Self-Sovereign Identities

Will the identities of Swiss university members be controlled by themselves in future?

Annett Laube, Gerhard Hassenstein
Version 1.0 - 12/11/2020

Bern University of Applied Sciences
Department of Engineering and Information Technology
Institute for Data Applications and Security (IDAS)

1 Management Summary

There are serious concerns about any kind of centralized Identity Providers (IdPs) as used in many areas of our daily life (e.g. in social logins). In the digital age our personal information is stored on computer systems. Databases store millions of records that are hosted on servers or in data centers which often belong to private companies. This probably sensitive information is stored centrally and is thus often at risk from data theft by hackers.
At this point, it must be taken into account that these dangers usually come from public institutions, e.g. in the private sector. An identity used in a "specific sector" (e.g. the academic landscape) only, is much less exposed. Additionally, SWITCH is controlled by a community built by Swiss universities, which mitigates any misuse of the issued Identities (e.g. the SWITCH edu-ID) significantly.
But it is still worthwhile to deal with new technologies (i.e. Self-Issued Identities) and include them in future planning.
"Self-Issued Identities" mitigate these risks by design, because individuals have their personal information stored locally in an ID-wallet and not with a central Identity Provider. This increases and preserves the users' control and privacy by preventing any centralized instances or third parties from having the ability to track which web applications a user is interacting with (to create user profiles).

More and more users bring along an identity which they want to use in a specific context. This is partly due to the fact that a user already has a nearly unmanageable number of identities/credentials and wants to reuse them. Bring your own Identity (BYOID) is the keyword. SWITCH should face this challenge and be prepared for future changes.

A "decentralized identity" approach requires rethinking. Identities are no longer issued and maintained by an Identity Provider but may be created anywhere. Only claims (credentials) must be confirmed by an authoritative source (Issuer) and be bound to the identity to avoid misuse. The owner of the identity (Holder) may then present this information in a trustworthy manner to a service (Verifier) to gain access to it.

Identities will be asserted by the homeland government in form of verified credentials (VC) attestation. SWITCH can also act as Issuer of Identities and claims provided by Universities. Home organizations and other RP will act as verifiers in this case. To allow a smooth migration to this new world, a strategy of integrating SSI solutions into the existing infrastructures and governance rules from the beginning will be needed.

A key factor of the success of self-sovereign identity (SSI) solutions will be interoperability with the existing IAM infrastructure. Approaches to integrate SSI with authentication protocols, such as OIDC and SAML, are in development. But interoperability can come at the cost of SSI benefits.

Many activities around SSI are ongoing in Europe and other countries. Some of them are already testing prototypical solutions to replace passports and driving licence with digital credentials. It is important to follow these activities and to transfer the experience gained from these projects to the Swiss university landscape. Solutions based on the SSI principles could give users the possibility to exercise better control over the use of their own data and to better protect their privacy.

This report is presented by BFH on behalf of SWITCH.

Contents

1	Management Summary	2
2	Introduction	4
3	Content of the study	4
4	Situation at the Outset	4
5	Self-Sovereign Identities Basics	5
	5.1 Principles of SSI	5
	5.2 SSI Building Blocks	6
	5.3 SSI Architecture	9
	5.4 Trust Relationships	11
6	Use Cases	13
7	Processes using SSI	13
	7.1 “Creation” of an Identity	13
	7.2 “Collecting” Claims	14
	7.3 “Presenting” Claims	15
8	Roles	17
	8.1 The “traditional” role of SWITCH	17
	8.2 The “new” roles of SWITCH	19
	8.3 Home Organization (University)	20
	8.4 Government (and other authoritative sources)	20
9	Risks, Benefits, Challenges…	20
	9.1 Advantages	21
	9.2 Challenges	21
	9.3 Open Issues (not conclusive)	21
10	Related Work	21
	10.1 Governmental activities	22
	10.2 Existing solutions	24
	10.3 SSI + OIDC	25
11	Next steps	26
12	Conclusion	26
13	List of illustrations	27
14	List of tables	27
15	Glossary	28
16	Bibliography	29
17	Version control	29

2 Introduction

Current authentication and identity schemes are characterized by communication between a Relying Party (RP) and an Identity Provider (IdP). Any information about the entity which demands access to a resource of the RP is issued and maintained by this IdP. Protocols like OpenID Connect (OIDC)/OAuth2.0 and Security Markup Language (SAML) are commonly used in this area. Nowadays, this is often used in social login schemes. For example, Google uses the OIDC protocol for their "sign-in service". After a user authenticates herself and consents to distribute some attributes to a RP, three different tokens are exchanged. An *id-token*, a *refresh-token*, and an *access-token*. The RP will use these tokens to obtain data about the user from this Identity Provider, which is maintained by a more or less unknown instance. This approach typically has an impact on the user's privacy by allowing this IdP to track the user's behaviour, because the IdP is involved in every access procedure.

Let's assume that an identity is no longer assigned by a central instance, but by the entity itself – some kind of a "self-issued identity". This requires the handling of some sort of "decentralized identities". More generally spoken – we do not know, where the identity is coming from. But we have to build a trust in this Identity. It is not the identity itself that is of much importance, but rather the attributes or characteristics of an entity which are significant. These attributes have to be attached to an identity, so that no abuse can happen. Actually, the registration process – which takes care of this – is the task of the same instance which issues assertions about an entity.

Note: The "decentralized identity" approach requires rethinking. Identities may be created anywhere, only claims (credentials) must be confirmed by an authoritative source (issuer) and be bound to the identity to avoid misuse.

But which Identities are allowed in a specific ecosystem, and which claims are accepted by Relying Parties (or a Verifier)?
Until now, the system has been quite simple, because identity and claims come from the same source, to which we have a trust relationship – i.e. in the University environment from SWITCH and the home organizations. But if the identity is from another origin (be it a state, another identity provider or the owner himself) the whole process may shift.

On behalf of SWITCH BFH is addressing these questions in this report.

3 Content of the study

In this study the following topics are covered:

- How one should deal with users who already have an electronic (self-sovereign) identity which they want to use to access services in the Swiss University environment?
- What would be the procedure of Identity creation, claim issuance and accessing a resource of a Relying Party in the world of self-issued identities?
- Which technical implementations and standards of self-issued identities have already been published or are in progress?
- What could be the role of SWITCH if a shift were to take place toward a foreign or self-issued identity? What are the risks, benefits, and challenges for SWITCH in such a setting?

4 Situation at the Outset

Considering trends like increased mobility and collaboration between universities, but above all lifelong learning, the SWITCH Community is currently changing the organization-centered approach (SWITCHaai) towards user-centric identities of the SWITCH edu-ID. This identity federation concept based on the central SWITCH edu-ID identity provider provides many advantages for the home organizations and the users. Technological innovations, e.g. OIDC, FIDO2, …, can be adapted faster and offered more easily to the entire community.
But a central identity management also has a couple of issues, mostly regarding data protection and privacy. Although SWITCH is a trusted entity in the community and fulfils existing data security and

privacy guidelines exemplarily, a central place with user data attracts attackers and needs a permanently increasing effort for protection.
Growing privacy awareness and the users' desire to control their own data is the starting point of a paradigm-shift from a central solution towards self-issued and self-managed identities. Other drivers are trends such as *Bring your own Identity* (BYOID), and the development of identities with similar properties compared to SWITCH edu-ID, like Edulog or the Swiss E-ID.

5 Self-Sovereign Identities Basics

The notion of self-sovereign identity has emerged in the past few years. It not only refers to the creation of a self-issued identity, but also includes the idea that individuals shall retain control over their personal data and, to a certain degree, over the representations of their identities (or personas) within a particular identity management system.
A short description of self-sovereign identities (SSI) principles, building block and architecture establish a common understanding throughout the rest of the document.

5.1 Principles of SSI

These principles [1] attempt to ensure the user control that is at the heart of self-sovereign identity. However, they also recognize that identity can be usable for both beneficial and pernicious purposes. Thus, an identity system must balance transparency, fairness, and support of the commons with protection for the individual.

1. **Existence**. Users must have an independent existence.
   Any self-sovereign identity can never exist wholly in digital form. It simply makes some real-life aspects of a person public and accessible.
2. **Control**. Users must control their identities.
   The user is the ultimate authority on their identity; they decide on referring to it, updating it, or even hiding it.
3. **Access**. Users must have access to their own data.
   The user must always be able to access all claims and data stored within his identity. This does not mean that they can change all claims, but they should be aware of it.
4. **Transparency**. Systems and algorithms must be transparent.
   To be consistent with the decentralized approach, it is necessary to disclose the functionality of the systems and algorithms, including the way they are managed and updated.
5. **Persistence**. Identities must be long-lived.
   Identities should last as long as the user wishes. Private keys and data might change, the identity remains. Disposal of an identity is possible (“right to be forgotten”), that includes claims being modified or removed as appropriate over time.
6. **Portability**. Information and services about identity must be transportable.
   Identities must not be held solely by a third party, even if it is a trustworthy entity (e.g. state).
7. **Interoperability**. Identities should be as widely usable as possible.
   It is essential that identities function globally and across different systems and international boundaries.
8. **Consent.** Users must agree to the use of their identity.
   It is essential that when an identity and its claims data is shared, the user has to give her consent specifically.
9. **Minimalization**. Disclosure of claims must be minimized.
   This principle can be supported by selective disclosure and other zero-knowledge techniques to support privacy as much as possible.
10. **Protection**. The rights of users must be protected.
    User rights must always take a higher priority than the needs of identity networks. In order to guarantee this, the authentication of the identity must be carried out by independent algorithms that are censorship-resistant, force-resilient and are executed decentrally.

5.2 SSI Building Blocks

The building blocks [2] of an SSI solution are:

- Decentralized identifiers (DIDs)
- Verifiable credentials
- Digital wallets
- Digital agents
- Decentralized networks

5.2.1 Decentralized identifiers

SSI is based on globally unique persistent identifiers, called decentralized identifiers (DIDs), which, like the DNS, ensure the mapping to an entity (user).

A **decentralized identifier (DID)** (see Figure 1) functions as the identifier of a user's public key stored on a blockchain or other decentralized networks. In most cases it is also the identifier for locating an agent for the entity (user) identified by the DID.

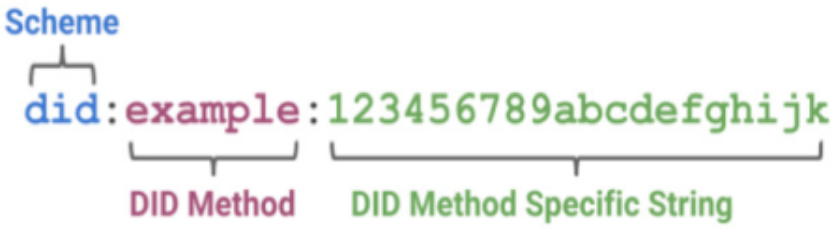

Figure 1: The general format of a DID [2]

The DID has four core properties:

1. **Permanent**. The identifier never changes, no matter how often the identity owner uses different service providers or uses different devices.
2. **Resolvable**. The identifier points to the current public key(s) for the identity owner, but also the current addresses to reach the owner's agent(s).
3. **Cryptographically verifiable**. The identity owner needs to be able to cryptographically prove that they control the private key for each public key associated with that identifier.
4. **Decentralized**. The identifier must use decentralized networks such as blockchains, distributed ledgers, distributed hash tables, distributed file systems, peer-to-peer networks, etc. to avoid control by a single authority.

A DID can be stored in any type of decentralized network (see Section 5.2.5) or even be exchanged peer-to-peer.

A DID contains a **DID method** written specifically for a target system. The method defines four atomic operations on any DID:

1. How to create/write the DID and its accompanying DID document (file containing the public key(s) and other data describing the DID subject) to the target system.
2. How to use DIDs to read the DID document
3. How to update the DID document (e.g. rotation of a public key)
4. How to deactivate a DID (usually by updating the DID document to contain no information)

The informal **DID Method Registry**[1] maintained by W3C Credentials Community Group (W3C CCG)[2] includes an up-to-date list of the DID methods for more than 30 different target decentralized networks.

[1] https://w3c.github.io/did-spec-registries/#did-methods

[2] https://w3c-ccg.github.io/

A **DID** is an URN (network location) that can lookup up with a software (or hardware) component, called **DID resolver** to get a standardized set of information, called **DID document**. For more details, see [3].

Every DID has exactly one associated DID document.

```
{
"@context": "https://www.w3.org/ns/did/v1",
"id": "did:example:123456789abcdefghi",
"authentication": [{
        "id": "did:example:123456789abcdefghi#keys-1",
        "type": "Ed25519VerificationKey2018",
        "controller": "did:example:123456789abcdefghi",
        "publicKeyBase58" : "H3C2AVvLMv6gmMNam3uVAjZpfkcJCwDwnZn6z3wXmqPV"
}],
"service": [{
        "id":"did:example:123456789abcdefghi#vcs",
        "type": "VerifiableCredentialService",
        "serviceEndpoint": "https://example.com/vc/"
}]
}
```

Figure 2: Example DID document in JSON-LD encoding with one public key and one service [2]

5.2.2 Verifiable credentials

Verifiable credentials (VC) are a set of claims about the subject (user). It is issued by an issuer to the holder, which is usually the subject. The claims must be digitally verifiable. The verification process answers the following 4 questions:

1. Is the credential in a standard format that can be electronically processed by a verifier and does it contain the data the verifier needs?
2. Does it include a valid digital signature from the issuer (thus establishing its origin and that it has not been tampered with in transit)?
3. Is the credential still valid, that is, not expired or revoked?
4. (If applicable) Does it provide cryptographic proof that the holder of the credential is the subject of the credential?

They consist of a unique identifier, meta data (e.g. expiration date), the claims about the subject (e.g. name, date of birth) and cryptographic proof.
VC preserve the subject's privacy: the subject ID in the claims is a pseudonym ID for the subject in form of a URI. Bearer VCs (without link to a subject) are possible.
VC support selective disclosure either by including a minimum of properties in a single VC (*atomic VCs*) or by using *Zero Knowledge Proof VCs*.

5.2.3 Digital wallets

A digital wallet has the same purpose as a physical wallet:

- Store credentials (VCs)
- Ensure confidentiality
- Ensure availability (across all devices)

An SSI digital wallet should have the following key features:

- Implementation of open standards for portable, self-sovereign verifiable credentials and other sensitive private data
- Works with a digital agent to form connections and perform credential exchange
- Acceptance of any standardized verifiable credential
- Platform independence (synchronization between different devices)
- Backup and migration of key and verifiable credentials between digital wallets
- One experience, no matter what wallet you use (focus on usability and user experience)

5.2.4 Digital agents

A digital wallet requires a piece of software, called **digital agent** or **agent**, that operates the wallet and makes is possible for the users to manage and use their cryptographic keys and VCs (see Figure 3). The digital agent ensures that only the wallet's controller, typically the identity owner, can access the stored VC and keys.

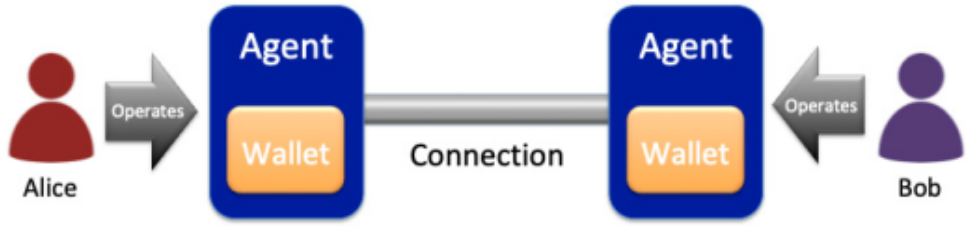

Figure 3: Digital wallet wrapped by a digital agent [2]

A second function of the agent is to communicate with other agents on behalf of the user/holder to form connections and exchange credentials by using a decentralized secure messaging protocol.

There are two categories of agents, based on where they are located:

- **edge agents** operate at the edge of the network, on identity owner's local devices.
- cloud agents operate in the cloud, where they are hosted either by standard cloud computing platform providers or specialized cloud service providers called **agencies**.

5.2.5 Decentralized networks

Any type of decentralized network can be used to store a DID. This section briefly introduces the most used approaches.

Blockchains

Blockchains are highly tamper-resistant transactional distributed databases that no single party controls. They can provide an authoritative source of data that many different peers can trust without any one peer being in control.
The main properties that support SSI are:

- Decentralization
- Transparency
- Immutability

GNS

The GNU Name System (GNS) [4] is a fully decentralized public key infrastructure and name system with private information retrieval semantics.

The GNU Name System (GNS) [4] was originally designed to replace the Domain Name System (DNS), a means of addressing network services on the Internet, with a more decentralized, secure and privacy preserving protocol. GNS can be used as the basis for a broadly applicable authentication and identity management system.

ReclaimId [5] is a self-sovereign identity using name systems and attribute-based encryption based on GNS.

Decentralized file systems

Interplanetary file system (IPFS) [6] is a peer-to-peer network for storing and sharing data over a distributed file system. IPFS uses content-addressing to uniquely identify each file in a global namespace. IPFS is built around a decentralized system of user-operators who hold a portion of the overall data, creating a resilient system of file storage and sharing. Any user in

the network can save a file by its content address, and other peers in the network can find and request that content from any node who has it, using a distributed hash table (DHT).
The advantages of IPFS [7] are the following:

- Hash addressing makes the content immutable with respect to its address
- Saves bandwidth by collecting content from multiple nodes and pieces instead of from one server
- Access to content offline or in low connectivity 3rd world or rural areas, in the same sense that git works offline.
- Censorship resistant

5.3 SSI Architecture

5.3.1 Protocol layers

The SSI stack can be considered as a four-layer model (see Figure 1). The lower two layers are primarily about achieving technical trust, while the upper two layers are about human trust. The lower layers are important, but essentially invisible. The two upper layers embody concepts that are visible to ordinary users and are directly involved in business processes, regulatory policy and jurisdiction.

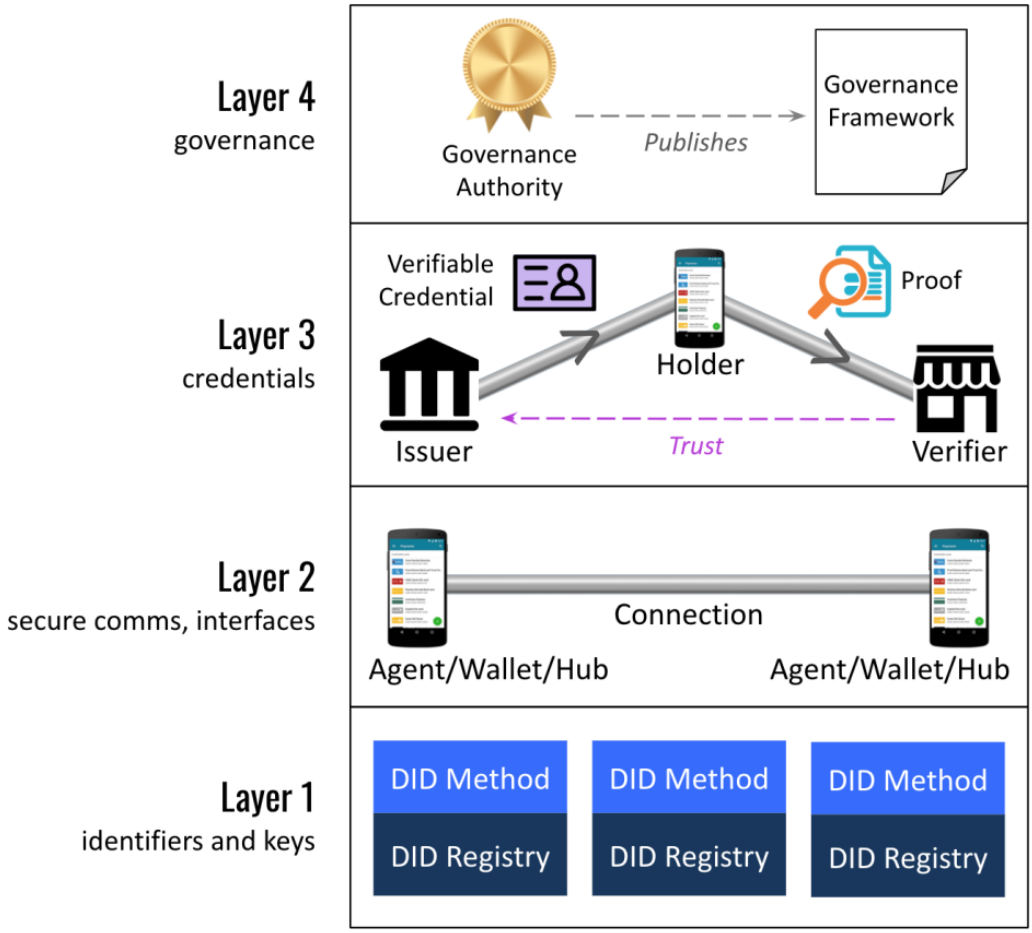

Figure 4: The SSI stack [2]

Layer 1: Identifier & Keys

DIDs and the corresponding public keys (often called trust roots) are defined and managed. This layer must ensure that all parties involved agree on what an identifier references and how the ownership can be proven. It must allow every party in the ecosystem to read and write data without having to rely on central authorities.

Typically, the required functionality is exposed by a **DID registry** through a **DID method** (see Section 5.2.1).

Layer 2: Communication & Interfaces

Layer 2 is about establishing trustworthy communication between the parties based on layer 1. This is the layer where the digital agents and wallets are located (see Sections 5.2.3 and 5.2.4). These components represent people, organizations, and things, i.e. actors from the real world.

The trust is still based exclusively on cryptography (technical trust). It is trusted that:

- A DID is controlled by another peer.
- A DID-to-DID connection is secure.
- A message sent over a connection is authentic and has not been tampered with.

There are two main approaches for communication protocols:

- **TLS based**: online two-party protocol (client server), widely spread with known privacy and security issues and an asymmetric security model which contradicts the philosophy of SSI,
- DID communication (**DIDComm**): message-oriented, transport-agnostic protocol, rooted in interactions among peers.

3 different interface design options are possible (API-oriented, Sata-oriented, Message-Oriented).

Layer 3: Credentials

The goal of Layer 3 is to support interoperable, verifiable credentials that can be used in all aspects (personal, business, etc.) by any issuer, for any holder, to any verifier.

VC can come in different formats (JWT [8], Blockcert[3], W3C VC format [9]) and a wide range of credential exchange protocols already exist.

Layer 4. Governance

Governance frameworks are the bridge between the technical implementations of the SSI stack and the real-world business, legal, and social requirements of SSI solutions. Governance frameworks are the set of business, legal, and technical rules for how SSI infrastructure will be used that are published by a particular governance authority that is trusted by the members of a particular trust community.
Not many SSI-specific governance frameworks have been created yet, if even.

5.3.2 Using the protocol stack

Two identity owners with DIDs can use the SSI protocol stack to form a connection and exchange data over a cryptographically secure connection. These connections differ from connections in many other networks and can bring five new properties into digital relationships:

1. Permanence (a connection will never break unless one or both parties want it to)
2. Privacy (all communications are automatically encrypted and digitally signed)
3. End-to-end (a connection has no intermediaries)
4. Trust (a connection supports verifiable credential exchange to establish trust between to parties)
5. Extensibility (the connection can be used for any other application that needs secure, private, reliable digital communication)

[3] Examples are available on https://www.hylandcredentials.com/new-about-3/examples/ .

5.4 Trust Relationships

5.4.1 VC Ecosystem

The Verifiable Credentials ecosystem is composed of four primary roles [10]:

- The **Issuer** issues verifiable credentials about a specific **Subject**.
- The **Holder** stores VCs on behalf of a **Subject**. Holders are typically also the subject of a credential.
- The **Verifier** requests a profile of the **Subject**. A profile contains a specific set of VCs. The verifier verifies that the credentials provided in the profile are fit-for-purpose.
- The **Identifier Registry** is a mechanism that is used to issue identifiers for **Subjects**.

A visual depiction of the ecosystem above is shown below:

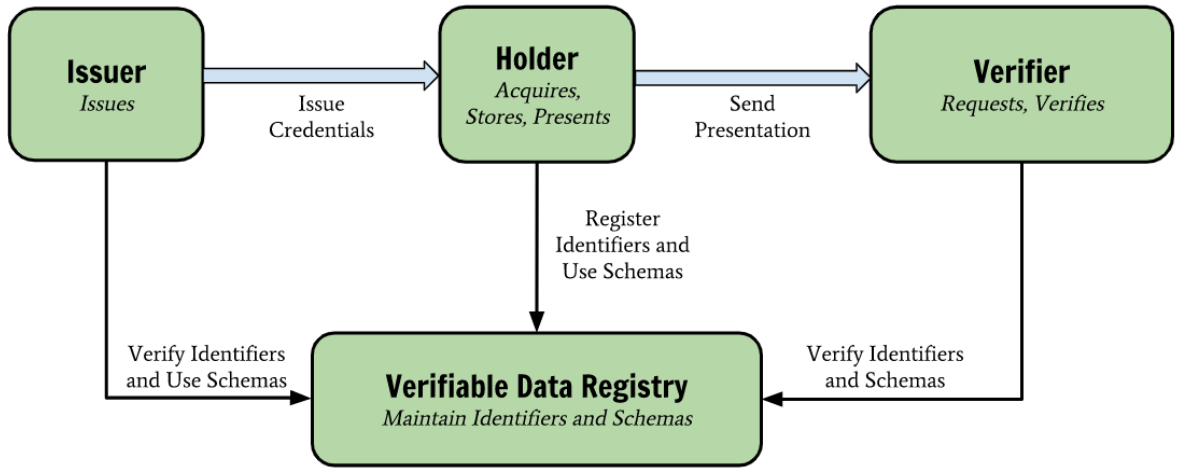

Figure 5: Roles and Information flow [9]

5.4.2 VC Trust Triangle

The roles introduced in Section 5.4.1 form the trust triangle shown in Figure 6.

- **Issuers** are the sources of credentials. All entities (also individuals and things) can be issuers. Mostly, however, issuers are organizations such as government agencies, corporations, and universities.
- **Holders/Provers** request a set of verifiable credentials from issuers, hold them in their digital wallets and present them to verifiers. Holders/provers can also be users (individuals), things or organizations.
- **Verifiers** request proofs from holders/provers. If the holder agrees, the holder's agent responds with a proof. The proof normally contains the issuer's digital signature.

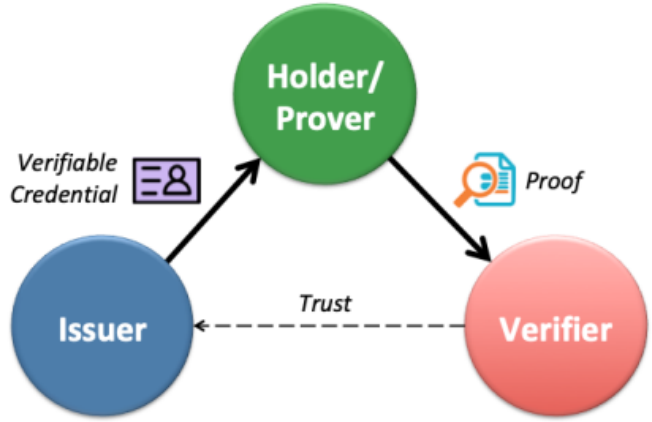

Figure 6: VC trust triangle [2]

In many business transactions the holder becomes a verifier and vice versa. The trust triangle therefore describes only one side of a business transaction.

5.4.3 Extended VC Trust Triangle

When presented with a proof of a credential from an issuer the verifier does not know, the verifier can request a second proof from the issuer (now acting as a holder/prover) proving that the issuer is authorized under a governance framework the verifier trusts. This proof comes from another verifiable credential issued by the governance authority to the issuer.

Governance frameworks specify the policies and procedures that issuers must follow to issue those credentials. They can also specify the terms and conditions to which holders must agree to obtain them. When verifiers are paying issuers for the value of the credential, a governance framework can also specify liability policies, insurance requirements, and other legal and business variables that verifiers can factor into their trust decisions.

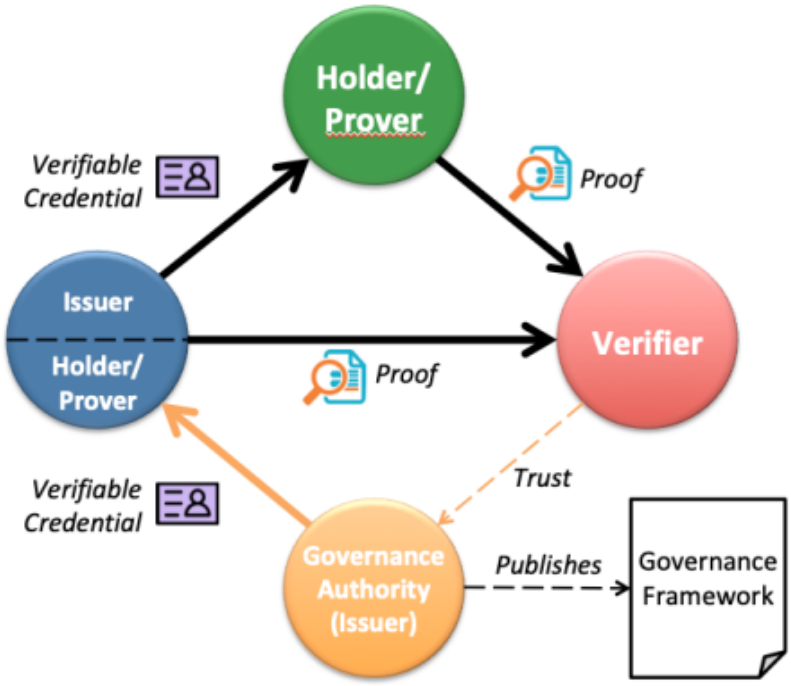

Figure 7: Extended trust triangle [2]

6 Use Cases

We consider two use cases. Our concept addresses less how credentials are presented to a Verifier, but rather how and by whom identities can be built and how claims can be bound to it.
Note: For the time being, these use cases extend only to natural persons (i.e. students) and not to services or things.

1. A student already has (or can get) an electronic identity (be it "self-issued", "provided by an unknown identity provider" or "provided by the homeland government").
2. A student has no identity available or is not willing to get one but likes to use services in the Swiss Universities network.

In any case, a student reclaims access to a Relying Party of the Swiss Universities network.

7 Processes using SSI

The main process can be divided in three parts:

1. The creation of an electronic identity. In general, this could be done by different instances, however, a Self-Sovereign Identity is created by the owner herself.
2. The Holder of this Identity then collects assertions exposed by issuers.
3. During runtime the Holder presents these properties to third parties in a trustworthy manner.

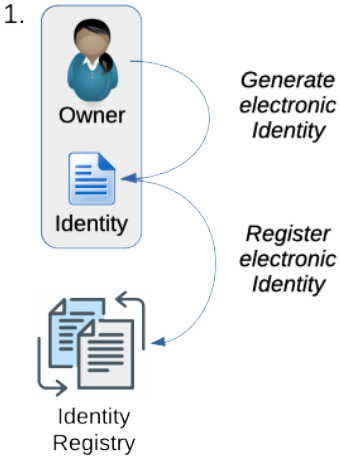

Figure 9: Creating Identity

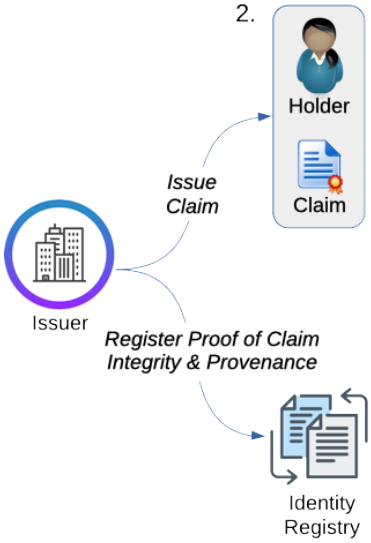

Figure 10: Collecting Claims

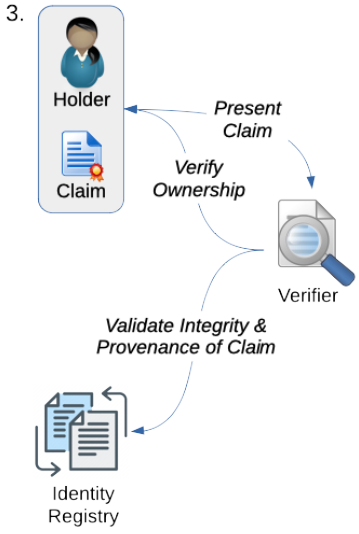

Figure 8: Presenting Claims

These steps are described in more detail in the following sections.

7.1 "Creation" of an Identity

As with a traditional Identity Provider (which normally is offered by a dedicated provider in the network), a classical process of onboarding (registration) and creation of an identificator no longer exists with a self-sovereign identity. Instead, in a first step the owner creates her own identity and links it to a key pair.
This process includes the creation of a DID and a DID-Doc, as described in Chapter 5 Section 5.2.1. It is very important to create this identity without interaction with any particular authority. The Identity and the corresponding "public key" are usually recorded in an identity registry (DLT/Network), just to be better visible and verifiable by others. This process can be executed equally by a Holder, Verifier or Issuer.

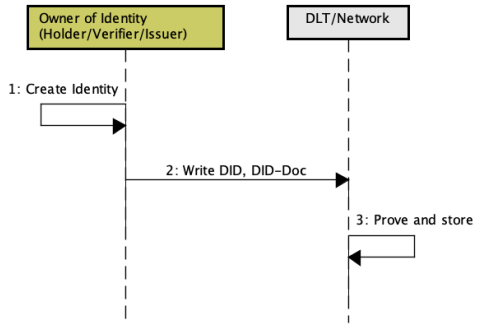

Figure 11: Identity Creation

Example of a process flow:
By accessing a Verifier for the first time, the Holder reads about an App she could download and install locally on her mobile (or in the Browser). This App includes a digital wallet and an edge-agent which takes care of all the communication and security matters for the identity owner (in this case a Person). She opens the App and an account is automatically created (1). This includes that a key-pair and an initial DID are generated. A DID-Doc is also created containing the "public key". DID and DID-Doc are automatically published (2) on a public DLT service (e.g. Ethereum). The "private key" is kept locally in the environment of the App/OS. The DID-Doc with the public key is validated and stored (3) by the public DLT service.
Note: The whole process is executed automatically and not visible for the user.

This "private key" might be saved (not shown in the figure above) for a key recovery process on several "guardians", which allows the Holder to recover access to her Identity if she should lose access to her phone.

Note: With this setup, the student is in complete control of the Identity and can't lose access due to loss of the private key.

7.2 "Collecting" Claims

The Holder of an identity can now create some "self-asserted claims" (1) and can choose to present these to a Verifier. But these claims are not verified by an authoritative source (authority). Hence, they may not have any value for a Verifier. It would make more sense if the Holder were to present Verifiable Credentials (VC) to a Verifier which have been issued and cryptographically signed by an authoritative entity.
Note: If the interaction requires a degree of trust in the claim presented, the Verifier can ask for a Credential from a trusted Issuer that satisfies the Verifier's requirements for that specific interaction. The Holder needs some sort of trustworthy claims from an authorized authority. Either the homeland Government confirms her Identity, or any other provider which functions as Identity issuer.

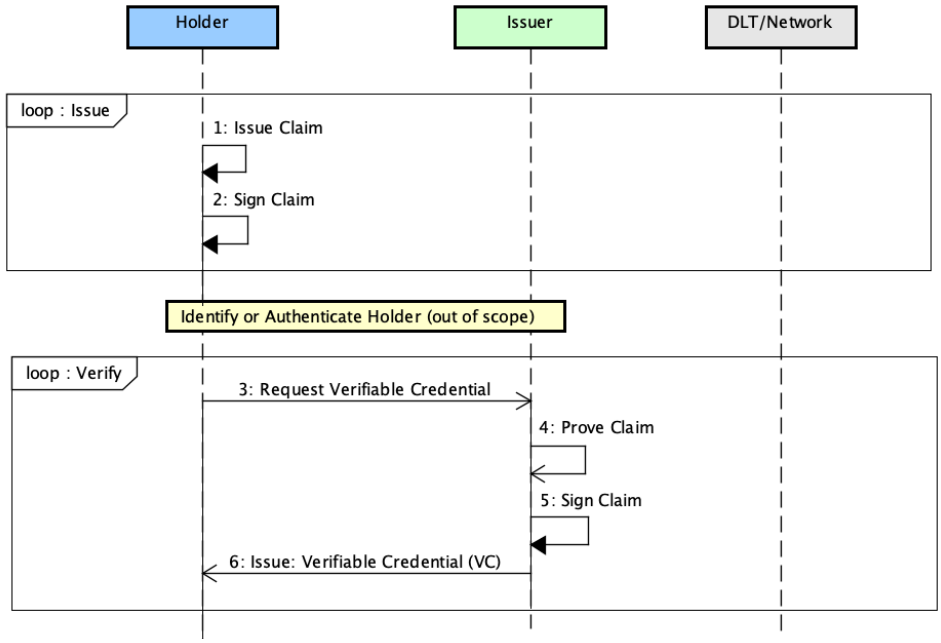

Figure 12: Issuance of Verifiable Credential

Example of a Process flow: The App tells the Holder that she first must register her Identity by proving it. After sending (3) a request to the issuer using the App, in case of a Government's vetting she probably has to visit the citizen registration office for an "in-person verification". Once the identity has been confirmed (4), the Government issues a verified attestation of personal claims which is signed by the Governments Identity (5).

The attestation of an authorized source (authority) contains the verified information. This can be "personal data" which represents the identity or any other information (i.e. an affiliation).
Note: Depending on the content this data might be stored on the DLT or on the device of the Holder only.
Note: Person Identifiable Information (i.e. a passport number, date of birth or other sensitive information) should never be revealed to others scanning the DLT.

A claim of the Holder must be linked to the DID in a vetting process. This is done by double signing (2,5) of each VC by the Holder and by the Issuer. When presenting verifiable claims about themselves issued by third parties, the trustworthiness of the claims is rooted on the authority of those parties, which implies that the issuer of the claim is really the entity it is supposed to be.
Note: The verification of the issuer's identity becomes essential.

The DID to VC bounding does not necessarily have to be made resolvable to a Verifier for privacy reasons. That's why some DLT providers offer to generate pairwise unique DIDs (with individual service endpoints) for each connection to a Verifier. These DIDs can reference the same claims, so that data does not have to be confirmed multiple times (this is referred to as "Multiple DIDs"). The goal of this approach is to avoid being identifiable by a single DID assigned to a Holder.
Note: Most implementations do not use "multiple DIDs" per person for the time being.

7.3 "Presenting" Claims

The Holder chooses to whom she wants to selectively disclose a claim. Therefore, the information (claim) is fragmented and individually signed so that it can be selectively transferred from the Holder to the Verifier if requested. The Verifier is able to validate the Issuer of the claim and the Identity of the owner (even if a pairwise unique DID is used) using the information in the DLT.
Note: *In order to disclose as little data as possible, instead of the content of a claim, only evidence of the fulfillment of requirements (e.g. legal capacity) or attributes, so-called proofs, are calculated and*

sent to the communication partner. In this scenario the Holder can prove to the Verifier by means of a "Zero Knowledge Proof" (ZKP) that she is in possession of the requested information without revealing it.

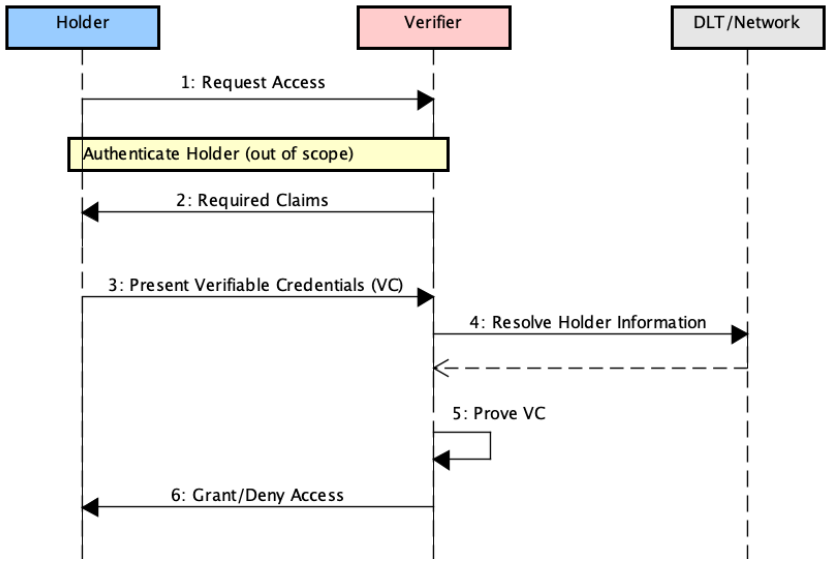

Figure 13: Verification Process

Example of a Process flow: The Holder decides to access (1) a service (Verifier). The service requests an authentication and one or multiple claims (2) to grant access for the User. The User authenticates and authorizes claims that can be shared with the server. The user agent of the User presents Verifiable Credentials (3) to the Verifier. The service verifies that the claim is from a trustworthy issuer and belongs to the Identity of the Holder (4). If the claim satisfies (5) the requirement, the Verifier redirects (6) the user agent of the User to the web site with appropriate authorization.

The process shown above describes the first use case, where a Holder creates a "self-issued identity" and then gets asserted claims from the homeland government. This identity could also have been created by another external instance. This instance could be unknown to the Swiss University community. Whether this instance is accepted by a relying party or not is up to the Governance (or to be decided by each Verifier individually).
It might also be possible for the identity (i.e. the DID and DID-Doc) to be issued by the state itself for its citizens. In this case the initial identity is given to the citizen for safekeeping. This is a "user-centric" rather than "self-issued" approach. However, this approach is not in the sense of SSI, because the owner does not issue her identity herself.

If the User has no Identity at all the second use case comes into play. In this case the User receives a "SWITCH edu-ID" which entitles him/her to access services that do not require further claims. If additional claims are requested by a RP to grant access, the User has to bring along claims which may be verified by the study administration or the human resources of a Home-Organization (i.e. University). In this case, personal information of a Holder is collected by the Home-Organization.

8 Roles

Our role model uses the standard SSI roles (Issuer, Holder and Verifier). These standard roles are extended to better reflect the digital ecosystem of a university environment:

- *Issuer:* An entity that asserts Claims about one or more Subjects, creates a Credential from these Claims, and transmits this Credential to a Holder (This is a typical role of a University, which asserts the affiliation of a student or staff member).
- *Holder:* An entity that controls a Credential from which a proof can be generated and presented to a Verifier.
- *Verifier:* An entity that consumes and accepts proofs of Claims for the purposes of delivering services or administering programs.
- *Infrastructure Provider:* A representation of a decentralized network (i.e. an Identity Registry).
- *Governance:* The overall policy, defined and maintained by the community.

Note: The Government is also listed as an entity, as it may have an important role for asserting the Identity of a Holder by issuing personal data. A Holder could also present her Claims to the Government (which acts as Verifier is this case), but we consider this case as out-of-scope and assume that a Holder would normally not use her academic Identity to use governmental services.

Entity	**Roles**				
	Issuer	Holder	Verifier	Governance	Infrastructure provider
SWITCH	x	x	x	x	(x)
University (Home Organization)	x	x	x	(x)	-
Students/Staff	-	x	x	-	-
Government	x	x	-	-	-

Table 1: Roles in a University ecosystem

8.1 The "traditional" role of SWITCH

In the previous chapter, we have shown that there is no need of a classical central IdP anymore. Rather every user is her own "Identity Provider". This means that the classical role of an "Identity Provider" may become obsolete, if the user already has (or can get) an identity.
Actually, SWITCH already acts as an issuer of electronic identities for users of the Swiss Universities environment, by creating and issuing an identifier – the "SWITCH edu-ID". These Identities are more or less self-asserted by the user herself and may be enriched by claims asserted by Home-Organizations (Universities).

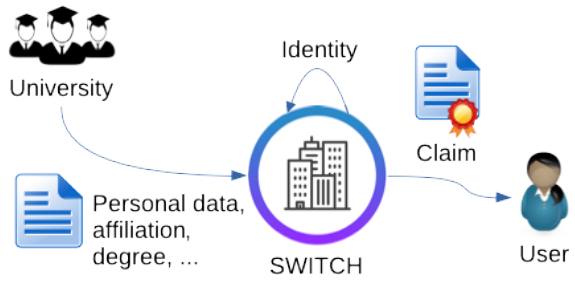

Figure 14: Current Identity Management Service of SWITCH

In this scenario, the Home-Organization provides "person-related information" and other assertions concerning the role of a user in this organization. The common identifier of each user is the "SWITCH edu-ID".

In fact, though, SWITCH could obtain more valuable “personal data” by receiving it from more trustworthy sources, asserted by the homeland-state itself or another authorized authority. In this case, the authority (e.g the government) would act as an issuer of confirmed Identities for SWITCH.

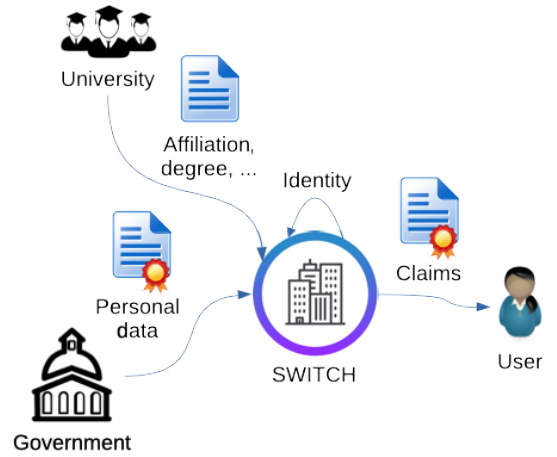

Figure 15: SWITCH as «Identity Aggregator»

This would be feasible for Swiss citizens, since a “user-mapping” between a “SWITCH edu-ID” and an “eID Registration number” (provided by the SWISS Government) could be done by SWITCH. Any other claims (i.e. affiliations or study degrees) would be added by the Home-Organization(s) of the user.

But how should one deal with foreign students or employees who basically have an identity of their own or one issued by their home country? Here, no simple solution is available.
To make things more flexible, a better approach would be, if the user were to create her own Identity locally and the home government (or any authorized authority) issued verifiable credentials tied to this Identity.

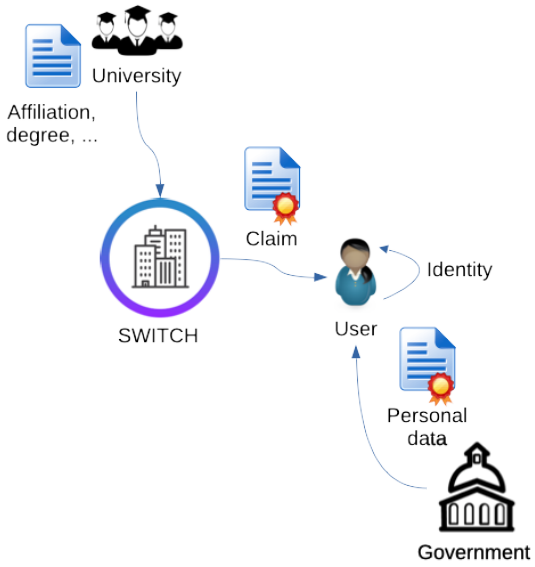

Figure 16: Self-Issued Identity

In case of a “self-sovereign Identity” this would be a DID, but this Identity could also be provided by SWITCH in the form of a “SWITCH edu-ID”. SWITCH already maintains an "Identity Management Service" which entitles any user to get a “bootstrap identity” in form of a “SWITCH edu-ID”. This service could be continued as a kind of hybrid Identity Management in which SWITCH issues and maintains the Identity on behalf of the user but any claim (Personal data, affiliation, ...) would be provided by the authoritative source itself (collecting claims) in Section 7.2.

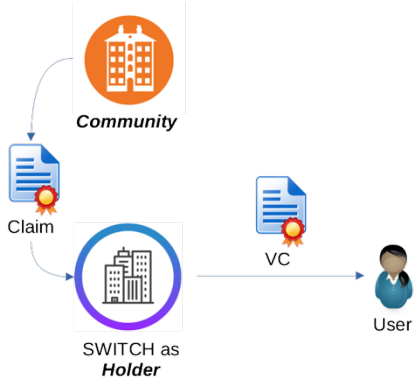

Figure 17: SWTICH as Holder entitled by the Community

SWITCH, a Home-Organization (University) or the Government can also act as Holder in a University environment. If SWITCH acts as an Issuer, it can be entitled by the Community to issue VCs (i.e. the "SWITCH edu-ID") about a User by Claim. In this case SWITCH acts as a Holder, which presents a VC to a User which this can verify.

8.2 The "new" roles of SWITCH

Other roles and benefits are imaginable and explained in the following sections.

8.2.1 Issuer of "quality seals"
The following question arises: How can the user be convinced to trust a specific RP in a decentralized approach? Until now this has been an implicit part of the "Resource Registry" (metadata). This can be solved in SSI by requiring a RP (Verifier) to present a VC to the Holder. This VC could be issued by SWITCH as the trustworthy instance of the community. All RPs with a "seal of approval" have been checked by SWITCH and are thus entitled to offer their services in the Swiss University network.

If SWITCH no longer holds the role of a central IdP, the issuance of a "release policy" is probably no longer given. A decentralized approach requires that the user herself has more responsibility. The Holder of an Identity must decide for herself whether she wants to trust an RP (or verifier) and whether she wants to release the required attributes to access a service. Until now, the release policy was anchored to the SWITCHaai "Resource Registry". Currently, a user can issue his or her approval for an attribute release or deny it altogether (for each RP).

In this model, SWITCH would categorize required data of a RP. The Holder can then decide for herself whether she wants to supply this data to the RP. This decision can be commissioned to an agent and stored for future access.
Three categories are imaginable in this context:

- RP requires Person Identifiable Information (PII) like name, birthday, gender, …
- RP additionally requires an affiliation and optionally other data from the Home-Organization
- RP requires no information, except a valid SWICH edu-ID

8.2.2 Attendant for users
Actually, an important service of SWITCH is the issuance of Identities for any user. This service must remain to enable users to easily access collaboration services and RPs which do not require claims.

Process of getting a "Bootstrap Identity":
In the current environment, a user starts as a "Nobody" by simply requesting an edu-ID from SWITCH (only a valid email address is required for this process). SWITCH acts as a kind of Identity anchor for users in the Swiss University environment.
Note: The SWITCH edu-ID, and the control of a valid e-mail address, offers only a weak claim to identify the user. A desirable side effect is binding potential new users to the university network, even if they do not have an identity from a university yet.

Selecting the Privacy-Level:
SWITCH can point out to users that they can use a “privacy-aware solution”, by selecting the self-issued identity approach (where they have more privacy, but also more responsibility) or a more comfortable, but privacy-unaware solution, by selecting the central approach provided by SWITCH.

8.2.3 Enabling migration

If the replacement of a classical central Identity approach with decentralized Identity system should become acceptable for the community, the existing infrastructure can continue to be used, maintained by SWITCH.

8.2.4 DLT Provider

This service includes a system which mediates the creation and verification of identifiers, keys, and other relevant data, such as verifiable credential schemas, revocation registries, issuer of public keys, and so on, which might be required to use verifiable credentials. A dedicated DLT provider is not necessary in the Swiss University network. This service can be implemented by a standard service like Ethereum. In any case, the question of costs must be addressed and further observed.

8.2.5 Key Recovery Provider

SWITCH could offer a service to recover a lost secret or key. This service could be one service among others, or it could be offered for the community by SWITCH alone. However, in the latter case a distribution of the secret would be no longer be possible. The user must have full trust in one key recovery provider.

8.2.6 Cloud Agents

A cloud agent offers high availability, and forwards messages from an edge agent to another. Holders can decide for themselves which agents (and what type of agents) they want use. SWITCH could provide cloud agents for the community.

8.3 Home Organization (University)

The process shown in Chapter 7 includes that each University would be a publisher of claims (i.e. affiliation or a similar VC for their students or members). Each University would have to provide such a service. This scales quite badly. In a more sophisticated system, each University remains the authoritative source for claims (because they are responsible for the content), but SWITCH could take over the role of a central Issuer of claims, based on the SWITCH edu-ID (which most likely will be a claim provided by SWITCH itself).

8.4 Government (and other authoritative sources)

As already shown in Section 8.1 the Governments take the role of vetting a user’s Identity. As already shown in Section 6, a government agency acts as an issuer of personal information in form of VCs. Possibly the agency is authorized to do so (hence the role of a Holder).

9 Risks, Benefits, Challenges…

The previous chapter has shown that a mixed form is conceivable, in which SWITCH creates a "Bootstrap Identity" for the user, which is then enriched with different claims over time. Claims mainly have two types: rather static Claims (i.e. PII) and those which are valid for a certain time only (i.e. affiliation). More and more users bring along an identity which they want to use in a specific context. This is partly due to the fact that a user already has an unmanageable number of identities and wants to reuse them. Bring your own Identity (BYOID) is the keyword. Self-Sovereign Identities are a very comprehensive approach. But there are also critical voices that claim that this makes “Identity Management” even more complicated for the user, because she has to take more tasks.

9.1 Advantages

The following points can be listed as advantages for the use of a Self-Issued Identity:

- **Minimize costs of an Identity Provider (IdP):** As already pointed out in the preceding chapter, the role of an IdP may be omitted. The expenses for the maintenance of a user management system and protection against possible attacks (e.g. data theft) is transferred to the Holder and/or cryptographically secured.
- **GDPR Compliance:** The principles of Self-Sovereign Identities (as shown in Section 5.1), point out that self-issued Identities can be more GDPR compliant, because only minimal data are to be shared and held. The identity itself can be fully under users' control.

9.2 Challenges

If the user gets more control over her identity and data, she will also be given more responsibility. So, the story of "Self-Sovereign Identity" is easy to sell, but the implementation raises questions.

- **Key Management or Key Recovery:** How can a Holder recover a "private key", if the device on which the Holder's private keys are stored is no longer usable and how can a Holder be certain that her private keys cannot be compromised? A solution with a high level of user experience is crucial. With "Self-Sovereign Identity", each user has a private key, designed in such a way that a brute force attack is close to impossible. This is clearly a good thing, as it prevents others taking over your digital identity but on the other hand it might be a problem, because there exists no "back-door", so nobody can help you if the private key is lost. Various approaches already exist to solve this problem, and undoubtedly there will be some more in the near future.
- **Trust relationship:** How can a Verifier be convinced that only a certain Identity possesses a claim which is asserted by a trustworthy instance?

9.3 Open Issues (not conclusive)

- **Traceability/Auditability**: VC have no history. It is not possible to prove that a VC had a certain value at a certain point in the past.
- **Implementation effort**: Each partner involved must implement the infrastructure for issuing and validating the VC documents themselves.
- **Portability/Interoperability**: Is transfer of claims (VC) of the same user from one SSI-Provider to another possible/desirable? At the moment, the existing solutions are not really compatible…
- **Attribute Metadata**: How to define a common schema for attribute exchange on an international scale, as required in academia?
- **Costs**: How would an overall system deal with costs (e.g. when using public blockchains)
- **Different flavours of privacy**: The terms data protection and privacy cover several tendencies. The requirements range from a
    - *decentralized issuance of the identity (decentralization)* to a
    - *decoupling of the issuance of a claim and its usage (presentation to a Verifier)* and the
    - *anonymity in any action and by any entity* and the
    - *unlinkability between "group of verifiers" or "sole verifiers"*

  These requirements can partly be met by using individual DIDs per Verifier which share a VC or with Zero Knowledge Proofs (ZKP). Research work is to be expected in this context.

10 Related Work

In this section, similar activities in other countries and available SSI solutions are listed and described briefly. In Section 10.3, some options of integrating SSI solutions into existing identity infrastructures based on OIDC are outlined.

10.1 Governmental activities

10.1.1 Jolocom/Bundesdruckerei Germany

In this proof-of-concepts for a decentralized digital German IDs, built in 2019, Jolocom software for decentralized identity and access management were merged with existing government IT infrastructure for identification and verification. The proof-of-concept enables a citizen to obtain a digital version of their official, government-issued credentials—like their national ID card, driver's license, or residency card—directly to their mobile devices, equipped with a Jolocom SmartWallet. Citizens can then reuse their credentials to engage public & private sector services in a variety of interactions—to ride share, request a student ID card, receive discounts on public transportation, and more.

Maturity: Online Demo Available

Link: https://jolocom.io/blog/jolocom-self-sovereign-identities-at-work-in-bundesdruckerei-proof-of-concept-for-e-government/

10.1.2 Findy in Finland

Findy (**F**innish **Indy** network) is a decentralized identity ledger, based on the Hyperledger Indy project (https://www.hyperledger.org/use/hyperledger-indy) to enable pilot use cases and services with use of self-sovereign identifiers in Finland.
The development is driven by the Finnish MyData Alliance (mydata.fi) that develops human centered solutions for data management.

Maturity:

- Ledger and sandbox systems available since April 2019
- Governance framework for Sandbox and production environment

Links:

- https://www.tietoevry.com/en/blog/2019/11/this-is-how-we-evolve-digital-trust-with-mydata/
- https://github.com/TrustNetFI/Findy (Findy ledger)
- https://www.findy.fi/
- http://mydata.fi/

10.1.3 Trustchain SSI in Netherlands

The Dutch Blockchain Coalition (DBC) is a joint venture between partners from the government, knowledge institutions and industry. One of the goals is the development of Digital Identities based on the blockchain technology of TU Delft, known as *Trustchain*.

As part of a pilot program, the two municipalities (Utrecht and Eindhoven) tested two identity verification services ('I am it' and 'I am older than 18') in summer 2018 in a customer trial (see Video: https://youtu.be/-RTMEQKdon8).

Maturity:

- DLT and prototype available and tested

Links:

- https://www.odyssey.org/hackathon-2020-dutch-blockchain-coalition-ministry-of-the-interior-challenge-self-sovereign-identity-in-action/
- https://www.tudelft.nl/en/2018/tu-delft/tu-delft-helps-develop-digital-id-for-use-on-your-phone/
- https://essay.utwente.nl/71274/1/Baars_MA_BMS.pdf
- Trustchain: https://tools.ietf.org/id/draft-pouwelse-trustchain-01.html

10.1.4 The European Self-Sovereign Identity Network (ESSIF)

ESSIF is part of the European Blockchain Services Infrastructure (EBSI).
ESSIF aims to implement a generic self-sovereign identity (SSI) capability, allowing users to create and control their own identity across borders without having to rely on centralized authorities. ESSIF will allow an EU entity to "obtain" verifiable credentials, to "register" verifiable mandates/consents, and to "verify" verifiable claims, which can then be used to identify/authenticate relying parties and provide those with required claims/attestations. All activities of ESIIF are aligned to the eIDAs regulations [Link: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32014R0910])

Maturity:

- 18 Technical Specifications published
- Prototype planned for 2020

Links:

- https://docs.google.com/presentation/d/1I_LbcMxOlKcIh9nhjGJoREN5V6EnF0byup1pXUvHHlQ/edit#slide=id.g5ecbd42356_0_62
- Technical documentations (DID, VC, ..): https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pageId=262505734

10.1.5 **Pan-Canadian Trust Framework**

The PCTF is a technology-agnostic model that consists of a set of agreed-on concepts, definitions, processes, conformance criteria (no "standard"). The role of the PCTF is to rely and complement existing standards and policies.
The PCTF defines two types of digital representations that are essential for the development of the digital ecosystem:

1. Digital identities of entities such as persons, organizations, and devices; and
2. Digital relationships between entities.

The framework comprises business process to create and maintain the digital representations (see the example process to confirm an identity in Figure 18).

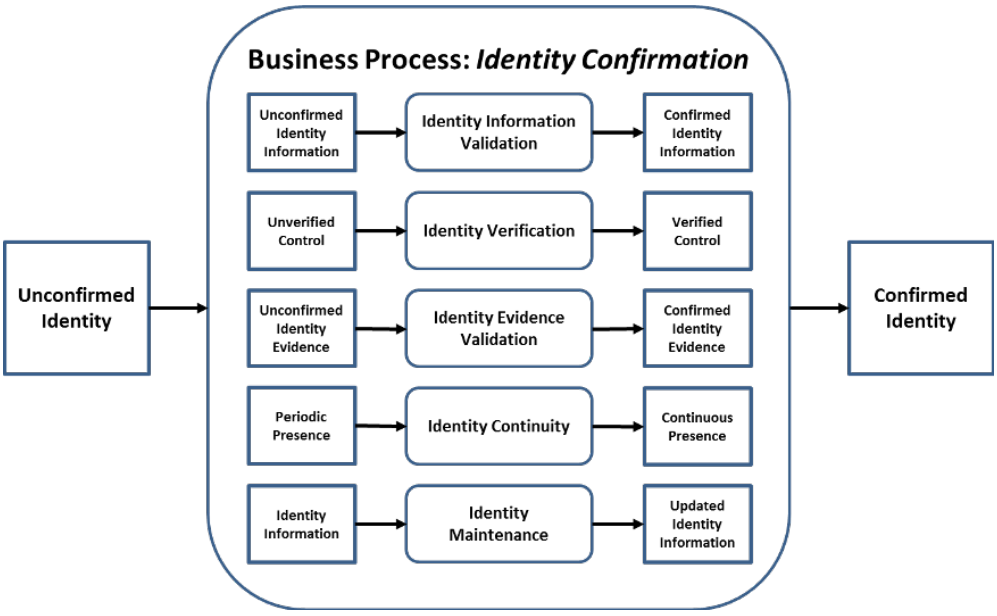

Figure 18: Example process of PCTF

Maturity:

- Consulting draft available

Link:
https://canada-ca.github.io/PCTF-CCP/

10.2 Existing solutions

In this section, commercial SSI solutions are briefly presented (without claiming completeness).

10.2.1 Sovrin/Evernym

Evernym is the creator of Sovrin, an SSI Solution based on Hyperledger Indy. The Sovrin Network is an open source project. The Sovrin Network allows for digital credentials to be privately issued, controlled, managed, and shared using a security standard called Zero Knowledge Proofs (ZKPs). The Sovrin Foundation (https://sovrin.org/) administers the Governance Framework governing the Sovrin Network.

Maturity:

- White Papers, Infrastructure (productive and sandbox), services and products (wallets, agents) available
- Supports privacy and ZKPs
- Governance framework

Links:

- https://www.evernym.com/
- https://sovrin.org/
- https://www.trendreport.de/das-sovrin-netzwerk-und-aktuelles-identitaetsmanagement/

10.2.2 Selfkey/UPort

SelfKey is an SSI Solution based on Ethereum. UPort offers services and products (agents/wallets) for the SelfKey solution. With the UPort wallet App it is possible to issue an SSI and VCs.

Maturity:

- Whitepaper & Wallet, Blockchain available
- A Prototype of a BFH Identity is developed in a bachelor thesis which will prove the feasibility of this solution

Links:

- https://selfkey.org/self-sovereign-identity/
- https://www.uport.me/

10.2.3 SeLF (esatus AG)

SelF is an SSI solution by the esatus AG based on the Sovrin network (Wallet App available on Google Play and app store). SeLF allows to integrate the Self-Sovereign Identity into existing infrastructure without modifying the legacy IT-applications, directories, or management systems. SeLF follows a credential-based access rule (CrBAC) approach, which uses SSI as new technology to authenticate and authorize objects that can be synchronized and used by conventional technologies like SAML or LDAP.

Links:

- https://self-ssi.com.
- https://esatus.com/loesungen/self-self-sovereign-identity/
- Used by cardossier (https://cardossier.ch/)

10.3 SSI + OIDC

Important for the acceptance of an SSI solutions is the possibility to integrate them in the existing IAM infrastructure and protocols. While SAML is losing importance, OIDC/OAuth2 is the current standard and actively maintained. OIDC/OAuth2 has a lot of support from the industry and many independent OIDC client implementations are available.

Here are a few solutions/projects which try to combine SSI with OIDC:

- **VCAuthN** for OIDC (https://github.com/bcgov/vc-authn-oidc) - a project from the government of British Columbia.

- **Decentralized Identity Authentication** via JOSE (https://github.com/decentralized-identity/did-auth-jose) – a project of the Decentralized Identity Foundation (DIF) itself.

- **SIOP**: The original OpenID innovators already had a vision of a decentralized identity concept by supporting personal, self-hosted OPs that issue self-signed ID Tokens. Self-Issued OPs (SIOP) use the special Issuer Identifier: https://self-issued.me. SIOP has been part of the OIDC core specification since 2014 (https://openid.net/specs/openid-connect-core-1_0.html). The messages used to communicate with Self-Issued OPs are mostly the same as those used to communicate with other OPs (see "SIOP DID Profile" (SIOP DID), a DID AuthN found at: https://didsiop.org). The SIOP-DID focuses on authentication rather than authorization, because OIDC is an authentication layer on top of OAuth2 (the essential authorization framework). There is a big discussion going on about how verifiable credentials can be exchanged and how they can be bound to an identity. The integration of SSI with OIDC/OAuth2 is therefore not finished yet.

A key factor of the success of SSI solution will be interoperability with the existing IAM infrastructure. But interoperability can come at the cost of SSI benefits. E.g., with a protocol like OIDC, a mutual authentication of user agent and relying party could become more difficult or even unfeasible. Therefore, the different solutions for the integration of SSI concepts into existing authentication protocols must be analysed in great depth.

11 Next steps

The development of SSI is in the early stages, but solutions can pop up fast und spread quickly. It is important to observe the activities in other countries, esp. in Europe and build up solid knowledge about the underlying technologies.
With a definition of the 3 basic processes identified in Chapter 7, a detailed concept with a prototypical implementation could demonstrate the feasibility and usability of the solutions available today and also point out better the disadvantages and missing parts. An essential part of this should be the integration into the existing IAM solutions, e.g. based on OIDC.
Today, SWITCH defines governance policies for the SWITCHaai infrastructure and the SWITCH edu-ID services. SWITCH could retain its role as governance authority for the SWITCH communities, also in an environment mixed with SSI, and support home organizations and users in migrating to the new paradigm of Self-Issued Identities. With the SWITCH edu-ID, SWITCH has increased its visibility to students. This will get more importance when SWITCH wants to act as trust anchor for Self-Issued Identities and claims.

12 Conclusion

SSI offers many interesting aspects for more user control and privacy. Therefore, many initiatives are actively driving the development; many solutions are already available as prototypes or even pilots.

The SWITCH edu-ID services show a couple of aspects which can also be found in SSI. Today SWITCH issues user-centric identities and enriches these identities with claims received from the university. SWITCH could easily convert this mechanism to the issuance of VC.
The SWITCH edu-ID can be used as bootstrap identity for users without an own SSI and therefore allow smooth migration for these users. In a second step, SWITCH could transform the SWITCH edu-ID to a DID-Format and serve as trust anchor for these identities.
An important role for SWITCH could also be the development of governance rules for the integration of SSI in the Swiss academic infrastructure and the support for home organizations and equally users.

But a lot of issues around SSI are still unresolved. Crucial are interoperability with existing services and usability, esp. because the users have more responsibility, and no central entity can support them. A prototype supporting the outline processes of creating an identity, collecting and presenting claims based on technology available today could show the advantages and limitations of SSI today.

13List of illustrations

Figure 1: The general format of a DID [2] 6
Figure 2: Example DID document in JSON-LD encoding with one public key and one service [2] 7
Figure 3: Digital wallet wrapped by a digital agent [2] 8
Figure 4: The SSI stack [2] 9
Figure 5: Roles and Information flow [9] 11
Figure 6: VC trust triangle [2] 12
Figure 7: Extended trust triangle [2] 12
Figure 8: Presenting Claims 13
Figure 9: Creating Identity 13
Figure 10: Collecting Claims 13
Figure 11: Identity Creation 14
Figure 12: Issuance of Verifiable Credential 15
Figure 13: Verification Process 16
Figure 14: Current Identity Management Service of SWITCH 17
Figure 15: SWITCH as «Identity Aggregator» 18
Figure 16: Self-Issued Identity 18
Figure 17: SWTICH as Holder entitled by the Community 19
Figure 18: Example process of PCTF 23

14List of tables

Table 1: Roles in a University ecosystem 17

15 Glossary

DID Decentralized Identifier
DHT Distributed Hash Table
DNS Domain Name System
GNS Gnu Name System
IdP Identity Provider
IPFS Interplanetary File System
JWT JSON Web Token
SAML Security Assertion Markup Language
SIOP Self-Issued OpenID Connect Provider
SSI Self-Sovereign Identity
OIDC OpenID Connect
PII Person Identifiable Information
PCTF Pan-Canadian Trust Framework
URN Uniform Resource Name
VC Verifiable credentials
W3C CCG W3C Credentials Community Group
ZKP Zero Knowledge Proofs

16 Bibliography

[1] C. Allen, "The path to self-sovereign identity.," 2017. [Online]. Available: https://github.com/ChristopherA/self-sovereign-identity/blob/master/ThePathToSelf-SovereignIdentity.md.

[2] A. Preukschat and D. Reed, Self-Sovereign Identity MEAP V5., Shelter Island, New York: Manning, 2020.

[3] W3C, "Decentralized Identifiers (DIDs) v1.0. Core achitecture, data model, and representations. Working Draft.," 21 July 2020. [Online]. Available: https://www.w3.org/TR/did-core/. [Accessed 2020 September 09].

[4] M. Wachs, M. Schanzenbach and C. Grotthoff, "A censorship-resistant, privacy-enhancing and fully decentralized name system.," in *13th International Conference on Cryptology and Network Security (CANS 2014)*, 2017.

[5] M. Schanzenbach, G. Bramm and J. Schütte, "reclaimid: Secure, self-sovereign identities using name systems and attribute-based encryption.," in *Proceedings of the International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, 2018.

[6] Protocol Labs, "IPFS powers the Distributed Web," Protocol Labs, [Online]. Available: https://ipfs.io/. [Accessed 07 09 2020].

[7] T. Terado, "What is Decentralized Storage? (IPFS, FileCoin, Sia, Storj & Swarm)," 4 July 2018. [Online]. Available: https://medium.com/bitfwd/what-is-decentralised-storage-ipfs-filecoin-sia-storj-swarm-5509e476995f. [Accessed 7 September 2020].

[8] Internet Engineering Task Force (IETF) , "JSON Web Token (JWT), RFC 7519," May 2015. [Online]. Available: https://tools.ietf.org/html/rfc7519.

[9] W3C, "Verifiable Credentials Data Model 1.0," 24 June 2020. [Online]. Available: https://w3c.github.io/vc-data-model/. [Accessed 4 September 2020].

[10] D. B. Manu Sporny, "A Verifiable Credentials Primer," 4 January 2019. [Online]. Available: https://github.com/WebOfTrustInfo/rwot8-barcelona/blob/master/topics-and-advance-readings/verifiable-credentials-primer.md. [Accessed 4 September 2020].

[11] D. Gisolfi, "Self-sovereign identity: Why blockchain?," IBM, 13 June 2018. [Online]. Available: https://www.ibm.com/blogs/blockchain/2018/06/self-sovereign-identity-why-blockchain/. [Accessed 03 September 2020].

17 Version control

Version	Date	Description	Author
1.0	12.11.2020	Finalization	Annett Laube, Gerhard Hassenstein