L'ICAM RÉALISÉ AVEC L'APPROCHE DID : AVANTAGES, ÉTUDE DE CAS

MARYLINE LAURENT, DIRECTOR OF RST DEPARTMENT
SAMOVAR, TÉLÉCOM SUDPARIS, INSTITUT POLYTECHNIQUE DE PARIS
COFOUNDER OF CHAIR VP-IP OF INSTITUT MINES TÉLÉCOM
REPRESENTATIVE OF FRANCE, IFIP TC11 COMMITTEE ON SECURITY AND PRIVACY

CAMPUS CYBER, 13 MARS 2025

SPECIAL THANKS

TRACIA project, funded under France 2030 programme, reference ANR-22-PESN-0006

MoreMedDiet project, as part of the PRIMA Programme, reference ANR-23-P012-0013

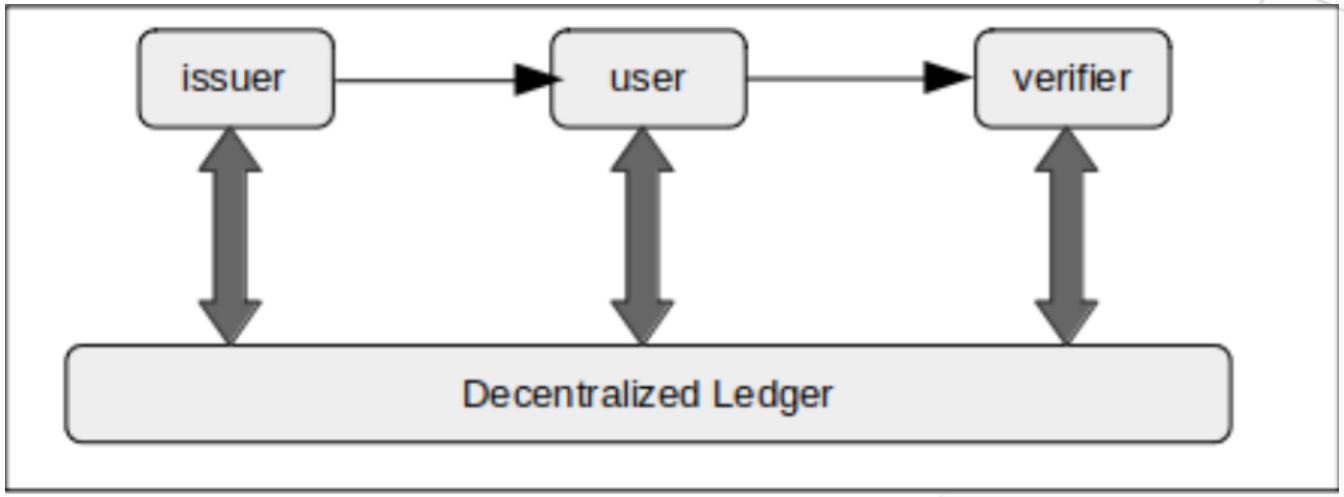
University of Murcia

SELF-SOVEREIGN IDENTITY – A NEW WAY TO MANAGE DIGITAL IDENTITIES

More control by users over their ID and data

Identifiers are decentralized and owned by individuals (due to the underlying decentralized architecture)

ID fully managed by the individual through their wallet

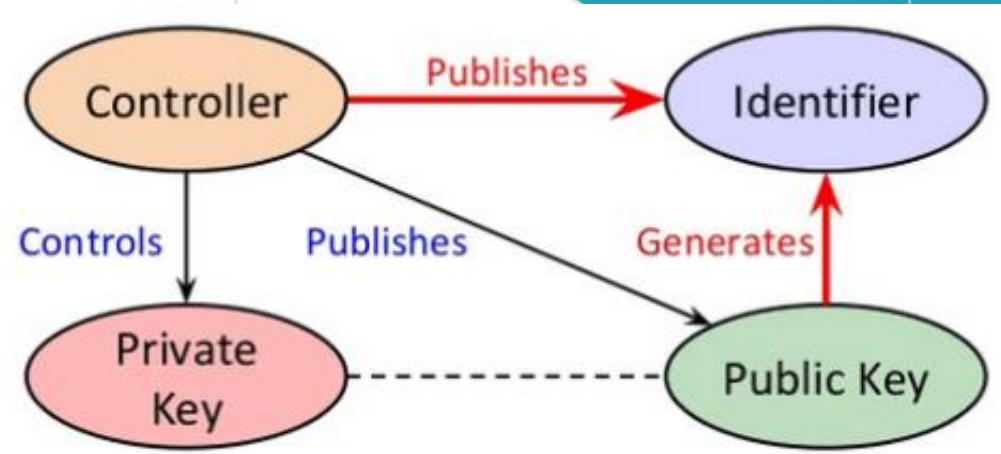


SSI: BASIC NOTIONS

Join our VP-IP chair

DID – Decentralized Identity

- W3C stantard
- Globally unique (e.g. DID:DIDMethod:DIDMethodSpecificString)
- Cryptographically verifiable thanks to DID-public key direct relationship, thus enabling support of authentication
- With no central authority



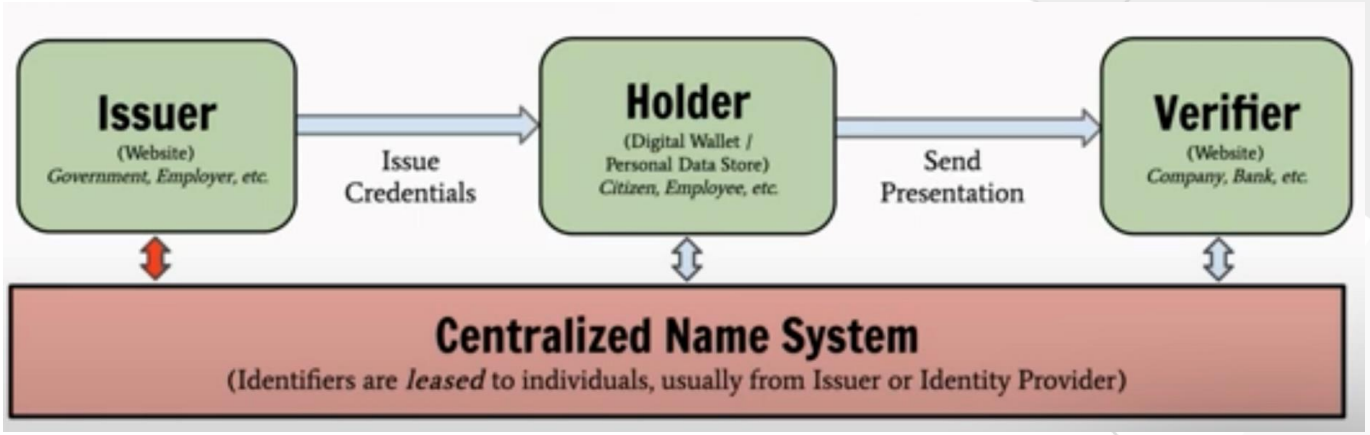
Verifiable credentials (VC) = evidence of authenticity, of status, of right

- Information related to the subject (e.g. name, license, age)
- Information related to the issuer (e.g. government)
- Evidence related to how the credential was formed
- Complementary information (e.g. expiry date)

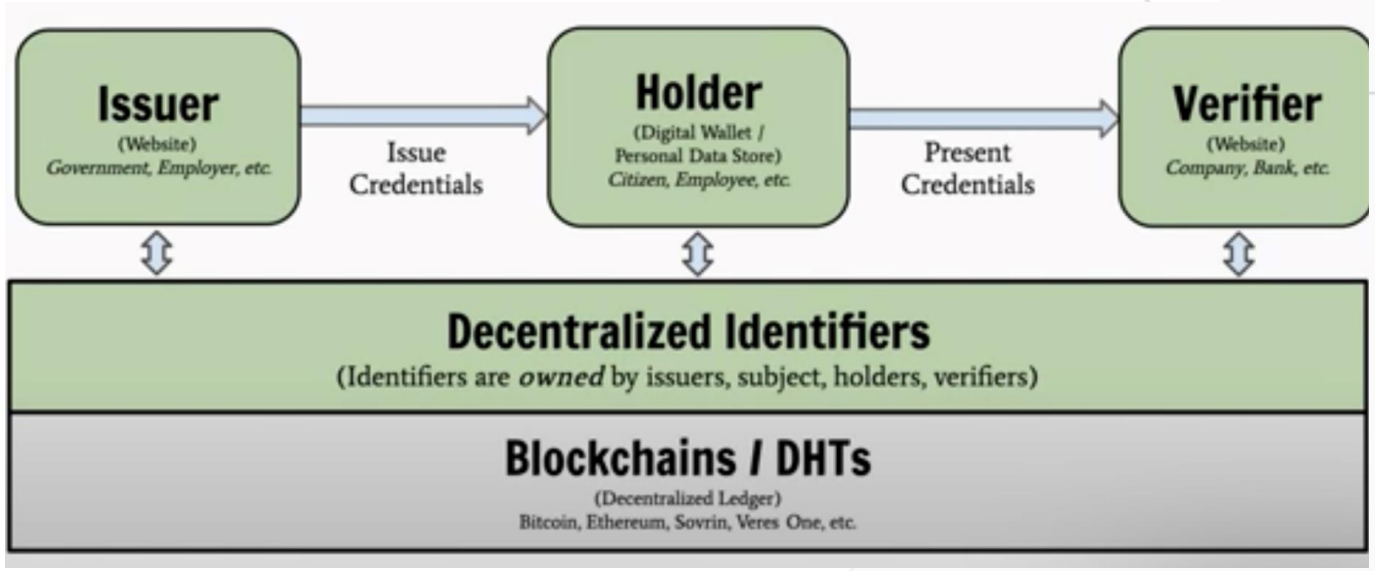
Cf. M. Naghmouchi, M. Laurent, C. Levallois-Barth, N. Kaaniche, « Comparative Analysis of Technical and Legal Frameworks of Various National Digial Identity Solutions », available on Arxiv http://arxiv.org/abs/2310.01006

COMPARATIVE USER CENTRIC VS SSI

User centric ID



SSI



(source Christopher Allen, cochair W3C Credentials CG)

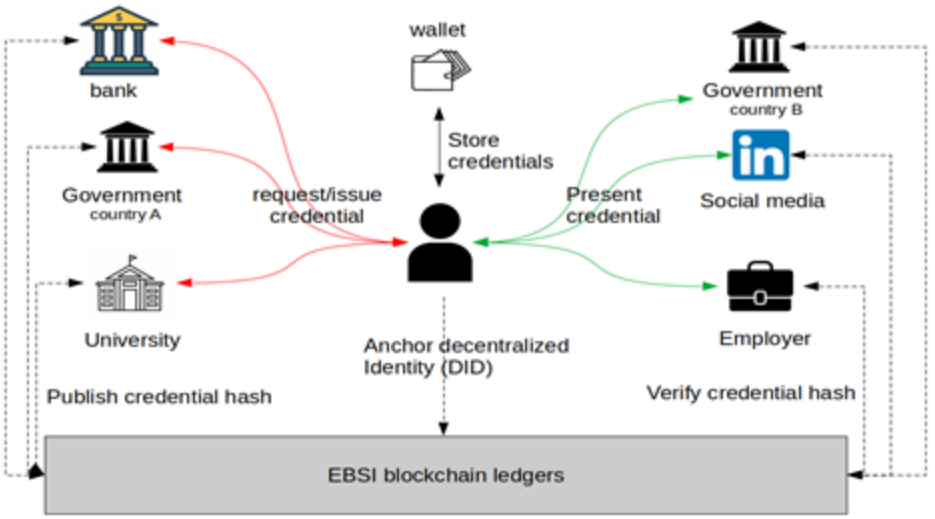
CONCRETE PROGRESS WORLDWIDE

The EBSI (European Blockchain Service Infrastructure) joint initiative between European Commission and the European Blockchain Partnership (EBP) - to deliver EU-wide cross-border public services using blockchain technology:

- ESSIF for European SSI Framework – as part of the EBSI infrastructure with each Member state assumed to have at least one node of the EBSI

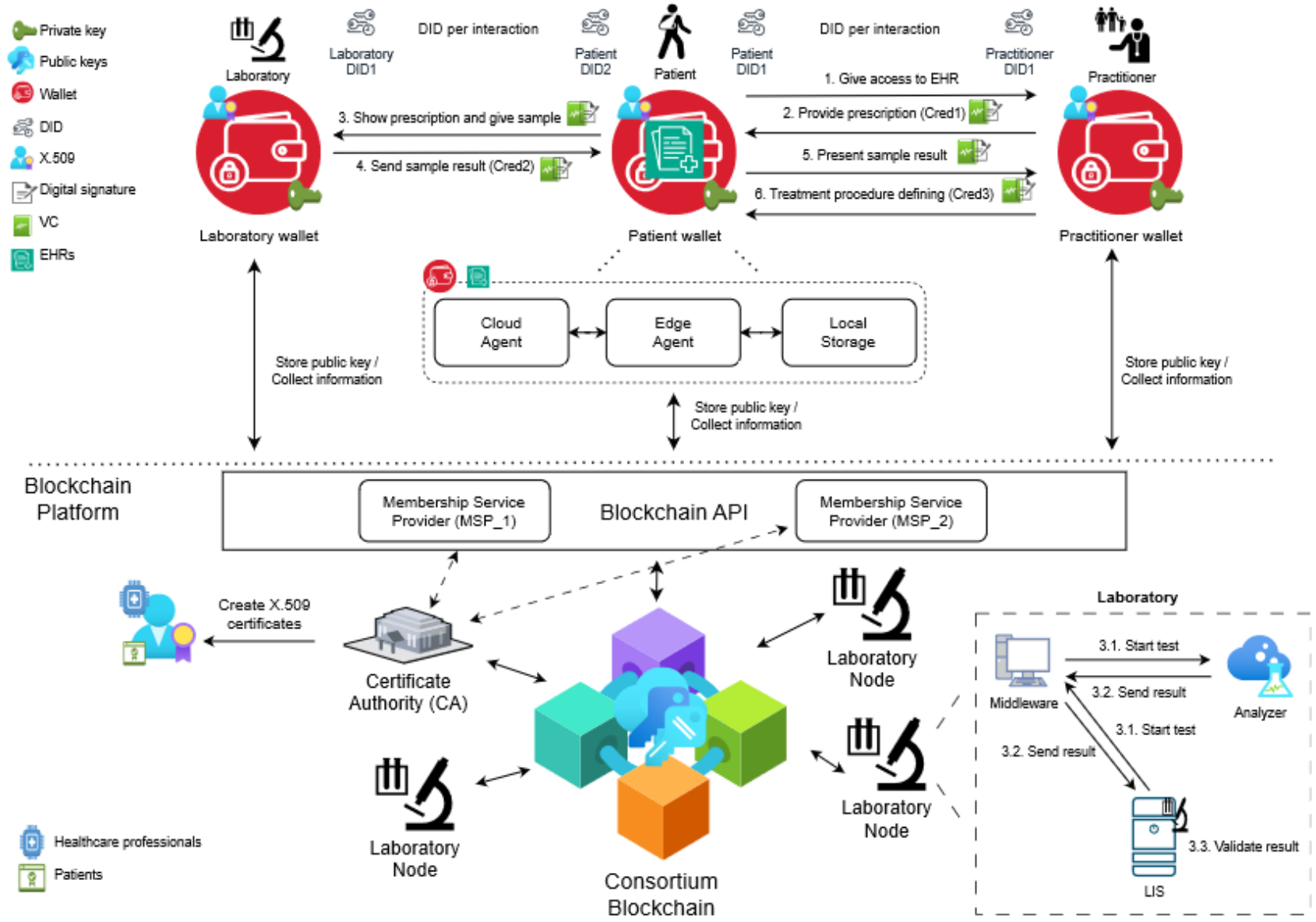
- EBSI use cases: Notarisation, Diplomas, European digital identity, Trusted data sharing + SME financing, European Social Security Identification Number (ESSIN), Asylum process management

Bhutan launched a national blockchain-based SSI with a wallet pilot for its national digital ID.



ESSIF high-level architecture

USE CASE – HEALTH DATA MANAGEMENT



López et al, « Empower Healthcare through a Self-Sovereign Identity Infrastructure for Secure Electronic Health Data Access », Jan 2025, https://doi.org/10.48550/arXiv.2501.12229

GitHub

Paper

HOW DOES SSI ANSWER TO ICAM NEEDS?

Benefits of SSI:

- User full control over the system, ownership over their identity management data, and autonomy

=> privacy, trust

- Stronger reliability and security of Blockchains as an infrastructure than other web-based infrastructures

=> security, availability

- A collectively owned and managed blockchain infrastructure (in case of a consortium blockchain) by a consortium-blockchain integrating authorities and trusted parties

=> availability, higher sovereignty than for infrastructures that are owned by third-parties (e.i IaaS)

- Integrating authorities and trusted parties as issuers and governors in the SSI solution instead of removing them

⇒ **sovereignty**

- A decentralized and scalable Blockchain infrastructure relying on a consensus protocol before validating transactions to be written onto the blockchain

⇒ **transparency, auditability, performance**

Challenges:

- Privacy-preserving solutions - ID isolation while keeping high security level
- Right delegation through dynamic credential transfers
- Consent and right to be fogotten

M. Naghmouchi, M. Laurent, « Privacy by Design for Self-Sovereign Identity Systems: An in-depth Component Analysis completed by a Design Assistance Dashboard », Fév 2025