myIdP - The Personal Attribute Hub

Annett Laube and Severin Hauser
Bern University of Applied Sciences
Devision of Computer Science
Biel/Bienne, Switzerland
Email: annett.laube@bfh.ch, severin.hauser@bfh.ch

***Abstract*—The myIdP service is an extension to the Swiss eID infrastructure with the aim to provide a service that handles personal attributes (like address, telephone number, email), which are neither part of the SuisseID identity providers nor of a Claim Assertion Services (CAS) because there is no official authority owning and certifying these data. The myIdP service is a (pseudo-)local CAS that can reuse data, which a user has already given to an application via an Internet transaction. The data is thus validated by the web application before being transferred - as SAML 2.0 attribute assertion - to the myIdP service. The myIdP service comes in two flavors with different trust relations: the attribute provider and the claim proxy. The attribute provider unites several claims for a given attribute and provides an optional quality assessment before sending it to a requesting web application. A trust relationship must consist between myIdP and the web application. The claim proxy only collects the received claims for a given attribute and transfers them with all details to the requesting application. The application can evaluate the confidence in the data based on the claim details. The myIdP service is evaluated in a scenario of prefilling e-forms in a eGovernment application.**

Keywords*—*electronic identity; SuisseID; attribute authority; e-form

I. Introduction

Like in many European countries, also in Switzerland an infrastructure for electronic proof of identities (eID) was developed and introduced in 2010 as SuisseID Infrastructure. The basis is the SuisseID [1] available as USB stick or chip card containing two digital certificates: (1) the SuisseID identification and authentication certificate (IAC) and (2) the SuisseID qualified digital certificate (QC). The SuisseID IAC can be used to identify the owner in Internet transactions. The SuisseID QC can be used to sign electronic documents in a forgery-proof manner. The SuisseIDs are issued by identity providers (IdP). In contrary to other European countries, where electronic identities are issued by the government together with offline identification (ID card), there are actual three commercial and one governmental SuisseID IdP.

The SuisseID itself and its certificates contain only a minimum of personal data (SuisseID number, name or pseudonym and optional email address) due to stringent privacy and data protection requirements in Switzerland. Additionally, a subset of the personal data from the identification document (e.g., a passport) and a well-known set of additional attributes gathered during the registration process (so called Registration process data, RPD) are stored in the identity provider service (extended IdP). The only way to retrieve this data is by strong authentication with the IdP service using the appropriate SuisseID IAC. The SuisseID Infrastructure is completed with a set of Claim Assertion Services (CAS) [2]. The purpose of a CAS is to provide and certify specific properties or attributes, which had been assigned to the SuisseID owner by some private or public authority. Examples are the membership of an organization or a company, and the proof of professional qualifications, like a notary or a doctor. Especially in the context of eGovernment, there is a need for an extension of the beforehand described SuisseID Infrastructure.

Many more personal attributes (like invoice address, telephone number, email) used in web applications, e.g., online shops, or in electronic forms often used in the eGovernment, are neither subject of the SuisseID IdPs nor the CAS because there is no official authority owning and certifying these data. The myIdP service fills that gap and allows storing and maintaining personal attributes for a SuisseID owner. The idea is to store information, which was at least entered (and thus used) once in a web application, for later reuse. The data is used and thus validated by the web application before being transferred as SAML attribute statement [3] (the so-called attribute claim) to the myIdP service. From now on, the user can reuse the attribute for other applications, which improves usability and reduces the error potential in the daily internet transactions.

The paper starts with the related work in Section II, before outlining the architecture and flavors of myIdP in Section III. In Section V, the integration of myIdP in a scenario of prefilling e-forms is shown. Section VI concludes the document.

II. Related Work

A service like myIdP or a SuisseID CAS corresponds technically to an Attribute Authority defined by SAML [3]: An Attribute Authority is a system entity that produces attribute assertions.[4]

In general, most of the known SAML Identity Providers (IdPs) can act as an Attribute Authority and issue attribute assertions beside their usual authentication functionality. Examples are the government-issued electronic identities of the European Countries, like the German Identity Card [5], the beID from Belgium [6] or the Citizens Card from Austria [7]. Similar to the SuisseID, all these government-issued eIDs provide only a small number of personal attributes related to the identity document they belong to.

The national electronic identities of the European member states are made interoperable with the STORK European eID Interoperability Platform [8]. With six pilots, the STORK project offers several cross-border eGovernment identity services. In the follow-up project STORK2.0 [9] also personal attributes related to eIDs are subject of investigation. E.g., in the banking pilot, public and private identity and attribute providers are included in the process of ”Opening a bank account” in a foreign country online with a national eID without physical presence. myIdP could be used in this context as attribute provider for personal attributes, like address, telephone number, email, etc.

In contrast to the central, government-regulated eID services, OpenID [10] is a decentral authentification service for web based services. The user is free to choose his favorite OpenID identity provider to get a OpenID, which is an URL or XRI including an end-user chosen name (e.g., alice.openid.example.org). OpenID providers are, e.g., Clavid [11] , CloudID [12], Google [13] etc. The OpenID providers themselves can support different authentification methods. For example, Clavid offers username/password, one time passwords, SuisseID authentication and the biometric AXSionics Internet Passport.

User attributes, like name, gender or favorite movies, can be also transferred from the OpenID identity providers to the relying party following the OpenID Attribute Exchange Specification [14]. The attributes can be (almost) freely defined according to the requirements of the relying party. As many OpenID providers do not validate the information entered by the users, the provided attributes have a low level of assurance. There is a need for a validation by a trusted 3rd party, a so called attribute provider (AP). Google started the Open Attribute Exchange Network (Open AXN, also known as ”street identity”, see [15]) to include validated information from APs. myIdP has the potential to act as an OpenID attribute provider, but is currently only enabled for use together with the SuisseID.

WebIDs [16] are especially common in social media (FaceBook, LinkedIn . . .) to allow users to identify themselves in order to publish information. Each user can make his own WebID or rely on an identity provider. The WebID is a URL with a #tag pointing to a foaf file [17] containing a cross-link to a (self-generated) certificate. Information that should be included but are not required to be present in a WebID Profile are the name (foaf:name) of the individual or agent, the email address associated (foaf:mbox) and the agent’s image (foaf:depiction). More attributes and links to all kind of web objects (other persons, groups, publications, account, . . .) can be also included. WebIDs can be connected to OpenIDs and vice versa.

III. ARCHITECTURE

myIdP consists of four components (see orange boxes in Figure 1): the myIdP Service, the myIdP WebApp, the myIdP Admin and the myIdP API.

The **myIdP Service** is an attribute authority according to the SAML 2.0 [3] standard distributing assertions in response to identity attribute queries from an entity acting as an attribute requester. Like a typical SuisseID CAS [2], the myIdP service let the users select and confirm the properties, which were formerly received from an attribute issuer and are stored in the myIdP database.

New, to the concept of CAS, is the provisioning of a quality (level of assurance, level of confidence) together within the attribute assertions. myIdP integrates a quality module, that calculates the trustworthiness of the provided information on the basis of the ages, number of affirmations and quality of the issuer of the received and stored attribute assertions. This assurance level or quality can be used by an attribute requester to insist on a certain level of assurance for the requested attributes. The calculation of the assurance level or quality is a research topic on its own and therefore not included in this paper. A possible approach is shown in [18].

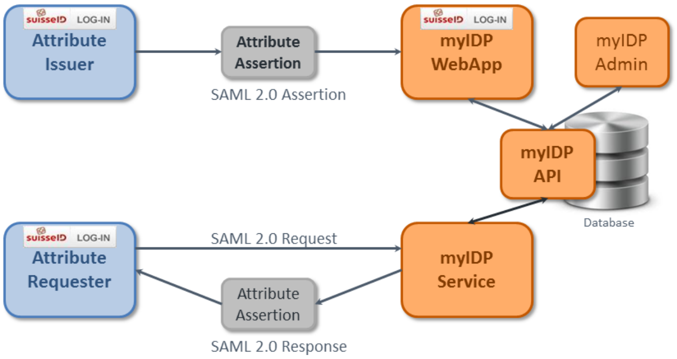


Figure 1. myIdP components and service provider roles

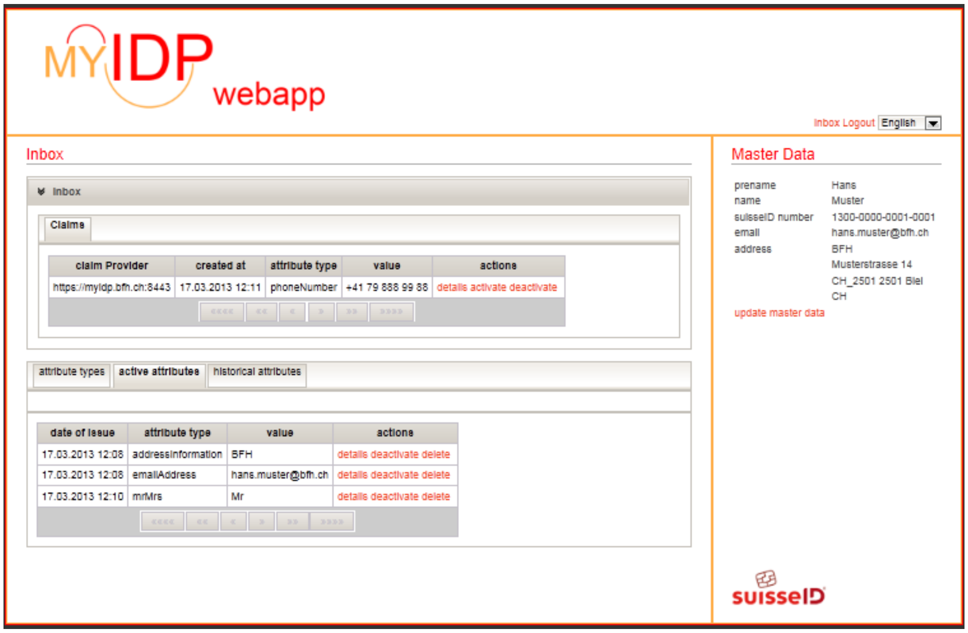
The **myIdP WebApp** is the end user front-end of myIdP where users – after the successful authentication with their SuisseID IAC – can view and manage their attributes. Attributes can not be entered directly in the myIdP WebApp, except the master data related to the myIdP account. Attributes always come from a service provider, e.g., a web application, acting as attribute issuer, which forwards – after confirmation by the user – the attribute assertions to myIdP. The attributes then arrive in the so-called **Inbox** (see Figure 2) where they can be detailed viewed and manually activated before they are exposed via the myIdP service. Corresponding to the user centric approach of the SuisseID, the users are always in control of their data and can activate/deactivate and delete attributes at any time. As a side effect, the user gets an usage history of his attributes in the web.

The **myIdP Admin** is an administration tool for myIdP. It supports the maintenance of attribute definitions and the registration process of service providers, which is needed to set up secure connections and trust relationships. New attributes can be enabled for usages simply by importing the related XML Schemata or by the use of the SAML Metadata Exchange [19].

The **myIdP API** provides an interface to the central database used commonly by the other three myIdP components.

A service provider can interact with myIdP incorporating two roles (see the blue boxes in Figure 1):

- **Attribute Requester:** The service provider electronically sends an attribute query to the myIdP service in order to draw a confirmation statement - a SAML 2.0 attribute assertion - from the myIdP service and uses it in further actions, e.g., prefilling of web forms.
- **Attribute Issuer:** The service provider sends SAML



claim Provider	created at	attribute type	value	actions
https://myidp.bfh.ch:8443	17.03.2013 12:11	phoneNumber	+41 79 888 99 88	details activate deactivate

date of issue	attribute type	value	actions
17.03.2013 12:08	addressInformation	BFH	details deactivate delete
17.03.2013 12:08	emailAddress	hans.muster@bfh.ch	details deactivate delete
17.03.2013 12:10	mrMrs	Mr	details deactivate delete

prename	Hans
name	Muster
suisseID number	1300-0000-0001-0001
email	hans.muster@bfh.ch
address	BFH Musterstrasse 14 CH_2501 2501 Biel CH

Figure 2. Screenshot myIdP WebApp - Inbox

2.0 attribute statements to myIdP. (Despite the possibility to group several attributes in one SAML statement, myIdP prefers single attribute statements, in order to expose a minimum of information in the claim proxy case.) The attribute values where entered either manually by the users or requested beforehand from the myIdP service.
A special attribute provider is the myIdP WebApp, which uses the master data (address, email) entered during the myIdP registration process, to provide the first attribute statements to the users.

The myIdP service is available in two flavors: the **Attribute Provider** and the **Claim Proxy**.

The attribute provider summarizes the in the myIdP database available attribute assertions for the given request. All details about the original attribute provider of the information are hidden. After the user has selected and confirmed the attribute values, the newly built attribute assertion is signed by the myIdP service. When requested, an assurance level is included in this assertion. For this myIdP flavor, a direct trust relationship is established between the myIdP service and the web application in the attribute requester role.

This is different in the second myIdP flavor. The claim proxy extracts the stored attribute assertions from the myIdP database for a given attribute request. After the selection of attribute values and the explicit confirmation by the user, an attribute assertion containing an URI and optional the assurance level is returned to the requesting web application. This attribute request is also signed by myIdP but only to ensure integrity. The web application can use the URI from the attribute assertion to assess the originally received attribute assertions enveloped in an XML document. The web application can now access all details of the original assertions, including the issuers and timestamps, and perform its own quality assessment. The trust relationship has changed: the web application trusts directly the attribute issuers.

```
<complexType name="AttributeType">
  <sequence>
    <element ref="saml:AttributeValue"
      minOccurs="0" maxOccurs="unbounded"/>
  </sequence>
  <attribute name="Name" type="string"
    use="required" />
  <attribute name="NameFormat" type="anyURI"
    use="optional" />
  <attribute name="FriendlyName" type="string"
    use="optional" />
  <attribute name="myidp:Quality" type="decimal"
    use="optional" />
  <attribute name="myidp:ClaimListURI" type="anyURI"
    use="optional" />
  <attribute name="myidp:ClaimList" type="boolean"
    use="optional" />
  <anyAttribute namespace="##other"
    processContents="lax" />
</complexType>
```

Figure 3. Extended xsd `AttributeType`

In order to support the provision of a quality assessment of an attribute value and of the claim list URI, the SAML attribute assertions was extended (see the XSD fragment shown in Figure 3).

IV. Privacy

One important characteristic of myIdP (valid for both flavors) is the user-centric approach. The user is always aware which information is exchanged and has explicitly to confirm every single attribute, which is sent out by myIdP.

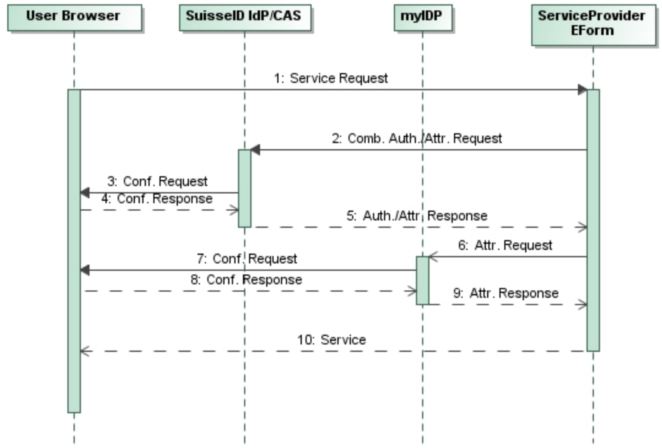


Figure 4. Sequence diagram ”Get e-form”

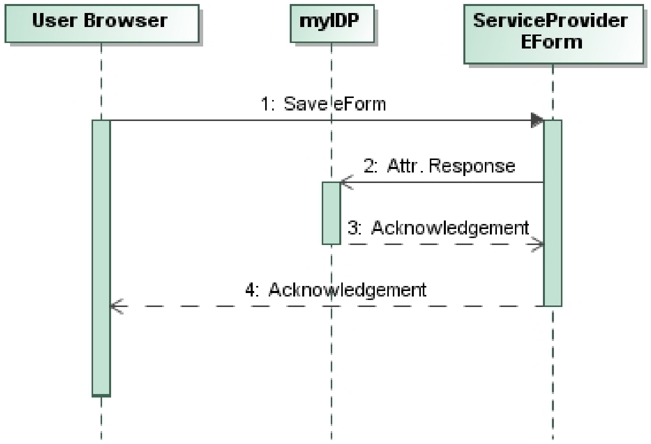


Figure 5. Sequence diagram ”Save e-form”

myIdP implements multiple measures to ensure the privacy of the user: First, every Attribute Issuer has to get an user consent before sending any attribute statement to myIdP. Secondly, in myIdP the arriving attributes are deactivated by default. The user has explicitly to confirm if he wants to activate these attributes for further use. At any time, the user is free to delete attribute statements in the myIdP WebApp or to deactivate them. Thirdly, the user is involved in every message exchange with an Attribute Requester and has to confirm all attribute values. In the claim proxy case, he has also to confirm the disclosure of original attribute assertions. The attribute assertions contain information about visited web sites and could be used to track the user and to create user profiles. In any case, myIdP only sends attribute statements to Attribute Requesters only if there is a valid authentication with a SuisseID in addition to the user consent. These procedures ensures that the user exposes only the data he wants to use and protects his privacys.

V. Application Scenario

A scenario of completing electronic forms (e-forms) validates our approach. E-forms are commonly used in the Swiss eGovernment. With the help of the SuisseID, the citizen can be securely identified and the attributes stored in the core SuisseID components, like name, birthday, place of birth or nationality, can be used to prefill the e-forms. As the number of attributes available in the core SuisseID is quite limited, we want to use myIdP to provide additional values for the e-forms.

For our proof of concept, we chose the form ”Proof of residence”, which had already an integration with the core SuisseID infrastructure. In Figure 4, the interactions between the user, the e-form provider, the core SuisseID components and myIdP are depicted:

1) Service Request: the user requests an e-form from the e-form provider (e.g., by clicking on a link).
2) Authentication with SuisseID: the e-form provider issues an authentication and attribute request to the SuisseID IdP/CAS service. The following attributes are requested: name, first name and birthday.
3) Confirmation request: the user has to identify himself by entering his secret key (PIN) and in a second step to confirm his SuisseID attributes.
4) Confirmation response: the user’s decisions are sent back to the SuisseID IdP/CAS.
5) Authentication and Attribute response: the SuisseID IdP/CAS sends a combined authentication and attribute assertion back to the e-form provider.
6) myIdP attribute request: the e-form provider issues an attribute request to the myIdP service asking for the address and the email.
7) Confirmation request: the user has to select the attribute values in case several emails or addresses are stored in myIdP and to confirm the selection.
8) Confirmation response: the user’s decisions are sent back to myIdP.
9) Attribute response: myIdP sends an attribute assertion back to the e-form provider.
10) Service: the e-form is displayed to the user and contains the selected and confirmed values from the SuisseID IdP/CAS and myIdP.

The user has now to complete the form and to enter the number of copies he wants to receive. In case, his email or home address has changed, he can also manually correct the data on the e-form (the data from the SuisseID IdP/CAS are read-only and can not be changed). When he saves the document the governmental process of providing the requested documents is started. But, the confirmed data from the e-form are also transferred – as new attribute assertions containing validated information – to myIdP (see Figure 5).

A crucial point to use myIdP in eGovernment applications and also in other domains is the selection and standardization of attributes. In our scenario, we could reuse attributes defined and published as Swiss standards, e.g., the eCH-0010 [20] for the address and eCH-0042 [21] for the email.

VI. Conclusion and Future Work

myIdP is an extension to the SuisseID infrastructure. It proposes a Claim Assertion Service (SAML attribute authority), which handles personal data used and validated beforehand in other internet transactions. The concept is extensible to other eID solutions and can be also integrated in the STORK European eID Interoperability Platform. In a next step, the possibility to use myIdP as OpenID attribute provider will be investigated. Also the combination with a WebID seems feasible.

The myIdP concept was validated with a prototypical implementation following the proposed architecture. The implementation on the basis of the SuisseID SDK[22] showed quickly some limitations, especially related to a flexible attribute set and structured attributes, like address.

As proof-of-concept, the prototype was integrated in an eGovernment scenario of prefilling an e-form in order to obtain a proof of residence. The integration of more e-forms is planned. As precondition the set of myIdP attributes has to be extended to have a standardized basis for the information exchange.

The promoting of the myIdP service showed that many applications are willing to act as Attribute Requester and to use the personal attributes available in myIdP. The functionality to act as Claim Provider and to provide validated information to myIdP and to confirm the reuse is often seen as burden. But, both roles have to be equally provided to create a network of validated personal attributes.

Soon as more service providers will use myIdP and provide attribute claims, the model to calculate the assurance level can be validated on a real data basis and be further improved.

To strengthen even more the user-centric approach and to protect the private attribute, the central storage of claims in the myIdP database could be changed towards a pseudo-local approach that let the user choose where the store the data: on his own device or on a central place. The storage of SAML assertions on the user's device would also enable the usage of myIdP - in addition to the normal online scenario - in environments with limited or no connectivity.

ACKNOWLEDGMENT

Thanks to all students from the Bern University of Applied Sciences who helped with their bachelor theses [23][24] to realize this project.

REFERENCES

[1] Arbeitsgruppe Spezifikation des Trägerschaftsverein SuisseID, "eCH0113 SuisseID Specification, Version 1.5," November 30, 2011.

[2] Arbeitsgruppe SuisseID c/o Staatssekretariat für Wirtschaft SECO, "Claim Assertion Service (CAS), Technical Specification, Version 0.99.07," January 13, 2011.

[3] N. Ragouzis et al., "Security Assertion Markup Language (SAML) V2.0 Technical Overview. OASIS Committee Draft," March 2008. [Online]. Available: http://www.oasis-open.org/committees/download.php/27819/sstc-saml-tech-overview-2.0-cd-02.pdf

[4] J. Hodges, R. Philpott, and E. Maler, "Glossary for the OASIS Security Assertion Markup Language (SAML) V2.0," March 2005. [Online]. Available: https://www.oasis-open.org/committees/download.php/21111/saml-glossary-2.0-os.html

[5] M. Margraf, "The new German ID card," February 2011. [Online]. Available: http://www.personalausweisportal.de/SharedDocs/Downloads /EN/Paper_new_German_ID-card.pdf

[6] (2013, Mar) The official beID website. [Online]. Available: http://eid.belgium.be/en/

[7] (2013, Mar) Austrian Citiziens Card - Official Website. [Online]. Available: http://www.buergerkarte.at/index.en.php

[8] (2013, Mar) STORK - Project Website. [Online]. Available: www.stork-eid.eu

[9] (2013, Mar) STORK 2.0 - Project Website. [Online]. Available: www.eid-stork2.eu

[10] specs@openid.net, "OpenID Authentication 2.0 - Final," December 2007. [Online]. Available: http://openid.net/specs/openid-authentication-2_0.html

[11] (2013, Mar) Clavid - Official Website. [Online]. Available: clavid.ch

[12] (2013, Mar) Cloudid.de - OpenIDentity Provider - Website. [Online]. Available: cloudid.de

[13] Google, "Federated Login for Google Account Users," June 2012, accessed January 2013. [Online]. Available: https://developers.google.com/accounts/docs/OpenID

[14] D. Hardt, J. Bufu, and J. Hoyt, "OpenID Attribute Exchange 1.0 - Final," December 2007. [Online]. Available: http://openid.net/specs/openid-attribute-exchange-1_0.html

[15] Open AXN group. (2013, Mar) Street Identity - Website. [Online]. Available: https://sites.google.com/site/streetidentitylmnop/

[16] H. Story and S. Corlosquet (eds.), "WebID 1.0. Web Identification and Discovery. W3C Editor's Draft." January 2013. [Online]. Available: http://www.w3.org/2005/Incubator/webid/spec/

[17] D. Brickley and L. Miller, "FOAF Vocabulary Specification 0.98," August 2010. [Online]. Available: http://xmlns.com/foaf/spec/

[18] A. Keller, "Qualitätsmodell im Kontext von myIdP. CASE Arbeit." Master's thesis, BUAS - WGS, June 2012. [Online]. Available: http://www.myidp.ch/acms/fileadmin/documents/case_Qualitaetsmodell_v1.0.pdf

[19] S. Cantor, J. Moreh, R. Philpott, and E. Maler, "Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0," March 2005. [Online]. Available: http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf

[20] Verein eCH, "eCH-0010: Datenstandard Postadresse für natürliche Personen, Firmen, Organisationen und Behörden," October 2011. [Online]. Available: http://www.ech.ch/vechweb/page?p=dossier&documentNumber=eCH-0010&documentVersion=5.00

[21] ——, "eCH-0042: Vorgehen zur Identifizierung von eGovernment-relevanten Geschäftsinhalten," June 2005. [Online]. Available: http://www.ech.ch/vechweb/page?p=dossier&documentNumber=eCH-0042&documentVersion=1.00

[22] (2013, Mar) SuisseID SDK - website. [Online]. Available: https://www.e-service.admin.ch/wiki/display/suisseid/Home

[23] R. Imwinkelried and D. Ehrler, "Bachelorthesis: Specification myIdP," Master's thesis, BUAS - TI, January 2012.

[24] R. Bühlmann and M. Jeker, "Bachelorthesis: Specification myIdP Extensions," Master's thesis, BUAS - TI, June 2012.