Hybrid trust models (X509 & Decentralised PKI): The EBSI/DC4EU and ISBE cases

Dr. Ignacio Alamillo-Domingo

ITU-T 5th X.509 Day
May, 12th 2026

eIDAS 2 Regulation

Key benefits of the new Regulation

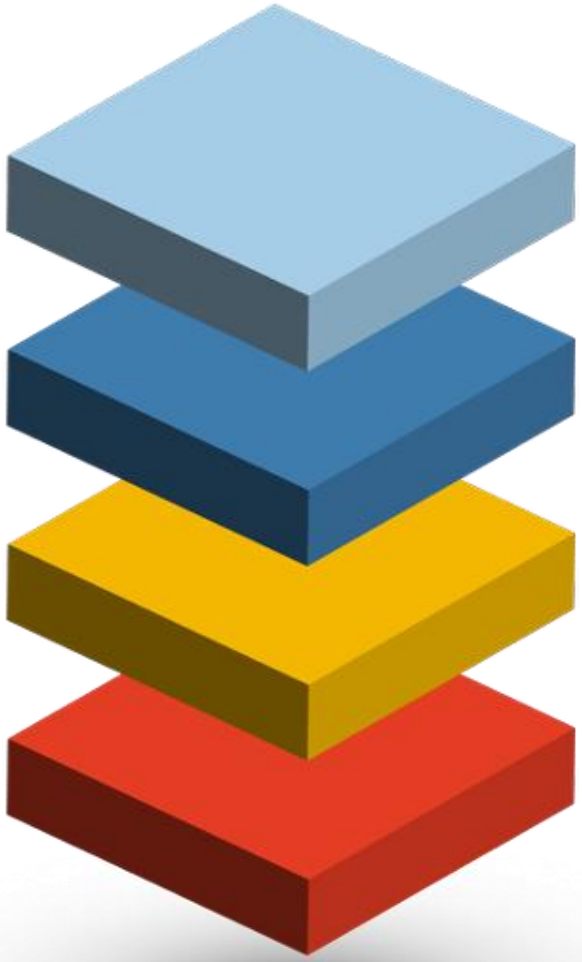
- The most significant benefit of eIDAS 2 is the European Digital Identity Wallet (EDIW), which facilitates the verification of the individual requesting an Electronic Attestation of Attributes (EAA), ensuring that the EAA has been issued to that person and is under their control (precluding the possibility of them transferring their Person Identification Data – PID – or their EAAs to a third party for sharing).
- The EDIW approach is a forward-thinking solution that **addresses the limitations of data exchange between the authentic source and relying parties** by enabling direct data exchange between the user and the relevant parties. This innovative approach is founded on four key innovations:
  - Firstly, there is lightweight registration of user parties, and access control by them to the EDIW.
  - Selective disclosure of attributes, using specially designed data formats.
  - Embedded disclosure policies are incorporated into the EAAs issued by Qualified Trust Service Providers (QTSPs) and Public Sector Bodies' providers (Pub-EAA).
  - The EDIW allows reporting directly to the personal data control authority.

eIDAS 2 Regulation

Why this is good for authentic sources?

- The modified eIDAS is a game-changer, adopting an **abstract approach to the reliability of electronic attestations of attributes** (EAAs), regardless of whether they are issued by QTSPs or public EAA providers. This innovative development makes cross-border use of public documents a breeze, paving the way for seamless international collaboration and exchange.
- It is essential to emphasise the concept of public sector body responsible of an **authentic source**, whether to issue directly (acting as a Pub-EAA provider), through a Pub-EAA provider operating autonomously, through a QTSP contracted for this purpose by the authentic source, or simply by granting access to a QTSP (when there is an obligation or in a collaborative way).
- eIDAS 2 represents a **new way to issue legally valid electronic documents in the EU, both for domestic purposes and in cross-border scenarios.**
- To benefit from the provisions of eIDAS 2, it is necessary to work on the definition of the typology/typologies of EAA/s, in terms of specific vocabularies and governance rules. For example, for the EHIC EAA or the PDA-1 EAA, or Learning Achievements EAAs or Professional Qualifications EAAs.

eIDAS 2 scenarios



1

2

3

4

Scenario 1 – non-eIDAS scenario

Closed systems operate through contractual relationships between trusted issuers, remaining outside eIDAS Regulation (without EUDIW ecosystem connection)

Scenario 2 – non-qualified Trust Service Provider

Non-qualified Trust Service Providers operate under permissive regulatory frameworks, allowing immediate EAA issuance without prior supervisory approval, though relying parties face significant trust assessment challenges.

Scenario 3 – Public Sector Body in charge of an Authentic Source

Public sector Electronic Attestations require strict regulatory compliance equivalent to qualified providers, enjoying legal equivalence with paper documents and automatic cross-border recognition across EU Member States.

Scenario 4 – Qualified Trust Service Provider

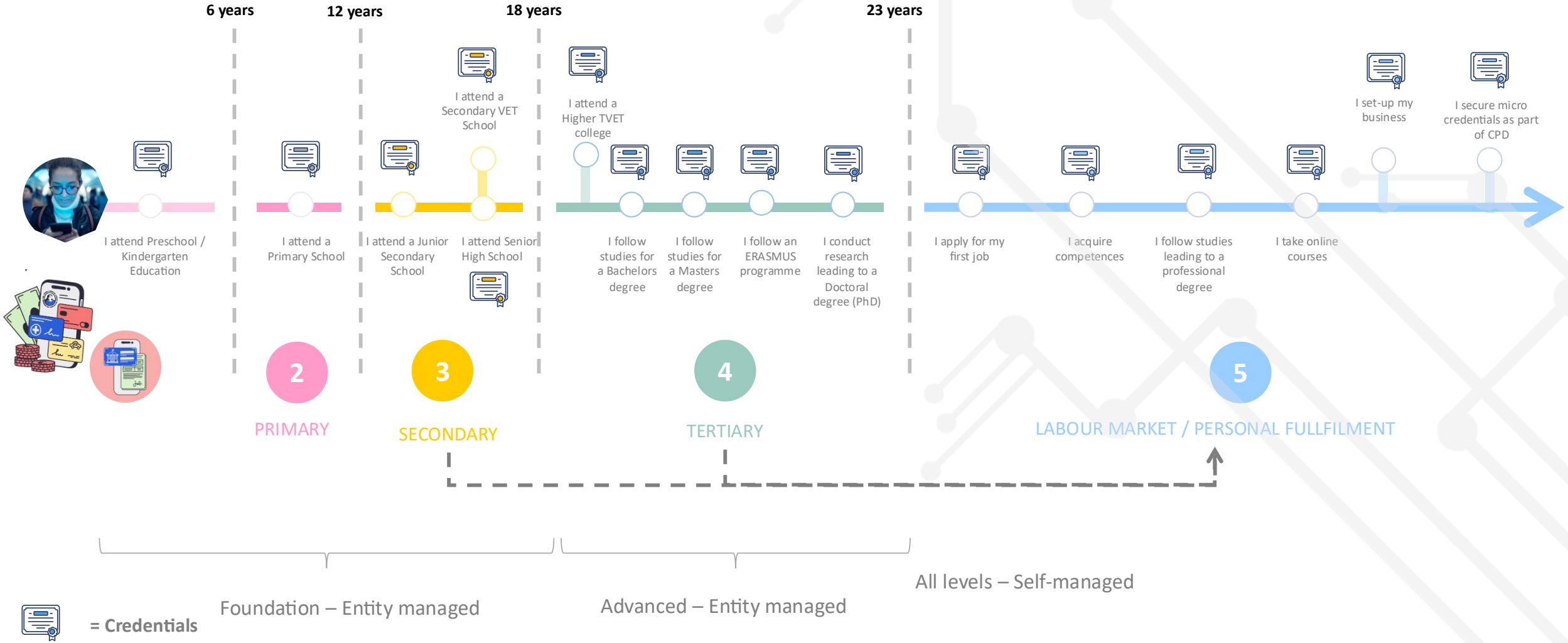
Qualified Electronic Attestations represent the highest credential tier, requiring stringent qualification by national supervisory bodies and providing guaranteed cross-border recognition with legal parity across European Union.

Flexible

Hard

Education and Professional Qualifications

Context: Vertical (Institutional) vs Transversal (citizen's) perspective – Enabling real lifelong learning



Education and Professional Qualifications

Context: Governance(s) complex at all levels (European, Member State, Regional, Institutional)

Characteristic	Formal Education	Professional Qualifications	Educational Quality Assurance	Non-Foundational Digital Identity
Authority Level	Ministries act as RootTAOs	Ministries and professional bodies oversee licensing	National and regional agencies, linked to European bodies	Sector-specific authorities issue credentials
Actor Types	Ministries, educational institutions	Ministries, professional bodies	National/regional QA agencies, ENQA, EQAR	Various sector-specific bodies
EAA Focus	Authorising institutions, delivering programs	Issuing, verifying, and recognising licenses	Institutional and program-level QA	EducationalID, ProfessionalID, AllianceID, MyAcademicID

Extending Classical PKI with EAA-based authorisation model
(Able to cover European, Sectoral, National, Regional and Institutional needs/autonomy)

Core concept

Electronic attestations of attributes (EAAs) establish trust chains by defining which entities can authorise others to issue specific types of credentials within educational and professional domains.

Verification process

1. Integrity check - validate authenticity
2. Issuer recognition - verify granter authority
3. Status verification - check validity period
4. Jurisdictional compliance - validate scope
5. Trust anchor resolution - trace to root

Trust chain hierarchy

Root trusted authority
National ministry / European body

↓

Trusted accreditation organisation
Delegated authority / Regional agency

↓

Trusted issuer
University / Professional body

↓

End user credential
Student diploma / Professional licence

Practical example

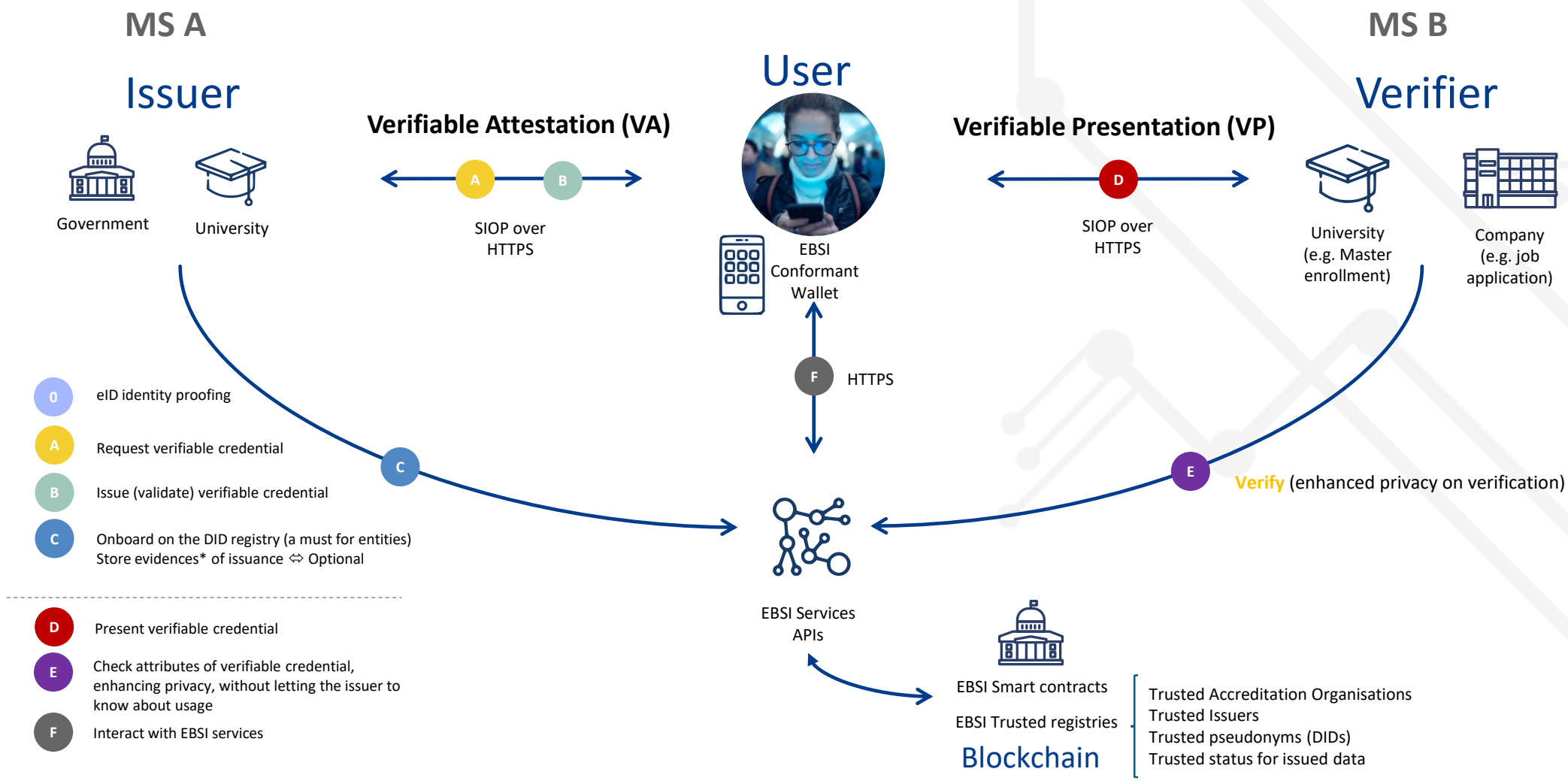
When URV (university) issues a master's degree, verifiers can automatically validate that the Spanish Ministry of Universities authorised URV to issue EQF Level 7 qualifications.

i. Ministry of Science, Research and Universities

- Can accredit:
  - "HigherEducationInstitution"
  - "LicenceToActAtNationalLevel" to Higher Education Institutions
  - "LicenceToActAtEuropeanLevel" to Higher Education Institutions
  - "EQFlevel6" to Higher Education Institutions
  - "EQFlevel7" to Higher Education Institutions
  - "EQFlevel8" to Higher Education Institutions
  - "EducationalID" to Higher Education Institutions

DC4EU WP5 Global architecture

The initial approach: Verifiable data registries based on the EBSI decentralised PKI



WP5 Global architecture

The final approach: Hybrid mode - X.509 plus decentralised PKI

SDG/OOTS

MS' means

QTSPs

University/Professional body A

Digital asset

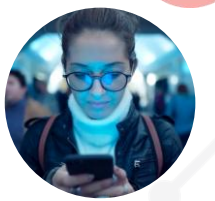
Authentic source

- Expose database records that would become EAAs
- Adapt/convert to ELM
- Generate/Gather/Keep/Preserve evidences
- Compliance and availability

Datastores

Issuer

- Gather Authentic source to provide EAAs
- Enable issued EAA's lifecycle management (revoke/suspend)
- Enable EAAs' status consultation
- Meet legal requirements (TSP,PSB,QTSP)
- Sectorial rulebook compliance
- Generate/gather evidences
- Availability



- Digital competences
- eIDAS framework

Relying party/RPI

- Registered and authorised to request PID and/or specific EAAs
- Add new means to request/verify EAAs
- Integrate with production systems
- Sectoral rulebook compliance
- Generate/Gather/Keep/Preserve evidences
- Availability

University/ Professional bodies

Company (e.g. job application)

Classical PKI for identity & basic Issuer/RP identification

Verifiable Data Registries to extend classical PKI and support/cover EU/Sector/MS/ Regional and Institutional governances(s)/role(s)/capabilities

Bridging the AI Compliance Gap:
How ISBE Solves the EU AI Act Challenge

The EU AI Act and parallel regulations create strict requirements for autonomous AI agents, yet current frameworks lack the infrastructure to comply. **ISBE** (Infraestructura de Servicios Blockchain de España) provides a production-ready, eIDAS-aligned blockchain network designed to facilitate these mandatory compliance tasks.

THREE CRITICAL INFRASTRUCTURE GAPS

Non-Human Identity (NHI) Governance

Traditional identity systems cannot handle the dynamic, per-action privilege requirements of autonomous agents.

The Traceability Deficit (Article 12)

Current agent frameworks fall to produce independent audit trails that reconstruct causal relationships.

Behavioral Drift & "Substantial Modification"

No existing infrastructure effectively tracks autonomous model changes to trigger required new conformity assessments.

ISBE AS THE COMPLIANCE LAYER

Verified Non-Human Identities

Uses DID Registries and Verifiable Credentials for just-in-time provisioning and on-chain revocation.

Immutable Audit Anchoring

Provides neutral-operator ledgers where action-chain hashes are anchored independently of the agent.

Model State Registry

Anchors model snapshots and model-state hashes to provide cryptographic evidence of continuous conformity.

DATA TABLE

REQULATORY REQUIREMENT	ARTICLE/STANDARD	ISBE COMPONENT
NHI Governance	Art. 15(4) AI Act	DID Registry + VC Issuance
Immutable Audit Log	Art. 12 AI Act	Neutral-operator Ledger
Identity Spoofing Prevention	Art. 13 & 14 AI Act	On-chain Verifiable DIDs

EBSI - DC4EU - ISBE

What lessons have we learnt? Some of them…

1. The EDIW ecosystem is an **extraordinary platform** to transform the way authentic sources can fulfil their public mission, directly or though (qualified) trust service providers. It surely will create a data market under the control of the user.

2. While the governance rules for notified public sector bodies and qualified trust service providers ensure the reliability and acceptance of some EAAs, we envisage **a world with many issuers**, both non-notified public sector bodies or non-qualified trust service providers.

3. To protect users and relying parties, a **hybrid trust infrastructure** is needed. Built on the valuable components of the Regulation (classical PKI), it will allow the management of the additional trust anchors we need, specially trust chains for complex authorisation structures representing sectorial accreditations, it will provide scalability and fast key rotation dissemination, using a public permissioned blockchain (decentralised PKI).

4. To deliver its promise, the EDIW ecosystem should be connected to other trust management infrastructures, especially **global identity federations**. More work is needed to explore the role of RP intermediaries and advance proper standards.

5. **Agentic AI** will benefit from the verifiable credential and decentralised PKI approach.

THANK YOU!

Dr. Ignacio Alamillo-Domingo

ITU-T 5th X.509 Day
May, 12th 2026