Verifiable credentials, sovereignty, decentralization and lifelong learning: a new paradigm for education

My digital backpack

Lluís Ariño

Tirana

2023/06/07
Classical issuers trust models

Classic solutions often require Verifiers to contact Issuers in order to ensure that the information they receive from Holders can be trusted. This pattern is called “phoning home”.

- **Issuer** needs to create and maintain APIs **available to Verifiers** and ensure that connectivity is available **24x7**
- **Verifier** needs to **create and maintain calls to all those APIs from every credential Issuer**
- **Non-privacy preserving**: a way for issuers and Verifiers to correlate an identity holder’s usage of a credential
The verification of credentials across the entire education ecosystem remains a complex, laborious exercise.

Multiple different databases, multiple data formats, multiple protocols, multiple and different user experiences.
Decentralisation and sovereignty: a new paradigm

Centralised Ecosystem → Siloed Ecosystem → Federated Ecosystem → Decentralised Ecosystem

Non-managed Identity → Managed Identity → Federated Identity → Self Sovereign Identity

Paper Documents → Digital Documents → Digital Credentials → Verifiable Credentials

Non-managed Data → Managed Data → Single Digital Gateways → Self Sovereign Data Mgt.

Recognition of Formal Education

Quality Assurance, Standards, Interoperability (technical, legal, semantic, governance)… → Recognition of All Learning

Source: Arino, Ll. and Grech, A. (2021)
Decentralisation and sovereignty: putting learners and citizens in control of their data!

Centralised and federated models

- The user is not in control
- The user experience is on the context of each domain (often also different within the same domain)
- There are few crossdomain information exchanges
- Verification is costly

Decentralised models

- The user is fully in control
- The user experience remains the same across domains and within the same domain
- There are multiple crossdomain information exchanges
- Verification is easy and fast

From 'Trust by law...'
.to 'Trust by Design'
Conceptual Trust Models of Issuers that avoid “phoning home”

Scalability, flexibility and interoperability

Centralised Trust Model
For example:
Certificates e.g. managed PKI

Federated Trust Model
For example:
Trusted Lists (*)

Distributed Trust Model
For example:
- Public Keys of Issuers
- Registry of Issuers
- Trusted Schemas Registry

Three basic Trust Models of Issuers of Verifiable Credentials (models can be combined)
3 key technologies for citizen’s sovereignty

Information is easy to verify, almost impossible to fake and controlled by citizens

**Blockchain / Ledger**
Don’t Trust, Verify

**Digital Wallet**
Not your keys, not your digital asset

**Verifiable Credentials**
A new way of expressing and automating information
- Metadata
- Claims
- Proofs (signatures)
Advantages that highlight the transformative potential of verifiable credentials based on electronic ledgers

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Verifiable credentials leverage cryptographic techniques to ensure authenticity and integrity. They provide a higher level of trust compared to non-verifiable digital credentials, as they are tamper-resistant and can be easily verified.</td>
<td>Verifiable credentials are stored in decentralized systems, such as blockchain or distributed ledgers. This distributed nature enhances security and makes the credentials immutable, preventing unauthorized changes or fraud.</td>
<td>Verifiable credentials enable individuals to have more control over their personal data. They allow selective disclosure, meaning individuals can share only the necessary information without revealing their entire credential or identity.</td>
<td>Verifiable credentials streamline the verification process, reducing reliance on manual checks. Relying parties can quickly verify the authenticity of a credential by validating it against the distributed ledger, saving time and effort.</td>
<td>Verifiable credentials adhere to standardized formats and protocols, ensuring interoperability across different systems and platforms. They can be easily shared and transferred between individuals, organizations (public and private), or services, making them highly portable.</td>
<td>Verifiable credentials, with their built-in trust mechanisms, significantly reduce the risk of fraud and counterfeiting. The cryptographic techniques used in verifiable credentials make it extremely difficult for malicious actors to forge or tamper with the information.</td>
<td>Verifiable credentials offer a forward-looking solution that can adapt to evolving technological advancements. The decentralized nature of electronic ledgers provides scalability, allowing for a large number of credentials to be managed efficiently.</td>
<td>Verifiable credentials recorded on electronic ledgers enable greater transparency and auditability. The transaction history and verification records can be traced back, providing a verifiable and immutable audit trail.</td>
</tr>
</tbody>
</table>
3 elements enable a new paradigm to exchange data between parties in a sovereign way
Interoperability dimensions

Organizational

Legal

Semantics

Technical
Interoperability dimensions: Governance
Interoperability dimensions: Legal

• Identity
  • The eIDAS trust framework: the common language for cross-border
  • Current eIDAS only defines “levels of assurance” for Verifiable IDs: Only IDs with substantial or high LoA must be accepted by Member States
  • but … IDs with others LoA low may also be accepted on a voluntary basis, according to the corresponding national legislation applicable to e-Government processes

• Data
  • Privacy - GDPR
  • Data typically embody juridical acts, such as certifying acts by public authorities and other authoritative sources (including private sector bodies with respect to data they’re authoritative for).
  • Therefore, in the logic of eIDAS, they constitute legally binding electronic documents, that should be authenticated according to the national legislation (so national legislation/rules applies for cross-border mobility data)
Interoperability dimensions: Technical

Verifiable credentials are the standardized way to pack, deliver and unpack information (for any domain/industry)
Interoperability dimensions: Semantic

• An unique opportunity at EU level (… and abroad?)

• (Only) EBSI exists at EU level in the verifiable credentials space aligned to the European Self-Sovereign Identity Framework (eSSIF)
  • And, of course, aligned to W3C, OpenID, eIDAS, ETSI

• Some agreements reached (27MS+LI+No)
  • European Learning Model – ELM: an opportunity
    • Only for learning (formal, non-formal, informal)
    • Proper governance must be established (not only DG-EMPL)
  • MyAcademicID
    • Partial schema in EBSI Wave2
    • GEANT will enter EBSI Wave 3 – full schema serialization will be available
      • MyAID governance will be established
      • Schema ownership
      • Review/approval eduPerson
      • Review/approval ESI
  • MyEUAID?
New paradigm achievements: focusing on citizen, breaking educational SILOs, enabling LLL, PLP, SC

- Aligned to (EBSI VALUE FOR EDUCATION):
  - EU Digital Strategy
  - EU Data Strategy
  - EU digital credentials action plan
  - EU Digital action plan
  - Europass decision
  - Europass Digital Credentials
  - European education area
  - European research area
  - European universities initiative
  - European skills agenda
  - Individual Learning Record
  - eIDas trust framework
  - GDPR
  - Once only principle (enabling the citizens perspective)
  - State of the Union address (091620) and European Council Conclusions (100220) for both, identity and data
  - European Declaration on Digital Rights and Principles for the Digital Decade
It’s not the future, it’s already available:

Experience cross-borders services with EBSI.
The first public sector blockchain services in Europe

By the European Commission and the European Blockchain Partnership

Get started ↓

Event and podcast  Do you want to experience the future of Web3? | Discover the Experience Centre

Learn more →
More than 100 HEIs and 7 European Universities Alliances have/are entering in the new paradigm

Currently, in Wave 3
More than 15 conformant wallets (also open source ones)

Are you a wallet provider?
Interested to join this ecosystem and accelerate its development and adoption?

Become conformant →
Challenges for educational institutions, citizens, and private sector

- Citizens
  - State of the Union address (091620)
  - European Council Conclusions (100220)
  - eIDas 2

- Education
  - EU Digital Strategy
  - EU Data Strategy
  - EU Digital action plan
  - EU Digital credentials action plan
  - Europass decision
  - Europass Digital Credentials
  - European education area
  - European research area
  - European universities initiative
  - European skills agenda

Citizens in full control of both, their Identity & Data

Needed:
A more flexible education ecosystem
Embracing LLL, PLP, 21st Century Skills
(Up+Re)skilling of the workforce
eIDAS review (eIDAS2)

- **eIDAS 1:** inherent limitations to the public sector; limited possibilities and complexity for online private providers to connect to the system; insufficient availability of notified eID solutions in all Member States; citizens identity non-mandatory in all Member States; lack of flexibility to support a variety of use cases.
- **Identity solutions falling outside the scope of eIDAS** (social media providers and financial institutions), raise privacy and data protection concerns, and do not have cross-border recognition.
- A new environment where the **focus** has shifted from the provision and use of rigid digital identities to the provision and reliance on specific attributes related to those identities.
- An increased demand for electronic identity solutions that can deliver these capabilities providing efficiency gains and a **high level of trust** across the EU, both in the private and the public sector, relying on the need to identify and authenticate users with a high level of assurance.
- A new approach to ensure that both, citizens and companies, can **trust on digital services** of the digital decade.
- A new approach to citizen’s privacy and sovereignty on their identity and data.
• **Natural and legal persons.**
• **All MS** are mandated to issue EUDIW (including PID)
• That these solutions are linked to a variety of attributes and allow for the targeted sharing of identity data **limited to the needs** of the specific service requested.
• The user shall be **in full control** of their identity(es) and data.
• The issuer of the EUDIW shall **not collect information about the use** of the wallet.
• **Obligation of admission**
  • by **public sector entities** and by **private providers**.
  • by **very large online platforms that require authentication**.
• **Cross border recognition principle:**
  • A qualified electronic attestation of attributes issued in one Member State shall be recognised as a qualified electronic attestation of attributes in any other Member State.
  • An attestation of attributes issued by or on behalf of a public sector body responsible for an authentic source shall be recognised as an attestation of attributes issued by or on behalf of a public sector body responsible for an authentic source in all Member States.
Large Scale Pilots

**20 countries**
- 56 public and 80+ private entities

**Use cases:**
- Electronic Government services, Bank Account opening, SIM registration, mobile driving licence, Remote Qualified Electronic Signature and ePrescription.

**22 countries**
- 36 public and 40+ private entities

**Use cases:**
- Educational credentials and professional qualifications, Portable Document A1 (PDA1), European Health Insurance Card (EHIC).

**19 countries**
- 18 public and 40+ private entities

**Use cases:**
- Digital Travel Credentials, Payments, Legal persons

**8 countries**
- 6 private and 15 private entities

**Use cases:**
- Payments use-cases at both a cross-country and cross-sector level with partners coming from both private and public sector

Total budget: >90 Million (50% EU contribution), >250 Participants,
Digital Credentials for Europe (DC4EU) is a multinational consortium, lead by the Spanish Ministry of Economic Affairs and Digital Transformation and conformed by 80 organizations from 22 countries (20 EU Member States + Norway and Ukraine).

The aim of the proposal is to develop large-scale piloting projects of the EUDI reference wallet addressing two use cases in compliance with the EU toolbox process.

The work of the consortium will be carried out during a two-year period and will be guided by the iterative releases of the EUDI reference wallet.

Total budget = 19.216.899,94 €* distributed from the European Commission in the form of 2 payments.
The EUDI wallet is the real container for the Individual Learning Record (ILR)
Different models, different paradigms: it’s not one or the other

Cross-border mobility programs are accelerators of the change from a managed to a self-managed/sovereign model (Erasmus+, etc.)
Thank you
Any questions?