



Digital Identity and Identification in the EU

The way to trusted Assertions

Dietmar Gattwinkel
European Commission
eGovernment & Trust

eIDAS: boosting trust & supporting businesses!

Strengthen EU Single Market by boosting **TRUST** and **CONVENIENCE** in **secure** and **seamless** cross-border electronic transactions

Provide a consistent set of rules throughout the EU

Chapter II

Mutual recognition of e-identification means

Chapter III

Electronic trust services

Chapter IV



Electronic Documents



17.09.2014
Entry into force of the eIDAS Regulation

29.09.2015
Voluntary cross-border recognition

29.09.2018
Mandatory cross-border recognition



eSignature Directive rules

1.07.2016
Date of application of eIDAS rules for trust services

What is a verifiable assertion?

Person A

to employer Y

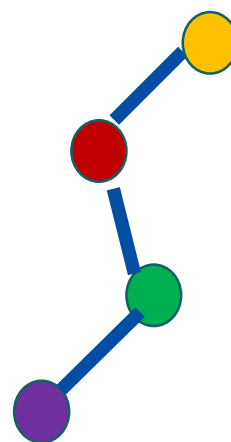
that they hold a degree in Z

from University X

claims

What is a verifiable assertion?

User
to Receiver
Assertion
Issuer



claim

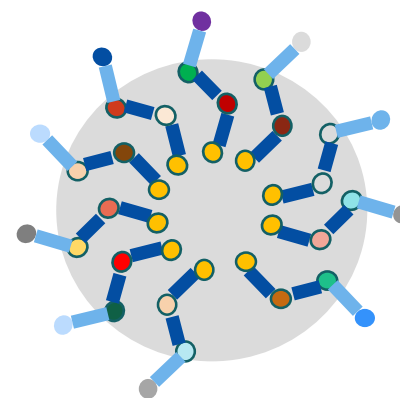
Identity is a collection of assertions

Users

Hold

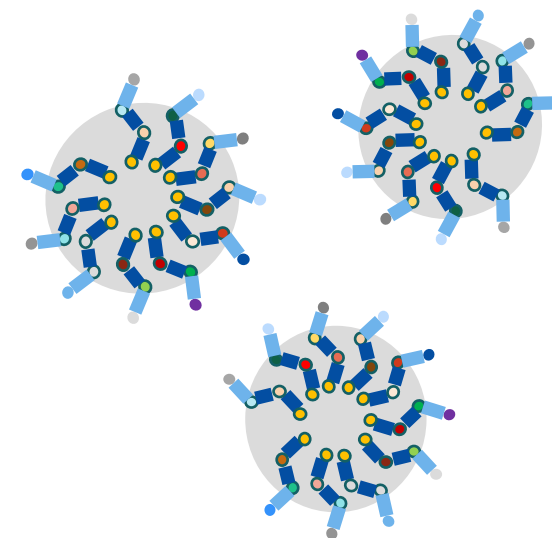
Multiple

claims



and

identities



Self-Sovereign Identity (SSI) main perceived benefits

- 🔒 **SSI allows the user to decide which identity data to share**, with whom, and with which limits and constraints for third parties.
- 🔒 As identity information, and specially credentials are stored in a way that **reduces the risk of massive identity theft**.
- 🔒 The SSI “Identity Provider” (the issuer) does not intervene in the authentication process, and has no information about the user activity, **reducing the “big brother” risk and GDPR compliance costs**.
- 🔒 **The base identity (the Decentralized ID or ID) can only be suspended or revoked by the user**, ending with “digital feudalism” business models, aligning identity management with GDPR principles.
- 🔒 **Technological and infrastructure capabilities of the identity provider** (resilience, continuity, capacity, security...): the substitution of the authentication node by a DLT allows to transfer the risk of the single point to a network, as long as it offers guarantees.
- 🔒 **Financial and liability** aspects: with DLT there may be a financial model in which the relying parties bear the cost of authentication, without the need to establish complex legal relationships.

Identification of user

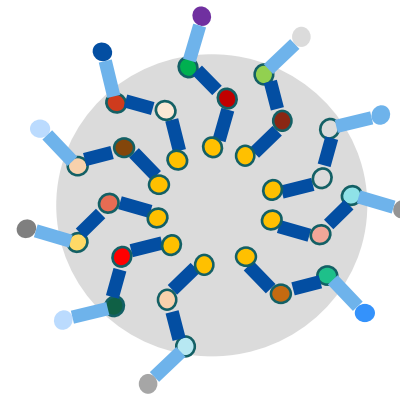
Receivers

May

Request

User

Identification



The need for verified identities

- Three types of interactions in the digital world
 - Fully anonymous interaction
 - Anonymous identity, but verifiable under certain conditions
 - **Fully disclosed real identity** -> attributes allowing identifying uniquely the person
- Service providers / relying parties may impose requirements on the type of interaction allowed
- Users should be able to decide

The need for verified identities

- DLT Self-Sovereign Identity (SSI) should, by design, support the three types of interactions
- **The trustworthiness of digital credentials is rooted on the authority of the issuer**
 - **Verifying the identity of the issuer is key**
- Under SSI, the trust on the actual identities of the parties is built out of the system
 - There is no binding of digital identifiers to real-world entities
- **eIDAS can provide the trust framework** for this binding

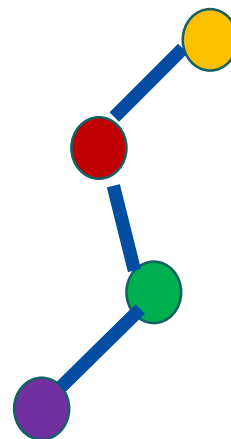
What is a verifiable assertion?

Receiver may

request

Issuer

Identification

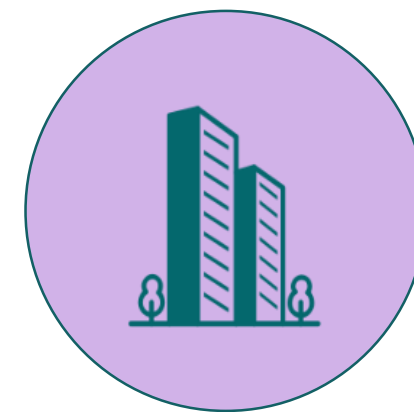
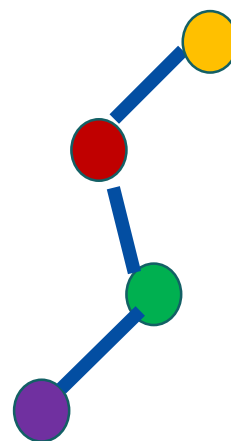


What is a verifiable assertion?

*User may
request*

Receiver

Identification



A first step

Linking assertions with eIDAS eID

eIDAS: Trust services

Horizontal principles

Liability

International
aspects

Supervision

Security
requirements

Data protection

Trusted lists

Qualified services

Prior authorisation

EU trust mark

Electronic signatures, including validation and preservation services

Electronic seals, including validation and preservation services

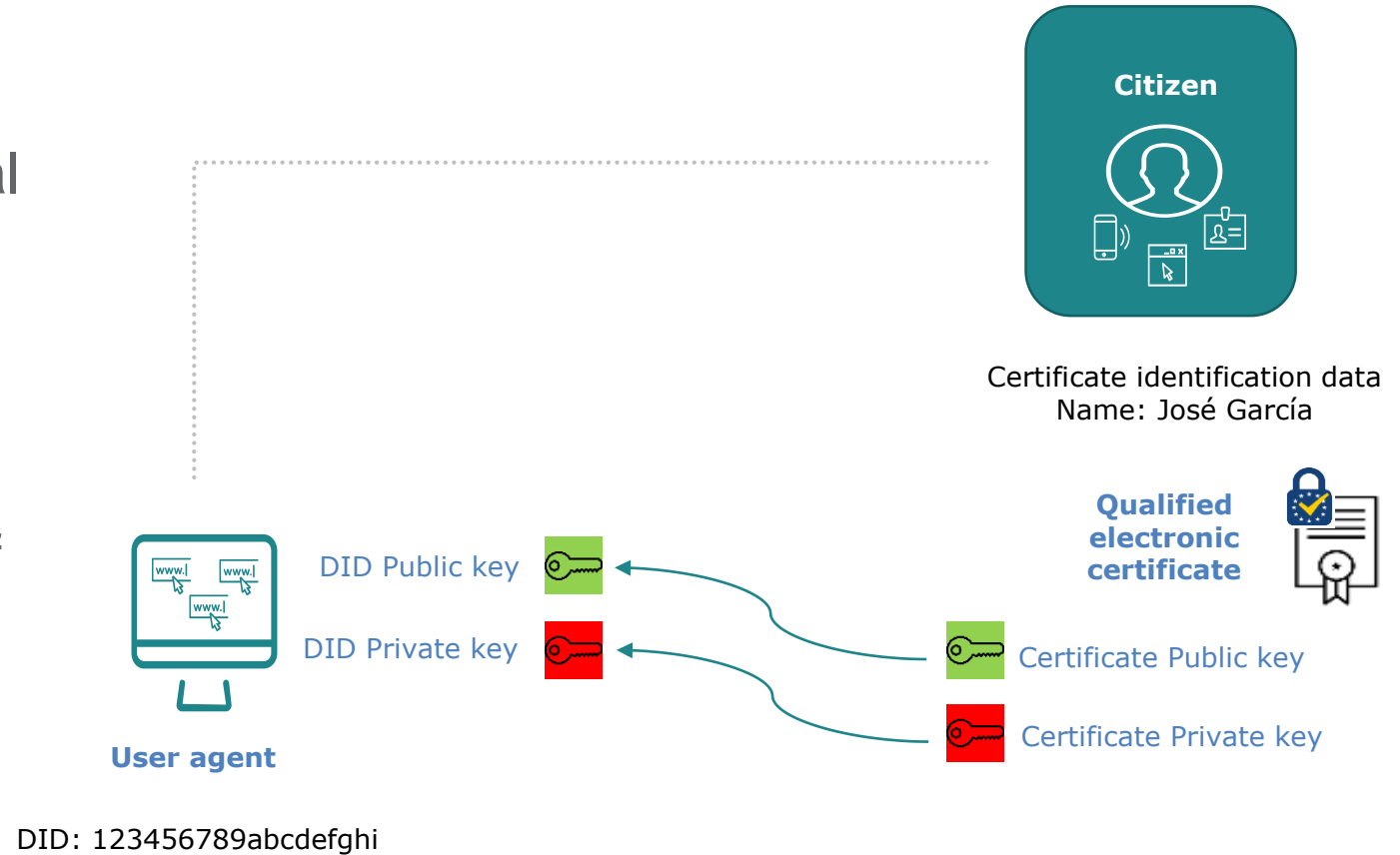
Time stamping

Electronic registered delivery service

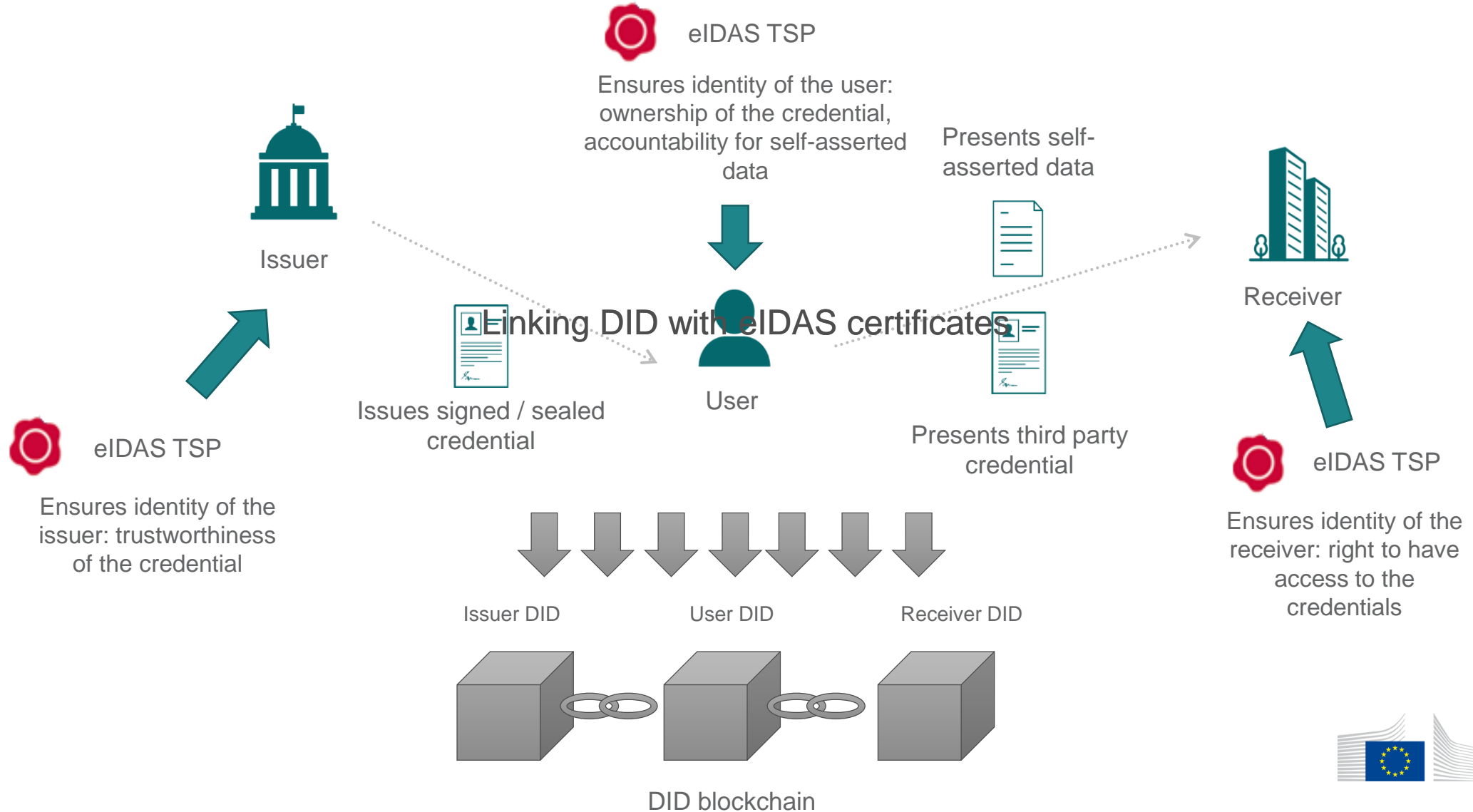
Website authentication

Linking DID with eIDAS certificates

- Increased legal certainty
- Advanced signature / seal produced with a qualified certificate
- Verifiable by a third party
 - Checking the validity of the certificate



How eIDAS Regulation is relevant to blockchain: Blockchain for “identity”



SSI eIDAS Bridge – a video



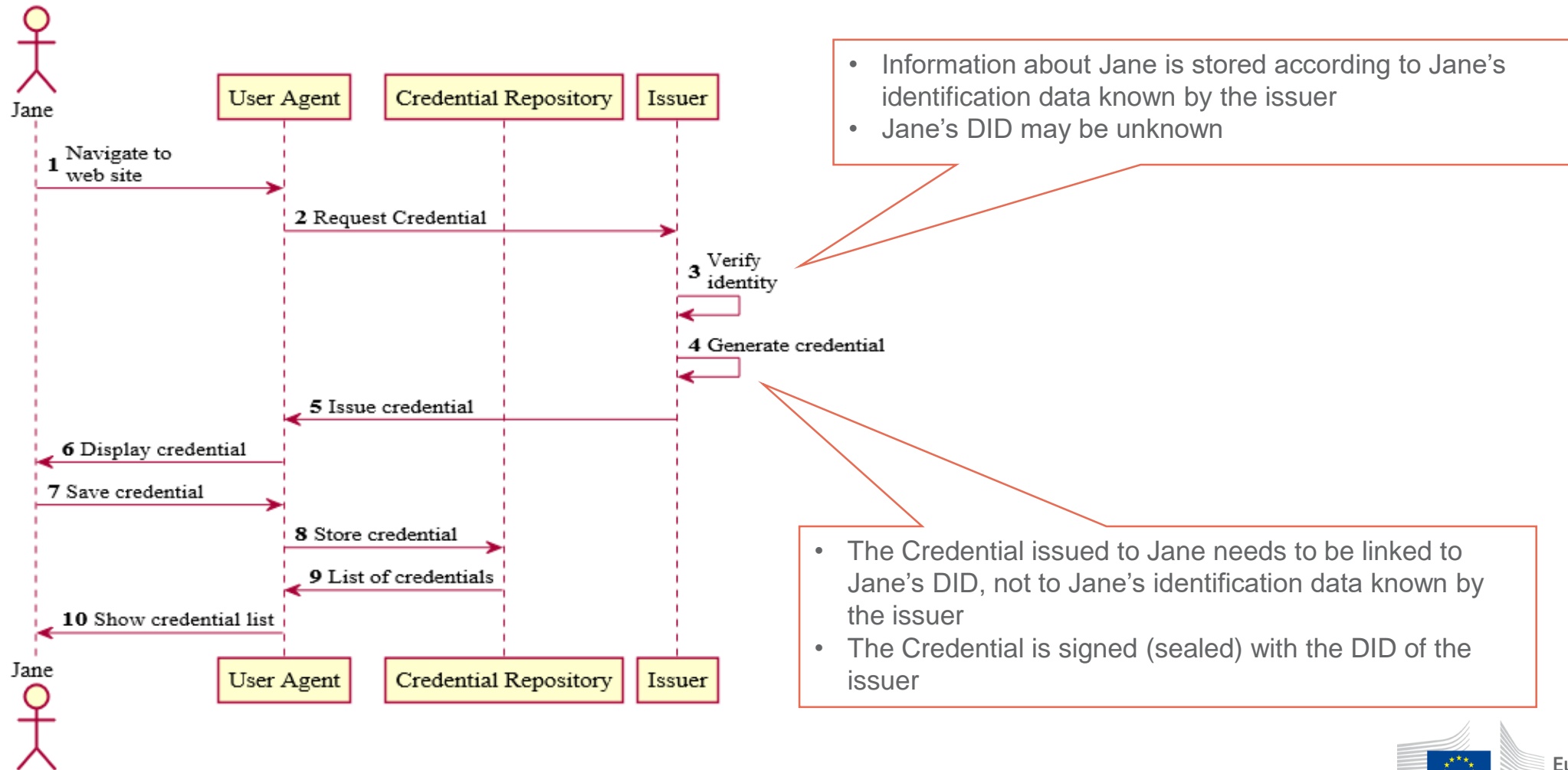
https://youtu.be/ATXCzY-GM_U

More Challenges

Linking assertions with eIDAS eID

Supporting identity matching and verification through eIDAS

Example credential creation flow

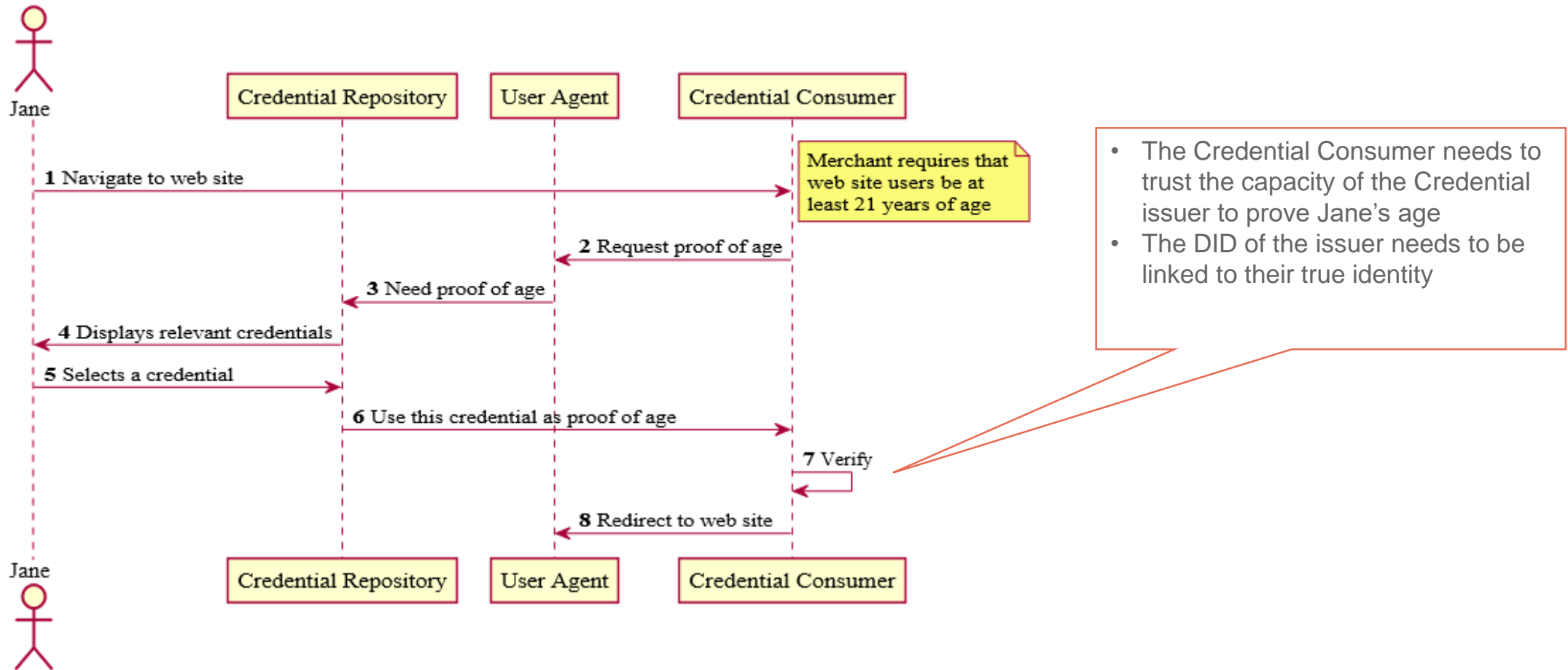


- Information about Jane is stored according to Jane's identification data known by the issuer
- Jane's DID may be unknown

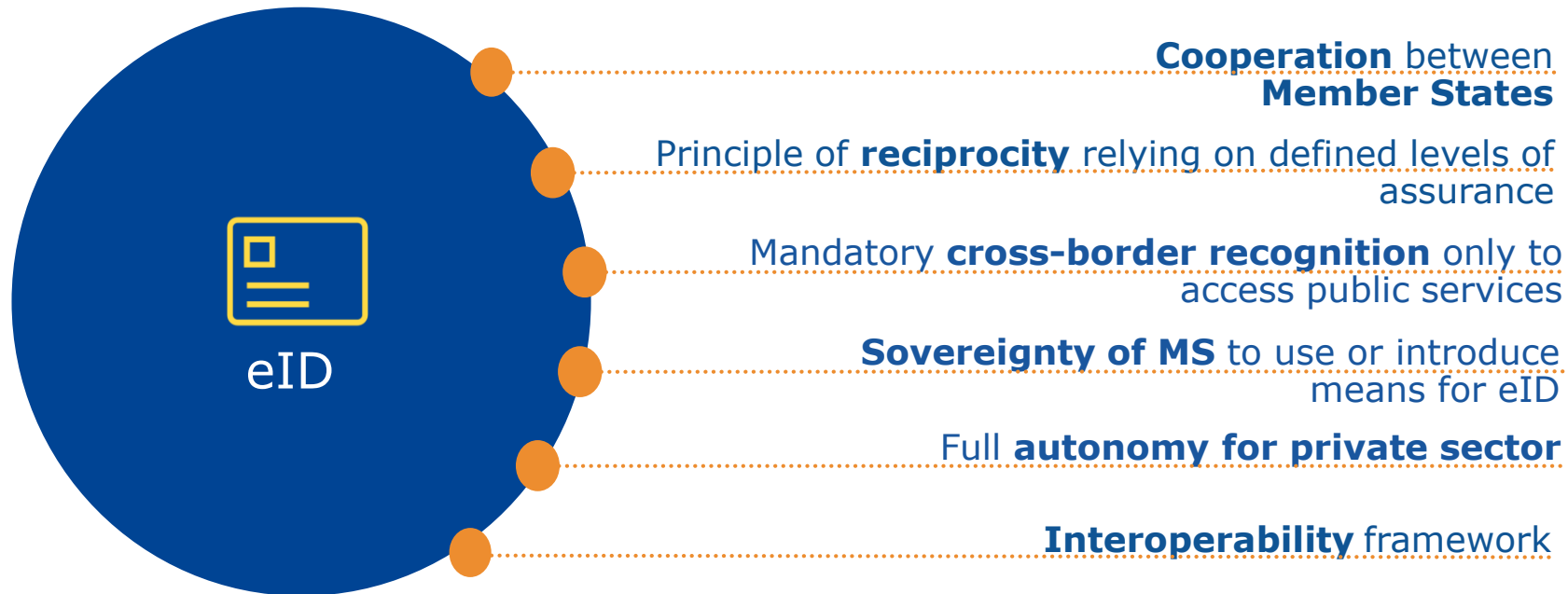
- The Credential issued to Jane needs to be linked to Jane's DID, not to Jane's identification data known by the issuer
- The Credential is signed (sealed) with the DID of the issuer

Supporting identity matching and verification through eIDAS

Example age verification flow


















eIDAS: Key principles for eID



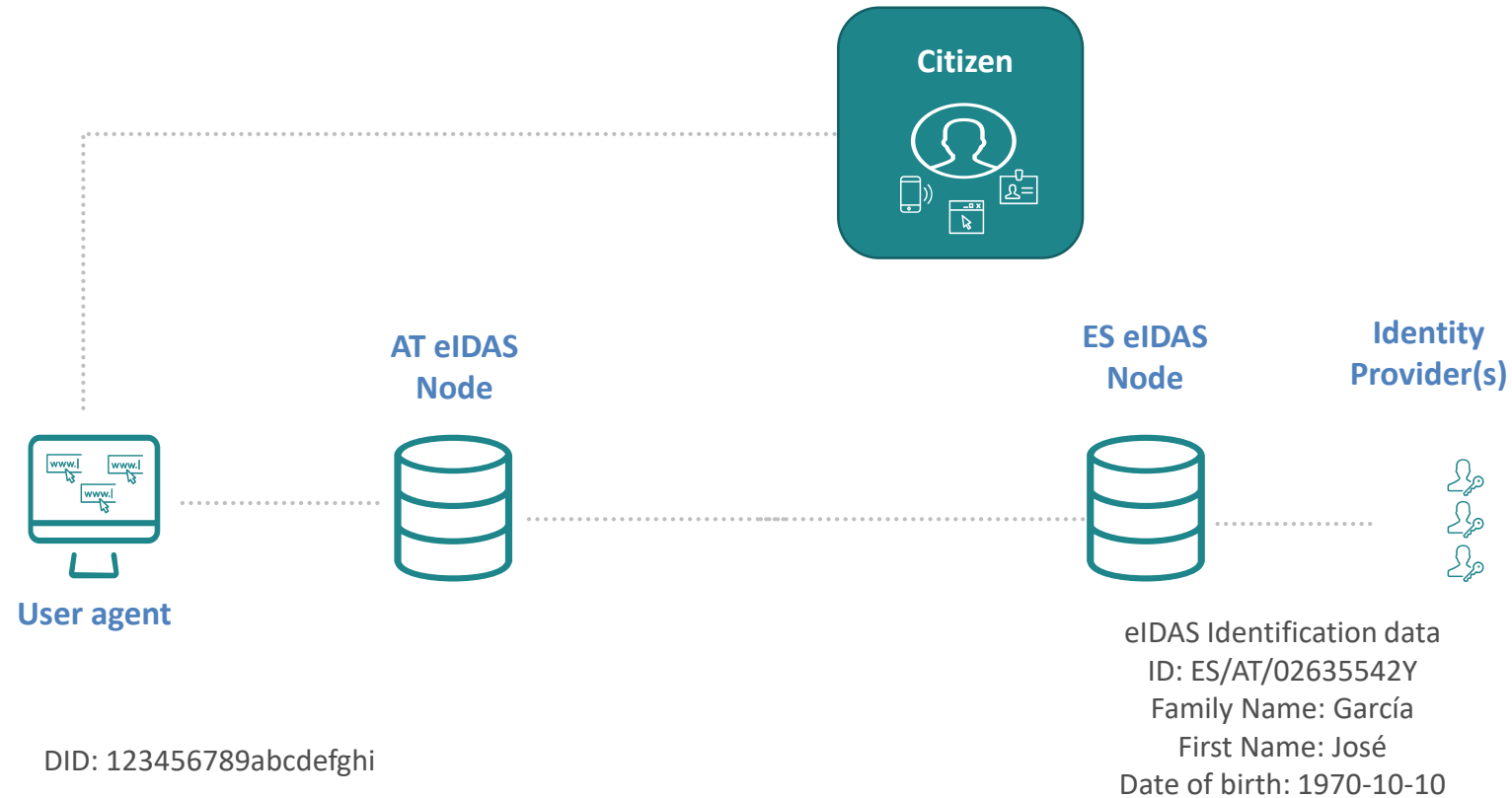
*The Regulation does not impose the use of eID, only mutual recognition when eID is required

Overview of notified eID schemes

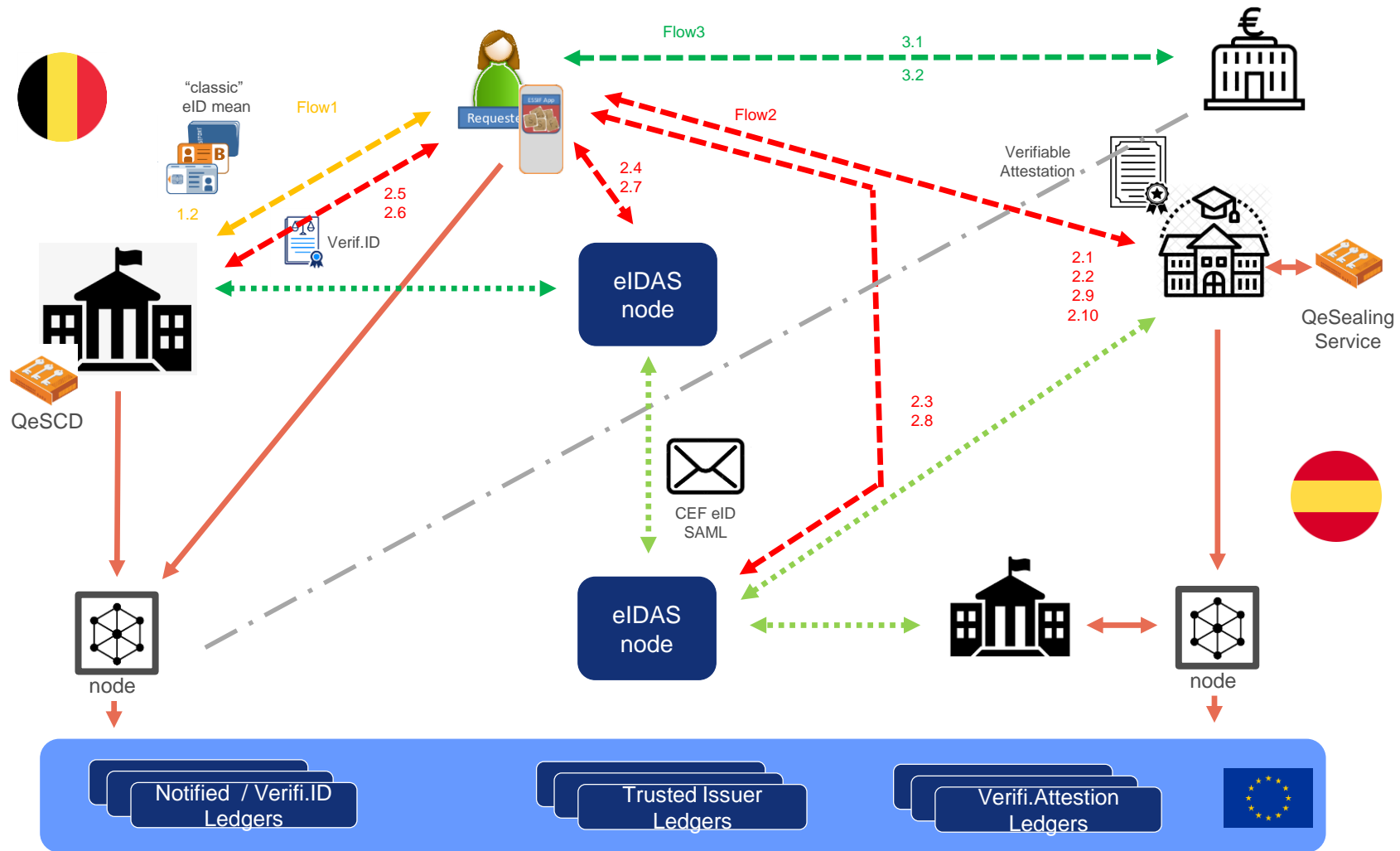
Overview of notified eID schemes under eIDAS					
Country	eID scheme	Publication in OJ	Country	eID scheme	Publication in OJ
 Germany	National ID card	26.9.2017	 UK	GOV.UK Verify	2.5.2019
 Italy	SPID	10.9.2018	 Czech Republic	National eID card	13.9.2019
	National eID card	13.9.2019			
 Spain	National ID card	7.11.2018	 Netherlands	eHerkenning	13.9.2019
				DigiD	21.08.2020
 Luxembourg	Luxembourg eID card	7.11.2018	 Slovakia	National eID card	18.12.2019
 Estonia	ID card, Mobiil-ID, e-Residency	7.11.2018	 Latvia	eID karte, eParaksts	18.12.2019
 Croatia	Personal ID card (eOI)	7.11.2018	 Denmark	NemID	8.4.2020
 Belgium	Citizen eCard	27.12.2018	 Lithuania	National eID card	21.08.2020
	FAS/itsme	18.12.2019			
 Portugal	National ID card	28.2.2019			
	CMD - mobile	8.4.2020			

~58% of the EU population covered by notified eID schemes

Linking DID with eIDAS eID



- Issue with the verification by third parties – the authentication is only valid for the requester

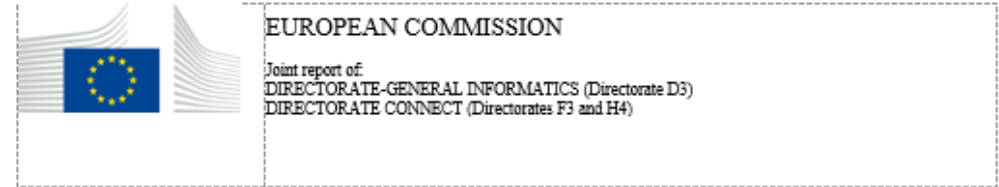


Flow1: Obtain Verifiable ID using "classic eID mean" (eSealed by Issuer)
 Flow2: Request V.Attestation in existing CEF eID context (AuthN via CEF eID PEPS)
 Flow3: Submission of a Verifiable Attestation (validation by relying party based on eSeal)
 Note: flow2 (and 3) allows NOTIFIED classic eID AND V.ID based AuthN

eIDAS and SSI

SSI eIDAS Legal Report

How eIDAS can legally support digital identity and trustworthy DLT-based transactions in the Digital Single Market



ESSIF – eIDAS/GDPR

**A Vision of / Study wrt
Architecture Principles and Possible Roadmap
of a secure-by-design, privacy-protecting
and eIDAS-compliant
European SSI Framework**

as to enable

**Easy and Fast and Trustworthy
Cross-border Exchanges
in a European Digital Single Market**

