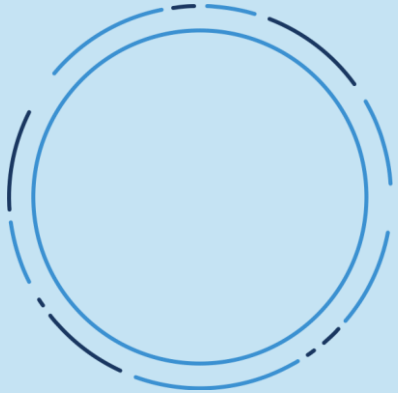
Joining forces towards European digital credentials

30 November 2021 – EBSI Evangelisation deck

Index

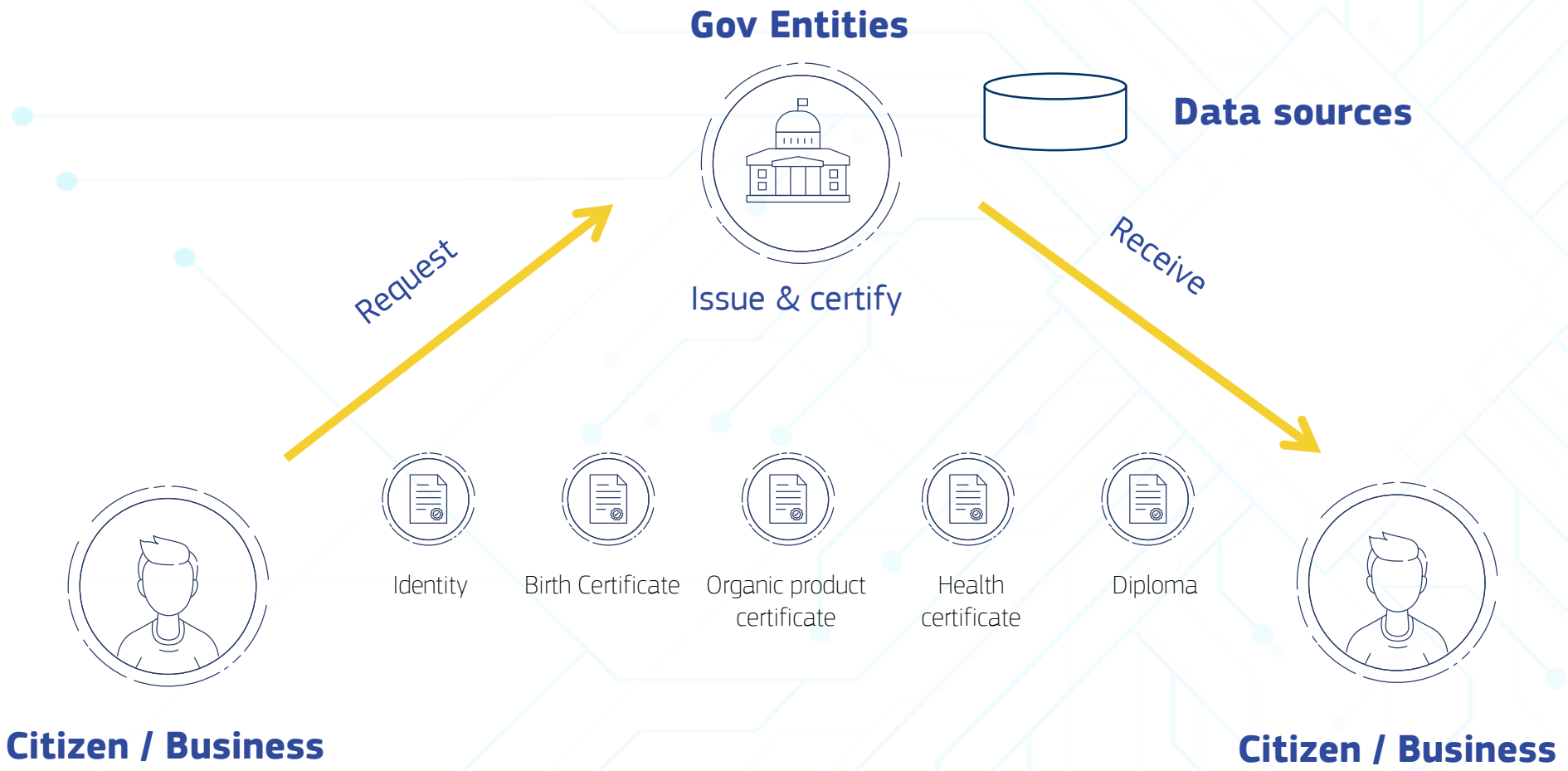


Context

A new way of exchanging information

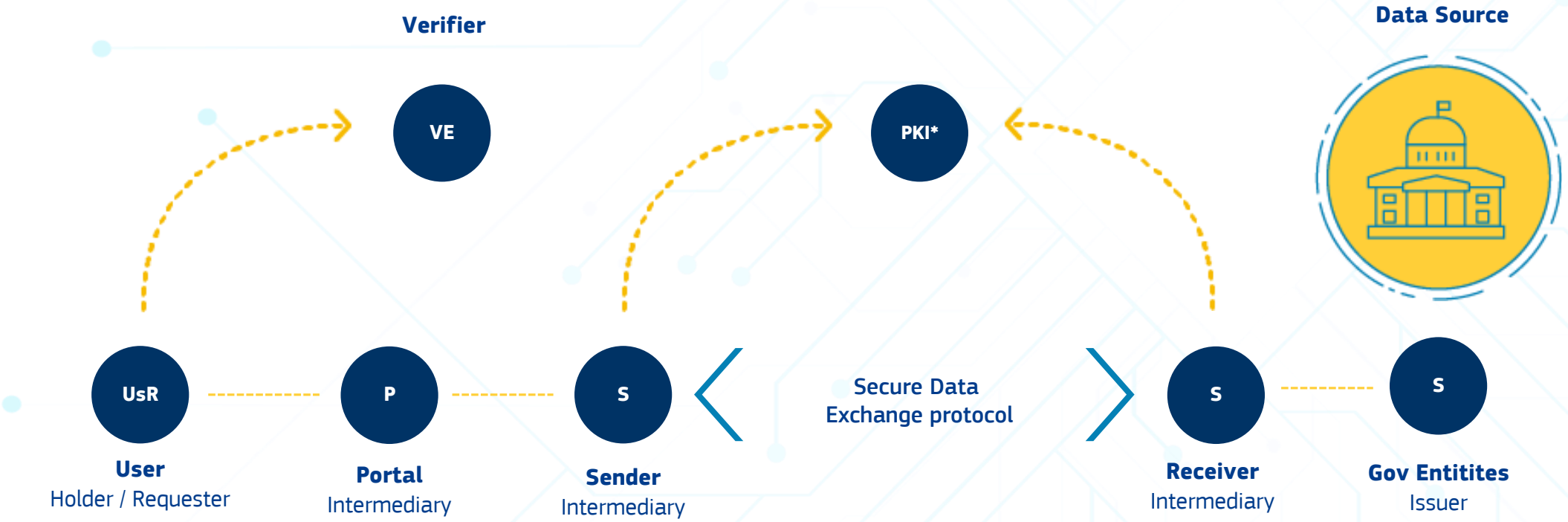
Governmental entities are issuers of documents.

Governmental entities are issuers of documents used as evidence in different life events.



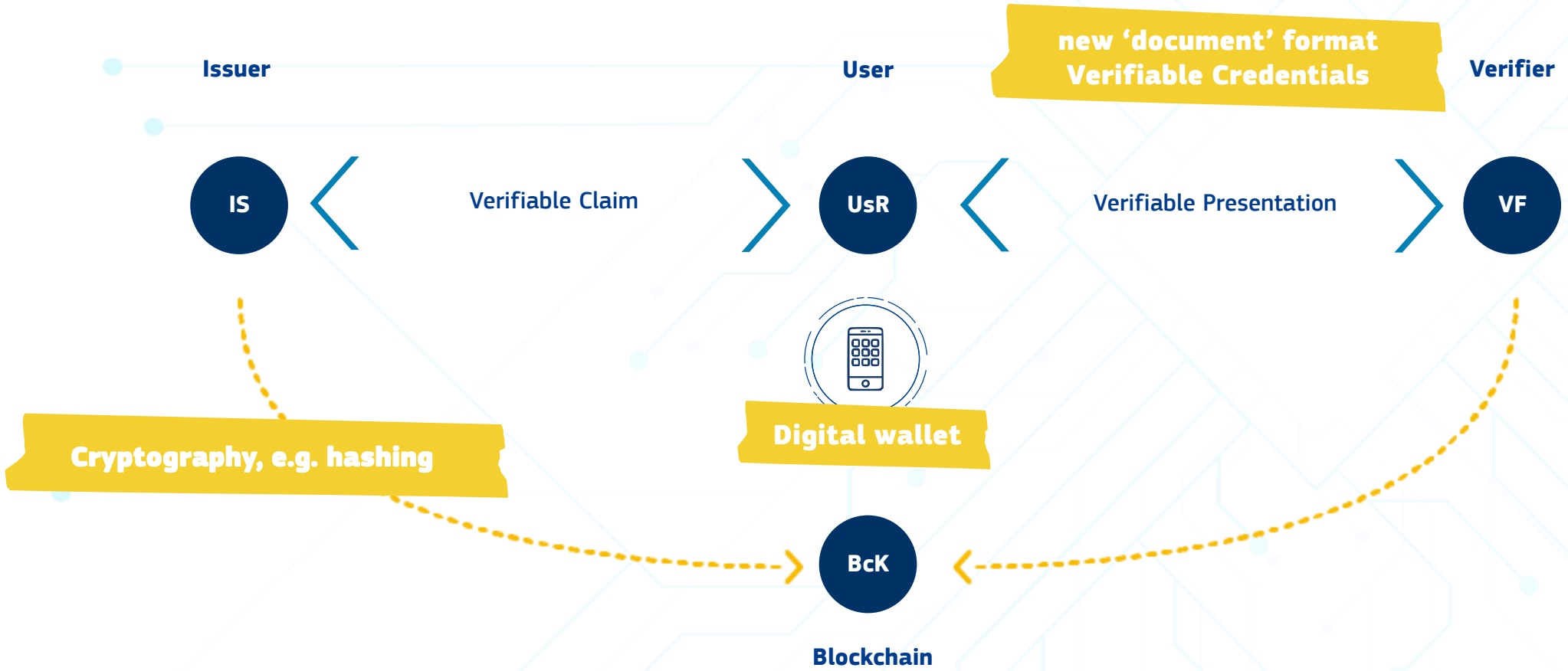
Traditional data sharing pattern

In the classic pattern of information sharing, the citizen, or the verifier of the information, receives the information directly from the authentic source in real time (e.g. a population register, a land register or a business register). This pattern creates and maintains a number of intermediaries that ensure that the exchange of information can be trusted.



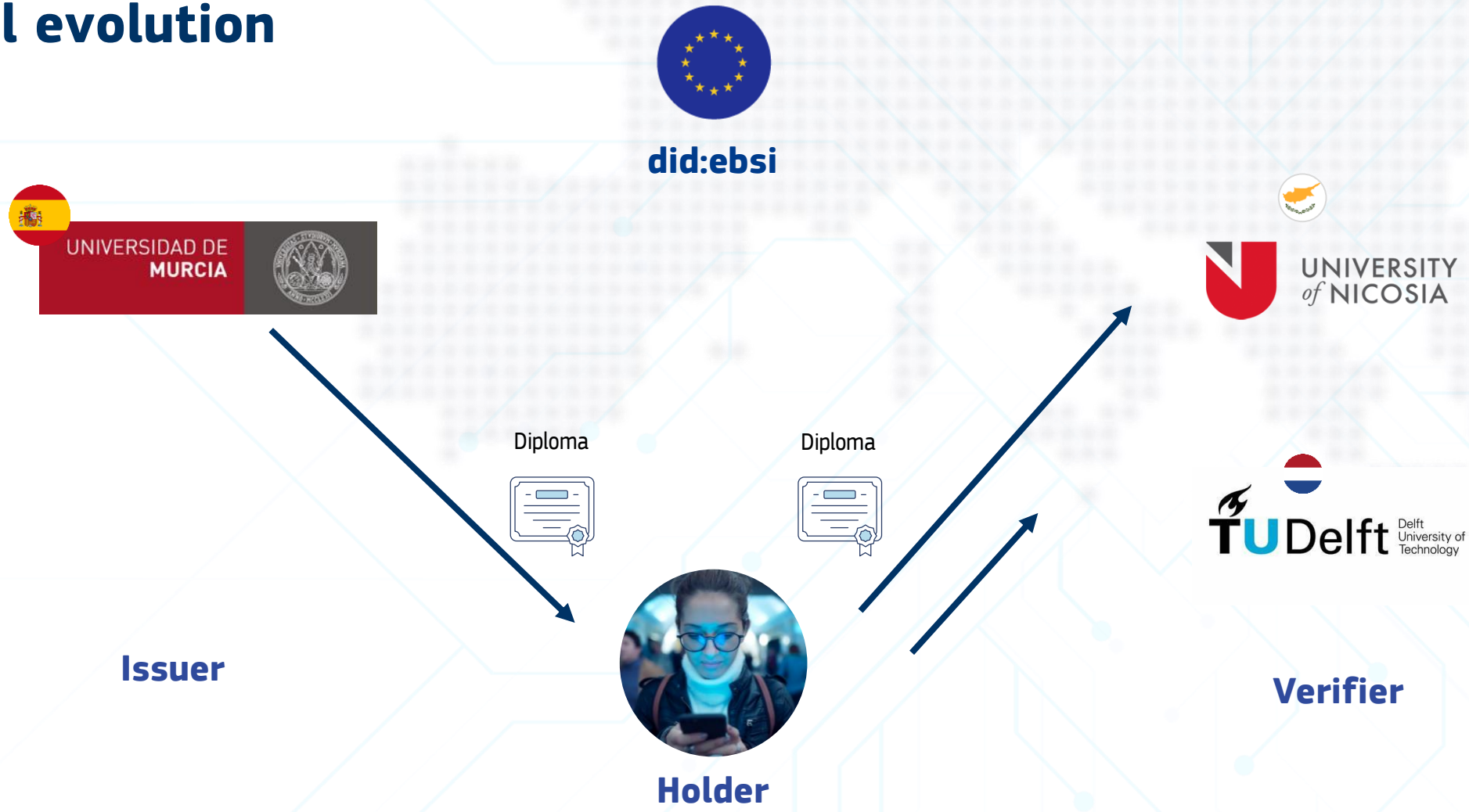
Verifiable Credentials (and Digital Wallet) pattern

The VC (and Wallet) proposes a different pattern for exchanging information (distributed and decentralised) where blockchain acts as a point of truth, supporting the verification of the entities involved in the transaction and ensuring the authenticity of information without requiring real-time access to the information source.



Black list of documents, White list of documents, Status of documents, etc.
Possibility to verify the authenticity of entities when coupled with Self-Sovereign identity

Decentralisation and VCs are the next digital evolution



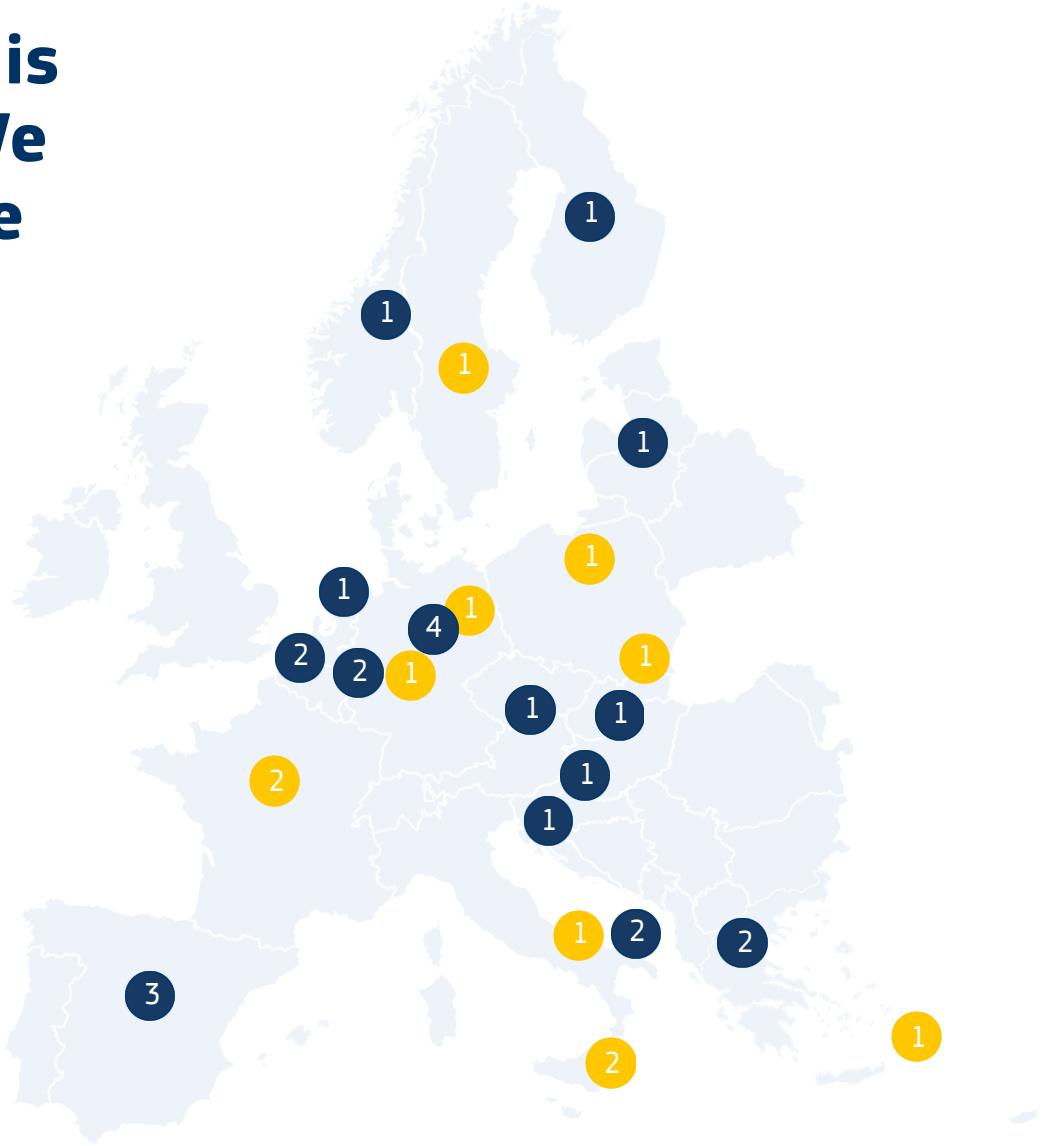
EBSI

EBSI, in a nutshell

The European Blockchain Partnership is a group of 29 countries and the EC. We help public administrations accelerate the creation of trustworthy cross border digital services.

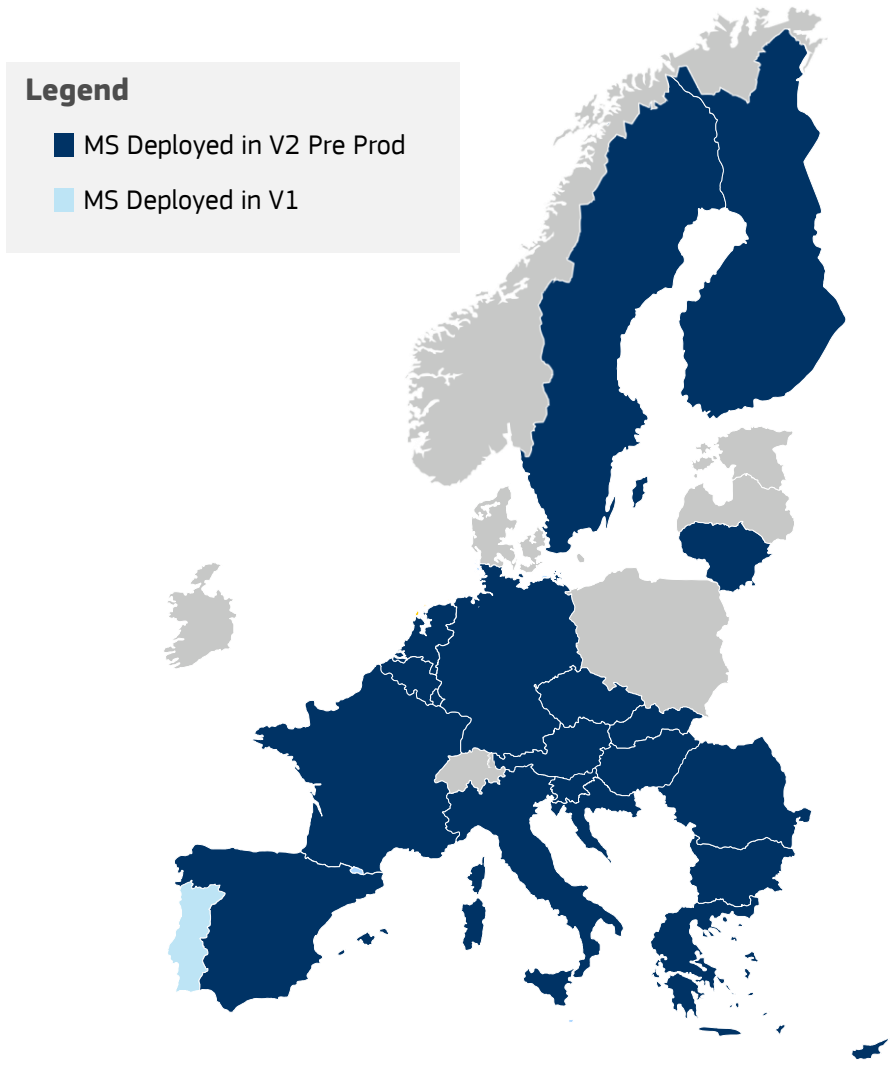
Having this opportunity in mind, the EBSI (European Blockchain Services Infrastructure) has been developed. **Our vision is to accelerate the creation of cross-border services and put blockchain at the service of public administrations for the purpose of verifying information, making the services trustworthy**.

EBSI is the first EU-wide blockchain infrastructure, driven by the public sector, in full respect of European values and regulations. EBSI is supported by 29 countries (All EU Member States, Norway and Lichtenstein) and the EC forming the European Blockchain Partnership (EBP).



A solid node network

A solid network of 38 nodes across Europe



From 30 to **38 nodes** in **21 countries**

of which 30 on V2

Nodes per country:

- Austria (1)
- Belgium (1)*(1)*
- Bulgaria (2)
- Croatia (1)
- Cyprus (1)
- Czechia (2)
- Finland (1)*(1)*
- France (2)
- Germany (2)*(2)*
- Greece (1)*(1)*
- Hungary (1)
- Italy (2)*(1)*
- Liechtenstein
- Lithuania (1)
- Luxembourg (1)
- Netherlands (2)
- Norway (1)
- Portugal (1)
- Romania (1)*(1)*
- Slovakia (1)
- Slovenia (1)
- Spain (3)
- Sweden (1)
- EC Nodes

(Blue Italics are nodes on V1)

A ready-to-use infrastructure

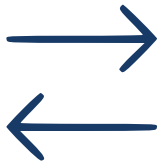
Overview on the work that has been done so far

Q1 2020

EBSI V1

Basic blockchain infrastructure and a user web wallet

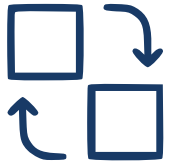
Q3 2020



Preparing for EBSI engagement

First approach and guidance to users for future exploitation of EBSI

Q1/Q2 2021



EBSI V2 Pre-production

EBSI v2 capabilities deployed to the pre-production environment. Early Adopters on EBSI v2 pre-production

Q4 2021

EBSI V2 Production

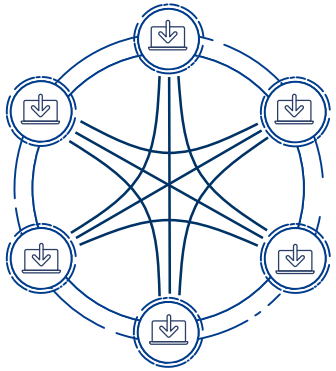
New capabilities will be deployed to the production environment.

Three key ingredients

Three components to benefit from the next evolution of the Web3.

Verifiable Credentials

A new way of
expressing information



Blockchain

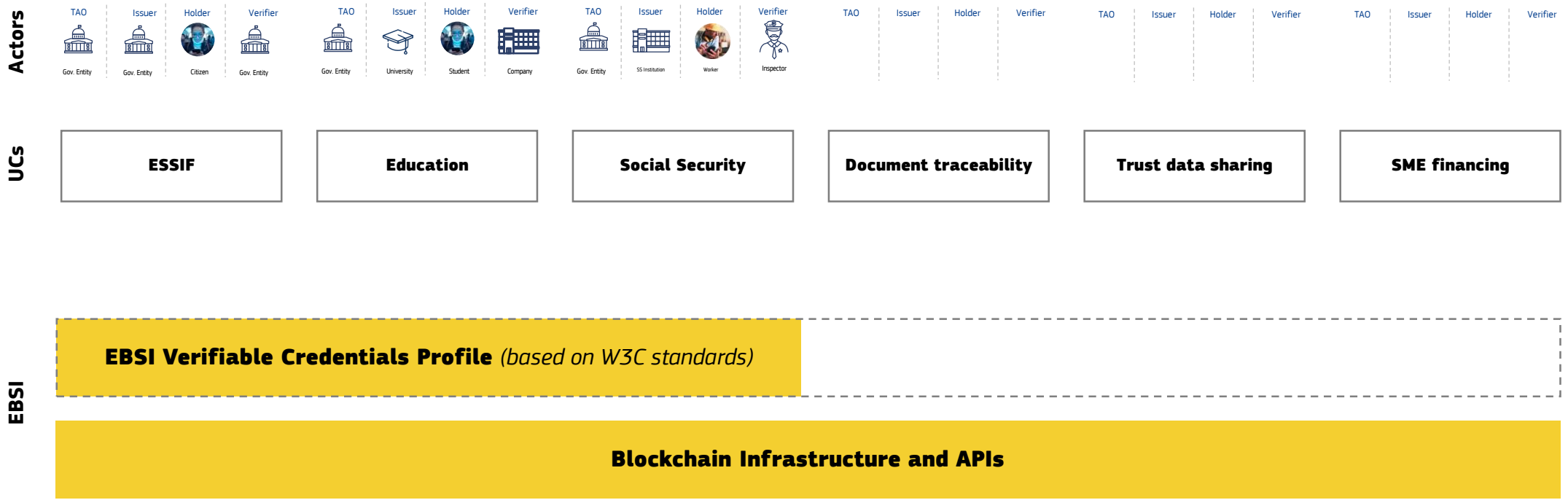
A new decentralised
infrastructure

Digital Wallet

A new way to interact
for/with citizens

What is EBSI today?

EBSI is user centric, decentralised and reusable in multiple contexts and use cases. It is based on open standards to stimulate interoperability and the creation of cross-border public services



Verifiable Credentials

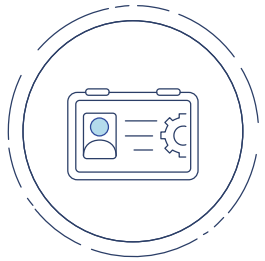
Verifiable Credentials, explained.

Three concepts to ensure interoperability

There are three important concepts to understand

Verifiable Credentials

- A set of claims made by an issuer about a subject
- Tamper-proof
- Cryptographically verifiable
- Digital versions of physical credentials / attestations



Decentralised Identifiers

- Unique Identifier without the need for a central registration authority
- Immutable over time
- Globally resolvable
- Privacy respecting
- Cryptographically verifiable

VC Lifecycle

- Tackling the challenge of scalable implementation
- Common reference model to structure the specifications
- Path to standardisation

VCs are Digital versions of physical credentials / attestations

The concepts of Verifiable Credential (VC) and Verifiable Presentation (VP) and partial disclosure of information

CONCEPT 1

Verifiable Credential (VC)

is an electronic information **structured in a standardised way** (semantic and format).

Verifiable ID (V-ID)

Core legal ID

a special form of a Verifiable Credentials used only for identification / authentication (passports or national eIDs)

- Family name
- First name
- Birth date
- Place of birth
- Unique identifier
- Etc.

Verifiable Attestation (VA)

Electronic attestation of attributes

a special case of a Verifiable Credentials used as evidence of attributes

- **Diplomas**
- Bus tickets
- Membership
- Postal address
- E-mail address
- Bank account
- Etc.

a special case of a Verifiable Credential used as evidence of a permit / authorisation

- Driving license
- Work permit
- Access control
- Etc.

CONCEPT 2

Verifiable Presentation (VP)

represents the **minimum set of data** passing from an entity to a relying party **for a given purpose**.

Extract of **(V-ID)**

+

Extract of **(VA)**

+ **GIVEN PURPOSE**

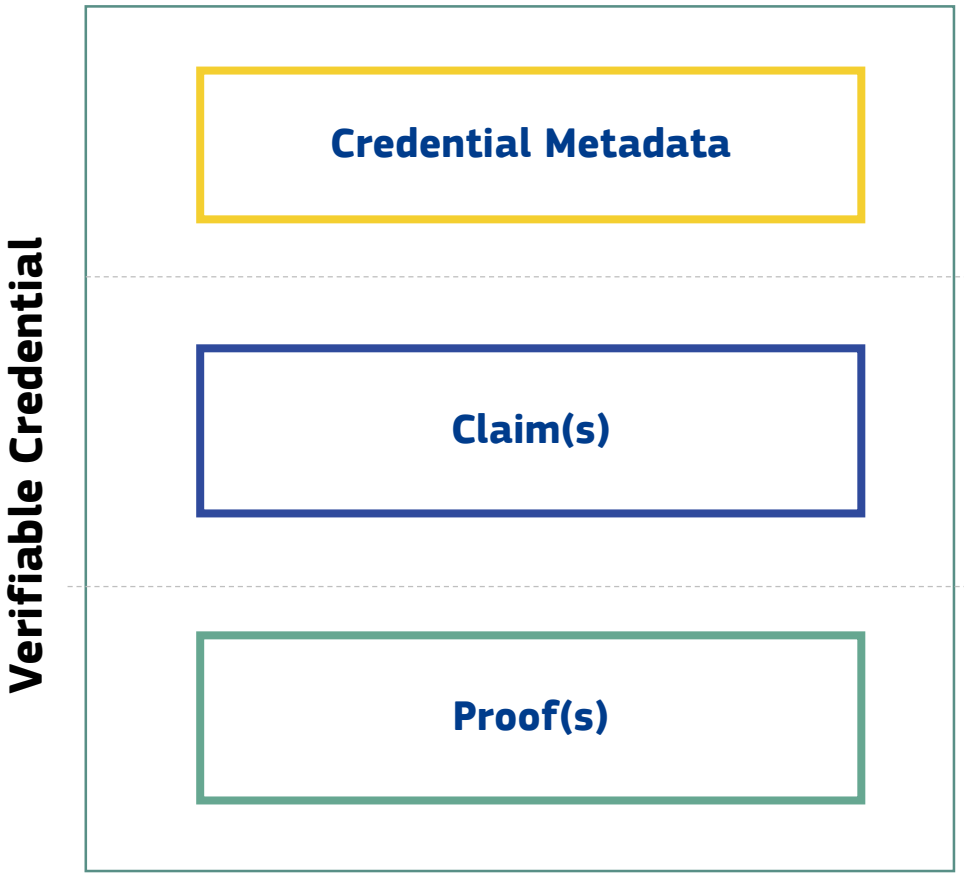
usually composed of V-ID, VA and the purpose of sharing such data. Verifiable Presentation can be easily verified following a cryptographic-based procedure and by accessing trusted information stored in the EBSI Trusted Registries

- **Diplomas**
- Bank account
- Etc.

+ **APPLY FOR A MASTER DEGREE IN UNIVERSITY**

Decomposing a Verifiable Credential

A set of claims made by an issuer about a subject in a manner that is tamper-proof and cryptographically verifiable



> The entity that issued the credential

Who is the **issuer** of this credential?

> Discover different status of the credentials

What is the **current status** of this credential?

> The subject of the credential

Who is the **subject of the credential**?

> The assertions on the subject

What does **the issuer assert about the subject**?

> Digital proof to make the credential tamper-evident

How can a **Verifier find the Public Key of the issuer to verify the Digital Signature** that ensures the integrity and provenance of the credential?

Decentralised Identifier (DID)

The DID allows for rapid verification processes with a robust and privacy preserving approach

01

The DID is unique

A **Decentralised identifier (DID)** is permanent (persistent) identifier. A person cannot have the same DID generated twice but can have multiple DIDs linked to his identity/wallet

02

The DID is easily retrievable

The DID can be looked up to retrieve a **DID Document**, which describes how to interact with the DID owner

03

The DID does not contain pers. info

The DID **does not** provide any kind of information about the DID owner. The version-specific identifier MUST be random and MUST not be derived from any information (e.g., a hash of personal information of any document).

04

The DID is retrieved in autonomy

DIDs leverage on the inherent properties **of blockchain or distributed ledgers**, by creating a tamper-proof and distributed sequence of events. This allows any DID owner to update and keep track of the changes in the DID document **without the need of any central authority**.

05

A person can have more than one DID

A person may **have more than a single DID**. A person cannot have the same DID generated twice but can have multiple DIDs linked to his identity/wallet

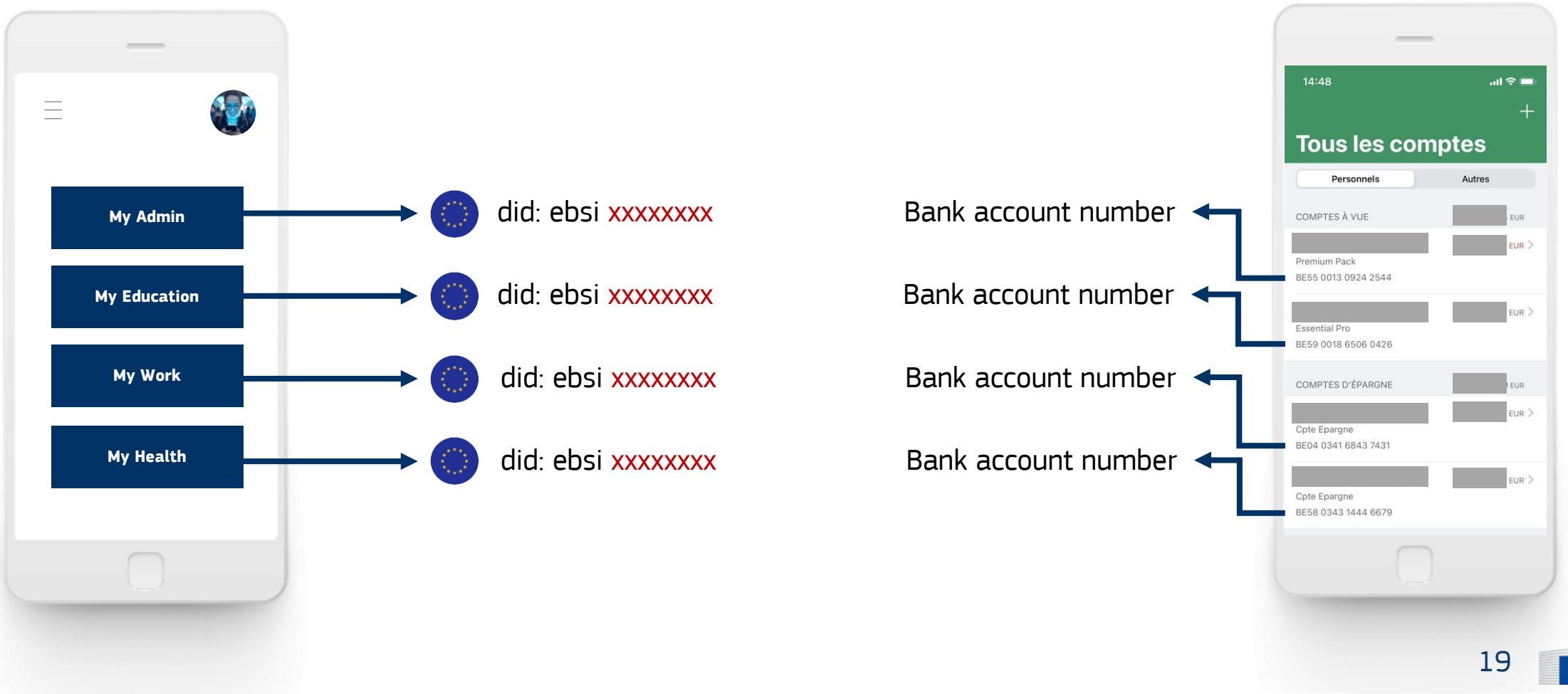
06

A transaction is not logged on the ledger

No access logs to the DIDs for retrieving Public Keys are stored, hence it is not possible to trace the transactions associated to a DID. VC exchange/issuance is not logged on the ledger or EBSI as it happens solely between the Issuer and the holder. Same happens for verification, the verification is based on public accessibly information, i.e. DID method, so that it's easy to verify but impossible to trace.

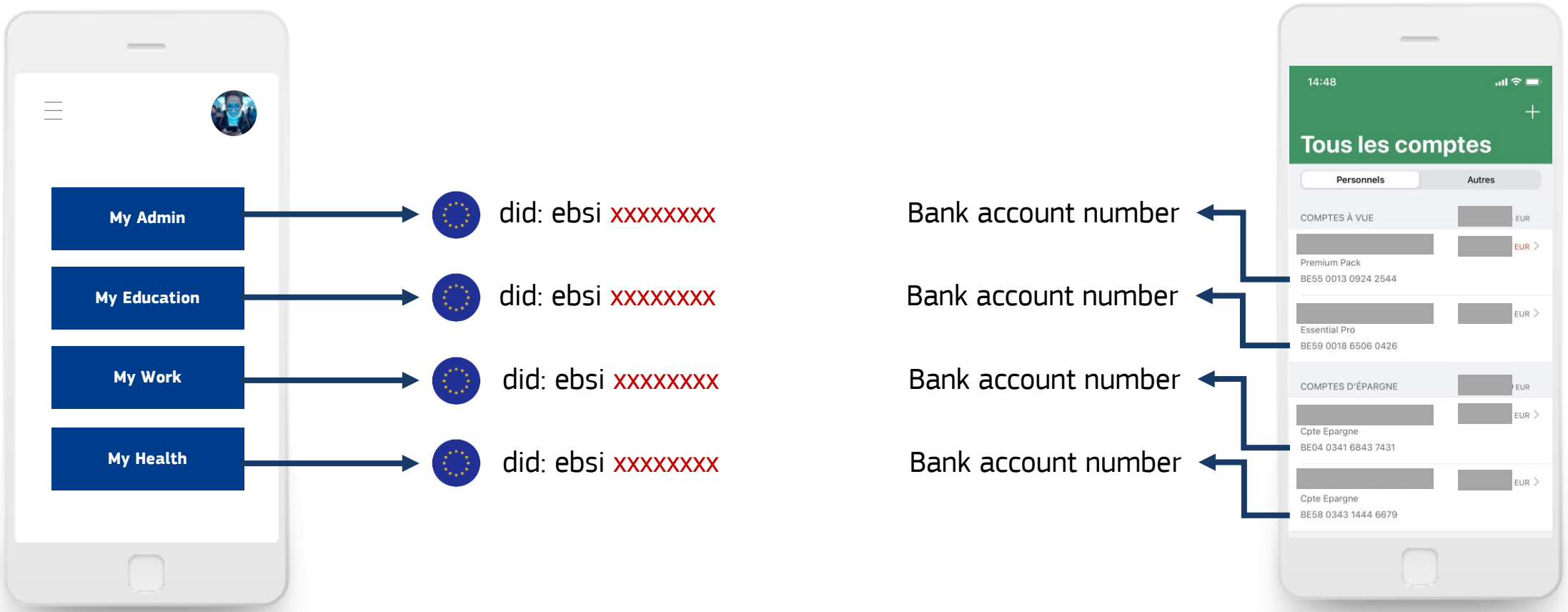
A person may have more than a single DID.

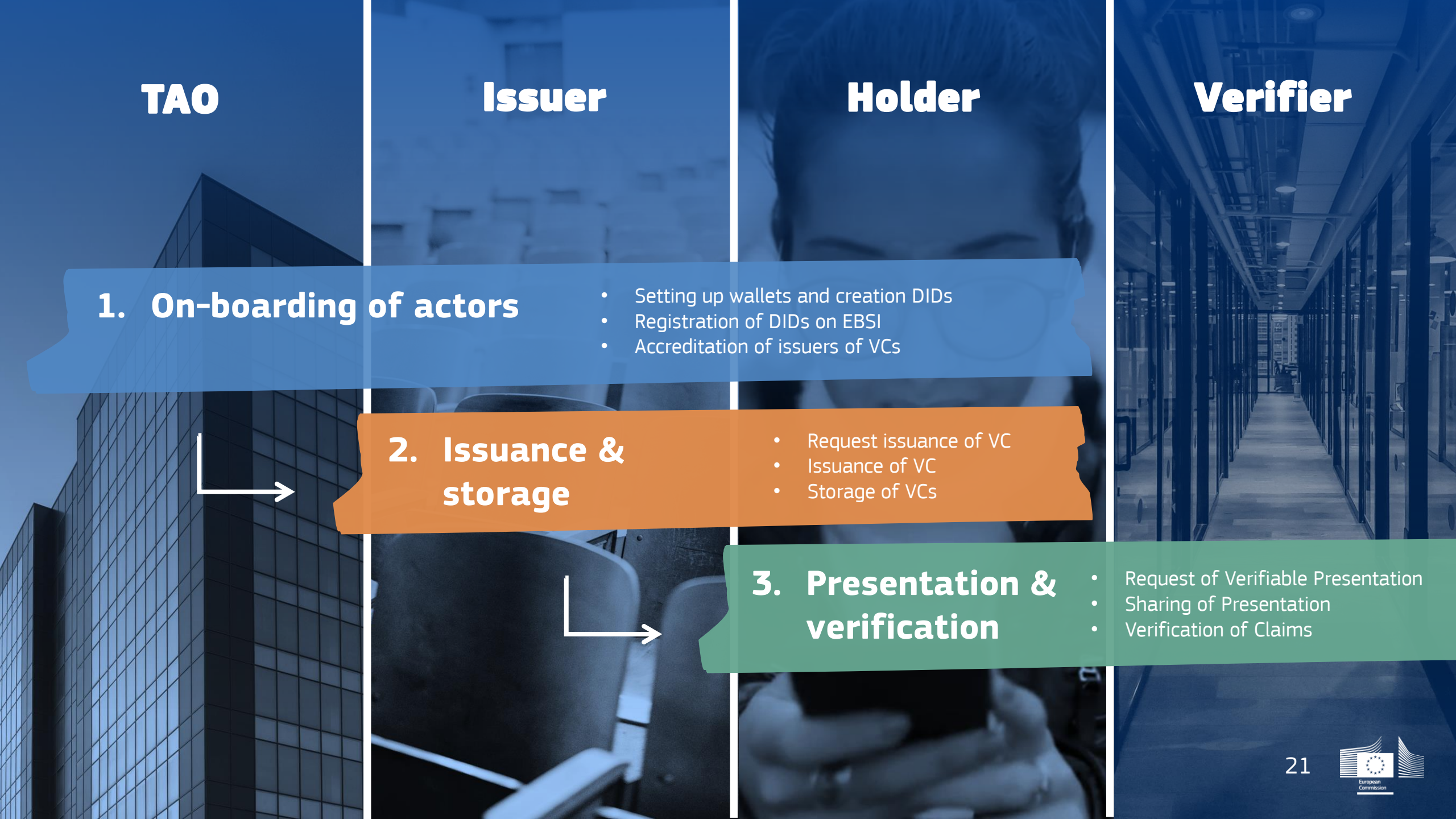
A DID is very similar to an account number (similar to IBAN). The person needs the account number to perform transactions. You can have multiple ones (current, savings, investment, etc.). The wallet is the app that facilitates this set up.



A person may have more than a single DID.

A DID is very similar to an account number (similar to IBAN). The person needs the account number to perform transactions. You can have multiple ones (current, savings, investment, etc.). The wallet is the app that facilitates this set up.




TAO
Issuer
Holder
Verifier
1. On-boarding of actors
• Setting up wallets and creation DIDs
• Registration of DIDs on EBSI
• Accreditation of issuers of VCs
2. Issuance & storage
• Request issuance of VC
• Issuance of VC
• Storage of VCs
3. Presentation & verification
• Request of Verifiable Presentation
• Sharing of Presentation
• Verification of Claims

The Verifiable Credentials Lifecycle

One common Verifiable Credentials Lifecycle based on W3C specifications

01	02	03
On-boarding	**Issuance & storage**	**Presentation & verification**
On-boarding of actors (holders and issuers) supported by EBSI	**Issuing and storage of Verifiable Credentials**	**Presentation and Verification of Verifiable Credentials**
• Setting up wallets and creation of DIDs • Registration of DIDs on EBSI • Accreditation of issuers of VCs	• Request issuance of VC • Issuance of VC • Storage of VCs	• Request of Verifiable Presentation • Sharing of Presentation • Verification of Claims
W3C Specifications		
• Not specified by W3C's spec	• Issuance of one or more VCs. • Storage of VCs in a credential repository (such as a digital wallet).	• Composition of VPs. • Verification of the VPs

1. On-boarding

On-boarding of Issuers and Holders of Verifiable Credentials

Onboarding of **Issuers** of Verifiable Credentials

	Set-up wallet and create DID		Register DID on EBSI			Register Issuer on EBSI			Register Schema
TAO							1.0.X.16 Creates Verifiable Accreditation to accredit the issuer		1.0.X.19 | 1.0.X.17 Registers VC schema on Trusted Schema Register
Issuer	1.0.X.1 Sets-up an EBSI conformant wallet	1.0.X.3 Creates a DID, a Public and a Private key	1.0.X.16 Requests authorization to register the DID on the ledger		1.0.X.5 Registers DID (and associated public key) on the ledger	1.0.X.16 Requests the registration of the Issuer in the issuer register		1.0.X.16 Registers Verifiable Accreditation on the TIR	1.0.X.19 | 1.0.X.17 Registers VC schema on Trusted Schema Register
EBSI on-boarding services				1.0.X.16 Creates Verifiable Authorisation to authorise the publication of DID					1.0.X.19 | 1.0.X.17 Registers VC schema on Trusted Schema Register upon request

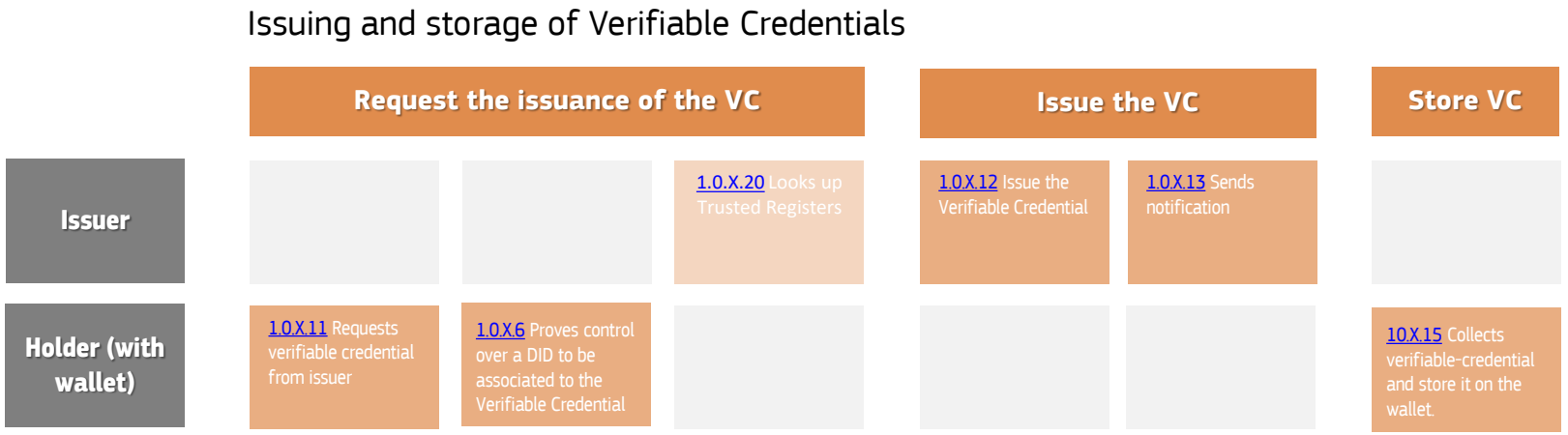
Onboarding of **Holders** of Verifiable Credentials

Holder	1.0.X.2 Sets-up an EBSI conformant wallet	1.0.X.3 Creates a DID, a Public and a Private key	1.0.X.4 Requests authorization to register the DID in the ledger		1.0.X.5 Registers DID (and associated public key) on the ledger				
EBSI on-boarding service				1.0.X.4 Creates authorization-credential to authorize the publication of DID					

Legend Mandatory | Multiple implementations possible | Alternative options (one must be used)

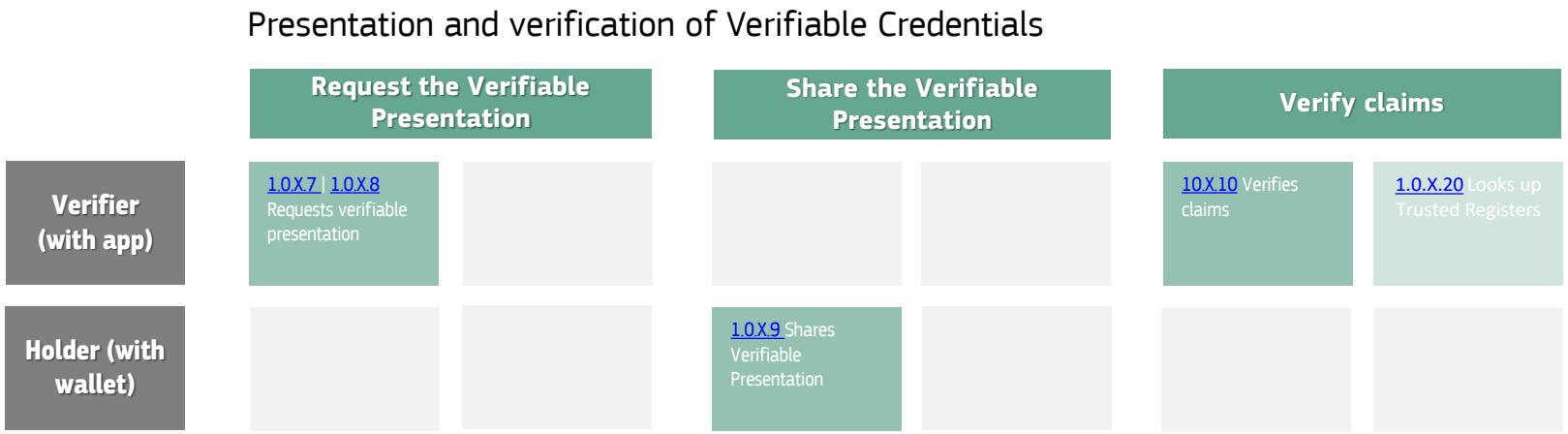
2. Issuing & storage

Issuing and storage of Verifiable Credentials



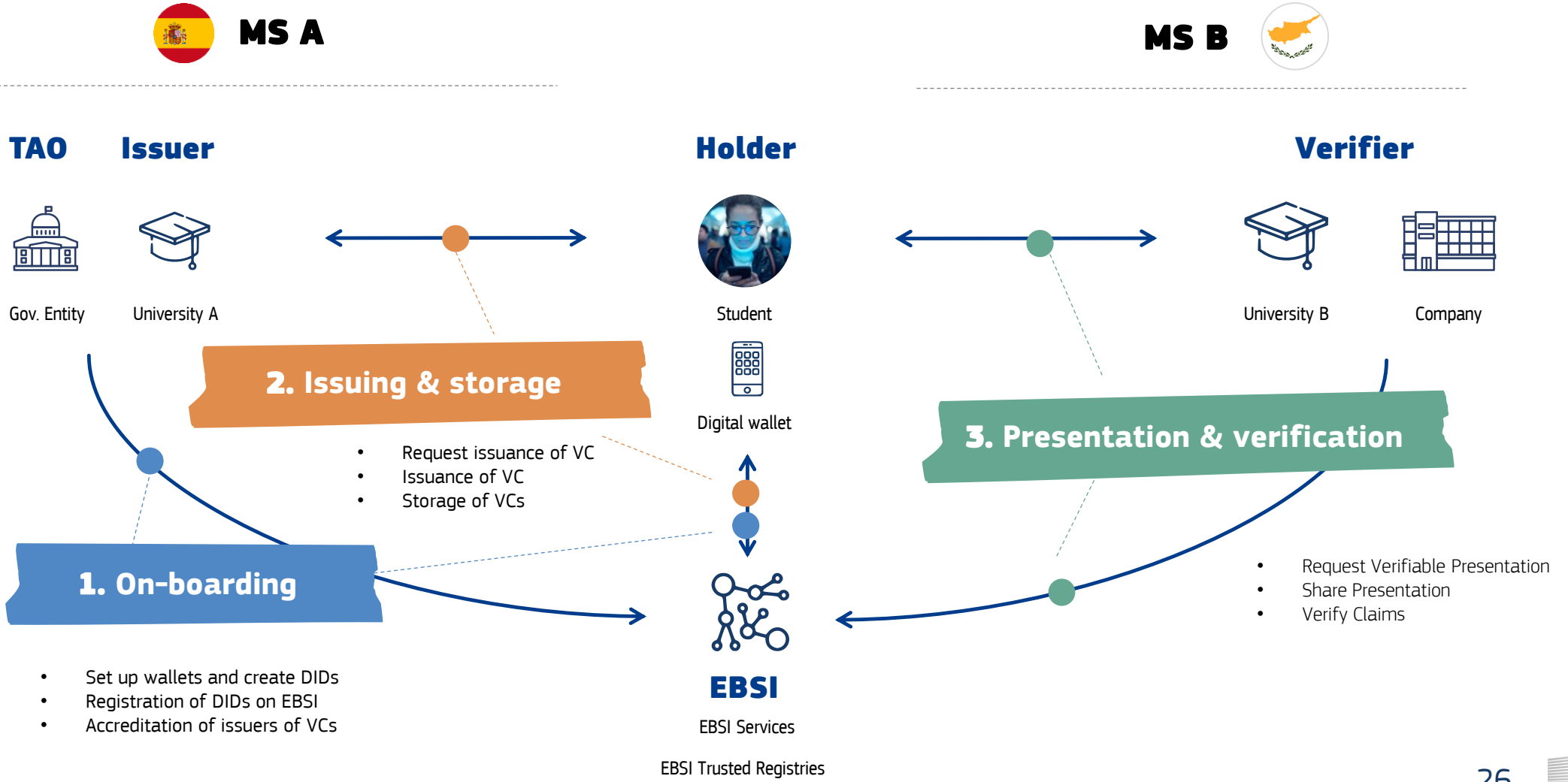
3. Presentation and verification

Presentation and verification of Verifiable Credentials



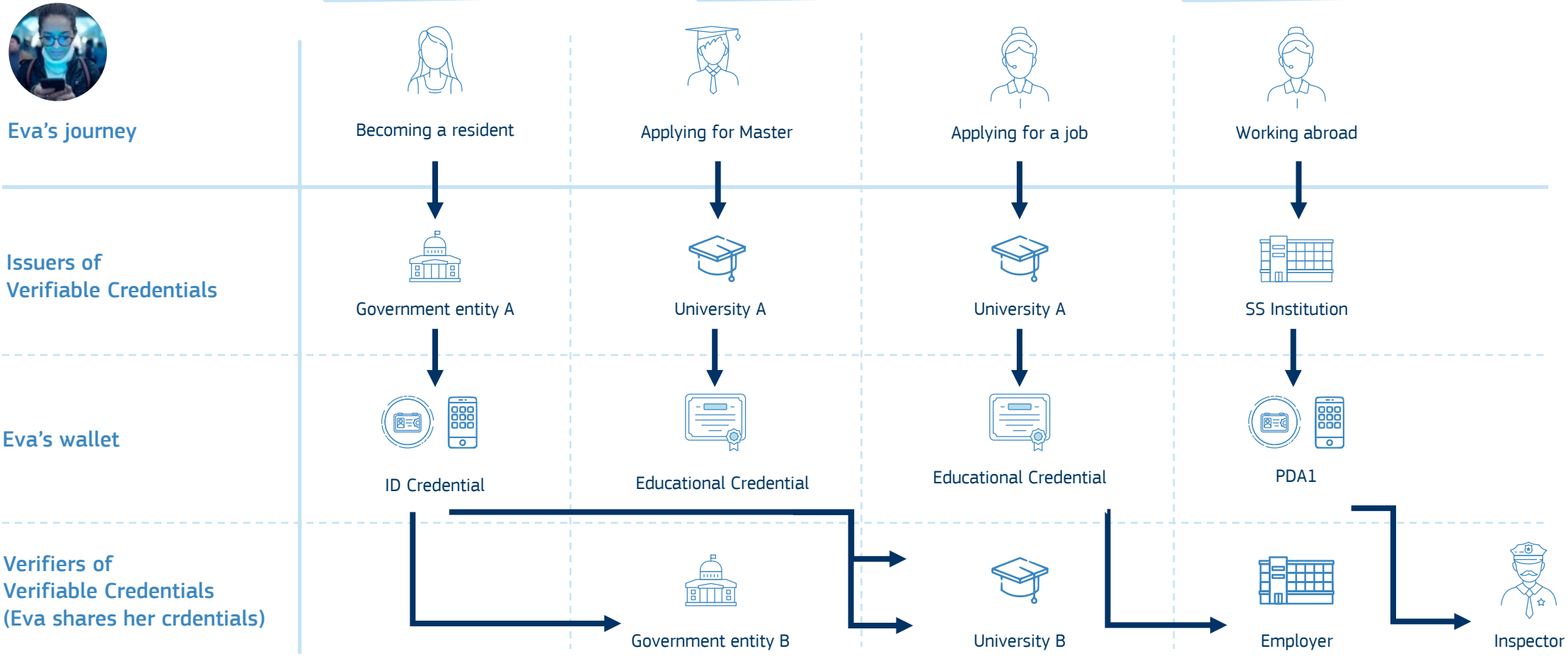
Applying the VC lifecyle in a cross border context

Applying the VC lifecycle in a cross-border context



The exchange of VCs applied to EBSI use cases

Let's look at the exchange of Verifiable Credentials applied to EBSI use cases

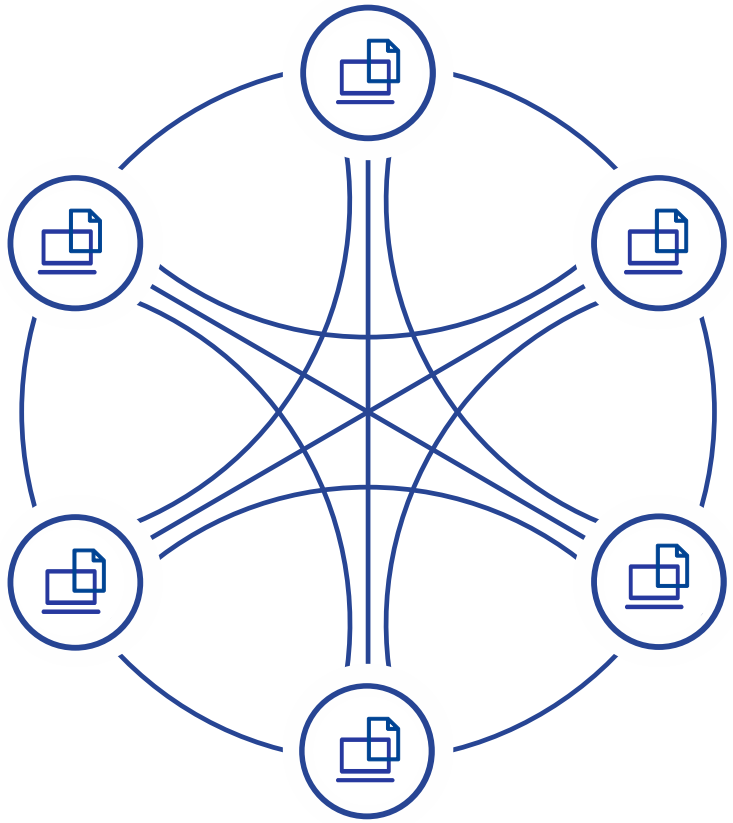


Blockchain

How does it work?

A distributed ledger

Blockchain is a distributed ledger to decentralise permanent digital records / transactions.



A **LEDGER** is a well-known concept used in business as a log keeping a definitive record of transactions.

LEDGERS are used to record transactions of almost any type. For example, the status of a document.

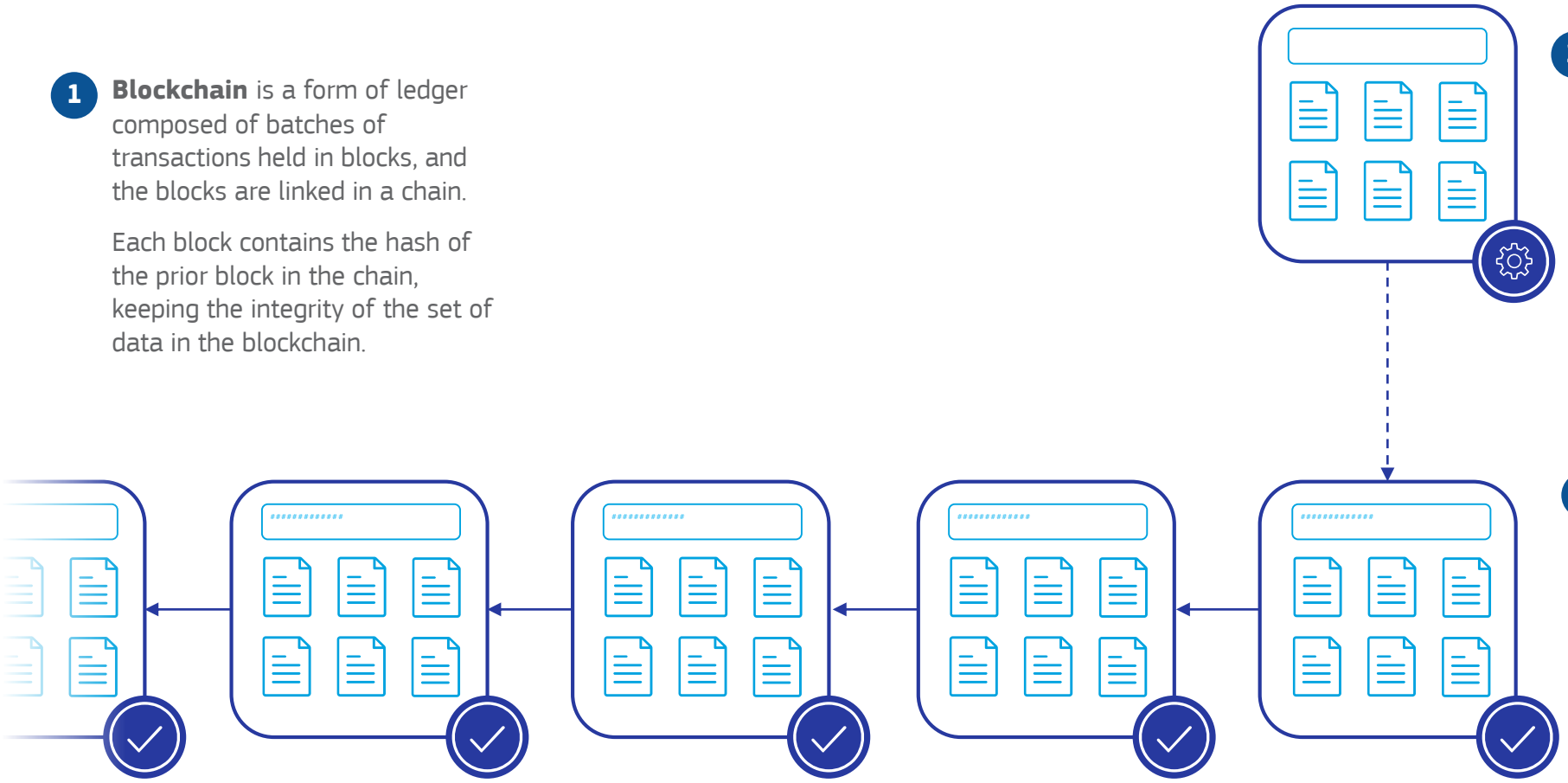
A **DISTRIBUTED LEDGER** is a ledger that has its entries stored across a series of nodes in a network, rather than in a single location making it "tamper-proof".

Blockchain uses cryptographic methods

Blockchain uses cryptographic methods that creates trust between disparate systems.

1 **Blockchain** is a form of ledger composed of batches of transactions held in blocks, and the blocks are linked in a chain.

Each block contains the hash of the prior block in the chain, keeping the integrity of the set of data in the blockchain.



2 *Each block can contain transactions, data and a **reference to the previous blocks** (creating the chain)*

3 *Transactions recorded **chronologically** and **cannot be changed** once added to the chain*

*For **blocks to be added** to the blockchain, it must be achieved through **consensus***

EBSI is based on the Proof of Authority consensus.

EBSI is based on the Proof of Authority consensus. This consensus model relies on the partial trust of publishing nodes through their known link to real world identities. Publishing nodes must have their identities proven and verifiable within the blockchain network (e.g. identifying documents which have been verified and included on the blockchain).

Proof of Work

Proof of Stake

Permissionless
No authentication needed to write on the blockchain
[Miners]

Proof of Authority

Permissioned
Transactions and blocks are validated by approved accounts
[Validators*]

*Every MS has elected a representative to perform the validation

How does it work?

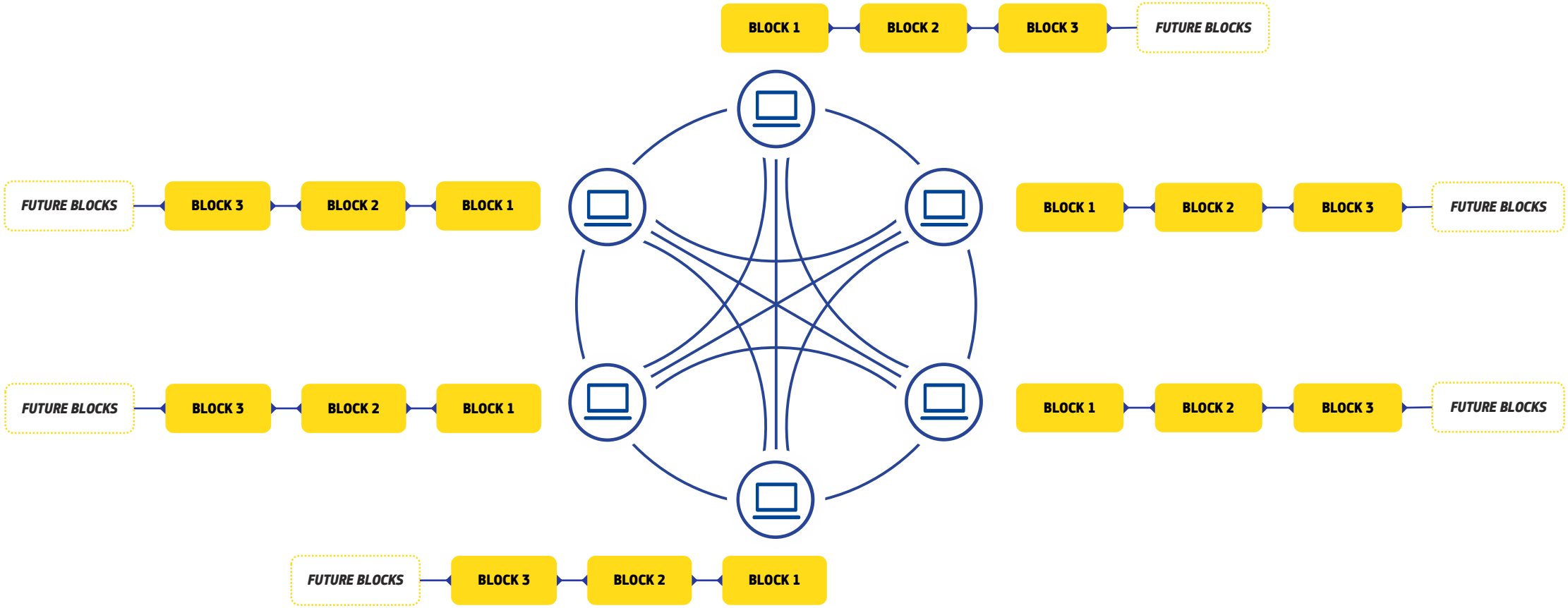
The publishing node is staking its identity/reputation to publish new blocks. Blockchain network users directly affect a publishing node's reputation based on the publishing node's behavior.

Publishing nodes can lose reputation by acting in a way that the blockchain network users disagree with, just as they can gain reputation by acting in a manner that the blockchain network users agree with. The lower the reputation, the less likelihood of being able to publish a block.

Therefore, it is in the interest of a publishing node to maintain a high reputation. This algorithm only applies to permissioned blockchain networks with high levels of trust.

Transactions are added to a block and validated by the network

When transactions are added to a block, the blocks are validated by the network. Every node maintains an identical copy of the blockchain

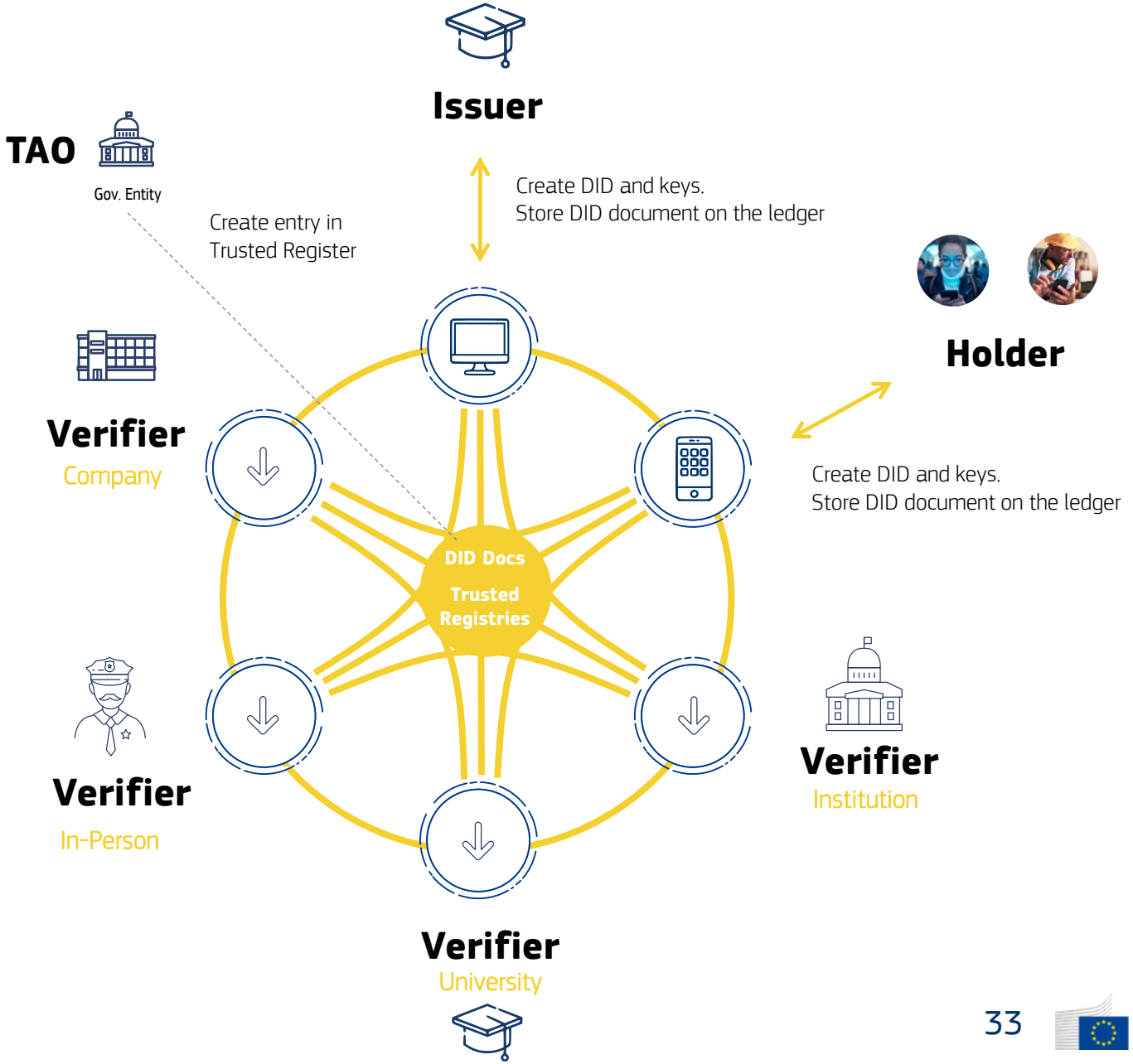


Transactions are added to a block and validated by the network

The credentials are **not stored on chain**.

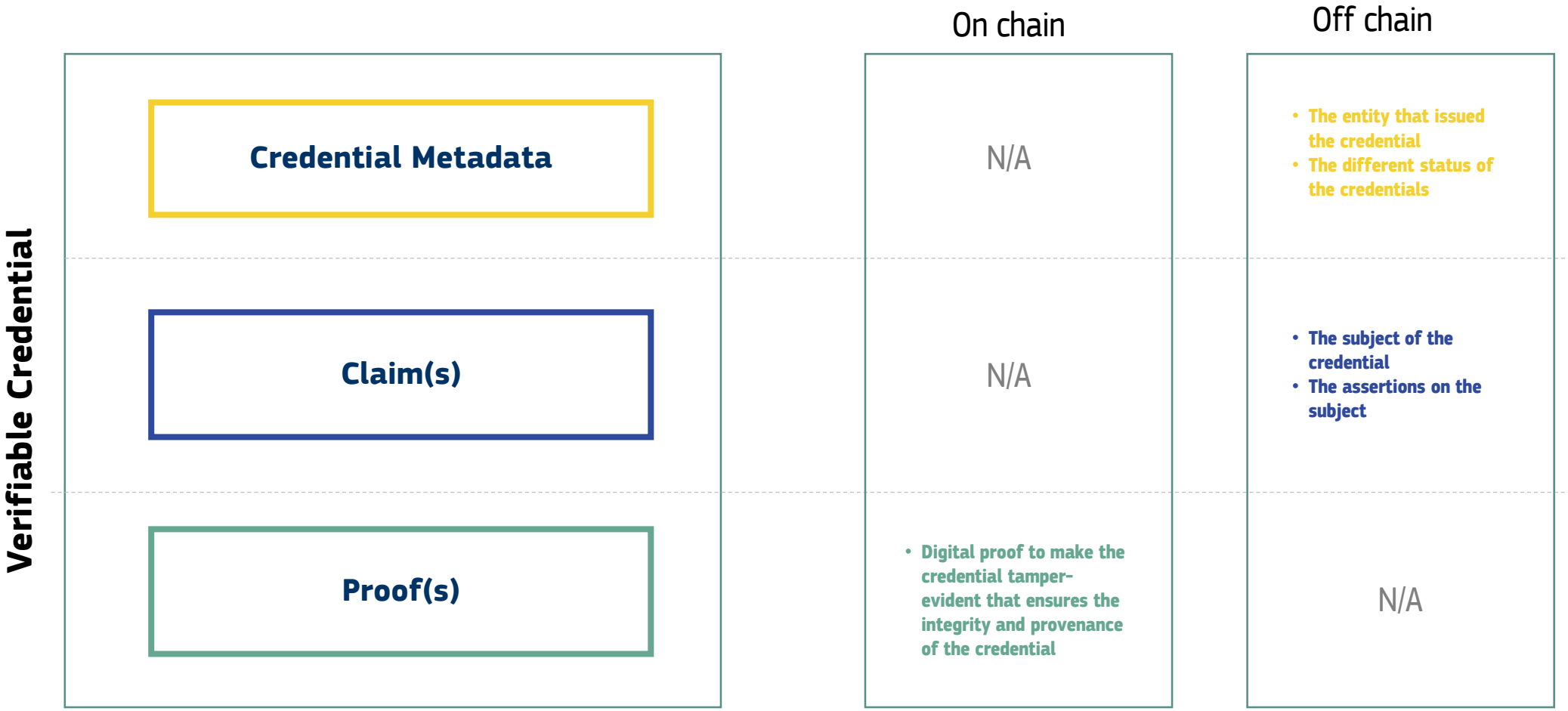
The credentials are **cryptographically secured** by electronic signatures to make it possible to verify its integrity and authenticity. It also **includes verification of the DID of the Issuer and the DID of the Holder**.

This allows the Holder to cryptographically prove the ownership of the credential. The legitimacy of the issuer must be proved passing verification of the information stored on EBSI Trusted Registries.



What is stored on chain?

Let's decompose a VC and see what is stored on chain

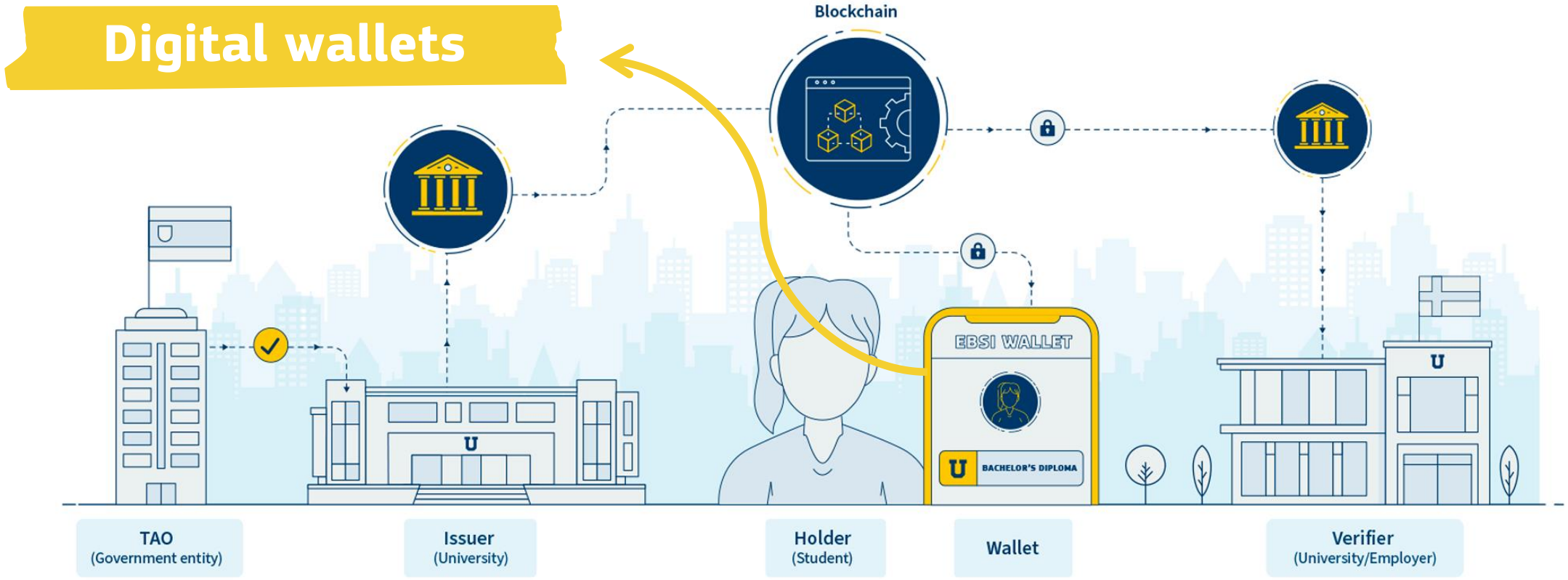


Digital Wallets

Introduction

Wallets mediate almost all user interactions.

The vast majority of interactions to exchange VCs depend on the wallet

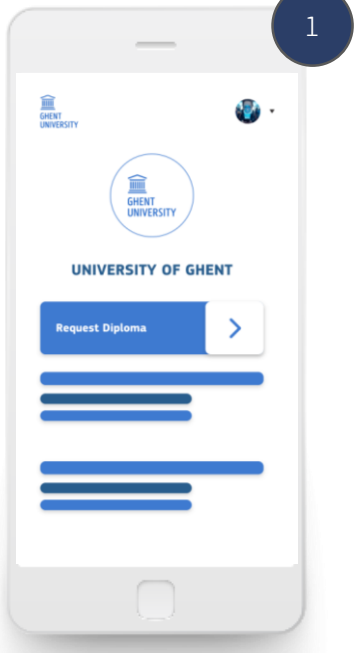


The interaction needs to happen via an EBSI compliant wallet. (1)

Example (1): Eva requests the issuance of her Bachelor's diploma to the University of Ghent (BE)

Eva initiates the request for the issuance of her Bachelor's Diploma

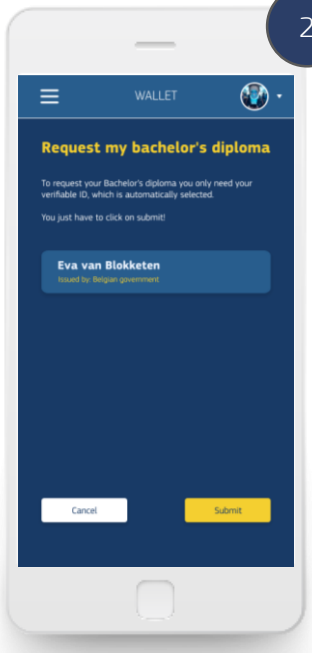
1



- Connect to University platform
- Initiate the action

Eva requests the issuance of her Bachelor's Diploma from the University of Ghent

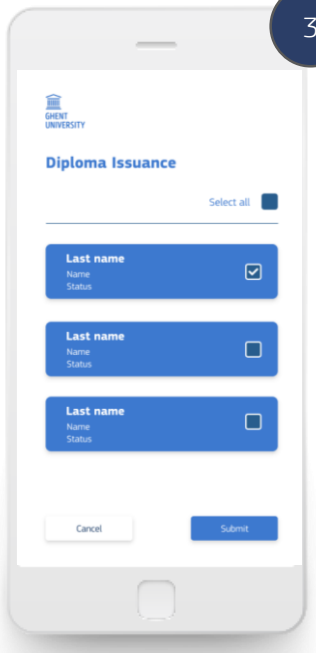
2



- Select Verifiable ID
- Submit the request

The University of Ghent issues the Bachelor's Diploma

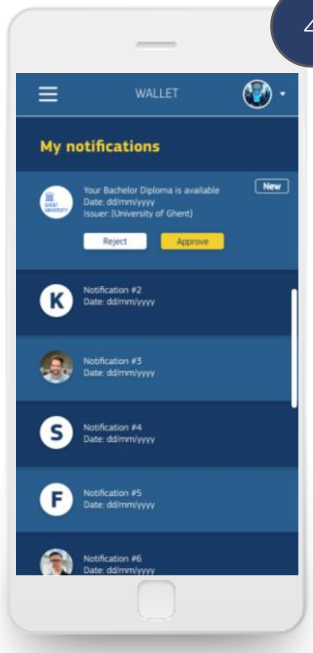
3



- Check list of students
- Select the students
- Submit the credential

Eva receives and accepts the Bachelor's Diploma.

4

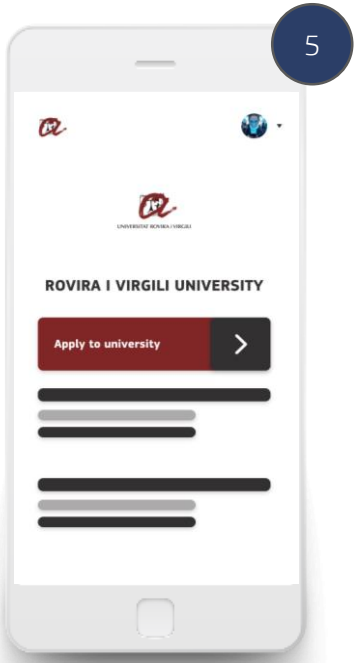


- Get notification
- Accept the credential
- Store in the wallet.

The interaction needs to happen via an EBSI compliant wallet. (2)

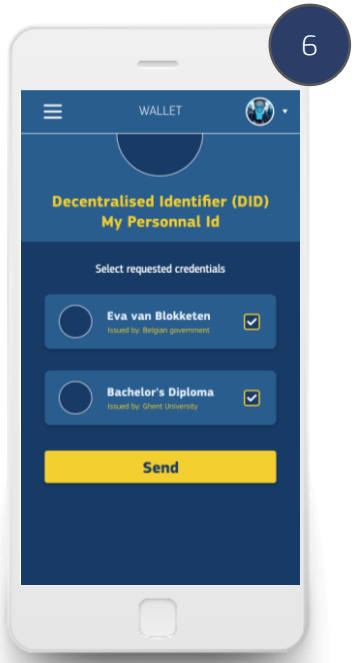
Example (2): Eva requests her enrolment at the University of Rovira i Virgili (ES).

Eva initiates the application to the University of Rovira i Virgili



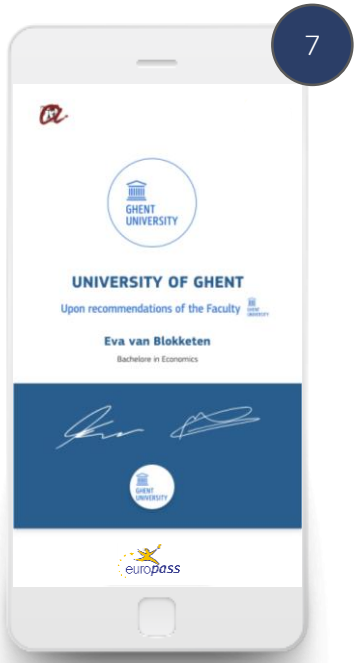
- Connect to University platform
- Initiate the action

Eva shares her Bachelor's Diploma with the University of Rovira i Virgili



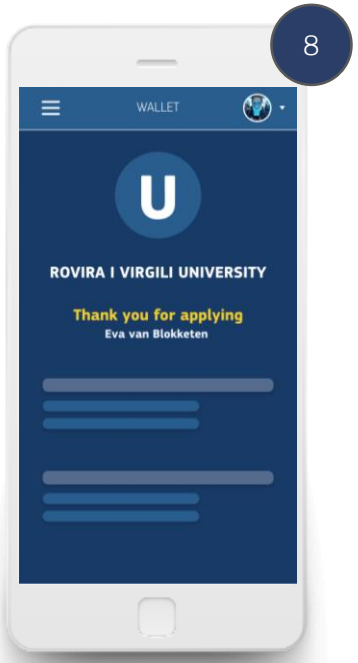
- Select Verifiable ID
- Select Bachelor's diploma
- Submit the request

The University of Rovira i Virgili verifies the Bachelor's Diploma of Eva



- Get notification
- Check list of requests
- Check details of diploma

Eva enrols for a Master's Degree at the University of Rovira i Virgili



Walk through a scenario

Introduction

The Verifiable Credentials Lifecycle

One common Verifiable Credentials Lifecycle based on W3C specifications

01 On-boarding

On-boarding of actors (holders and issuers) supported by EBSI

- Setting up wallets and creation of DIDs
- Registration of DIDs on EBSI
- Accreditation of issuers of VCs

02 Issuing & storage

Issuance and storage of Verifiable Credentials

- Request issuance of VC
- Issuance of VC
- Storage of VCs

03 Presentation & verification

Presentation and verification of Verifiable Credentials

- Request of Verifiable Presentation
- Sharing of Presentation
- Verification of Claims

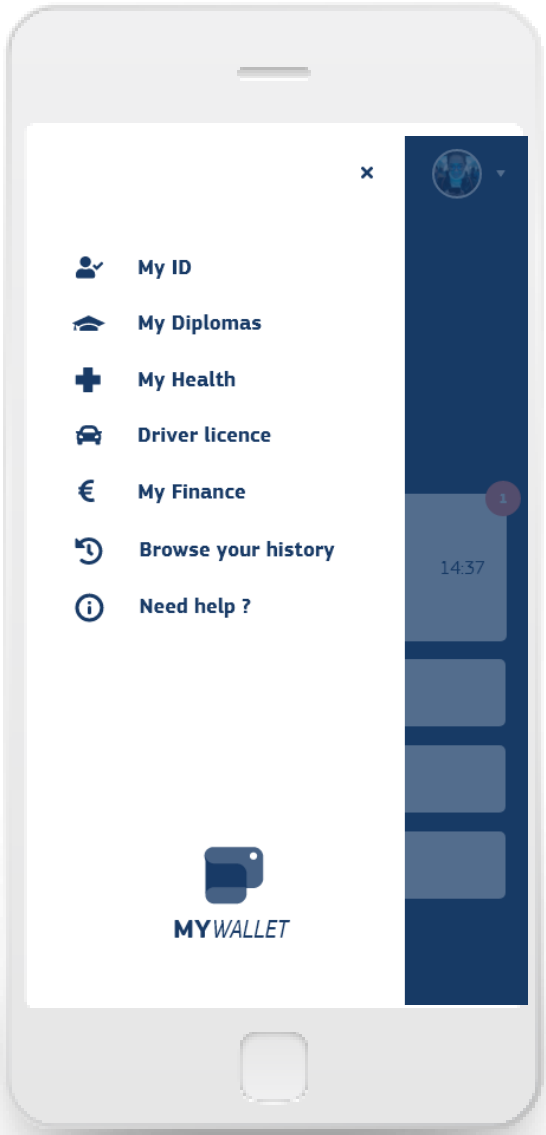
W3C Specifications

- Not specified by W3C's spec

- Issuance of one or more VCs.
- Storage of VCs in a credential repository (such as a digital wallet).

- Composition of VPs.
- Verification of the VPs

Different wallet architectures are possible (Mobile Wallet, Desktop Wallet, Cloud Wallet). EBSI is not putting any constraints to the wallet architecture.
We will walk you through a scenario to illustrate the VC lifecycle by considering a Mobile Wallet.



1. Onboarding

1. Onboarding

On-boarding of Issuers and Holders of Verifiable Credentials

Onboarding of **Issuers** of Verifiable Credentials

	Set-up wallet and create DID		Register DID on EBSI			Register Issuer on EBSI			Register Schema
TAO							1.0.X.15 Creates Verifiable Accreditation to accredit the issuer		1.0.X.19 | 1.0.X.17 Registers VC schema on Trusted Schema Register
Issuer	1.0.X.1 Sets-up an EBSI conformant wallet	1.0.X.3 Creates a DID, a Public and a Private key	1.0.X.16 Requests authorization to register the DID on the ledger		1.0.X.5 Registers DID (and associated public key) on the ledger	1.0.X.16 Requests the registration of the Issuer in the issuer register		1.0.X.15 Registers Verifiable Accreditation on the TIR	1.0.X.19 | 1.0.X.17 Registers VC schema on Trusted Schema Register
EBSI on-boarding services				1.0.X.16 Creates Verifiable Authorisation to authorise the publication of DID					1.0.X.19 | 1.0.X.17 Registers VC schema on Trusted Schema Register upon request

Onboarding of **Holders** of Verifiable Credentials

Holder	1.0.X.2 Sets-up an EBSI conformant wallet	1.0.X.3 Creates a DID, a Public and a Private key	1.0.X.4 Requests authorization to register the DID in the ledger		1.0.X.5 Registers DID (and associated public key) on the ledger				
EBSI on-boarding service				1.0.X.4 Creates authorization-credential to authorize the publication of DID					

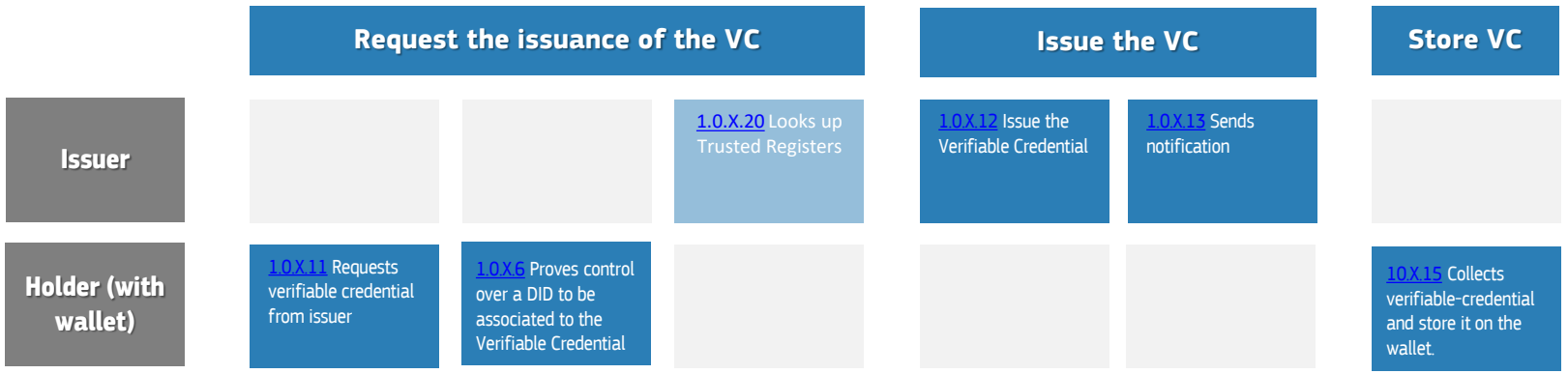
Legend Mandatory | Multiple implementations possible | Alternative options (one must be used)

2. Issuance and storage of Verifiable Credentials

2. Issuance & storage

Issuance and storage of Verifiable Credentials

Issuing and storage of Verifiable Credentials

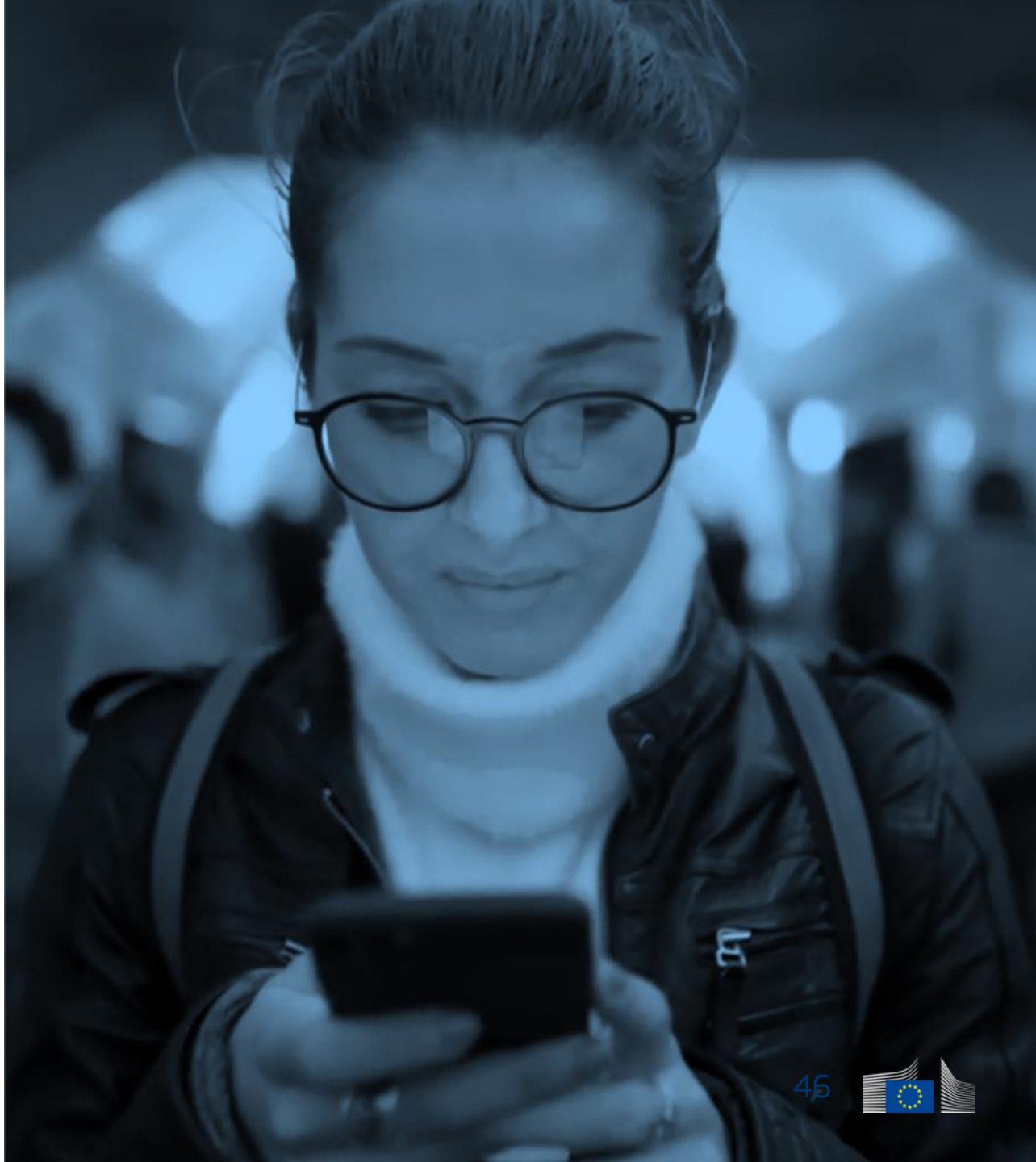


2. Issuance and storage of Verifiable Credentials

2.1. Eva requests the issuance of her Bachelor's diploma to the University of Ghent (BE).

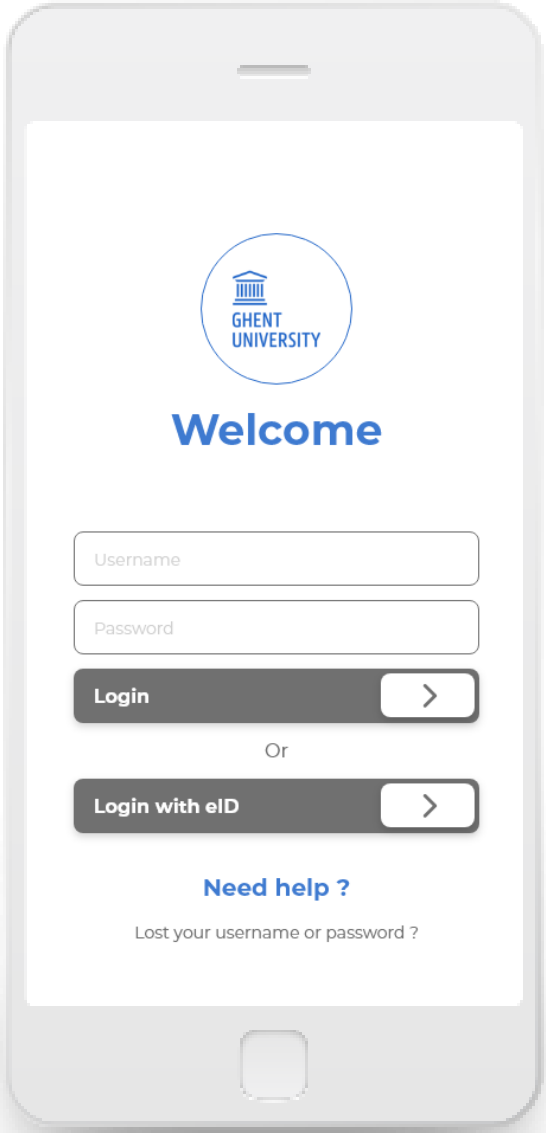
2.2. The University of Ghent (BE) issues her Bachelor's diploma and send it to Eva.

2.3. Eva receives and stores her Bachelor's diploma in her wallet.

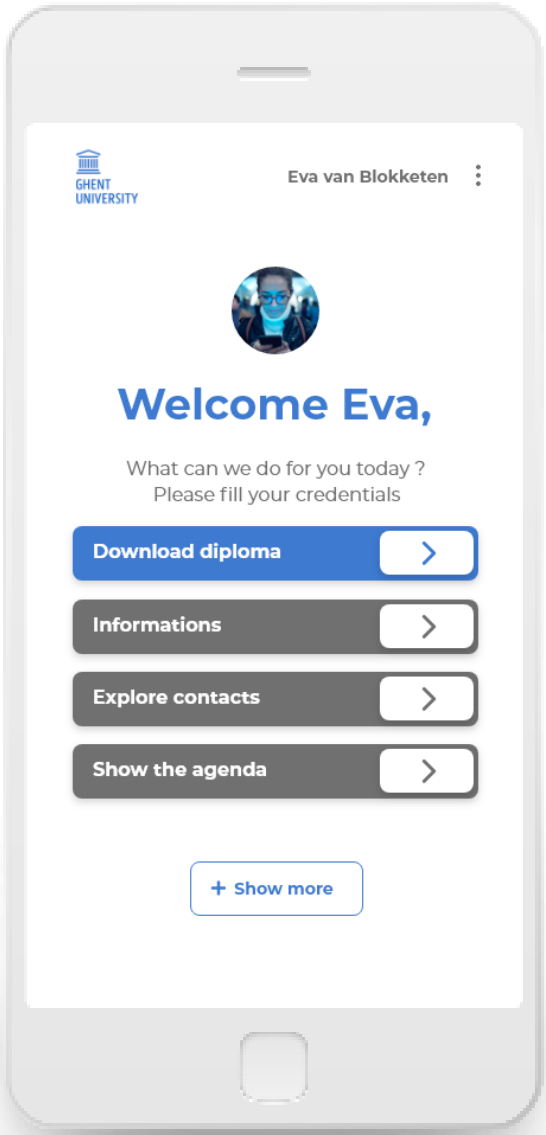


2.1. Eva requests the issuance of her Bachelor's diploma to the University of Ghent (BE).

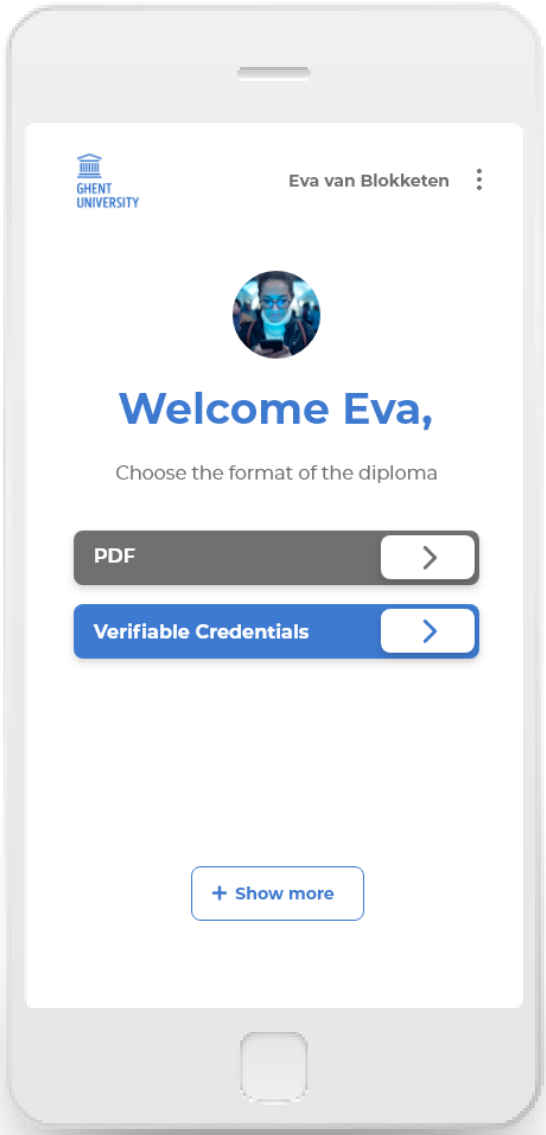
Eva authenticates to the platform of the University of Ghent using Belgian eID (e.g. from the University or from the federal Government).



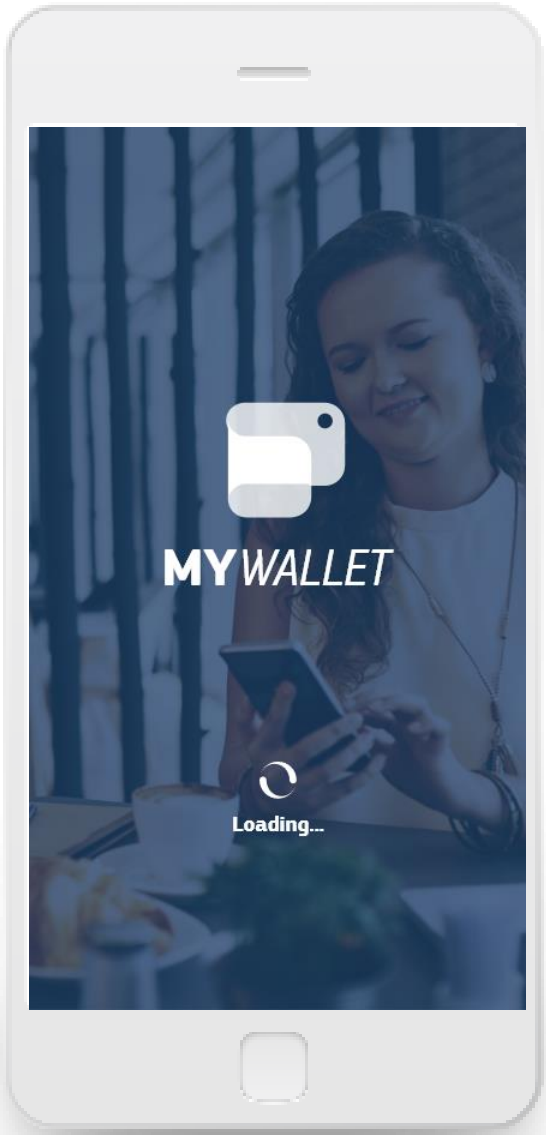
Eva can perform a number of actions in the portal of the University of Ghent. She wants to download her Bachelor's diploma so she initiates the request.



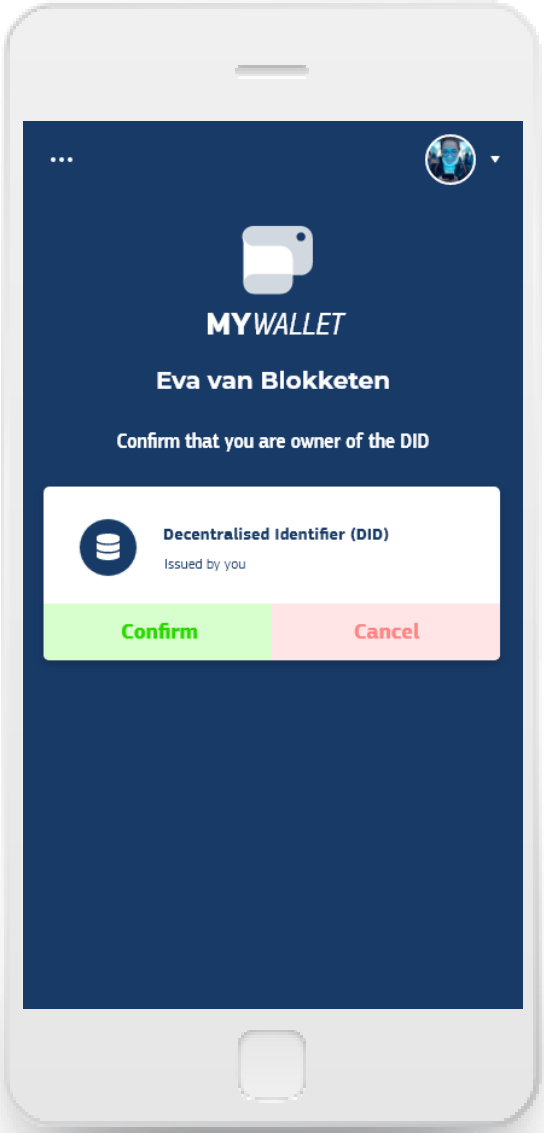
Eva can choose the format between a PDF or a Verifiable Credential. She chooses the Verifiable Credentials format.



Eva is redirected immediately to her personal wallet. The portal from the University of Ghent receives her DID.



The wallet asks Eva to confirm the sharing of her DID with the portal. Eva confirms and proves control over a DID and submits the request to the University of Ghent.



What happens here ?

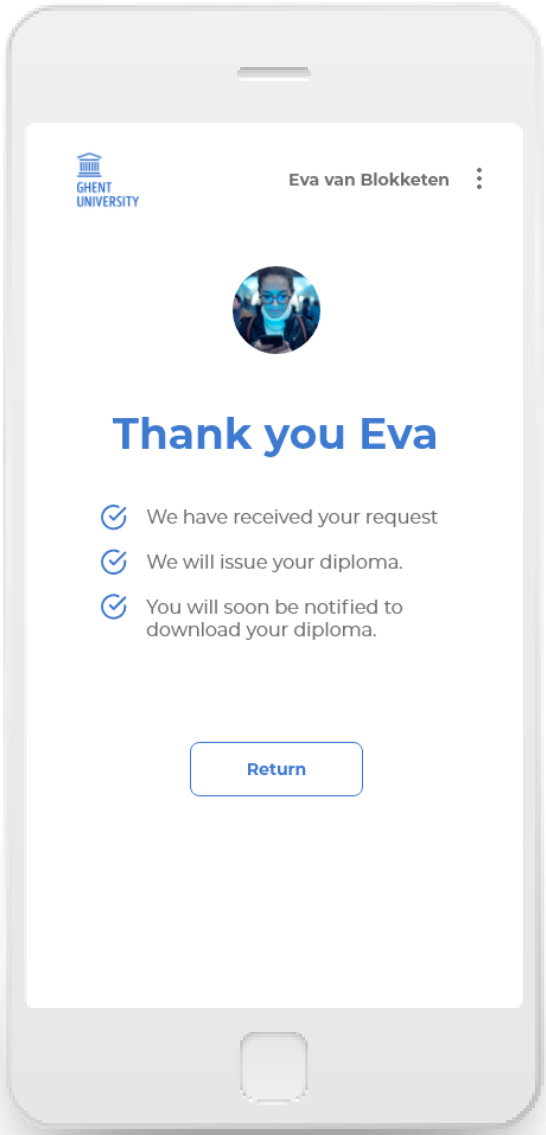
1. The wallet is asking Eva to confirm the sharing of her DID with the portal.
2. She confirms. It means that the wallet sends a signed confirmation with the DID to the portal when Eva is redirected to the portal.

Eva is redirected to the portal of the University of Ghent and receives a confirmation that the diploma request has been submitted and that she will soon receive a notification to download her diploma.

What happens here ?

Eva is back on the portal page.

1. When the portal gets that signed message, it verifies the signature. This means that the confirmation of DID ownership is concluded (this wallet is the owner of that DID)
2. Please note that the portal gets the public keys to verify the signature (need to integrate the portal with EBSI)

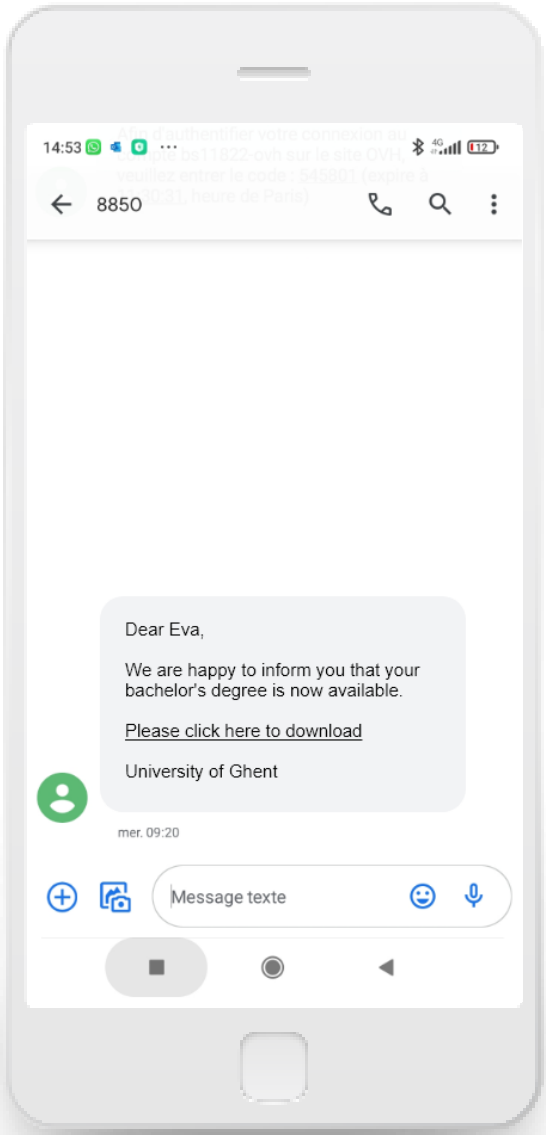


2.2. The University of Ghent (BE) issues her Bachelor's diploma and send it to Eva.

The University of Ghent (BE) issues automatically her Bachelor's diploma and send it to Eva. Eva is notified that she can now download the diploma.

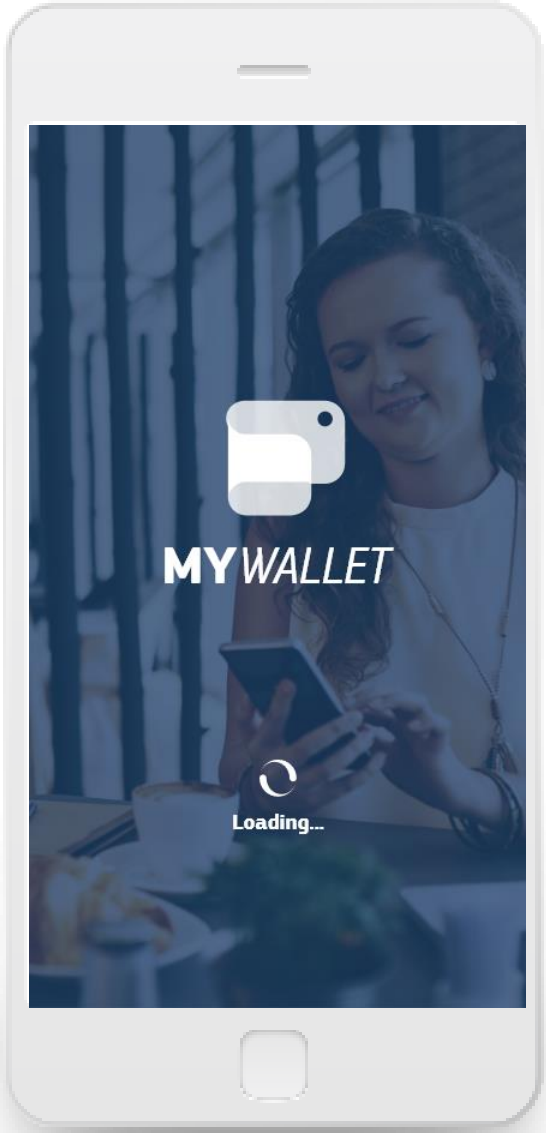
What happens here ?

The University back-office has issued the diploma and sends a notification to Eva **via e-mail or SMS** to inform her that her bachelor's degree is available. By clicking there the wallet is informed that there is a VC available to download. She arrives to the wallet and the wallet ask her to confirm. The process will ask to confirm the identity of the wallet



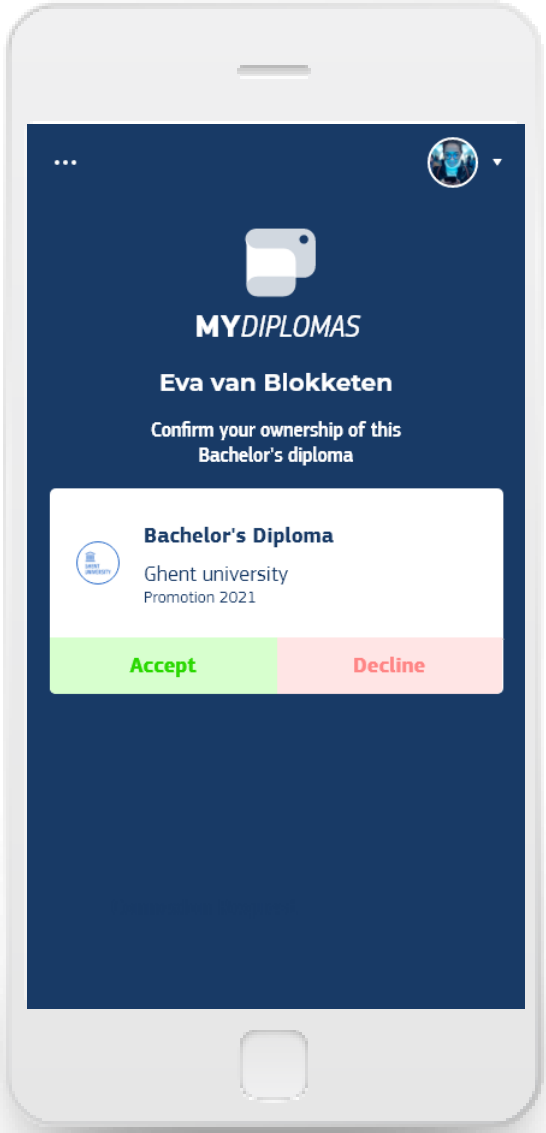
2.3. Eva receives and stores her Bachelor’s diploma in her wallet.

Once Eva clicks on the link from the SMS, she is immediately redirected to her wallet.



The wallet* asks Eva to confirm the good reception of the diploma. Eva confirms and stores it on the wallet.

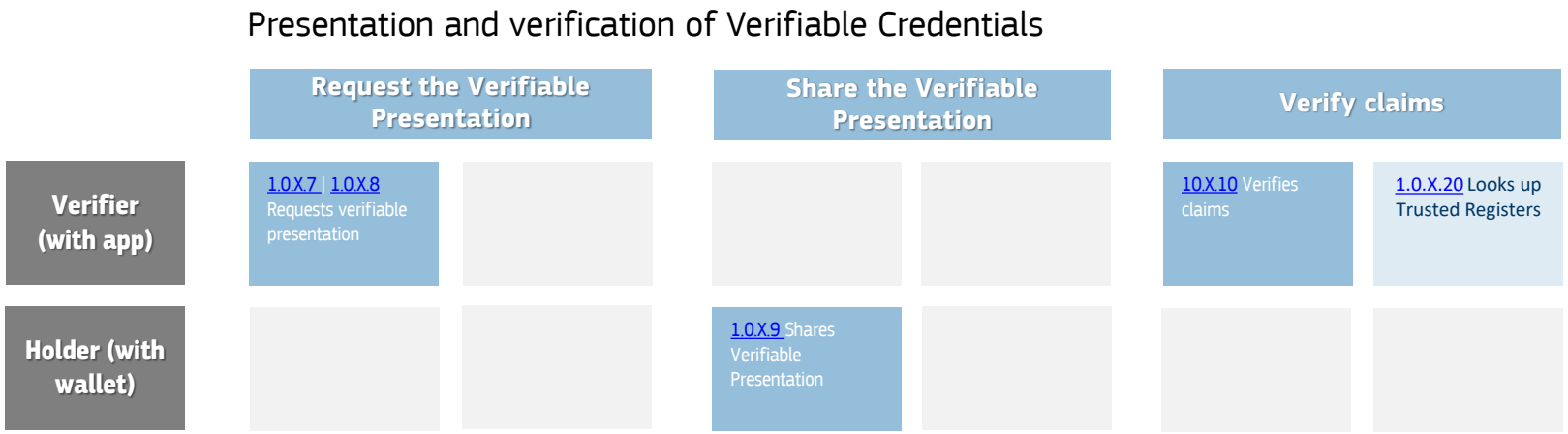
*The Wallet uses EBSI to verify the issuer, schema and accreditations.



3. Presentation and verification of the Verifiable Credentials

3. Presentation and verification

Presentation and verification of Verifiable Credentials

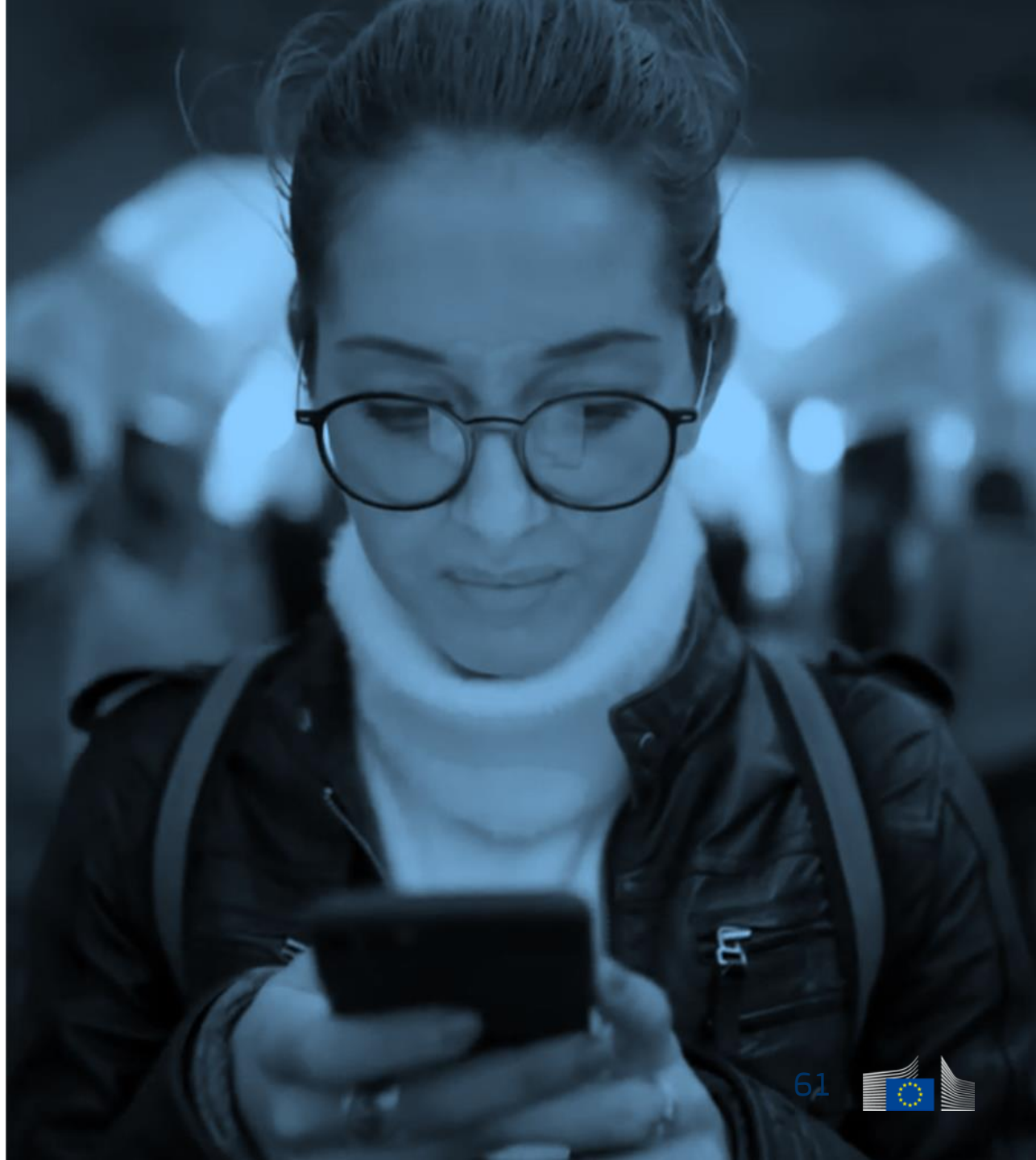


3. Presentation and verification of the Verifiable Credentials

3.1. Eva requests her enrolment at the University of Rovira i Virgili (ES).

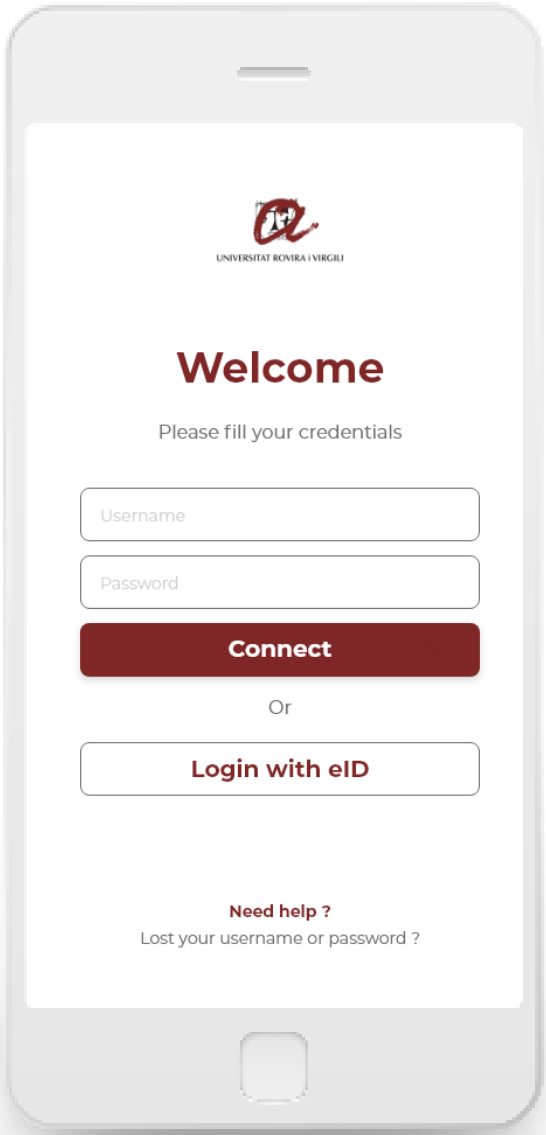
3.2. Eva shares her Bachelor's Diploma with the University of Rovira i Virgili.

3.3. The University of Rovira i Virgili verifies it. Eva enrolls for a Master's Degree

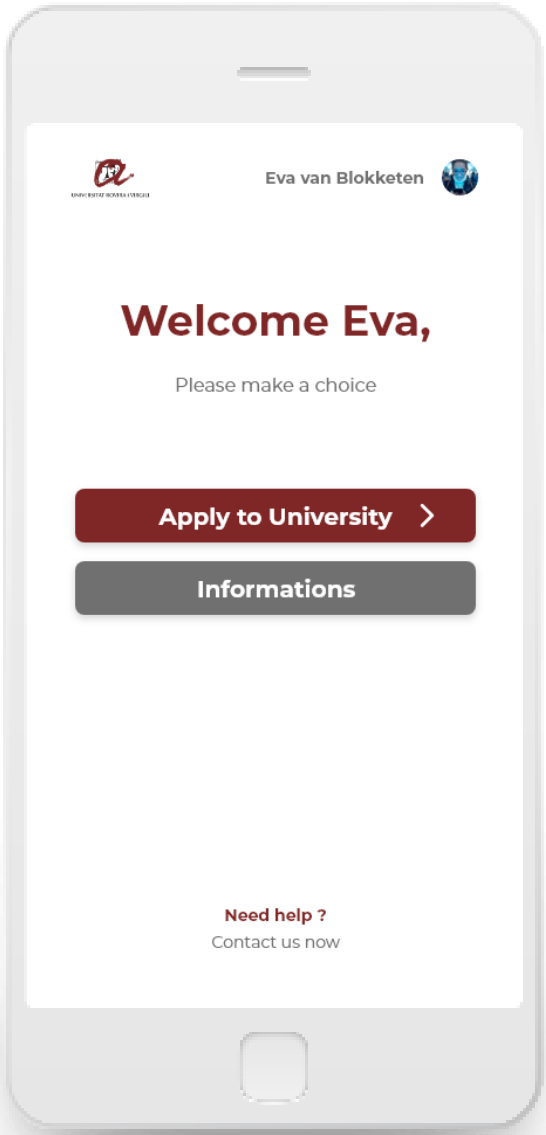


3.1. Eva requests her enrolment at the University of Rovira i Virgili (ES).

Eva authenticates to the platform of the University of Rovira I Virgili using a Spanish eID (e.g. from the University)

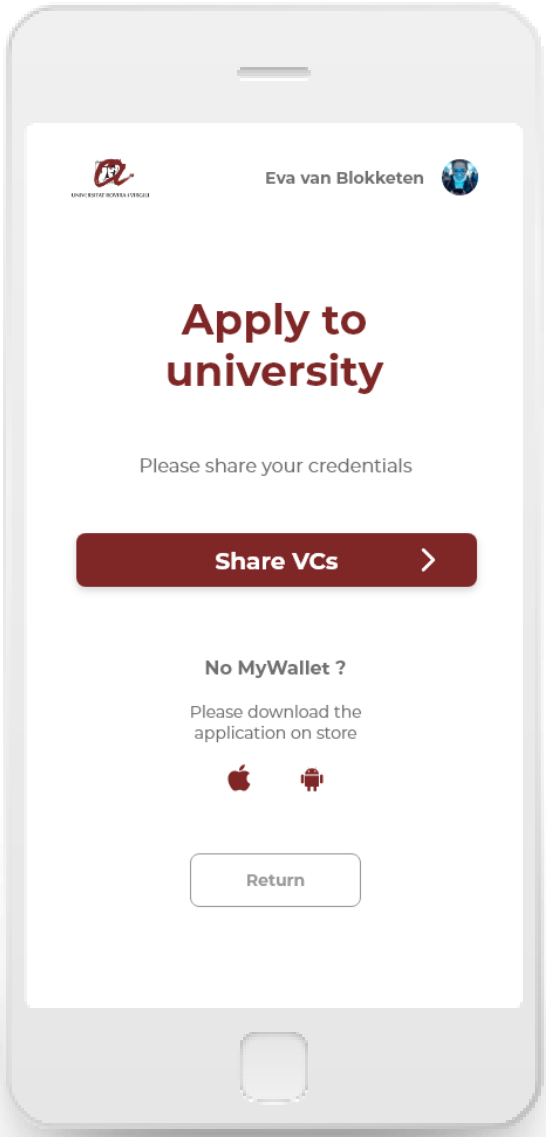


Eva initiates her enrolment to the University of Rovira I Virgili.



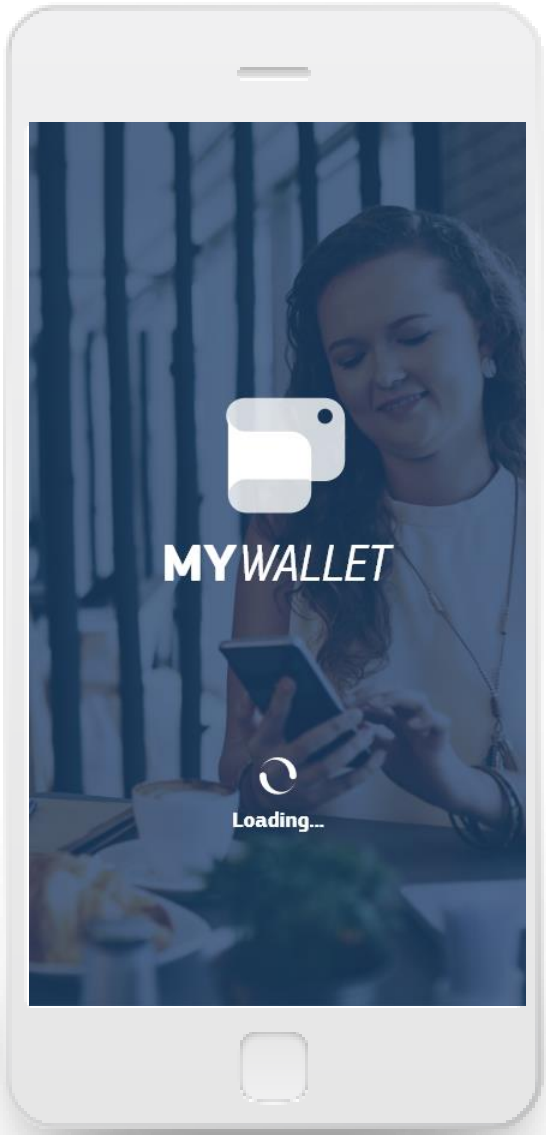
Platform asks Eva to share her credentials. Eva click on a button ”Share VCs” and is redirected to her wallet.

NB: due to technical limitations in case Eva has multiple wallets, Eva might select a wallet she wants to use to share her credentials.

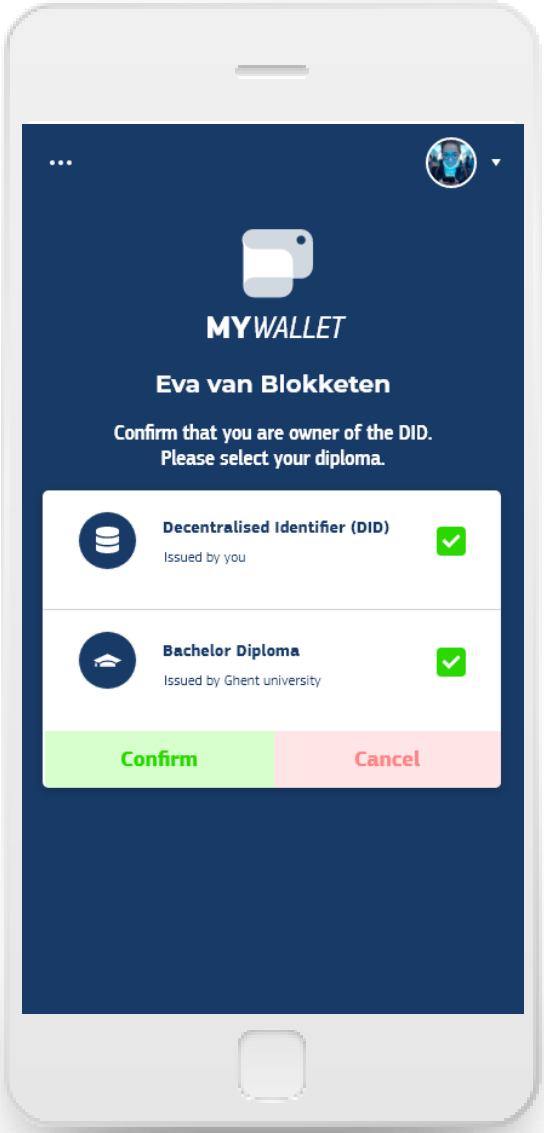


3.2. Eva shares her Bachelor’s Diploma with the University of Rovira i Virgili.

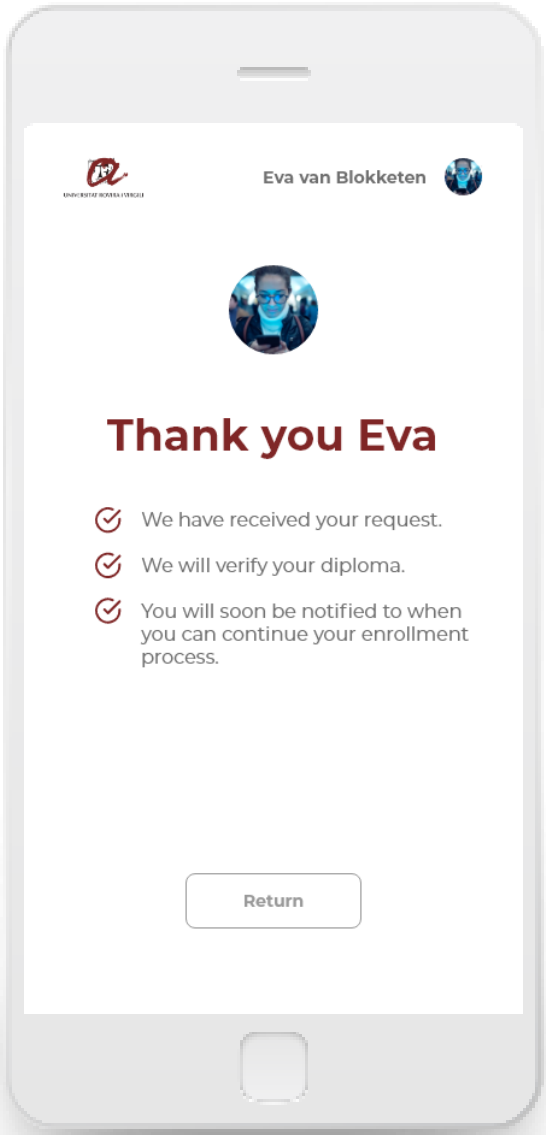
Eva is redirected immediately to her personal wallet.



The wallet asks Eva to confirm the sharing of her DID and diploma VC with the portal. Eva confirms control over her DID and the Diploma issued by the University of Ghent and submits them the University of Rovira I Virgili.

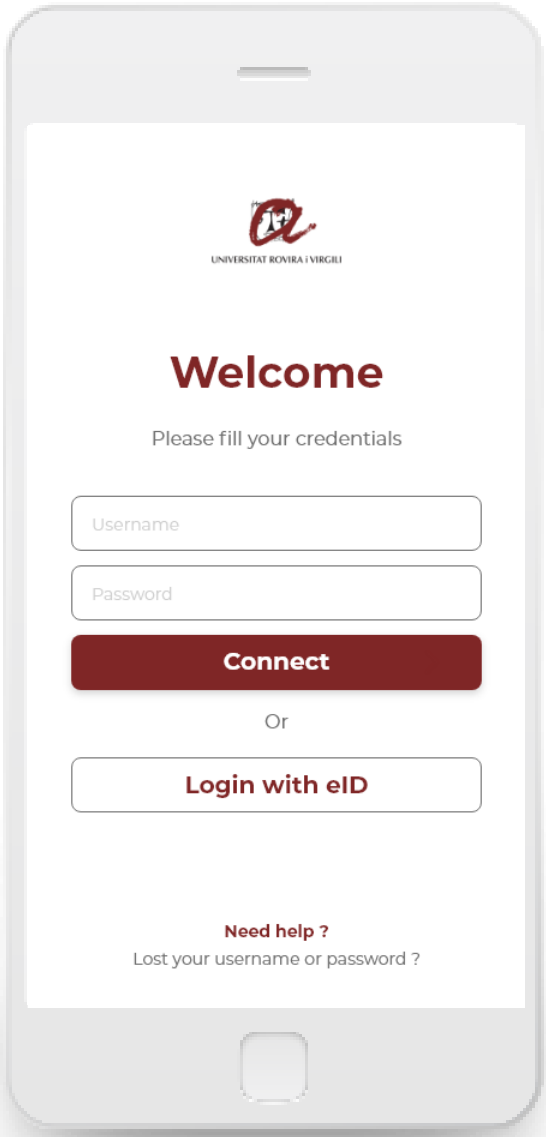


Eva is redirected to the portal of the University of Rovira I Virgili and receives a confirmation that the request for enrolment has been submitted and that she will soon receive a notification to continue the process.



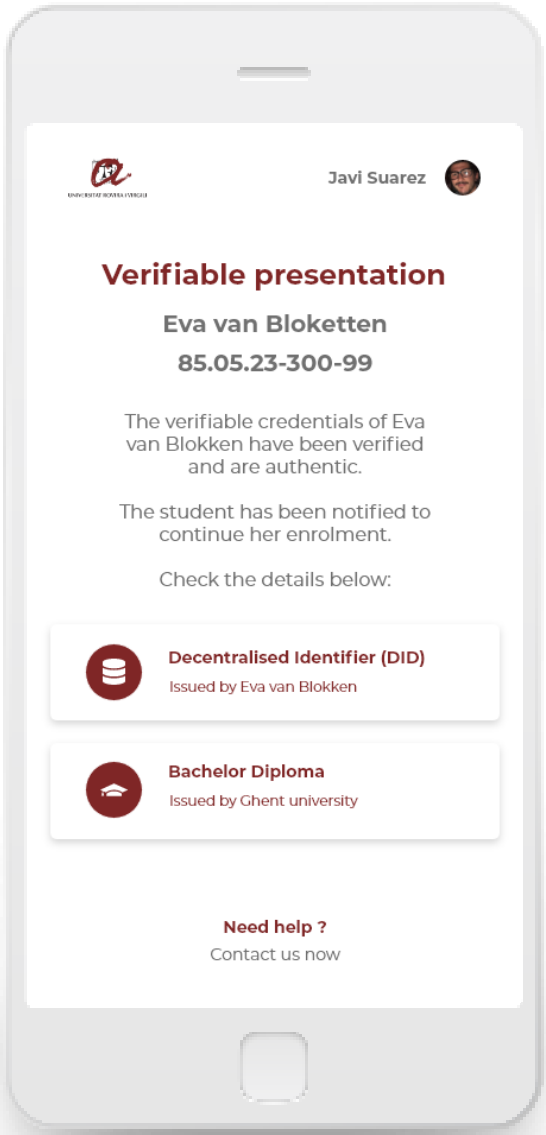
3.3. The University of Rovira i Virgili verifies it. Eva enrolls for a Master's Degree

The staff Member of the University of Riviria I Virgili authenticates to the portal.

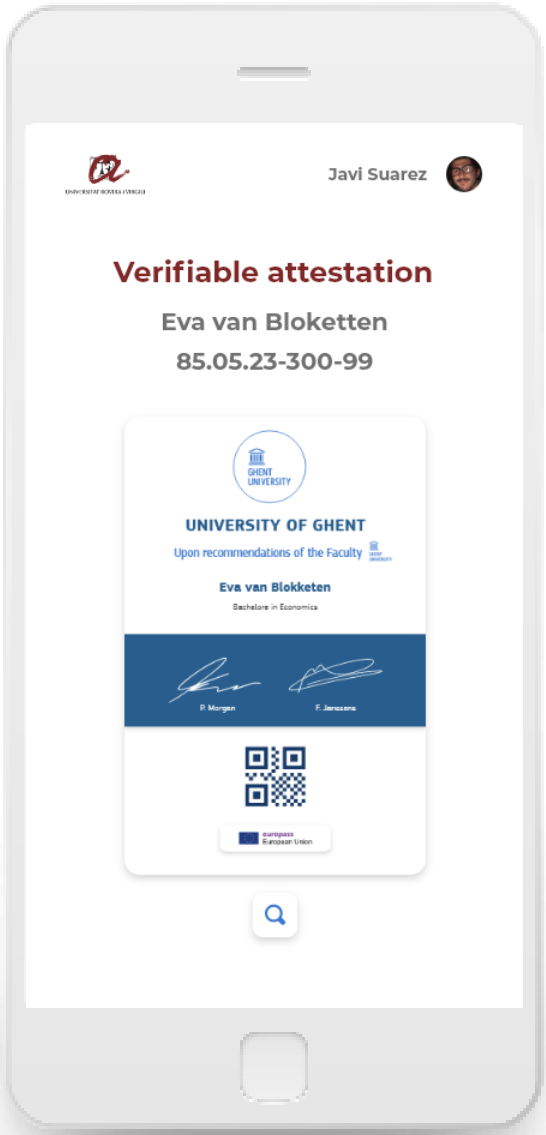


The credentials are automatically* verified by the system. The staff member of the University of Roviria I Virgili is informed that the credentials shared by Eva are authentic and that the student has been notified that she can continue her enrolment process.

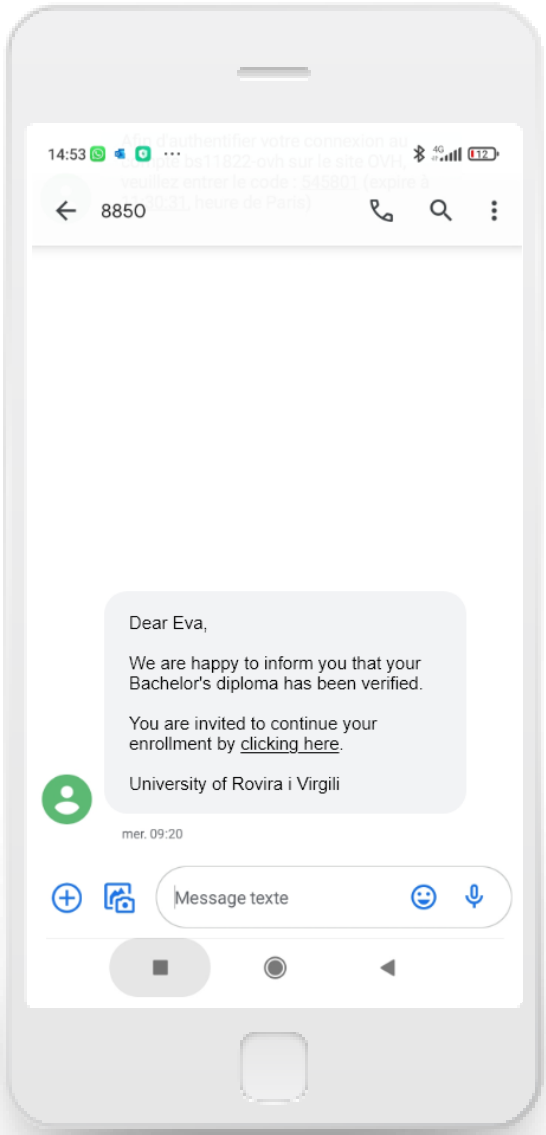
(*) Automatic verification is possible due to EBSI.



The staff member of the University of Roviria I Virgili can check further details about the Bachelor’s diploma of Eva.



Eva is notified that she can continue her enrolment process.

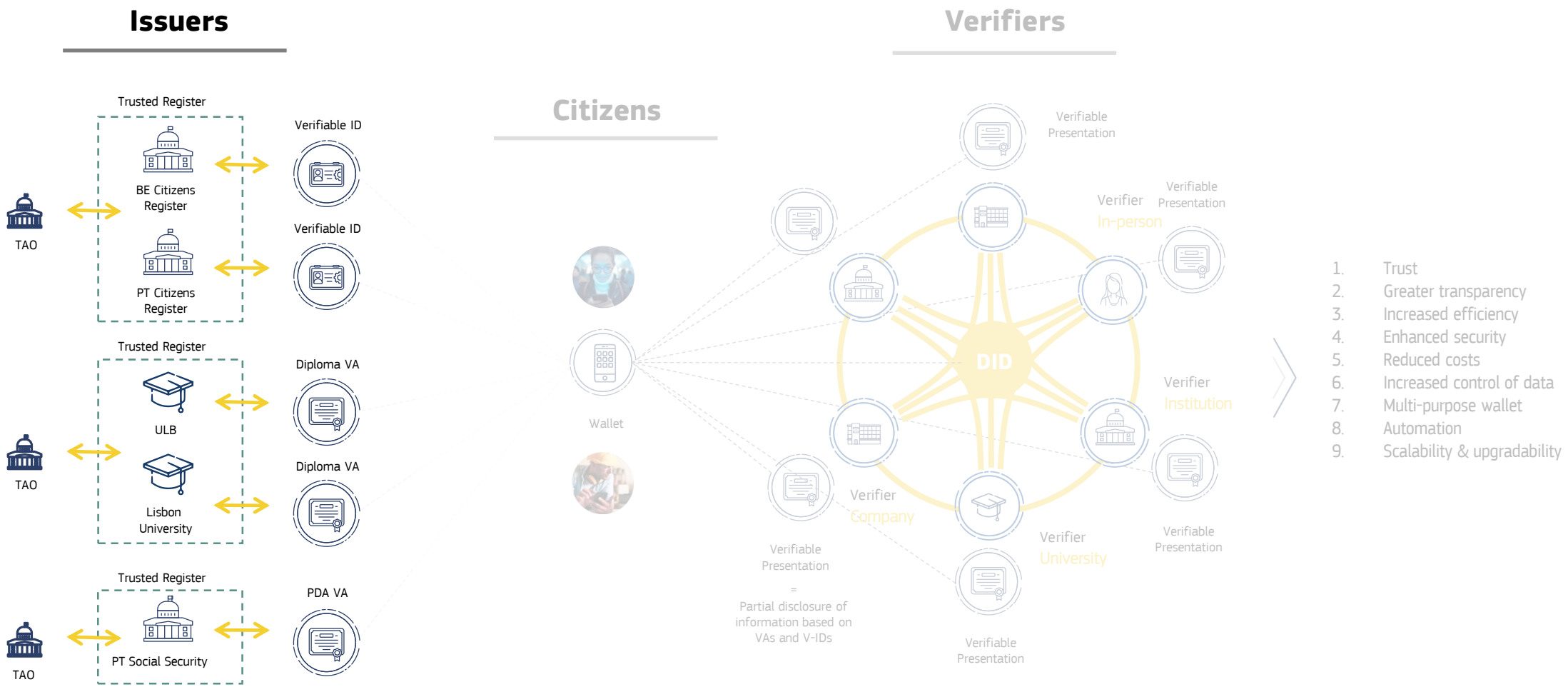


Summary of the value

Introduction

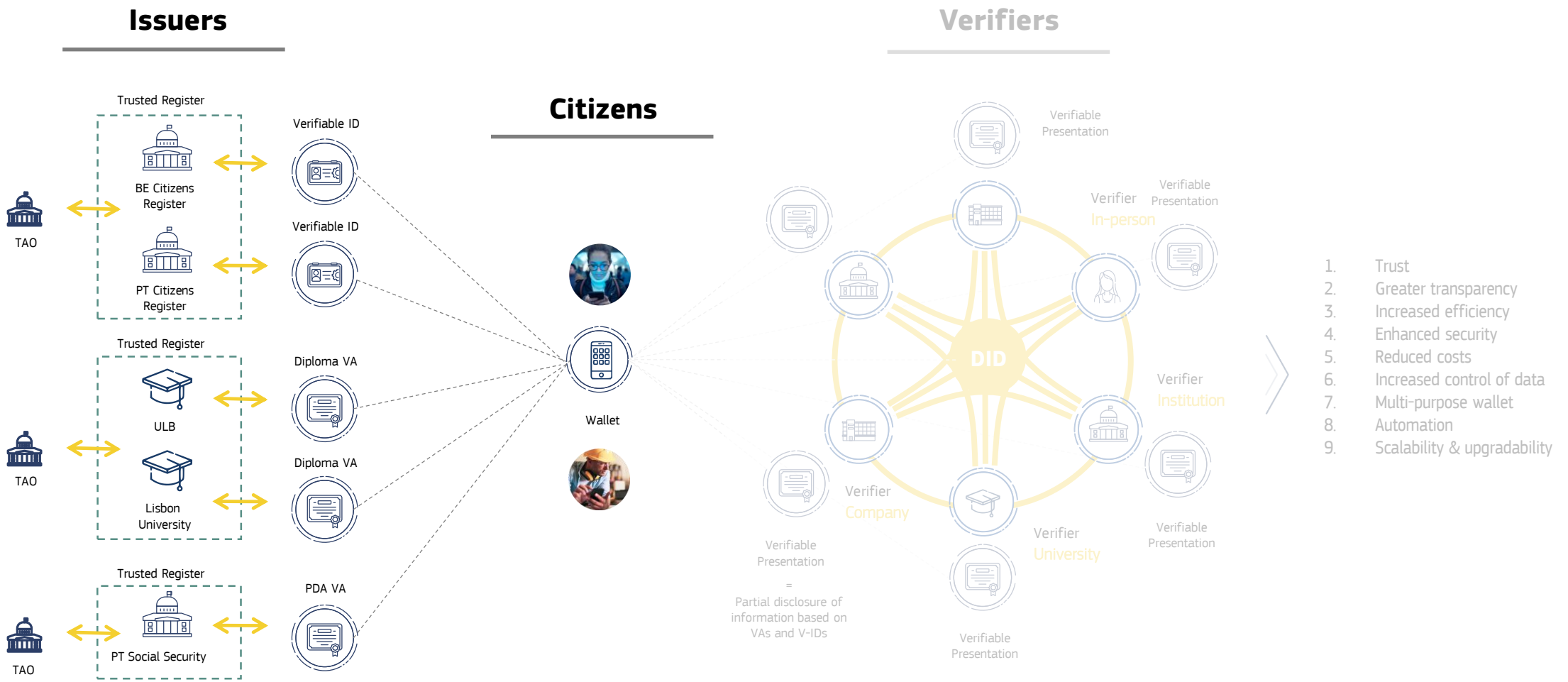
A new way for PAs to issue documents

EBSI provides a new way for PAs to issue documents thanks to a new trust chain and a new verifiable format.



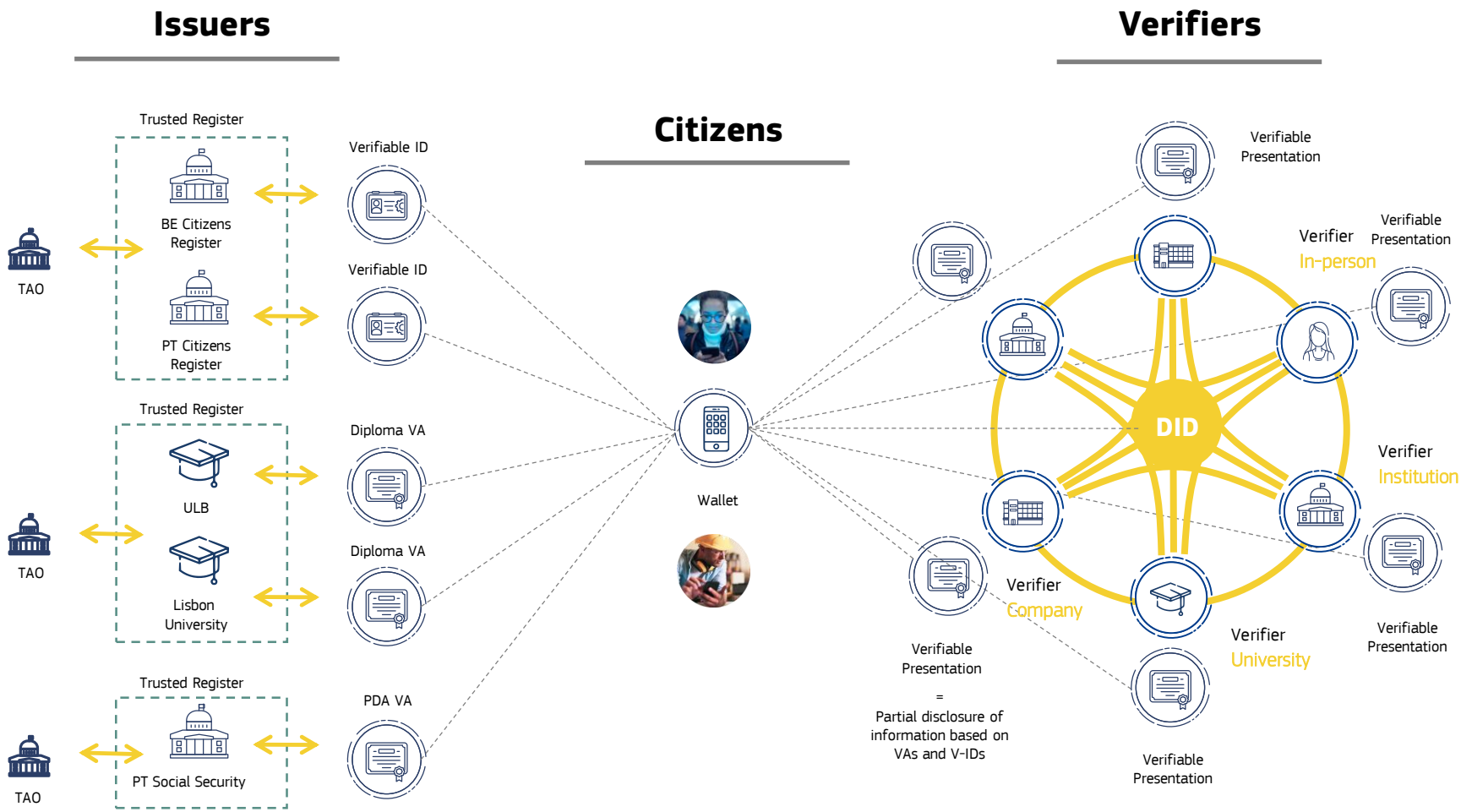
A new way for citizens to manage them

EBSI provides a new way for citizens to manage their documents through a digital wallet.



A new way for the ecosystem to verify them

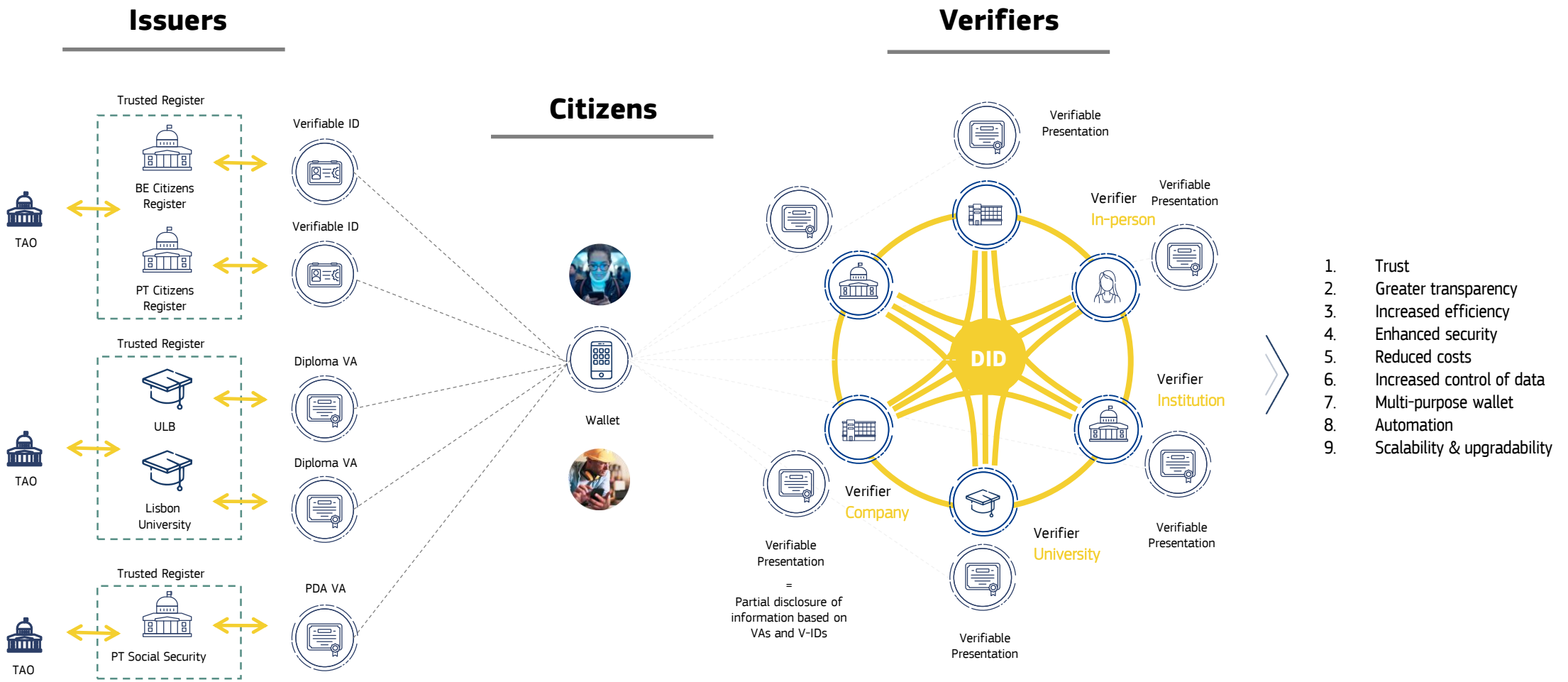
EBSI provides a new way an entire ecosystem of actors to verify these documents.



1. Trust
2. Greater transparency
3. Increased efficiency
4. Enhanced security
5. Reduced costs
6. Increased control of data
7. Multi-purpose wallet
8. Automation
9. Scalability & upgradability

A new way to create value.

EBSI provides a new way to create value for the ecosystem.



EBSI Use cases

EBSI Use cases, explained

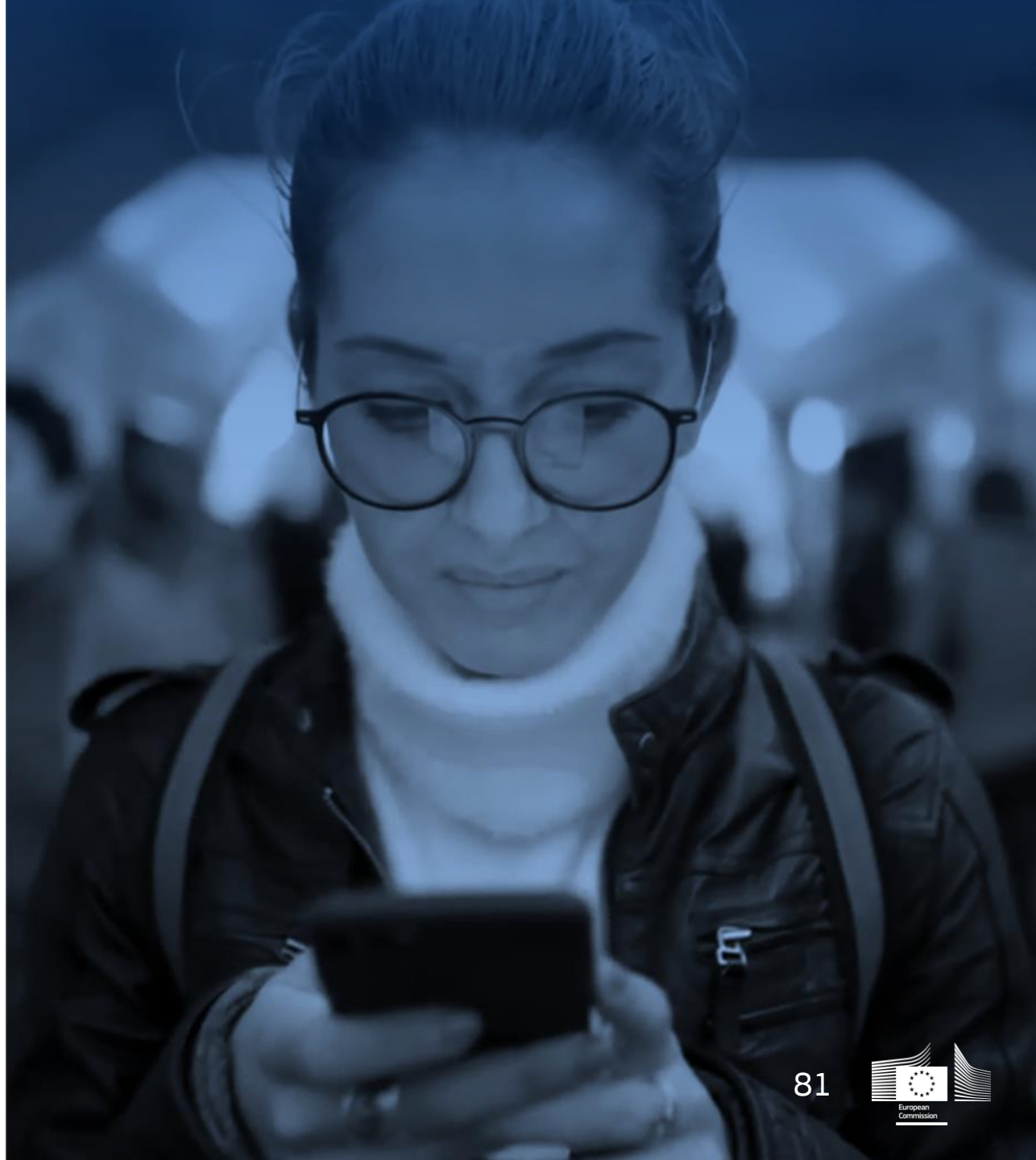
Studying abroad Use Case

What do we want to achieve?

The Diploma Use Case will demonstrate that EBSI can implement cross-border verification of educational credentials based on the Verifiable Credential lifecycle

This means that a verifiable attestation (such as a diploma) issued by Member State A can be verified by an university or third party, e.g. “employer” from Member State B.

The value proposition is the simplicity and reliability of the cross-border verification process.



Understanding the roles

Distribution of roles per Member State

MS A

Mobile

MS B

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

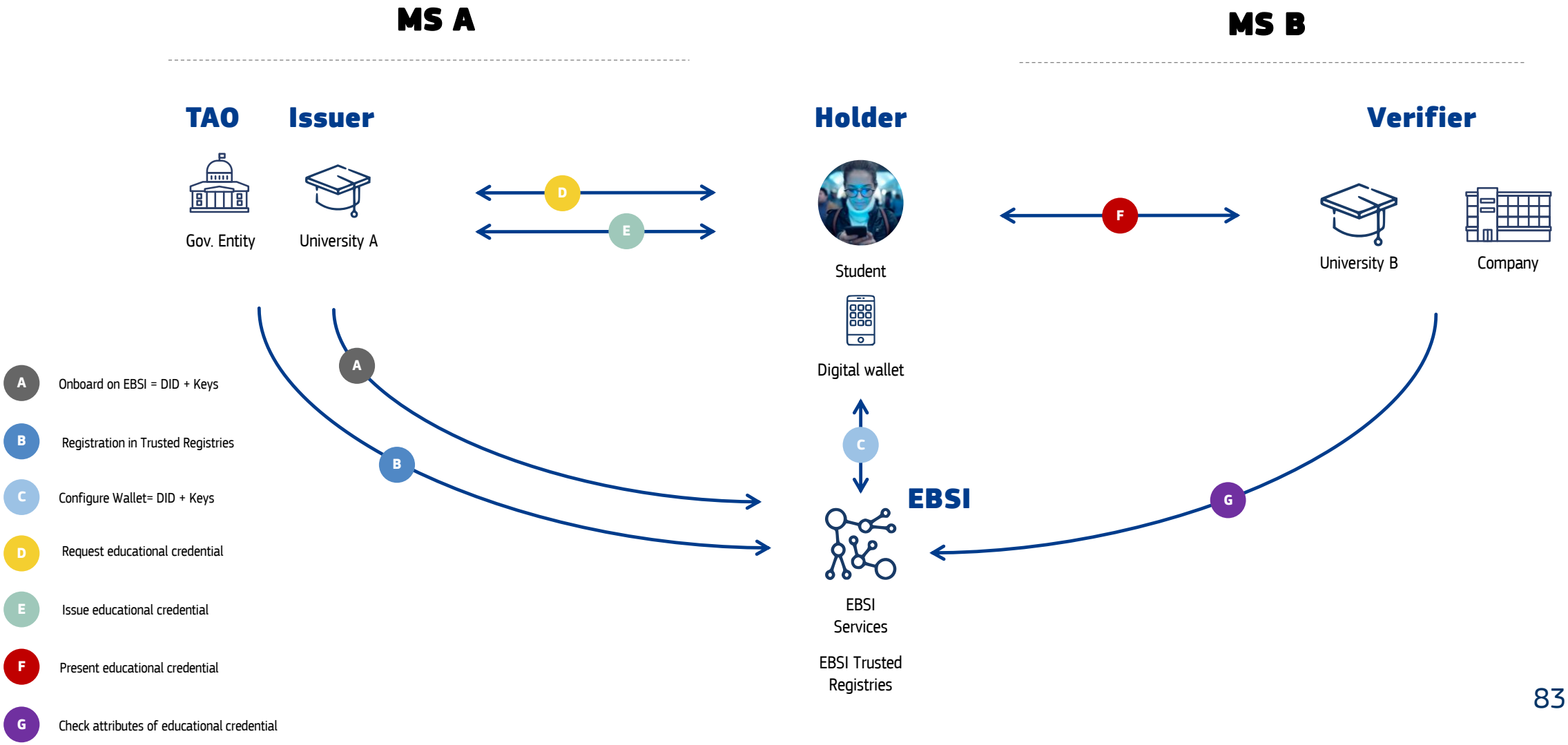
University B

Company

Verifies the educational credentials shared by the student

Scenario in practice

Who will participate in the scenario and what are the tools to be used?



Working abroad Use Case

What do we want to achieve?

The European Social Security Pass Use Case will demonstrate that EBSI can implement cross-border verification of social security coverage of posted workers, i.e. verification of the PDA-1 document.

This means that a Social Security competent institution in a Member State issues the PDA-1 document as a verifiable attestation and an inspector in another Member State verifies it.

The value proposition is the simplicity and reliability of the cross-border verification process.

Understanding the roles

Distribution of roles per Member State

MS A

Mobile

MS B

Trusted Accreditation Organisation (TAO)

Gov.
Entity

Registers issuers of PDA-1 credentials in the Trusted Register of Social Security Institutions

Issuer

Social Security
Competent
Institution

Issues PDA-1 upon the request of the employer

Holder

Posted
Worker

Receives PDA-1 and presents it to the inspector

Verifier

Inspector

Verifies the PDA-1

Understanding the roles

Distribution of roles per Member State

MS A

Trusted Accreditation Organisation (TAO)

Gov.
Entity

Registers issuers of PDA-1 credentials in the Trusted Register of Social Security Institutions

Issuer

Social Security
Competent
Institution

Issues PDA-1 upon the request of the employer

Mobile

Holder

Posted
Worker

Receives PDA-1 and presents it to the inspector

MS B

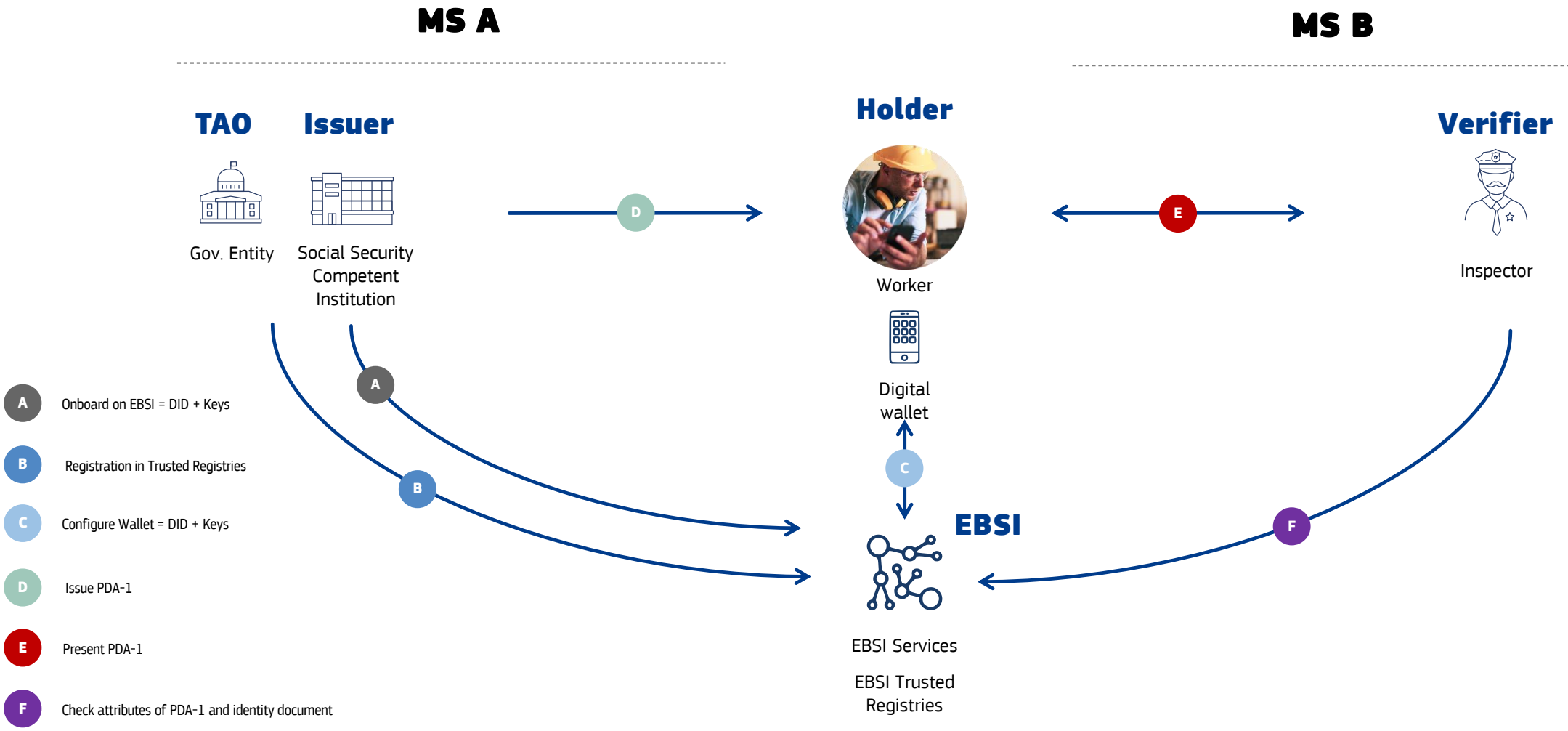
Verifier

Inspector

Verifies the PDA-1

Scenario in practice

Who will participate in the scenario and what are the tools to be used?



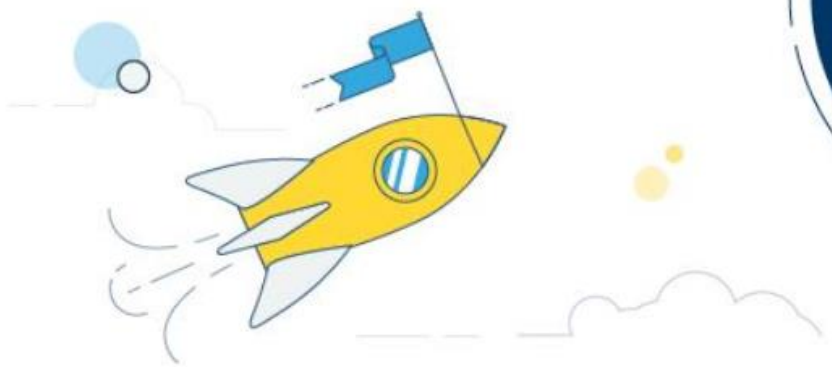
09

EA Programme / MU Pilot

Piloting with Member States

Early Adopters Programme. Imagining what EBSI can do for European citizens.

An incubator to help Early Adopters and their partners imagine, build and launch their blockchain pilot project(s).



Evolving towards a cross border MU pilot

Towards a cross-border pilot

Wave 1

From **April until now**

10

Projects started to experiment with EBSI by taking part in the Wave 1 of the EA Programme. Today, these projects are all building their solutions.

Wave 2

From **July until now**

18

Projects started to experiment with EBSI by taking part in the Wave 2 of the EA Programme.
Today, these projects will soon start building their solutions.

Together

Multi-university pilot

22

We launched the MU pilot and invited all projects to take part in it. Today, 22 projects from both waves (14 projects from Wave 2) are designing their solutions together.

MU PILOT JOURNEY

EBSI Multi-University Pilot

DISCOVER

01/07

MU PILOT KICK-OFF

DESIGN

27/09

DESIGN WORKSHOP

BUILD

22/10

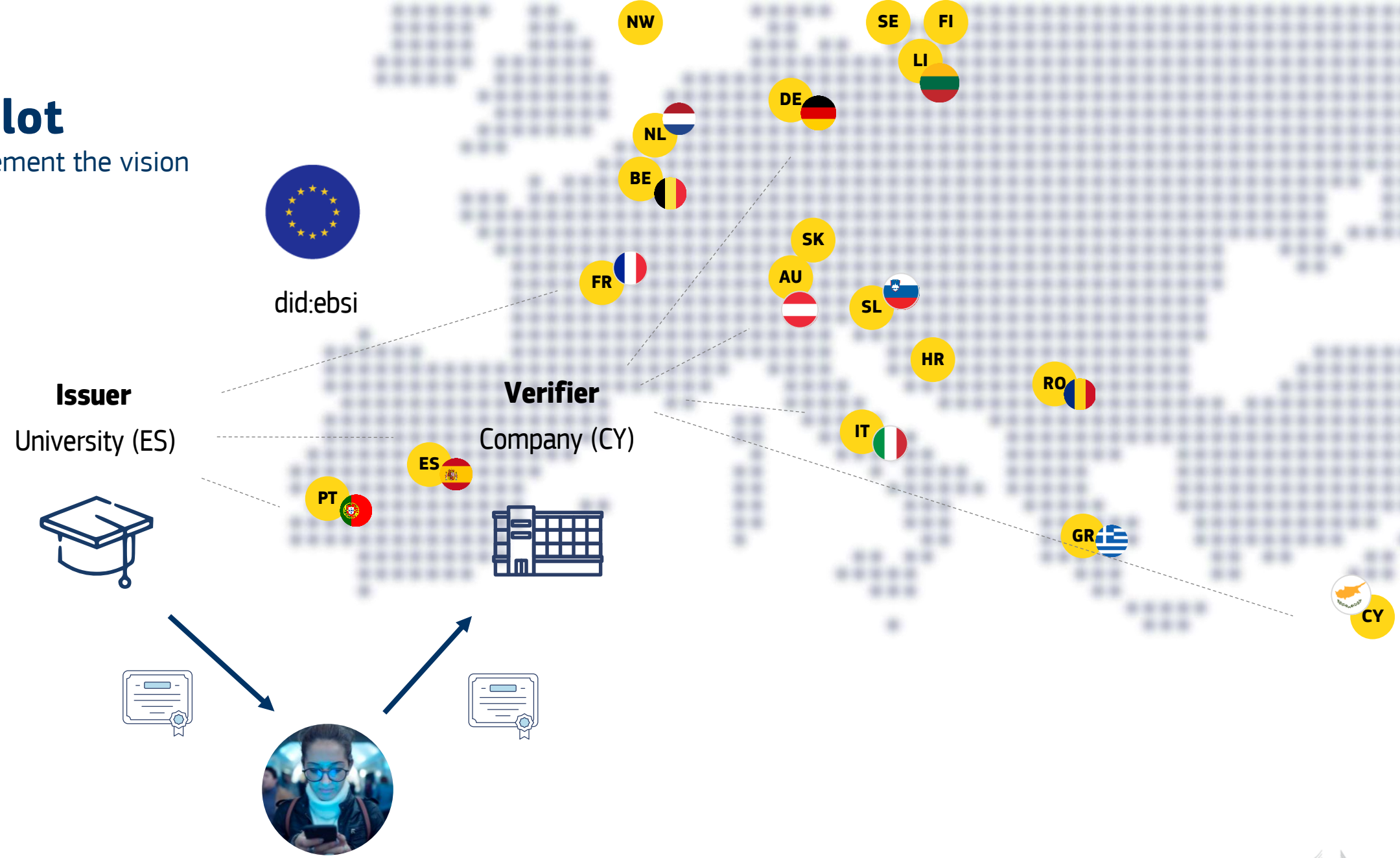
PREPARE FOR INTEGRATION

END OF NOVEMBER

INTEGRATION IN PRE-PROD & CONFORMANCE TEST

MU Pilot

Let's implement the vision



They are designing the MU Pilot

2 European universities alliances, +18 universities from +15 countries

Clusters to facilitate collaboration

After the Design workshop, we created different functional clusters to facilitate collaboration

CLUSTER 1
Verifiable Identity and Full journey

- Slovak national EBSI node (SK)
- Impulse (EU)
- Eva's journey in a real Spanish setting (ES)
- CY-EBSI (CY)
- Croatia Diploma (CroEduPass) (HR)
- A passport grade implementation and wallet for ESSIF (NL)

CLUSTER 2
Diploma credentials journey

- UniCert (IDunion) (DE)
- EBSILUX (LU)
- EBSI4Austria (AU)
- Germany-NRW (DE)
- DE4A (EU)
- POPCORN (FR)
- Eledger (GR)
- EBSI4RO (RO)
- Fr.EBSI (FR)
- Diplo.me (IT)

CLUSTER 3
Other educational credentials journey

- AOC (ES)
- Una Europa (BE)
- DLTNode (LT)
- Microblock (FI)

CLUSTER 4
Base capabilities for education

- DEQAR (EU)

9 cross-border scenarios can be delivered in 2021 (*)

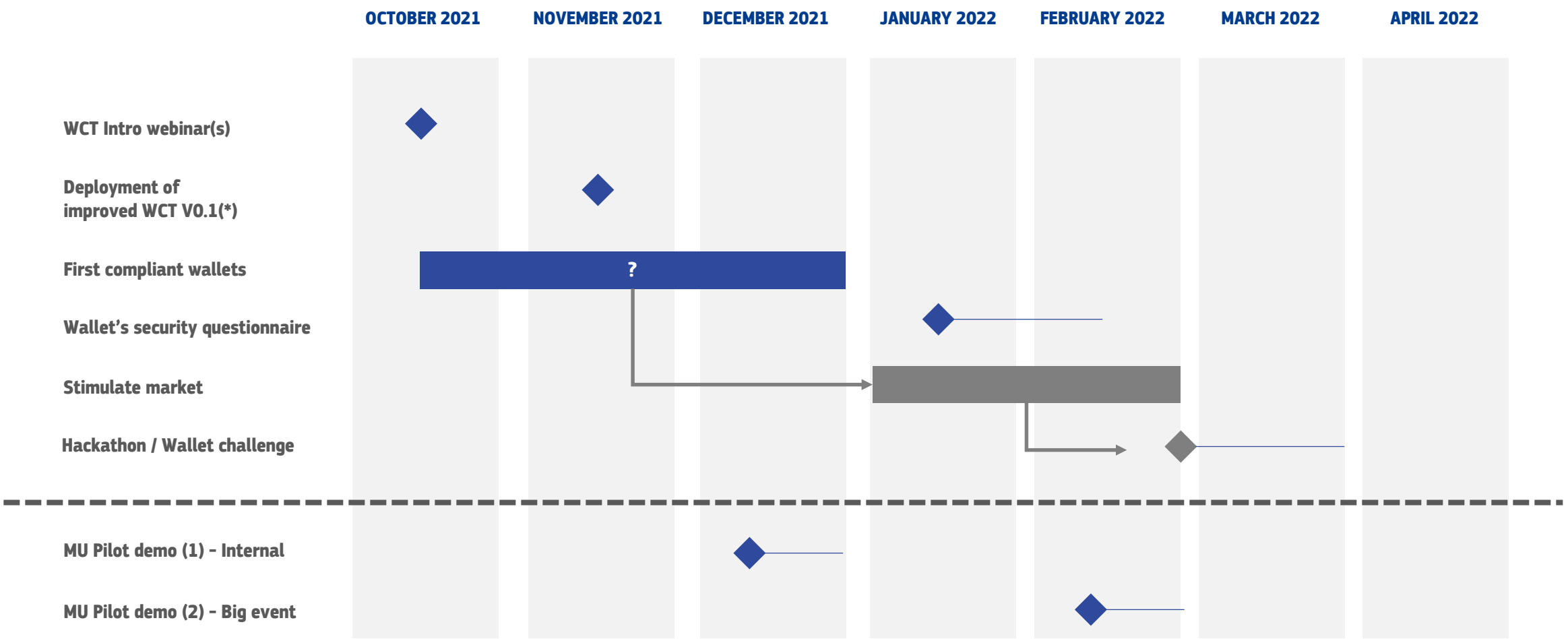
23 scenarios identified, 14 are cross-border (60%) and 9 (cross-border) will be delivered in 2021!

Scenario	Issuer	Country of the Issuer		VC type		Verifier	Country of the Verifier	DEC 2021*	Q1 2022
Scenario 1	Fabrica National De Moneda	Spain	will issue	V.ID	that is verified by	Univ R&V	Spain	✓	
Scenario 2	Univ R&V	Spain	will issue	V.Attestation (student ID)	that is verified by	Univ R&V	Spain	✓	
Scenario 3	Slovakia eID	Slovakia	will issue	V.ID	that is verified by	Demo bank	Slovakia	✓	
Scenario 4	Slovakia eID	Slovakia	will issue	V.ID	that is verified by	Univ R&V	Spain	✓	
Scenario 5	Fabrica National De Moneda	Spain	will issue	V.ID	that is verified by	Demo bank	Slovakia	✓	
Scenario 6	RvIG	NL	will issue	V.ID					✓
Scenario 7	RvIG	NL	will issue	Trusted Issuer (university)					✓
Scenario 8	Government portal (ARIADNI)	Cyprus	will issue	V.ID	that is verified by	(a) Univ Nicosia (b) GUNet - eDiplomas.gr	(a)Cyprus (b)Greece	✓	
Scenario 9	Univ Nicosia	Cyprus	will issue	Diploma credentials	that is verified by	ETEK			✓
Scenario 10	ETEK	Cyprus	will issue	License practice credentials					✓
Scenario 11	GUNet (Greek Universities Network)	Greece	will issue	Diploma credentials to a Cyprus citizen	that is verified by	ETEK	Cyprus	✓	
Scenario 12	Sample/Dummy Municipality	Europe	will issue	V.ID	that is verified by	Sample/Dummy Municipality	Europe		✓
Scenario 13	Technical University of Berlin	Germany	will issue	Bsc Computer Science	that is verified by	Agency for Science and Higher Education	Croatia		✓
Scenario 14	Technical University of Berlin	Germany	will issue	Bsc Computer Science	that is verified by	WU Wien, TU Graz (EBSI4Austria)	Austria	✓	
Scenario 15	Politehnica University of Timisoara	Romania	will issue	Electronics Engineer Diploma	that is verified by	University of Lille	France		✓
Scenario 16	University of Athens	Greece	will issue	University Diploma	that is verified by	Politehnica University of Timisoara	Romania		✓
Scenario 17	University of Lille	France	will issue	Certified Translation	that is verified by	University of Athens	Greece		✓
Scenario 18	KU Leuven university	Belgium	will issue	a Student id (V.Attestation)	that is verified by	Università di Bologna	Italy	✓	
Scenario 19	Università di Bologna	Italy	will issue	a Transcript of Records (V.Attestation)	that is verified by	KU Leuven university	Belgium	✓	
Scenario 20	Tampere	Finland	will issue	micro-credential	that is verified by	KTU	Lithuania		✓
Scenario 21	KTU	Lithuania	will issue	micro-credential	that is verified	Tampere	Finland		✓
Scenario 22	AOC	Spain	will issue	a verifiable ID	that is verified by	KU Leuven university	Belgium	✓	
Scenario 23	KU Leuven university	Belgium	will issue	a Student id V.Attestation	that is verified by	AOC	Spain	✓	

(*) cross-border scenarios that will be delivered in December 2021 and present at Quarterly meeting on 9th and 10th of December

What are the next milestones?

What are the next milestones regarding WCT and MU Pilot?



(*) not fully automated yet – foreseen end 2021

Ready and open to stimulate the European market for creating EBSI-compliant wallet.

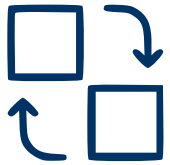
Current list of wallet providers

Current list of wallet providers and their status regarding WCT

Country	Initiative	Driven by national public sector	Wave	Sourcing solution	Wallet solution and provider	WCT Status
Europe	IMPULSE	No	2	Solution provider	InfoCert & Gradiant wallet use libs by SSIKIT	
Croatia	CroEduPass	Yes	2	Solution provider	Identyum wallet	
Cyprus	CY-EBSI	Yes	2	Custom solution	CY-EBSI wallet	
Slovakia	Slovak national EBSI node	Yes	1-M	Custom solution	Custom wallet by DXC-Slovakia	
Spain	Eva's journey in a real Spanish setting	Yes	1-M	Solution provider	GATACA IDENTITY by GATACA	
The Netherlands	A passport grade implementation and wallet for ESSIF	Yes	1-I	Solution provider	GATACA IDENTITY by GATACA, ESATUS WALLET by ESATUS	
Germany	UniCert	No	2	Solution provider	ESATUS WALLET by ESATUS	
France	POPCORN	No	2	Solution provider	PWA by UNIKNAME	
Luxembourg	EBSILUX	Yes	2	Solution provider	Walt.ID by WALT.ID	
Greece	ELEDGER	Yes	2	Custom solution	Custom wallet by eLedger	
Austria	EBSI4Austria	No	1-M	Solution provider	VERES WALLET by DIGITALBAZAAR via Danubetech	
Germany	Germany-NRW	Yes	1-M	Solution provider	Walt.ID by WALT.ID	
France	Fr.EBSI	Yes	1-M	Solution provider	BCdiploma wallet	
Italy	Diplo.me	No	1-I	Custom solution	Diplo.me	
Romania	EBSI4RO	Yes	2	Solution provider	BCdiploma wallet, Walt.ID by Walt.ID, CERTME by CERTSIGN	
Slovenia	DE4A	Yes	1-I	Custom solution	Custom wallet by DE4A via Hyperledger Aries and Walt.ID	
Spain	Social benefits for citizens (AOC)	Yes	2	Solution provider	Vidchain by ValidateID	
Belgium	Una Europa exchange	No	2	Solution provider	GATACA Identity by GATACA	
Lithuania	DLTnode	No	2	Solution provider	Walt.ID, Protokol wallet	
Finland	Microblock	No	2	Solution provider	Walt.ID by WALT.ID	
Spain	Eva's journey in a real Spanish setting	Yes	1-M	Solution provider	GATACA Identity by GATACA	
Europe	DEQAR	Yes	2	Solution provider	Walt.ID by WALT.ID	
Slovenia	SI Blockchain	Yes	2	Solution provider	Hashnet by Tolar.net	

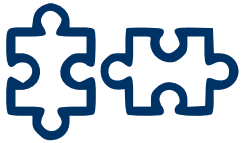
Services to support the Early Adopters

What are the services we provide to support to the Early Adopters?



EBSI's Verifiable Credentials Lifecycle for Early Adopters

Navigating EBSI's Verifiable Credentials Profile



EBSI Verifiable Credentials Playbook for Early Adopters

Creating EBSI's Verifiable Credentials Profile containing all the EBSI specifications.

EBSI Wallet Conformance Testing for Early Adopters

Verifying the conformance of a wallet with EBSI specifications and standards.

Get started

How to get started with EBSI?

All of this can be done across domains

All of this can be done across domains

Food / Beverage

I want to guarantee / verify the **origin / authenticity of a product (e.g. organic product)**

Business

I want to guarantee / verify **the origin of funding.**

Health

I want to guarantee / verify the origin / authenticity of **a health certificate.**

Administration

I want to guarantee / verify the origin / authenticity of a **birth certificate**.

Transport

I want to guarantee / verify the origin / authenticity of **the consignments transported**.

Audit

I want to guarantee / verify the origin of **publications / books of accounts**

Diploma

I want to guarantee / verify the origin of diploma credentials

Identity

I want to guarantee / verify the authenticity of the identity of a person / legal entity

Energy

I want to guarantee / verify my **energy consumption is green.**

Law

I want to guarantee / verify the origin / authenticity of **the apostille**

Get started with EBSI

How to get started?

You are interested to know more about EBSI? Visit our website. Watch the videos and consult the full set of documentation.

https://ec.europa.eu/cefdigital/ebsi

You are a Public Administration and you want to use EBSI for your project? Join the Early Adopter Programme.

https://ec.europa.eu/cefdigital/wiki/x/PgIdGQ

You are a solution provider and you want to build an EBSI-compliant wallet? Verify the conformance of your wallet with EBSI specifications and standards.

https://ec.europa.eu/cefdigital/wiki/x/PgIdGQ

Ready to get started?

Reach out to us to learn more!
Send an e-mail to EU-EBSI@ec.europa.eu