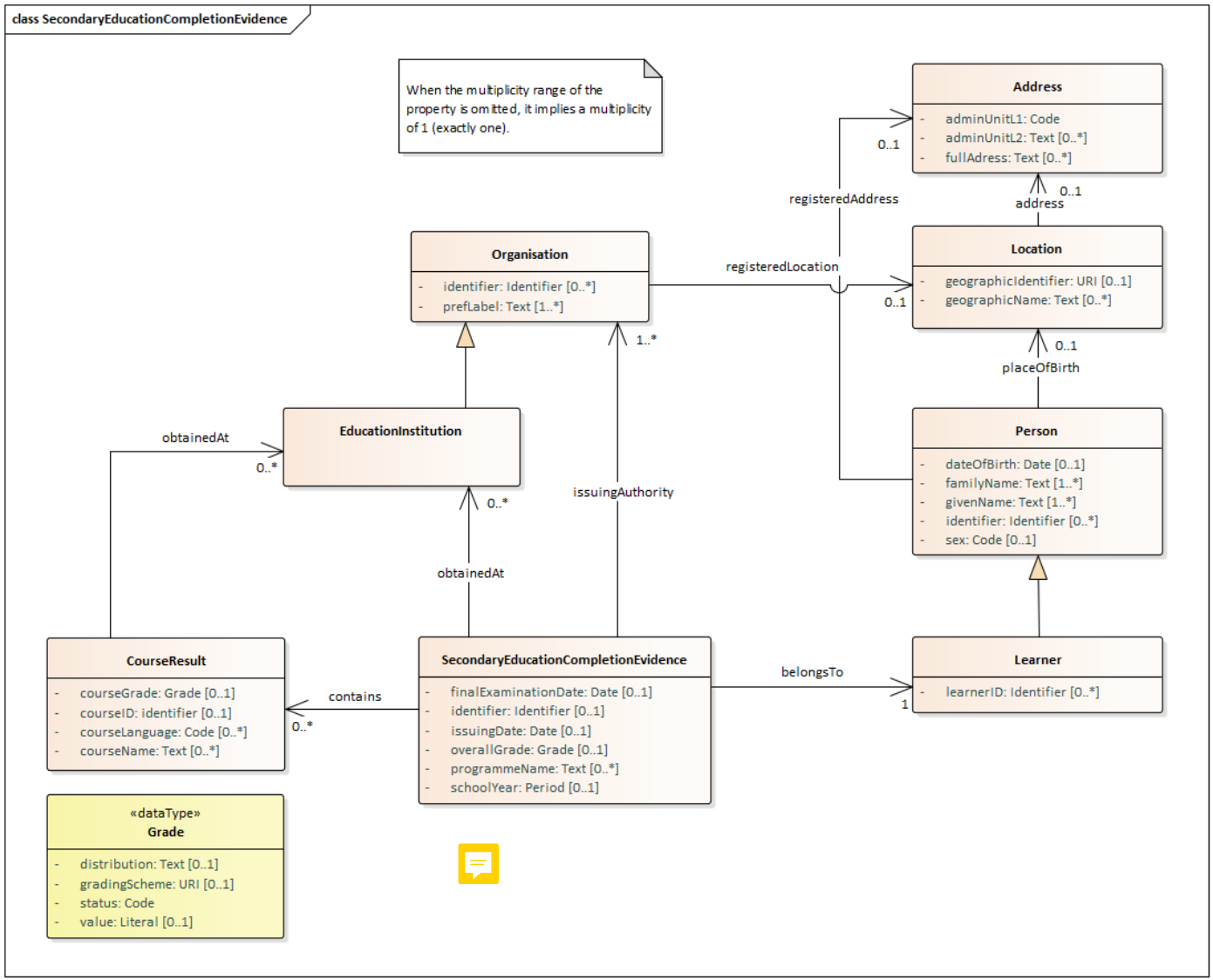
Click here to see the links to the SDG Sandbox common data models

- Evidence of completion of secondary education
- Tertiary education diploma evidence
- Tertiary education diploma supplement evidence
- Record of results evidence

5.2.1.3 Data models for Education Domain evidence types

- Evidence of completion of secondary education

5.2.1.4 Secondary Education Completion Evidence


class SecondaryEducationCompletionEvidence
When the multiplicity range of the property is omitted, it implies a multiplicity of 1 (exactly one).
Address
- adminUnitL1: Code
- adminUnitL2: Text [0..*]
- fullAdress: Text [0..*]
0..1
registeredAddress
0..1
address
Organisation
- identifier: Identifier [0..*]
- prefLabel: Text [1..*]
registeredLocation
Location
- geographicIdentifier: URI [0..1]
- geographicName: Text [0..*]
0..1
1..*
0..1
placeOfBirth
obtainedAt
0..*
EducationInstitution
0..*
issuingAuthority
Person
- dateOfBirth: Date [0..1]
- familyName: Text [1..*]
- givenName: Text [1..*]
- identifier: Identifier [0..*]
- sex: Code [0..1]
obtainedAt
CourseResult
- courseGrade: Grade [0..1]
- courseID: identifier [0..1]
- courseLanguage: Code [0..*]
- courseName: Text [0..*]
contains
0..*
SecondaryEducationCompletionEvidence
- finalExaminationDate: Date [0..1]
- identifier: Identifier [0..1]
- issuingDate: Date [0..1]
- overallGrade: Grade [0..1]
- programmeName: Text [0..*]
- schoolYear: Period [0..1]
belongsTo
1
Learner
- learnerID: Identifier [0..*]
«dataType»
Grade
- distribution: Text [0..1]
- gradingScheme: URI [0..1]
- status: Code
- value: Literal [0..1]

5.2.1.5 Secondary Education Completion Evidence

5.2.1.5.1 Entities

5.2.1.5.1.1 Secondary Education Completion Evidence

Definition: Official document or data proving that a Learner completed secondary education (ISCED 2011 level 3).

attribute	expected type	definition	cardinality	code list
identifier	Identifier	An unambiguous reference to the Secondary Education Completion Evidence.	[0..1]	N/A
overall grade	Grade	A mark indicating a degree of accomplishment.	[0..1]	N/A
school year	Period	The annual period of sessions of the Education Institution.	[0..1]	N/A
final examination date	Date	The date of the final assessment designed to test the qualification or knowledge acquired.	[0..1]	N/A
issuing date	Date	The date on which the Secondary Education Completion Evidence was issued.	[0..1]	N/A
programme name	Text	The programme name of the Secondary Education.	[0..*]	N/A
issuing authority	Organisation	The Organisation that issued the Secondary Education Completion Evidence.	[1..*]	N/A
contains	Course Result	The Course Result(s) which the Secondary Education Completion Evidence contains.	[0..*]	N/A
belongs to	Learner	The Learner to whom the Secondary Education Completion Evidence belongs.	[1..1]	N/A
obtained at	Education Institution	The Education Institution(s) that educated the Learner.	[0..*]	N/A

5.2.1.5.1.2 Course Result

Definition: Grade obtained after finishing/completing a course, for each course the Learner attended.

attribute	expected type	definition	cardinality	code list
course name	Text	Name given to a number of lectures or other matters dealing with a subject.	[0..*]	European Science Vocabulary
course grade	Grade	A mark indicating a degree of accomplishment for a particular course.	[0..1]	N/A

attribute	expected type	definition	cardinality	code list
course language	Code	Language in which the course was taught.	[0..*]	Language
course id	Identifier	An unambiguous reference to the course.	[0..1]	N/A
obtained at	Education Institution	The Education Institution that organised and delivered the course.	[0..*]	N/A

5.2.1.5.1.3 Education Institution

Definition: An Organisation that provides instructional services to individuals or education-related services to individuals and other educational institutions.

Subclass of: Organisation

No additional attributes are defined for this entity. It does inherit, however, all the attributes from Organisation listed here below.

5.2.1.5.1.4 Organisation

Definition: Represents a collection of people organised together into a community or other social, commercial or political structure. The group has some common purpose or reason for existence which goes beyond the set of people belonging to it and can act as an Agent. Organisations are often decomposable into hierarchical structures.

Source: The Organization Ontology

attribute	expected type	definition	cardinality	code list
preferred label	Text	As defined in the ORG Ontology, a preferred label is used to provide the primary, legally recognised name of the organisation. An organisation may only have one such name in any given language. Primary names may be provided in multiple languages with multiple instances of the preferred label property.	[1..*]	N/A
identifier	Identifier	Many organisations are referred to by an acronym or some other identifier. For example, among the EU institutions, the ECB is the identifier for the European Central Bank, OLAF for the European Anti-Fraud Office, and so on. These are formally recognised by the European Commission which provides a list of such acronyms. Analogous lists should be used in other contexts.	[0..*]	N/A

attribute	expected type	definition	cardinality	code list
registered location	Location	The registered location of the Organisation.	[0..1]	N/A

5.2.1.5.1.5 Learner

Definition: A Person who attends a Secondary Education Institution.

attribute	expected type	definition	cardinality	code list
learner id	Identifier	An unambiguous reference to the Learner.	[0..*]	N/A

5.2.1.5.1.6 Person

Definition: An individual person who may be dead or alive, but not imaginary.

Source: ISA² Core Person Vocabulary

attribute	expected type	definition	cardinality	code list
identifier	Identifier	The identifier relation is used to link a Person to any formally issued Identifier for that Person.	[0..*]	N/A
given name	Text	A given name, or multiple given names, are the denominator(s) that identify an individual within a family. These are given to a Person by his or her parents at birth or may be legally recognised as 'given names' through a formal process. All given names are ordered in one field so that, for example, the given name for Johann Sebastian Bach is “Johann Sebastian”.	[1..*]	N/A
family name	Text	A family name is usually shared by members of a family. This attribute also carries prefixes or suffixes which are part of the family name, e.g. “de Boer”, “van de Putte”, “von und zu Orlow”. Multiple family names, such as are commonly found in Hispanic countries, are recorded in the single family name field so that, for example, Miguel de Cervantes Saavedra's family name would be recorded as "de Cervantes Saavedra".	[1..*]	N/A
date of birth	Date	The day on which the Person was born.	[0..1]	N/A

attribute	expected type	definition	cardinality	code list
sex	Code	The chromosomal state, and reproductive organs and structures of a Person that allows them to be distinguished as female or male.	[0..1]	Human Sex
place of birth	Location	The Location where the Person was born.	[0..1]	N/A
registered address	Address	The registered address of the Person.	[0..1]	N/A

5.2.1.5.1.6.1 Location

Definition: An identifiable geographic place or named place.

Source: ISA² Core Location Vocabulary

Given that both attributes are optional, at least one of the attributes must be provided.

attribute	expected type	definition	cardinality	code list
geographic name	Text	A geographic name is a proper noun applied to a spatial object. The INSPIRE Data Specification on Geographical Names [INGN] provides a detailed model for describing a 'named place', including methods for providing multiple names in multiple scripts.	[0..*]	N/A
geographic identifier	URI	A URI that identifies the Location.	[0..1]	GeoNames
address	Address	The address property relationship associates a Location with the Address entity.	[0..1]	N/A

5.2.1.5.1.7 Address

Definition: A spatial object that identifies a fixed location of a property in a human-readable way.

Source: ISA² Core Location Vocabulary

attribute	expected type	definition	cardinality	code list
admin unit level 1	Code	The uppermost administrative unit for the address, almost always a country.	[1..1]	Country
admin unit level 2	Text	The region of the address, usually a county, state or other such area that typically encompasses several localities.	[0..*]	NUTS
full address	Text	The complete address written as a string, with or without formatting.	[0..*]	N/A

5.2.1.5.2 Complex datatypes

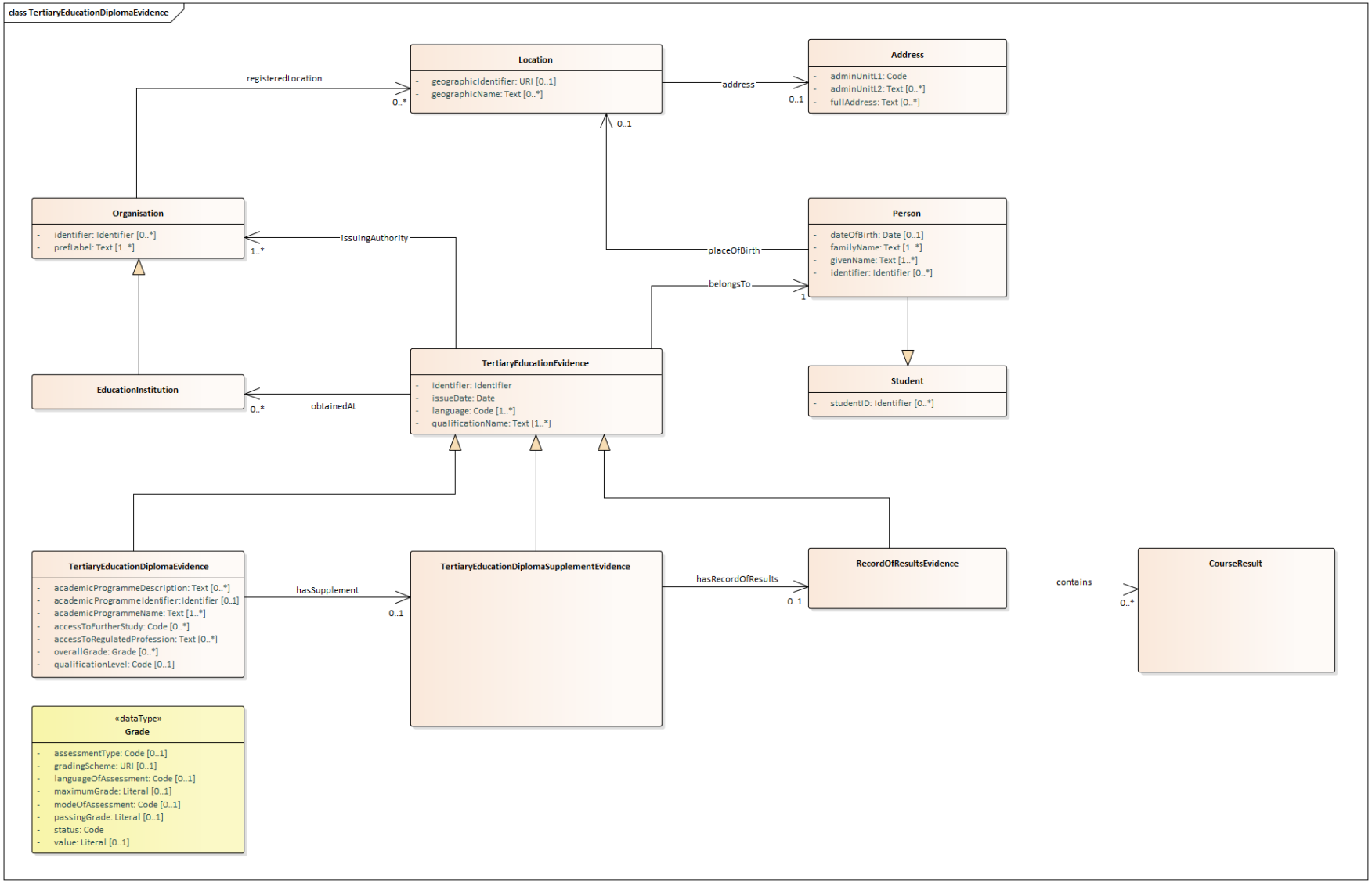
5.2.1.5.2.1 Grade

Definition: Mark indicating a degree of accomplishment.

attribute	expected type	definition	cardinality	code list
distribution	Text	Statistical distribution of grades over the number of students that obtained the respective grade.	[0..1]	N/A
grading scheme	URI	Dereferenceable identifier to the grading system that was used to give the grade.	[0..1]	N/A
status	Code	An indicator of the status of the course and the obtained grade, e.g. pass, fail, in-progress, unknown.	[1..1]	TBD
value	Literal	A (quantitative or qualitative) value according to the definition in the grading scheme.	[0..1]	N/A

- Tertiary education diploma evidence

5.2.1.6 Tertiary Education Diploma Evidence


class TertiaryEducationDiplomaEvidence
Location
- geographicIdentifier: URI [0..1]
- geographicName: Text [0..*]
Address
- adminUnitL1: Code
- adminUnitL2: Text [0..*]
- fullAddress: Text [0..*]
registeredLocation
0..*
address
0..1
0..1
Organisation
- identifier: Identifier [0..*]
- prefLabel: Text [1..*]
issuingAuthority
1..*
Person
- dateOfBirth: Date [0..1]
- familyName: Text [1..*]
- givenName: Text [1..*]
- identifier: Identifier [0..*]
placeOfBirth
belongsTo
1
TertiaryEducationEvidence
- identifier: Identifier
- issueDate: Date
- language: Code [1..*]
- qualificationName: Text [1..*]
EducationInstitution
0..*
obtainedAt
Student
- studentID: Identifier [0..*]
TertiaryEducationDiplomaEvidence
- academicProgrammeDescription: Text [0..*]
- academicProgrammeIdentifier:Identifier [0..1]
- academicProgrammeName: Text [1..*]
- accessToFurtherStudy: Code [0..*]
- accessToRegulatedProfession: Text [0..*]
- overallGrade: Grade [0..*]
- qualificationLevel: Code [0..1]
hasSupplement
0..1
TertiaryEducationDiplomaSupplementEvidence
hasRecordOfResults
0..1
RecordOfResultsEvidence
contains
0..*
CourseResult
«dataType»
Grade
- assessmentType: Code [0..1]
- gradingScheme: URI [0..1]
- languageOfAssessment: Code [0..1]
- maximumGrade: Literal [0..1]
- modeOfAssessment: Code [0..1]
- passingGrade: Literal [0..1]
- status: Code
- value: Literal [0..1]

Access the high resolution picture from this page.

5.2.1.6.1 Entities

5.2.1.6.1.1 Tertiary Education Evidence

Definition: Abstract superclass for evidences that are issued after obtaining a Tertiary Education grade.

Superclass of: Tertiary Education Diploma Evidence, Tertiary Education Diploma Supplement Evidence and Record of Results Evidence

attribute	expected type	definition	cardinality	code list
identifier	Identifier	An unambiguous reference to the Tertiary Education Evidence.	[1..1]	N/A
issue date	Date	The date on which the Tertiary Education Evidence was issued.	[1..1]	N/A
language	Code	The language in which the Tertiary Education Evidence is issued.	[1..*]	Language
qualification name	Text	Full name of the qualification, at least in the original language(s) as it is styled in the original qualification, e.g. Master of Science, Kandidat nauk, Maîtrise, Diplom, etc.	[1..*]	N/A
belongs to	Person	The Person that is the holder of the Tertiary Education Evidence.	[1..1]	N/A
obtained at	Education Institution	The Education Institution that educated the Student.	[0..*]	N/A
issuing authority	Organisation	The Organisation that issued the Tertiary Education Evidence.	[1..*]	N/A

5.2.1.6.1.2 Tertiary Education Diploma Evidence

Definition: Any formally awarded qualification/credential, issued by a competent authority attesting the successful completion of a recognised programme of study of tertiary education.

Subclass of: Tertiary Education Evidence

attribute	expected type	definition	cardinality	code list
academic programme name	Text	Full name of the academic programme, at least in the original language(s) as it is styled in the original qualification, e.g. Art & Education, Biochemistry & Molecular Pharmacology, Cybersecurity, Economics, etc.	[1..*]	N/A
academic programme identifier	Identifier	An unambiguous reference to the academic programme.	[0..1]	N/A
academic programme description	Text	An optional plain-text inventory of activities, content and/or methods employed for the purpose of education or training (acquiring knowledge, skills and/or competences) that occur in a logical sequence over a specified period of time.	[0..*]	N/A
access to further study	Code	Access to further academic and/or professional studies that the qualification provides, especially to specific qualifications, or levels of study, e.g.: access to Doctoral studies in the country or institution.	[0..*]	ISCED 2011 Levels
access to regulated profession	Text	Any rights to practise, or professional title, accorded to the holder of the qualification, in accordance with national legislation or requirements by a competent authority.	[0..*]	N/A
overall grade	Grade	The final grade awarded to the student.	[0..*]	N/A
qualification level	Code	Level of the obtained qualification.	[0..1]	ISCED 2011
has supplement	Tertiary Education Diploma Supplement Evidence	Supplementary document that serves as an annex, with additional information related to the Tertiary Education Diploma Evidence.	[0..1]	N/A

5.2.1.6.1.3 Tertiary Education Diploma Supplement Evidence

Definition: Document accompanying a Tertiary Education Diploma Evidence, providing a standardised description of the nature, level, context, content and status of the studies completed by its holder.

Subclass of: Tertiary Education Evidence

For further information, please see the tertiary education diploma supplement evidence data model

5.2.1.6.1.4 Record of Results Evidence

Definition: An official record or breakdown of a student's progress and achievements.

Subclass of: Tertiary Education Evidence

For further information, please see the record of results evidence data model

5.2.1.6.1.5 Course Result

Definition: Grade obtained after finishing/completing a course.

For further information, please see the record of results evidence data model

5.2.1.6.1.6 Education Institution

Definition: An Organisation that provides instructional services to individuals or education-related services to individuals and other educational institutions.

Subclass of: Organisation

No additional attributes are defined for this entity. It does inherit, however, all the attributes from Organisation listed here below.

5.2.1.6.1.7 Organisation

Definition: Represents a collection of people organised together into a community or other social, commercial or political structure. The group has some common purpose or reason for existence which goes beyond the set of people belonging to it and can act as an Agent. Organisations are often decomposable into hierarchical structures.

Source: The Organization Ontology

attribute	expected type	definition	cardinality	code list
preferred label	Text	As defined in the ORG Ontology, a preferred label is used to provide the primary, legally recognised name of the organisation. An organisation may only have one such name in any given language. Primary names may be provided in multiple languages with multiple instances of the preferred label property.	[1..*]	N/A
identifier	Identifier	Many organisations are referred to by some identifier. For example, among the EU institutions, the ECB is the identifier for the European Central Bank, OLAF for the European Anti-Fraud Office, and so on. These are formally recognised by the European Commission which provides a list of such acronyms. Analogous lists should be used in other contexts.	[0..*]	N/A
registered location	Location	The registered location of the Organisation.	[0..*]	N/A

5.2.1.6.1.8 Student

Definition: A person who attends a Tertiary Education Institution.

attribute	expected type	definition	cardinality	code list
student ID	Identifier	An unambiguous reference to the Student.	[0..*]	N/A

5.2.1.6.1.9 Person

Definition: An individual person who may be dead or alive, but not imaginary.

Source: ISA² Core Person Vocabulary

attribute	expected type	definition	cardinality	code list
identifier	Identifier	The identifier relation is used to link a Person to any formally issued Identifier for that Person.	[0..*]	N/A
given name	Text	A given name, or multiple given names, are the denominator(s) that identify an individual within a family. These are given to a Person by his or her parents at birth or may be legally recognised as 'given names' through a formal	[1..*]	N/A

attribute	expected type	definition	cardinality	code list
		process. All given names are ordered in one field so that, for example, the given name for Johann Sebastian Bach is “Johann Sebastian”.		
family name	Text	A family name is usually shared by members of a family. This attribute also carries prefixes or suffixes which are part of the family name, e.g. “de Boer”, “van de Putte”, “von und zu Orlow”. Multiple family names, such as are commonly found in Hispanic countries, are recorded in the single family name field so that, for example, Miguel de Cervantes Saavedra's family name would be recorded as "de Cervantes Saavedra".	[1..*]	N/A
date of birth	Date	The day on which the Person was born.	[0..1]	N/A
place of birth	Location	The Location where the Person was born.	[0..1]	N/A

5.2.1.6.1.9.1 Location

Definition: An identifiable geographic place or named place.

Source: ISA² Core Location Vocabulary

Given that both attributes are optional, at least one of the attributes must be provided.

attribute	expected type	definition	cardinality	code list
geographic name	Text	A geographic name is a proper noun applied to a spatial object. The INSPIRE Data Specification on Geographical Names [INGN] provides a detailed model for describing a 'named place', including methods for providing multiple names in multiple scripts.	[0..*]	N/A
geographic identifier	URI	A URI that identifies the Location.	[0..1]	GeoNames
address	Address	The address property relationship associates a Location with the Address entity.	[0..1]	N/A

5.2.1.6.1.10 Address

Definition: A spatial object that identifies a fixed location of a property in a human-readable way..

Source: ISA² Core Location Vocabulary

attribute	expected type	definition	cardinality	code list
admin unit level 1	Code	The uppermost administrative unit for the address, almost always a country.	[1..1]	Country
admin unit level 2	Text	The region of the address, usually a county, state or other such area that typically encompasses several localities.	[0..*]	NUTS
full address	Text	The complete address written as a string, with or without formatting.	[0..*]	N/A

5.2.1.6.2 Complex datatypes

5.2.1.6.2.1 Grade

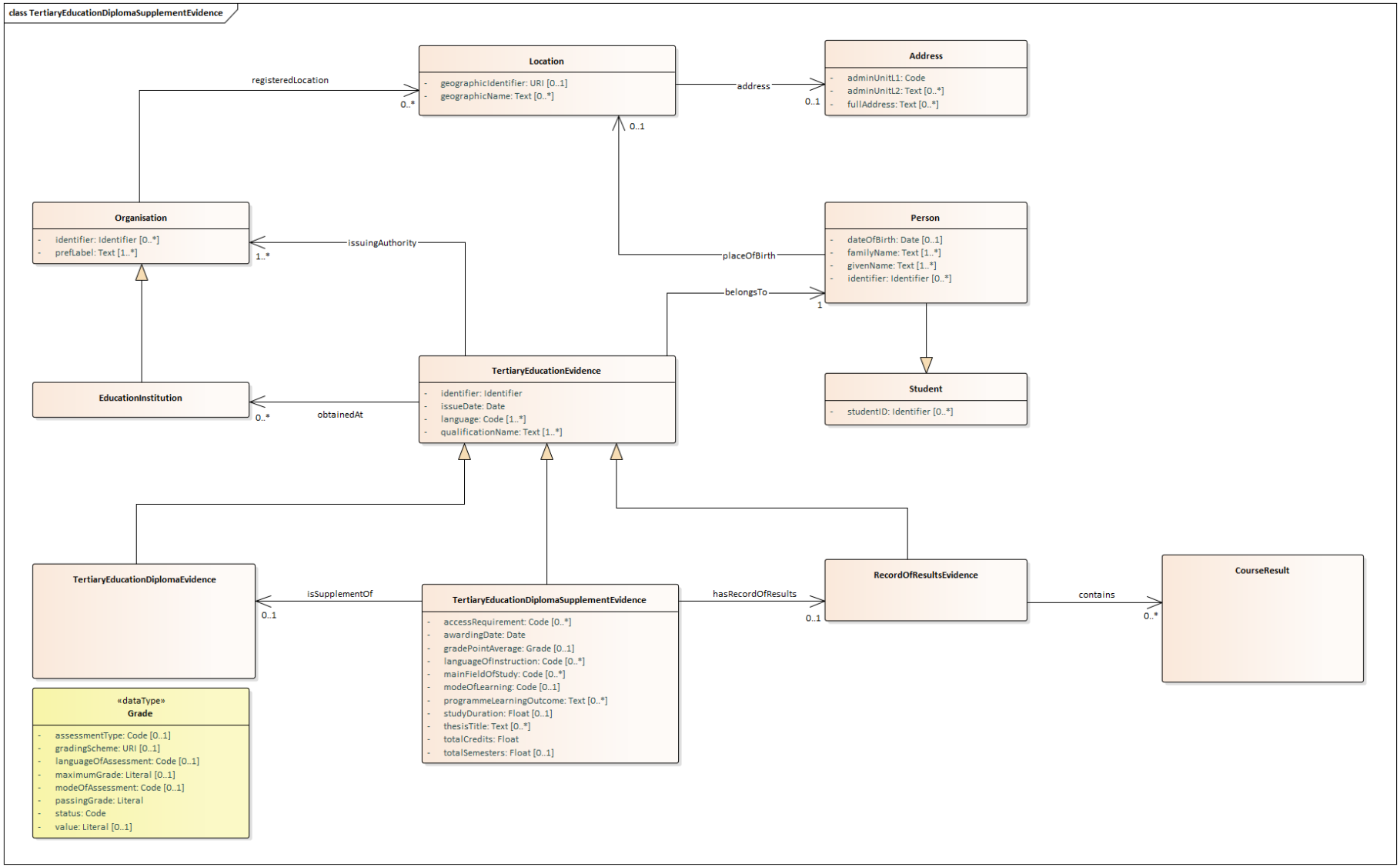
Definition: Mark indicating a degree of accomplishment.

attribute	expected type	definition	cardinality	code list
assessment type	Code	The type of assessment.	[0..1]	Europass Standard List of Assessment Types.
grading scheme	URI	Dereferenceable identifier to the grading system that was used to give the grade.	[0..1]	N/A
language of assessment	Code	The language(s) of assessment used.	[0..*]	Language
maximum grade	Literal	The maximum (quantitative or qualitative) value that can be achieved in an exam.	[0..1]	N/A

attribute	expected type	definition	cardinality	code list
mode of assessment	Code	The mode of assessment.	[0..1]	Europass Standard List of Modes Of Learning and Assessment.
passing grade	Literal	The (quantitative or qualitative) value that must be achieved in order to be successful in an exam.	[0..1]	N/A
status	Code	An indicator of the status of the course and the obtained grade, e.g. pass, fail, in-progress, unknown.	[1..1]	TBD
value	Literal	A (quantitative or qualitative) value according to the definition in the grading scheme.	[0..1]	N/A

- Tertiary education diploma supplement evidence

5.2.1.7 Tertiary Education Diploma Supplement Evidence


class TertiaryEducationDiplomaSupplementEvidence
Location
- geographicIdentifier: URI [0..1]
- geographicName: Text [0..*]
Address
- adminUnitL1: Code
- adminUnitL2: Text [0..*]
- fullAddress: Text [0..*]
registeredLocation
0..*
address
0..1
0..1
Organisation
- identifier: Identifier [0..*]
- prefLabel: Text [1..*]
issuingAuthority
1..*
placeOfBirth
Person
- dateOfBirth: Date [0..1]
- familyName: Text [1..*]
- givenName: Text [1..*]
- identifier: Identifier [0..*]
belongsTo
1
EducationInstitution
0..*
obtainedAt
TertiaryEducationEvidence
- identifier: Identifier
- issueDate: Date
- language: Code [1..*]
- qualificationName: Text [1..*]
Student
- studentID: Identifier [0..*]
TertiaryEducationDiplomaEvidence
isSupplementOf
0..1
TertiaryEducationDiplomaSupplementEvidence
- accessRequirement: Code [0..*]
- awardingDate: Date
- gradePointAverage: Grade [0..1]
- languageOfInstruction: Code [0..*]
- mainFieldOfStudy: Code [0..*]
- modeOfLearning: Code [0..1]
- programmeLearningOutcome: Text [0..*]
- studyDuration: Float [0..1]
- thesisTitle: Text [0..*]
- totalCredits: Float
- totalSemesters: Float [0..1]
hasRecordOfResults
0..1
RecordOfResultsEvidence
contains
0..*
CourseResult
«dataType»
Grade
- assessmentType: Code [0..1]
- gradingScheme: URI [0..1]
- languageOfAssessment: Code [0..1]
- maximumGrade: Literal [0..1]
- modeOfAssessment: Code [0..1]
- passingGrade: Literal
- status: Code
- value: Literal [0..1]

Access the high resolution picture from this page.

5.2.1.7.1 Entities

5.2.1.7.1.1 Tertiary Education Evidence

Definition: Abstract superclass for evidences that are issued after obtaining a Tertiary Education grade.

Superclass of: Tertiary Education Diploma Evidence, Tertiary Education Diploma Supplement Evidence and Record of Results Evidence

attribute	expected type	definition	cardinality	code list
identifier	Identifier	An unambiguous reference to the Tertiary Education Evidence.	[1..1]	N/A
issue date	Date	The date on which the Tertiary Education Evidence was issued.	[1..1]	N/A
language	Code	The language in which the Tertiary Education Evidence is issued.	[1..*]	Language
qualification name	Text	Full name of the qualification, at least in the original language(s) as it is styled in the original qualification, e.g. Master of Science, Kandidat nauk, Maîtrise, Diplom, etc.	[1..*]	N/A
belongs to	Person	The Person that is the holder of the Tertiary Education Evidence.	[1..1]	N/A
obtained at	Education Institution	The Education Institution that educated the Student.	[0..*]	N/A
issuing authority	Organisation	The Organisation that issued the Tertiary Education Evidence.	[1..*]	N/A

5.2.1.7.1.2 Tertiary Education Diploma Supplement Evidence

Definition: Document accompanying a Tertiary Education Diploma Evidence, providing a standardised description of the nature, level, context, content and status of the studies completed by its holder.

Subclass of: Tertiary Education Evidence

attribute	expected type	definition	cardinality	code list
awarding date	Date	The date when the qualification was awarded.	[1..1]	N/A
access requirement	Code	Qualification(s) or periods of study required for access to the programme.	[0..*]	ISCED 2011
grade point average	Grade	The grade point average of the course results, i.e. grades weighted based on the number of credits.	[0..1]	N/A
language of instruction	Code	The different languages in which the programme was given.	[0..*]	Language
main field of study	Code	The main disciplines or subject areas of a qualification.	[0..*]	ISCED 2013
mode of learning	Code	The mode of learning and/or assessment.	[0..1]	Europass Standard List of Modes Of Learning and Assessment.
programme learning outcome	Text	A statement of what the individual knows, understands and is able to do on completion of a learning process.	[0..*]	N/A
study duration	Float	Official duration of the programme in years of full-time study.	[0..1]	N/A
thesis title	Text	Title of the dissertation completed by a student as part of a tertiary education degree.	[0..*]	N/A
total credits	Float	The total number of credit points assigned to the qualification, following the ECTS credit system.	[1..1]	ECTS scoring scheme from Europass Standard List of Educational Credit Systems.
total semesters	Float	Number of 6-month periods the student has already studied in total.	[0..1]	N/A
is supplement of	Tertiary Education Diploma Evidence	The Tertiary Education Diploma Evidence to which this Supplement refers.	[0..1]	N/A

attribute	expected type	definition	cardinality	code list
has record of results	Record of Results Evidence	The Record of Results Evidence that is complementary to the Tertiary Education Diploma Supplement Evidence.	[0..1]	N/A

5.2.1.7.1.3 Tertiary Education Diploma Evidence

Definition: Any formally awarded qualification/credential, issued by a competent authority attesting the successful completion of a recognised programme of study of tertiary education.

Subclass of: Tertiary Education Evidence

For further information, please see the tertiary education diploma evidence data model

5.2.1.7.1.4 Record of Results Evidence

Definition: An official record or breakdown of a student's progress and achievements.

Subclass of: Tertiary Education Evidence

For further information, please see the record of results evidence data model

5.2.1.7.1.5 Course Result

Definition: Grade obtained after finishing/completing a course.

For further information, please see the record of results evidence data model

5.2.1.7.1.6 Education Institution

Definition: An Organisation that provides instructional services to individuals or education-related services to individuals and other educational institutions.

Subclass of: Organisation

No additional attributes are defined for this entity. It does inherit, however, all the attributes from Organisation listed here below.

5.2.1.7.1.7 Organisation

Definition: Represents a collection of people organised together into a community or other social, commercial or political structure. The group has some common purpose or reason for existence which goes beyond the set of people belonging to it and can act as an Agent. Organisations are often decomposable into hierarchical structures.

Source: The Organization Ontology

attribute	expected type	definition	cardinality	code list
preferred label	Text	As defined in the ORG Ontology, a preferred label is used to provide the primary, legally recognised name of the organisation. An organisation may only have one such name in any given language. Primary names may be provided in multiple languages with multiple instances of the preferred label property.	[1..*]	N/A
identifier	Identifier	Many organisations are referred to by some identifier. For example, among the EU institutions, the ECB is the identifier for the European Central Bank, OLAF for the European Anti-Fraud Office, and so on. These are formally recognised by the European Commission which provides a list of such acronyms. Analogous lists should be used in other contexts.	[0..*]	N/A
registered location	Location	The registered location of the Organisation.	[0..*]	N/A

5.2.1.7.1.8 Student

Definition: A person who attends a Tertiary Education Institution.

attribute	expected type	definition	cardinality	code list
student ID	Identifier	An unambiguous reference to the Student.	[0..*]	N/A

5.2.1.7.1.9 Person

Definition: An individual person who may be dead or alive, but not imaginary.

Source: ISA² Core Person Vocabulary

attribute	expected type	definition	cardinality	code list
identifier	Identifier	The identifier relation is used to link a Person to any formally issued Identifier for that Person.	[0..*]	N/A
given name	Text	A given name, or multiple given names, are the denominator(s) that identify an individual within a family. These are given to a Person by his or her parents at birth or may be legally recognised as 'given names' through a formal process. All given names are ordered in one field so that, for example, the given name for Johann Sebastian Bach is “Johann Sebastian”.	[1..*]	N/A
family name	Text	A family name is usually shared by members of a family. This attribute also carries prefixes or suffixes which are part of the family name, e.g. “de Boer”, “van de Putte”, “von und zu Orlow”. Multiple family names, such as are commonly found in Hispanic countries, are recorded in the single family name field so that, for example, Miguel de Cervantes Saavedra's family name would be recorded as "de Cervantes Saavedra".	[1..*]	N/A
date of birth	Date	The day on which the Person was born.	[0..1]	N/A
place of birth	Location	The Location where the Person was born.	[0..1]	N/A

5.2.1.7.1.9.1 Location

Definition: An identifiable geographic place or named place.

Source: ISA² Core Location Vocabulary

Given that both attributes are optional, at least one of the attributes must be provided.

attribute	expected type	definition	cardinality	code list
geographic name	Text	A geographic name is a proper noun applied to a spatial object. The INSPIRE Data Specification on Geographical Names [INGN] provides a detailed model for describing a 'named place', including methods for providing multiple names in multiple scripts.	[0..*]	N/A

attribute	expected type	definition	cardinality	code list
geographic identifier	URI	A URI that identifies the Location.	[0..1]	GeoNames
address	Address	The address property relationship associates a Location with the Address entity.	[0..1]	N/A

5.2.1.7.1.10 Address

Definition: A spatial object that identifies a fixed location of a property in a human-readable way.

Source: ISA² Core Location Vocabulary

attribute	expected type	definition	cardinality	code list
admin unit level 1	Code	The uppermost administrative unit for the address, almost always a country.	[1..1]	Country
admin unit level 2	Text	The region of the address, usually a county, state or other such area that typically encompasses several localities.	[0..*]	NUTS
full address	Text	The complete address written as a string, with or without formatting.	[0..*]	N/A

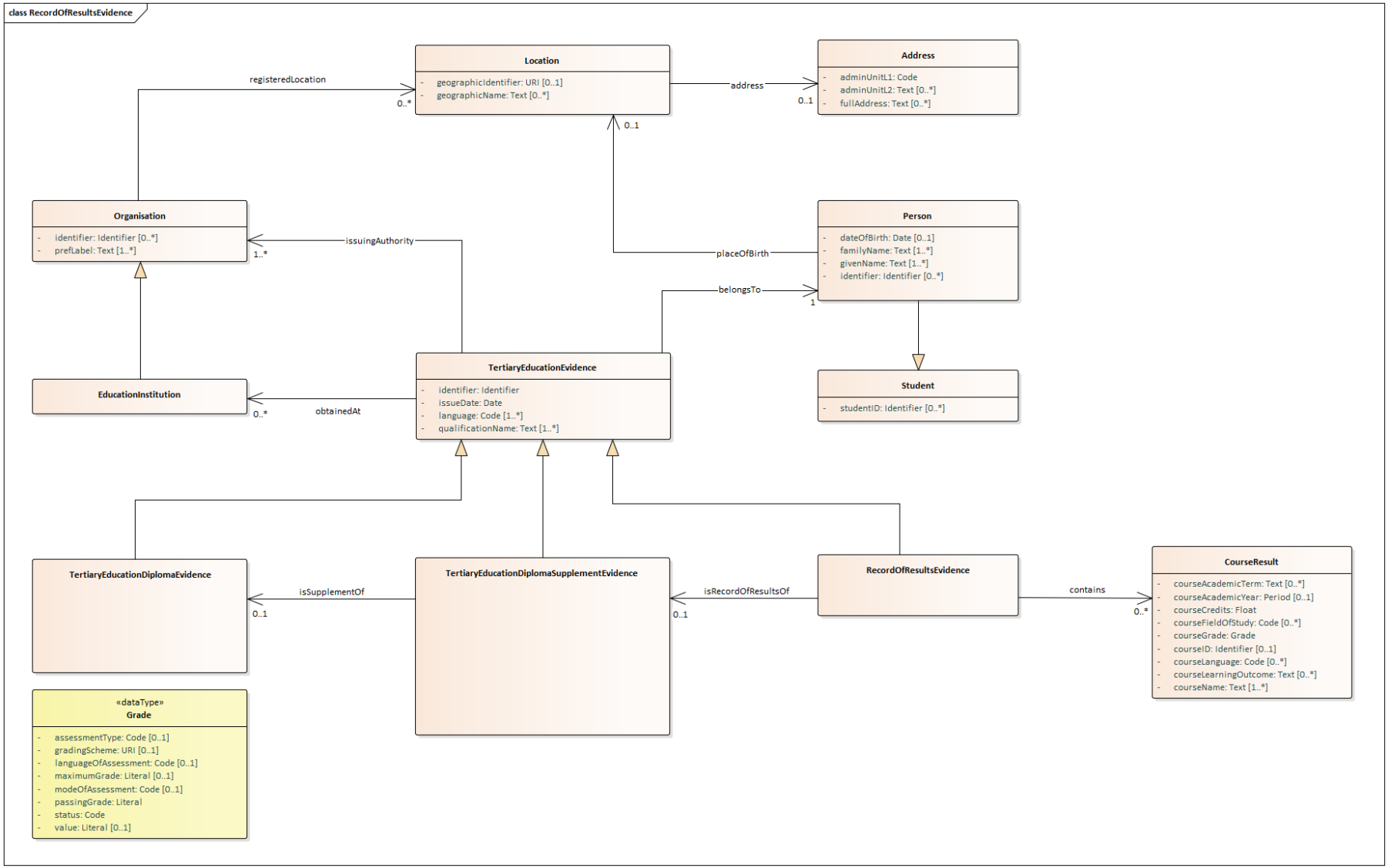
5.2.1.7.2 Complex datatypes

5.2.1.7.2.1 Grade

Definition: Mark indicating a degree of accomplishment.

attribute	expected type	definition	cardinality	code list
assessment type	Code	The type of assessment.	[0..1]	Europass Standard List of Assessment Types.
grading scheme	URI	Dereferenceable identifier to the grading system that was used to give the grade.	[0..1]	N/A
language of assessment	Code	The language(s) of assessment used.	[0..*]	Language
maximum grade	Literal	The maximum (quantitative or qualitative) value that can be achieved in an exam.	[0..1]	N/A
mode of assessment	Code	The mode of assessment.	[0..1]	Europass Standard List of Modes Of Learning and Assessment.
passing grade	Literal	The (quantitative or qualitative) value that must be achieved in order to be successful in an exam.	[0..1]	N/A
status	Code	An indicator of the status of the course and the obtained grade, e.g. pass, fail, in-progress, unknown.	[1..1]	TBD
value	Literal	A (quantitative or qualitative) value according to the definition in the grading scheme.	[0..1]	N/A

5.2.1.8 Record of Results Evidence


class RecordOfResultsEvidence
Location
- geographicIdentifier: URI [0..1]
- geographicName: Text [0..*]
Address
- adminUnitL1: Code
- adminUnitL2: Text [0..*]
- fullAddress: Text [0..*]
registeredLocation
0..*
address
0..1
0..1
Organisation
- identifier: Identifier [0..*]
- prefLabel: Text [1..*]
issuingAuthority
1..*
placeOfBirth
Person
- dateOfBirth: Date [0..1]
- familyName: Text [1..*]
- givenName: Text [1..*]
- identifier: Identifier [0..*]
belongsTo
1
EducationInstitution
0..*
obtainedAt
TertiaryEducationEvidence
- identifier: Identifier
- issueDate: Date
- language: Code [1..*]
- qualificationName: Text [1..*]
Student
- studentID: Identifier [0..*]
TertiaryEducationDiplomaEvidence
isSupplementOf
0..1
TertiaryEducationDiplomaSupplementEvidence
isRecordOfResultsOf
0..1
RecordOfResultsEvidence
contains
0..*
CourseResult
- courseAcademicTerm: Text [0..*]
- courseAcademicYear: Period [0..1]
- courseCredits: Float
- courseFieldOfStudy: Code [0..*]
- courseGrade: Grade
- courseID: Identifier [0..1]
- courseLanguage: Code [0..*]
- courseLearningOutcome: Text [0..*]
- courseName: Text [1..*]
«dataType»
Grade
- assessmentType: Code [0..1]
- gradingScheme: URI [0..1]
- languageOfAssessment: Code [0..1]
- maximumGrade: Literal [0..1]
- modeOfAssessment: Code [0..1]
- passingGrade: Literal
- status: Code
- value: Literal [0..1]

Access the high resolution picture from this page.

5.2.1.8.1 Entities

5.2.1.8.1.1 Tertiary Education Evidence

Definition: Abstract superclass for evidences that are issued after obtaining a Tertiary Education grade.

Superclass of: Tertiary Education Diploma Evidence, Tertiary Education Diploma Supplement Evidence and Record of Results Evidence

attribute	expected type	definition	cardinality	code list
identifier	Identifier	An unambiguous reference to the Tertiary Education Evidence.	[1..1]	N/A
issue date	Date	The date on which the Tertiary Education Evidence was issued.	[1..1]	N/A
language	Code	The language in which the Tertiary Education Evidence is issued.	[1..*]	Language
qualification name	Text	Full name of the qualification, at least in the original language(s) as it is styled in the original qualification, e.g. Master of Science, Kandidat nauk, Maîtrise, Diplom, etc.	[1..*]	N/A
belongs to	Person	The Person that is the holder of the Tertiary Education Evidence.	[1..1]	N/A
obtained at	Education Institution	The Education Institution that educated the Student.	[0..*]	N/A
issuing authority	Organisation	The Organisation that issued the Tertiary Education Evidence.	[1..*]	N/A

5.2.1.8.1.2 Record of Results Evidence

Definition: An official record or breakdown of a student's progress and achievements.

Subclass of: Tertiary Education Evidence

attribute	expected type	definition	cardinality	code list
contains	Course Result	The specific course results that together make up the Record of Results Evidence.	[0..*]	N/A
is record of results of	Tertiary Education Diploma Supplement Evidence	The Tertiary Education Diploma Supplement Evidence to which this Record of Results Evidence is complementary.	[0..1]	N/A

5.2.1.8.1.3 Course Result

Definition: Grade obtained after finishing/completing a course.

attribute	expected type	definition	cardinality	code list
course academic term	Text	Term of the academic year when the course took place, e.g. first semester, second trimester, etc.	[0..*]	N/A
course academic year	Period	The time interval expressed in years during which the course took place.	[0..1]	N/A
course credits	Float	The number of ECTS credits the student has achieved by completing the course, following the ECTS system	[1..1]	ECTS scoring scheme from Europass Standard List of Educational Credit Systems.
course field of study	Code	The discipline or subject area of a course.	[0..*]	ISCED 2013
course grade	Grade	A mark indicating a degree of accomplishment for a particular course.	[1..1]	N/A
course identifier	Identifier	An unambiguous reference to the course	[0..1]	N/A
course language	Code	Main language in which the course was taught.	[0..*]	N/A

attribute	expected type	definition	cardinality	code list
course learning outcome	Text	A free text describing a student's (expected) learning outcome of the course. A detailed learning outcome description may include, knowledge, skills and responsibility achieved upon completing the course.	[0..*]	N/A
course name	Text	Name given to a number of lectures or other matters dealing with a subject, i.e. the course.	[1..*]	N/A

5.2.1.8.1.4 Tertiary Education Diploma Supplement Evidence

Definition: Document accompanying a Tertiary Education Diploma Evidence, providing a standardised description of the nature, level, context, content and status of the studies completed by its holder.

Subclass of: Tertiary Education Evidence

For further information, please see the tertiary education diploma supplement evidence data model

5.2.1.8.1.5 Tertiary Education Diploma Evidence

Definition: Any formally awarded qualification/credential, issued by a competent authority attesting the successful completion of a recognised programme of study of tertiary education.

Subclass of: Tertiary Education Evidence

For further information, please see the tertiary education diploma evidence data model

5.2.1.8.1.6 Education Institution

Definition: An Organisation that provides instructional services to individuals or education-related services to individuals and other educational institutions.

Subclass of: Organisation

No additional attributes are defined for this entity. It does inherit, however, all the attributes from Organisation listed here below.

5.2.1.8.1.7 Organisation

Definition: Represents a collection of people organised together into a community or other social, commercial or political structure. The group has some common purpose or reason for existence which goes beyond the set of people belonging to it and can act as an Agent. Organisations are often decomposable into hierarchical structures.

Source: The Organization Ontology

attribute	expected type	definition	cardinality	code list
preferred label	Text	As defined in the ORG Ontology, a preferred label is used to provide the primary, legally recognised name of the organisation. An organisation may only have one such name in any given language. Primary names may be provided in multiple languages with multiple instances of the preferred label property.	[1..*]	N/A
identifier	Identifier	Many organisations are referred to by some identifier. For example, among the EU institutions, the ECB is the identifier for the European Central Bank, OLAF for the European Anti-Fraud Office, and so on. These are formally recognised by the European Commission which provides a list of such acronyms. Analogous lists should be used in other contexts.	[0..*]	N/A
registered location	Location	The registered location of the Organisation.	[0..*]	N/A

5.2.1.8.1.8 Student

Definition: A person who attends a Tertiary Education Institution.

attribute	expected type	definition	cardinality	code list
student ID	Identifier	An unambiguous reference to the Student.	[0..*]	N/A

5.2.1.8.1.9 Person

Definition: An individual person who may be dead or alive, but not imaginary.

Source: ISA² Core Person Vocabulary

attribute	expected type	definition	cardinality	code list
identifier	Identifier	The identifier relation is used to link a Person to any formally issued Identifier for that Person.	[0..*]	N/A
given name	Text	A given name, or multiple given names, are the denominator(s) that identify an individual within a family. These are given to a Person by his or her parents at birth or may be legally recognised as 'given names' through a formal process. All given names are ordered in one field so that, for example, the given name for Johann Sebastian Bach is “Johann Sebastian”.	[1..*]	N/A
family name	Text	A family name is usually shared by members of a family. This attribute also carries prefixes or suffixes which are part of the family name, e.g. “de Boer”, “van de Putte”, “von und zu Orlow”. Multiple family names, such as are commonly found in Hispanic countries, are recorded in the single family name field so that, for example, Miguel de Cervantes Saavedra's family name would be recorded as "de Cervantes Saavedra".	[1..*]	N/A
date of birth	Date	The day on which the Person was born.	[0..1]	N/A
place of birth	Location	The Location where the Person was born.	[0..1]	N/A

5.2.1.8.1.9.1 Location

Definition: An identifiable geographic place or named place.

Source: ISA² Core Location Vocabulary

Given that both attributes are optional, at least one of the attributes must be provided.

attribute	expected type	definition	cardinality	code list
geographic name	Text	A geographic name is a proper noun applied to a spatial object. The INSPIRE Data Specification on Geographical Names [INGN] provides a detailed model for describing a 'named place', including methods for providing multiple names in multiple scripts.	[0..*]	N/A

attribute	expected type	definition	cardinality	code list
geographic identifier	URI	A URI that identifies the Location.	[0..1]	GeoNames
address	Address	The address property relationship associates a Location with the Address entity.	[0..1]	N/A

5.2.1.8.1.10 Address

Definition: A spatial object that identifies a fixed location of a property in a human-readable way.

Source: ISA² Core Location Vocabulary

attribute	expected type	definition	cardinality	code list
admin unit level 1	Code	The uppermost administrative unit for the address, almost always a country.	[1..1]	Country
admin unit level 2	Text	The region of the address, usually a county, state or other such area that typically encompasses several localities.	[0..*]	NUTS
full address	Text	The complete address written as a string, with or without formatting.	[0..*]	N/A

5.2.1.8.2 Complex datatypes

5.2.1.8.2.1 Grade

Definition: Mark indicating a degree of accomplishment.

attribute	expected type	definition	cardinality	code list
assessment type	Code	The type of assessment.	[0..1]	Europass Standard List of Assessment Types.

attribute	expected type	definition	cardinality	code list
grading scheme	URI	Dereferenceable identifier to the grading system that was used to give the grade.	[0..1]	N/A
language of assessment	Code	The language(s) of assessment used.	[0..*]	Language
maximum grade	Literal	The maximum (quantitative or qualitative) value that can be achieved in an exam.	[0..1]	N/A
mode of assessment	Code	The mode of assessment.	[0..1]	Europass Standard List of Modes Of Learning and Assessment.
passing grade	Literal	The (quantitative or qualitative) value that must be achieved in order to be successful in an exam.	[0..1]	N/A
status	Code	An indicator of the status of the course and the obtained grade, e.g. pass, fail, in-progress, unknown.	[1..1]	TBD
value	Literal	A (quantitative or qualitative) value according to the definition in the grading scheme.	[0..1]	N/A

5.2.2 Education Domain Code Lists - June 2022

Code lists give control over which values can be encoded for specific properties of the various data models. The constraints imposed by code lists facilitate semantic interoperability and help to scale up the automated processing and exchange of evidences.

5.2.2.1 Code lists for Education evidence types

During the development of data models, the editors have identified together with experts from Member States existing code lists that can be reused as part of the common data models. They have also identified the properties for which code lists should be created. The table below gives an overview of both the

existing and the potential candidates for Education code lists, categorising them by scope, status and described property. The creation of new code lists and the updates of existing ones will be done in the next quarter of 2022.

By default, code lists should follow the SKOS principles, be published with persistent identifiers and be managed by an an authoritative organisation, ideally the Publications Office.

Member States have the possibility to either make use of the code lists directly or to do a mapping exercise with their national code lists. In the latter case, SKOS, which stands for Simple Knowledge Organization System, can be used. It is a W3C recommendation for sharing and linking knowledge organisation systems. The SKOS mapping properties are skos:closeMatch, skos:exactMatch, skos:broadMatch, skos:narrowMatch and skos:relatedMatch. These properties are used to express the nature of the alignment between concepts from different concept schemes.

Scope	Code list	Status*	Described property	Comment
Secondary education completion evidence	Human Sex	Existing	Sex	Missing non-binary genders
Tertiary education diploma evidence, record of results, tertiary education diploma supplement, secondary education completion evidence	Country	Existing	Admin unit level 1	Missing stateless concept
Tertiary education diploma evidence, record of results, tertiary education diploma supplement, secondary education completion evidence	NUTS	Existing	Admin unit level 2	Other alternative such as Administrative territorial unit type Named Authority List or Local Administrative Units. See GitHub
Tertiary education diploma evidence, record of results, tertiary education diploma supplement, secondary education completion evidence	Language	Existing	Language, language of assessment, language of instruction, course language etc.	
Tertiary education diploma evidence, record of results, tertiary education diploma supplement, secondary education completion evidence	GeoNames	Existing	Geographic identifier	
Tertiary education diploma evidence	ISCED 2011 levels	To create	Access to further study	
Tertiary education diploma evidence, tertiary education diploma supplement	ISCED 2011	To create	Access requirements, qualification level	Or EQF?

Record of results, tertiary education diploma supplement	ISCED 2013	To create	Main field of study, course field study	Or EQF, European Science Vocabulary?
Tertiary education diploma supplement	Learning Activity	Existing	Mode of learning	
Secondary education completion evidence	European Science Vocabulary	Existing	Course name	
Tertiary education diploma evidence, record of results, tertiary education diploma supplement	N/A	To create	Assessment type	Europass Standard List of Assessment Types
Tertiary education diploma evidence, record of results, tertiary education diploma supplement	N/A	To create	Mode of assessment	Europass Standard List of Modes Of Learning and Assessment
Tertiary education diploma evidence, record of results, tertiary education diploma supplement	N/A	To create	Status	E.g. passed, failed

*In the status column, there are two values, *'existing'* or *'to create'*. In the first instance, there is an existing code list that is proposed for reuse. In the second instance, there is - to our knowledge - no existing code list to be reused and therefore a new one needs to be created. It must be noted that all code lists have been proposed, but they haven't been validated by the Member States.

5.3 Vehicle Domain - June 2022

This section contains data models and code lists for evidence related to the vehicle domain.

This section also includes some information on the relation of the OOTS and EUCARIS.

NOTE
The data models and code lists have not been updated since the release of July 2021.
The restructuring of the existing content of this chapter on specific evidence types and the creation of the three domain categories is a first step towards creating more detailed specifications for evidence exchanges in the various procedures in scope of the SDG regulation. In the future, these sections will also include (or reference) the deliverables of the work on procedures, requirements and evidence types and provide more detailed coverage of alignment with other initiatives, including so-called related systems.

5.3.1 Vehicle Domain Data Models - June 2022

5.3.1.1 Introduction

The data models are available as **UML diagrams** and **Tables:**

- **UML Diagrams:** Models are visually represented in a diagram based on the UML (Unified Modeling Language) with the purpose of displaying the classes, their attributes and cardinalities along with the relationships between the classes.
- **Tables:** Models are represented in a tabular view with additional information not included in the UML diagram such as expected type, definition and code list.

5.3.1.2 SDG Sandbox

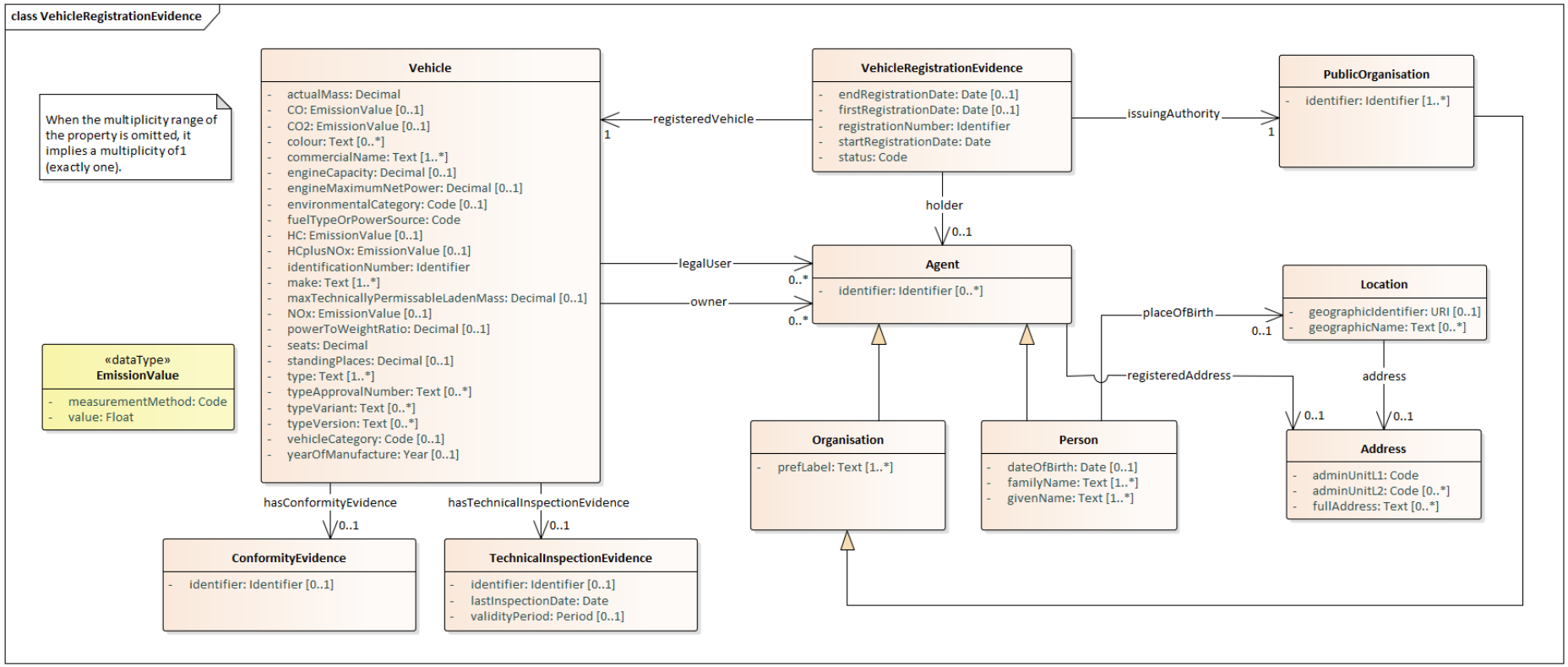
Click here to see the links to the SDG Sandbox common data models

Vehicle registration evidence

5.3.1.3 Data model for vehicle domain

- Vehicle registration evidence

5.3.1.4 Vehicle Registration Evidence



Access the high resolution picture from this page.

5.3.1.4.1 Entities

5.3.1.4.1.1 Vehicle Registration Evidence

Definition: Official document or data proving the registration of a Vehicle.

Source: Council Directive 1999/37/EC of 29 April 1999 on the registration documents for vehicles

attribute	expected type	definition	cardinality	code list
registration number	Identifier	A numeric or alphanumeric identifier that uniquely identifies the Vehicle (or vehicle owner) within the isssuing region's vehicle register. Also known as license/number plate.	[1..1]	N/A
status	Code	Actual status of the vehicle's registration.	[1..1]	Issue #16
first registration date	Date	Date of first registration of the Vehicle (somewhere in the world).	[0..1]	N/A
start registration date	Date	Start date of registration of the Vehicle in the Member State.	[1..1]	N/A
end registration date	Date	End date of registration of the Vehicle in the Member State. (This property is used if the vehicle has been de-registered in the Member State.)	[0..1]	N/A
registered Vehicle	Vehicle	The Vehicle that is the subject of the Vehicle Registration Evidence.	[1..1]	N/A
issuing authority	Public Organisation	A Public Organisation with official authority in charge of issuing the Vehicle Registration Evidence.	[1..1]	N/A
holder	Agent	The natural person or legal person in whose name the Vehicle is registered.	[0..1]	N/A

5.3.1.4.1.2 Vehicle

Definition: A machine, usually with wheels and a means of propulsion (e.g. an engine or a motor), used for transporting people or goods on land, especially on roads.

Source: Council Directive 1999/37/EC of 29 April 1999 on the registration documents for vehicles

attribute	expected type	definition	cardinality	code list
identification number	Identifier	Vehicle identification number (VIN).	[1..1]	N/A

attribute	expected type	definition	cardinality	code list
make	Text	The make of the Vehicle, e.g. Ford, Opel, Renault, etc.	[1..*]	N/A
type	Text	The type of the Vehicle as described in B. of Annex II of Directive 2007/46/EC.	[1..*]	N/A
type variant	Text	The type variant of the Vehicle as described in B. of Annex II of Directive 2007/46/EC.	[0..*]	N/A
type version	Text	The type version of the Vehicle as described in B. of Annex II of Directive 2007/46/EC.	[0..*]	N/A
vehicle category	Code	The category of the Vehicle as described in A. of Annex II of Directive 2007/46/EC.	[0..*]	A. of Annex II of Directive 2007/46/EC
commercial name	Text	The commercial name of the Vehicle, e.g. Focus, Astra, Megane.	[1..*]	N/A
maximum technically permissable laden mass	Decimal	The maximum technically permissible laden mass of the Vehicle (in kg).	[0..1]	N/A
actual mass	Decimal	The mass of the vehicle in service with bodywork, and with coupling device in the case of a towing vehicle in service from any category other than M1 (in kg).	[1..1]	N/A
type approval number	Text	The type-approval number.	[0..*]	N/A
engine capacity	Decimal	The engine capacity (in cm3).	[0..1]	N/A
engine maximum net power	Decimal	The engine maximum net power (in kW).	[0..1]	N/A
fuel type or power source	Code	The type of fuel or power source.	[1..1]	TBD
power to weight ratio	Decimal	The power to weight ratio (in kW/kg). (Only for motorcycles.)	[0..1]	N/A

attribute	expected type	definition	cardinality	code list
seats	Decimal	The number of seats, including the driver's seat.	[1..1]	N/A
standing places	Decimal	The number of standing places (where appropriate).	[0..1]	N/A
colour	Text	The main, basic color of the Vehicle.	[0..1]	N/A
year of manufacture	Year	The year in which the Vehicle was produced.	[0..1]	N/A
environmental category	Code	Indication of the environmental category of EC type-approval.	[0..1]	Directive 70/220/EEC (for positive-ignition engines) or Directive 88/77/EEC (for diesel engines)
CO2	EmissionValue	Exhaust emissions of carbon dioxide (in g/km).	[0..1]	N/A
CO	EmissionValue	Exhaust emissions of carbon monoxide (in g/km).	[0..1]	N/A
HC	EmissionValue	Exhaust emissions of hydrocarbon (in g/km).	[0..1]	N/A
NOx	EmissionValue	Exhaust emissions of nitrogen oxides (in g/km).	[0..1]	N/A
HC + NOx	EmissionValue	Exhaust emissions of hydrocarbon and nitrogen oxides (in g/km).	[0..1]	N/A
has conformity evidence	Conformity Evidence	The Conformity Evidence of the Vehicle.	[0..1]	N/A
has technical inspection evidence	Technical Inspection Evidence	The last Technical Inspection Evidence of the Vehicle.	[0..1]	N/A
owner	Agent	The natural person or legal person that is the legal owner of the Vehicle (i.e. the entity that has bought the Vehicle, and has the right to sell it).	[0..*]	N/A
legal user	Agent	The natural person or legal person that has the legal right to use the Vehicle.	[0..*]	N/A

5.3.1.4.1.3 Conformity Evidence

Definition: Official document or data proving that the technical characteristics of the produced type of vehicle fulfils all the technical, safety and environmental requirements needed for EC Whole Vehicle Type Approval (EC-WVTA), at the time of its production.

attribute	expected type	definition	cardinality	code list
identifier	Identifier	The identifier relation is used to link a Technical Inspection Evidence to any formally issued Identifier for that Technical Inspection Evidence.	[0..1]	N/A

5.3.1.4.1.4 Technical Inspection Evidence

Definition: Official document or data proving the Vehicle's (non)compliance to the technical and legal specifications by means of an inspection.

attribute	expected type	definition	cardinality	code list
identifier	Identifier	The identifier relation is used to link a Technical Inspection Evidence to any formally issued Identifier for that Technical Inspection Evidence.	[0..1]	N/A
last inspection date	Date	The last date on which the Vehicle underwent a Technical Inspection.	[1..1]	N/A
validity period	Period	The Period of time during which the Vehicle is deemed technically safe to drive on public roads and after which it needs to be inspected again.	[0..1]	N/A

5.3.1.4.1.5 Agent

Definition: Any entity that is able to carry out actions.

attribute	expected type	definition	cardinality	code list
identifier	Identifier	The identifier relation is used to link an Agent to any formally issued Identifier for that Agent.	[0..*]	N/A

attribute	expected type	definition	cardinality	code list
registered address	Address	The registered Address of the Agent.	[0..1]	N/A

5.3.1.4.1.6 Person

Definition: An individual natural person who may be dead or alive, but not imaginary.

Subclass of: Agent

Source: ISA² Core Person Vocabulary

attribute	expected type	definition	cardinality	code list
given name	Text	A given name, or multiple given names, are the denominator(s) that identify an individual within a family. These are given to a Person by his or her parents at birth or may be legally recognised as 'given names' through a formal process. All given names are ordered in one field so that, for example, the given name for Johann Sebastian Bach is “Johann Sebastian”.	[1..*]	N/A
family name	Text	A family name is usually shared by members of a family. This attribute also carries prefixes or suffixes which are part of the family name, e.g. “de Boer”, “van de Putte”, “von und zu Orlow”. Multiple family names, such as are commonly found in Hispanic countries, are recorded in the single family nme field so that, for example, Miguel de Cervantes Saavedra's family name would be recorded as "de Cervantes Saavedra".	[1..*]	N/A
date of birth	Date	The day on which the Person was born.	[0..1]	N/A
place of birth	Location	The Location where the Person was born.	[0..1]	N/A

5.3.1.4.1.7 Organisation

Definition: Represents a collection of people organised together into a community or other social, commercial or political structure. The group has some common purpose or reason for existence which goes beyond the set of people belonging to it and can act as an Agent. Organisations are often decomposable into hierarchical structures.

Subclass of: Agent

Source: The Organization Ontology

attribute	expected type	definition	cardinality	code list
preferred label	Text	As defined in the ORG Ontology, a preferred label is used to provide the primary, legally recognised name of the organisation. An organisation may only have one such name in any given language. Primary names may be provided in multiple languages with multiple instances of the preferred label property.	[1..*]	N/A

5.3.1.4.1.8 Public Organisation

Definition: Any organisation that is defined as being part of the public sector by a legal framework at any level.

Subclass of: Organisation

Source: ISA² Core Public Organisation Vocabulary

attribute	expected type	definition	cardinality	code list
identifier	Identifier	The identifier relation is used to link a Public Organisation to any formally issued Identifier for that Public Organisation.	[1..*]	N/A

5.3.1.4.1.9 Location

Definition: An identifiable geographic place or named place.

Source: ISA² Core Location Vocabulary

Given that both attributes are optional, at least one of the attributes must be provided.

attribute	expected type	definition	cardinality	code list
geographic name	Text	A geographic name is a proper noun applied to a spatial object. The INSPIRE Data Specification on Geographical Names [INGN] provides a detailed model for describing a 'named place', including methods for providing multiple names in multiple scripts.	[0..*]	N/A
geographic identifier	URI	A URI that identifies the Location.	[0..1]	GeoNames
address	Address	The address property relationship associates a Location with the Address entity.	[0..1]	N/A

5.3.1.4.1.10 Address

Definition: A spatial object that identifies a fixed location of a property in a human-readable way.

Source: ISA² Core Location Vocabulary

attribute	expected type	definition	cardinality	code list
admin unit level 1	Code	The uppermost administrative unit for the address, almost always a country.	[1..1]	Country
admin unit level 2	Code	The region of the address, usually a county, state or other such area that typically encompasses several localities.	[0..*]	NUTS
full address	Text	The complete address written as a string, with or without formatting.	[0..*]	N/A

5.3.1.4.2 Complex datatypes

5.3.1.4.2.1 Emission Value

Definition: Value of an exhaust emission, as assessed via a certain measuring method.

attribute	expected type	definition	cardinality	code list
measurement method	Code	The method or procedure that was used to measure and/or calculate the exhaust emission.	[1..1]	{WLTP, NEDC}
value	Float	The actual value of the Emission as measured via the measurement method.	[1..1]	N/A

5.3.2 Vehicle Domain Code Lists - June 2022

Code lists give control over which values can be encoded for specific properties of the various data models. The constraints imposed by code lists facilitate semantic interoperability and help to scale up the automated processing and exchange of evidences.

5.3.2.1 Code lists for vehicle domain

During the development of data models, the editors have identified together with experts from Member States existing code lists that can be reused as part of the common data models. They have also identified the properties for which code lists should be created. The table below gives an overview of both the existing and the potential candidates for Vehicle Domain code lists, categorising them by scope, status and described property. The creation of new code lists and the updates of existing ones will be done periodically.

By default, code lists should follow the SKOS principles, be published with persistent identifiers and be managed by an authoritative organisation, ideally the Publications Office.

Member States have the possibility to either make use of the code lists directly or to do a mapping exercise with their national code lists. In the latter case, SKOS, which stands for Simple Knowledge Organization System, can be used. It is a W3C recommendation for sharing and linking knowledge organisation systems. The SKOS mapping properties are skos:closeMatch, skos:exactMatch, skos:broadMatch, skos:narrowMatch and skos:relatedMatch. These properties are used to express the nature of the alignment between concepts from different concept schemes.

Scope	Code list	Status*	Described property	Comment
Vehicle registration evidence	Country	Existing	Admin unit level 1	Missing stateless concept
Vehicle registration evidence	NUTS	Existing	Admin unit level 2	Other alternative such as

				Administrative territorial unit type Named Authority List or Local Administrative Units. See GitHub
Vehicle registration evidence	GeoNames	Existing	Geographic identifier	
Vehicle registration evidence	N/A	To create	Vehicle status	See GitHub, EUCARIS VAT XSD
Vehicle registration evidence	N/A	To create	Vehicle category	Directive 2007/46/EC (A. of Annex II)
Vehicle registration evidence	N/A	To create	Environmental category	Directive 70/220/EEC (for positive-ignition engines) & directive 88/77/EEC (for diesel engines)
Vehicle registration evidence	N/A	To create	Measurement methods for emission value	Method or procedure to measure the exhaust emission of a vehicle {WLTP, NEDC}
Vehicle registration evidence	N/A	To create	Fuel type or power source	Based on Eurostat, development of a simple code list containing the following values (petroleum products, diesel, alternative energy).

*In the status column, there are two values, *'existing'* or *'to create'*. In the first instance, there is an existing code list that is proposed for reuse. In the second instance, there is - to our knowledge - no existing code list to be reused and therefore a new one needs to be created. It must be noted that all code lists have been proposed, but they haven't been validated by the Member States.

5.3.3 EUCARIS

EUCARIS and OOTS have similar content and processes. The Article 14(10) exemption does not apply to EUCARIS, as there is no Union wide legal basis that mandates use of EUCARIS in procedures in the scope of OOTS

EC and the EUCARIS Secretariat have been authoring a joint non-paper to:

- Analyse the relation between OOTS and EUCARIS, how EUCARIS can be leveraged for OOTS and how OOTS can complement or extend the use of EUCARIS.
- Illustrate how unnecessary overlap or duplication can be avoided and, to the contrary, the two systems will complement and extend each other.

The main initial findings of the joint work are that:

- OOTS can directly use data models and schema from EUCARIS, leveraging decades of work on semantic interoperability for the vehicle domain.
- A variety of options are available to connect EUCARIS and OOTS. A technical "bridge" would reduce initial and recurrent development and operational costs enormously.
- Evidence Requesters that currently use EUCARIS capabilities in their back-end processes can continue to do so.
- OOTS can complement and extend the automated exchange of vehicle information, including to Member States that do not currently use EUCARIS for an OOTS procedure.

The non-paper is close to being finalized and will be made available to the Member States.

The Commission and EUCARIS teams believe that:

- a cost-effective and useful combination of the two systems can be created that reuses the vast majority of EUCARIS investments and opens the vehicle domain data to new user-centric applications.
- a range of next steps should be taken to create and deliver an integrated system combining elements from OOTS and EUCARIS in an efficient and effective way

Short term actions:

- Proof-of-concept of technical integration.
- Identification of schemas from the EUCARIS catalogue for use in OOTS procedure steps.
- Align with the OOTS workshops on procedure requirements and evidence types.
- Planning to deliver a proven production integration by December 2023.

5.4 Public Documents - June 2022

The public documents section includes data models for specific evidences that can be used in multiple domains as for example Birth and Marriage evidence.

NOTE
The data models and code lists have not been updated since the release of July 2021.

The restructuring of the existing content of this chapter on specific evidence types and the creation of the three domain categories is a first step towards creating more detailed specifications for evidence exchanges in the various procedures in scope of the SDG regulation. In the future, these sections will also include (or reference) the deliverables of the work on procedures, requirements and evidence types and provide more detailed coverage of alignment with other initiatives, including so-called related systems.

The content of this chapter is structured in the following sub-chapters:

5.4.1 Public Documents Data Models - June 2022

5.4.1.1 Introduction

The data models are available as **UML diagrams** and **Tables:**

- **UML Diagrams:** Models are visually represented in a diagram based on the UML (Unified Modeling Language) with the purpose of displaying the classes, their attributes and cardinalities along with the relationships between the classes.
- **Tables:** Models are represented in a tabular view with additional information not included in the UML diagram such as expected type, definition and code list.

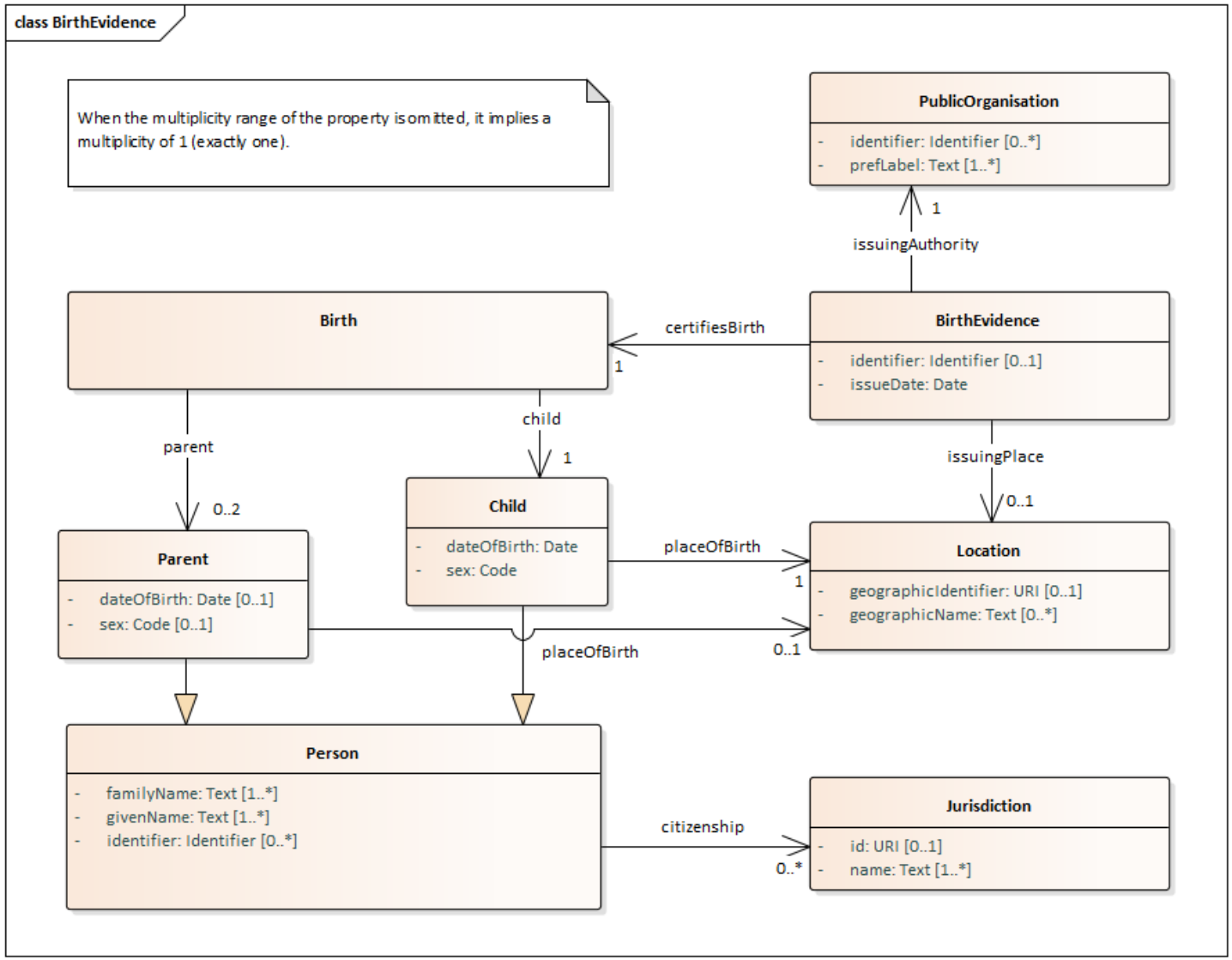
5.4.1.2 SDG Sandbox

Click here to see the links to the SDG Sandbox common data models

- Birth evidence
- Marriage evidence
- Absence of a criminal record

5.4.1.3 Data models for specific evidence types

5.4.1.4 Birth Evidence


class BirthEvidence
When the multiplicity range of the property is omitted, it implies a multiplicity of 1 (exactly one).
PublicOrganisation
- identifier: Identifier [0..*]
- prefLabel: Text [1..*]
1
issuingAuthority
Birth
certifiesBirth
1
BirthEvidence
- identifier: Identifier [0..1]
- issueDate: Date
child
1
parent
0..2
issuingPlace
0..1
Child
- dateOfBirth: Date
- sex: Code
placeOfBirth
1
Location
- geographicIdentifier: URI [0..1]
- geographicName: Text [0..*]
Parent
- dateOfBirth: Date [0..1]
- sex: Code [0..1]
placeOfBirth
0..1
Person
- familyName: Text [1..*]
- givenName: Text [1..*]
- identifier: Identifier [0..*]
citizenship
0..*
Jurisdiction
- id: URI [0..1]
- name: Text [1..*]

5.4.1.4.1 Entities

5.4.1.4.1.1 Birth Evidence

Definition: Official document or data proving the Birth of a Child.

Source: Public documents forms

attribute	expected type	definition	cardinality	code list
identifier	Identifier	An unambiguous reference to the Birth Evidence.	[0..1]	N/A
issue date	Date	The date on which the Birth Evidence was issued.	[1..1]	N/A
certifies birth	Birth	Attesting in a formal way that the Birth is true.	[1..1]	N/A
issuing authority	Public Organisation	A Public Organisation with official authority in charge of issuing the Birth Evidence.	[1..1]	N/A
issuing place	Location	The Location where the Birth Evidence was issued.	[0..1]	N/A

5.4.1.4.1.2 Birth

Definition: The event indicating the moment a Child emerges from the body of another Person, i.e. start of life.

Source: Public documents forms

attribute	expected type	definition	cardinality	code list
child	Child	The Person who is born at the Birth.	[1..1]	N/A
parent	Parent	The Parent of the Child.	[0..2]	N/A

5.4.1.4.1.3 Child

Definition: A Person of any age, who is a son or daughter.

Subclass of: Person

Source: ISA² Core Person Vocabulary

attribute	expected type	definition	cardinality	code list
date of birth	Date	The day on which the Child was born.	[1..1]	N/A
place of birth	Location	The Location where the Child was born.	[1..1]	N/A
sex	Code	The chromosomal state, and reproductive organs and structures of a Person that allows them to be distinguished as female or male.	[1..1]	Human Sex

5.4.1.4.1.4 Parent

Definition: One of the two Persons who are jointly the cause of the Child's Birth, i.e. natural parent.

Subclass of: Person

Source: ISA² Core Person Vocabulary

attribute	expected type	definition	cardinality	code list
date of birth	Date	The day on which the Parent was born.	[0..1]	N/A
sex	Code	The chromosomal state, and reproductive organs and structures of a Person that allows them to be distinguished as female or male.	[0..1]	Human Sex
place of birth	Location	The Location where the Parent was born.	[0..1]	N/A

5.4.1.4.1.5 Person

Definition: An individual natural person who may be dead or alive, but not imaginary.

Source:ISA² Core Person Vocabulary

attribute	expected type	definition	cardinality	code list
identifier	Identifier	The identifier relation is used to link a Person to any formally issued Identifier for that Person.	[0..*]	N/A
given name	Text	A given name, or multiple given names, are the denominator(s) that identify an individual within a family. These are given to a Person by his or her parents at birth or may be legally recognised as 'given names' through a formal process. All given names are ordered in one field so that, for example, the given name for Johann Sebastian Bach is “Johann Sebastian”.	[1..*]	N/A
family name	Text	A family name is usually shared by members of a family. This attribute also carries prefixes or suffixes which are part of the family name, e.g. “de Boer”, “van de Putte”, “von und zu Orlow”. Multiple family names, such as are commonly found in Hispanic countries, are recorded in the single family name field so that, for example, Miguel de Cervantes Saavedra's family name would be recorded as "de Cervantes Saavedra".	[1..*]	N/A
citizenship	Jurisdiction	The citizenship relationship links a Person to a Jurisdiction that has conferred citizenship rights on the individual such as the right to vote, to receive certain protection from the community or the issuance of a passport. Multiple citizenships are recorded as multiple instances of the citizenship relationship.	[0..*]	N/A

5.4.1.4.1.6 Jurisdiction

Definition: The authority that an official organisation has, to make legal decisions about somebody/something.

Source: ISA² Core Person Vocabulary

attribute	expected type	definition	cardinality	code list
name	Text	The name is simply a string that identifies the Jurisdiction, typically a country, with or without a language tag.	[1..*]	N/A
id	URI	The value for the id property is a URI for that Jurisdiction.	[0..1]	Country *Addition of stateless concept needed*

5.4.1.4.1.7 Public Organisation

Definition: Any organisation that is defined as being part of the public sector by a legal framework at any level.

Source: ISA² Core Public Organisation Vocabulary

attribute	expected type	definition	cardinality	code list
preferred label	Text	As defined in the ORG Ontology, a preferred label is used to provide the primary, legally recognised name of the organisation. An organisation may only have one such name in any given language. Primary names may be provided in multiple languages with multiple instances of the preferred label property.	[1..*]	N/A
identifier	Identifier	Many organisations are referred to by an acronym or some other identifier. For example, among the EU institutions, the ECB is the identifier for the European Central Bank, OLAF for the European Anti-Fraud Office, and so on. These are formally recognised by the European Commission which provides a list of such acronyms. Analogous lists should be used in other contexts.	[0..*]	N/A

5.4.1.4.1.8 Location

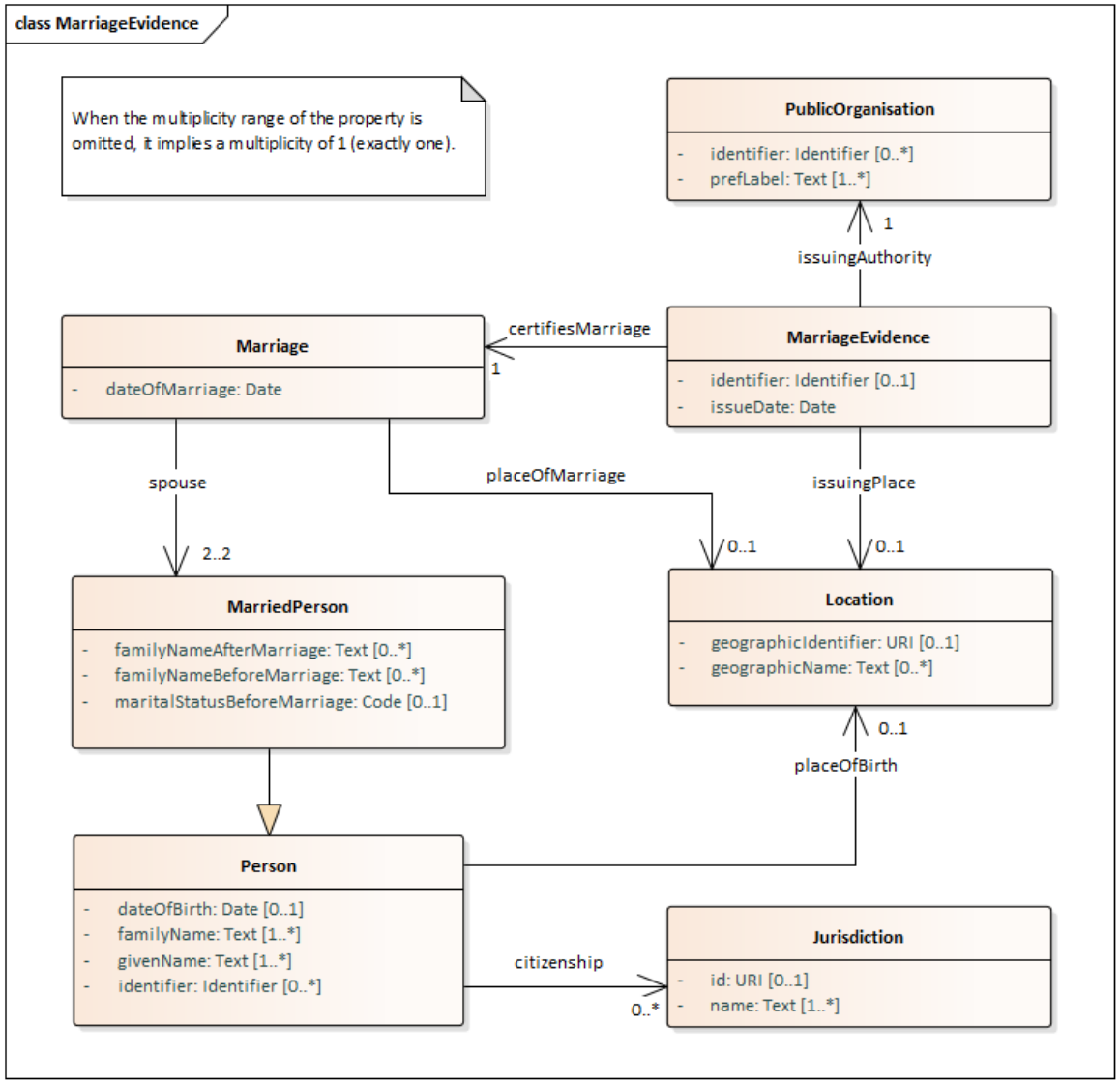
Definition: An identifiable geographic place or named place.

Source: ISA² Core Location Vocabulary

Given that both attributes are optional, at least one of the attributes must be provided.

attribute	expected type	definition	cardinality	code list
geographic name	Text	A geographic name is a proper noun applied to a spatial object. The INSPIRE Data Specification on Geographical Names [INGN] provides a detailed model for describing a 'named place', including methods for providing multiple names in multiple scripts.	[0..*]	N/A
geographic identifier	URI	A URI that identifies the Location.	[0..1]	GeoNames

5.4.1.5 Marriage Evidence


class MarriageEvidence
When the multiplicity range of the property is omitted, it implies a multiplicity of 1 (exactly one).
PublicOrganisation
- identifier: Identifier [0..*]
- prefLabel: Text [1..*]
1
issuingAuthority
Marriage
- dateOfMarriage: Date
certifiesMarriage
1
MarriageEvidence
- identifier: Identifier [0..1]
- issueDate: Date
spouse
2..2
placeOfMarriage
0..1
issuingPlace
0..1
MarriedPerson
- familyNameAfterMarriage: Text [0..*]
- familyNameBeforeMarriage: Text [0..*]
- maritalStatusBeforeMarriage: Code [0..1]
Location
- geographicIdentifier: URI [0..1]
- geographicName: Text [0..*]
0..1
placeOfBirth
Person
- dateOfBirth: Date [0..1]
- familyName: Text [1..*]
- givenName: Text [1..*]
- identifier: Identifier [0..*]
citizenship
0..*
Jurisdiction
- id: URI [0..1]
- name: Text [1..*]

5.4.1.5.1 Entities

5.4.1.5.1.1 Marriage Evidence

Definition: Official document or data proving the Marriage of two Persons.

Source: Public documents forms

attribute	expected type	definition	cardinality	code list
identifier	Identifier	An unambiguous reference to the Marriage Evidence.	[0..1]	N/A
issue date	Date	The date on which the Marriage Evidence was issued.	[1..1]	N/A
certifies marriage	Marriage	Attesting in a formal way that the Marriage is true.	[1..1]	N/A
issuing authority	Public Organisation	A Public Organisation with official authority in charge of issuing the Marriage Evidence.	[1..1]	N/A
issuing place	Location	The Location where the Marriage Evidence was issued.	[0..1]	N/A

5.4.1.5.1.2 Marriage

Definition: A legally accepted relationship between two Persons in which they live together.

Source: Public documents forms

attribute	expected type	definition	cardinality	code list
date of marriage	Date	The date on which the Marriage took place.	[1..1]	N/A
place of marriage	Location	The Location where the Marriage took place.	[0..1]	N/A
spouse	Married Person	The Person who was married.	[2..2]	N/A

5.4.1.5.1.3 Married Person

Definition: A Person who has entered into a Marriage.

Source: Public documents forms

Subclass of: Person

attribute	expected type	definition	cardinality	code list
family name after marriage	Text	This property contains the family name after the Marriage of the Person.	[0..*]	N/A
family name before marriage	Text	This property contains the family name before the Marriage of the Person.	[0..*]	N/A
marital status before marriage	Code	Situation with regard to whether a Person was single, married, separated, divorced or widowed.	[0..1]	Marital Status *Discussion ongoing to add terms to the code list*

5.4.1.5.1.4 Person

Definition: An individual natural person who may be dead or alive, but not imaginary.

Source: ISA² Core Person Vocabulary

attribute	expected type	definition	cardinality	code list
given name	Text	A given name, or multiple given names, are the denominator(s) that identify an individual within a family. These are given to a Person by his or her parents at birth or may be legally recognised as 'given names' through a formal process. All given names are ordered in one field so that, for example, the given name for Johann Sebastian Bach is 'Johann Sebastian'.	[1..*]	N/A
family name	Text	A family name is usually shared by members of a family. This attribute also carries prefixes or suffixes which are part of the family name, e.g. "de Boer", "van de Putte", "von und zu Orlow". Multiple family names, such as are	[1..*]	N/A

attribute	expected type	definition	cardinality	code list
		commonly found in Hispanic countries, are recorded in the single family name field so that, for example, Miguel de Cervantes Saavedra's Family Name would be recorded as "de Cervantes Saavedra".		
date of birth	Date	The day on which the Person was born.	[0..1]	N/A
identifier	Identifier	The identifier relation is used to link a Person to any formally issued Identifier for that Person.	[0..*]	N/A
place of birth	Location	The Location where the Person was born.	[0..1]	N/A
citizenship	Jurisdiction	The citizenship relationship links a Person to a Jurisdiction that has conferred citizenship rights on the individual such as the right to vote, to receive certain protection from the community or the issuance of a passport.	[0..*]	N/A

5.4.1.5.1.5 Jurisdiction

Definition: The authority that an official organisation has, to make legal decisions about somebody/something.

Source: ISA² Core Person Vocabulary

attribute	expected type	definition	cardinality	code list
name	Text	The name is simply a string that identifies the Jurisdiction, typically a country, with or without a language tag.	[1..*]	N/A
id	URI	The value for the id property is a URI for that Jurisdiction.	[0..1]	Country *Addition of stateless concept needed*

5.4.1.5.1.6 Public Organisation

Definition: Any organisation that is defined as being part of the public sector by a legal framework at any level.

Source: ISA² Core Public Organisation Vocabulary

attribute	expected type	definition	cardinality	code list
preferred label	Text	As defined in the ORG Ontology, a preferred label is used to provide the primary, legally recognised name of the organisation. An organisation may only have one such name in any given language. Primary names may be provided in multiple languages with multiple instances of the preferred label property.	[1..*]	N/A
identifier	Identifier	Many organisations are referred to by an acronym or some other identifier. For example, among the EU institutions, the ECB is the identifier for the European Central Bank, OLAF for the European Anti-Fraud Office, and so on. These are formally recognised by the European Commission which provides a list of such acronyms. Analogous lists should be used in other contexts.	[0..*]	N/A

5.4.1.5.1.7 Location

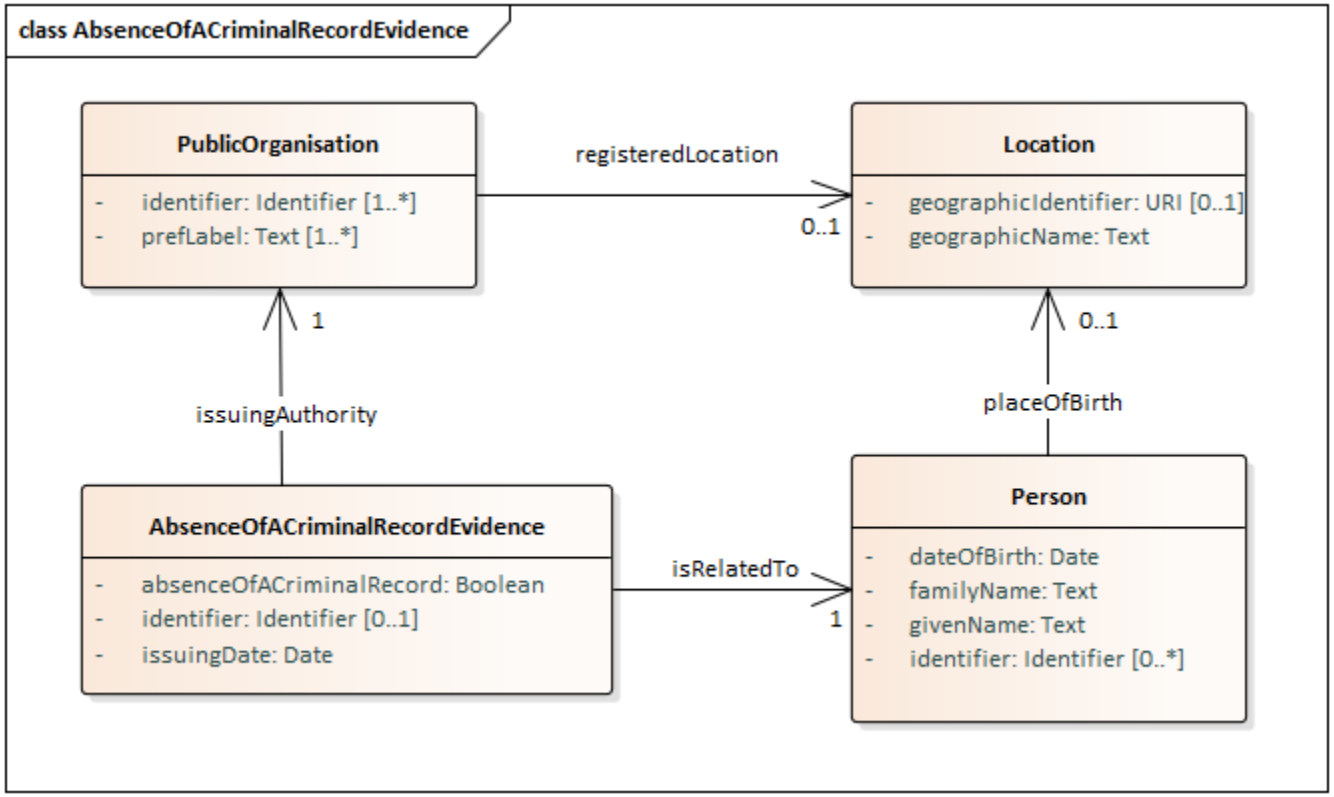
Definition: An identifiable geographic place or named place.

Source: ISA² Core Location Vocabulary

Given that both attributes are optional, at least one of the attributes must be provided.

attribute	expected type	definition	cardinality	code list
geographic name	Text	A geographic name is a proper noun applied to a spatial object. The INSPIRE Data Specification on Geographical Names [INGN] provides a detailed model for describing a 'named place', including methods for providing multiple names in multiple scripts.	[0..*]	N/A
geographic identifier	URI	A URI that identifies the Location.	[0..1]	GeoNames

5.4.1.6 Absence of a Criminal Record Evidence



5.4.1.6.1 Entities

5.4.1.6.1.1 Absence of a criminal record

Definition: Official document attesting that there is no known record of a Person having been arrested in the past for committing a crime.

attribute	expected type	definition	cardinality	code list
absence of a criminal record	Boolean	An indicator that declares the (non)existence of a criminal record for a Person.	[1..1]	N/A
identifier	Identifier	An unambiguous reference to the Absence of a Criminal Record Evidence.	[0..1]	N/A
issuing date	Date	The date on which the Absence of a Criminal Record Evidence was issued.	[1..1]	N/A
is related to	Person	The Person to whom the Absence of a Criminal Record applies.	[1..1]	N/A
issuing authority	Public Organisation	A Public Organisation with official authority in charge of issuing the Absence of a Criminal Record Evidence.	[1..1]	N/A

5.4.1.6.1.2 Person

Definition: An individual person who may be dead or alive, but not imaginary.

attribute	expected type	definition	cardinality	code list
identifier	Identifier	The identifier relation is used to link a Person to any formally issued Identifier for that Person.	[0..*]	N/A
given name	Text	A given name, or multiple given names, are the denominator(s) that identify an individual within a family. These are given to a Person by his or her parents at birth or may be legally recognised as 'given names' through a formal process. All given names are ordered in one field so that, for example, the given name for Johan Sebastian Bach is 'Johan Sebastian'.	[1..1]	N/A
family name	Text	A family name is usually shared by members of a family. This attribute also carries prefixes or suffixes which are part of the family name, e.g. "de Boer", "van de Putte", "von und zu Orlow". Multiple family names, such as are commonly found in Hispanic countries, are recorded in the single family name field so that, for example, Miguel de Cervantes Saavedra's Family Name would be recorded as "de Cervantes Saavedra".	[1..1]	N/A
date of birth	Date	A date that specifies the birth date of a Person.	[1..1]	N/A

attribute	expected type	definition	cardinality	code list
place of birth	Location	The Location where a Person was born.	[0..1]	N/A

5.4.1.6.1.3 Public Organisation

Definition: Any organisation that is defined as being part of the public sector by a legal framework at any level.

attribute	expected type	definition	cardinality	code list
preferred label	Text	As defined in the ORG Ontology, a preferred label is used to provide the primary, legally recognised name of the organisation. An organisation may only have one such name in any given language. Primary names may be provided in multiple languages with multiple instances of the preferred label property.	[1..*]	N/A
identifier	Identifier	Many organisations are referred to by an acronym or some other identifier. For example, among the EU institutions, the ECB is the identifier for the European Central Bank, OLAF for the European Anti-Fraud Office, and so on. These are formally recognised by the European Commission which provides a list of such acronyms. Analogous lists should be used in other contexts.	[1..*]	N/A
registered location	Location	The registered location of the Public Organisation.	[0..1]	N/A

5.4.1.6.1.4 Location

Definition: A spatial region or named place.

attribute	expected type	definition	cardinality	code list
geographic name	Text	A geographic name is a proper noun applied to a spatial object. The INSPIRE Data Specification on Geographical Names [INGN] provides a detailed model for describing a 'named place', including methods for providing multiple names in multiple scripts.	[1..1]	N/A

attribute	expected type	definition	cardinality	code list
geographic identifier	URI	A URI that identifies the location.	[0..1]	N/A

5.4.2 Public Documents Code Lists - June 2022

Code lists give control over which values can be encoded for specific properties of the various data models. The constraints imposed by code lists facilitate semantic interoperability and help to scale up the automated processing and exchange of evidences.

5.4.2.1 Code lists for specific evidence types

During the development of data models, the editors have identified together with experts from Member States existing code lists that can be reused as part of the common data models. They have also identified the properties for which code lists should be created. The table below gives an overview of both the existing and the potential candidates for code lists, categorising them by scope, status and described property. The creation of new code lists and the updates of existing ones will be set up in the fourth quarter of 2021.

By default, code lists should follow the SKOS principles, be published with persistent identifiers and be managed by an authoritative organisation, ideally the Publications Office.

Member States have the possibility to either make use of the code lists directly or to do a mapping exercise with their national code lists. In the latter case, SKOS, which stands for Simple Knowledge Organization System, can be used. It is a W3C recommendation for sharing and linking knowledge organisation systems. The SKOS mapping properties are skos:closeMatch, skos:exactMatch, skos:broadMatch, skos:narrowMatch and skos:relatedMatch. These properties are used to express the nature of the alignment between concepts from different concept schemes.

Scope	Code list	Status*	Described property	Comment
Birth evidence	Human Sex	Existing	Sex	Missing non-binary genders
Birth evidence, marriage evidence	GeoNames	Existing	Geographic identifier	
Marriage evidence	Marital status	Existing	Marital status before marriage	Missing terms (see GitHub)

Birth Evidence	Country	Existing	Jurisdiction identifier	Addition of stateless concept needed

*In the status column, there are two values, *'existing'* or *'to create'*. In the first instance, there is an existing code list that is proposed for reuse. In the second instance, there is - to our knowledge - no existing code list to be reused and therefore a new one needs to be created. It must be noted that all code lists have been proposed, but they haven't been validated by the Member States.

6 Chapter 6: OOTS Guidance & UX Recommendations - June 2022

6.1 Summary

This chapter provides two things:

1. The Once-Only Guidance document provides a high-level overview of how the Once-Only Technical System (OOTS) of the Single Digital Gateway (SDG) works.
2. The first set of UX recommendations that were developed as part of the OOTS UX Lab.

The guidance document is a PowerPoint presentation and can be used to introduce the OOTS to stakeholders.

The first set of UX recommendations are based on three rounds of user testing and provide a foundation for more UX work going forward.

- See the OOTS Guidance Document (online only)
- See the OOTS UX Recommendations

6.2 OOTS Guidance document

- See the OOTS Guidance Document (online only)

6.3 OOTS UX Recommendations

OOTS UX Recommendations

Dear Colleagues,

This first release of the UX Recommendations is based on the work the EC team has done over the last couple of months in our newly established OOTS UX Lab. The recommendations are just a starting point. We hope Member States will share their challenges and insights so we can incorporate them into the next iterations of the recommendations. The aim is to deliver a great user experience of the OOTS, to ensure the seamless uptake by European citizens, businesses, government authorities and institutions. So far we have run three rounds of user testing and the insights have allowed us to improve our prototype and define the first set of recommendations to overcome some of the key user pain points.

Below is a simplified user journey, illustrated through the example of procedure 4 (Submitting an initial application for admission to public tertiary education institution).

0. Discover the OOTS — Sophie wants to enrol for a master's degree abroad in the EU. She discovers on the application portal of the university, that she can complete the procedure online with the help of OOTS.

1. Authenticate with eID — Sophie is asked to authenticate herself; she selects the option to sign in with her eID.

2. Locate evidence — Once signed in, Sophie chooses to provide the necessary document (a bachelor's degree issued by an internationally recognised university) by using OOTS. She needs to specify the location where the bachelor's degree was issued.

3. Request evidence — After locating the evidence, Sophie confirms she wants to request the evidence.

4. Redirect to evidence — After her request, Sophie needs to authenticate to the provider to preview the document.

5. Preview evidence — After re-authenticating, she is able to preview the document and select the language she needs the document in.

6. Evidence response — The provider sends a response to the requester with the evidence and Sophie is redirected back to the application portal.

7. Submit evidence — In the application portal, Sophie sees that the document has been received and completes any remaining steps of the procedure before finally submitting her application.

Each of these phases needs to be considered to deliver a great end-to-end experience.

This report is just the first release, more variations of user flows, scenarios and error messages still need to be designed and tested. Next, we are planning to look at:

- Helping users who are retrieving multiple pieces of evidence from the *same* Member State
- Helping users who are retrieving multiple pieces of evidence from *different* Member States
- Helping users preview structured data
- Developing error messages that can be reused

6.3.1 Get involved

We know that the broad scope of procedures, procedure portals and MS implementations of the OOTS will mean that some of the UX recommendations will not necessarily be applicable in all cases. We also know that there will many common UX challenges across the Member States. We hope the UX Recommendations can become a hub where UX teams can share the challenges they see and solutions they have tested so others can benefit from them. In September, we will set up a dedicated meeting to discuss how we can connect UX teams working on once-only, but in the meantime, please:

1. Review the first set of recommendations

2. Feel free to share the pages with relevant teams in your Member State
3. For now, please add any comments, questions or mention any additional UX challenges you see via the MS feedback space. By September, we will ensure we have a space for regular online collaboration.

Go to the UX recommendations

6.3.2 discover OOTS

Helping users...

discover OOTS

6.3.2.1 P1.1 | Helping users understand that they do not need to have a copy of the required evidence as it can be retrieved from the issuer

Pain point:
If citizens are not aware that they can ask the authority to retrieve the evidence from the issuer, they might not initiate the procedure if they do not have a copy of the evidence themselves.

User Testing Quote:

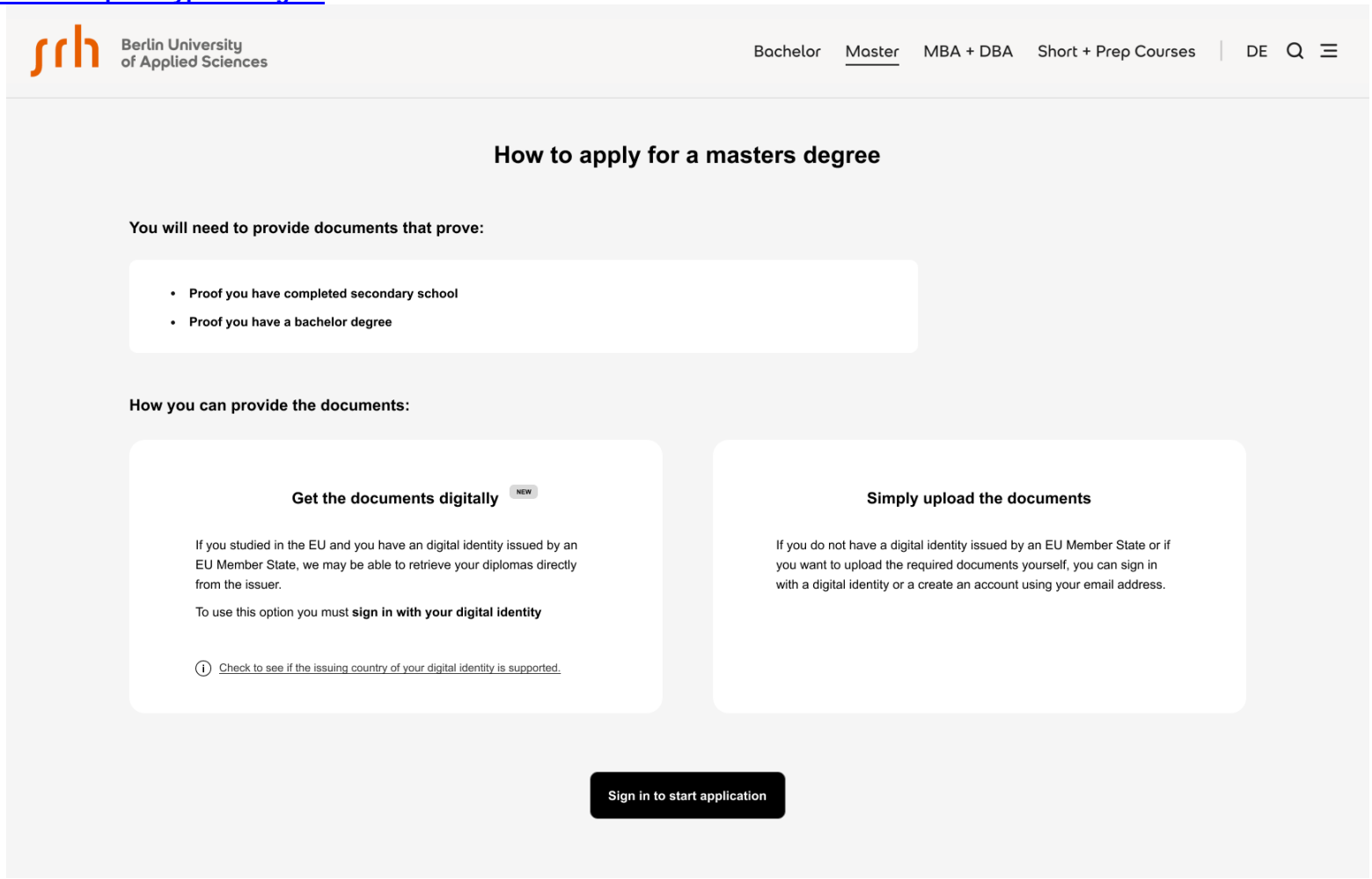
> *"It wasn't clear to me at the beginning that I could get my documents automatically online, I was surprised this was possible. I thought I would need to contact my previous universities to get my diplomas before starting the procedure."*

Recommendation:
Before a user initiates a procedure, explain which documents are required and which of the documents the authority may be able to retrieve, at the user's request, from the issuer in another Member State.

Idea:
Some users may want to know the legal basis for the data exchange and how the exchange takes place. Instead of each procedure portal providing a web page with the information, the EC UX team thought it could be an idea to create a single page hosted and maintained by the EC that procedure portals could link to. MS feedback would be welcome on this point.

6.3.2.2 Wireframe

Access the clickable prototype on Figma



6.3.3 authenticate

Helping users...

authenticate

6.3.3.1 P2.1 | Helping users authenticate with a notified eID means

Pain point:
If an online procedure portal lets users sign in with a username and password and users choose to do so, they won't be able to benefit from the once-only technical system.

User Testing Quote:
> *"How do I know which sign-in method I should use?"*

Recommendation:
Explain to users the consequences of choosing to authenticate with one or another method. If users choose to authenticate with a notified eID, they will be able to ask the authority to retrieve an evidence on their behalf. Whereas if the user signs-in with a username and password they will have to upload the documents themselves. Also, ensure the eIDAS authentication option is clearly visible to users.

6.3.3.2 P2.2 | Helping users understand that they can retrieve evidence using the OOTS

Pain point:
Users may have an eID from a non-notified eID scheme. We want to ensure these users know that if they use that eID, they will have to provide the documents themselves as they won't be able to retrieve them using the OOTS.

User Testing Quote:
> *"How do I know if the eID I have will allow me to get my document through the system?"*

Idea:
Should we EC create and host a web page with an overview of notified eID schemes that procedure portals can link to? That way a user can check if their eID scheme allows them to retrieve evidence using the OOTS before they initiate the procedure.

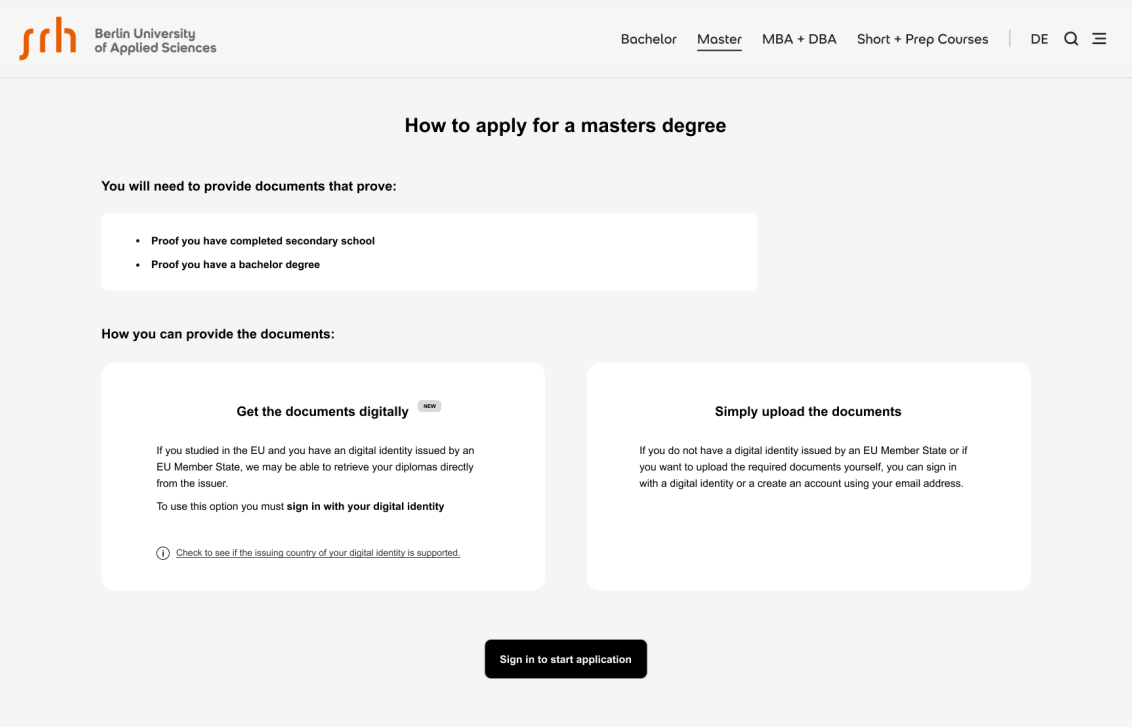
6.3.3.3 P2.3 | Helping users re-authenticate if they choose to authenticate with non-eIDAS notified eID means

Pain point:
Users who have a notified eID means may still choose to authenticate with a username and password or a non-notified eID means.

Recommendation:

Give users the chance to re-authenticate with a notified eID means so they can retrieve evidence using the OOTS.

[Access the clickable prototype on Figma]



6.3.4 locate evidence

Helping users...

locate evidence

6.3.4.1 P3.1 | Helping users to provide their evidence in the right language

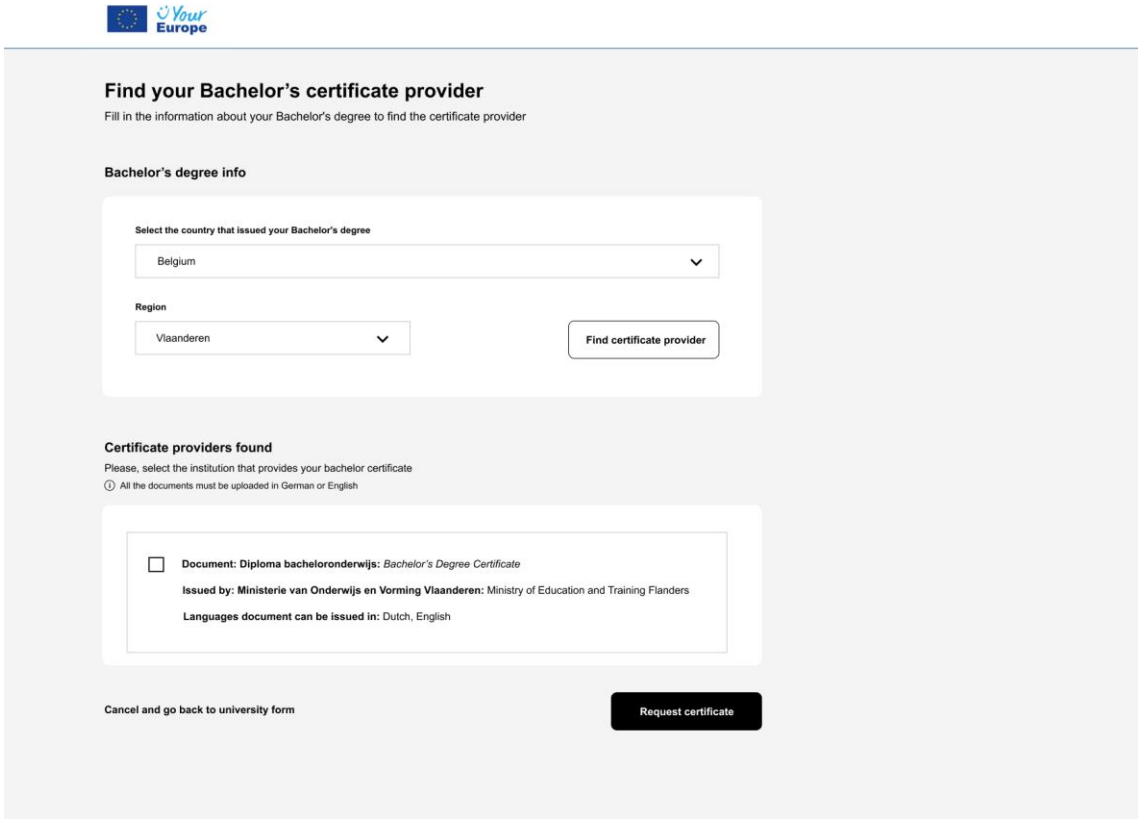
Pain point:
If the user retrieves a piece of evidence from the provider using the OOTS, but the evidence is in a language the evidence requester cannot process, the user may be frustrated as they will have gone through the steps needed to retrieve their evidence but will still need to get the evidence officially translated and upload it themselves.

Recommendation:

1. The procedure portal should list the languages that they can accept for a piece of evidence
2. Providers should include the languages the evidence can be issued in, so it can be displayed to the user at this stage in the journey.

Idea
Could the portal warn the user if there is no match between the required language and the available language(s)?

[Access the clickable prototype on Figma]



6.3.5 request evidence

Helping users...

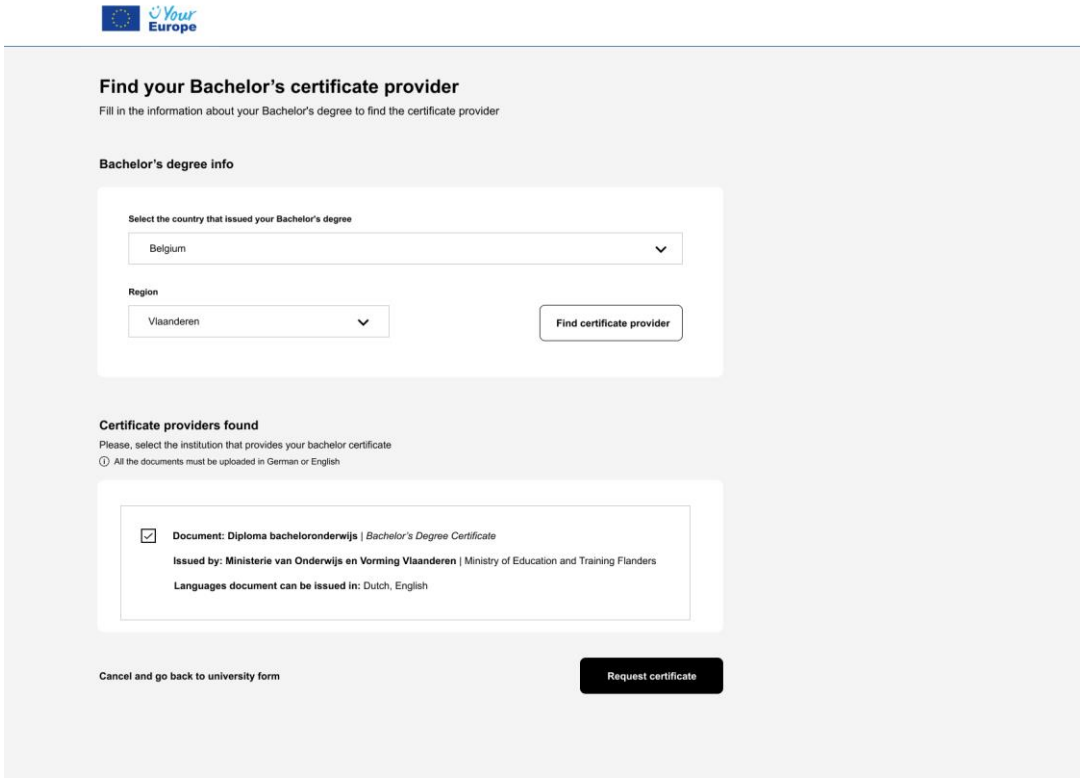
request evidence

6.3.5.1 P4.1 | Helping users request their evidence

Pain point:
Users need enough information to make an informed request for evidence.

Recommendation:
Procedure portals should provide the name of the evidence provider and the evidence type so that users can make an informed explicit request to exchange evidence using the Once-Only Technical System.

Access the clickable prototype on Figma



6.3.6 redirect

Helping users...

redirect

6.3.6.1 P5 | Helping users navigate across multiple interfaces

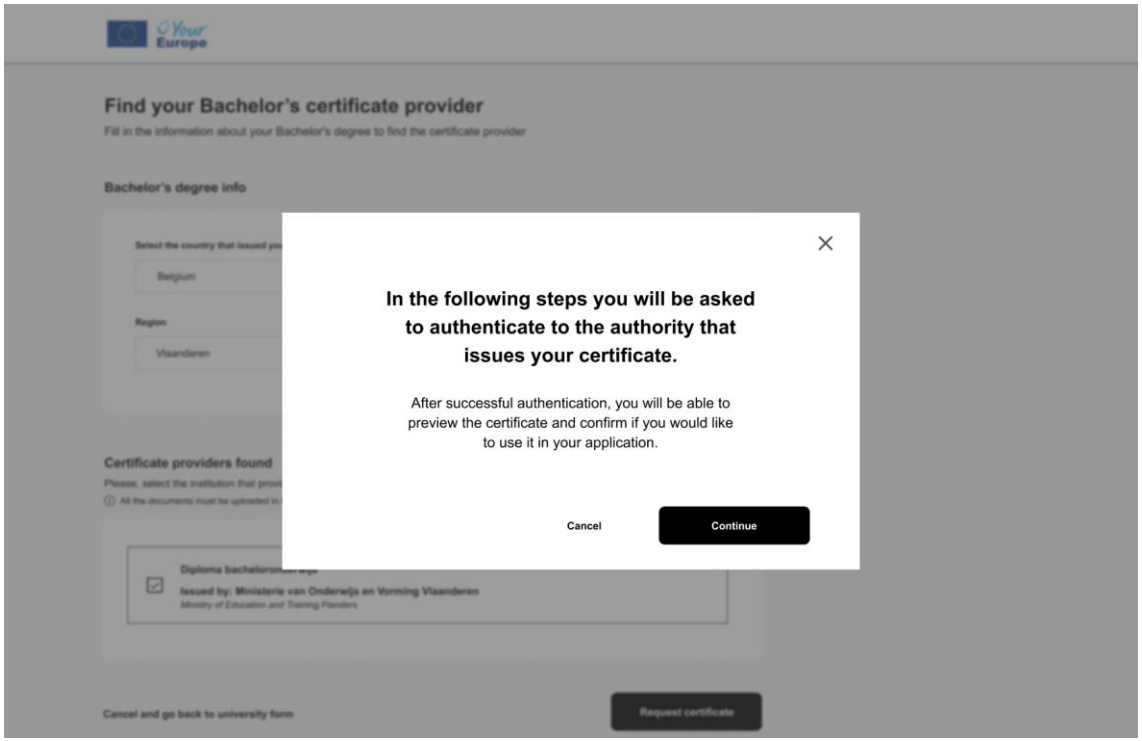
Pain point:
To retrieve their evidence users will be redirected from the procedure portal to a preview space in another Member State via an authentication service and then back to the procedure portal. As these steps in the journey are provided by different stakeholders, the interfaces will all look and feel different and users may feel disorientated.

User Testing Quotes:

> - *“It feels weird to do it all over again, this re-authentication process."*
> - *“The step seems weird, why do I have to re-authenticate again? Now that you have explained why, I get it, but it’s still kind of annoying."*

Recommendation:
Explain to the user that they will be redirected to the provider side and will need to authenticate themselves again.

Access the clickable prototype on Figma



6.3.7 Preview

Helping users...

preview

Coming soon.

6.3.8 evidence response

Helping users...

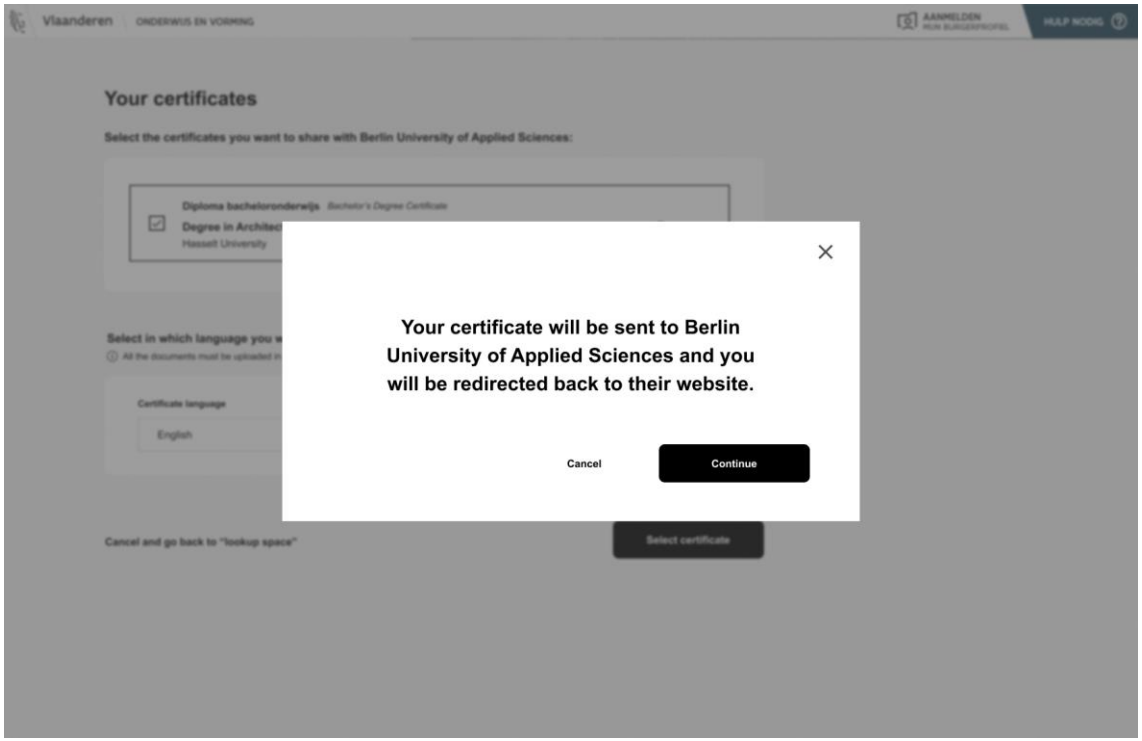
evidence response

6.3.8.1 P5 | Helping users navigate across multiple interfaces

Pain point:
As we saw in the redirect step, users will be redirected from the procedure portal to a preview space in another Member State via an authentication service and then back to the procedure portal. As these steps in the journey are provided by different stakeholders, the interfaces will all look and feel different and users may feel disorientated.

Recommendation:
Explain to users that they will be redirected back to the procedure portal and confirm that their evidence will be sent to the evidence requester.

Access the clickable prototype on Figma



6.3.9 submit

Helping users...

submit

6.3.9.1 P8 - Helping users check their information before submission

Pain point:
Before submitting the procedure, users tend to do a final check of the information they are going to submit.

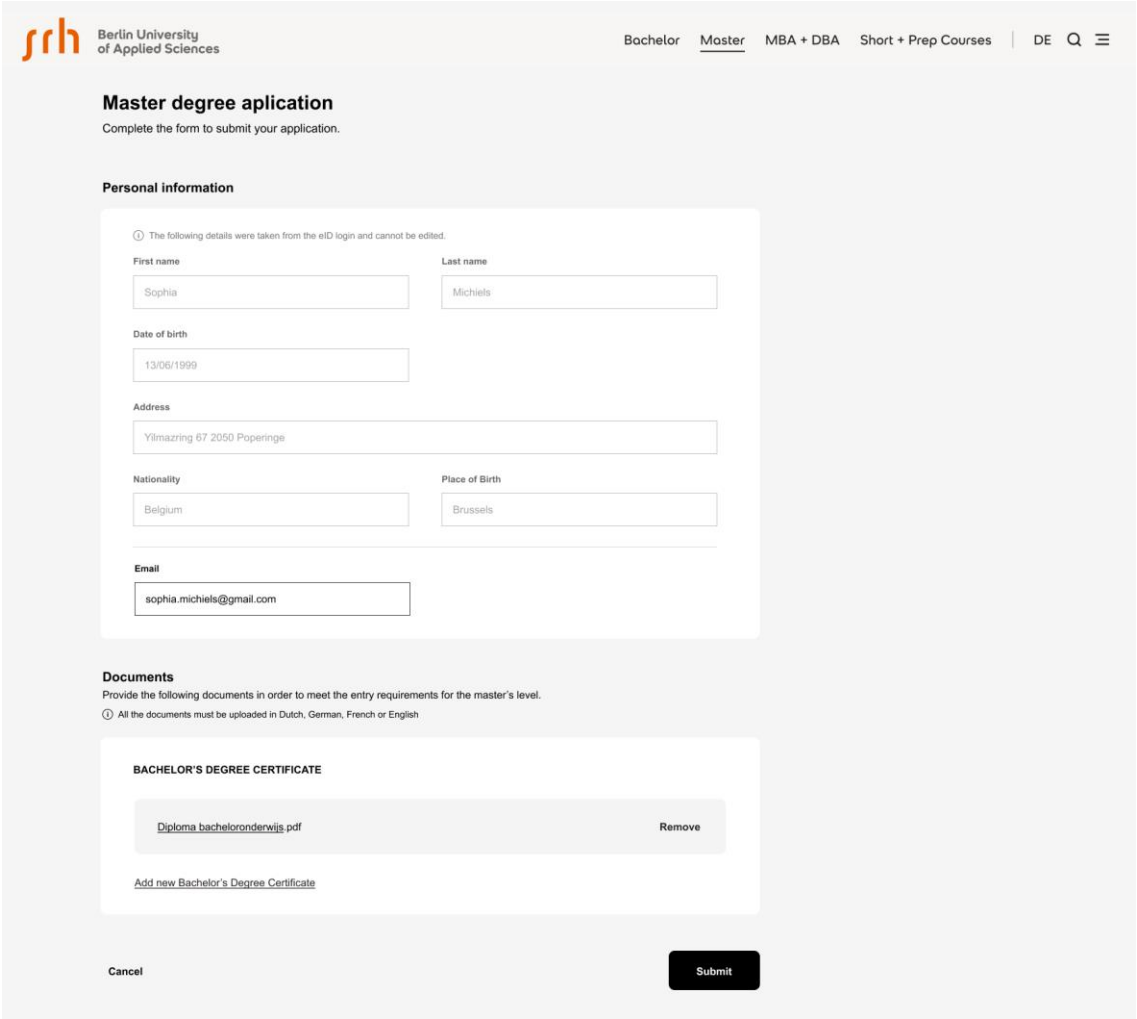
User Testing Quote:

> *"I would like to be able to check the document I am about to submit."*

Recommendation:

Even if users had the chance to preview their evidence in the preview space, give users the opportunity to preview the evidence in the procedure portal before they submit their form. This way users can feel secure that they are submitting the right information.

Access the clickable prototype on Figma


Berlin University of Applied Sciences
Bachelor
Master
MBA + DBA
Short + Prep Courses
DE
Master degree aplication
Complete the form to submit your application.
Personal information
The following details were taken from the eID login and cannot be edited.
First name
Sophia
Last name
Michiels
Date of birth
13/06/1999
Address
Yilmazring 67 2050 Poperinge
Nationality
Belgium
Place of Birth
Brussels
Email
sophia.michiels@gmail.com
Documents
Provide the following documents in order to meet the entry requirements for the master's level.
All the documents must be uploaded in Dutch, German, French or English
BACHELOR'S DEGREE CERTIFICATE
Diploma bacheloronderwijs.pdf
Remove
Add new Bachelor's Degree Certificate
Cancel
Submit