EBSI Deep Dive

Murcia, 23nd November 2023

01

The Challenge

Information is easy to fake,
challenging to verify

Verification matters

EUIPO
EUROPEAN UNION INTELLECTUAL PROPERTY OFFICE

SOCIETAL CHALLENGE

In 2020...

9% of EU consumers (40 million citizens approx.)

were tricked into buying a fake product instead of a genuine one.

This figure represents the size of the combined populations of Belgium, Bulgaria, Greece, Ireland and Portugal.

33% (approximately 150 million in total), **wondered** whether the product they had purchased online was **real or fake**

5.8% of EU imports (**EUR 119 billion**) in 2019 are attributed to counterfeit and pirated goods

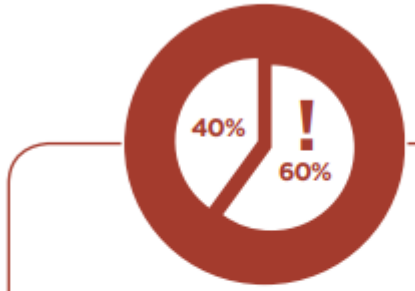
European Commission

Verification matters

NATIONAL STUDENT CLEARINGHOUSE

Your Organization's Reputation on the Line:

The Real Cost of Academic Fraud



In a recent CareerBuilder.com survey, **nearly 60 percent** of hiring managers reported catching fabrications on job applicants' resumes.

Replacing an employee can cost anywhere from **$3,500 to $40,000**.

European Commission

Verification is the antidote for fake

European Commission

When someone claims something, we want to verify it

Claim

I studied economics

True or **False**?

When someone claims something, we want t[illegible] it

Not all proofs have the same value

Claim

I studied economics

You can Google me

I can send you the **PDF**

I can show you the paper document

You can contact my university

Trust

high

low

LISBON SCHOOL OF ECONOMICS & MANAGEMENT
UNIVERSIDADE DE LISBOA

Diploma

PDF

Time

minutes

hours

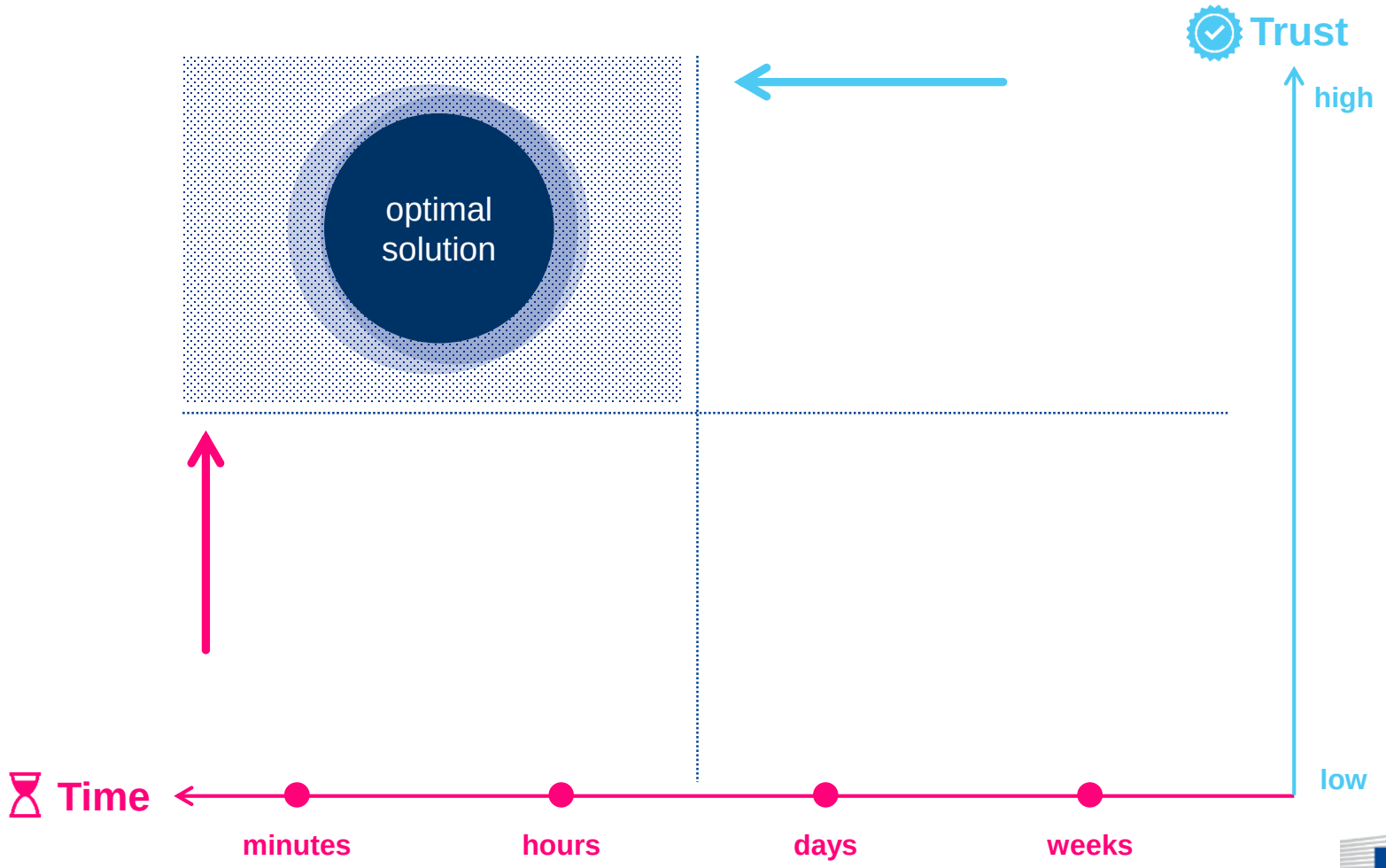
days

weeks

European Commission

When someone claims something, we want to Verify it

Not all proofs have the same value

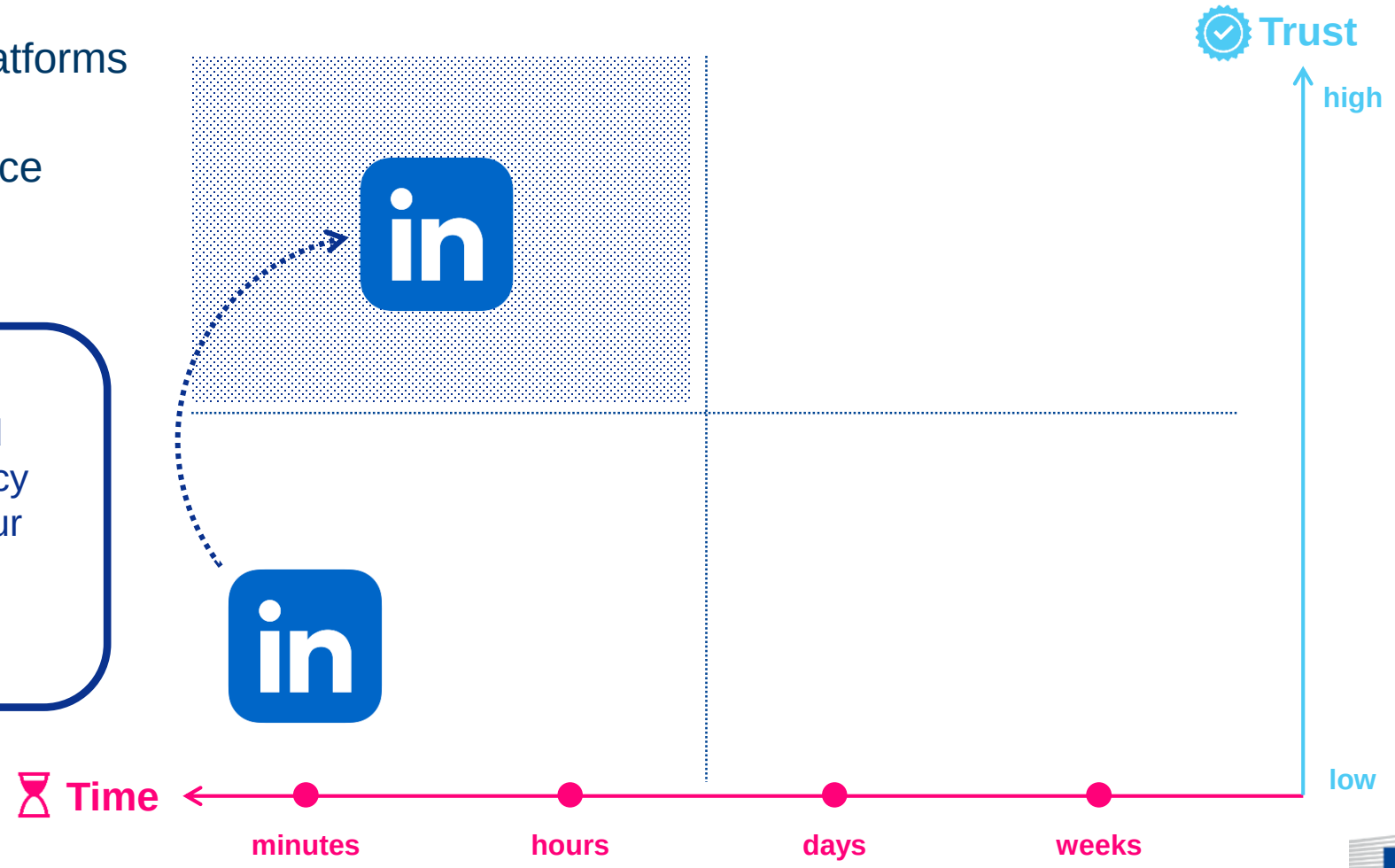


European Commission

Technology can help cut verification time

For example, platforms could provide a verification service

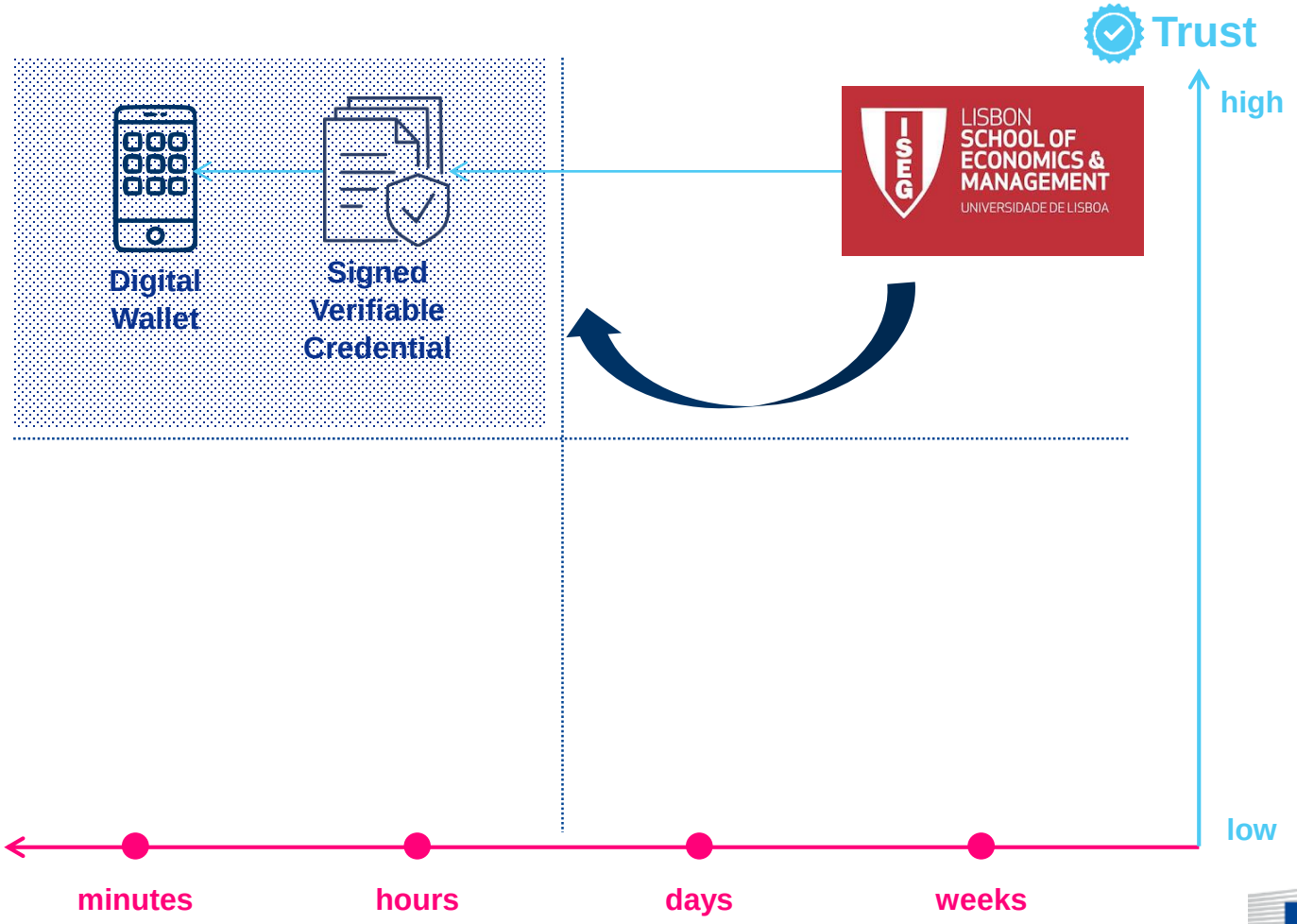
However this would create a dependency on platforms and our data would be controlled by them



European Commission

Today, we can do this without giving our data to a platform

We can use Web3 technologies such as Digital Wallets, Verifiable Credentials and Blockchain to achieve the same



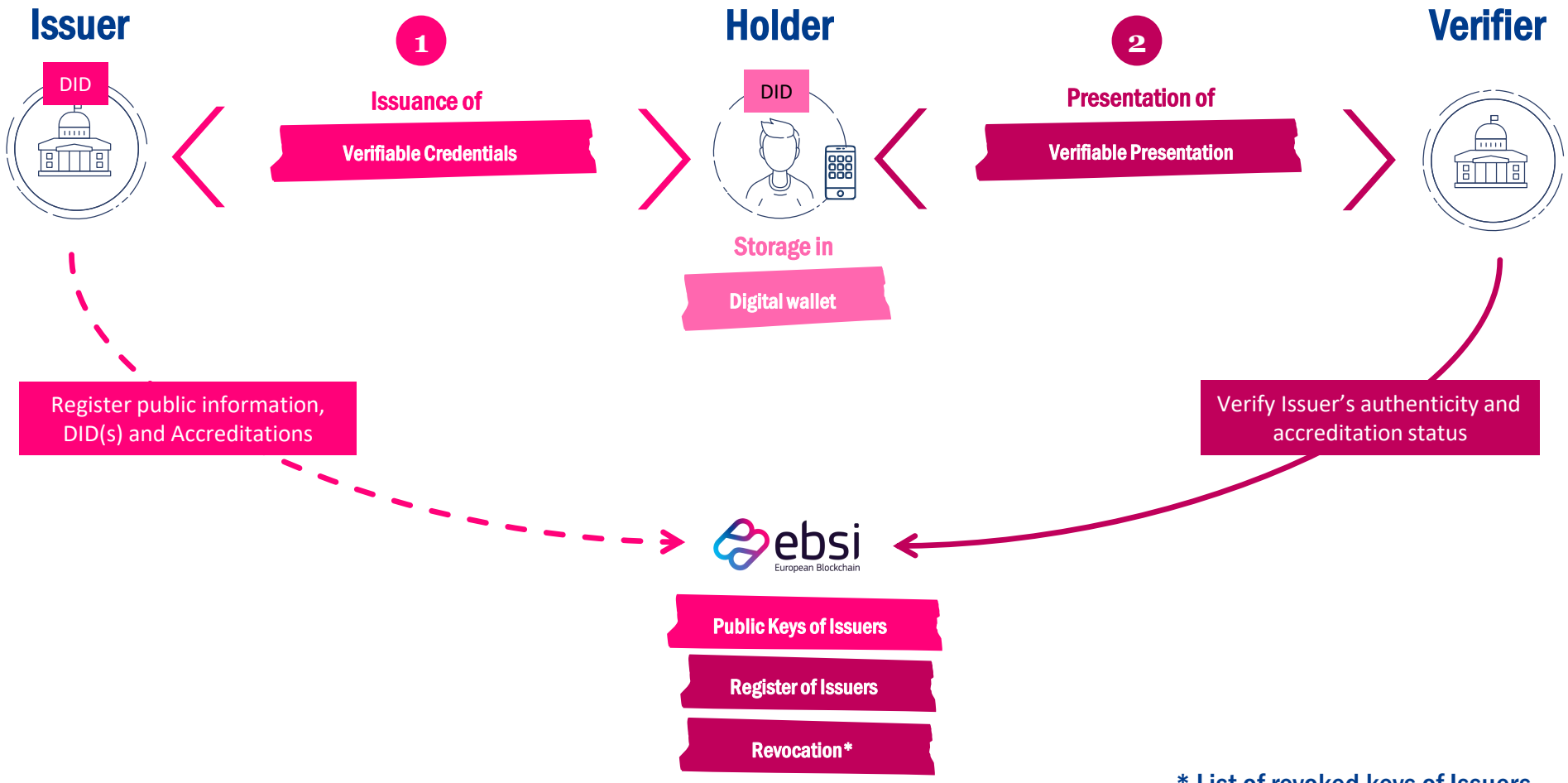
ebsi
European Blockchain

Trusted list of Issuers used to distribute public keys and accreditation info

European Commission

How EBSI helps use cases to simplify the verification?

By establishing a framework for verifiable information exchange

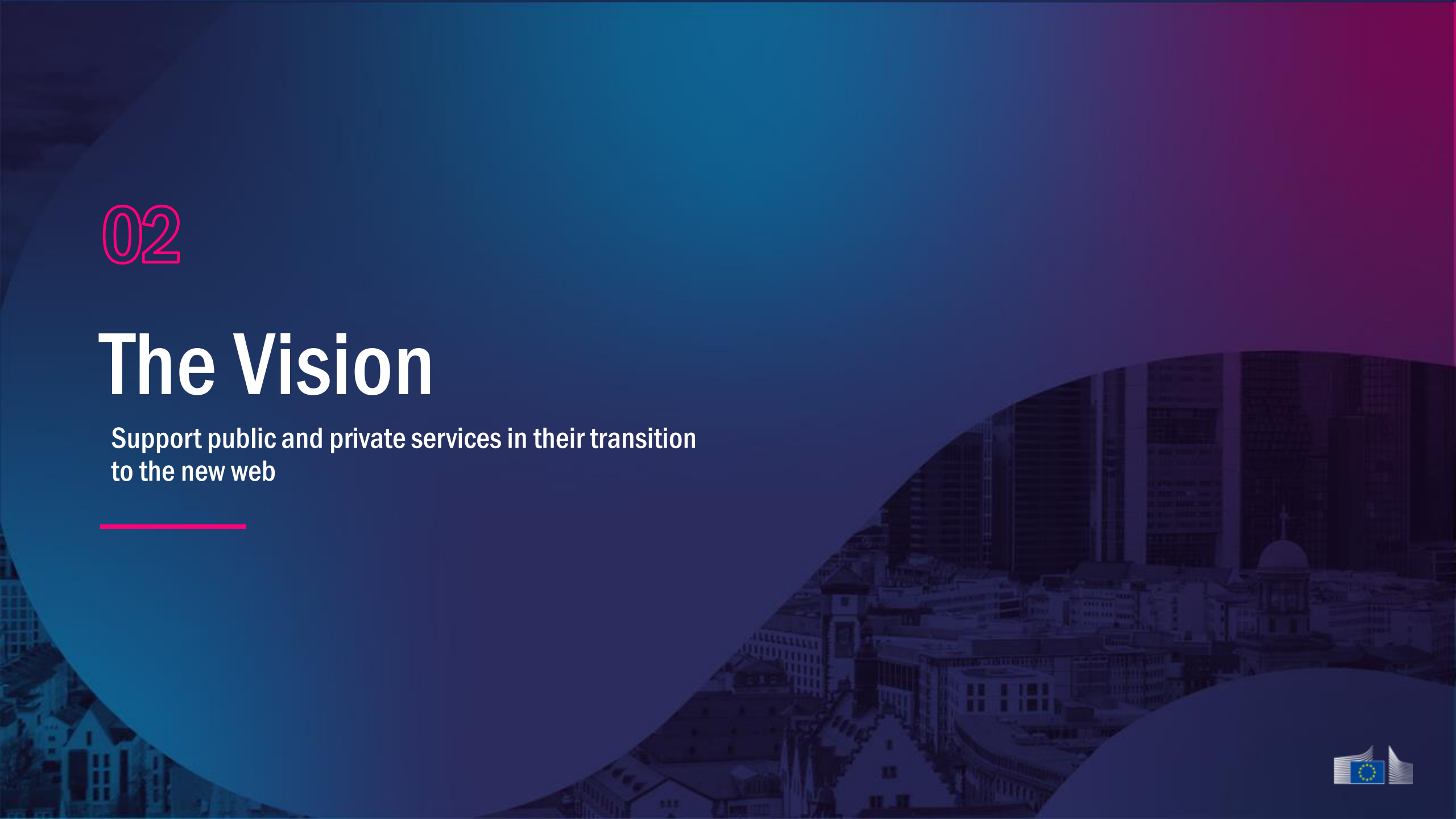


* List of revoked keys of Issuers

02

The Vision

Support public and private services in their transition to the new web



EBSI established a multi-domain trust infrastructure

A unique sovereign pan-European decentralized network

01.

Provide transparent services that everyone can trust.

Open, Transparent and Privacy Preserving information exchange

02.

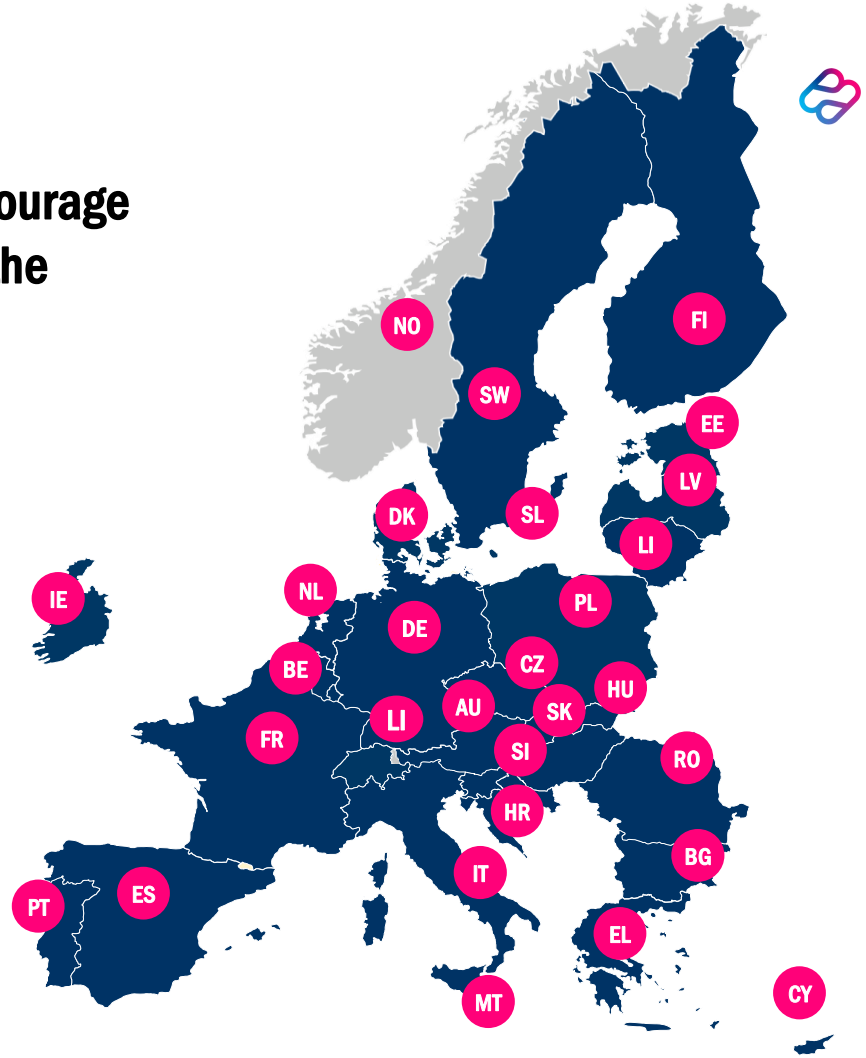
Contribute to data spaces (discourage data monopolies) and support the green agenda.

Eco-friendly and efficient

03.

EBSI Services run in line with EU values and regulations.

EU governed, sovereign infrastructure – public information is always available and can always be trusted and verified



Blockchain is one of the technologies that will pave the way to Europe's Digital Decade

ebsi
European Blockchain

European
Blockchain
Services
Infrastructure

Accreditation management

Verification of Authentic documents

Anti-counterfeiting

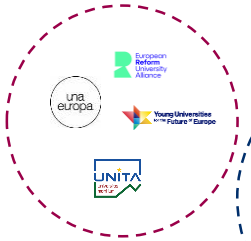
IP Rights Management

European Commission

Numerous use cases are already piloting with EBSI

A growing ecosystem of +350 organisations
From private and public sector (9 different types)
from +30 countries
Mobilised through 9 different “programs”

- 5 University Alliance
- 67 University
- 18 Research Institute
- 106 Public Administration
- 20 Private company
- 2 Non-profit
- 109 IT Provider
- 14 Association
- 7 Accelerator



How does EBSI empower various use cases?

Formal Accreditations
A consortium composed Greek Ministry of Education, the Greek University Network, two Swiss accreditation authorities and the University of Lausanne are working on the **future of formal accreditation** in Europe by enabling seamless applications of students with a degree to a higher education programme in the same field but in another national or European university

My Academic ID
MyAcademicID is a consortium of public administrations, universities and IT providers from Spain, Romania and Ireland, shaping the **simplicity and reliability of cross-border student educational identification** throughout Europe using EBSI. Providing verifiable identification services for students to streamline access to cross-institutional educational resources and facilities.

University Alliances
Una Europa, ERUA and Film EU are three major university alliances in Europe representing +50 universities, +100k students from +15 different countries.

Together, they are pioneering the future of education in Europe using EBSI by enabling **seamless verification of students' affiliations** and offering them easy access to programs, courses, workshops, and resources across partner universities.

Vocational Education & Training
A consortium composed of a Federal Ministry of Education and Research, certification authorities, five universities from Germany, France, and Sweden as well as two private companies.

*Together, they are pioneering the **future of vocational education** in Europe using EBSI by facilitating the issuance, acceptance, and recognition of all types of vocational, educational, and training certifications across Europe.*

How does EBSI empower various use cases?

Public Services

Together representing +5 Spanish Public Law entities, Spanish Regional Governments, and +3 IT providers, this consortium is **shaping the future of National Public Administration** in Europe by helping citizens effortlessly gain access to local resources and facilities between regional and national public administrations in Spain.

EUIPO

EUIPO has launched the ground-breaking European Logistics Services Authentication initiative for products within the global supply chain (using the European Blockchain Services Infrastructure). his initiative is designed to **ensure product authenticity by promoting information sharing among the participants in the supply chain** within a secure environment using blockchain technology.

EUROPASS

Together with EUROPASS we are shaping the **evolution of the European Learning Model and the EUROPASS student wallet** that will give students a seamless user experience when studying abroad or proving their educational achievements.

ESSPASS

The European Social Security Pass (ESSPASS) is a project designed to make it easier for individuals **to exercise their social security rights when they are in another European country**. This initiative is part of the European Pillar of Social Rights Action Plan.

INPS - National Institute for Social Security (Italy)

Digitalization of the **mandate that enable authorized public bodies to act on behalf of a citizen** (i.e. to request a grant).

03

The Offer

Verifiable information exchange framework

What EBSI offers?

EBSI offers a complete VC exchange framework and supporting services

New way to exchange information

- Complete VC exchange framework
- VC exchange profile

Data models and Schemas

- Data models for attestation & accreditations
- Re usable data schemas

Trust Models

- Issuer trust model
- Verifier Trust model

Revocation Framework

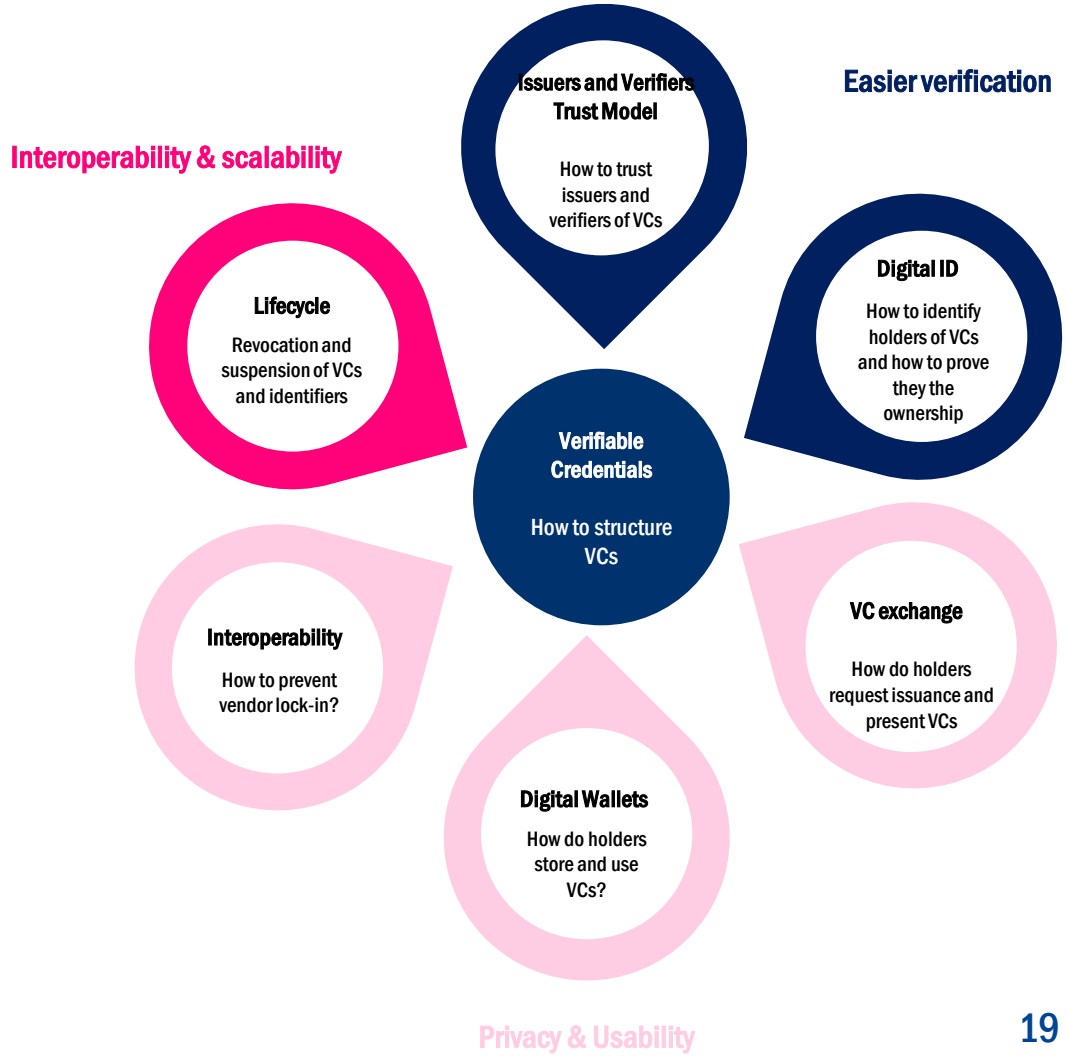
- Revocation Framework

Interoperable wallets and issuer/verifier solutions

- Stable Specifications
- Conformance Testing

Decentralised Infrastructure

- Trusted Registries



European Commission | ebsi

3.2 EBSI specifications for a VC profile

EBSI specifications for Verifiable Credentials exchange

EBSI collected UC requirements and over the last three/four years, together with the UC representatives (eSSIF, Diploma, DG-EMPL Europass, TAXUD, EUIPO, Traceability UC, DG-EMPL ESSPASS) defined a profile for a W3C VC exchange.

EBSI has been working on **VC exchange profile** based on

- W3C Verifiable Credentials
- W3C Decentralised Identifiers
- OpenID4VC family of specifications

All specifications cover a range of options (VC format, signature format, identification/authentication, issuing and presentation profiles), hence a profile that meets the functional and business requirements must be defined.

Short summary of the profile

- JSON-based VCs (compatible with SD-JWT)
- ready to be compatible with **JSON-LD** if the context is defined by Use Cases
- **JAdES** and JWS e-seals/e-signatures : minimise the potential interoperability issues
- EBSI DID method for Legal Entities, simple public-key based DID method for Natural Persons
- OpenID4VC profile for B2B/G2B and B2C/G2C VC issuance and presentation for cloud and mobile wallets

EBSI defines profiles for B2B and B2C VC exchange

- **B2B VC exchange** profile required for Verifiable Accreditations and other organisational credentials – no B2B profile has been defined elsewhere
- **B2C VC exchange** profile for Natural Person VC issuance and presentation
  - **Verifiable Presentation profile is similar to the ISO mDL 18013-7 proposal**
- **All the profiles have been designed to be interoperable with the existing eIDAS "v1" infrastructure (and v2, when in place)**

- Both profiles build on OID4VC specifications
- Applicable to server/cloud or mobile wallets
- Pluggable authentication and identification

- Based on EBSI's **stable specifications release cycle** and **conformance testing framework** (next section) .Namely, many of the specifications are drafts and are still subject to change

European Commission | ebsi

3.4 Trust Models

EBSI Trust Model : understanding the roles

Distribution of roles per Member State and per Use Case

MS A

Mobile

MS B

Authorizing organizations/Trusted Accreditation Organisation (TAO)

Gov. Entity

Registers issuers of educational credentials in the Trusted Register of Universities

Issuer

University A

Issues educational credential upon the request of the student

Holder

Student

Configures the wallet, requests the issuance of educational credentials and share it with university / employer

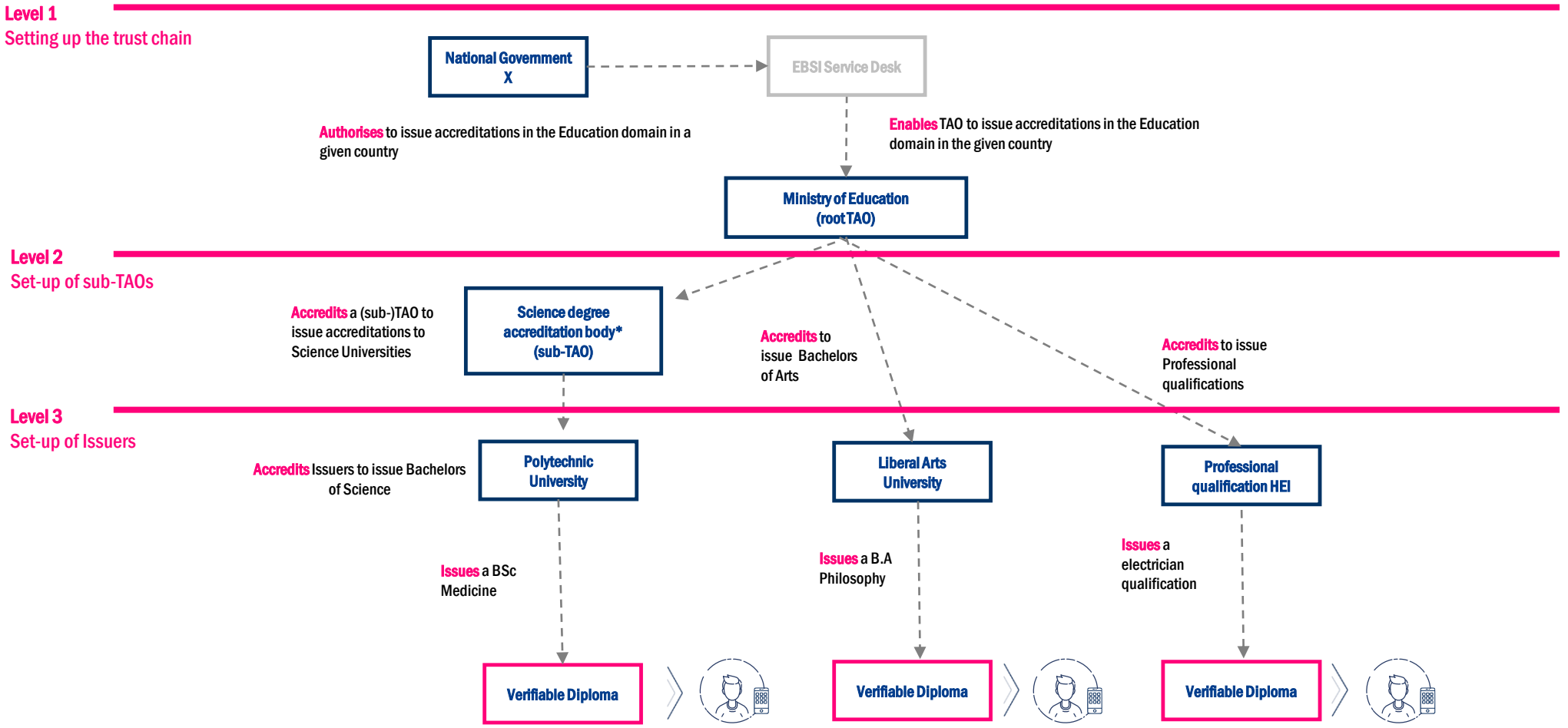
Verifier/Relying party

University B

Company

Verifies the educational credentials shared by the student

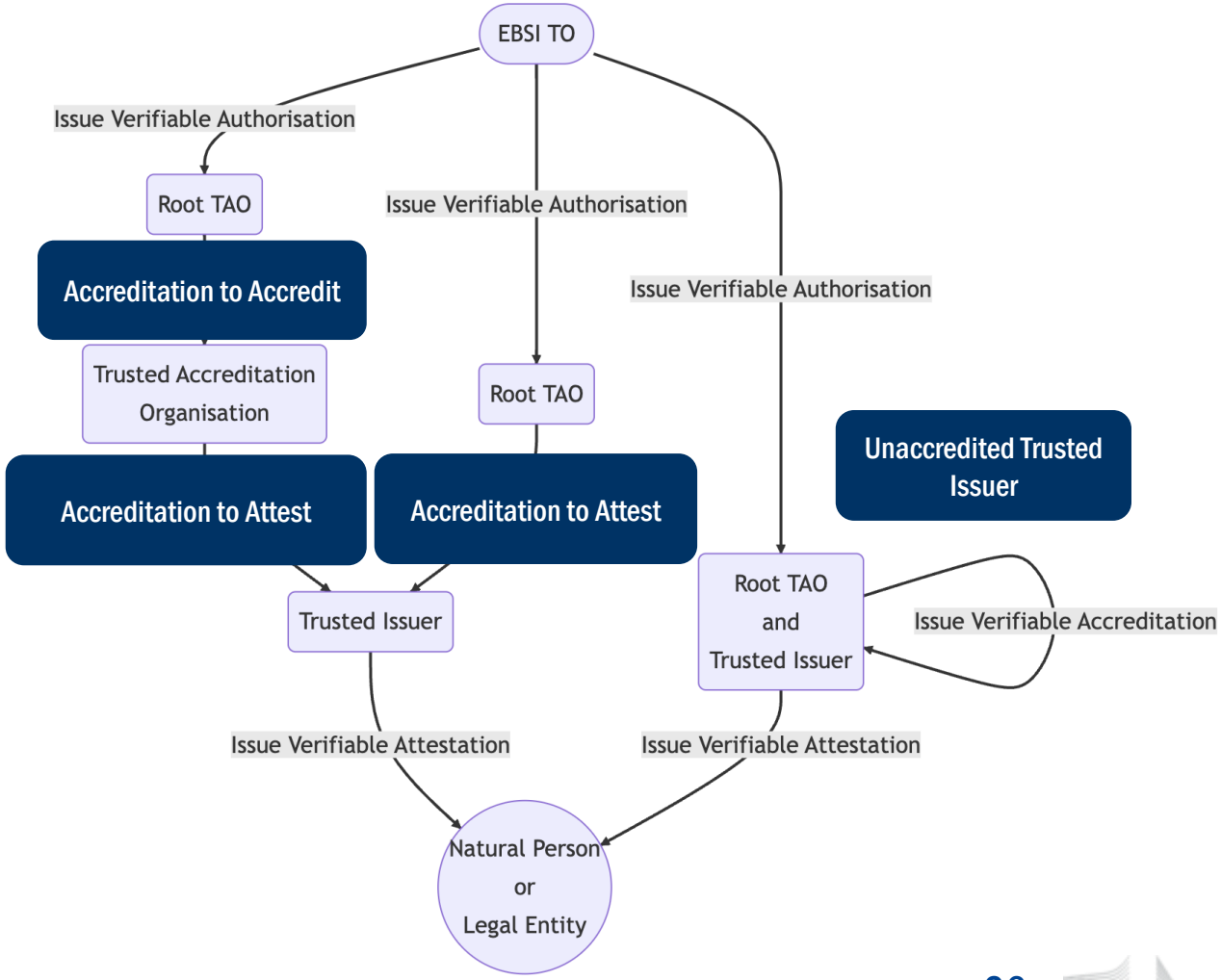
A trust model ready-to-use to support the Governance of an SSI ecosystem



Issuer trust model overview

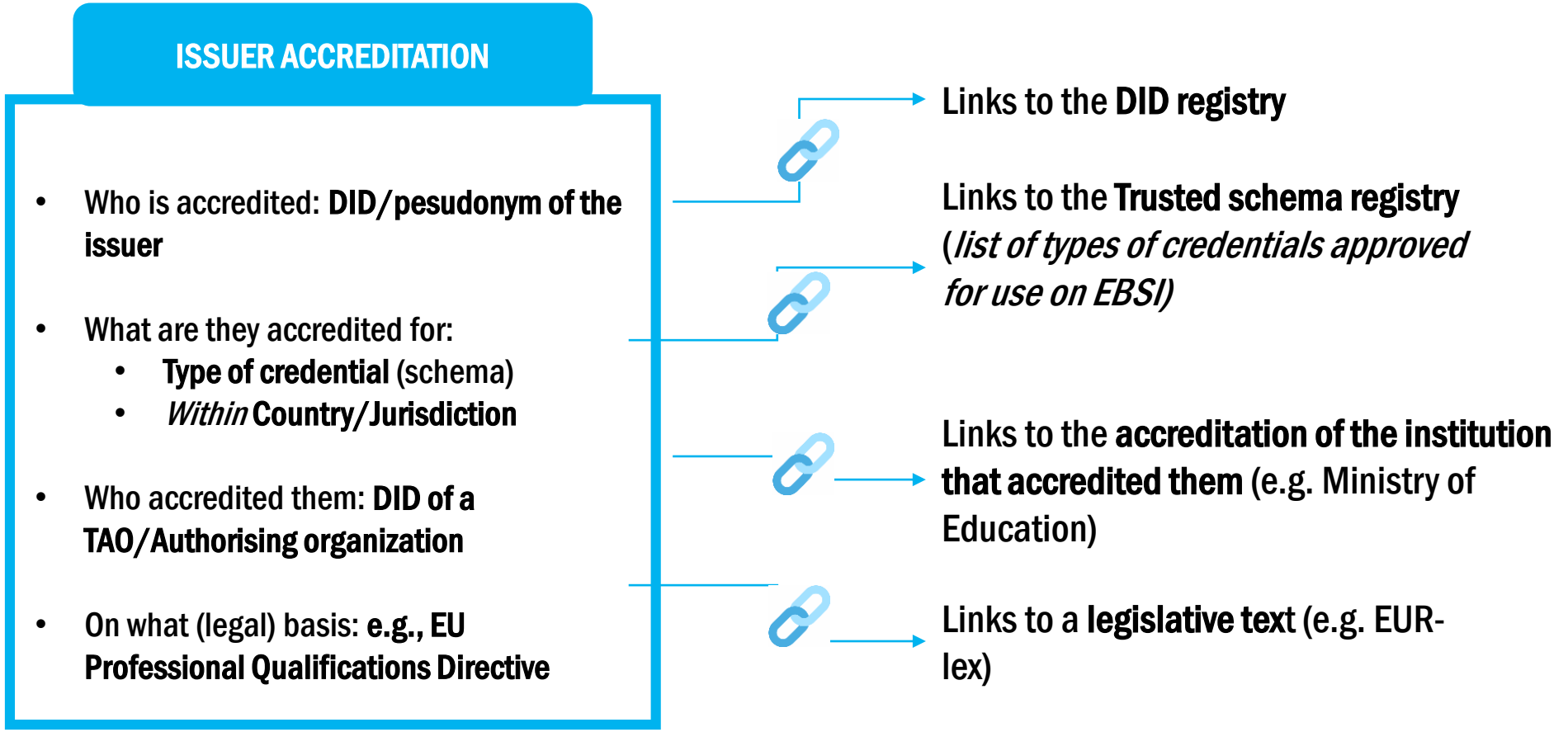
Verifiable Credentials issued to different actors

- **EBSI TO** EBSI Technical office is responsible for the technical onboarding
- **Root TAO** is responsible for the domain definition and onboarding of the TAOs and TIs it is responsible for
- **TAO** is responsible for onboarding of other TAO and TI, according to its accreditations
- **TI** are responsible for issuing Verifiable Attestations to Natural Persons or Legal Entities



https://api-pilot.ebsi.eu/docs/specs/trust-model/issuers-trust-model

What does an Issuer accreditation on the ledger contain?



A flexible model that **accredits Trusted Issuers, but also can represent any accrediation**: for example, the conformity assessment report (CAR) issued by an accredited conformity assessment body (CAB) for QTSPs. The CARs confirms that the QTSP provide a QTS that fulfill the requirements laid down in the eIDAS Regulation.

What information do EBSI store on the EBSI ledger?

Information about entities

Matching keys and identifiers

DID registry

Identifiers (DIDs) and keys (to verify) of:

Trusted issuers

AND Trusted accreditation organisations

PID/EAA Providers registry
Authentic Sources registry

Trusted Issuers Registry

Verifiable Accreditations

- mandates to issue a specific type of credential

OR mandates to accredit issuers

Relying parties registry

Verifiers registry

Verifiable Accreditations

- mandate to verify a type of credential

Redy to test with use cases

Information about credentials

Attestation Schemas

Trusted schema registry

A list of recognised and trusted Verifiable Credential types (schema) – e.g. European Learning Model for Diplomas, EduPerson, MyAcademicID, etc.

Revocation capabilities

Revocation

Points to where the revocation information is. Privacy preserving: **only contains endpoints**.

Information about Wallet providers

EUDI Wallet providers

Wallet providers registry

Verifiable Accreditation for Wallet providers

IT Providers conformance with EBSI

in EBSI roadmap

We never store personal data or any information about ***persons*** on the blockchain

European Commission | ebsi

3.5 Trusted Lists implemented by a decentralized network

Our philosophy: facilitate the adoption and ensure an easy integration

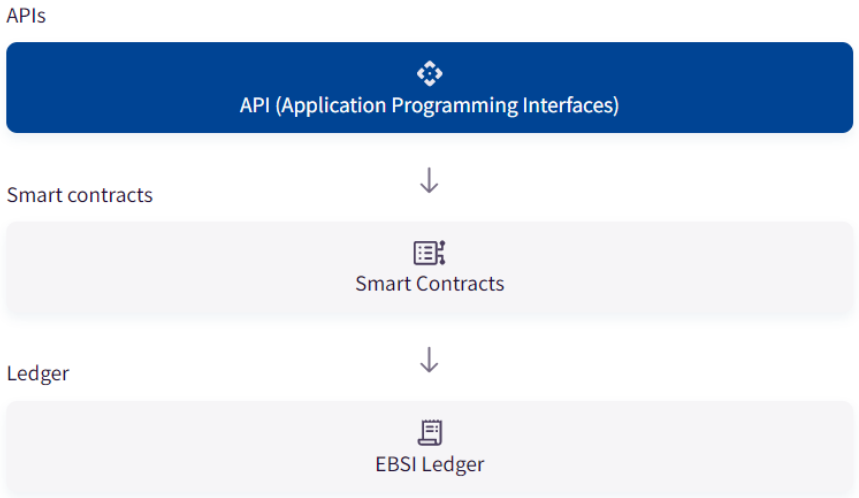
EBSI network is providing HTTP APIs for interaction

EBSI is well-aware that an easy integration is key to ensure adoption.

In that sense, actors "**do not have to speak blockchain**", all interaction with ledgers to;

- Deploy business domain governance
- Onboard Issuers/Attestation providers or Verifiers/Relying Parties
- Register information for verification
- Obtain information to verify digital credentials

All interactions are done through **HTTP APIs.** It can not be easier.

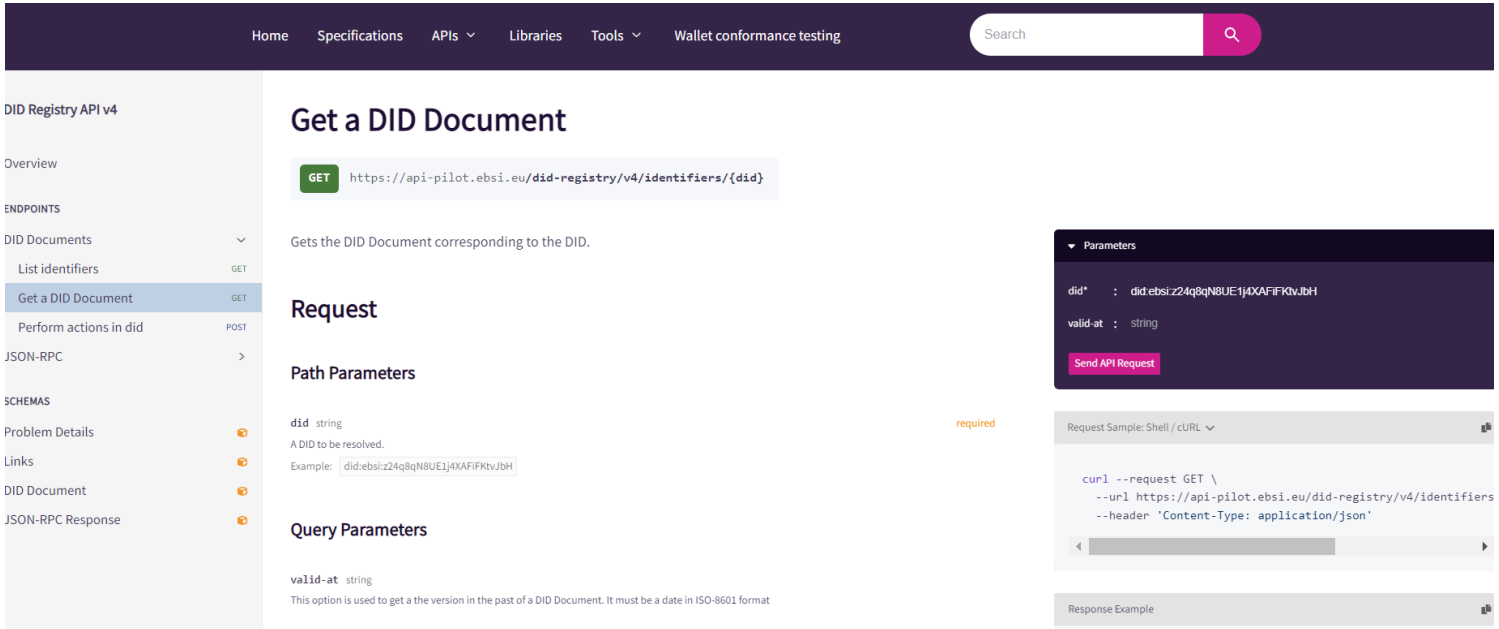


Our philosophy: facilitate the adoption and ensure an easy integration (2)

Interactive set of OpenAPIs

EBSI work does not finish in drafting specifications and in providing HTTP APIs easy to integrate.

EBSI is also providing a **detailed website to facilitate the adoption to IT providers by including a whole set of open and interactive APIs.**



So…why ledgers?

Are ledgers justified because you don ´t trust on The Trusted List ™?

Short answer: NO

Long answer: next slides.

Implementation posibilities for a Trusted Lists

Blockchain supports a resilient, tamper-proof trust model – with low energy consumption thanks to specific consensus algorithm based on proof of Authority (EBSI is not a crypto blockchain)

Distributed static XML files

Defined in the Commission Implementing Decision (EU) 2015/1505 and ETSI TS 119 612

Current implementation of Trusted lists

Distributed data base

Business requirements and security **properties can be added to enhance current model of Trusted Lists**: syncronization, replication, traceability, accountability....**until we reach a Distributed Ledger technologies.**

A Hybrid approach.

Distributed Ledgers Technologies

Supported by EBSI and rely on a network provided by Member States

EBSI decentralized network

Implementation posibilities for Trusted Lists

Blockchain supports a resilient, tamper-proof trust model – with low energy consumption thanks to proof of Authority

Distributed static XML files

Integrity
Authenticity
Proof of existence

Distributed database

Integrity
Authenticity
Proof of existence
Distribution and replication
Resilience
High performance

Distributed Ledgers Technologies

- Integrity
- Authenticity
- Proof of existence
- Distribution and replication
- Resilience
- High performance
- Accountability
- Chronological set of data records
- Access management provided in an accountable way and incorporated in the protocol (SC)
- Information can not be deleted / only appended
- Integrity / tamper proof protection by a network, not single nodes

Current implementation of Trusted lists

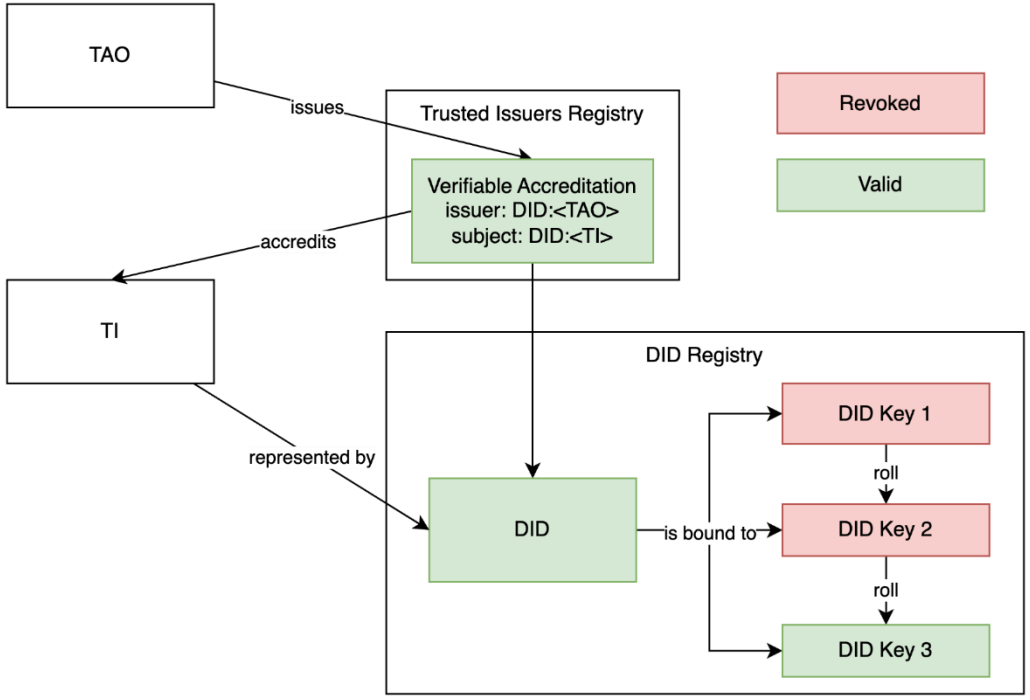
A Hybrid approach.

EBSI decentralized network

Trusted Lists - Benefits from a Distributed PKI model based on Ledgers

Ledger as a chronological set of data records keeps the information ”forever”

Key rolling does not invalidate a Verifiable Accreditation



Benefits of ledgers as a source of immutability and chronological sequence

- Information cannot be removed or modified
- It ensures chronological sequence of events
- Reduces the complexity of long-term signature verification

- **e-Signatures/e-Seals** ensures **authenticity, integrity and non-repudiation**
- **Timestamp** ensures the **proof of existence**

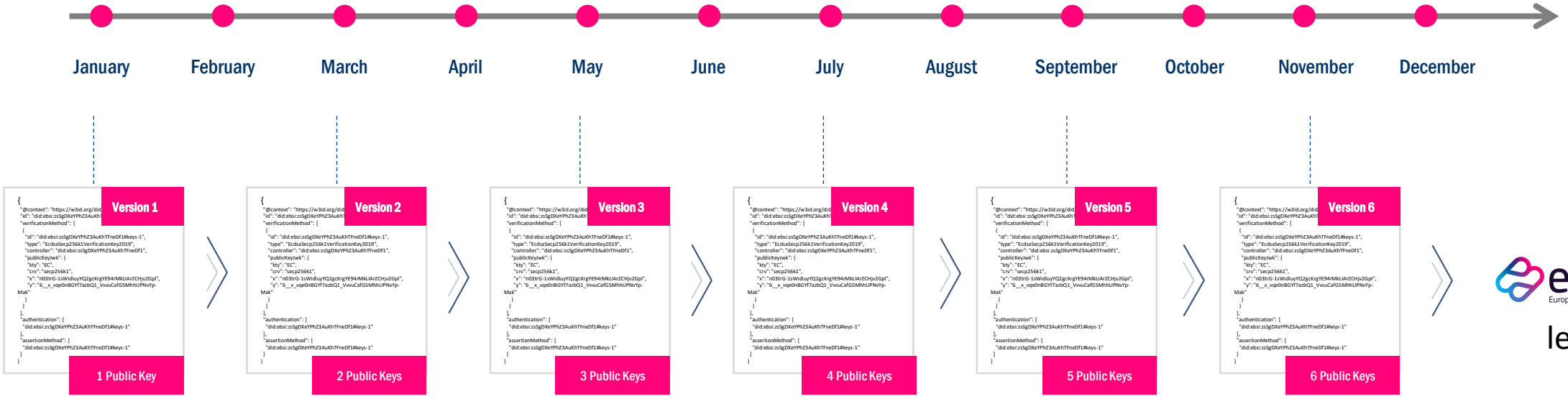
BUT

- **Ledgers** provide **immutability :** it ensures that the information cannot be removed or modified
- **Ledgers** provide a chronological sequence **that ensures verification of data in the past**
- A model based on a **Distributed PKI (Verifiable Attestations and DID Documents)** implies that **if a key is compromised, issuers minimise the impact as less Verifiable Credentials will be signed with the same key. In a key rotation, the Accreditation remains as it is linked to the DID**.

A scalable system for frequent, self managed Issuer key rotation

Once accredited, EBSI enables Issuers to manage their keys, according to EBSI's DID method, independently of the TAO/Authorising organisation

By rotating/updating keys frequently, Issuers **minimise the impact of an eventual compromise of their (private) key as less Verifiable Credentials will be signed with the same key**. Technically speaking, **the use of DIDs/pseudonym(s)** and DID documents **enables Issuers to rotate their keys**, i.e., to update their cryptographic keys regularly (e.g. every other month) **without impacting the Verifiers** as they can easily retrieve the right version of the DID document from EBSI. This enables a much **smoother and secure management of keys in large ecosystems**. Issuers can have multiple active keys bound to their DID.



In this case, the Issuer decides to update its keys every other month. This is done by registering a new version of the (Issuer's) DID document on EBSI. Each version will therefore contain an additional public key. **The Verifier knows the DID of the Issuer and therefore it can resolve the latest DID Document from EBSI with the updated keypair.**

European Commission | ebsi

3.6 EBSI credential status framework

Our revocation criteria

Adheres to the GDPR.

Prevents holder traceability.

Respects the privacy of holders.

Does not store or process personal data on the EBSI blockchain.

Prevents issuers or 3rd parties linking revocation checks with the holders.

What types of credentials are we trying to revoke?

In EBSI, there are different types of “claims” (or “attestations”) that need to be revoked, be it for natural persons or legal entities

LEGAL ENTITIES

Verifiable Authorisation

- give **Legal Entity** access to the infrastructure
- give **Legal Entity** authorisation to start a trust chain

Verifiable Accreditation

Legal entity accreditation, describing **rules & boundaries for legitimate VC issuance**

PERSONS

Verifiable Attestation

Statements or claims about holders – Natural Persons

EBSI defined three revocation method families

In a privacy-by-design service, different approaches are possible in EBSI when the Issuer is managing the Verifiable Credential status

Binary valid/invalid status

It is a simple yes/no format without additional metadata. Privacy by design principles.

Properties
- herd privacy
- small in size

Limitations
- No additional metadata (date, reason) is provided, which could be needed for certain domains
- State changes can be tracked

Status with VA metadata

It contains VC status with additional metadata, such as reason, date, and other.

Properties
- herd privacy
- per-VC metadata

Limitations
- State changes can be tracked

Status with VA metadata and limited visibility

It contains VC status with additional metadata, such as reason, date, and other.

Properties
- herd privacy
- per-VC metadata
- State changes cannot be tracked

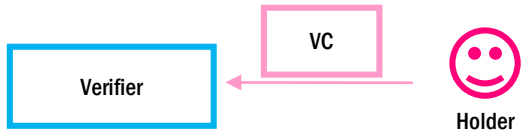
Limitations
- None identified so far

Strategies to manage the status of Verifiable Attestation

Natural Person Verifiable Attestation revocation/suspension options possible today

Short-lived Verifiable Credentials

Case A: Holder obtains a fresh VC.



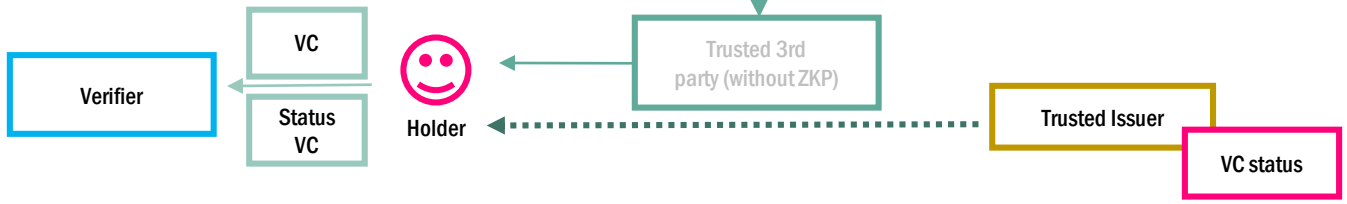
Short-lived VCs don't require suspension/revocation infrastructure.

Long-lived Verifiable Credentials

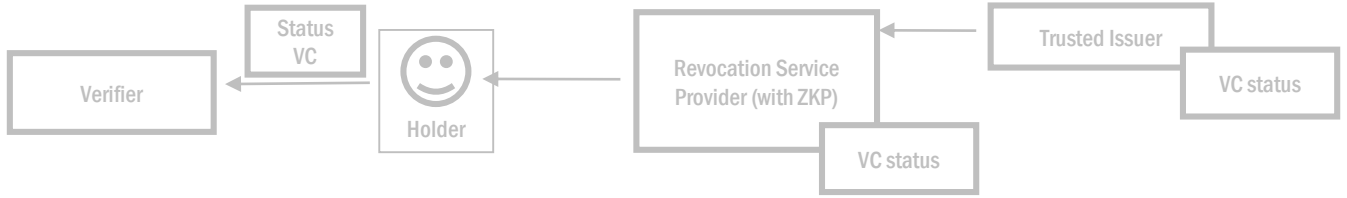
Case B: VC status is obtained directly from the Trusted issuer

Case C: VC status is obtained from the Trusted issuer via EBSI

Case D: Holder obtains a **status VC** from the issuer or a 3rd party



Case E: Holder obtains a **status VC** from a Revocation Service Provider



Retrieval methods

Five retrieval methods are possible

VC Status Strategy	Description	Legal Entity	Natural Person	Information revealed
Short VC lifetime*	Issuer issues VCs with a short lifetime, e.g., hours, days. Two strategies are possible: a) Re-issuance of the original VC with new duration b) Issuance of an additional one-time status VC	✓	✓	The Issuer learns what VC is presented and when by a holder. It doesn't learn about the Verifier.
VC Status managed in a Trusted Registry	When a reliable history of the VC status is required, the information can be stored in the corresponding Trusted Registry. Applicable only to Legal Entities.	✓	X	No information is revealed to the Issuer.
VC Status managed by the Issuer - direct retrieval*	The Trusted Issuer hosts VC status information, and verifiers retrieve the VC directly from the Trusted Issuer.	✓	✓	The Issuer learns which Verifier and when one of the VCs is received in the revocation or suspension list.
VC Status managed by the Issuer - retrieval via the Holder	The Trusted Issuer hosts VC status information; however, Holder fetches and presents the revocation/suspension information.	✓	✓	The Issuer learns what VC is presented and when by a holder. It doesn't learn about the Verifier.
VC Status managed by the Issuer - retrieval via EBSI	The Trusted Issuer hosts VC status information; however, the verifiers retrieve the information via EBSI node. This way, issuers never learn who asked for the VC status information.	✓	✓	No information is revealed to the Issuer.

Today's landscape

What are the criteria we use for the analysis?

Criteria

Privacy

- The status record must not serve as globally unique identifier or correlator of the natural person
- Access to the status record alone must not reveal any information about the natural person
- Access to the status record must not allow the issuer or anyone else to track the natural person's use of the VC

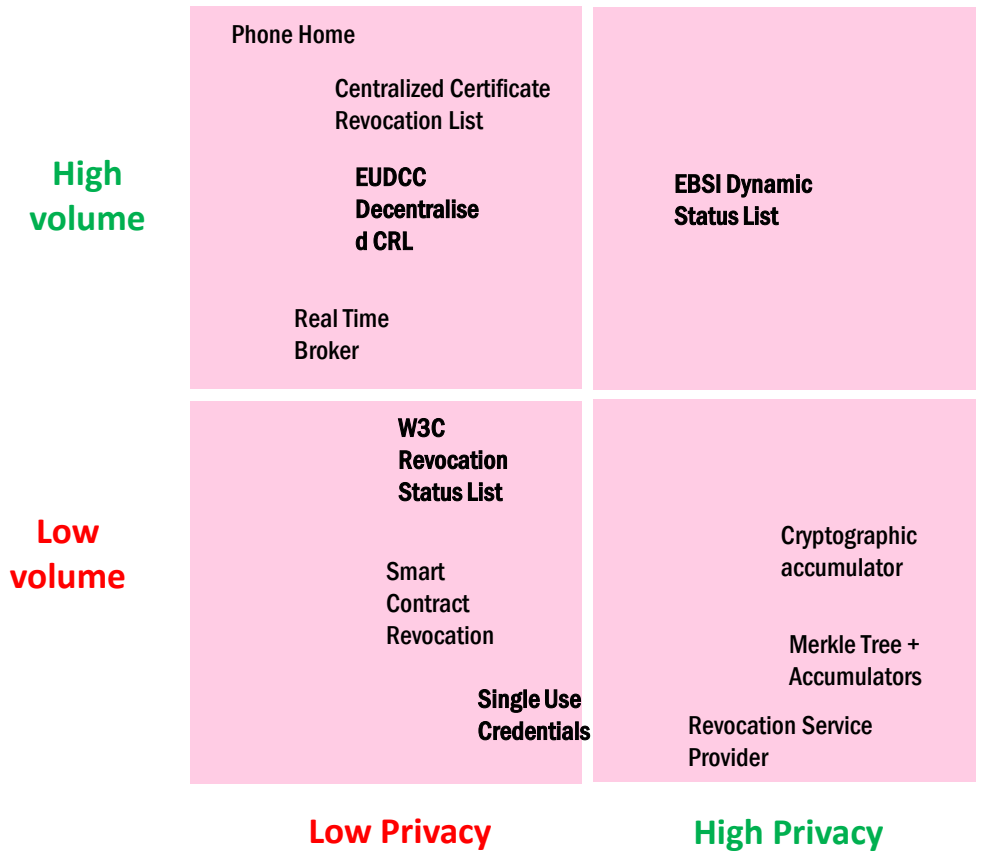
Erasure & Control

- The natural person must be able to view and request erasure of their own status
- The issuer must be able to modify or delete the status record (and thereby revoke the credential)
- In some jurisdictions, a third party (such as a court of law) must also be able to modify or delete a status record

Scalability

- The solution must be proven to scale to hundreds of millions of status records
- Holder and Verifier can be both online

Today's landscape



Revocation/Suspension formats marked with bold are supported/acknowledge today

To find out more about EBSI

Follow us & stay in touch

Find us at...

Our website: ebsi.eu

Twitter: @EU_EBSI | Linkedin: EBSI

EU_EBSI@ec.europa.eu

Or contact our HelpDesk