Sovrin for KYC

Commission expert group on electronic identification and remote KYC processes

L. Boldrin
September 28, 2018
InfoCert is a provider of the notified Italian National eID system - SPID

InfoCert runs an eIDAS node and a CEF project for connecting banks

InfoCert provides trusted digital onboarding services for most Italian banks, insurance, finance services

InfoCert is a Founding Steward of the SOVRIN Network
SSI & eIDAS

Regulation and Self Sovrin Identity

National-Sovereign Identity
- eIDAS

Centrally defined identity for any person and organization, strongly validated, largely available, with a closed and regulated set of (KYC) data and data providers

Self-Sovereign Identity
- Sovrin

Lifetime portable identity (identifier!) for persons and organizations that does not depend on any centralized authority and offers support for unlimited (KYC) data and data providers

trusted identity data and liability framework

access to disparate trusted data issuers
Portable KYC

Full Digitization and Access to Trusted Sources

- **Trusted Sources**
  - Direct access
  - Mixed
  - Self-asserted

- **Digitization**
  - Low LoA
    - self-claimed attr.
    - paper corroborated
  - Low/Subst LoA
    - different sources
    - some intermediated
  - High LoA
    - multiple digital sources
    - no intermediaries

**SOVRIN + eIDAS**

**eIDAS**
Sovrin Decentralized Identity
Cryptographic Trust and Preservation of Privacy

A global public utility for self-sovereign identity, designed for the governance, scalability, and privacy requirements

Structured in 3 layers

Provides a level playing field for:
- technical competition /innovation (layer 2)
- Trusted content offerings (layer 3)
A Governed Ledger

The Global Layer Zero for All Public Information

• It operates like the Domain Name System
• On a Public permissioned blockchain
• It uses standardized components (W3C, OASIS, DIF)
  **HYPERLEDGER Indy**
• It includes identifiers, templates, revocation
• It is governed by no-profit Sovrin Foundation
  • board of trustees includes representatives from NGOs, universities, and standard-savvy people
• It is run by Stewards – carefully selected and monitored
  • Financial institutions, Certification authorities, Tech companies, Law firms, NGOs, Universities
  • The network includes eIDAS operator
Use cases

The future is now

Decentralized Business Identities
Portable KYC Practices main pains

What need to be fixed

- Different sources normally provide data on different (proprietary) identifiers:
  - IBAN for banks, PointOfDelivery for utilities, fiscal code for public administrations, LEI for finance,…
  - This is key for information assembly
- There are competing standards (formats, protocols) and no common templates
- Privacy loss via disclosure of unnecessary information to the KYC consumer
- Privacy loss via disclosing KYC consumers to KYC issuers

- Recognize sources as trustworthy and liable for the data they provide, as in the paper world
- Enable sources of KYC data (facilitate, incentivize)
- Guaranteeing freshness / non-expiration of information
- Disintermediate: if information is intermediated, the assurance level is jeopardized
# Solution: Self Sovereign Identity

Portable KYC

<table>
<thead>
<tr>
<th>feature</th>
<th>Traditional PKI</th>
<th>Online Identity</th>
<th>SSI</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common Identifiers</td>
<td>Identifier owned by CA</td>
<td>Identifier owned by IdP (<a href="mailto:john.doe@gmail.com">john.doe@gmail.com</a>)</td>
<td>DID + master identity owned by user</td>
</tr>
<tr>
<td>Privacy loss: Data Minimisation</td>
<td>No</td>
<td>Yes, delegated to IdP</td>
<td>Yes, through ZKP</td>
</tr>
<tr>
<td>Privacy loss: undisclosed KYC consumer</td>
<td>Certificates are in the hands of the user</td>
<td>Data is siloed at IdPs</td>
<td>Credentials are in the hands of the user</td>
</tr>
<tr>
<td>Recognise the source</td>
<td>Sources are identified (via identity certificates)</td>
<td>Sources are identified (via TLS certificates)</td>
<td>Sources are identified</td>
</tr>
<tr>
<td></td>
<td>Trust needs a separate channel</td>
<td>Trust needs a separate channel</td>
<td>Trust is supported by the ledger</td>
</tr>
<tr>
<td>Facilitate and Incentivise</td>
<td>Off-line incentives</td>
<td>Off-line incentives</td>
<td>Supports value exchange via token</td>
</tr>
<tr>
<td>Freshness</td>
<td>Yes, but requires access to several CRLs</td>
<td>Yes, info freshness is granted by issuer</td>
<td>Yes, revocation is handled on the ledger</td>
</tr>
<tr>
<td>Public Templates</td>
<td>No</td>
<td>No</td>
<td>Yes (on the ledger)</td>
</tr>
<tr>
<td>Disintermediate</td>
<td>Yes</td>
<td>Yes, but issuer must run high-available service</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Re-usable KYC Proof

A set of credential in the User’s wallet serve as a verifiable proof

- Verifying entity pay token to the issuer.
- Belonging of issuer to Domain Trust Framework is checked on the ledger.
- By accepting the exchange of value, the vetting entity assumes liability.
- Many credentials may be composed into a single “proof”
- Trust may be assumed based on the underwriting policy acquired from the issuer (Domain specific Policy)
Reusable electronic Identity

Electronic recycle

- Personal DIDs + DID documents **need not be in the ledger**
- Issuer’s DIDs and DID documents **need to be in the ledger**
- Issuers are normally legal persons

e.g.: INFOCERT tests creation of SSI identities in parallel with SPID identities

e.g.: TUG runs a proof of concept of an identity broker for Austria
AML5 SOVRIN + eIDAS roadmap

A proposal

Define eKYC Liability Framework and resolve GDPR issues

Enhance AML and eIDAS directives and enforce on EU and national level

Enhance eIDAS attributes with PEP and BO functions (to correspond with national/EU PEP list of functions and BO registers) and further necessary attributes

Data and LoA eKYC requirements

Local KYC attribute providers implement VCs

Technical Blueprint & Standards based on eIDAS & W3C & OIC

Implement EU Citizen Sovrin Digital wallet and bridge to eIDAS data

Organizational set-up (Sovrin engagement vs. ad hoc network)

Joint Testing & Go-Live

Jan 2019
Sovrin Trust Framework v2

20.01.2020
AMLDS transposed into national laws

10.09.2020
national central registers of natural/legal persons holding bank/savings accounts

10.03.2021
EU Interconnection of national Beneficial Owner registers of legal entities and trusts

A proposal
Thank you