EBSI Verifiable Credentials explained

CHAPTER 4

EBSI digital identity

June 2022

European Commission | ebsi European Blockchain

EBSI, explained – first edition

What are the different chapters of this first edition?

01.

Verifiable Credentials Explained

02.

Verifiable Credentials in action

03.

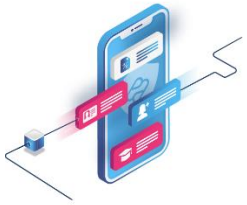
Decentralised Identifiers (DID) Methods

04.

Digital Identity

05.

Issuers Trust Model



06.

Open ID Connect for Verifiable Credentials

07.

Digital Wallets

04. Digital Identity explained – Index

What are you going to learn in this chapter?

04.1

What are the different approaches for Digital Identity?

Digital Identity is the foundation for all other digital services

Digital Identity sits at the foundation of all other digital services

My education

My finances

My work

My social benefits

My health

There are three different approaches to digital identity

The Holder's Digital Identity can be asserted in different ways

My Identity

My Digital Identity

National Approach

Authenticate to national services

eID means

- National
- Sectorial

Federated Approach

Authenticate to services that trust your IDP

Federation within a country

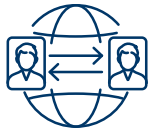
Cross-border authentication such as eIDAS (high LoA use cases)

Social Network login (low LoA use cases)

Level of Assurance (LoA)

Self-sovereign Approach

Share credentials and authenticate to services that trust Trusted Issuers



European SSI

Authentication (Verifiable ID - based on the eIDAS common data set)

Verifiable Credentials exchange

Self-sovereign Identity (SSI)

When is authentication and identification required?

The applications used by issuers and verifiers require authentication and identification as well as the digital wallet itself

Issuer

Authentication and identification

Issuance of

Verifiable Credentials

Holder

Authentication and identification

Digital wallet

Authentication and identification

Presentation of

Verifiable Presentation

Verifier

Must implement a:
- National and/or;
- Federated and/or;
- Distributed

approach to ensure the authentication and identification of Citizens (and Businesses) as part of the Issuing process.

Must implement a:
- National and/or;
- Federated and/or;
- Distributed

approach to ensure the authentication and identification of Citizens (and Businesses).

May (*) implement a:
- National and/or;
- Federated and/or;
- Distributed

approach to ensure the authentication and identification of Citizens (and Businesses) as part of the Issuing process.

* When verification is done in-person, instead of online, identification can be carried out using analogue identification means such as a Citizen card.

04.2

How do the different Digital Identity approaches work?

The National Approach

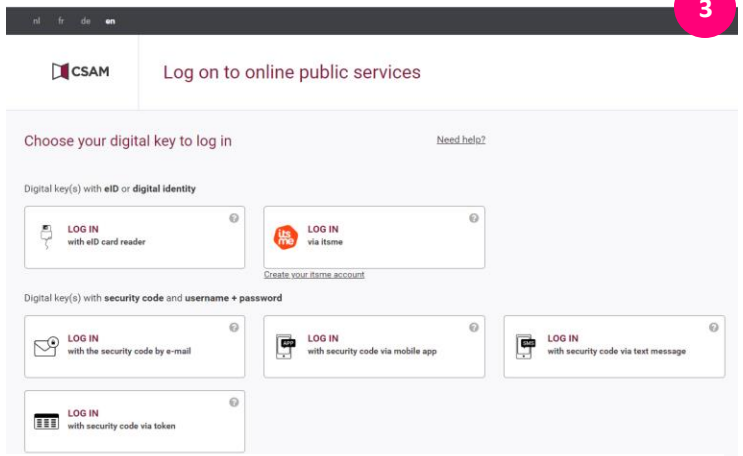
A **central authority**, e.g. a Member State, manages a **national identity service** responsible for authentication and identification of Citizens accessing its Digital Services.

The National Approach – How does it work?

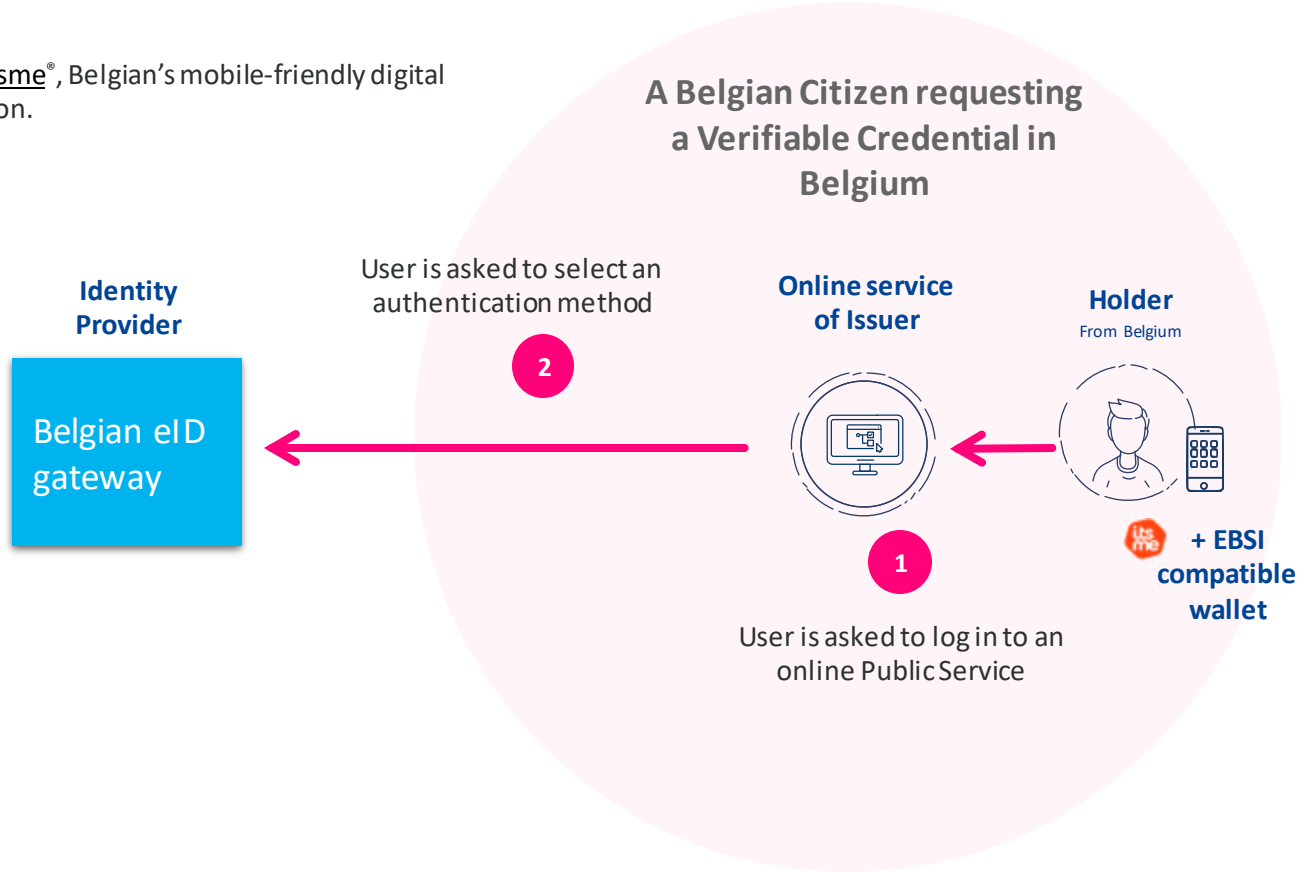
Example showing the use of national eID means to request a verifiable credential

User selects itsme®, Belgian's mobile-friendly digital identity solution.

3

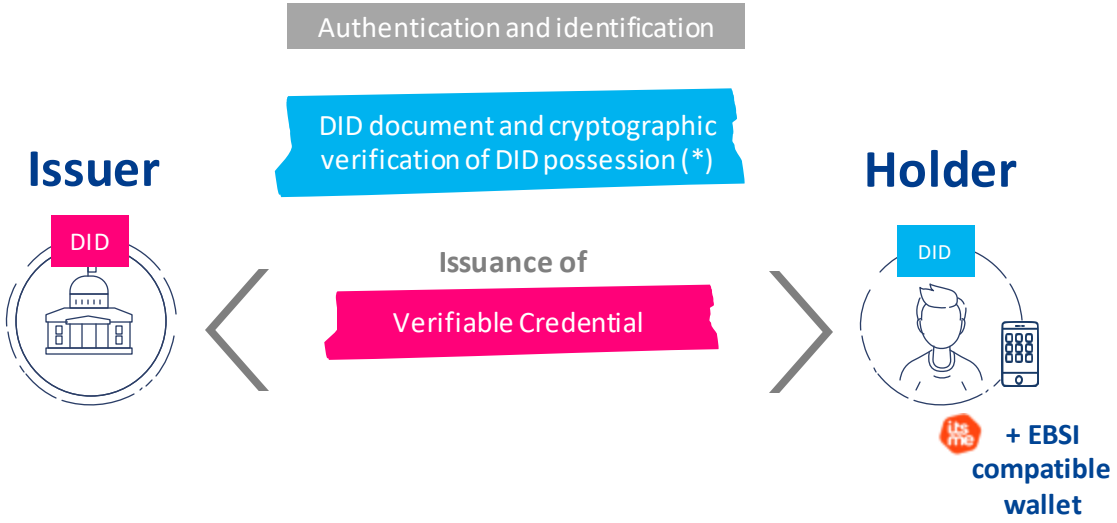


CSAM is the identity and access management gateway to the (public) services of the Belgian government



Verifiable credential is issued after successful authentication

If Holder has successfully proved ownership of the DID presented to the Issuer



(*) Chapter 3 explains this step-in detail

The National Approach – The benefits for the citizen

The National Approach – The benefits for the citizen

- ✓ I can choose the data I want to disclose
- ✓ I can choose my identity provider
- ✓ I can choose my authentication method

The Federated Approach

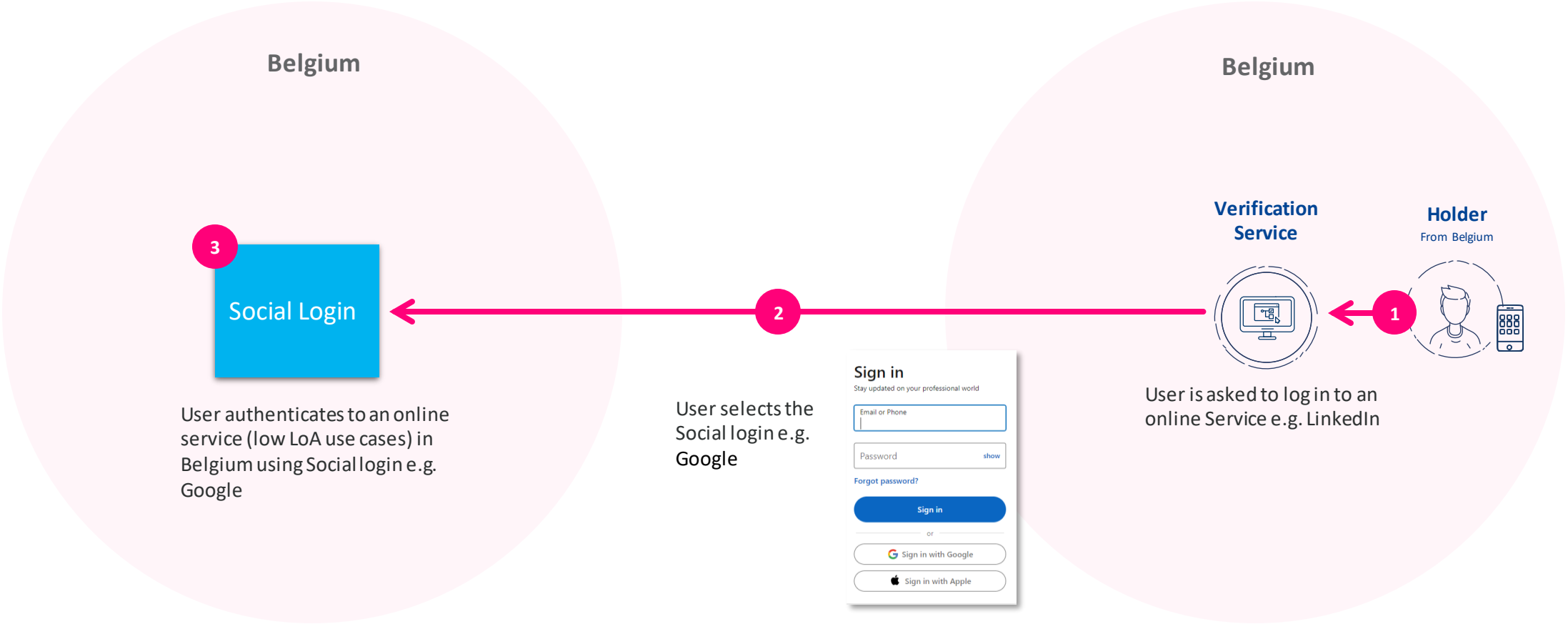
There are several federation approaches. For example, the eIDAS regulation(*) has put in place a **mutual recognition of notified national electronic identification schemes** (eID) across borders, enabling citizens to use their national eIDs when accessing online services from other European countries.

(*) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG

The Federated Approach – How does it work? (part 1/3)

Example showing the use of eIDAS in a cross-border verification scenario

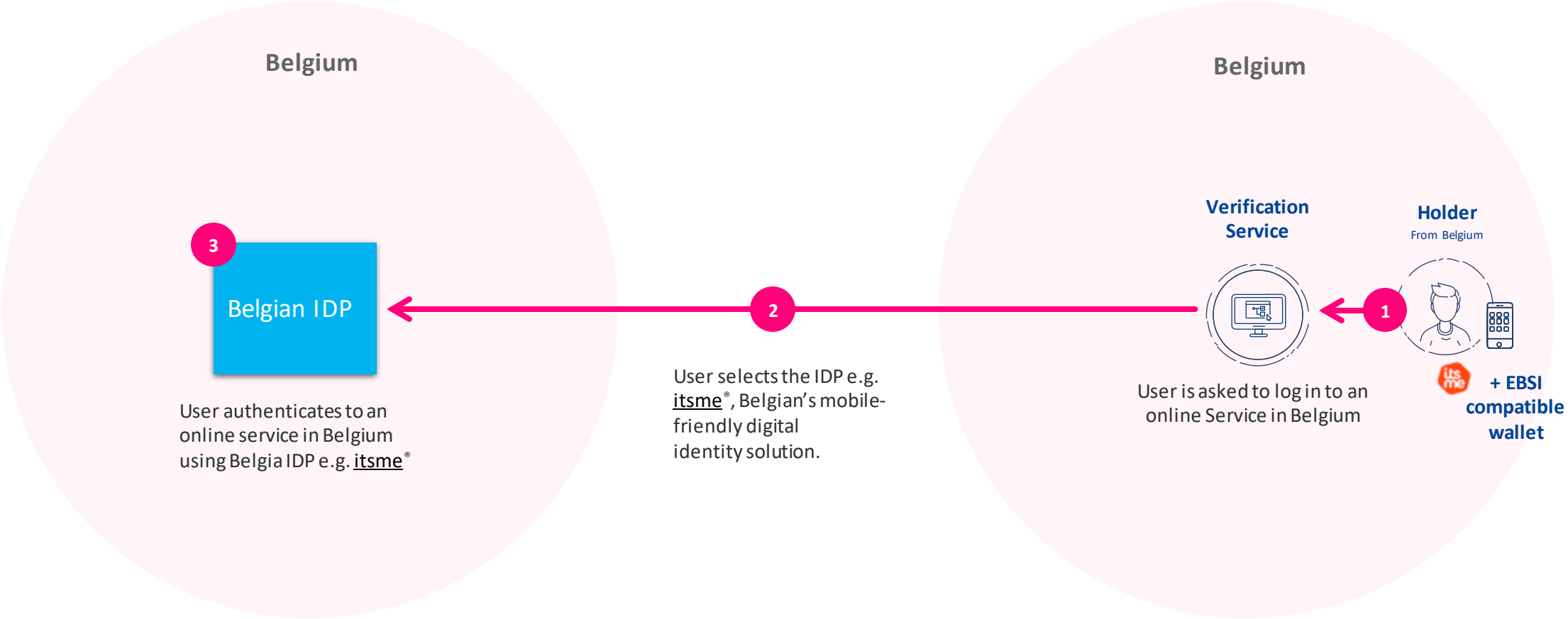
Social login (low LoA use cases)



The Federated Approach – How does it work? (part 2/3)

Example showing the use of eIDAS in a cross-border verification scenario

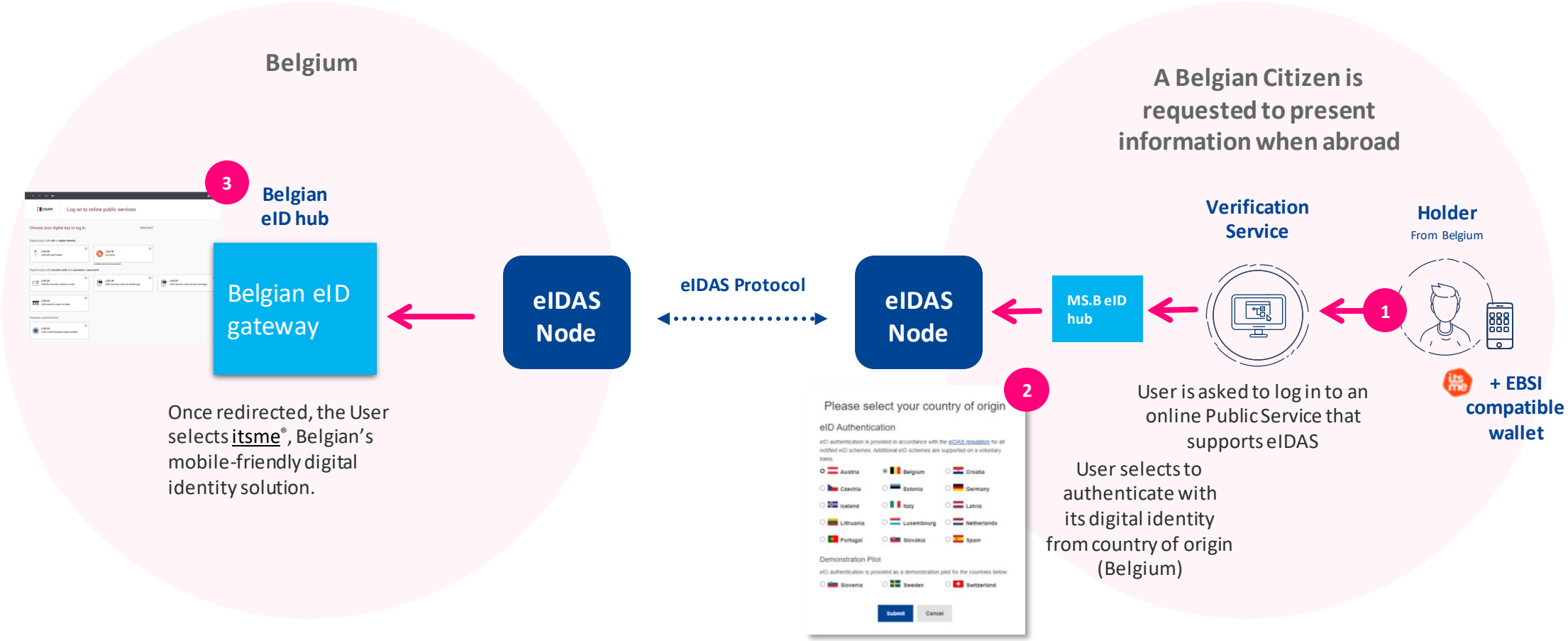
Federation within the country



The Federated Approach – How does it work? (part 3/3)

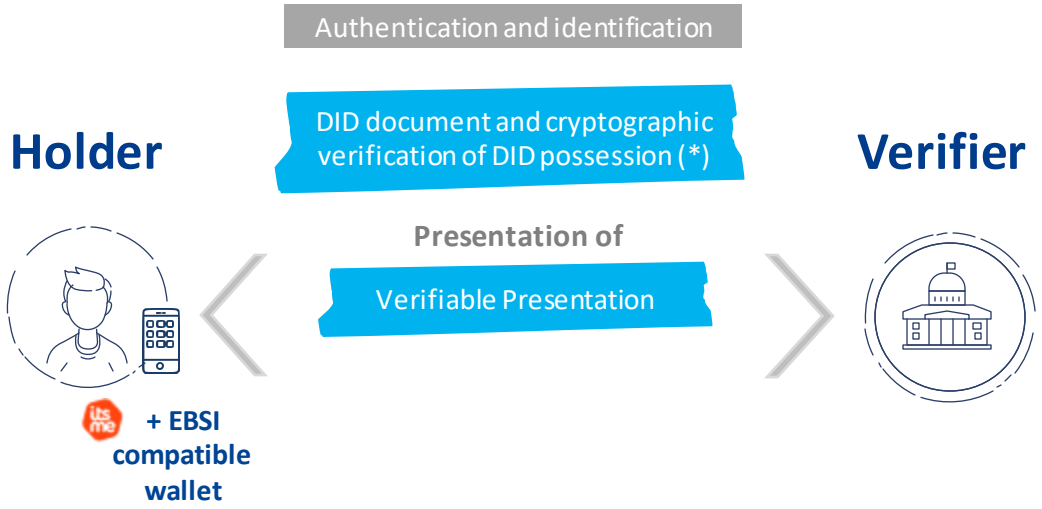
Example showing the use of eIDAS in a cross-border verification scenario

Cross-border authentication (eIDAS)



Verifiable presentation is shared after successful authentication

If Holder has successfully proved ownership of the DID presented to the Issuer



(*) Chapter 3 explains this step-in detail

The Federated Approach – The benefits for the citizen

The Federated Approach – The benefits for the citizen

- ✓ I can choose the data I want to disclose
- ✓ I can choose my identity provider
- ✓ I can choose my authentication method

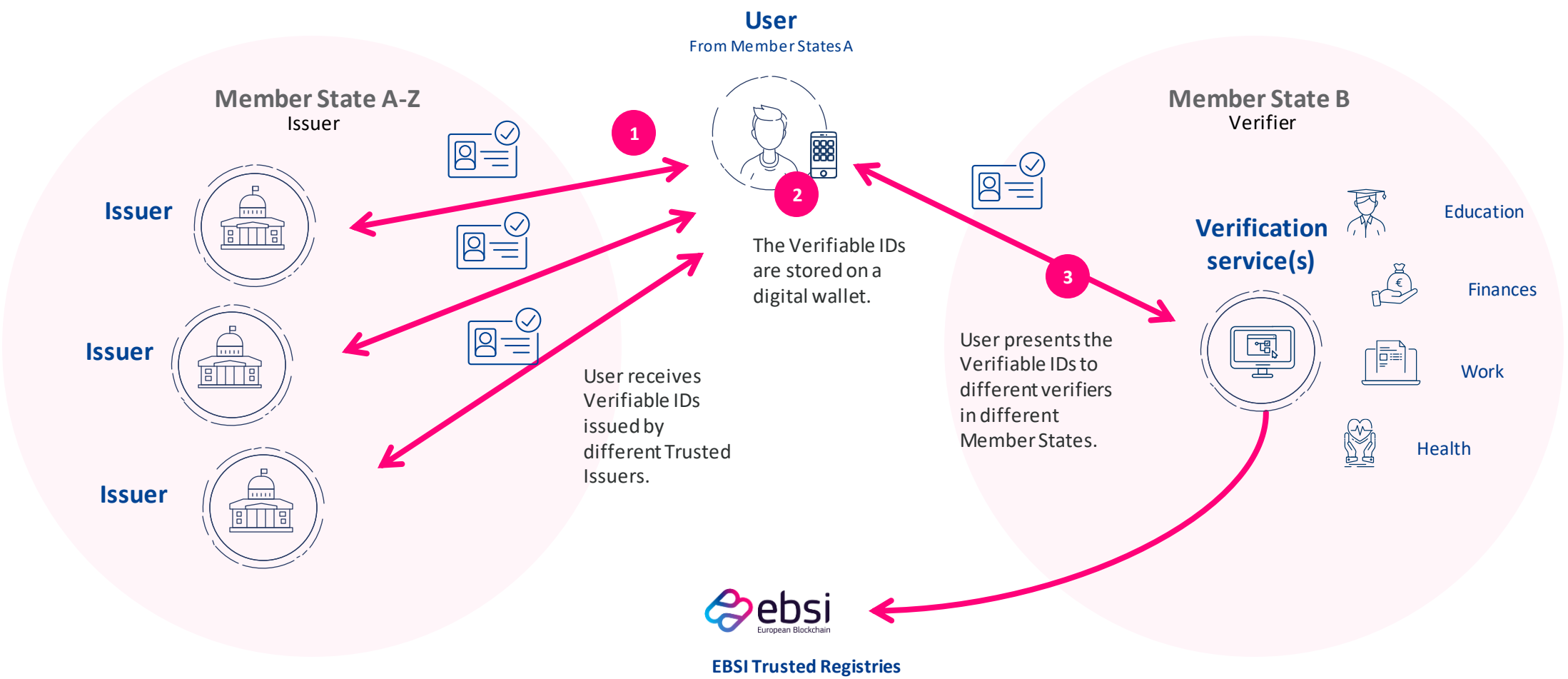
The Self-sovereign Approach

W3C’s **Verifiable Credentials** can be used to create Verifiable IDs which can be **easily combined** with other Credentials to expand the number of attributes used for authentication and identification purposes, but also for record matching. The model also supports the **issuance and presentation** of **Verifiable Attestations**.

Based on the work of the European Self Sovereign Identity (ESSIF) initiative part of EBSI

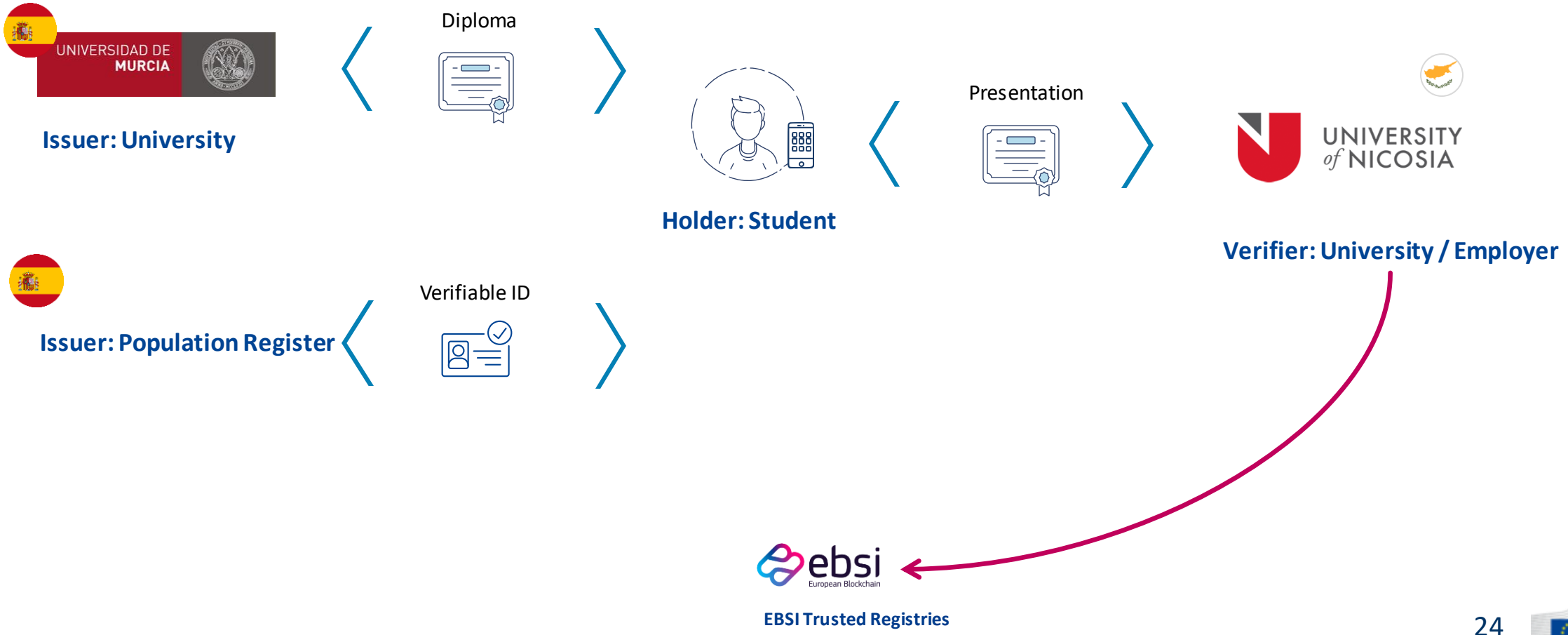
The Self-sovereign Approach – How does it work?

The Self-sovereign Approach – How does it work?



EBSI Multi-University pilot – example of self-sovereign scenario

Multi-University pilot using Verifiable ID and Verifiable Diploma



The Self-sovereign Approach – The benefits for the citizen

The Self-sovereign Approach – The benefits for the citizen

- ✓ I can choose the data I want to disclose
- ✓ I can choose my identity provider
- ✓ I can choose my authentication method

Identity management using wallets

User could use any wallet to authenticate and get the credentials

The decentralised model enables holders to choose their wallet and credentials they will share. Today 13 wallets are conformant with EBSI specifications, and more are to come.

DESKTOP

DANUBE TECH GMBH
eDiplomas GREEK UNIVERSITIES NETWORK
teknei

MOBILE

CIMEA THE ART OF CONNECTING ACADEMIA
SYSTEMS INTEGRATION SOLUTIONS
THALES Building a future we can all trust

DEKSTOP & MOBILE

GATACA
walt.id
iGrant.io Your data, your choice.
identyum
Posteitaliane
Validated ID
DXC.technology

04.3

What is the summary of the approaches?

Overall summary

Summary of the three approaches

	The National Approach	The Federated Approach	The Self-sovereign Approach
Concept	A Central authority, e.g. a Member State manages a **centralised service** responsible for authentication and identification of Citizens accessing its Digital Services.	The eIDAS regulation has put in place a **mutual recognition of notified national electronic identification schemes (eID)** across borders. Enabling citizens to use their national eIDs when accessing online services from other European countries.	**W3C's Verifiable Credentials can be used to create Verifiable eIDs** which can be easily combined with other Credentials to expand the number of attributes used for authentication and identification purposes but also for record matching.
Example	**e.g. CSAM**	**e.g. eIDAS eID network**	**e.g. ESSIF part of EBSI** **Note:** No personal data is stored on-chain.
Technology	**Electronic identity card (eID) and others.**	**Security Assertion Markup Language** and **the eIDAS common dataset.**	**Verifiable Credentials** and the **eIDAS common dataset.**
Wallet compatible?	**Yes** e.g. itsme	**Yes** e.g. itsme is an eIDAS notified eID means.	**Yes** e.g. Verifiable Credentials are designed for Digital Wallets.
Governance	A **Central authority** manages the service and acts as the custodian of the Citizens' identity.	**National nodes**, usually centrally managed, interconnect identity service providers that are eIDAS-compliant.	**National nodes**, usually centrally managed, interconnect identity service providers that are eIDAS-compliant.
Strength	**Control of service by** identity service provider.	**Interoperability** among different identity service providers.	**Flexibility:** selective disclosure of information and ease to combine it with other Verifiable Credentials.

Summary of the value for each type of actor

Summary of the value for each type of actor

	The National Approach	The Federated Approach	The Self-sovereign Approach
Issuer	Reliable **authentication and identification of MS nationals**	Useful for **cross border authentication**	Can be used **in combination with other authentications and Verifiable Credentials**
Wallet	Simple integration with **national services**	Useful for **cross border authentication**	Useful for **cross border authentication and Verifiable Credentials exchange**
Verifier	Reliable **information sources**	Useful for **cross border use cases**	Useful for **fast and reliable Verifiable Credentials validation**

Want to know more?

Key resources

Explore EBSI

Explore the EBSI website

https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/Home

Check the specs

Check the EBSI Playbook

https://ec.europa.eu/digital-building-blocks/wikis/display/EBSIDOC/EBSI+Verifiable+Credentials+Playbook

Watch the demos

Watch the EBSI Demo Day

https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/EBSI+Demo+Day

https://ec.europa.eu/ebsi