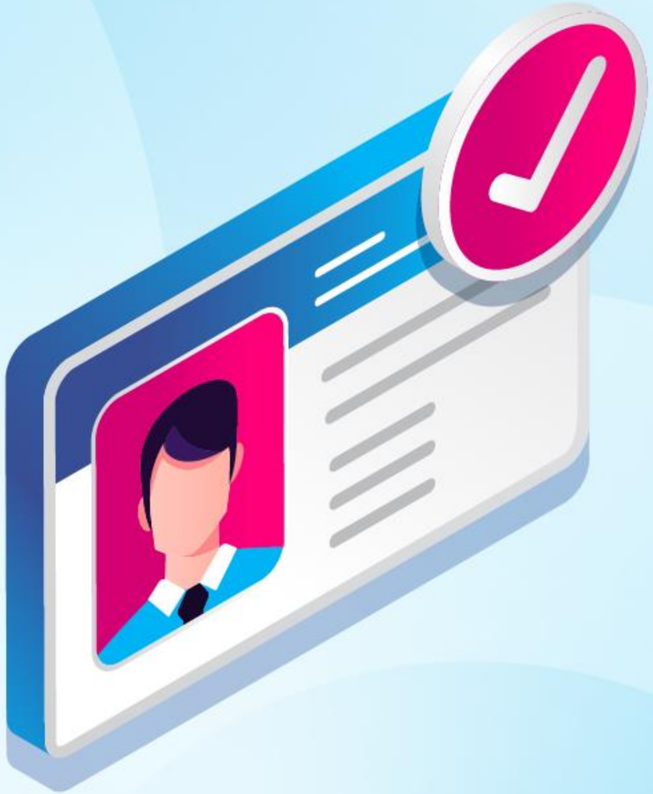
EBSI Verifiable Credentials explained



CHAPTER 1

EBSI Verifiable Credentials

June 2022

European Commission | ebsi European Blockchain

EBSI, explained – first edition

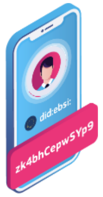
What are the different chapters of this first edition?

01.

Verifiable Credentials Explained

02.

Verifiable Credentials in action



03.

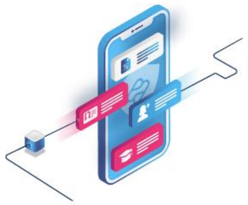
Decentralised Identifiers (DID) Methods

04.

Digital Identity

05.

Issuers Trust Model



06.

Open ID Connect for Verifiable Credentials

07.

Digital Wallets

01. Verifiable Credentials explained – Index

What are you going to learn in this Chapter?

01.1

Why Verifiable Credentials?

01.2

What are Verifiable Credentials?

01.3

How do Verifiable Credentials work?

01.

Why Verifiable Credentials?

Verification of documents and information remains challenging.

This is why we need to invest in technology that can help us to easily verify documents and information

17 billion

Money laundering through falsification

110 billion euros are said to be laundered in the European Union through the forging of documents

17 million

Illegal products and counterfeits

According to a report by the European Commission, last year, customs seized 17 million items (e.g. counterfeits) at the borders of Europe for a total value of 740 million euros.

30 million

Stolen / lost documents

In the last years, Interpol has seen a sharp uptick in the number of missing passports — within Europe and around the globe. In Europe the amount reached 30 million in 2015 and +60 million in the world. The latest would be estimated to 89 million in 2020 (Interpol).

20%

Fake labels on food and beverage

One in five labels in Europe would be false and therefore show a lack of compliance with European rules

?

Fake COVID-19 tests

As long as travel restrictions remain in place due to the pandemic. it is very likely that criminals will seize the opportunity of producing and selling fake COVID-19 test certificates. Several cases have already emerged of fraudulent COVID-19 test certificates being sold to travelers (Europol)

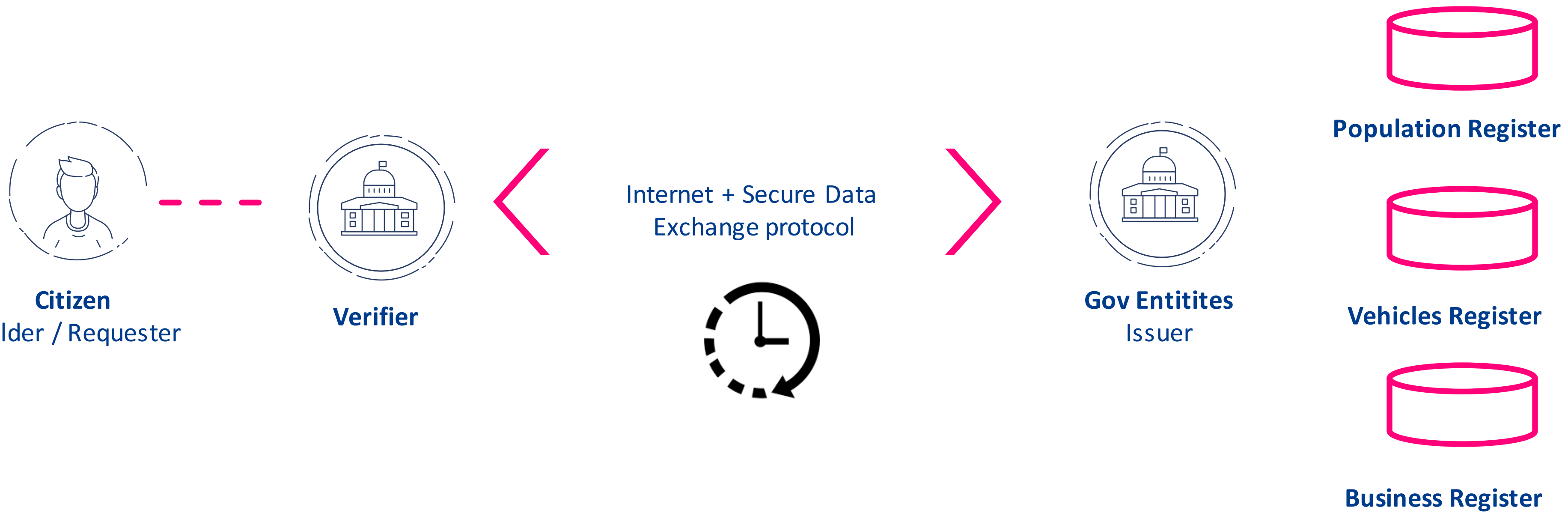
Documents are easy to fake and difficult to verify.

The creation of national registers was a major advancement to distinguish fake from real information.

Authentic data sources are now digital and online

But real-time access is often not possible, this is done by intermediaries

Verification by accessing the authentic sources of information is often intermediated (i.e. an entity on behalf of another entity)



Citizen
Holder / Requester

Verifier

Internet + Secure Data
Exchange protocol

Gov Entitites
Issuer

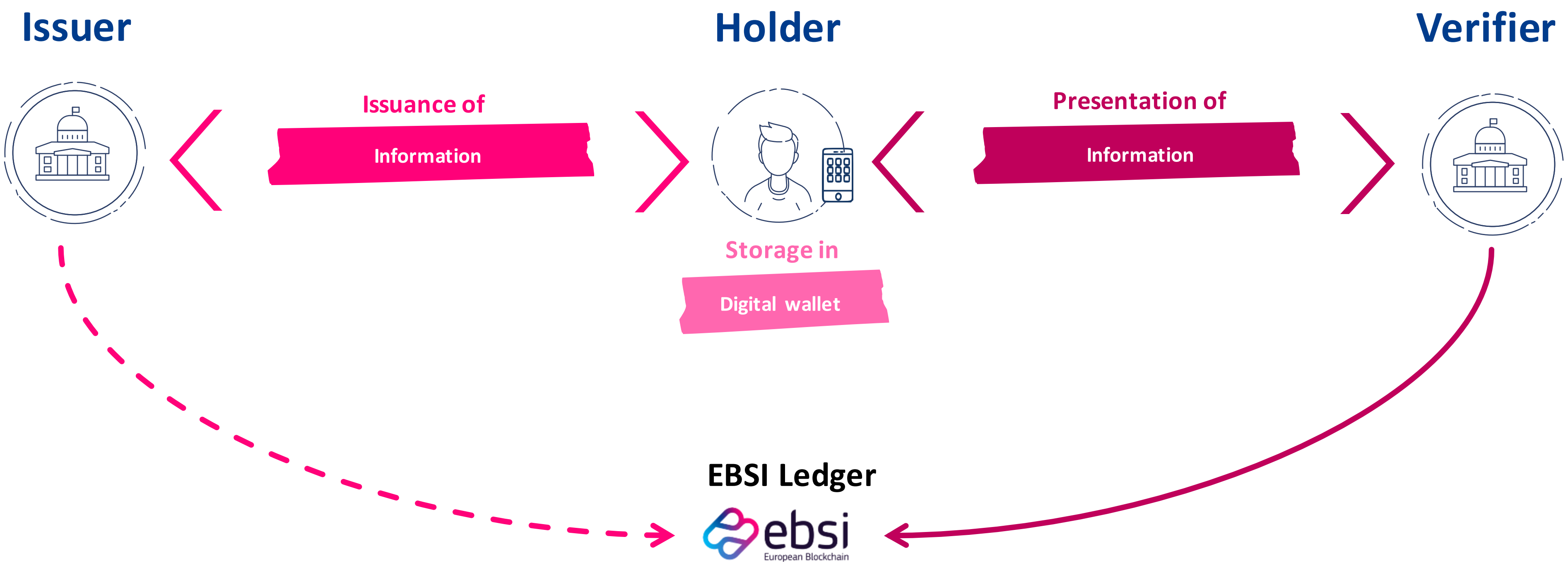
Population Register

Vehicles Register

Business Register

Direct verification/ self-sovereign scenario.

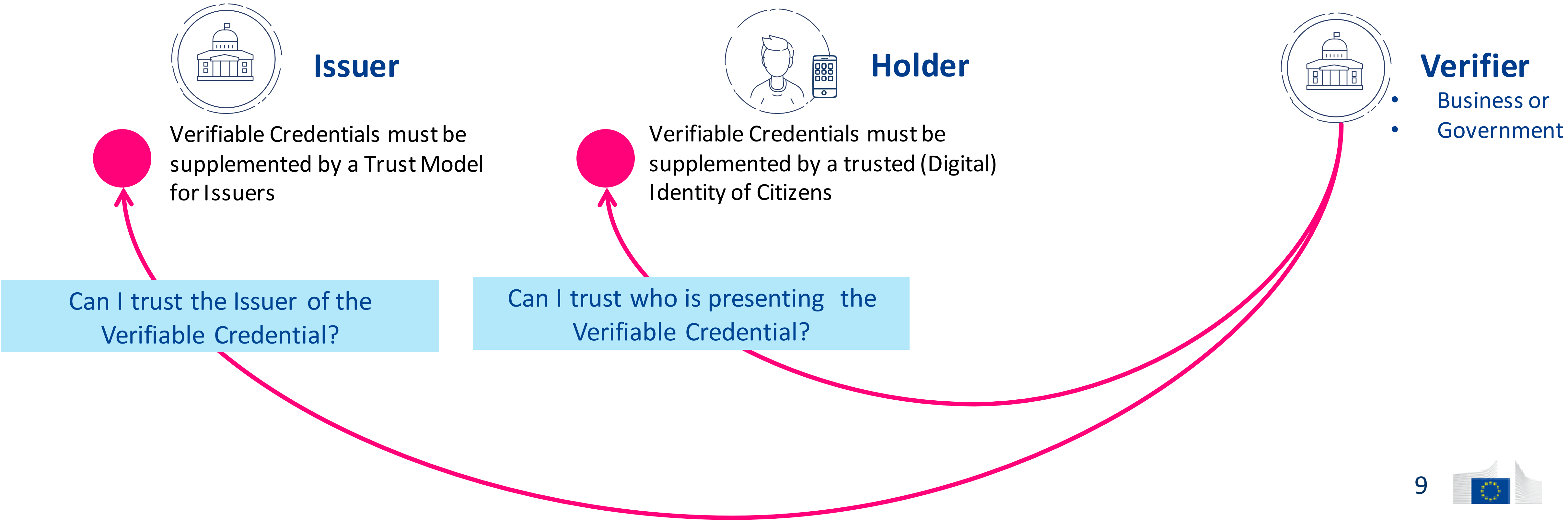
A new pattern for sharing information



Challenges associated to the self-sovereign scenario.

Technology can help

We aim at significantly easing the verification of information in a Citizen to Business (C2B) and Citizen to Government (C2G) context. VERIFIABLE CREDENTIALS are an essential but not sufficient element to achieve this objective . There are two other challenges:



Issuer

Verifiable Credentials must be supplemented by a Trust Model for Issuers

Holder

Verifiable Credentials must be supplemented by a trusted (Digital) Identity of Citizens

Verifier

- Business or
- Government

Can I trust the Issuer of the Verifiable Credential?

Can I trust who is presenting the Verifiable Credential?

Three key technologies

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

Verifiable Credentials

A new way of expressing information

Metadata
Claims
Proofs (signatures)

Blockchain/ ledger

A new decentralised infrastructure

Digital Wallet

A new way to interact for/with citizens

Why invest in these technologies?

Almost impossible to fake but easy to verify

Almost impossible to fake but easy to verify

Verifiable Credentials are becoming the *de facto* standard because…

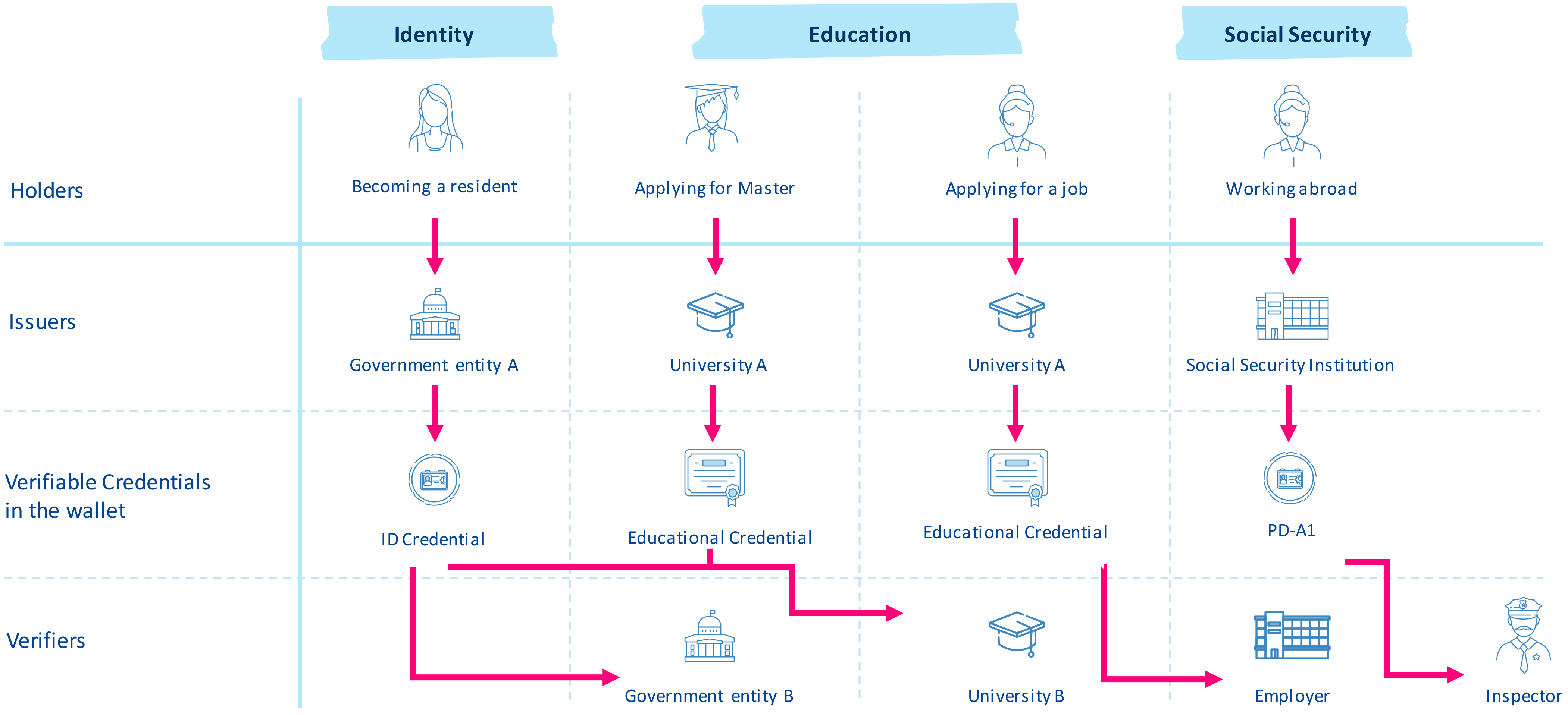
- ✓ High level of certainty that the issuer is trusted alongside the time of issuance, expiry date, etc.
- ✓ High level of certainty that the holder is the one that the Verifiable Credential was issued to.
- ✓ Verifiers have easy access to information but the holder keeps data control and ownership with possibility of partial disclosure of information.

02.

What are Verifiable Credentials?

Verifiable Credentials can be used in many Citizen journeys

Verifiable Credentials can be used in almost all types of Citizen Journeys



Identity

Education

Social Security

Holders

Becoming a resident

Applying for Master

Applying for a job

Working abroad

Issuers

Government entity A

University A

University A

Social Security Institution

Verifiable Credentials in the wallet

ID Credential

Educational Credential

Educational Credential

PD-A1

Verifiers

Government entity B

University B

Employer

Inspector

Three key ingredients

Three components to benefit from the next evolution of the Decentralised Identity.

Verifiable Credentials

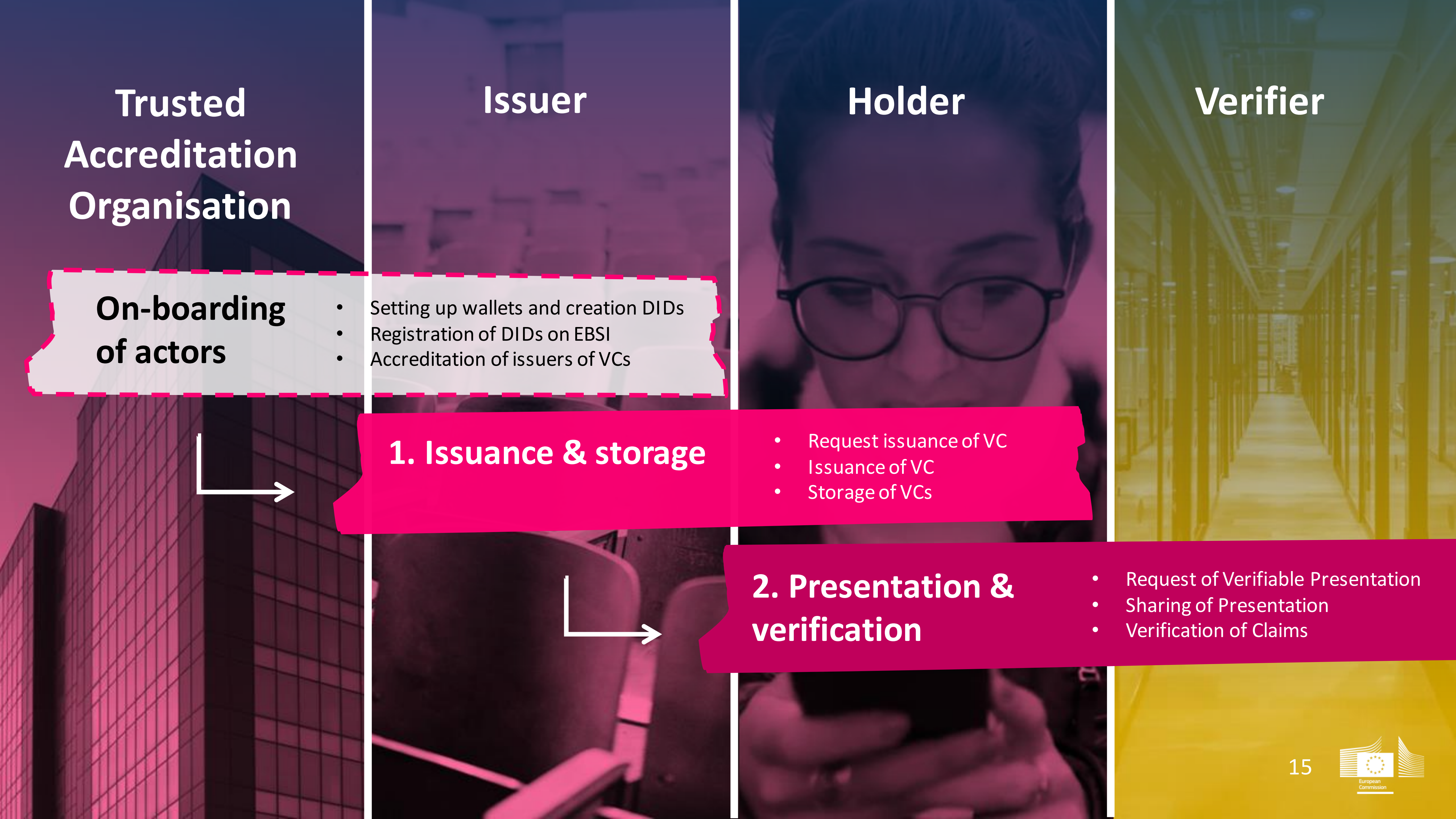
A new way of expressing information

Verifiable Data Registries

A new decentralised Infrastructure for establishing trust

Digital Wallet

A new way to interact for/with citizens



Trusted Accreditation Organisation

Issuer

Holder

Verifier

On-boarding of actors

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

1. Issuance & storage

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

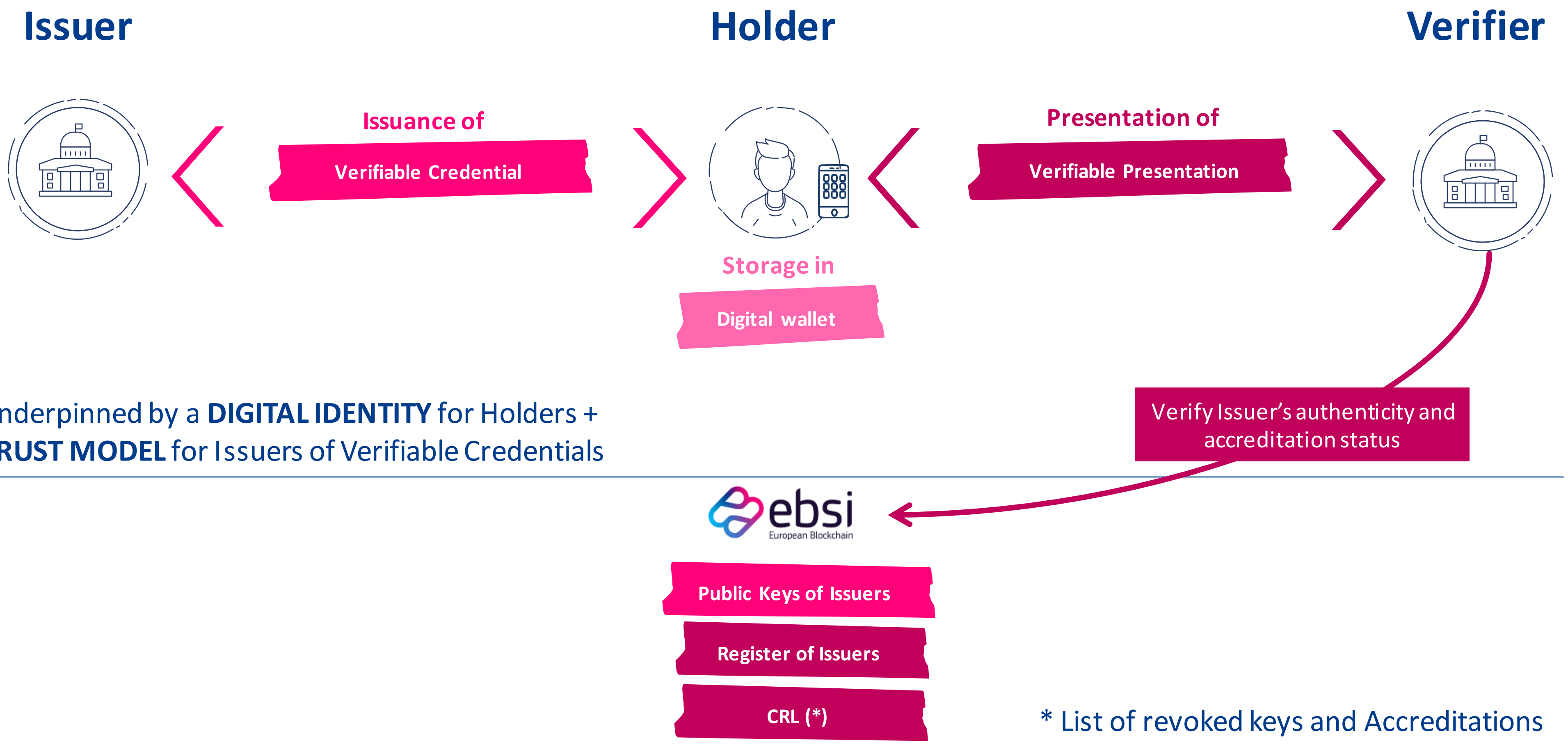
2. Presentation & verification

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

Verifiable Credentials, the basic information sharing scenario

A new pattern for C2B and C2G information exchange

Verifiable Credentials enable a **C2G and C2B Information sharing model**



Issuer

Holder

Verifier

Issuance of

Verifiable Credential

Storage in

Digital wallet

Presentation of

Verifiable Presentation

Verify Issuer's authenticity and accreditation status

underpinned by a **DIGITAL IDENTITY** for Holders + **TRUST MODEL** for Issuers of Verifiable Credentials

ebsi
European Blockchain

Public Keys of Issuers

Register of Issuers

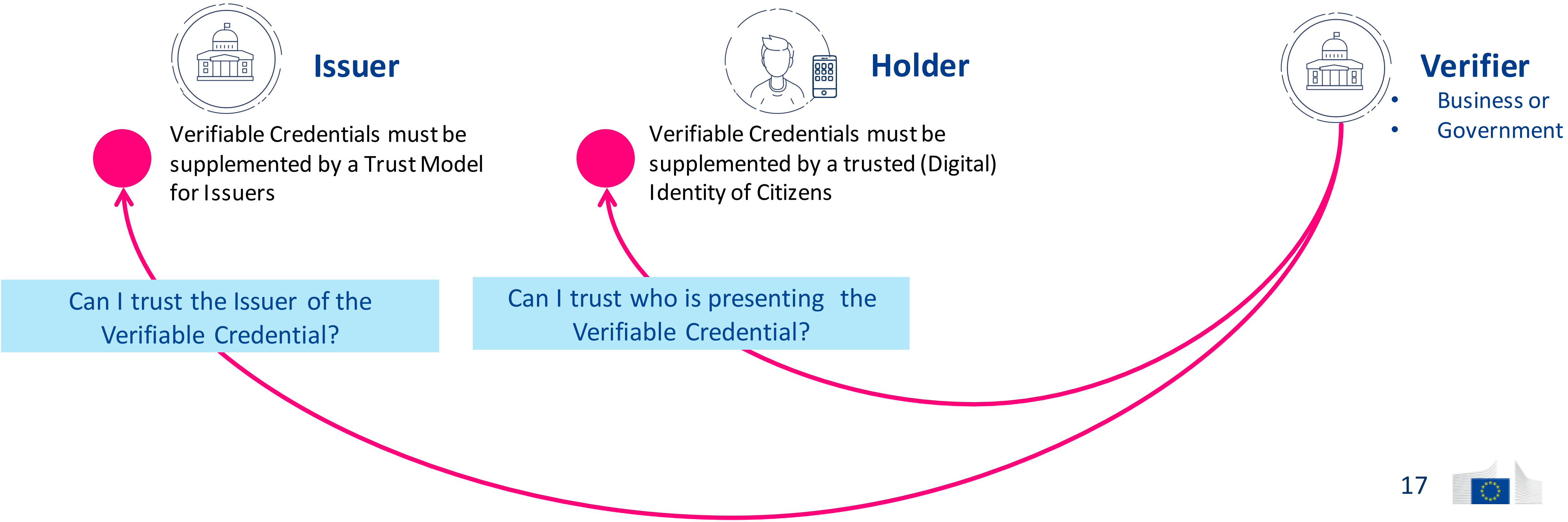
CRL (*)

* List of revoked keys and Accreditations

Verifiable Credentials, the challenges

A new pattern for C2B and C2G information exchange

Verifiable Credentials aim at significantly easing the verification of information in a Citizen to Business (C2B) and Citizen to Government (C2G) context. VERIFIABLE CREDENTIALS are an essential but not sufficient element to achieve this objective. There are two other challenges:



Issuer

Verifiable Credentials must be supplemented by a Trust Model for Issuers

Holder

Verifiable Credentials must be supplemented by a trusted (Digital) Identity of Citizens

Verifier

- Business or
- Government

Can I trust the Issuer of the Verifiable Credential?

Can I trust who is presenting the Verifiable Credential?

Why Verifiable Credentials?

Impossible to fake but easy to verify

Impossible to fake but easy to verify

Verifiable Credentials are becoming the *de facto* standard because…

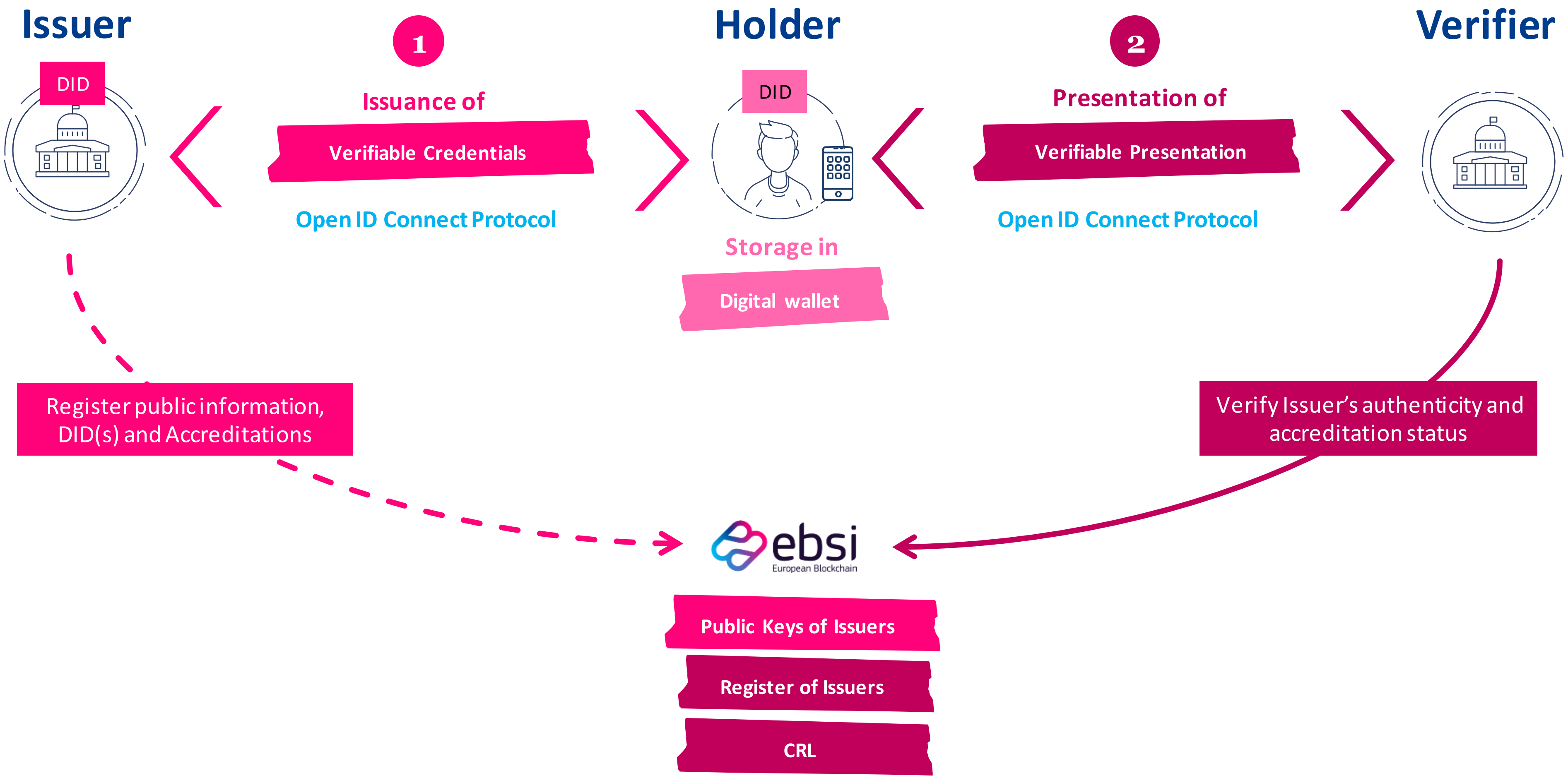
- ✓ High level of certainty that the issuer is trusted alongside the time of issuance, expiry date, etc..
- ✓ High level of certainty that the holder is the one that the Verifiable Credential was issued to.
- ✓ Verifiers have easy access to information, but the holder keeps data control and ownership with possibility of partial disclosure of information.

03.

How do Verifiable Credentials work?

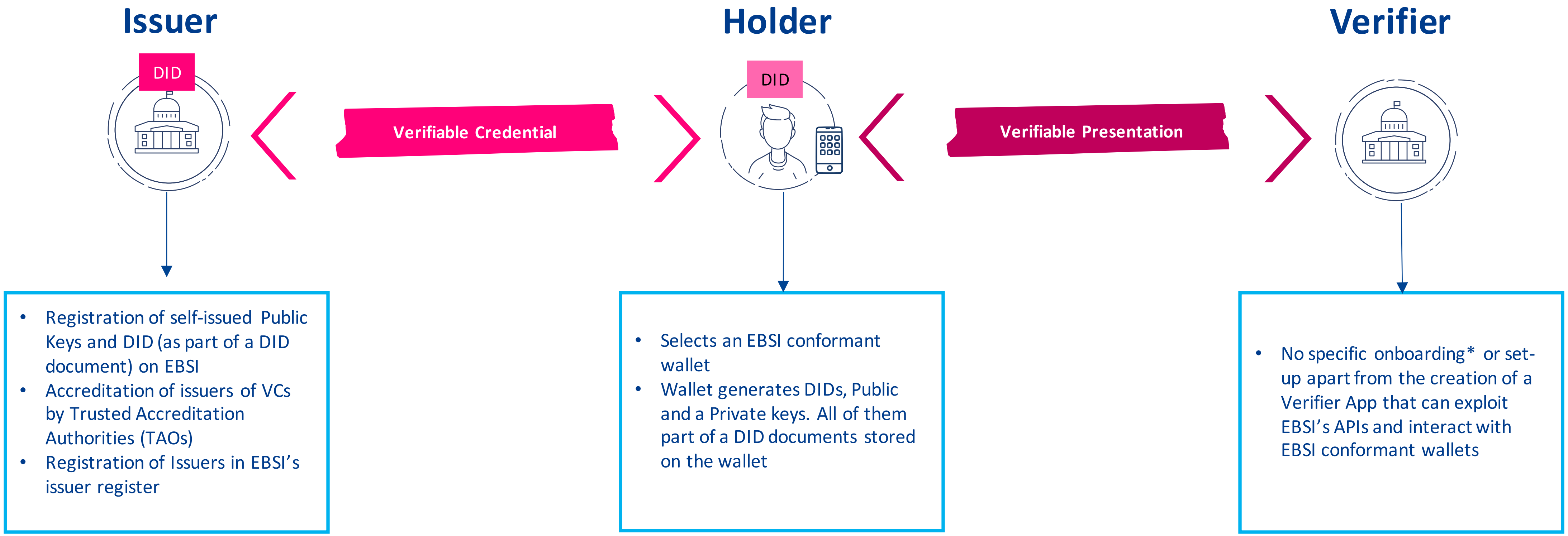
Verifiable Credentials, the scenario.

A new pattern (distributed and decentralised) for exchanging information



How does it work?

Step 0. Issuers are onboarded, wallets are setup and verifiers environments are established



Issuer

DID

- Registration of self-issued Public Keys and DID (as part of a DID document) on EBSI
- Accreditation of issuers of VCs by Trusted Accreditation Authorities (TAOs)
- Registration of Issuers in EBSI’s issuer register

Verifiable Credential

Holder

DID

- Selects an EBSI conformant wallet
- Wallet generates DIDs, Public and a Private keys. All of them part of a DID documents stored on the wallet

Verifiable Presentation

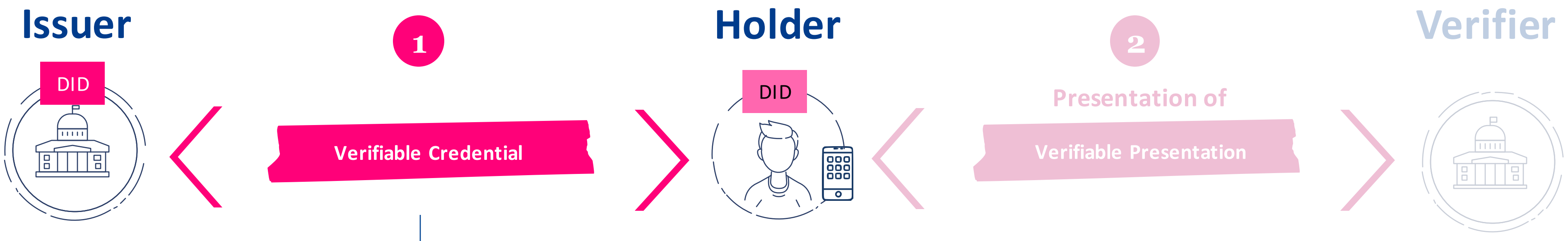
Verifier

- No specific onboarding* or set-up apart from the creation of a Verifier App that can exploit EBSI’s APIs and interact with EBSI conformant wallets

* Verifier trust model is not required by the existing use cases, but it can be supported.

How does it work?

Step 1. Issuance of a Verifiable Credential which is then stored on an EBSI conformant wallet



What does it contain?

Credential Metadata

> **The DID of the entity that issues the credential**
> **The status of the credential** (Issuance date, Expiration date)

Claim(s)

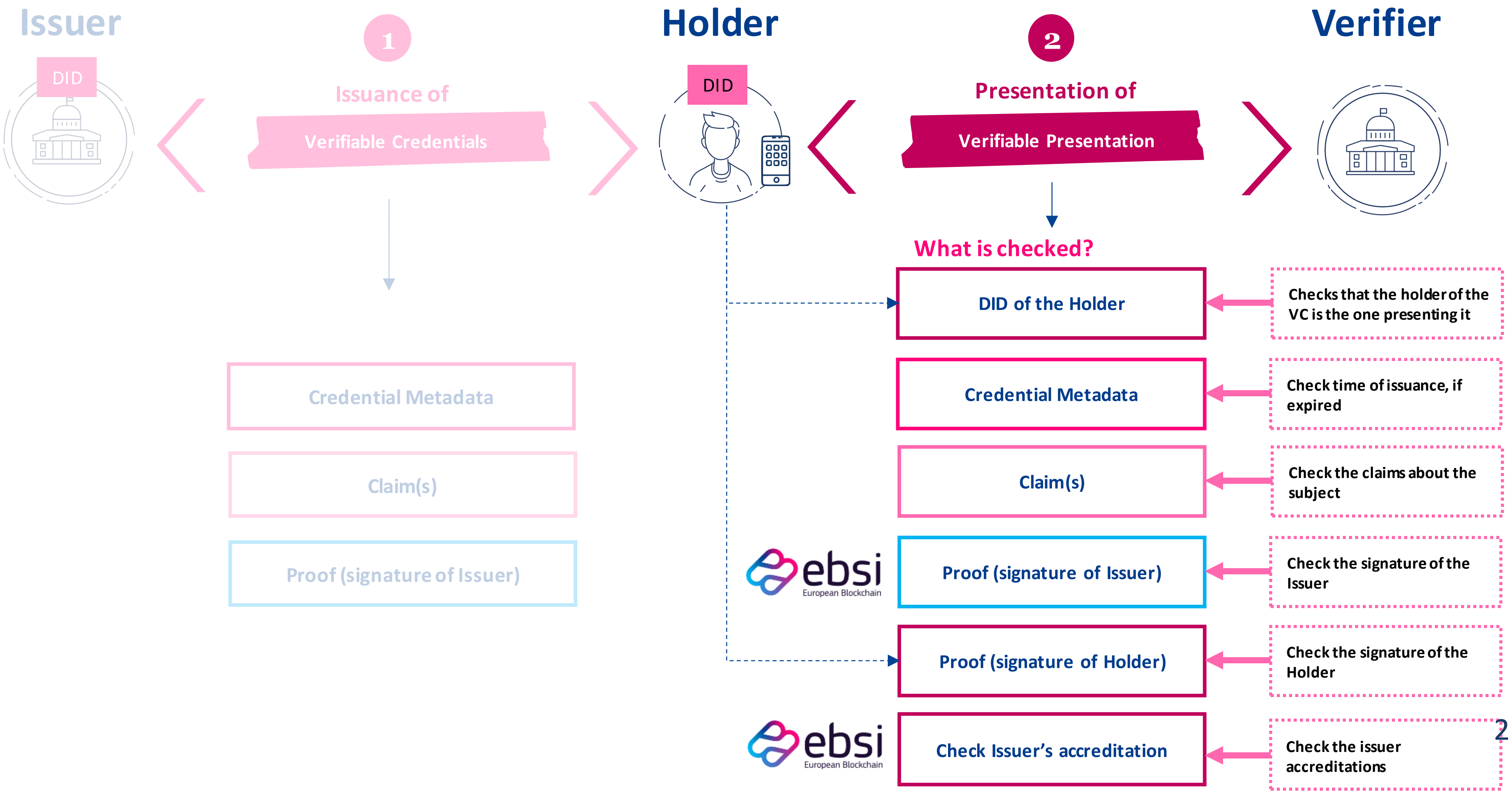
> **The DID of the Holder of the credential**
> **The claims about the subject** (What the issuer asserts about the subject)

Proof (signature of Issuer)

> **Digital proof to make the credential tamper-evident** (One or more cryptographic proofs that can be used to detect tampering and verify the authorship of a credential).

How does it work?

Step 2. Presentation of a Verifiable Credential for verification



Issuer

DID

1

Issuance of

Verifiable Credentials

Credential Metadata

Claim(s)

Proof (signature of Issuer)

Holder

DID

2

Presentation of

Verifiable Presentation

Verifier

What is checked?

DID of the Holder	Checks that the holder of the VC is the one presenting it
Credential Metadata	Check time of issuance, if expired
Claim(s)	Check the claims about the subject
Proof (signature of Issuer)	Check the signature of the Issuer
Proof (signature of Holder)	Check the signature of the Holder
Check Issuer’s accreditation	Check the issuer accreditations

Standards and recommendations

EBSI invests in the dissemination of industry recognised Standards

W3C standards and recommendations

- Decentralized Identifiers v1
- Verifiable Credentials Data Model v1.1
- Presentation Exchange v2

OpenID Connect

- OpenID Connect SIOP v2
- OpenID Connect for Verifiable Presentations
- OpenID Connect for Verifiable Credentials Issuance

eIDAS

- JAdES
- eID authentication and identification

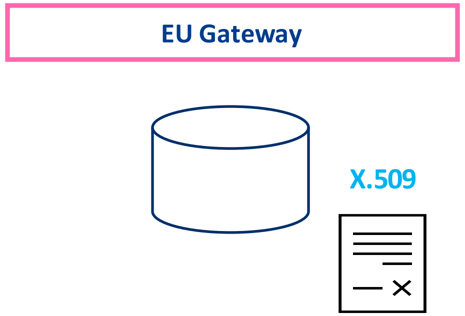
JWT RFC family

- IETF RFC 7515-7520

Three Trust models of Issuers of Verifiable Credentials

Scalability, flexibility and interoperability

Centralised Trust Model

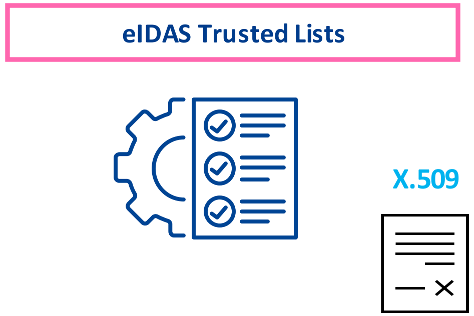


EU Gateway

X.509

The Commission can manage a centralised service responsible for managing and distributing the certificates of issuers of electronic documents.

Federated Trust Model

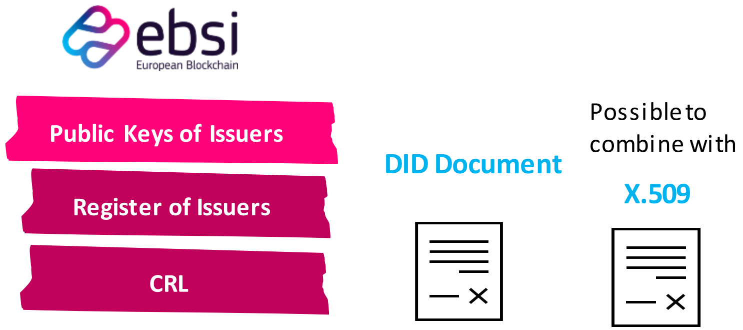


eIDAS Trusted Lists

X.509

The eIDAS regulation has put in place a EU-wide list of all providers of qualified certificates. This list can be used to support the verification of information about issuers of electronic documents.

Distributed Trust Model



ebsi European Blockchain

Public Keys of Issuers

Register of Issuers

CRL

DID Document

Possible to combine with

X.509

EBSI leverages blockchain and W3C’s Decentralised Identifier standard to create a fully distributed trust model where each sector or Member State defines and manages the issuer accreditations of electronic documents.

Important note! Combination of trust models is possible

Can we compare the Issuers' Trust Model?

	Centralised Trust Model	Federated Trust Model	Distributed Trust Model
Concept	A Central authority, e.g. the Commission, manages a **centralised service** responsible for managing and distributing the certificates of issuers of electronic documents.	The eIDAS regulation has put in place a **EU-wide list of all providers of qualified certificates**. This list can be used to support the verification of information about issuers of electronic documents.	Leveraging **blockchain and W3C's Decentralised Identifier standard** to create a fully distributed trust model where each sector or Member State/ Region/ etc. defines and manages the issuers of electronic documents without any the need for a Central Authority.
Example	EU Gateway	eIDAS Trusted Lists	EBSI
Technology	**X.509 Certificates**	**X.509 Certificates**	**DID documents** **Verifiable Accreditations** Possible to combine with **X.509 Certificates**
Governance	This is **hierarchical and not that flexible requiring many roles**: Certificate Authority, Registration Authority, Validation Authority, Distribution Authority	This is a **federation of Centralised Trust Models** which comply to a common set of requirements. Nonetheless the foundation is similar with greater scalability and interoperability.	The model enables decentralisation and **greater flexibility**. Only **two roles are required**: Trusted Accreditation Organisation (TAO) and Trusted Issuer (TI)
Strength	**Control of service** The delivery of service is centered around a Central Entity. As a result rollout can be much faster than the other models.	**Interoperability** The eIDAS List Of Trusted Lists provides a reliable cornerstone to securely access all EU trusted lists and promoting cross-border interoperability	**Flexibility** • Rotation of keys allows issuers to minimise the number of revoked Verifiable Credentials as a consequence of the revocation of the Issuer's signing keys. • Can be combined with classical X.509/ PKI. • Can also support both Centralised and Federated trust models.

The Holder’s Digital Identity verification

There are 3 different approaches for digital identity

Centralised Approach

National eID means

eID means
- National
- Sectorial
- …

Federated Trust Model

Trusted Identity networks

eIDAS Nodes for mutual authentication (common data set + SAML)

Distributed Trust Model

European Self Sovereign Identity (ESSIF)

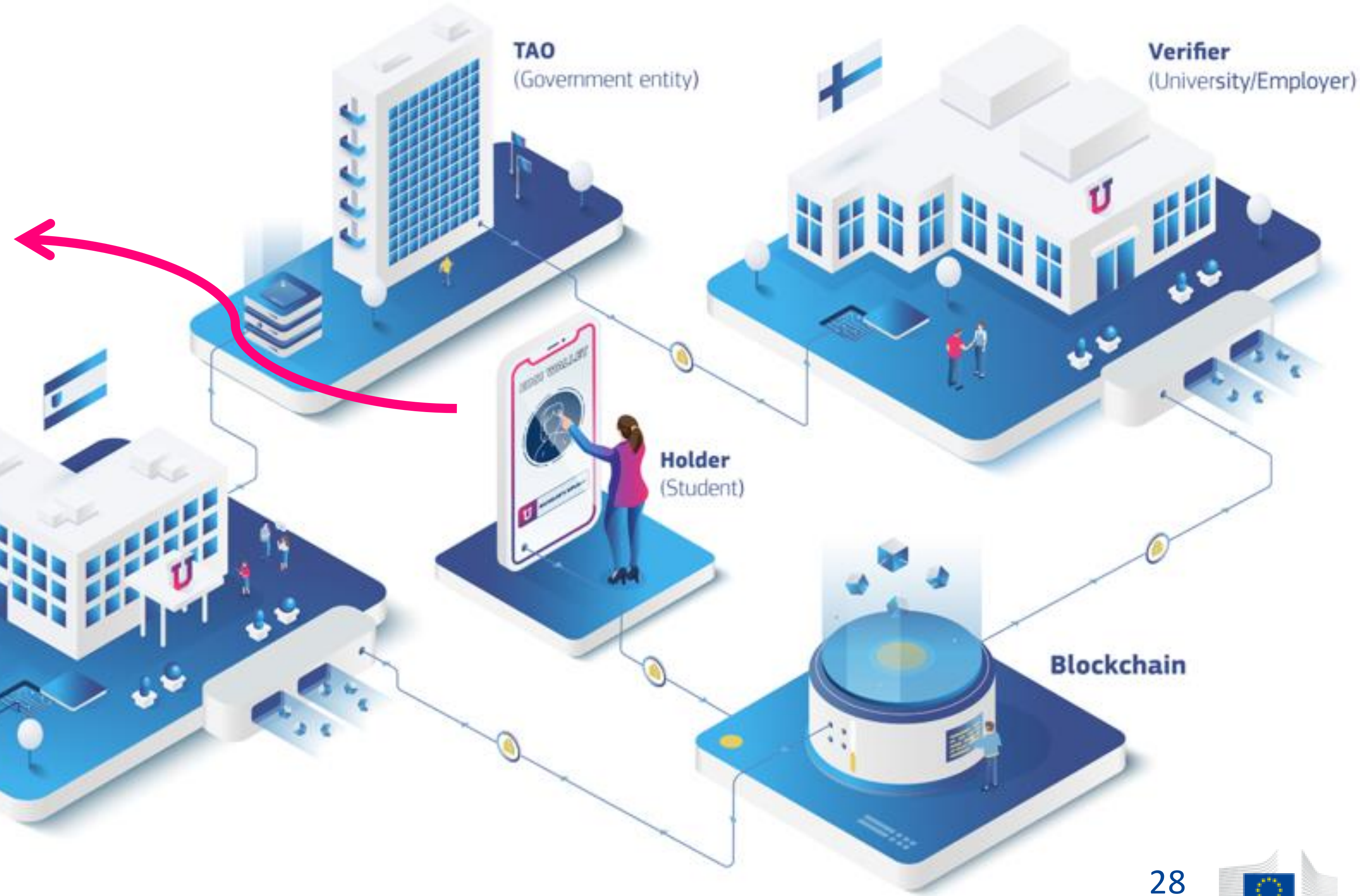
Verifiable ID (Verifiable Credential using eIDAS common data set)

Important note! EBSI conformant wallets and Verifier Apps are encouraged to support several approaches for verification of Digital Identity

Wallets mediate almost all user interactions.

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

Digital wallets



Want to know more?

Key ressources

Explore EBSI

Check the EBSI website

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

Explore Specs

Check the EBSI Playbook

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

Watch Demos

Check the EBSI Demo Day

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

https://ec.europa.eu/ebsi

ebsi

European Blockchain