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

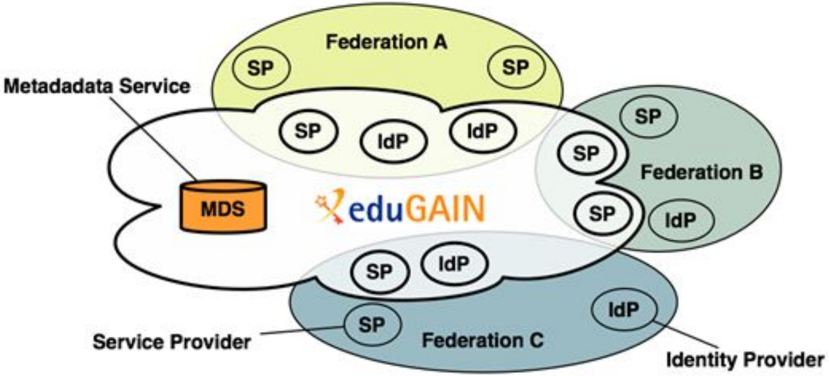
Methodology

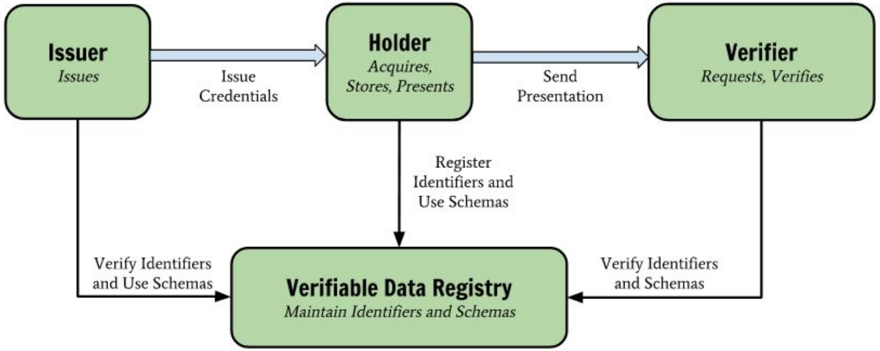
- Conduct interviews with stakeholders
  - NRENs (*SWITCH*, SURF, SUNET)
  - Academic community (*UniBw*, Elixir,..)
  - GEANT Service owners (eduGAIN, eduTEAMS, InAcademia)
  - Other (*UniBw Gov use case*)

- Describe use cases

- Conduct business canvas analysys

Comparing FIM to SSI




Issuer
Issues
Issue Credentials
Holder
Acquires, Stores, Presents
Send Presentation
Verifier
Requests, Verifies
Register Identifiers and Use Schemas
Verify Identifiers and Use Schemas
Verifiable Data Registry
Maintain Identifiers and Schemas
Verify Identifiers and Schemas

FIM and SSI equivalents

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

FIM and SSI differences

Property	***FIM (SAML)***	***SSI***	***Benefit***
Interaction model	Front channel browser, IdP -> Sp	**Wallet**	Credential Ownership Limited release
Proof of ownership	Provided by IdP / OP	**Provided by Holder, Wallet, backed by VDR**	No direct authN
Traceability, Linkability	At IdP and potentially SP	**None** (if properly implemented)	Privacy, GDPR
Transaction identifiers	Transient, Persistent	DID: **URL *and* Method**	Flexibility

Trust model	Federation policy;
	Trusted third party;
	pki (https and XML signing)
		Verifiable Data Registry;
		Blockchain or ledger;
		Zero Knowledge Proofs;
		Verifier decides
			Flexibility,
			Scale,
			Implementation dependent

Trust establishment cost	Fairly high	**Lower?**	Tbd
Aggregation	Proxy; SP	**Wallet**	No Man in the Middle, no SPOF

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

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