Self Sovereign Identity use cases

3rd TF-DLT Meeting (February 2022)

Niels van Dijk,
SURF & GÉANT Trust & Identity Incubator

Feb 21, 2022
www.geant.org
Topics

- Methodology
- Where is SSI of interest?
- Use cases being investigated
Methodology

● Conduct interviews with stakeholders
  ○ NRENs (*SWITCH*, SURF, SUNET)
  ○ Academic community (*UniBw*, Elixir,..)
  ○ GEANT Service owners (eduGAIN, eduTEAMS, InAcademia)
  ○ Other (*UniBw Gov use case*)

● Describe use cases

● Conduct business canvas analyses
Comparing FIM to SSI
## FIM and SSI equivalents

<table>
<thead>
<tr>
<th>Property</th>
<th>FIM (SAML)</th>
<th>SSI</th>
</tr>
</thead>
<tbody>
<tr>
<td>User, Student, researcher</td>
<td>Principal; Subject</td>
<td>Holder</td>
</tr>
<tr>
<td>Identity</td>
<td>attributes; attribute bundle</td>
<td>(Verifiable) Credential (VC)</td>
</tr>
<tr>
<td>Authoritative source</td>
<td>Identity Provider (IdP); Attribute Authority (AA)</td>
<td>Issuer</td>
</tr>
<tr>
<td>Service</td>
<td>Service provider (SP)</td>
<td>Verifier</td>
</tr>
<tr>
<td>Trust framework</td>
<td>Federation; federation metadata; digital signatures</td>
<td>Verifiable Data Registry and optional policy; digital signatures</td>
</tr>
<tr>
<td>Transaction identifiers</td>
<td>Transient, Persistent</td>
<td>DIDs</td>
</tr>
<tr>
<td>Obtain credentials</td>
<td>AuthN at IdP/OP</td>
<td>AuthN at Issuers, AuthN at Wallet; Verifier Verification</td>
</tr>
<tr>
<td>User involvement</td>
<td>Transparency, consent</td>
<td>‘Full’ control over credential release</td>
</tr>
</tbody>
</table>
## FIM and SSI differences

<table>
<thead>
<tr>
<th>Property</th>
<th>FIM (SAML)</th>
<th>SSI</th>
<th>Benefit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interaction model</td>
<td>Front channel browser, IdP -&gt; Sp</td>
<td>Wallet</td>
<td>Credential Ownership</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Limited release</td>
</tr>
<tr>
<td>Proof of ownership</td>
<td>Provided by IdP / OP</td>
<td>Provided by Holder, Wallet, backed by VDR</td>
<td>No direct authN</td>
</tr>
<tr>
<td>Traceability, Linkability</td>
<td>At IdP and potentially SP</td>
<td>None (if properly implemented)</td>
<td>Privacy, GDPR</td>
</tr>
<tr>
<td>Transaction identifiers</td>
<td>Transient, Persistent</td>
<td>DID: <strong>URL and Method</strong></td>
<td>Flexibility</td>
</tr>
<tr>
<td>Trust model</td>
<td>Federation policy; Trusted third party; pki (https and XML signing)</td>
<td>Verifiable Data Registry; Blockchain or ledger; Zero Knowledge Proofs; Verifier decides</td>
<td>Flexibility, Scale, Implementation dependent</td>
</tr>
<tr>
<td>Trust establishment cost</td>
<td>Fairly high</td>
<td>Lower?</td>
<td>Tbd</td>
</tr>
<tr>
<td>Aggregation</td>
<td>Proxy; SP</td>
<td>Wallet</td>
<td>No Man in the Middle, no SPOF</td>
</tr>
</tbody>
</table>
Where might SSI make a difference?

- Reduce the cost of trust establishment
- Scales better, to allow for a longer tail
- Engaging with other sectors, both in the ability to (re)use, but also to deliver relevant data
- Better and easier end user interaction and control over personal data
- Removing the need to switch between multiple accounts
- Agility in establishing dynamic or ‘ad-hoc’ relations between (groups of) entities
Use cases - eduID

- A stable identity throughout educational and academic career
- In support of student mobility and life-long learning.
- A centralised FIM solution, under the control of the user
- Integration point for MFA, user identification, etc
- May also be used for Guest ID

- Wallet model is a natural evolution of this concept
- No need for centralised NREN infrastructure to hold credentials
- Use of academic credentials (esp. outside of academia) easier as compared to FIM model of current eduID implementations
Use cases - Diplomas and micro-credentials

- Trusted exchange of digital diploma information
- Issuance of verifiable digital credentials (badges)
- In support of student mobility and life-long learning
- Digital verification of diplomas
- Open ecosystem for verifiers

- Use of digital diploma and badges much easier for our and other sectors
- Cost saving due to easier, digital exchange
- Opportunity for standardisation
- No need for centralised infrastructure to hold credentials (?)
Use cases - Researcher identification and authorization

- In research collaborations, researcher identity is an aggregate of multiple sources (Institution, VO, Other)
- Need for flexible ‘Guest / External identity’
- AARC BPA proxy model has usability challenges
- Long tail still struggling to use FIM

- Only run centralised infrastructure to hold VO credentials, but not authN proxy
- Leverage ‘external’ credential sources, e.g. for Guest login, MFA and/or addition identity validation
- Removing the need to switch between multiple accounts
- Agility in establishing trust relations
Open questions

- Diploma and badges may still need user identification attached to credentials - does that challenge the Open ecosystem for verifiers?
- How to handle long term management of credentials?
- Can the trust ecosystem be shared between all use cases? Do we need to?
- What other elements can we consider shared?
  - DLT infrastructure(s)
  - ‘Translation’ between SSI ecosystems
  - Software implementations
  - Wallet
### SSI Challenges

<table>
<thead>
<tr>
<th>Property</th>
<th>SSI</th>
<th>Benefit</th>
<th>Challenge</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interaction model</td>
<td>Wallet</td>
<td>Credential Ownership</td>
<td>Inclusiveness</td>
</tr>
<tr>
<td>Proof of ownership</td>
<td>Provided by Holder, Wallet, backed by VDR</td>
<td>No direct authN</td>
<td>Trust needs other mechanism</td>
</tr>
<tr>
<td>Traceability, Linkability</td>
<td>None (if properly implemented)</td>
<td>Privacy, GDPR</td>
<td>Revocation is hard</td>
</tr>
<tr>
<td>Transaction identifiers</td>
<td>DID: <strong>URL and Method</strong></td>
<td>Flexibility</td>
<td>Too many methods, interop problems</td>
</tr>
<tr>
<td>Trust model</td>
<td><strong>Verifiable Data Registry; Blockchain or ledger; Zero Knowledge Proofs; Verifier decides</strong></td>
<td>Flexibility, Scale, Implementation dependent</td>
<td>Who owns the ledger? Ledger policies DLT footprint Do we really allow all Verifiers?</td>
</tr>
<tr>
<td>Trust establishment</td>
<td>Lower?</td>
<td>Tbd</td>
<td></td>
</tr>
<tr>
<td>Aggregation</td>
<td>Wallet</td>
<td>No Man in the Middle, no SPOF</td>
<td>Complex &amp; confusing to users</td>
</tr>
</tbody>
</table>