



European Blockchain Service Infrastructure: a new Building block, but not just another Building Block

Tuesday 3th November 2020

OUR AGENDA TODAY

- **Introduction to EBSI**
- **ESSIF**
- **Diplomas Use Case**
- **Open questions**

Introduction to European Blockchain Service Infrastructure



How did it all start?

The European Blockchain Services Infrastructure (EBSI) was born from a need to invest into blockchain technologies supported by the European Commission and 30 participating countries forming the European Blockchain Partnership (EBP)

2017

-
Tallinn declaration on eGovernment

In 2017, Member States and EFTA countries signed the Tallinn declaration on eGovernment outlining the importance of having efficient and secure digital public services in order to achieve the full potential of the Digital Single Market.



2018

-
European Blockchain Partnership declaration

In 2018, 27 EU Member States, Norway and Liechtenstein signed a declaration creating the European Blockchain Partnership (EBP) with the ambition to provide digital public services matching the required level of digital security and maturity of today's society.



2019

-
European Blockchain Services Infrastructure

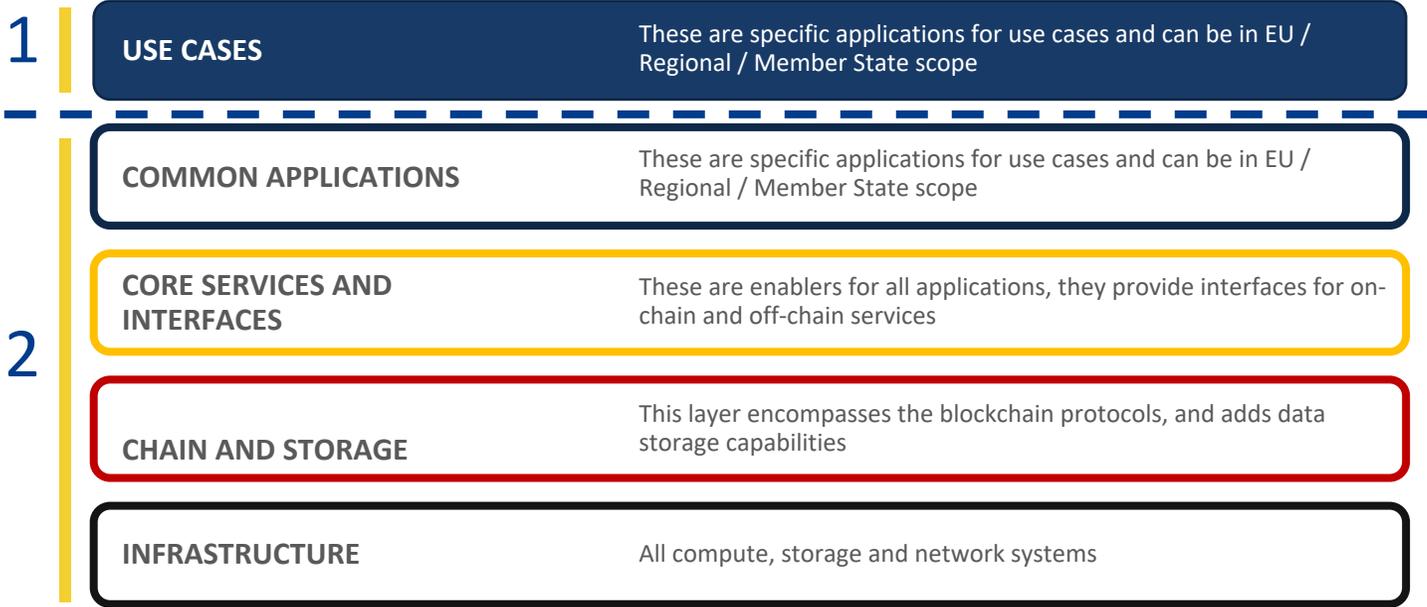
On 14 February 2019, the European Commission published the 2019 Telecommunications Work Programme of the Connecting Europe Facility (CEF) creating initial funding conditions for EBSI.

EBSI at a glance

The EBP members will operate EBSI nodes at national level. These nodes will be able to create and broadcast transactions that will update the ledger. The architecture of each node will be composed of two main layers.

1 Use Case Applications

2 Core Infrastructure



Additionally to the generic infrastructure, EBSI includes 4 initial use cases

These 4 use cases enable you to **simplify administrative processes, increase efficiency and instill trust in citizens.**



Notarisation of documents

Leverage the power of blockchain to create trusted digital audit trails, automate compliance checks in time-sensitive processes and prove data integrity.



European Self-Sovereign Identity

Implement a generic Self-Sovereign Identity capability, allowing users to create and control their own identity without relying on centralized authorities.



Diplomas management

Give control back to citizens to validate their education credentials, significantly reducing verification costs and improving authenticity trust.



Trusted data sharing

Securely share data (e.g. IOSS VAT identification numbers and import one-stop-shop) amongst customs and tax authorities in the EU.

To test all UCs, a joint citizen's journey was designed (and built) in EBSIv1



Open your EBSI wallet account

- Create an EU login account (citizen)
- Access your EBSI wallet (citizen)
- Create a decentralized identifier (DID) address (citizen)



Get your eID verifiable credential

- Request a verifiable eID (citizen)
- Issue the eID verifiable credential (government)
- Store the verifiable credentials (citizen)
- Access your verifiable credential (citizen)



Get your Bachelor Diploma

- Request your bachelor diploma verifiable attestation (citizen)
- Issue bachelor diploma verifiable attestation (government)
- Store your bachelor diploma verifiable attestation (citizen)
- Access your bachelor diploma verifiable attestation (citizen)



Get your Master Diploma

- Request your master diploma verifiable attestation (citizen)
- Issue master diploma verifiable attestation (university)
- Store your master diploma verifiable attestation (citizen)
- Access your master diploma verifiable attestation (citizen)



Notarize your documents

- Participate in a call for proposals to get EU funding for your start-up (citizen's company)
- Notarise documents justifying the spending of the grant received (citizen's company)
- Verify your notarized documents (EU auditors)



Securely share you data

- Create your IOSS VAT ID (company)
- Publish IOSS VAT ID (taxation authority)
- Verify validity of IOSS VAT ID (customs authorities)

This is the status of the EBSI network

27 Member State Nodes (EBP members)

27 nodes have been requested by Member State institutions from
6 nodes onboarding

+

6 Commission Nodes

=

39 Node TestNet Planned for 2020

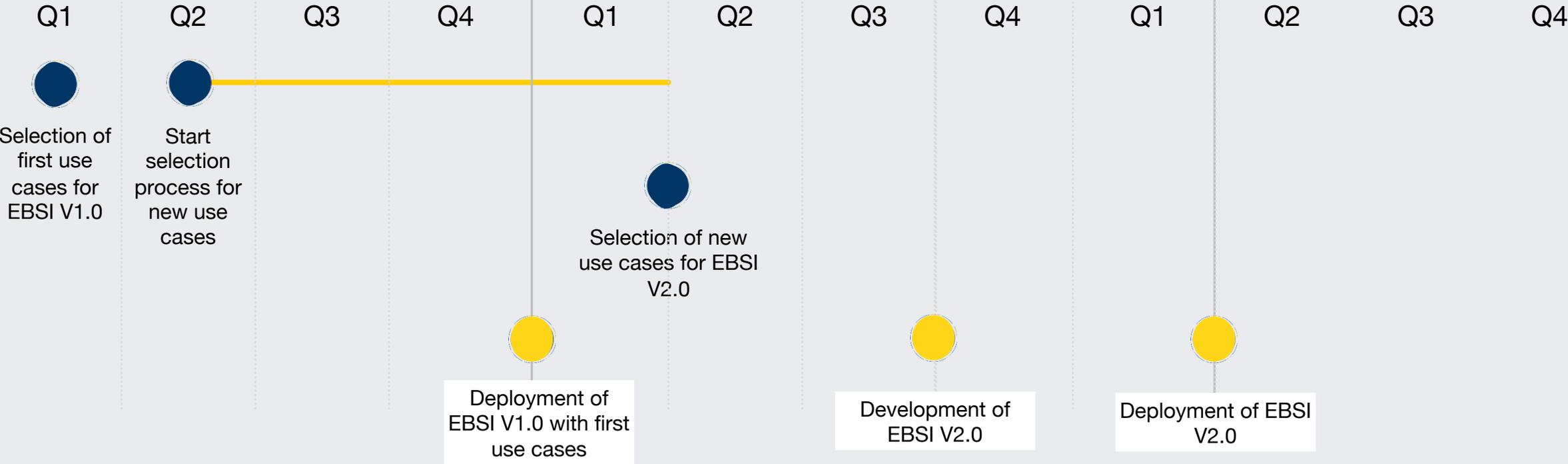


EBSI Roadmap

2019

2020

2021



European Self Sovereign Identity Framework ESSIF

Scope of ESSIF

- Empower citizen in the management of their data via SSI
- Stimulate the SSI-transformation of public services
- Facilitate cross-border interaction with SSI
- Make/keep national SSI projects interoperable
- Integrate/align existing building blocks such as eIDAS, e-delivery, once-only with SSI
- Conceptualize and build an identity layer in the new European Blockchain Services Infrastructure supporting the current use cases
- Preserve European/democratic values in the implementation of Self Sovereign identity
- Stimulate SSI development and standardization on global level (W3C, DIF, ISO, CEN-CENELEC, etc.)

European Self-Sovereign Identity (ESSIF)

New paradigm – empowered citizens

Decentralized identity

The essence of decentralized identity is “to move the utility and portability of physical identity credentials to our digital devices”

The term “credentials” extends to any (tamper-resistant) set of information that some authority claims to be true about you, and that enables you to convince others (who trust that authority) of these truths

The claims in a credential can state anything about the subject, such as **attributes** (age, height, weight, etc.), **relationships** (mother, father, employer, citizenship, or others), or **entitlements** (medical benefits, library privileges, membership rewards, legal rights, and so on).

To qualify as a credential, the claims must be **verifiable** in some way. This means a **verifier** must be able to determine the following:

- Who issued the credential
- That it has not been tampered with since it was issued
- That it has not expired or been revoked

+

Verifiable Credentials

With physical credentials, verification is typically accomplished through some proof of authenticity embedded directly in the credential itself (like a watermark, hologram, or some other special printing feature). It can also be done by checking directly with the issuer that the credential is valid, accurate, and current. But this manual verification process can be difficult and time-consuming — a major reason why there is a worldwide black market in falsified credentials.

This brings us to one of the fundamental advantages of verifiable credentials: using cryptography and the Internet, they can be digitally verified in seconds. This verification process can answer the following four questions:

1. Is the credential in a standard format that can be electronically processed by the verifier and does it contain the data the verifier needs?
2. Does it include a valid digital signature from the issuer (thus establishing its origin and that it has not been tampered with in transit)?
3. Is the credential still valid, that is, not expired or revoked?
4. If applicable, does the credential (or its signature) provide cryptographic proof that the holder of the credential is the subject of the credential.

=

Empowered citizen

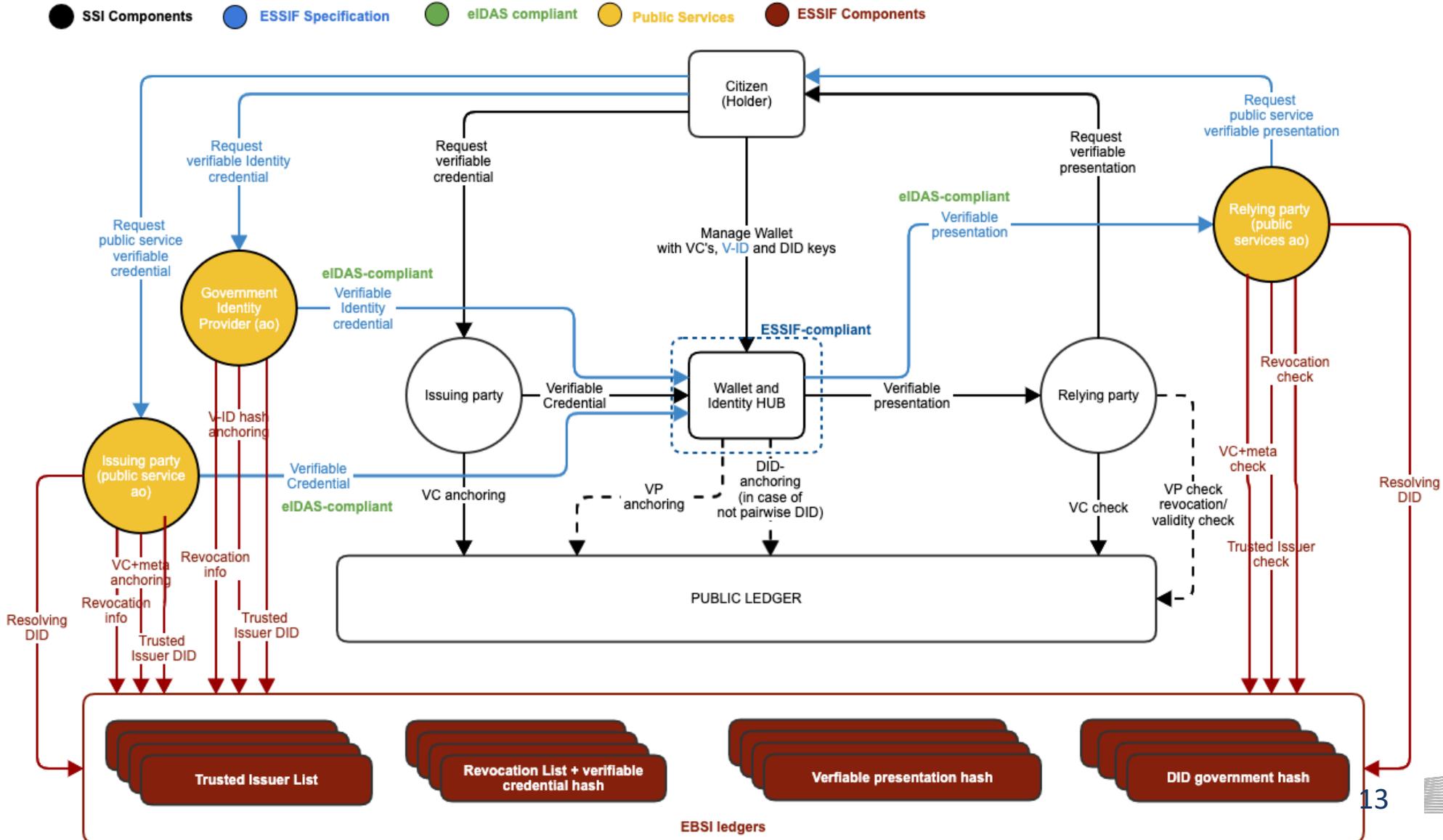
Establish connections with no intermediate service provider

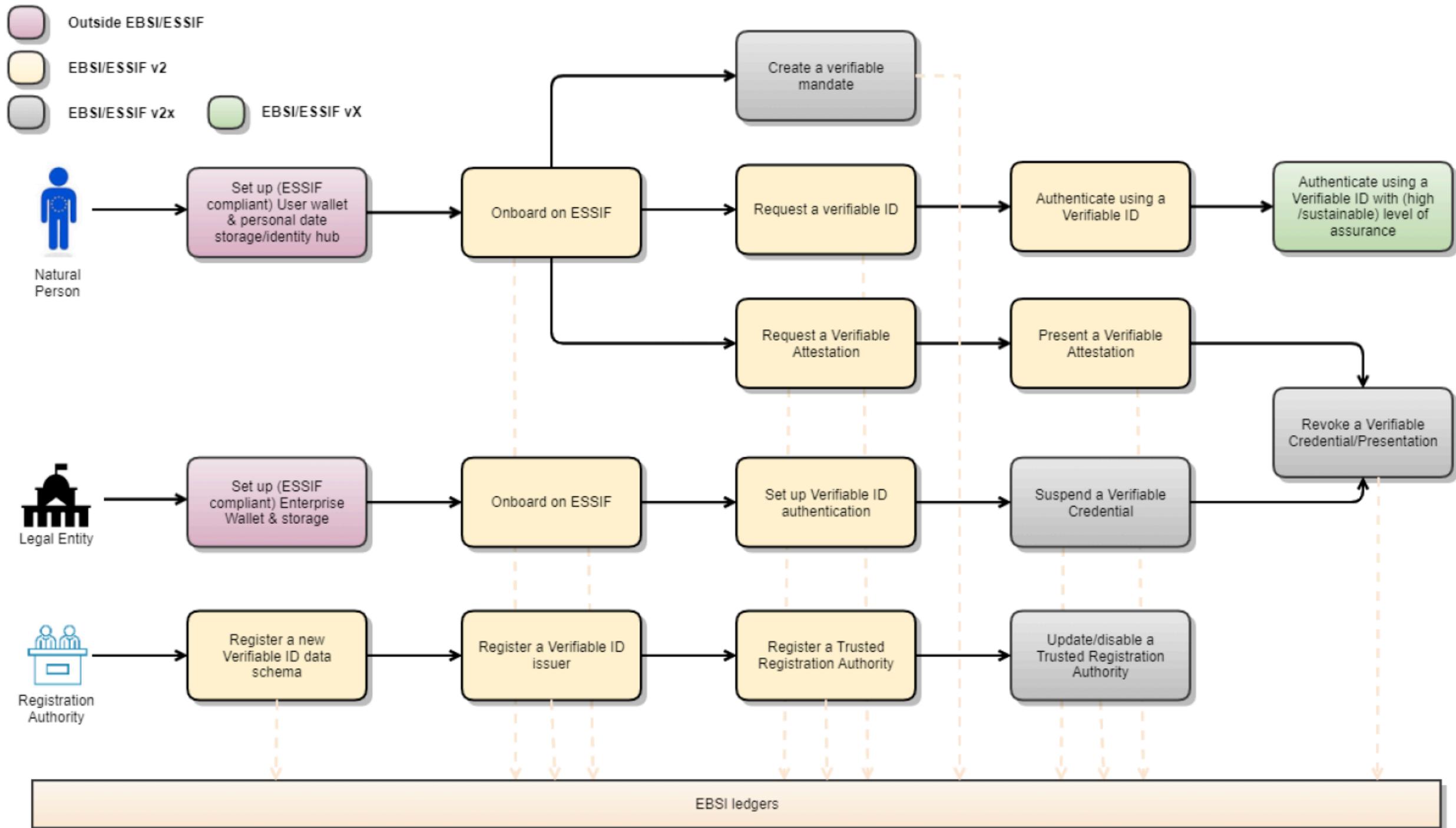
Citizens:

- **Owns their identity(ies)**
- **Owns, control, and manage their data (Verifiable credentials)**

Wallets are an application to manage public/private key pairs and run on mobile phones, personal computers, home servers, game consoles, or dedicated hardware devices. Wallets hold private keys associated with particular DIDs as well as other data, like verifiable credentials.

SSI ecosystem with ESSIF components

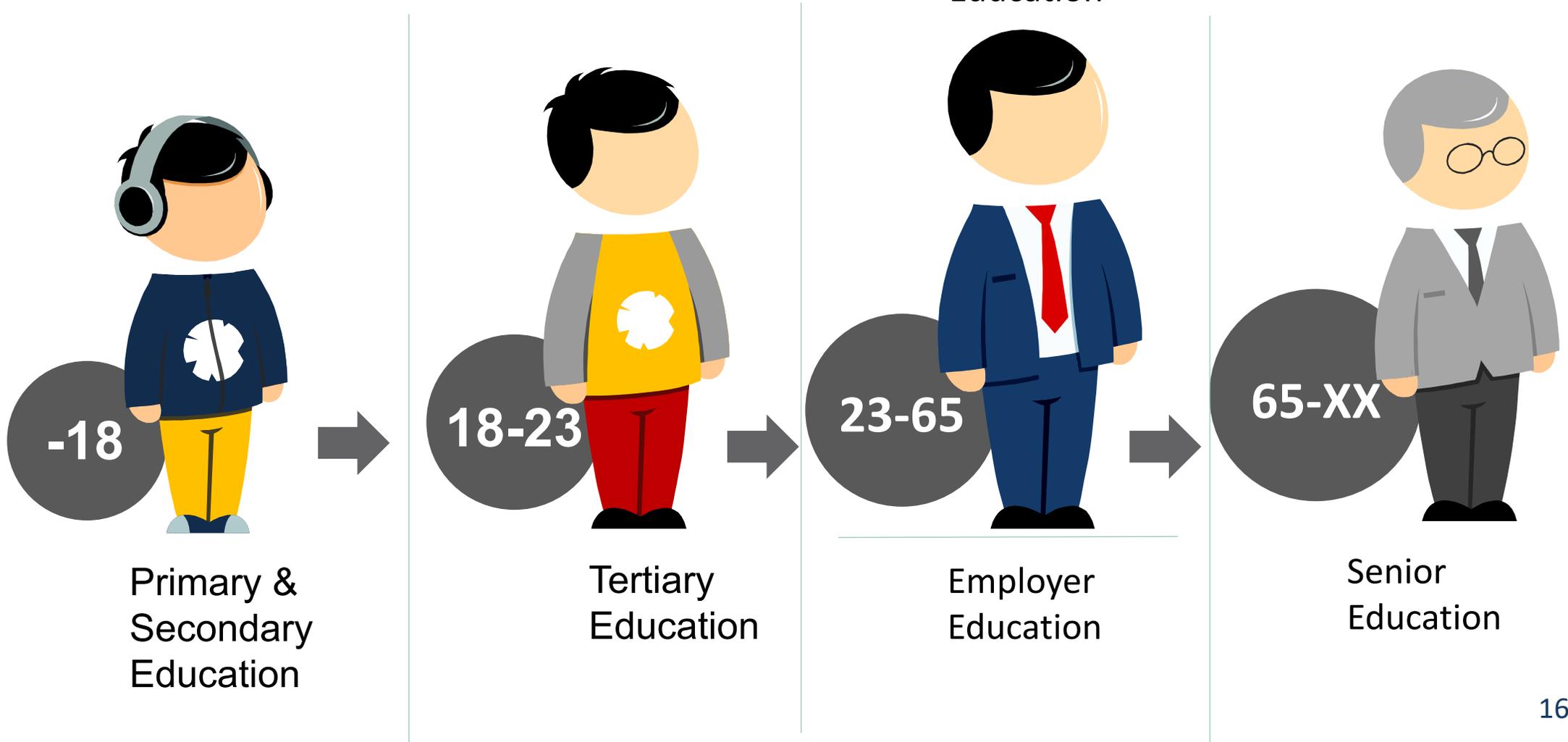




Diplomas Use Case

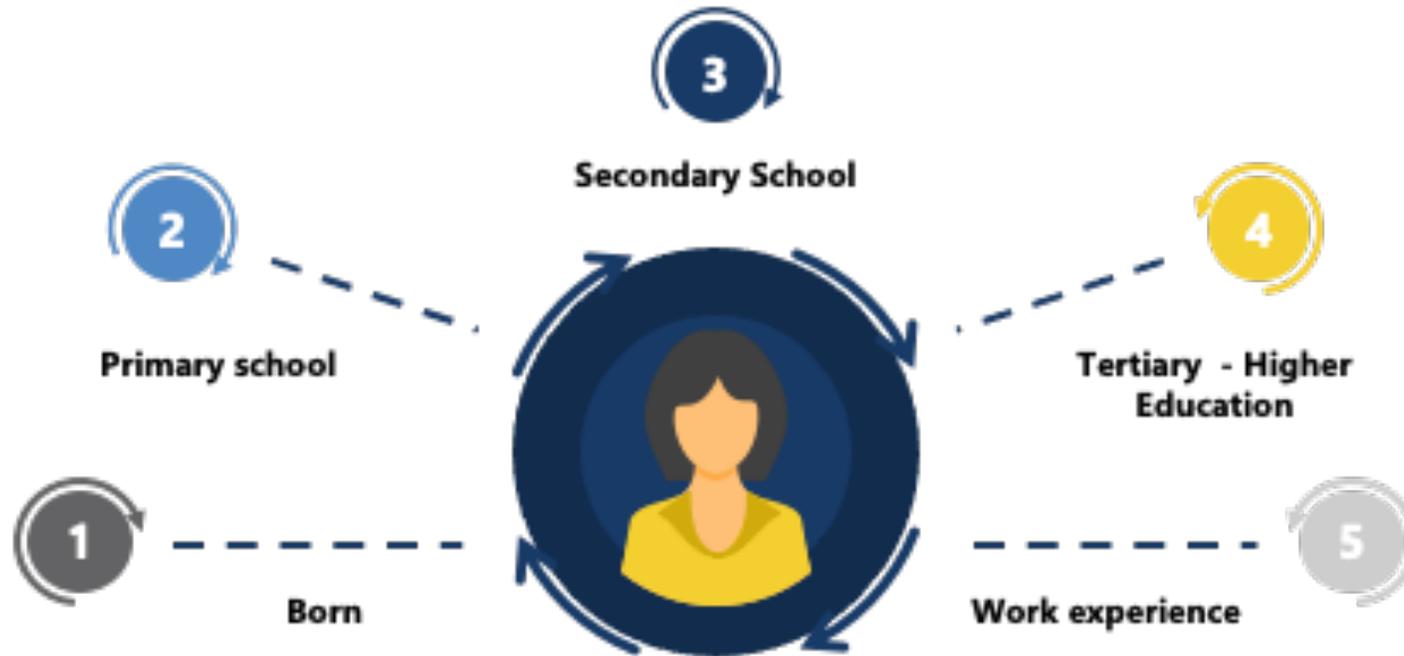
EBSI Diploma Use Case

Moving from a siloed education ecosystem...



Use case: Diplomas management

New paradigm: Focusing on citizen, breaking educational SILOs, enabling LLL, PLP & stacking credentials



Aligned to:

- EU Digital Strategy
- EU Data Strategy
- EU digital credentials action plan
- European education area
- EU Digital action plan
- Europass decision
- European skills agenda

- Student mobility for both, identity and records, will be a reality (on Student's Mobile wallet)
- Lifelong Learning will be a reality: credentials are owned, managed and controlled by the citizen
- Also, thanks to the stacking credentials feature, Personal Learning Pathways will be even easier
- Thanks to stacking credentials feature, this is a natural solution for microcredentials

EBSI Diploma Use Case

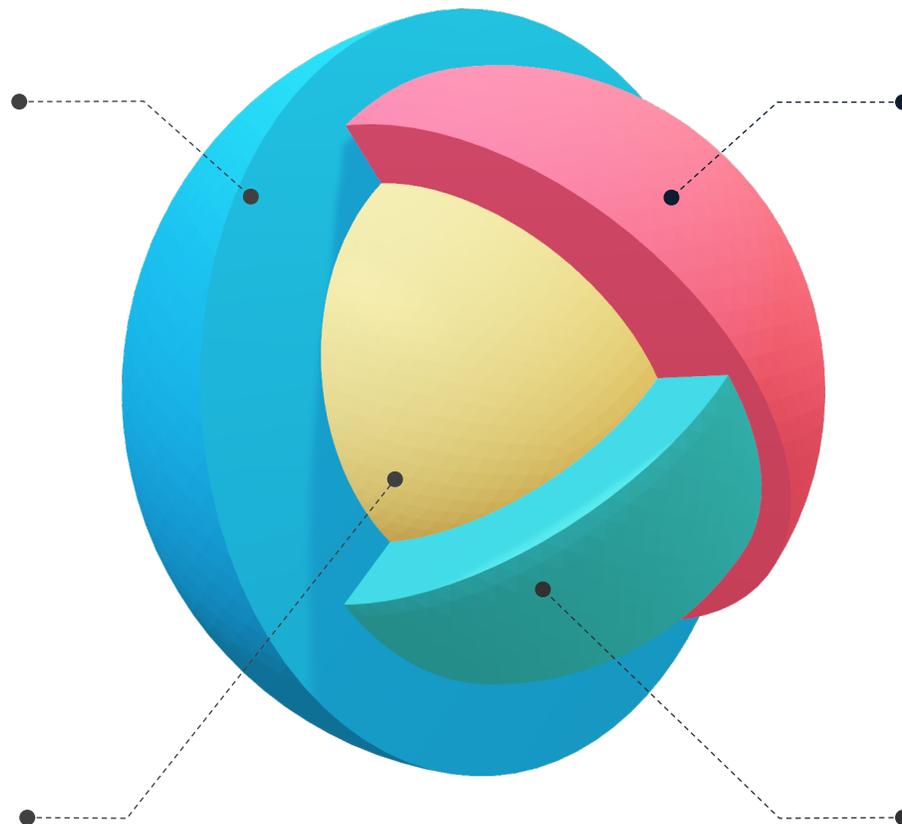
The different dimensions of Interoperability

Organizational

Legal

Semantics

Technical



EBSI Diploma Use Case

Interoperability – Legal dimension



SSI legal aspects are also Diplomas' aspects

- EBSIv1 legal report [available](#) at public EBSI site (SSI eIDAS & GDPR)

Ongoing dedicated UC assessment:

- Legal
 - Identities ↔ eIDAS
 - Data ↔ MS specific legal aspects
- GDPR

We will need both levels: EU and MS level compliance

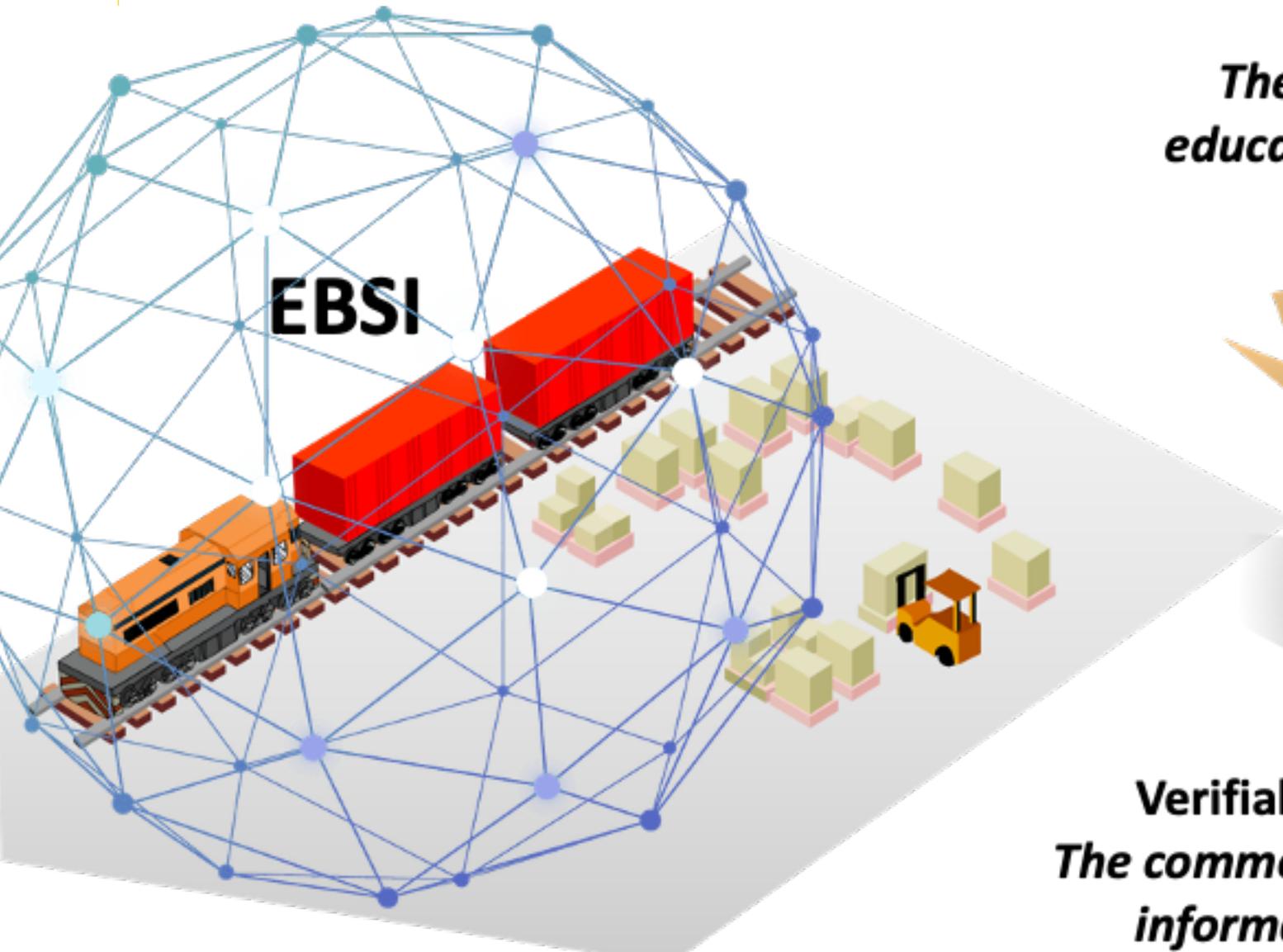
EBSI Diploma Use Case

Interoperability – Organizational dimension

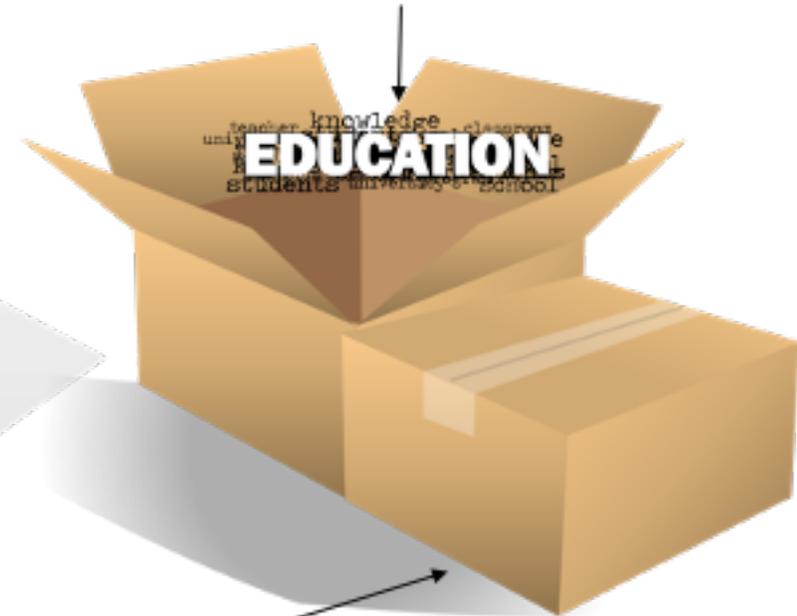


EBSI Diploma Use Case

Key benefit of EBSI Diploma: Interoperability (Technical & semantic)



Common Data Model
The common way to describe educational credentials (contents)



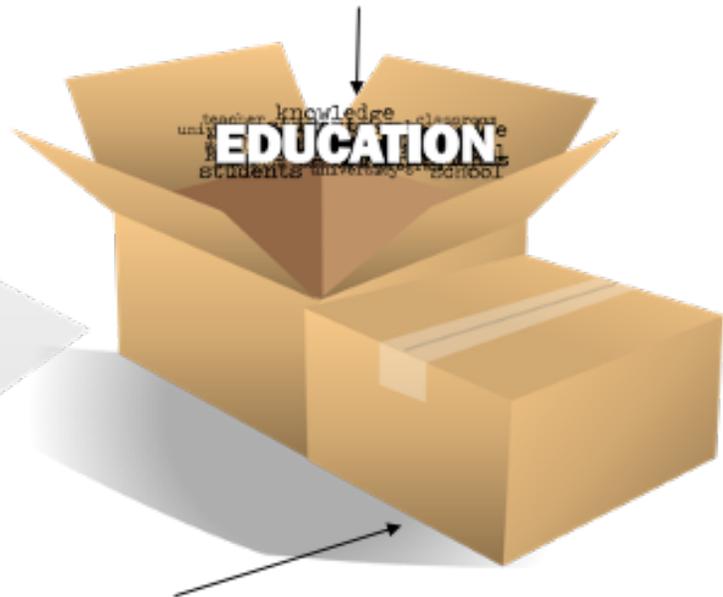
Verifiable Credentials
The common way to package information (content)

EBSI Diploma Use Case

Interoperability - Semantic dimension

Common Data Model

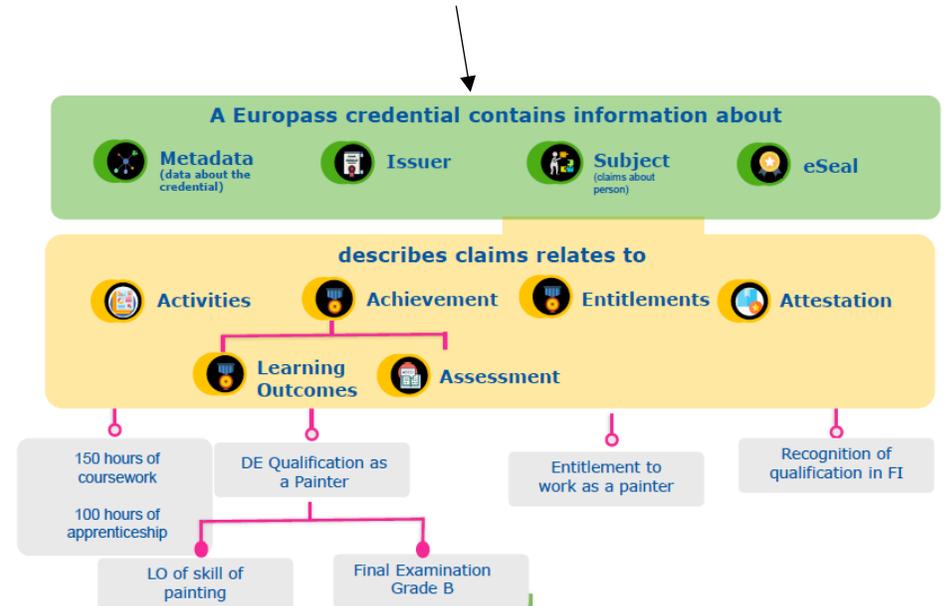
The common way to describe educational credentials (contents)



Verifiable Credentials

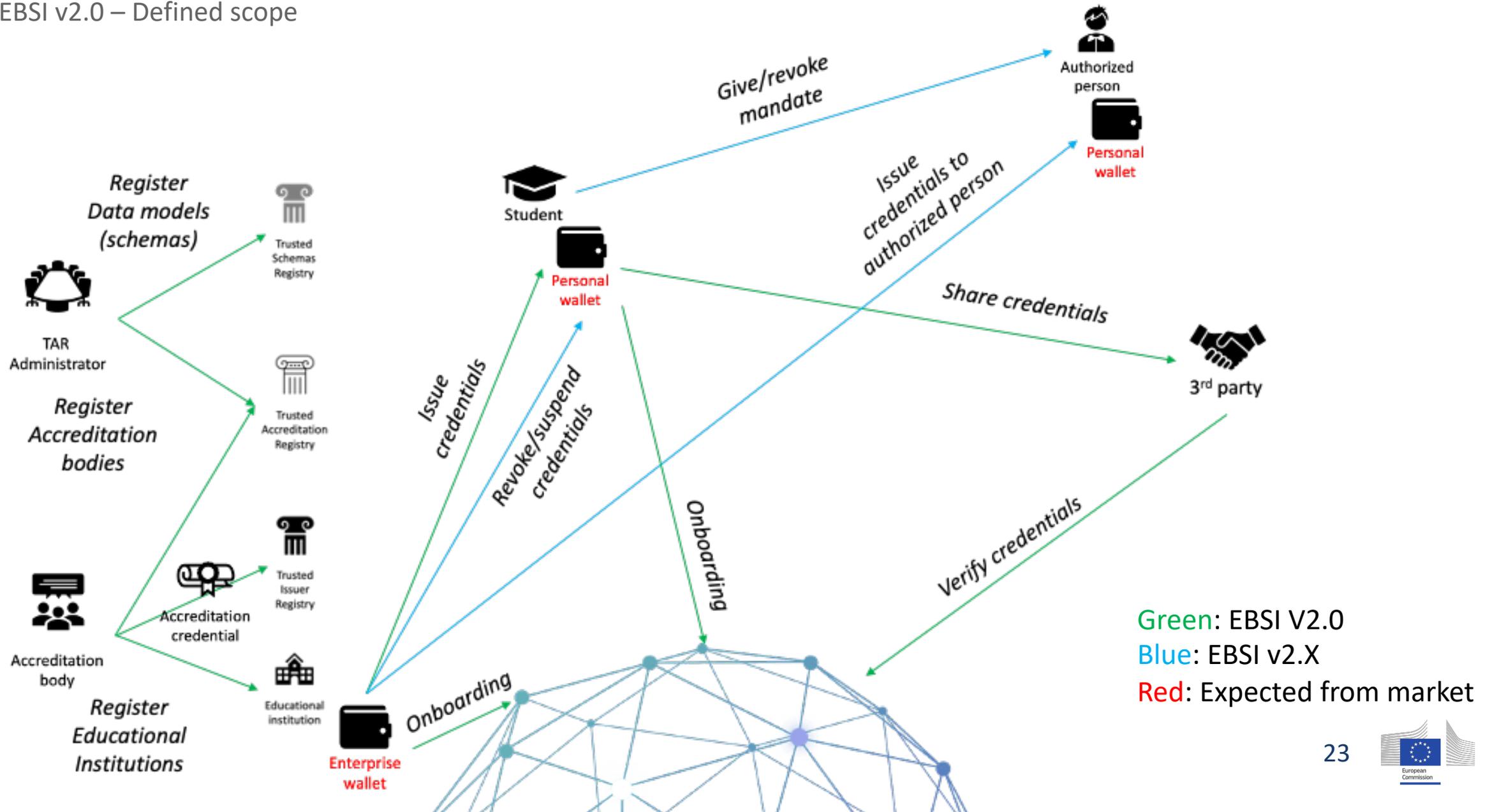
The common way to package information (content)

For example, like Europass is doing, been able to describe Any kind of education.



Diplomas challenges and requirements

EBSI v2.0 – Defined scope

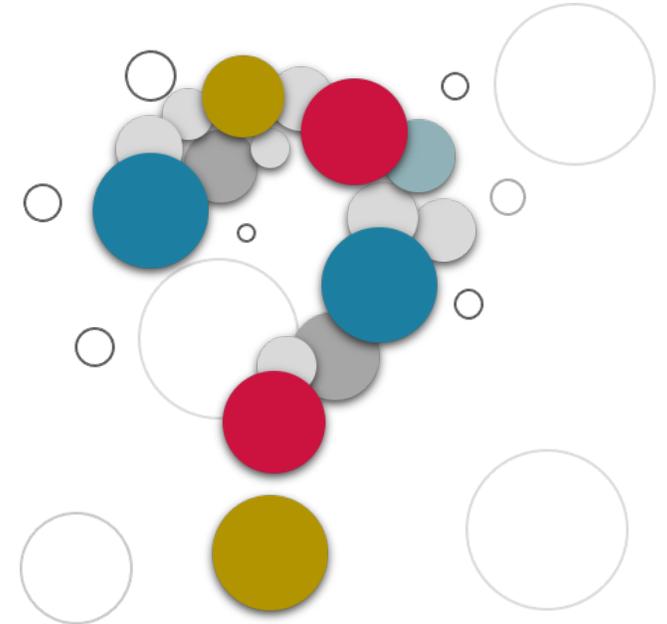


Open questions

All

Open Discussion

- Questions related to EBSI
- Potential interests between ECCA and EBSI?
 - Wallet
 - Student ID, eID
 - ...
- Any other business?



lluisalfons.arino@urv.cat

End of Meeting



CEF Digital
Connecting Europe

