Decentralised identity for GÉANT, NRENs and institutions - use cases and opportunities

May - December 2022

GÉANT (GN4-3 WP5T2)

Table of contents

Introduction **4**

Aims and audience **5**

SSI glossary **6**
Comparing FIM and SSI terminology 7
Comparing FIM and SSI elements and workflows 9
Aggregating data from multiple parties using FIM 10
Comparing FIM proxy model to SSI 12
SSI vs proxy 13

EU Digital Identity Wallet **14**

SSI Use Cases **16**
eduID 16
Diplomas and micro-credentials 17
Researcher identification and authorisation 18
Trust establishment and standardisation 19

Business canvas **20**
eduID 20
In brief 20
Value proposition 21
Key partners 22
Customer segments 23
Early adopters 23
Cost structure 24
Revenue and value streams 24
Diploma and micro-credentials 26
In brief 26
Value proposition 26
Key partners 27
Customer segments 28
Early adopters 29
Cost structure 29
Revenue and value streams 29
Researcher identification and authorisation 30
In brief 30
Value proposition 30
Key partners 31

Customer segments 32
Early adopters 32
Cost structure 33
Revenue and value streams 33

GÉANT opportunities and advantages 34

Work areas for NRENs 36

Work areas for institutions 36

Conclusion 37

Additional reading 39

Annex: Implementation-related observations from eID and SSI projects 41

Annex: From the workshop on implementation patterns on 21 October 44

Introduction

Distributed Identity (DI) presents an interesting new paradigm as well as a challenge for the T&I NREN community. Its concepts are very appealing and align well with public values in our community. At the same time, many of the technical, legal and functional properties are still in development and present numerous questions and obstacles, as was shown in recent work in NRENs and the Incubator.

The GÉANT community can hardly afford not to engage with this novel ecosystem. The learners and the academic users in our community are very mobile and are also quite well-versed in technology. Many of them will be highly interested in the potentialities of using decentralised or self-sovereign solutions for gaining more direct control over their data and leveraging the opportunities the use of SSI-based solutions bring.

Similarly, for the organisations there are several upsides to be had, ranging from easier collaboration and acceptance of data from other organisations, with less technical integration work than before; catering for niche use cases that were not economically viable with other technologies; overall cost savings. This report covers the terminology, the most relevant projects and the business canvases for key domains like eduID, diploma and micro-credentials and researcher use cases.

Aims and audience

The activity proposed builds on earlier work and investigates the following aspects of DI:

- What roles could/should GEANT and NRENs play in a DI ecosystem, and what are the associated benefits, challenges and risks?
- Which current services in the GEANT portfolio would benefit from the use of DI, and what would that look like?
- To what extent can existing initiatives implementing distributed ledgers technology be used to act as a Verifiable Data Registry to satisfy the above use cases and requirements? We should test with for example EBSI, Ethereum or Sovrin. How do these compare to the IRMA solution we previously tested (IRMA does not use DLT)?
- Initial testing with IRMA revealed a wallet-based approach may not always provide an optimal user experience. What requirements do we have for the User interface (wallet/app) and can we implement or mock these to test these requirements with stakeholders?

SSI glossary

This is a selected blend of descriptions and definitions for the most often used SSI terms from eSSIF-Lab Glossary, Sovrin Glossary V3, Verifiable Credentials Data Model v1.1, EBSI Terminology – EBSI Documentation and many other documents referred to in this report.

- **Controller** – An individual or organisation that is responsible on behalf of another entity for control over the stored VCs and (private) keys and for the actions that use them. The controller can be held legally accountable as described in GDPR.
- **Decentralised identifier (DID)** – An URL-based unique identifier associated with an entity that is used in SSI systems. An example of a DID as defined by the W3C is "did:example:123456abcdef". DID typically refers to a natural and legal person (individual and organisation) but it may be also applied to other types of subjects (including abstract ones). It is not directly linked to a formal identifier or ID document (such as a passport).
- **Decentralised identifier document (DID document)** – A machine-readable document containing information related to a specific DID, such as the associated documents repository, verification methods such as public key and services relevant to interactions with the Holder.
- **Holder** (sometimes referred to as Prover) – The owner of the credentials. Requests verifiable credentials from the Issuer, which will be stored in the Holder's digital wallet (or another credential repository). The Holder is an individual, an organisation using an enterprise wallet, or a machine acting on behalf of the Holder. The Holder is typically the subject of a credential but it may also store VCs associated with another entity, as when the Holder is a credential registry or is responsible for another subject such as a minor.
- **Issuer** – An authoritative source of credentials. It is an entity that can assert claims about a specific subject with a verifiable credential and securely provides it to the Holder. It typically authenticates a Holder, proves that the claim is valid for the Holder or the subject it represents and issues a corresponding VC. If the claim does not hold anymore, the Issuer must revoke the corresponding verifiable credential. It is typically an organisation such as a government agency, educational or financial institution (university or bank), employer, corporation or project management organisation, but it can be any other entity, such as an individual or even a machine acting on behalf of a Holder.
- **Presentation** – Data derived from one or more verifiable credentials, issued by one or more Issuers, and shared by the Holder with a specific relying party, who is typically the Verifier. Certain types of verifiable presentations might contain data synthesised from the original verifiable credentials, without containing them, thus ensuring zero-knowledge proofs. For example, instead of providing the actual age of the subject, the presentation may attest that the age limit is met. A verifiable presentation is a tamper-evident presentation encoded in such a way that authorship of the data can be trusted after a process of cryptographic verification.
- **Subject** – An entity about which claims are made.
- **Verifiable credential (VC)** – A set of claims about the subject made by the Issuer, who provides it to the Holder. The truth of claims from the trusted Issuer is assumed. The

claims must be cryptographically verifiable, e.g., by a digital signature from the Issuer. It contains a unique identifier, metadata (e.g., expiration date), claims about the subject and cryptographic proof.

- **Verifiable data registry** – A service used to mediate the creation and verification of identifiers, revocations (revocation registry), Issuer public keys, verifiable credentials (VC registry) and other relevant data required to use verifiable credentials, such as schemas defining data structures and their semantics. A credential registry may be authorised or accredited for a specific governance framework. The Trusted Issuer Registry (TIR) contains a list of entities authorised to issue certain types of credentials; there may be several TIRs within a governance framework. The identifier registry provides identifiers for subjects, resolves DID to DID documents and provides data for DID documents. A registry may be based on a distributed ledger such as a blockchain. A Trusted Schemes Registry (TSR) contains data templates of data objects such as VCs.
- **Verifier** – The Verifier requests proofs from the Holder of one or more claims to check the claim and subsequently grant access to a resource or perform a transaction. A Verifier is a person, organisation or automated entity such as a service or device. If the Holder agrees, one or more verifiable credentials of the subject are selected by the Holder. The Holder's software agent presents them to the Verifier's agent. The verification process checks the format of the credential and the presence of required content, a valid digital signature from the Issuer, that the credential is valid (not expired or revoked), and (if applicable) cryptographic proof that the Holder is the subject of the credential. In addition to formal verification, credentials need to be validated, i.e., checked for meeting the needs of a Verifier and other dependent stakeholders for a particular purpose. This may depend on the Issuer or meaning and level of assurance associated with the presented credentials. Some of these criteria such as those on the expiration date may be more stringent or relaxed than those used for verification.
- **Wallet (digital wallet)** – An architectural function providing secure storage of credentials acting as a repository of private keys, verifiable credentials and DID documents. It is used to obtain, securely store and present credentials from various Issuers and its use is restricted to its Holder. The wallet may need to be protected by a specially protected "secure element" or "secure area". It resides on a mobile device or personal computer or is supported by a remotely accessed agent service accessed from the Holder's device upon the use of multiple authentication factors. A key wallet is used to generate, manage, store or use private and public keys.

Comparing FIM and SSI terminology

The following table provides a mapping between SSI and FIM terminology. It serves as an initial orientation and overview; However, it is not always possible to achieve a perfect match.

SSI term	***Federated Identity Management (FIM)***
The user responsible for defining the types or	**Application owner**

SSI term	*Federated Identity Management (FIM)*
sources of VCs that need to be presented to the Verifier and associated validation criteria.	
The user's or other party's identity, i.e., that it is who it claims to be, is expressed by one or several identifying attributes. The Holder presents a VC with some identifying attributes to prove an identity to the Verifier. The Holder's identity is accepted if the VC is valid and obtained from an appropriate Issuer, as the Holder's control over the Wallet in which it has been stored is assumed. Typically, disclosing one's identity is not needed at all in most SSI scenarios.	**Authentication**
Determining whether the Holder is allowed to access a given resource or function at the Verifier. The Holder presents a VC used to prove to the Verifier the right to access a service or perform an action. The Holder's rights are deduced from the values and validity of attributes contained in the VC, and the Holder's control over the Wallet. Typically, this does not require disclosing one's identity nor even the exact value of an attribute but that it has specific characteristics, e.g., proofing that the Holder is a student or over 18, through the appropriate Presentation of agreed attributes.	**Authorisation**
The secret used by an entity to prove itself to the system. In SSI these credentials are used to grant the user access to a VC or Wallet and allow it to perform some action on them.	**Credential**
Holder or Verifiable data registry that is used to manage and provide information about Subjects and their characteristics that are typically expressed via VCs.	**Directory**
Holder – Controls the wallet and decides what content to present to the Verifier	The (end-) user or principal acting on behalf of the subject and deciding on sharing the information on the subjects expressed by data (attributes) within VCs contained in the Wallet.
In SSI, the IdP function is accomplished by	**Identity provider (IdP)**

SSI term	*Federated Identity Management (FIM)*
the Issuer of VCs that are used for subject identification.	
Issuer	Source of credentials that are provided by an FIM Identity Provider (IdP) or Attribute Authority (AA)
The system or organisation providing a service, The user interacts with it through the application used to access the service. In SSI, this application acts as a Verifier	**Service provider**
Verifiable credential (VC)	Set of attributes similar to those provided via SAML attribute statement, authorisation decision statement or assertion statement from an IdP or AAs to an SP.
Verifiable data registry	Certificate chains, certificate revocation lists (CRLs), lists and storages of trusted root certification authorities, SAML federation metadata, etc. In SSI, this data is closely related to VCs.
Verifier	The Relying Party (RP), Service Provider (SP) or person interested to verify some claim.
Wallet	Storage of attributes, typically managed by the end-user or its representative. There is no real equivalent in FIM, the most similar systems are password management applications and certificate managers with personal certificates.

Comparing FIM and SSI elements and workflows

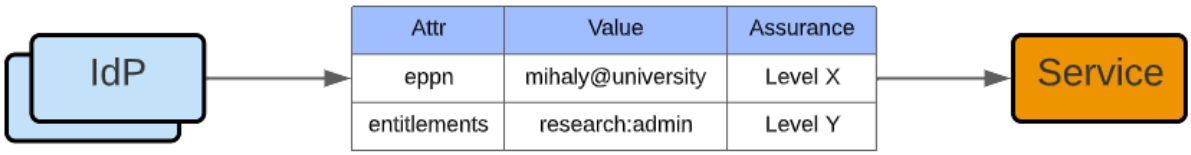
This section compares the elements and data flow from federated identity with the equivalent flow and elements from an SSI-based flow. In the example, we consider the flow of personal data used for allowing a user to gain access to a service operated by a research community.

Aggregating data from multiple parties using FIM

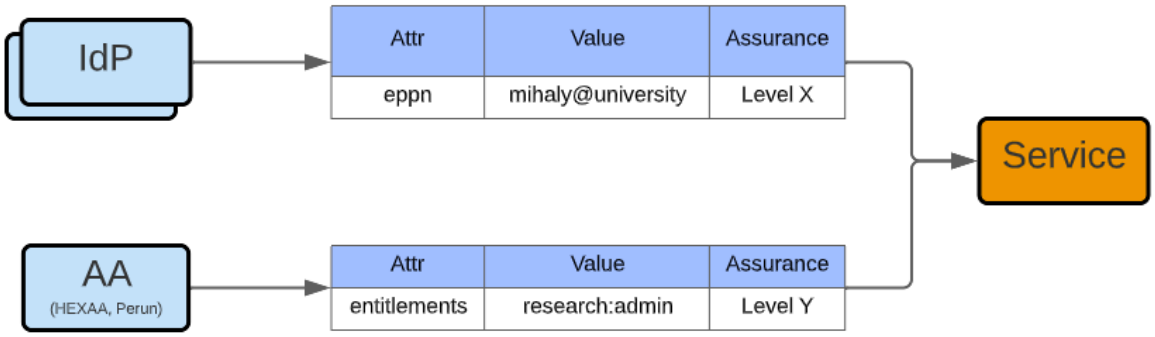
An identity federation relies on connections between IdP and SP. This allows for communicating identity and personal attributes very well. In some scenarios, however, multiple authoritative

sources need to be queried to construct a relevant set of user data. This is the case for research collaborations, where the research collaboration itself holds data on the roles and rights of the user in the context of the collaboration. For such a multi-party data exchange, a single IdP is typically not authoritative for all data. Also, the harmonisation of schemas is required for dealing with collaboration-specific data; an alternative would be storing and fitting together of that data on the SP side in the application (which is suboptimal for both provisioning and de-provisioning).

An approach that could be taken is to have multiple IdPs issuing data about the subject, but this is not user-friendly as it requires accounts at multiple IdPs and does not scale and integrate well from the perspective of the services.



This constraint makes it desirable to implement Attribute Authorities as third parties in the login flow. Such AAs can then be used to complement institutional data with data specific to the research collaboration.

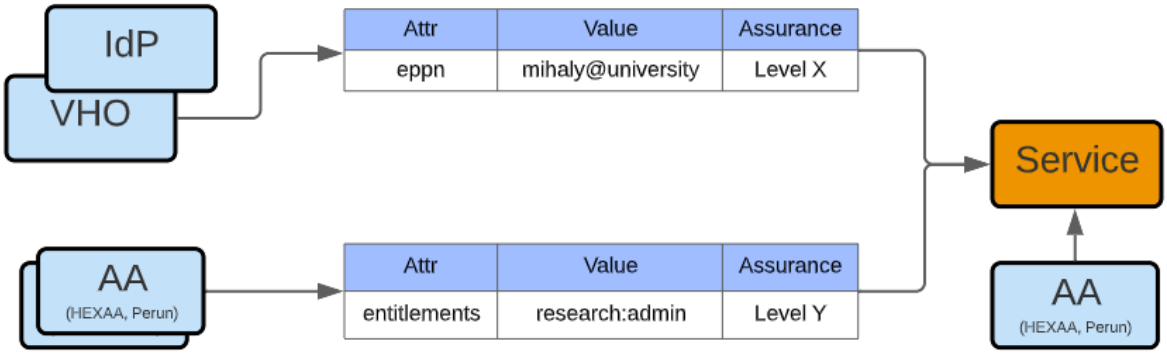


However, this model does not scale well either. One challenge is that the AA integration is fixed and ‘hard coded’. Some SPs will have to rely on multiple AAs to support multiple communities, but without an AA discovery, they always have to query all AAs, which creates technical problems.

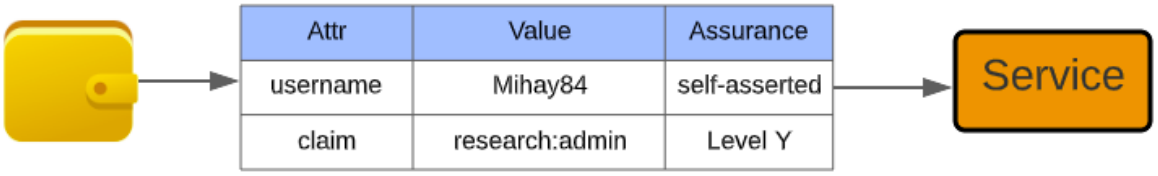
Furthermore, by querying an AA the SP will release a shared identifier, such as an eduPersonPrincipalName (ePPN) to all AAs and thus advertise the timestamp and the user of the authentication to all AAs, even if there is no relation between the AA and the user. This might be considered as leaking personal data.

This proliferation of AAs very quickly gets to its limits, especially for services that interact with many communities – without an AA discovery, they always have to query all AAs, which creates technical problems.

In the SSI scenario, the user brings some of their credentials in a wallet or similar technological solution. These credentials may be in the form of claims, in which case they should be verifiable. Since the claim Issuers are known from the claim itself, there is no need for discovery of where to turn for verification.



Finally, this approach may completely replace the home organisation and let the user present both their identity and attributes/claims to the service upon access.



In the case of the mesh federation, the SSI approach is a logical next step towards decentralisation: at the time of login, the home organisation is not even necessary, only when issuing the claims.

Also, while the connection between two institutions is a bureaucratic process involving both parties joining the multilateral framework of the federation, in the SSI case no such step is necessary: one organisation may unilaterally decide to release claims while another decides to accept those, with the user app/wallet being the mechanism of transport in between.

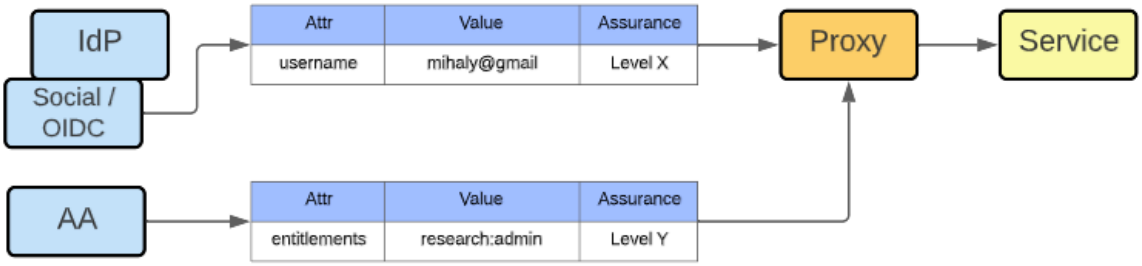
However, some infrastructure (e.g. containing public keys) is still necessary for verification.

This infrastructure can be more lightweight than federation metadata and tools: for instance, it may be implemented on a distributed ledger, not requiring any central nodes or governance.

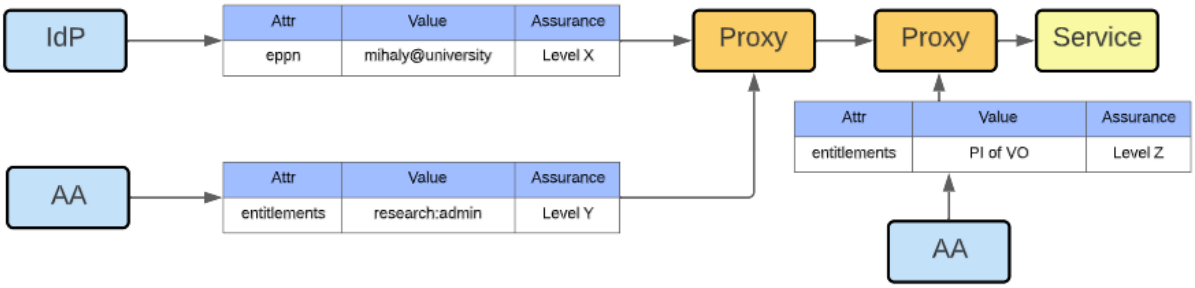
Comparing FIM proxy model to SSI

In some cases, a proxy model is used to aggregate IdPs or SPs following some organisational structure. This model helps concentrate and thus scale the interactions from the perspective of the connected entities. It does however introduce a central component that needs to be operated and trusted by all involved.

The SSI in proxy approach is a logical extension of the available data sources for a service, for which the multi-protocol proxy was created in the first place. This arrangement has the same limitations as the initial arrangement of the mesh federation: the sole source of all information is the IdP.



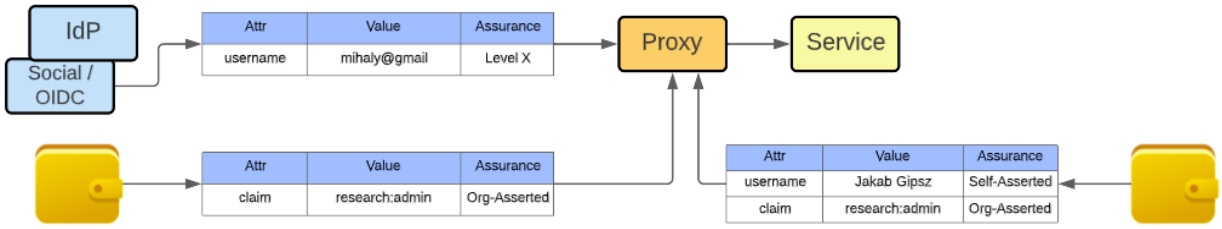
This is circumvented by the insertion of an attribute authority or a membership management system. In this arrangement, the proxy is the glue and the point of integration and protocol translation. Therefore, communication with the AA will happen at this point. The proxy implementation provides a place to execute some business logic, e.g., the selection of the AA based on the home organisation of the user.



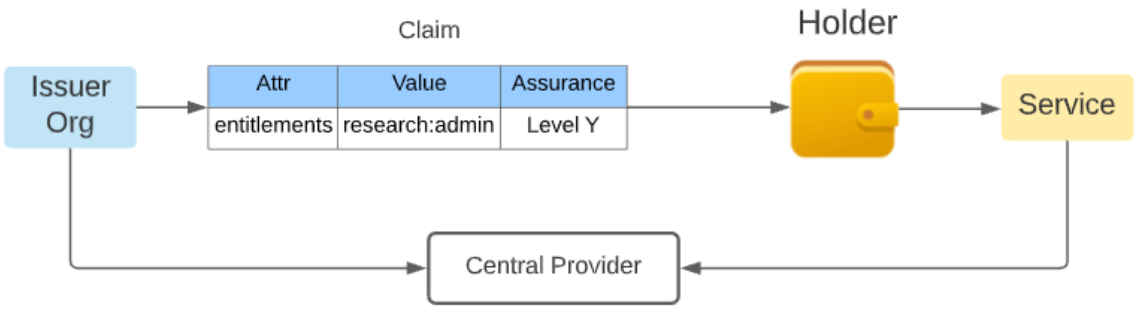
The repetition of the idea – inserting a proxy to handle conditionals or complement the data sets, leading to a chain of proxies – is quite common. In hub-and-spoke federations, users can

go through a chain of proxies. The reason for this is that there is no other way for two hub-and-spoke federations to inter-federate (if they follow the model exactly and IdPs only talk to a national proxy). Moreover, organisations within a federation also tend to have proxies. This poses some challenges: the single-log-out does not work very well and the interpretation of the GDPR roles (e.g. data processor, data controller etc.) is not straightforward in a chain of proxies.

SSI vs proxy



With the advent of SSI, some of these problems can be circumvented, especially if the role of the IdP is also taken over, instead of only the role of the AA. Data protection is enhanced by the fact that the wallet may hold, targeted or polymorphic pseudonymous encrypted data.



EU Digital Identity Wallet

Developed within the European Digital Identity framework proposed by the European Commission, eIDAS 2.0 is an evolution of an existing EU regulation eIDAS (electronic IDentification, Authentic and trust Services) established in 2014. This revision of eIDAS should ensure a convenient and transparent European Digital Identity Wallet (EDIW) and an EU-wide legal and technical framework that should serve as an equaliser, as opposed to the current national ID documents (compliant with current eIDAS but also traditional ones) it is based upon. Still, the implementations of EDIW are to be provided to end-users by EU states or

organisations mandated or recognized by states. This wallet may hold not only an EU digital Identity but also known attributes and other independently issued credentials. It will be a way for consumers and businesses across the EU to electronically prove their identity, authenticate, or prove their attestations and entitlements. For service providers, the EDIW will expand their customer base, save costs and time, streamline interactions and build trust in cross-border transactions.

All this is done to overcome the current huge discrepancies between the member countries in the availability and adoption of national digital IDs. According to a 2020 Eurobarometer survey, only about 60% of the population in 14 EU states can use their national eID cross-border. At the same time, only 14% of key public service providers across all EU states allow cross-border authentication with the eID [European Digital Identity]. Other necessary adaptations are related to the fact that the usage of digital services is getting more mobile in terms of access technologies and more often crosses borders authentication.

The EDIW could be implemented as a secure device, mobile application, secure software used to access the web or a cloud service that receives and stores digital credentials. This wallet will allow people to securely and transparently rent a flat or car or open a bank account in another country over the internet using their linked national identity. This will also allow businesses to provide the related services or use them as well across the EU. All this will happen without having to use private (service-specific) identification methods or unnecessarily share personal data.

Besides ensuring that the relying party can authenticate the user and receive electronic attestations of attributes, the wallet would also be a QSCD (qualified electronic signature/seal creation device). It will therefore also include signature management software or an authentication method for the QSCD and the related signature management service. It remains to be seen if the EDIW will support several IDs for a single person (including transient or pairwise ones), which is necessary to prevent worldwide tracking of users and aggregation of their data.

Among others, for eIDAS 2.0 to succeed, it will require (as stated in premises 27 and 28 of the eIDAS amendment proposal):

- Any entity that collects, creates and issues attested attributes such as diplomas or licences should be able to become a provider of electronic attestation of attributes.
- Relying parties should use the electronic attestations of attributes as equivalent to attestations in paper format.
- Private relying parties should accept the use of European Digital Identity Wallets for the provision of services where strong online user authentication for identification is required.
- Very large online platforms that require users to authenticate to access online services should be mandated to accept the use of European Digital Identity Wallets.

eIDAS 2.0 will define special Personal Identification Data (PID). It is crucial for wallet features to include authentication and handling of identity attributes, which are a basis for access to other attributes, but without bundling them to verifiers with access to identity attributes. The wallet should, in the appropriate scenarios, allow users to selectively present verifiable identification data to service and resource providers.

The EDIW's ability to keep credentials that are not issued by the approved Qualified Trust Service Providers makes the wallet far more useful for non-government use cases. This will significantly increase its adoption and use. But, even with Member States as providers of EDIW, legitimate use of non-government credentials should not be prohibited even after the governmental credentials are revoked. Even more important is that many use cases that currently do not require full identification should remain anonymous even if the use of eIDs becomes simple and ubiquitous – the users should not be baselessly coerced by service providers or other relying parties to identify themselves just because it is technically easy for them to present their personal data.

SSI Use Cases

In the next sections, we will investigate how the SSI paradigm [ref: The Path to Self-Sovereign Identity] and its associated technology may be leveraged to enable or improve three use cases:

- eduID
- Diplomas and micro-credentials
- Researcher identification and authorization

eduID

eduID is meant to accompany learners through their academic and professional careers and is not limited to active members of academic institutions of academic services, but it should also serve them after graduation. It is a foundation of services for universities and trusted partners in the digitization of their work in education and research-related scenarios. With it, those who study or work at several universities need a single identifier. Is a common base for alumni services, registration for continuing education and when a person returns to academic institutions for education or work and who needs access to experiment facilities, computing, repositories, data, journals, book borrowing and other resources for education and science.

Various national federations have adopted the concept of an eduID: a centralised solution, under the control of the user, that allows users to log in to services in a similar way as they would use the institutional account. The eduID account provides users with a stable identity throughout their educational and academic careers, thereby fostering student mobility and life-long learning. The eduID account may also help users to retain access to specific services or to acquire new ones after graduating from an institution. Using eduID for researcher-related

purposes allows for a smooth transition from learning to a research career during their academic life.

Most implementations allow anyone to create an account within the national eduID platform. It is therefore also usable as a guest identity provider solution. Some NRENs allow users to engage with services even if the user is not a learner at one of the member institutions. This is for example the case for users in companies that participate in the learning of students.

From a technical perspective, an eduID implementation typically consists of a proxy and a database or directory with user credentials and attributes. Academic affiliation and other institution-specific credentials are used to enrich the base identity provided by eduID. In some cases, additional sources or identifiers like a governmental identity may be linked to improving data quality and usability. Services that were connected to using the traditional federation model, either as part of the national identity federation or as part of a separate trust framework, can now connect more directly to their end-users, without having to be directly involved with and admitted into one or several specific trust domains.

Deploying SSI for eduID is a natural evolution of the eduID concept. Initially, the SSI solution could be deployed as a single Issuer, leveraging the federated eduID as a single source of credentials. This sets the scene for a future model where institutions and other authoritative sources become Issuers in an SSI-based eduID ecosystem. As eduID currently makes use of the national identity federation trust model, something similar will be needed for the SSI interactions. It would be a big advantage if the use of SSI would also allow for more easy use of academic credentials with third-party Verifiers that are not members of the current academic identity federation.

Several scenarios exist where the service is only interested in a specific credential, e.g like the user's affiliation to an institution or, e.g., a publisher who might only need a specific entitlement. Such scenarios fit very well with SSI as by default users can choose to release specific credentials from their wallet.

Diplomas and micro-credentials

One of the core activities of our industry is to educate and train people and subsequently certify that the learner has acquired these skills through certification or diploma. A growing number of institutions encourage their students to obtain a part of that education elsewhere.

Furthermore, there is an increasing need to express these certifications in a digital way across both sector and country borders. This will improve national and international student mobility and facilitate lifelong learning, allowing Higher Education to become more flexible.

Increasingly, recognition of skills and capabilities is handed out as micro-credentials. A micro-credential is a unanimously used term for a digital proof of the learning outcome that a

learner has acquired following a short learning experience. These learning outcomes have been assessed against transparent standards. The proof is contained in a certified document that lists the name of the Holder, the achieved learning outcomes, the assessment method, the awarding body and, where applicable, the qualifications framework level and the credits gained. Micro-credentials are owned by the learner, can be shared, are portable and may be combined into larger credentials or qualifications. They are underpinned by quality assurance following agreed standards. Micro-credentials may potentially become a bearer for European Credit Transfer and Accumulation System (ECTS) points.

With the use of SSI technology, three main use cases may be supported:

- Trusted exchange of digital diploma information between (government) accreditation agencies across Europe.
- Issuance of verifiable digital credentials (badges) by educational institutions and others for use in education and other sectors.
- Digital verification of diplomas or digital credentials.

Researcher identification and authorisation

In any given institution, researchers are engaged in large and small research collaborations, which span institution, sector and country borders. Many collaborations share resources across these borders as well. Enabling access to these resources is critical for the ability to collaborate.

What these collaborations often need is a generic and trusted mechanism for researcher identification. National identity federations and eduGAIN have helped to make this more available, but collaborators may also be outside of academia, or may not be able to use a federated identity from their institution for various reasons.

Next to a base identity, collaboration needs to verify that a person is a genuine researcher. The criteria for this are often collaboration specific. Upon accepting a researcher as a member, many research collaborations assign roles and rights to the user. These entitlements may be used to authorise the user upon entering the service to allow access to the resource.

SSI-based researcher identification may relieve the services from establishing their mechanisms for the identification of individuals. In essence, this is similar to how FIM enables access. However, as SSI is assumed to leverage a broader identity ecosystem and is not restricted to academia alone, the same mechanisms may be used to support users who for some reason cannot make use of academic FIM. While it is likely institutional identity has to be part of the SSI-based researcher identity, additional authoritative sources, like government-based digital credentials or for example bank ID may be used, which may be more robust. This may also help mitigate challenges that arise from researchers changing their home organisations.

In the current FIM ecosystem, attributes are typically passed to the service as part of the authentication transaction. For this to work, a technical trust relation, exchange of metadata, must exist between the identity provider (IdP) and the service provider (SP). In an SSI ecosystem, the service must still trust the Issuer, however, such a trust relationship does not require a mutual exchange of metadata. This may allow for more easy re-use of existing trust relationships, without the need to establish direct (technical) associations or potential data leakage for the purpose of verification.

The AARC Blueprint Architecture (BPA) describes a ‘Community AAI’ solution, a set of software building blocks that can be used to implement federated access management solutions for (inter)national research collaborations.

The benefit of the BPA is that its proxy-based architecture provides both a technical integration point for authentication and authorisation, as well as a centralised point for implementing the research communities' policies. The BPA also identifies a ‘membership management service’ which implements community-specific onboarding to help establish the researcher's status and may be used to issue community-specific attributes to establish roles and rights. Implementations of the BPA, like eduTEAMS and SRAM, have greatly improved the capability to use FIM for research communities.

Unfortunately, the BPA model also introduces a few challenges:

- The BPA proxy acts as an authentication gateway, which impacts the user flow. Depending on the authentication path taken by a user, the user may end up with a different identity and hence different permissions. This is confusing for end-users and leads to challenges for services.
- A centrally operated infrastructure is required, which is acting as a ’man-in-the-middle’ for all authentication transactions. This impacts data protection and user privacy and hence needs to be considered carefully.
- Institutions need to release attributes to all such BPA infrastructures their users want to make use of. Even though this already scales much better as compared to releasing attributes to individual services, this may still impede the ability of users to gain access to relevant services.
- A centrally operated infrastructure may not be feasible for all communities as it introduces operational costs and a certain level of organisation of the collaboration.

At first glance, an SSI model may offer similar benefits as the AARC BPA model, while reducing the number of impediments as a wallet model may take away the need to have a proxy as the central authentication gateway. This model will be further explored in this document.

Trust establishment and standardisation

It should be noted that SSI technology alone will not be enough to support any of the above scenarios: Transnational and cross-sector acceptance will require a high degree of standardisation, both technically as well as semantically. In addition, a trust framework is needed that goes beyond the technical trust of the SSI infrastructure. The trust framework, or frameworks, must allow for both hierarchical qualification frameworks that are typically laid out on a national level, as well as additional frameworks that may be more local or context-dependent.

In the current FIM ecosystem, Federation Operators already have a role as a trusted third party. The federations have established common practices in registration and also classify and categorise services and institutions. This is functional not only on a national level but even globally, as part of the eduGAIN inter-federation. This capability is very similar to the Trusted Issuer Registry (TIR) described in the SSI ecosystem.

The SSI ecosystem also describes the role of a Trusted Schemes Registry (TSR). This is very similar to what the academic sector has achieved by developing commonly used schema like eduPerson, VO person in both SAML and OIDC over all federations. In addition, a governance model was established to manage these schemas on a global level.

Rather than reinventing all of this for use in an SSI environment, it would be valuable to investigate how such existing trust and governance can be reused. At the same time, one should realise the SSI paradigm makes the user a first-class party in the ecosystem, which may mean that not all parts of the FIM model can be translated into the SSI world.

Business canvas

eduID

In brief

SSI distributed identifiers as eduID provide a basis for all other education and research-related scenarios. Its primary benefits are the separation of concerns and responsibilities for identifiers and related data and business and technical functions, which all greatly reduce the leakage and sharing of personal data.

The current (federated identity) paradigm of centralised or hierarchical governmental, commercial or academic services fully controls the generation, recording, processing, confirmation and providing of this information. This is justified by trustworthiness and ease of use, but is becoming increasingly misaligned with the growing privacy- and data protection-related concerns.

The SSI-based eduID contributes to the establishment of a truly privacy-oriented inclusive, user-controlled and extensible academic identity and personal data environment. Although centralised one federated identity may be conceptually simpler and presently more effective, the growing demands for privacy protection and data sovereignty, as well as emergent academic concepts such as continuing education, lifelong learning and citizen-scientists, do not fit well. The federated approach can be tweaked to work with the new concepts and act as Issuers, it is expected however long term this will no longer be needed with the growing adoption of the SSI solution. An SSI-based solution will also increase the use of services in engaging with the long tail of small educational organisations and research settings, in which the users will also want to directly establish the creation and use of SSI-managed information. The current federated ecosystem cannot cope with so many actors and relations.

Given the proposed goals of eduID, using SSI to implement eduID seems like a very logical choice, as SSI already provides many of the desired properties. As eduID data is likely to be included in the eIDAS 2.0 EDIW among other identifying data, eduID will be affected by the definition of eIDAS 2.0 personal identification data (PID).

Value proposition

The main value of SSI-based eduID is that it may be used as a base for all other academic learning and research-related usage scenarios and services. It is assumed such an SSI-based eduID will be able to use the existing or future state-governed identities, and will also make use of the identity established and verified within the academic institutions and communities.

At a more fundamental level, SSI-based eduID brings the general benefits of SSI, where:

- The user has control of their identity, which can be expressed through their academic career and beyond.
- Multiple formal identities may be expressed and aggregated in a wallet.
- The selective use and controlled release of attributes, as well as the use of data derived from credentials in the form of Presentations, is more privacy-preserving and helps prevent the services and AAI infrastructure from tracking users or collecting their data.

For end-users, a transition to an SSI-based eduID would allow them to maintain control over their education and research information independently of the issuing entity and what parts of their achievements and past relationships with academic and work-governing organisations they would like to expose to specific organisations and services. This would reduce the need to delegate this control to a specific service or institution and depend on a centrally-coordinated infrastructure. Effectively, this would in some cases even eliminate justifications for centralised aggregation, which could lead to unvetted data aggregation and potential misuse of personal information on education, work, research and interests. Still, the establishment of SSI eduID does not fully prevent parts of this information from being collected by other means.

For Issuers, SSI may present a new way of issuing digital credentials. In the FIM ecosystem, the issuance is mostly focused on authentication and authorization-related credentials, which will still have value in an SSI ecosystem as well. However, new opportunities arise for issuing credentials containing diplomas, badges and micro-credentials, with eduID being the base identity layer for those services. Finally, an SSI ecosystem may allow for a more dynamic establishment of trust and more freedom to establish their applications and define attributes for different educator and researcher groups.

For Verifiers, there is less need to engage with issuers and federations to be able to use the credentials they need, which may lead to far greater use. Within the sector, this may be beneficial for onboarding new or returning students and it should make it easier for research-managing organisations to engage with identity. When interacting outside of our sector, leveraging guest identity should become easier as incoming users will likely have a better quality identity in their wallets as compared to the currency commonly used ‘social’ identity. For entities who want to make use of data from our sector, like e.g. (future) employers or recruiters, the SSI ecosystem may present lower technical and organisational thresholds for both large and small resource and service providers.

Key partners

The key partners are learners, educators, employers and organisations who are part of or engaging with education and research.

Learners (students and individuals engaged in continuing education or lifelong learning) and **Researchers** (scientists, research staff and individuals engaged in citizen science) are very broad and often overlapping groups of users, with many of them enrolled in some level of formal education and therefore becoming users of GÉANT-provided networks and services. Regardless of their closer affiliation, these users may use SSI to gain access to services and resources while maintaining control over their personal data.

Academic institutions, research projects and open science communities need a reliable identity usable at scale. Typically such a system should be integrated with the student education or HR record-keeping systems that provide consistent and up-to-date information about users.

Employers and recruiters may act as Verifiers to benefit from available digital credentials.

Publishers may leverage SSI-based systems for allowing access and enabling collaboration, as they participate in the process of scientific publication, using researcher identity.

Infrastructure providers, both academic and commercial ones, could move from direct management of authentications and related data and collection and propagation of attributes to the governance of the rules and trust fabric.

eduID-like platforms may be incentivised by **governments and the EU** or by **NRENs**, who may adopt initiatives from their advanced members and home organisations and propagate them to GÉANT. This work may either be determined by government-provided platforms and infrastructure or simply regulated and endorsed with regulatory frameworks that recognise SSI.

Alternatively, **GÉANT** may gather a few interested NRENs and work with them on interoperability and standardisation or harmonisation of the efforts conducted by participating NRENs and home organisations. GÉANT could also act as a conduit toward related projects or infrastructural efforts (EBSI, ESSIF, Gaia-X, other (inter)governmental platforms and eID schemes) and large scientific collaborations or infrastructures or their identity systems. Therefore, GÉANT would evolve into a key player in the development of SSI standards and trust fabric and provider of SSI services and solutions. This will also result in a change in its relationship with identity federations in this area, where the relationship would be oriented toward harmonisation, interoperability and general SSI services instead of being a direct aggregator of live data from identity federations' services and operator of composite services. But it would remain as the aggregator of metadata and validator or guarantor of trust. An elaborate list of the elements of possible GÉANT involvement with SSI and a list of its comparative advantages is provided in GÉANT opportunities and advantages.

Solutions employed by collaborations home organisations may come from independent specialised **vendors of SSI platforms** and distributed, stewarded or proprietary **SSI infrastructure providers** or environments (such as Sovrin, Ethereum or Bitcoin). Owned solutions or supporting companies need to be contracted by home organisations or NRENs.

Big tech service providers are quite unlikely as solution suppliers at a small scale, as they are more likely to be interested in a direct adoption of their generalist SSI services. This may also coincide with the expansion of their brands and dominance in the fields of technology and control over personal data and behavioural tracking. Still, they are likely to be significantly influential toward specifications and standardisation, as well as later interoperability integration.

Customer segments

Involved user groups differ greatly in terms of their availability and intensity of interactions

- Graduate students
- Post-graduate students and early researchers
- Occasional or returning students and alumni
- Participants of research and development projects who manage or support or otherwise do not primarily work in research and education
- Accomplished or high-intensity researchers utilising sensitive or high-cost equipment, resources or data
- Citizen scientists

In terms of organisational customers, the main actors are:

- Educators
- Employers
- Research organisations

Early adopters

Possible early adopters include:

- Individuals who are currently not able to participate or not happy with the existing identity management schemes and (potential) Issuers and Verifiers they are mostly related to.
- New Services
- NRENs and governments
- Identity federations
- Large domain- and application-specific identity management and personal information players, such as OrcID or cloud identity providers
- Big tech

Which one of these groups will first gain momentum may significantly impact the flavour and fate of SSI in academia and research.

Cost structure

Most direct costs of eduID are infrastructural in nature and long-term. Individuals' eduID identities should remain valid indefinitely and support their way through lifelong learning and research, so eduID should adapt to the evolving implementations, technical standards, uses and expectations. Therefore, the primarily involved costs are those related to the establishment and provisioning of the infrastructure and technical governance of data and solutions.

As eduID provides a universal identification and login for lifelong learning and research, the costs related to validation of an individual's identity occur only once, unless the identity has been compromised or in rare cases when a higher level of assurance is required. Those costs could be significantly reduced by piggybacking the national identity validation schemes, while the part where physical validation is still necessary should be on those who require identity creation and verification for an individual, typically an educational or research organisation and considered as a part of the standard work on the onboarding of students, employees and external collaborators.

If the technical infrastructure makes use of a distributed ledger, additional cost may occur in the form of common utility which is a measure of how much computational work is required to process transactions and smart contracts. In this way, participating ledger nodes are compensated for ensuring the correctness of transactions on the ledger.

Revenue and value streams

At this point, we think the revenue streams for such a platform would closely mimic the current revenue streams and financing models we have in federated identity, e.g., project-based, or based on membership fees. Directly charging the wallet user is not likely. Charging the Issuer upon making data available is easy, however, may not be acceptable for Issuers. As verifiers generally benefit the most from the use of the SI ecosystem, charging these would make the most sense. However, because of the privacy-preserving nature of most SSI ecosystems, it is not possible to establish the rate of consumption of transactions from Verifiers. Another possible model could be to only allow verifiers in after they have paid a “membership fee”.

In the long run, since eduID is to be used as the base of the personal digital identity of all participating universities, other educational and research organisations and participants in supporting services, it could consume a part of the related revenue collected by these organisations and services or research projects’ indirect cost. This is particularly the case if for-profit organisations become more prominent users of eduID. However, collection of that kind of revenue would require either a wider proliferation of micropayment schemes or methods of bulk payments (consideration for the operator…).

Ideally, an ID should be applicable in as many countries as possible.

At this point, no direct monetary value is likely to be generated. We foresee how several directions would result in savings for entities in this and other sectors:

- Providing a base identity for latching additional credentials to
- Cost reduction at institutions for not having to establish the user’s identity upon returning when entering the education cycle again
- Cost saving for dealing with alumni
- Cost reduction for services wanting to use academic identity as provided by eduID Wallet as they do not need to join a federation
- Cost reduction in dealing with Guest Identity
- Improved privacy for end-users
- Usability and alignment with other uses of the common wallet used for other purposes, making data exchange more efficient

Diploma and micro-credentials

In brief

One of the core activities of our industry is to educate and train people and subsequently to certify that the learner has acquired these skills through certification or diploma. A growing number of institutions encourage their students to obtain a part of that education elsewhere.

Furthermore, there is an increasing need to express these certifications in a digital way across both sector and country borders. This will improve national and international student mobility and facilitate lifelong learning, allowing Higher Education to become more flexible.

Increasingly, recognition of skills and capabilities is handed out as micro-credentials. A micro-credential is a term that is used unanimously to describe proof of the learning outcomes that a learner has acquired following a short learning experience. These learning outcomes have been assessed against transparent standards. The proof is contained in a certified document that lists the name of the Holder, the achieved learning outcomes, the assessment method, the awarding body and, where applicable, the qualifications framework level and the credits gained. Micro-credentials are owned by the learner, can be shared, are portable and may be combined into larger credentials or qualifications. They are underpinned by quality assurance following agreed standards. Micro-credentials may potentially become a bearer for European Credit Transfer and Accumulation System (ECTS) points.

With the use of SSI technology, three main use cases may be supported:

- Trusted exchange of digital diploma information between (government) accreditation agencies across Europe.
- Issuance of verifiable digital credentials (badges) by educational institutions and others for use in education and other sectors.
- Digital verification of diplomas or digital credentials.

Value proposition

The main value lies in the fact that our primary users – the learners of ECTS credits, badges and diploma credentials – can receive and present their education information remotely without sending over scanned documents or physical certificates. This is even more useful if the learning is done from a distance – in this case, the retrieval of a paper certificate (via mail or by travel) can be of secondary concern, as the signed credential may be received immediately. As these credentials are made available to Verifiers in a selective manner by users, it is possible to selectively disclose only part of your educational accreditation(s).

For secondary users are the Issuers and the Verifiers of such educational certificates. There is an important element of potential cost-saving; moreover, a DI system facilitates the remote

servicing of learners, by completing the IT suite needed for distance teaching (remote lecturing and exams via video conferencing; materials on Moodle canvas or other systems; and with DI, credentials issued remotely.

For Verifiers there is also a considerable value proposition: by the virtue of the diplomas and micro-credentials being machine-readable, machine inference can be made. For instance for a case when there are mass applications for a position or a university slot, shortlisting can be made. Job listing firms can also make valuable inferences about personnel this way. What is more, the verification of the truthfulness of the claims is much easier than in the paper way.

For all parties involved, the product may be a simple way of receiving, storing (for the long term) and presenting the certificates. This could be a wallet. Optimally, some notions of ceremony and institutional authority should be also conveyed to emphasise the issuance and use of physical diplomas, including notifications and logs and counters of insights. This could be achieved by embedding logos and other visual elements. Diplomas and other micro-credentials in a wallet are easier to access and validate and are less likely to get lost, misplaced or destroyed, provided that proper backup arrangements are made.

Key partners

The key partners are learners, educators and credentials-consuming Verifiers such as employers, organisations providing further education, or funders receiving research proposals and results. Educators need a system to issue such credentials at scale; also that system should be integrated with the student education and record-keeping system mandated by law.

Fortunately, many of these systems are often already integrated with GÉANT T&I technologies, making it easier for the GÉANT project to find a way in. The use case is also important for organisations that often need to screen or select among a large number of candidates or proposals. These actors are new prospective users of GÉANT T&I solutions, and SSI has the potential to provide these solutions without a strong commitment of credentials consumers.

There may be SMEs or individual educators in the future that will be facilitated by this technology, who are currently locked out from the world of accredited educators who have larger resources and established interfaces with the government.

Learners are a very broad group, but many of them are enrolled in some level of formal education, therefore becoming users of GÉANT-provided networks and services. However, there may be learners – for instance, users of MOOCs who want to also do an exam from a material – who use such a system sporadically, e.g., only earn a 5-ECTS course on GDPR.

NRENs are key partners as they are technology providers and trust anchors for national organisations, and liaisons between Orgs and International organisations and GÉANT itself.

Government bodies, like ministries for education, may act as trust anchors issuing statements on which institutions are accredited to issue formal diplomas.

Customer segments

The usual segmentation (by purchasing power) would be both useless and inappropriate. However, it is possible to segment the learners by engagement: On the high end of the engagement scale, there are the learners who earn several diplomas or postgraduate certificates, exploiting the ERASMUS and other mobility schemes as well as remote learning and MOOCs to the maximum effect. On the low engagement level, there are sporadic users – someone who earns a few credits or does some vocational training once or twice in their lifetime.

The segmentation of educators is possibly by size and by public/private nature: On the higher end, we have large, established institutions, universities and colleges. These may be public or private; perhaps from the perspective of GÉANT, it is worth differentiating them by whether they are members of the local NREN or not. In the middle, there are associations, companies and other organisations whose main profile is not educational, but do education and maybe even internal certifications for their HR purposes, to educate juniors etc. Now, these can be made more valuable. On the smaller end, an SSI-based certification and diploma system may enable processes of disruptive innovation, that is, provide a path to the market to very small educational businesses that would be not viable otherwise. This could be just a single person accredited by some trusted body, who delivers certificates without some large back office. Several forms of vocational education, like specialised equipment inspectors and experts on niche topics, may be taught by a handful (or even just one) to a handful of learners, especially in smaller European languages. With the help of cheap digital certificates, coupled with low-cost digital education delivery methods such a venture may just turn from unviable to viable.

We can look at the segmentation from the perspective of the verifiers or certification consumers. The biggest one in this category is the government itself, as it mandates certain educational levels to fulfil jobs maintained by the state, especially in healthcare, law enforcement and judicial systems, as well as in primary and secondary education.

Higher education organisations have an interest in digitally exchanging diplomas and micro-credentials in the context of lifelong learning. This will more easily allow students to take courses at other places and include the results in the formal diploma. Also when a learner enters an institution to take up a study, either as an international student or as a returning one, digital credentials are easier to validate, and will hence reduce costs.

Companies and SMEs may also use a digital educational credential system to fulfil their human resources requirements. Finally, individuals may also consume educational credentials in certain specific cases, like hiring an advisor, an accountant or an estate planner or while entering into any other business relationship that requires a specialist.

Early adopters

Possible early adopters include

- innovative institutions and NRENs with many mobile students
- educators on specialised topics such as technical standards, methodologies or specific trade skills, and educators providing periodic certifications as required by law
- small outfits that struggle to enter the market
- distance learning platforms
- recipients of numerous applications based on skills or achievements
- consultants applying for short-term engagements

Cost structure

Any users of such an ecosystem will have to adapt to the evolving implementations, technical standards, uses and expectations. Therefore, the primarily involved costs are those related to the establishment and provisioning of the infrastructure and technical governance of data and solutions.

The costs related to the validation of an individual's identity occur only once unless the identity has been compromised or in rare cases when a higher level of assurance is required. Those costs could be significantly reduced by piggybacking the national identity validation schemes, while the part where physical validation is still necessary should be on those who require identity creation and verification for an individual, typically an educational or research organisation and considered as a part of the standard work on the onboarding of students, employees and external collaborators.

If the technical infrastructure makes use of a distributed ledger, additional cost may occur in the form of common utility which is a measure of how much computational work is required to process transactions and smart contracts. In this way, participating ledger nodes are compensated for ensuring the correctness of transactions on the ledger.

Revenue and value streams

- Reduced the cost of creation and exchange as part of fixed costs for diploma information (costs are on students on state/institution) The issuance of a diploma or a credential has some upfront costs that may be saved by SSI by the virtue of digitalization.
- Hugely reduced costs in the verification of diploma information through leveraging trust anchors and standard metadata formats. Even within the same country, it takes at least a lookup to verify that the document is authentic. A document issued in a foreign country that is not even issued in the language of the place of verification is very costly to authenticate if even possible.
- It is unlikely that this service will ever be billed separately to the learner. Much more likely is a situation where the cost will be part of the general overhead. However, using such a system may present significant cost-saving if physical credentials are partially or fully replaced, or even if there is a physical certificate but the delivery is not expedited and insured.

Researcher identification and authorisation

In brief

Collaboration across organisational boundaries is an important aspect of research activities. Trust establishment lays the foundation for researchers involved to work together and share resources without the need for lengthy identity proofing. Besides sharing identity information across collaboration partners, it is often important to verify the role of a given person. In many cases, it is important to know whether a person is affiliated with a research institution and what their position is. This was first enabled through the eduGAIN service, but only within academia.

An alternative approach would be to use SSI-based researcher identification to enable researcher access. The benefit of this mechanism compared to FIM is that it could include researchers without a home organisation in academia or a national identity federation. This could be enabled by accepting additional authorities sources like governments or banks, which also provide verified identities. Due to the distributed credentials, a few of them could be combined into one identity. This could be even more secure and allows researchers to continue to use their identity even after changing their home organisation.

It is to be expected that this use case provides similar risks and opportunities as the eduID and diploma use cases. SSI-based researcher access should be enabled by using existing concepts and mechanisms to increase the acceptance and adaptability of the approach. The SSI approach should be able to mimic trust establishment between identity and service providers in order to be included in the current ecosystem.

Value proposition

The researcher ID scenario shares most benefits with the eduID use case, but there are some specifics to this use case:

- The ability for researcher 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 the means (instrumentation, resources, tools, reporting, etc.) used in research projects, which are temporary endeavours and have their governance mechanisms.
- Ability to directly establish trust relations between participating entities in scientific collaboration.

Regardless of the benefits for a single institution, the decentralised identity approach might be the future of identity management. Therefore, R&E organisations need to support this upcoming technology to be in the position to achieve a seamless transition in case IDM moves in this

direction. A critical success factor will be interoperability with the existing FIM infrastructure, which requires research collaborations to rethink their current approach.

Key partners

The key partners for an SSI researcher ID are the same as the ones currently involved in FIM: researchers (end-user), NRENs (infrastructure providers), institutions (issuers), research service providers and GÉANT (facilitator or infrastructure provider).

These are key features for different stakeholders:

- GÉANT
    - Serve the needs of its constituents by ensuring that standards developed stay within our scope, use cases and practices (thus keeping to deliver value and stay relevant)
    - Development and operational cost-sharing broker for technical systems that interact with the SSI ecosystem
    - Protect the established infrastructure and work (such as eduGAIN) and ensure interoperability
    - Innovation and development coordinator/hub for new SSI solutions (TFs etc.)
    - Knowledge concentrator and disseminator
    - Being a bridge between other cross-national initiatives, EU projects, and the EU regulation targeting RI, identity management and privacy
- NRENs
    - No need for a central infrastructure
    - Trusted issuer registry and trusted scheme registry
    - Adapting to new technologies efficiently and effectively
- Institutions
    - Not more complicated than a hub and spoke federation
    - Data protection – it is easier to protect the data if you don’t store it in the first place!
    - Allow institutions to change backend AAI to a platform of their liking without breaking (international) interoperability
- End-users
    - No need to trust one single IdP
    - Not dependent on the infrastructure of the claims provider
    - Streamlining the access to all the identity-related elements the end-user has to interact with (currently there are identities, credentials, accounts, identity and OAuth providers, federations, attribute providers, etc.)
    - It is no longer possible to prove your identity/attributes again to different verifiers because it is possible to combine attributes from multiple issuers

Customer segments

- Researchers in our current FIM ecosystem

    - eduGAIN users
    - eduTEAMS users
    - Research collaborations
- Researchers without access to the existing ecosystem
    - Commercial companies
    - Users who are not part of a federation, like citizen scientists
- Research infrastructures such as GAIA-X, EOSC, ELIXIR, CLARIN, DARIAH-EU, LSC, umbrellaID, XSEDE or LUMI and their collaborative or interoperability networks such as WISE and FIM4R.
- Institutions

Early adopters

Research infrastructures

- Need for better quality identity
- Easier way to aggregate identity and entitlements for end-users for authentication
- Easier establishment of trust relations.
- They are in a position to enforce authentication methods on their users as they provide resources and control access to them.

End-users with special requirements

- Researchers in commercial companies who currently have no or limited access to R&E services.
- Researchers from countries without a national identity federation
- Researchers with multiple affiliations and research collaborations

Organisations with limited resources or not focused on identity-related services

- NRENs with few resources benefit from not having to operate their infrastructure for an identity federation.
- Organisations that lack the technical knowledge or resources to operate an IdP or join an identity federation
- Research institutions who want to reduce the data privacy security risk

Cost structure

We assume the cost structure of research-related SSI infrastructures would be very similar to current platforms. It is assumed these will be EU, state or project funded. Cost may be reduced if parts of the SSI ecosystem are provided generically, like e.g. on a national or pan-EU level.

Revenue and value streams

At this point, we think the revenue streams for such a platform would closely mimic the current revenue streams we have in research AAI, e.g. project-based, based on membership fees, or for a fixed part of the funding of the projects for identity-related services.
At this point, no direct monetary value is likely to be generated. We foresee several directions which would result in saving of costs for the entities in this and other sectors:

- Providing a base identity for latching additional credentials to

- Cost reduction at research collaborations and services for not having to establish a users identity when entering the collaborations or upon later return
- Cost reduction in dealing with Guest Identity
- Ability to use a base identity without the need for the institution to provide all parts of this identity.
- Cost reduction for services wanting to use academic identity as provided by eduID Wallet as they do not need to join a federation

GÉANT opportunities and advantages

It is believed GÉANT has a number of distinct properties that make it well suited to engage with SSI and help guide our community toward the uptake of this technology:

- Act on behalf of an aggregate of NRENs and institutions
- Access to educators through the NRENs
- GÉANT's existing services and brands (edu*)
- GÉANT's international profile positions it in the best place to facilitate remote learning and transition to SSI
- Access to money/funding
- Existing governance structures for pan EU and global collaboration between the NRENs
- Thorough understanding of the use cases and sometimes even the business cases
- Having actual users that have problems when dealing with (federated) identity
- Ability and need to ensure autonomy and independence as a sector, e.g., from big tech
- Willingness to prevent large entities from collecting data from our users
- Strong focus on ensuring interoperability and delivering multi-stakeholder solutions which prevent vendor lock-in
- Broad experience in building distributed ecosystems such as eduroam and eduGAIN, both technically as well as the accompanying governance structures
- Experience with AAI in our ecosystem: existing knowledge, tooling and best practices that may be reused
- Vested interest in making sure existing, well established federated infrastructure can be leveraged most efficiently in synergy with novel SSI ecosystems
- Have the power to bring together institutions and services in the field of trust and identity
- Already need to aggregate identity information from different 'sources'
- Offering solutions to existing customers, who might benefit from such service
- Facilitate proper integration into the existing ecosystem, may also help more easy migration
- May actively support the migration and integration of existing services

It is expected the developments around the new eIDAS regulation and technical framework (EDIF) will have a significant impact on the availability of SSI-based ecosystems in Europe. Because of this, GÉANT could:

- Closely monitor eIDAS 2.0 and EDIF-related developments to prevent potential problems with the future funding of GÉANT
- EDIF Toolbox process WG – important for GÉANT in determining its technological direction and SSI-related steps
- Influence and contribute to the development of the common technical architecture, standards and specifications, guidelines and best practices (based on solutions established based on the selected Toolbox), particularly in the parts relevant to the academic and research community

- Participate in the establishment of technical certification requirements and the establishment or operation of certification bodies
- Provide the management of internationally trustworthy trust lists of entities (such as trusted/qualified sources and relying parties), for the use with both the EDIF and other digital wallets used in academic (e.g., non-EU) scenarios
- Oversee or operate EDIF Qualified Trust Services (QTS), central registries for academic purposes
- Support designated intermediaries (such as NRENs) in verifying sources or attributes
- Propose or establish catalogues of attributes and schemes for the attestation of attributes in the R&E domain

As is clear from the previous sections in this document, SSI may bring opportunities and benefits; however, a new credential ecosystem will not be created overnight. As such, GÉANT should take care to:

- Engage with institutions, by way of the NRENs, making sure that any proposed system is capable of being integrated with whatever already-established infrastructure they use
- Engage, in close collaboration with NRENs and institutions, with key stakeholders like Learners and Researchers to understand and describe the use cases, situations and circumstances where they receive and present their credentials; discuss and enable Verifiers to use micro-credentials created by educators and provided by learners
- Contribute to standardisation and harmonisation on a pan-European and global level, including participation in the development of standards while working with its with communities and interest groups
- Identify issues and topics to be tackled by EU and national regulations that enable and facilitate SSI and its use in the research infrastructure and SSI to gain cross-sectorial acceptance (from academic, governmental, and private sectors) and interoperability.
- Support and collaborate within GÉANT and with NRENs to investigate, create, research and evaluate solutions that allow entities in our community to act as DLT providers, verifiers of Verifiers, or providers of registries
- Create a system that helps bridge between SSI platforms, such as a translator proxy
- Coordinate with other cross-national initiatives, EU projects, and the EU regulation targeting RI, identity management and privacy (through TFs and other fora)
- Coordinate innovation and development of new SSI solutions (via TFs, both internal and via projects with partners…) to ensure the academic use cases and needs are represented in such developments

Work areas for NRENs

- Coordinate or participate in the development of national SSI-related initiatives and regulation
- Define, govern and operate trust and certification schemes at the national level

- Promotion and facilitation of adoption of SSI solutions and standards within their communities
- Establish national reference registries of sources or sources of Verifiable Credentials
- Provide gateways or proxies for legacy federated systems
- Support the establishment of institutional SSI solutions within member institutions
- Participate in the establishment and operation of SSI registries or verification mechanisms for credential sources, identities and services that support trust and claims or provide proofs
- Contribute to the development of technical specifications, schemes and establishment of metadata, ledger, crypto, etc. mechanisms
- Contribute to the development and establishment of underlying technical services at national or international levels
- Promote SSI concepts, benefits and solutions to their end-users gradually shifting them together with the provided services to the SSI ecosystem.
- Prepare and localize explanatory materials, tutorials and guidelines for Learners, Researchers and Verifiers covering SSI and typical use cases; these materials could be based on their shared generic versions prepared with the help of GÉANT

Work areas for institutions

- Adaptation of existing institutional identity, credentials and attributes management systems to support new SSI-bound services and interfaces and meet the new formal requirements and expectations of data consumers
- Establishment of internal data and credentials management mechanisms that rely on SSI and minimise collection, preservation and proliferation of personal data, in particular within the identity and credential management systems
- Selection, acquisition and implementation of SSI-bound solutions that are suitable for the institution’s size, capabilities and requirements of their operations and sharing
- Promote SSI concepts, benefits and solutions to their end-users gradually shifting them together with the provided services to the SSI ecosystem

Conclusion

The concept of Self-Sovereign Identity is relatively novel. Nevertheless, it has been embraced with great enthusiasm. This is seen both on the technical side, where the possibility of building a trusted infrastructure based on distributed ledgers has attracted much attention.
Also, policymakers are very interested in the concept, as it is seen as an enabler for a more user-centric and privacy-preserving way of managing identity. At the same time, it could enable and facilitate the exchange of personal data for the benefit of digital transactions in many sectors.

Contrary to other sectors, for research and education, the SSI concept does not herald a brave new world. Due to years of diligent international collaboration, R&E already has a well-established, highly standardised and globally interoperable identity ecosystem in the form of Federated Identity management. Also, the use of blockchain-based technology is viewed with a fair degree of scepticism as it seems very few use cases mandate the use of a blockchain, while it introduces a whole new collection of challenges, both technical, in user experience and from a legal perspective.

That said, the FIM ecosystem does have some challenges and shortcomings in which an SSI-based solution may be supported or even be preferential over the existing solution.

In this study, we have identified three high-level use case scenarios for which SSI-based technology seems to offer significant benefits. We came to the selection based on interviews with various stakeholders in education, research, NRENs and other sectors. Using a business canvas we have tried to analyse these use cases and describe potential value and revenue. Allocating a direct monetary value turned out to be hard typically, we note most use cases may yield – sometimes significant – cost savings.

The cases identified are:

- SSI-based eduID is a natural evolution of the existing eduID effort being worked on by various NRENs. It is the underpinning concept that allows users to have a long-term persistent identity under their control, for their interactions with research and education. Typically, the core of this identity is provided by the institutions the user is attending or working for. By creating eduID as a base layer, taking care of fundamental properties like trust establishment, revocation, interoperability with multiple SSI ecosystems, privacy and policy harmonisation, it may become the trusted building block for the above and other use cases.
- Diploma and micro-credentials, where SSI may be used for long-term storage and easy exchange of diplomas and other accreditations, especially in other sectors. Creating an SSI-based system also brings an opportunity to standardise and harmonise the exchange of this type of information between government agencies, institutions and future employers and job agencies.

- Researcher ID, where an SSI-based system may complement the existing AARC BPA-based infrastructures with a capability to more easily aggregate data from various authoritative sources, while at the same time reducing the need for centralised proxy infrastructures. Also, the opportunity to potentially make use of external identities with a sufficient level of assurance, as could be available in the user's wallet, may be very helpful in allowing for better interaction between research communities and other sectors.

Additional reading

- T&I Incubator slides about SSI: Self Sovereign Identity Use Cases
- T&I Incubator report on Distributed Identity: https://wiki.geant.org/display/gn43wp5/DI4R+Report
- A Brief Guideline on Self-Sovereign Identities (SSI) with special regard to the distributed ledger technology (DLT) – https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/guideline_self-sovereign_identities.html, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/guideline_self-sovereign_identities.pdf?__blob=publicationFile&v=2
- Annett Laube, Gerhard Hassenstein, Self-Sovereign Identities: Will the identities of Swiss university members be controlled by themselves in future?, 12 November 2020 – https://www.switch.ch/about/innovation/overview/switch-innovation-lab-self-sovereign-identities/, https://www.switch.ch/export/sites/default/about/innovation/.galleries/files/SWITCHInnovationLab_IDAS.pdf
- Christopher Allen, The Path to Self-Sovereign Identity, 2016 – http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html
- European Union Agency for Cybersecurity (ENISA), Digital Identity: Leveraging the SSI Concept to Build Trust, January 20, 2022 – https://www.enisa.europa.eu/publications/digital-identity-leveraging-the-ssi-concept-to-build-trust, https://www.enisa.europa.eu/publications/digital-identity-leveraging-the-ssi-concept-to-build-trust/@@download/fullReport
- Marcos Allende López, Self-Sovereign Identity – The Future of Identity: Self-Sovereignty, Digital Wallets, and Blockchain – https://publications.iadb.org/publications/english/document/Self-Sovereign-Identity-The-Future-of-Identity-Self-Sovereignty-Digital-Wallets-and-Blockchain.pdf
- Pöhn D, Grabatin M, Hommel W. eID and Self-Sovereign Identity Usage: An Overview. Electronics. 2021, 10(22):2811 – https://doi.org/10.3390/electronics10222811, https://www.researchgate.net/publication/356260280_eID_and_Self-Sovereign_Identity_Usage_An_Overview, https://mdpi-res.com/d_attachment/electronics/electronics-10-02811/article_deploy/electronics-10-02811-v2.pdf
- Swiss Federal Department of Justice and Police FDJP, Federal Office of Justice FOJ, Discussion paper on the target vision for an e-ID – https://www.bj.admin.ch/bj/de/home/staat/gesetzgebung/staatliche-e-id/zielbild-e-id.html, https://www.bj.admin.ch/dam/bj/en/data/staat/gesetzgebung/staatliche-e-id/diskussionspapier-zielbild-e-id.pdf.download.pdf/diskussionspapier-zielbild-e-id.pdf, https://www.bj.admin.ch/dam/bj/de/data/staat/gesetzgebung/staatliche-e-id/diskussionspapier-zielbild-e-id.pdf.download.pdf/diskussionspapier-zielbild-e-id-d.pdf

- W3C, Decentralized Identifiers (DIDs) v1.0 – Core architecture, data model, and representations – https://www.w3.org/TR/did-core/
- W3C, Verifiable Credentials Data Model v1.1 – Expressing verifiable information on the Web – https://www.w3.org/TR/vc-data-model/

Annex: Implementation-related observations from eID and SSI projects

The following theses were extracted from the synthetic overview of the field provided by Pöhn D, Grabatin M, Hommel W in “eID and Self-Sovereign Identity Usage: An Overview” (Electronics. 2021, 10(22):2811 – https://doi.org/10.3390/electronics10222811, https://www.researchgate.net/publication/356260280_eID_and_Self-Sovereign_Identity_Usage_An_Overview). Some of the below theses are the result of additional interpretation and projection, and should not be taken as a literal interpretation of the original report. However, we hope that they may be useful in the design and implementation of future SSI-related endeavours.

- Resources, strategies and legislation must keep up with the evolving technology. To allow a wider application of SSI, the existing legislation needs to be adapted. Laws and governance structures must be changed, but also layered, as lawmakers are unlikely to keep up with the needs and challenges of the evolving technology. To exploit the full potential of the solutions, the regulation must apply to the widest area of application possible.
- On the other hand, the technical architecture should be as neutral and modular as possible, decoupling concerns, responsibilities and pieces of data. The parts of solutions should be loosely bound and replaceable.
- The new SSI ecosystem should integrate various SSI elements and solutions, digital wallets, existing and new eIDs (such as eIDAS) and other platforms and technologies with significant political, public or technological weights.
- All legal requirements must be met and appropriate technical solutions established and validated before legacy solutions are replaced with new ones.
- The SSI ecosystem has a specific market structure with network effects (more useful if used by many) and complex trust relationships (e.g., based on different relationships of a person).
- SSI changes the distribution of responsibilities and blurs clear organisational boundaries that exist within identity federations and toward IDPs and SPs.
- In identity federations, trust between the entities is provided with LoAs and contracts. The corresponding concepts needed to be established with SSI.
- Trust and LoAs should be addressed in several ways. They include a Web of Trust, a hybrid approach integrating certificate authorities and contracts with some Issuers and Holders, voluntary consortia adhering to the same conventions or policies, and distributed catalogues and registries in which curators appraise the content.
- IdPs lose the abilities and risks associated with being notified about what users are using which connected services, as they are no anymore involved in verification.
- Proxies, public directories and registries may help despite their collision with the SSI principles. Proxies enable legacy systems to be used during the transition while centralised or aggregating schemes are still used. They may be essential in bridging access to the existing IdPs and SPs with SSI. They should provide a balanced approach

to privacy, bring in more users and services, and should be phased out upon a transition (when users are ready to move on to newer solutions).

- Privacy-preserving decentralised derivatives of eID for use with SSI can be of great help. With them, the intermediate parties should be prevented from indiscriminately accessing users' attributes.
- Registries should be distributed, scalable and contain only the necessary data; their use in support of transactionality or trust should be formally and procedurally regulated.
- For a solution to become successful and grow further, it needs to attract a large number of users. In other words, nothing succeeds like success.
- Current user needs and aspirations must be taken into account, as well as the usability, simplicity and features of new solutions. They must bring equal or better benefits for users. Usability and functionality attract users. With easy integration of existing IdPs and SPs (by using proxies and other solutions), more services will be available, and therefore, a higher benefit for the users will be provided.
- Competition and market can help, but the establishment of the ecosystem is boosted by collaboration, harmonisation and standardisation. Documents, specifications and APIs should be publicly available.
- Open-source software and information availibilty help others to join and contribute. The overall environment should supports exchange among projects and stakeholders.
- Opening up to the private sector speeds up adoption. Also, consider if the private players may take the lead and when.
- Transparency is not only important for the follow-up projects, but also trust of end-users. This even applies to transparency about the current status of the projects, the next steps, and what went wrong and why.
- The key success factors are (actual or perceived) low complexity, ease of use, functionality, awareness, trust, privacy, security, control, empowerment and transparency. If they are present, they will provide an initial impulse and propel further the SSI.
- The growing popularity of OIDC in comparison to SAML emphasises the factors that facilitate technology adoption. These are ease of implementation, versatility and suitability for various platforms, lightweightness, developer- and user-friendliness, APIs based on prominent and favoured approaches, accessibility, and championing by large players who are relying on an already existing user base to provide access without a significant effort on their part. These factors can prevail even if the alternative is mature, feature-rich, covers a wide range of requirements and has a significant user base.
- Stable funding for the core work and services helps in attracting more services.
- Solutions and services should start free of charge to establish a large and growing list of partners and connected services. Free integration and support, bonuses and other incentives may also help. The free-of-charge model should be also applied in providing and accessing help, at least during the initial adoption.
- Killer applications and use cases are strong drivers for adoption. A few unforeseen public and private services can provide great benefits for the users or at least drive adoption.

- Ideally, there should be one wallet and a minimal number of eIDs and necessary applications to start with. Too many upfront choices decelerate uptake.
- Interoperability across all communities must be established - there should not be any isolated islands.
- Harmonisation of data schemes is an enabler for interoperability.
- Several forms of identification and authentication must be available. LoA should depend on authentication methods. Different authentication methods are appropriate different for users and applications.
- High-LoA authentication may dispel users. Do not insist on high LoA standards from the onset. This can be alleviated with step-up authentication. Linking higher LoA levels to smartphone hardware makes them easier to use.
- Citizens may have concerns regarding biometrics. This may be relieved by relying on the existing eIDs.
- The use of smartcards must be minimised, except for bootstrapping.
- Security must be layered. Users and staff need to be educated about secure behaviours and typical pitfalls and traps.
- Security incidents (identity theft, data leaks and other identity-related incidents) and attacks on the infrastructure (DDoS,...) may ruin public trust and impede adoption.
- The self-sovereign identity is primarily bound to the users' devices, which requires robust procedures to handle the loss or theft of devices.
- Backup solutions must exist for citizens without smartphones, empty batteries, forgotten phones and offline usage. QR and signature codes, helpdesks and offline apps may help.
- A robust system for regaining control over the technical components and lost or destroyed verifiable credentials or trust needs to be established. The simplest approach is to revoke the existing credential and start over with a new one, but it should be additionally optimised.
- The end user's right to be forgotten should be embedded into the design.
- There are privacy concerns in scenarios where several pieces of information are combined, as they may lead to successful identification.

Annex: Toward a research-friendly SSI

AARC-SSI workshops, feedback from outreach, expressed concerns, internal discussion
Something that would work with the existing services and capitalise on the benefits of existing solutions and specifications.

Gradual transition to SSI

In this annex we showcase how a gradual translation to SSI may be implemented, in this case taking a research community use case as an example.

In an ideal, perhaps ‘purist’ situation, in which all parties use SSI technology, there are only issuers and verifiers. No intermediate parties are needed to transfer personal data of the researcher to the services.

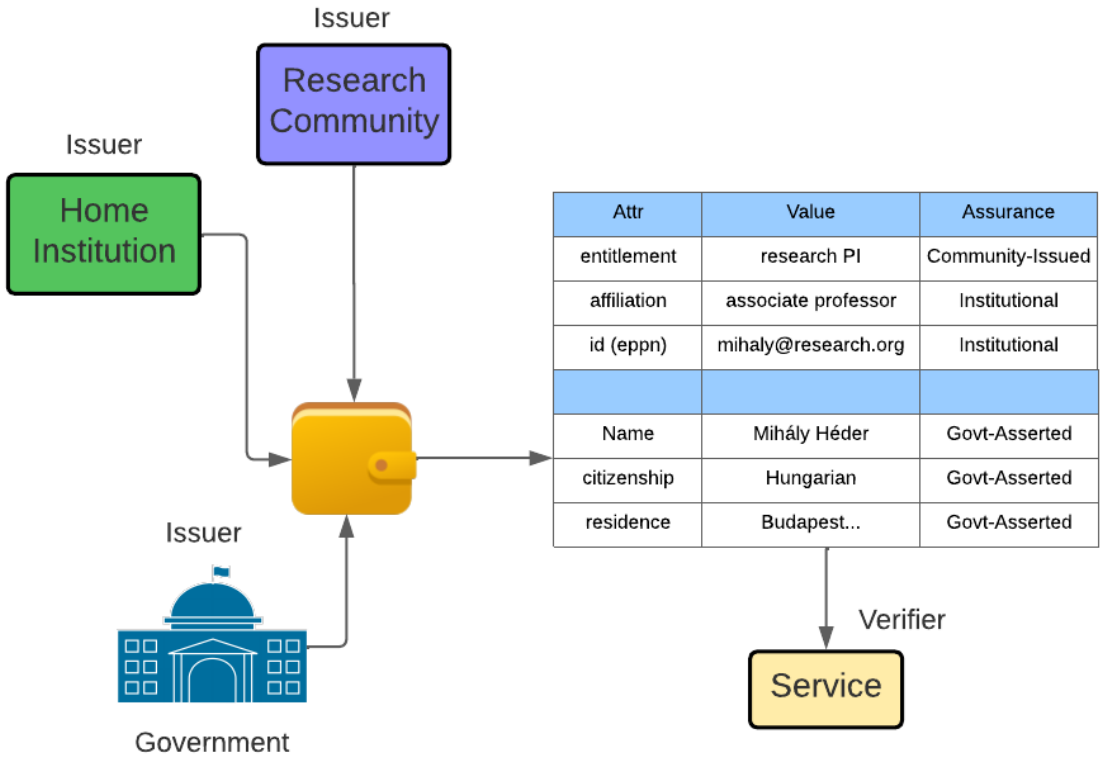


Figure 1: The ideal case SSI-based access to a research service.

In Figure 1, the user has a wallet with several claims, each issued by a relevant authority. For identity proofing the government is the ultimate source, the home institution provides affiliation and other basic academic information, while the research community issues entitlements in the context of a research project.

However, this purist design cannot be achieved quickly as this mandates all parties to have a working implementation, and, in addition, the services will have to incorporate a lot of business logic for authentication and authorization.

At the time of writing, federated AAI, based on national federations and eduGAIN support the exchange of attributes and authentication. In addition, various proxies are currently being used to facilitate access and harmonise the integration and business logic for authentication and authorization for the services. In addition, the research communities use proxy-based setup in accordance with the AARC Blueprint Architecture to !!!

How to get there? continuity of access/use, transition, evolving roles…

Using a proxy

Given that governments are already working on state-issued eIDs, there is a possibility that the Research and Education field can re-use some of the solutions. In case government-issued eID would be available as a wallet, the following scheme could work.

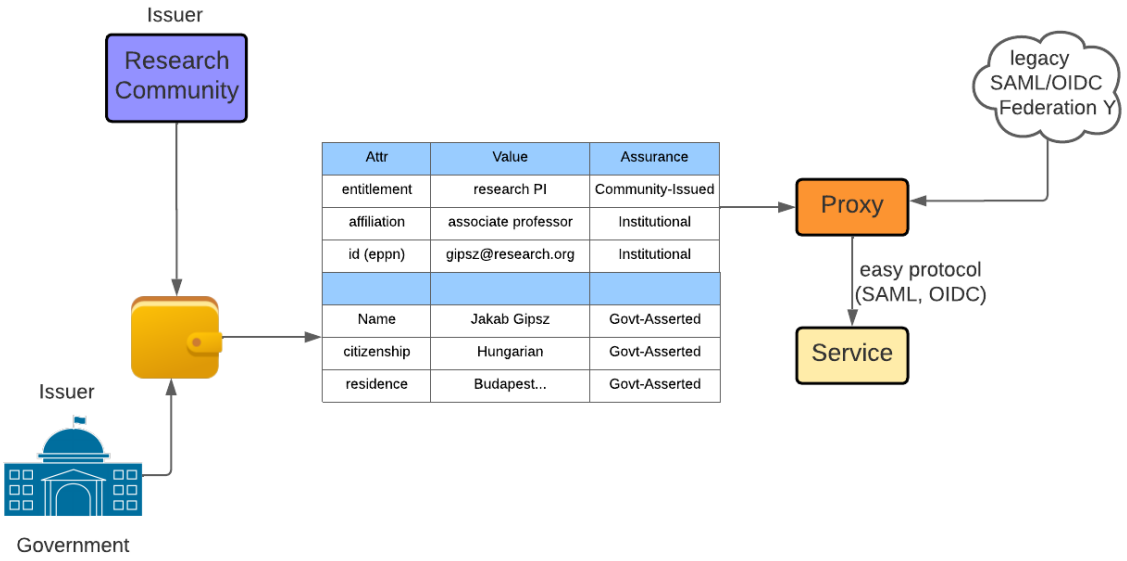


Figure 2: Combining government-issued identity with research community data and presenting them to legacy services.

In this case, we introduce a proxy, acting on behalf of the research community services, in order to simplify the integration for the SP. This setup mimics the current deployments as we see in the AARC Blueprint Architecture. The proxy could act as a verifier for all this information.

By using a proxy, the complexities of integrating the wallet-based technology may remain hidden for services while access to existing services will be ensured regardless of the switch to the SSI.

The user has credentials in their wallet about their identity from the government, while the research community placed into the wallet the claims about the researcher credentials and permissions.
--
3
Services with SSI interface cab use information form the wallet without relying on the proxy on the SP side

This could, eventually, result in removing the proxy altogether. However …on the Community side

Figure 3 details how a research community may use a membership management service, a sponsorship scheme and other sources to write the wallet with the help of a proxy that acts as a consumer of claims, federated identity and local policy, and an issuer of an aggregated claim, “research bundle”.
The user receives the composite VC bundle. Research Collaboration writes issued by the trusted Issuer/Proxy and incorporates it into their wallet after a federated login. This allows a complex and even semi-manual validation of various presented credentials from the valet and other data from the IdP and VO. Subsequently, the service can consume the product without requiring the repetition of federated login. While the initial proxy and federated login-based integration (1) may still be required for services that are not able yet to act as SSI Verifiers (3). In order for the transition to SSI to happen, the users’ wallet should obtain the produced bundle (2), which may need to be periodically refreshed from the Proxy/Issuer. After most services and users have migrated to the SSI, the Proxy functionality could be abolished.

RC issuing credentials into the wallet.
Still, the RC community authorised representative or another approving arbiter who approves has a role (issuing and updating credentials, access token).

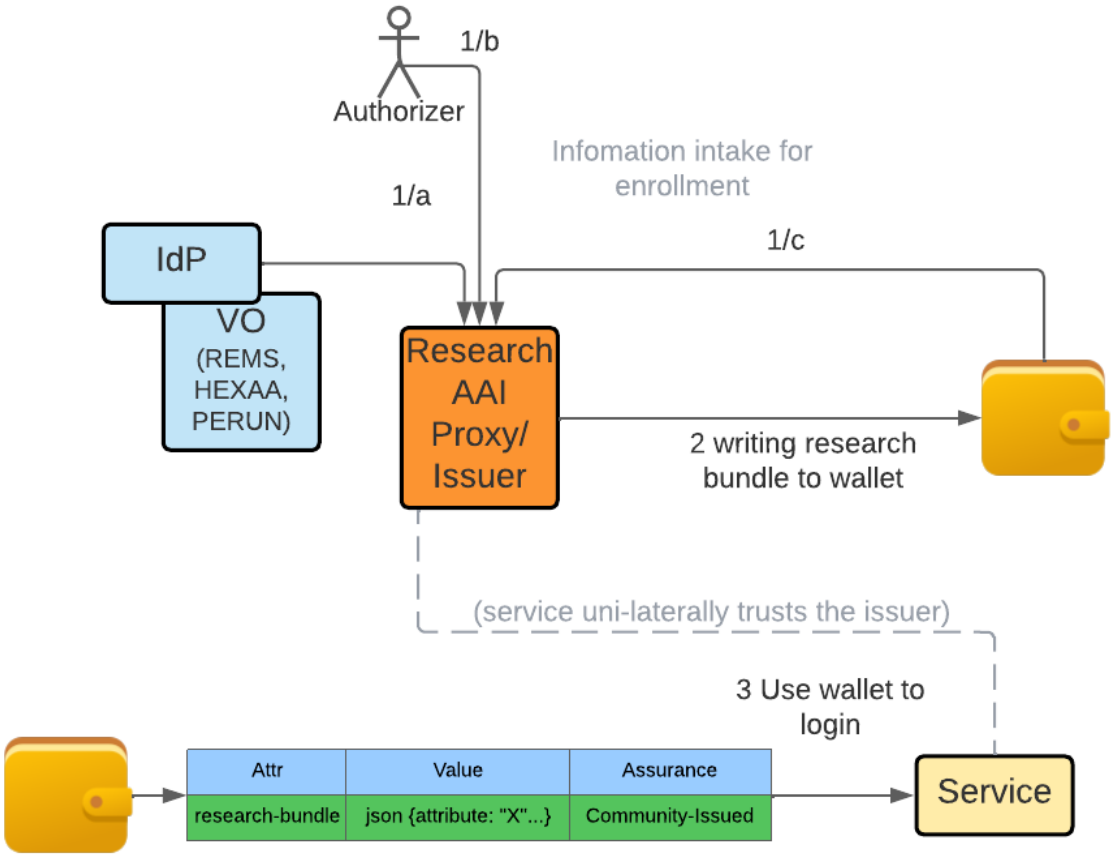


Figure 3: The Proxy/Issuer allows the community representative to control user access to the service, even if the credentials from the Wallet are used to access it.

Replacing the proxy altogether

As illustrated in the previous figures, a proxy can adapt the content of an SSI wallet for the use by legacy services that have only a SAML or OIDC interface, consolidate or uniform the available information coming from various sources, or provide an additional value by implementing and performing possibly complex validation and assertion of user characteristics or entitlements the information received from the user and other sources. How this is delivered may change in time, so the entity that initially acts as a SAML/OIDC proxy may later become an additional SSI Issuer in order to streamline validation or decide upon the information provided by other issuers and external services. However, any additional functionality should be made available regardless of the technology that is used by the involved parties at any given point in time, thus decoupling the technical implementation, sources of information, any additional data mapping or decision-making rules or roles.

The path from one setting to another should be natural and gradual while leading toward full SSI adoption. It should be functional at any point in time, without any excess components as unused leftovers from the past or scaffolds and placeholders for the future. One possible path for this transition consists of a sequence of implementation by progresively accomplishing three scenarios:

1. The **proxy** mediates between the wallet and the traditional SAML/OIDC service.
    - The presence of this data in the wallet ensures that the SSI-enabled service can get it **directly** upon the Holder's approval.
2. The **mediating service (Community Proxy)** produces an **asserted bundle** of research- or education-related data that can be added to the wallet as a VC. The VO or research community can be consulted in the process; this **consultation** may be automated and immediate, or human-guided and postponed, in which case the access to the VC and end service also has to be postponed.
    - For the SAML/OIDC service, the access token can be provided through the mediator's proxy interface upon successfully completed assertion or consultation.
3. The mediating service produces a time-constrained **access token** which the end service uses to grant access to the user (without having to get any user details), whereas it may also **ask the mediator** to broker the related user data it is allowed to see them. This process can also include **consultation**. The token and optional data are **added to the wallet** in order to be used with an SSI-enabled service. The holder decides whether they want to present the asserted bundle.

Figures!!!

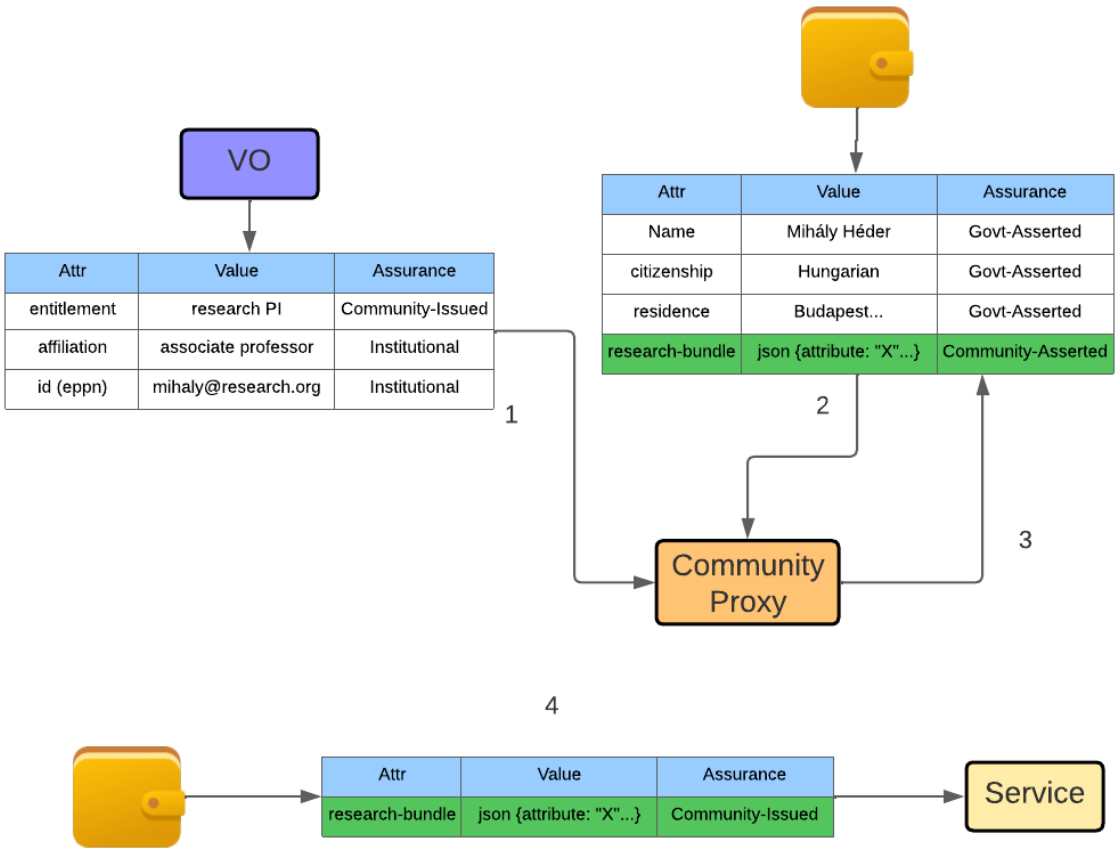


Figure 4: Community Proxy keeps the Wallet updated by maintaining a research bundle, while the Wallet also contains other claims.

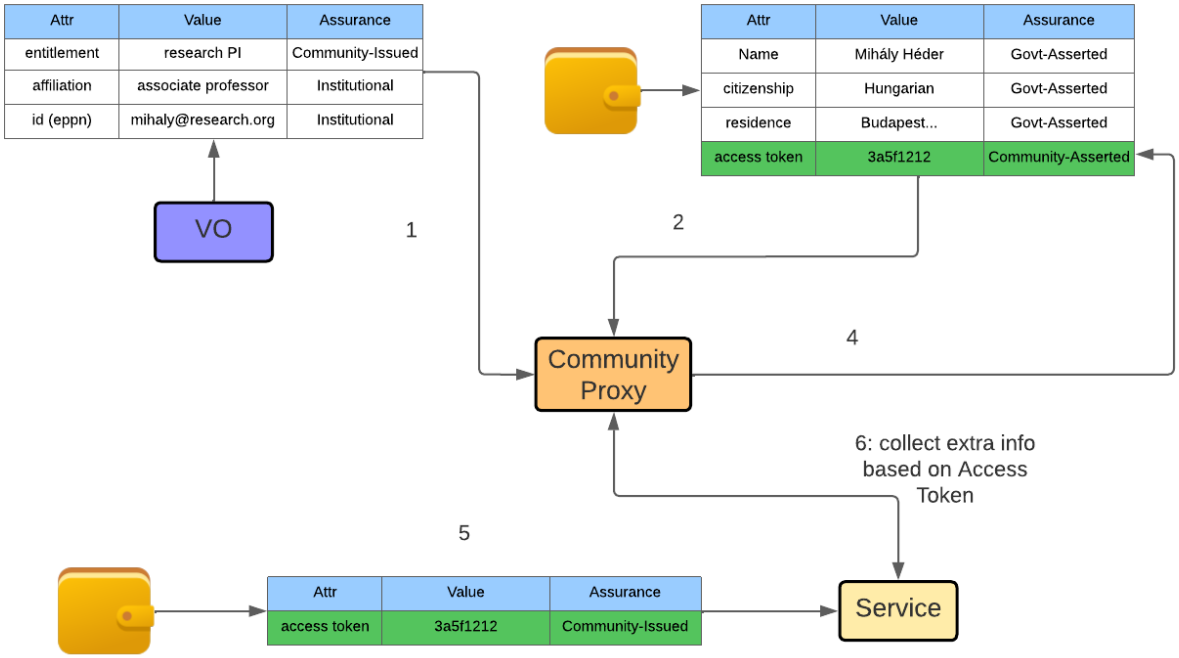


Figure 5: Proxy provides just an access token to the Wallet. The service collects attributes based on this token, requiring a direct channel between the service and the community Proxy.

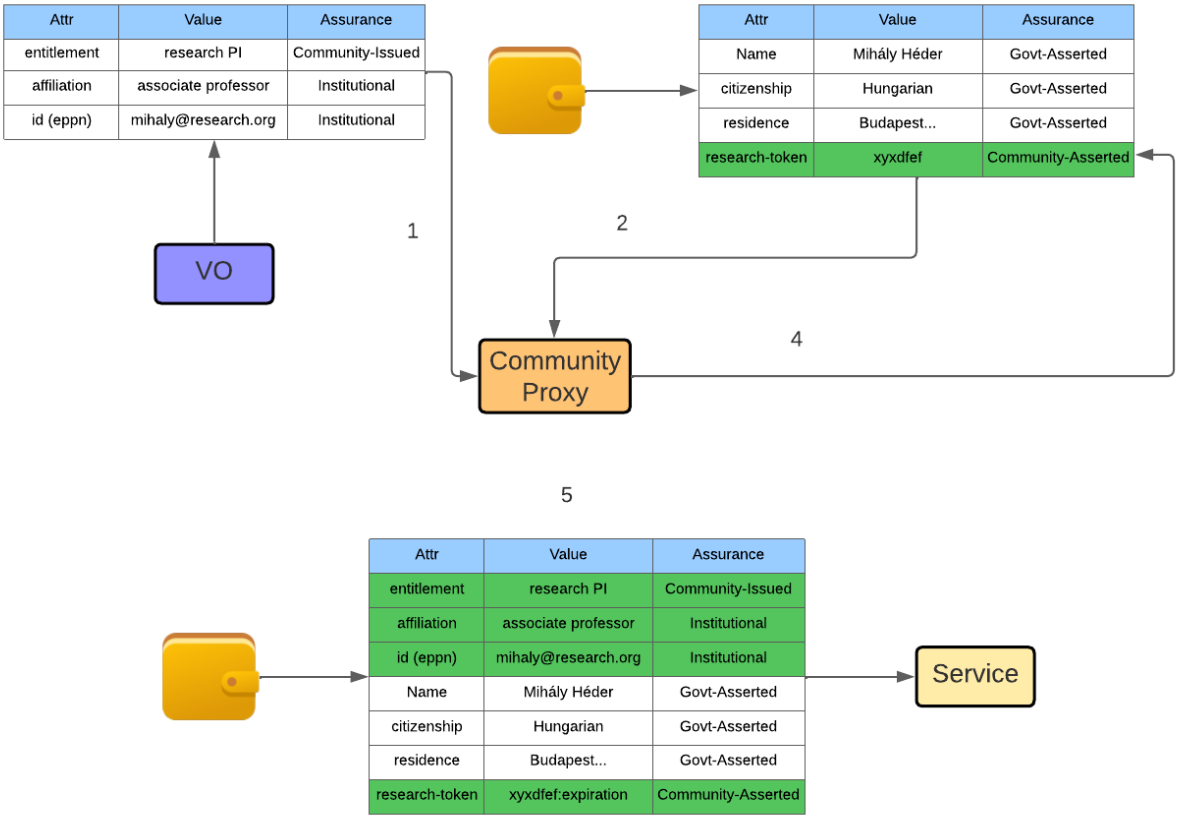


Figure 6: (I think this is redundant as it is just a variation of B) Community Proxy writes token to the Wallet, the relevant set of attributes can be also used.

No extra information from the token