

ETSI / CEN Workshop on EU Digital Identity Framework Standards

Trust models: Distributed trust

Dr. Ignacio Alamillo-Domingo, Logalty



What trust anchors do we need for identity management? ISO TR 23644

- Legal trust anchors are the trust anchors established and/or recognized by the legislation and regulations of relevant jurisdictions, by the contractual agreements and organizational by-laws. They set a legal foundation for the trust frameworks and underpin the operating rules and procedures. Legal trust anchors can mention or include references to other trust anchors.
- Data trust anchors are authoritative data sources that relate to the entities and attributes to be processed, where very high data quality is vitally important.
- Cryptographic trust anchors, which provide the roots of cryptographic trust and enable cryptographic binding, revocation, authentication, signing, encryption and other trust functions.
- Cybersecurity trust anchors, which monitor, detect and respond to policy violations, and enforce policy compliance. This includes assurance, testing and certification regimes, possibly augmented by the combined effort of a group responsible for defending an enterprise's use of information systems by maintaining its security (so-called "blue team"), known to the defenders, and a group of mock attackers ("red team"), unknown to the defenders.
- Social trust anchors. Subjective trust anchors can exist, particularly in the context of social situations and informal relationships where each individual can have a different view on the assessed risks and the requirements for risk mitigation or legal remedy.

A world with many wallets?

- eIDAS 2 will foster the provision of many wallets, both for natural and legal persons, with different models, including (in some Member States) the recognition of wallets issued by private companies.
- But the EEA approach will drive even more the provision of “other” wallets, alongside the “official” wallets, using EEAs instead of PIDs and offering a rich set of attestation types.
- How do we upkeep trust using different wallets, in different scenarios? Of course, it has to do with:
 1. How do we represent trust anchors.
 2. How and where do we store trust anchor information.
 3. How do we convey and exchange trust anchors.
 4. How do we verify the reliability of trust anchors during time.
- Classical PKI systems have generally failed to cover all these needs in real open scenarios.

“Classical” systems trust anchor management

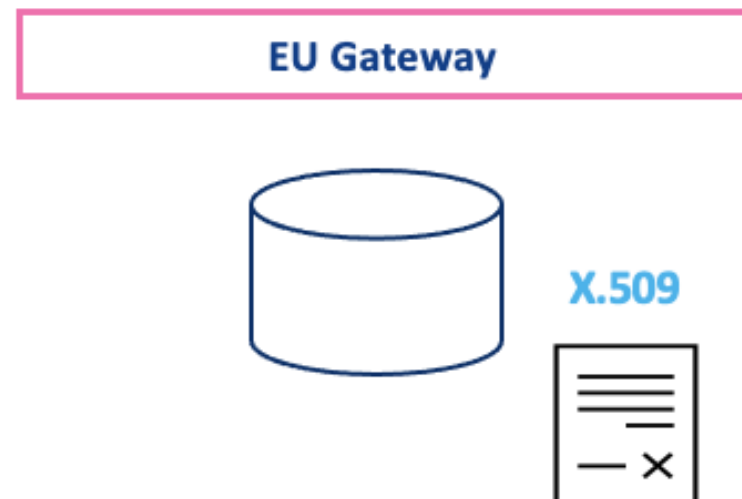
- eIDAS 1 trust anchor management is performed manually, as part of the service metadata management.
- eMRTD (such as eID documents and passports) and mDL systems require bilateral exchange of trust anchors, centralised registers or other non-automated out-of-band mechanisms.
- eIDAS trust services trust lists, as per ETSI TS 119 612, present scalability issues (assuming hundreds or thousands of issuers) and do not even provide support for EEAs issued by public sector bodies responsible of authentic sources.
- Federated systems can exchange trust anchor metadata (e.g. OIDC Federation), yes, but then the relying party must store all information for evidential purposes.
- If you forget to retrieve and store, you have a problem... this is really a risk when it comes to (Q)EEAs.
- And YES, it is going to be worse, as key duration policies impose quicker rotation periods as CAs will tend to roll-over the infrastructure more frequently...

What about decentralised trust store management?



Scalability, flexibility and interoperability

Centralised Trust Model



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

Federated Trust Model



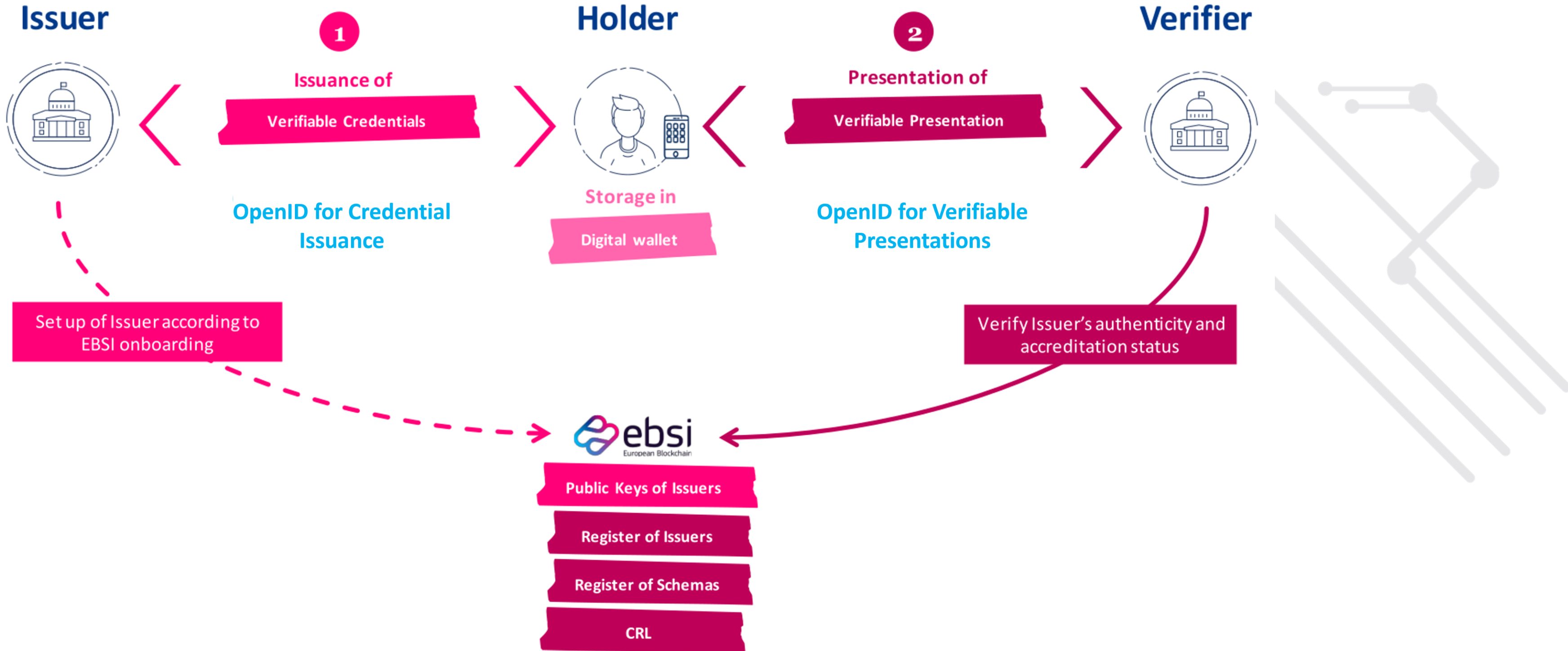
The eIDAS regulation has put in place a EU-wide list of all providers of qualified certificates. This list can be used to support the verification of information about issuers of electronic documents.

Distributed Trust Model

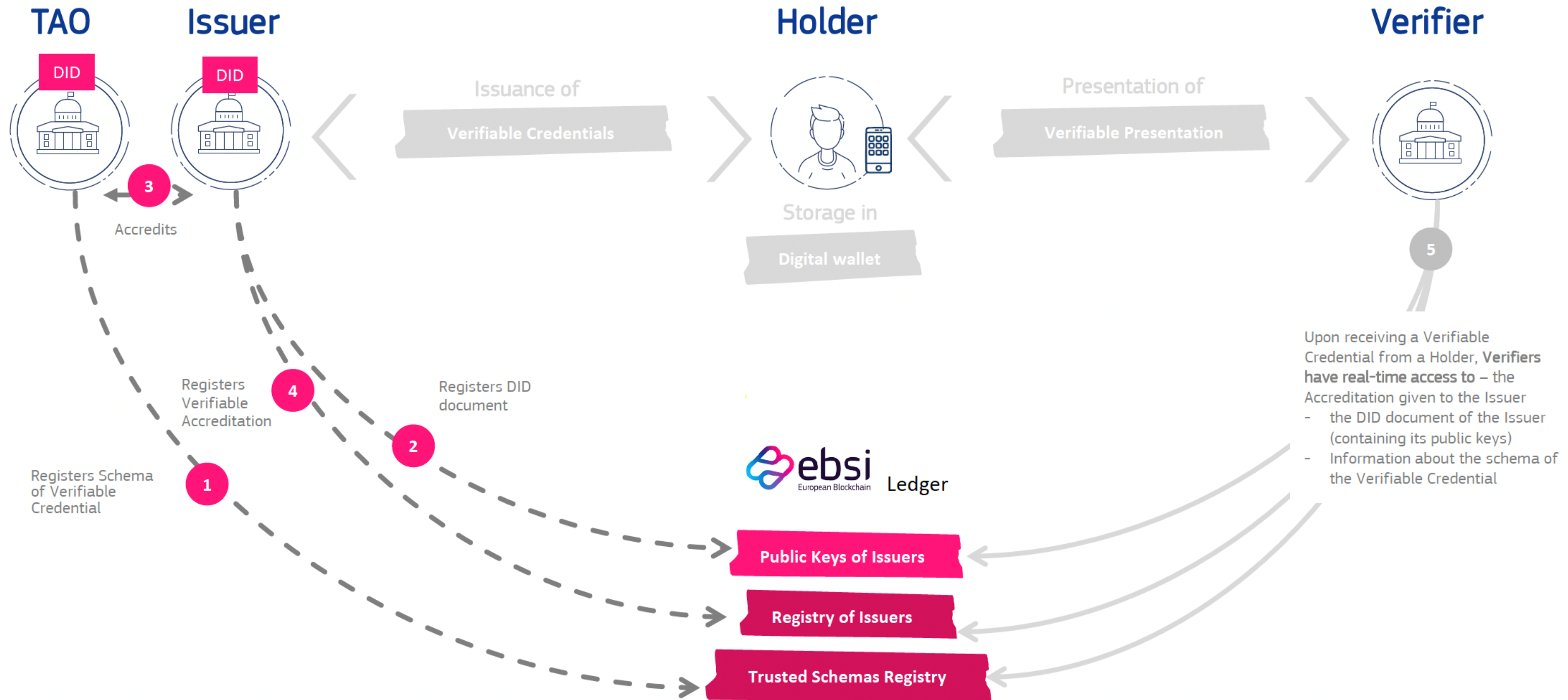


EBSI leverages blockchain and W3C's Decentralised Identifier standard to create a fully distributed trust model where each sector or Member State defines and manages the issuer accreditations of electronic documents.

Decentralised trust store management, EBSI & DC4EU LSP

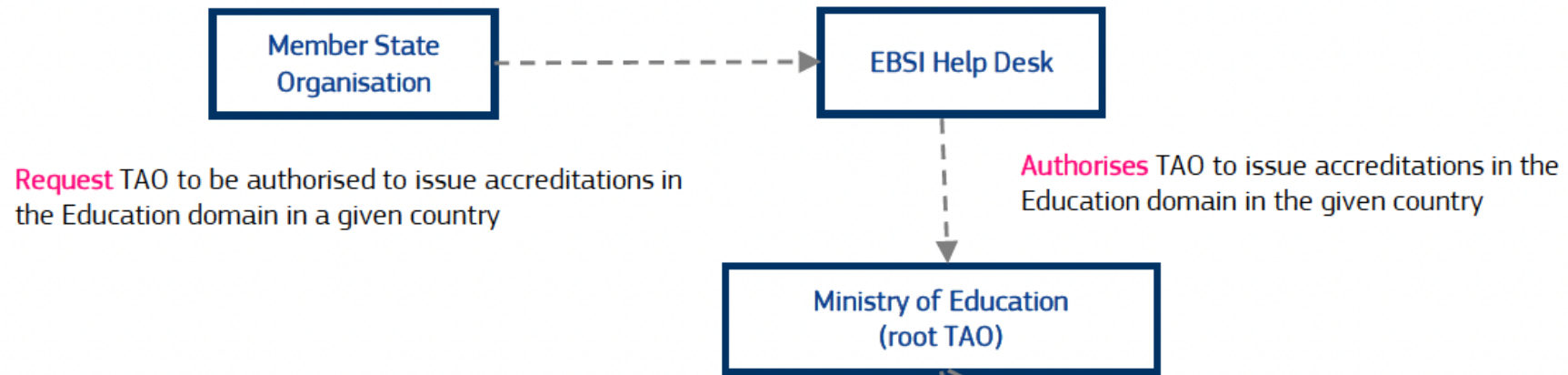


Decentralised trust store management, EBSI & DC4EU LSP



Decentralised trust store management, EBSI & DC4EU LSP

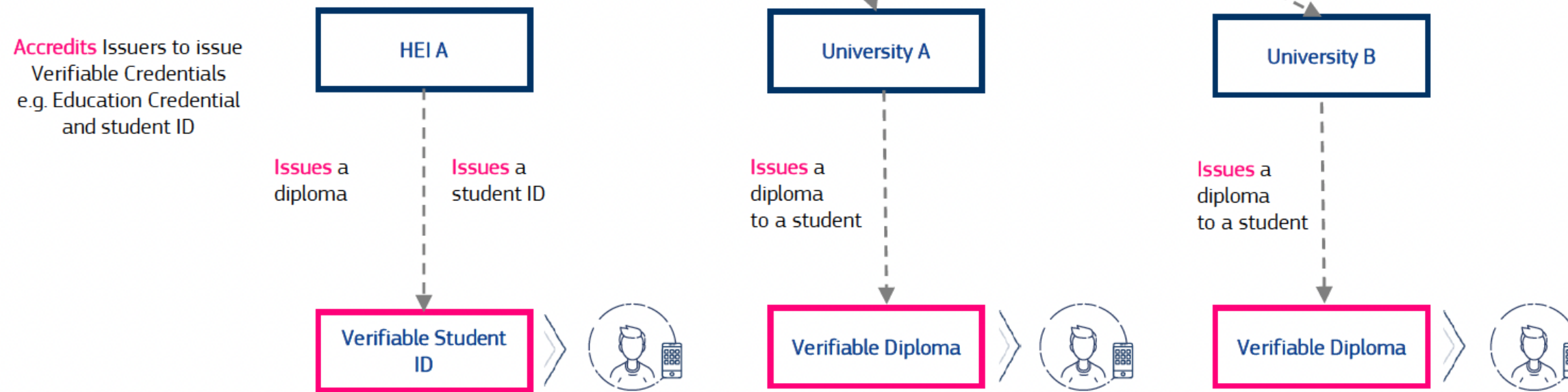
Level 1 Set-up of root TAO



Level 2 Set-up of sub-TAOs



Level 3 Set-up of Issuers



Decentralised trust store management: benefits

1. A common way to represent trust anchors, with no dependency on platforms, e.g., browsers, for the current eIDAS 1 infrastructure, mDL or eMRTD hierarchical PKI systems, future eIDAS 2 schemes...
2. A secure (in the future, qualified) store for trust anchor information, facilitating both existing and new systems. Not only cryptographic trust anchors, but data trust anchors as well.
3. Trust anchors can be read directly or exchanged using protocols such as OIDC Federations (to be tested in DC4EU).
4. As trust anchors are reliably stored in a decentralised and immutable system, its trustworthiness can be verified in the future, facilitating verification of PIDs, EEAs or other sectoral credentials over time by all actors.
5. Using DIDs for decoupling identities and its cryptographic representations (something we cannot do with X.509 certs PKI), the system facilitates both rollover management and the future transition into post-quantum safe algorithms.

Thank

YOU!



DC4EU



Co-funded by
the European Union

