Self Sovereign Identity Use Cases, Establishment and Governance

Niels van Dijk, Branko Marović, Michael Schmidt, Mihály Héder

AARC BPA SSI Expert Group

www.geant.org
Agenda

● Welcome and introductions
● Previous meeting and new Meeting dates
● SSI business canvas
● Slack onboarding
● Break & adding last cards
● Miro board discussion
● Card selection
Slack onboarding

Slack channel **eduGAIN ssi-and-aarc-bpa-expert-group** – have all received an invitation? Expired invitations:

- christoph.graf@switch.ch
- david.kelsey@stfc.ac.uk
- david.huebner@daasi.de
- daniela.poehn@unibw.de
- hardt@kit.edu
- peter.gietz@daasi.de
Schedule

So far

● 9 September 2021 – introductory meeting
  https://wiki.geant.org/display/gn43wp5/AARC+BPA+SSI+WG+-+Week+36
● 30 September 2021 – use cases, identification of priority topics

Next meetings

● Upon request we propose to meet bi-weekly
  Start Oct 7 or Oct 14? (Selected: Oct 7)
● We propose sticking to Fridays at 10.00-12.30 CE(S)T (Moved to 11.00-13.30 CE(S)T)
T&I Incubator cycle 5 on SSI (business level)

- Engaged with stakeholders
  - NRENs (SWITCH, SURF, SUNET)
  - Academic community (UniBw, Elixir,..)
  - GEANT Service owners (eduGAIN, eduTEAMS, InAcademia)
  - Other (UniBw gov use case)
- Study relevant literature (scientific and grey, EDI framework)
- Conduct overall business canvas analysis
- Report
  - SSI vs FIM glossary
  - Use cases: eduID, diplomas and micro-credentials, researcher identification and authorization
  - Detail use cases in the business canvas
  - eIDAS 2.0 and EDIW
  - Role of GÉANT and its engagement with SSI
Use case: eduID

- A stable identity throughout educational and academic career
- Supporting student mobility, lifelong learning, citizen-scientists
- Features of centralised FIM solution with data under user control
- Integration point for MFA, user identification, etc.
- It may also be used for guest IDs
- Long-tail of small educational organisations and research settings
- Wallet model is a natural evolution of the eduID concept, leveraging the existing institutional, community and federated identities
- Basis for other scenarios and future communities and usages
- Easier use (especially outside of academia) as compared to FIM and current eduID models
- Aligned with the growing privacy concerns and eIDAS 2.0 / EDIW
eduID – value

- No need for centralised NREN infrastructure to hold and exchange credentials
- Separation of concerns and responsibilities, reduced data sharing and aggregation

- **For users** – user control and ownership, long-term and ad-hoc usages, all identities in one wallet, selective release of attributes, tracking prevention (mostly general SSI benefits)
- **For issuers** – unified authentication and other credentials, diplomas, badges, micro-credentials…
- **For verifiers** – less interaction with issuers and federations, easier onboarding of new or returning users, richer and possibly better identities and credentials, lower entry threshold for employers, recruiters and small providers
eduID – Incubator business model canvas accents

- **Key activities**
  - GÉANT as a forum for NRENs
  - Standardisation among large communities and groups
  - Popularisation among researchers, educators and identity and credentials consumers at all levels – GÉANT: generic and customisable guidelines and materials

- **Costs**
  - Infrastructural and long-term – implementation, standards, uses and expectations management
  - Less frequent validation of identities – rely on national schemes and organisational onboarding
  - Use of a distributed ledger

- **Revenue**
  - Mimic the current FIM revenue streams and financing models – projects, membership fees
  - Should not charge issuing and wallet-related usages – free for individuals
  - Charging of Verifiers – membership fee, not per-use
  - As indirect cost for organisations, services and research projects

- **Value (streams)**
  - Base identity for various credentials and uses (and part of their value streams)
  - Improved end-user privacy
  - Cost reduction for: institutions – not having to (re)establish user identities; dealing with alumni; services using academic identities; guest identities and short-term usages
  - Better usability and alignment with the common wallet
Use case: 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 diplomas and badges is much easier for our and other sectors
- Cost-saving due to easier digital exchange
- Opportunity for standardisation
- No need for centralised infrastructure to hold and exchange credentials (?)
Use case: Researcher identification and authorization

● In research collaborations, researcher identity is an aggregate of multiple sources (institutions, VOs, others)
● Need for a flexible ‘Guest / External identity’
● AARC BPA proxy model has usability challenges
● Long-tail of those who are 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
Researchers need a trusted digital identity to collaborate
The current FIM model requires a home organisation and federation – not every researcher can join a federation for various reasons
SSI relieves services from establishing own mechanisms for identification of individuals
Can be built on top of eduID

Ability for research collaborations to issue community created entitlements towards the researcher
Leverage external identity, with proper assurance, for collaboration with users and partners from other sectors
Research collaborations can act as verifiers for researchers
A more flexible way for the management of roles and participation and short-term control of access to instrumentation, resources, tools, reporting, etc. used in research projects, which are temporary endeavours and have own governance mechanisms
Ability to directly establish trust relations between entities participating in a collaboration
Opportunities for GÉANT

- Should stay aligned with eIDAS 2.0 and EDIW developments to prevent potential funding problems
- EDIW Toolbox process WG is important for GÉANT’s technological and SSI-related moves
  - Influence and contribute to the common technical architecture, standards and specifications, guidelines and best practices, particularly in R&E related parts
  - Coordinate with other cross-national initiatives, EU projects, and the EU regulation targeting RI, identity management and privacy (through TFs and other fora)
  - Innovation and development coordinator/hub for new SSI solutions (TFs etc.)
  - Participate in establishment of technical certification requirements and operation of certification bodies
  - Act as development and operational cost-sharing broker for technical systems that interact with the SSI
  - Provide internationally trustworthy trust lists of entities (sources and relying parties), for use with both the EDIW and other (academic and non-EU) wallets
  - Oversee or operate Qualified Trust Services (QTS), registries for academic purposes, DLT, etc.
  - Support designated intermediaries (such as NRENs) in verifying sources or attributes
  - Propose or establish catalogues of attributes and schemes for attestation of attributes
  - Protect the established infrastructure and work (such as eduGAIN) and ensure interoperability
  - Knowledge concentrator, disseminator and producer for guidelines, policies, technical and promotional materials

Many more GÉANT advantages and potential activities are listed in the Incubator report!
Open questions

- Diplomas 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 as shared?
  - DLT infrastructure(s)
  - ‘Translation’ between SSI ecosystems
  - Software implementations
  - Wallet(s)
Cards in Use Cases boxes

1. Governmental eIDs use, also across borders
2. Student mobility (+ employment): diploma and supplement data (+ micro-credentials)
3. Student? Commercial benefits: discounts, fast-track services
4. Researcher? (+ Specifics about the field of research?) Allow SPs’ access to richer data?
Cards in Standards, Interoperation, Best Practices box

- Common practices and problems: Describing and sharing, based on existing experiences
- Standardised VC dataset specs: attributes, appropriate usages for datasets, likely source types
- Defined process for definition and maintenance of standard VCs datasets?
- (+Should VC compositions and their usages be also standardised?)
Cards in People box

- Better UI for educated decisions on personal data
  - Entity profiles for Issuers and Verifiers – easier interpretation
  - Access profiles and predefined verifiable presentations – pre-authorised user choices, understanding, less false warnings, convenience?
  - (Mobile OSes are having a similar problem with app rights management)
- Training materials: target audience groups? …?
Cards in Constraints box

● Role of IdPs in VCs distribution and validation???
  ○ (+Isn’t there just pull by Holders? Introduce per requester/Holder/principal limits for DoS resilience?)

● Use of several wallets: Blessing or curse?
  ○ Different UI, security, personas?
  ○ Business, private, state-mandated (EDIW)…?
  ○ How users choose or know which one they use?

● Cost/affordability of SSI (+ transition and operation)
  ○ Conflicting business models (Examples???)
  ○ Who pays for what in different use cases? (+ shared trust and infrastructure)
Cards in Technology box

- Will some of the infrastructure or services be limited to a subset of use cases?
  - E.g., just for EU residents?
  - Wallets and wallet certifications for specific use cases?

- Open source software for services, agents, wallets?
  - Will it come in the second wave of SSI software?
Break

- Get yourself some tea or coffee
- Read through the cards on the Miro board
- Think back to presentation for today and last meeting. What questions are still missing?