Zwattendorfer, B.; Tauber, A.; Zefferer, T., "A privacy-preserving eID based Single Sign-On solution,"
5th International Conference on Network and System Security (NSS), 2011, pp.295-299
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6060018&isnumber=6059944

A Privacy-Preserving eID based Single Sign-On Solution

Bernd Zwattendorfer, Arne Tauber, Thomas Zefferer
E-Government Innovation Center
Graz, Austria
{Bernd.Zwattendorfer, Arne.Tauber, Thomas.Zefferer}@egiz.gv.at

***Abstract*— Single Sign-On (SSO) has become a popular technology allowing users to identify and authenticate once and to gain access to different resources in a distributed computing environment. Austrian e-Government relies on a secure and privacy-preserving sectoral identity management model. Even if a sectoral identifier model improves privacy, it also negatively affects the usability of authentication processes. In Austria, most public sector applications use an open-source identity provider called MOA-ID. However, due to the sectoral identity management MOA-ID has not been Single Sign-On-capable. In this paper we present a security architecture that enables Single Sign-On between different governmental applications using MOA-ID as identity provider while meeting the requirements for sectoral data privacy protection at the same time. We achieve this by transforming unique sectoral identifiers of users with the help of an additional trusted attribute provider.**

Keywords-single-sign-on; SSO; identity management, privacy, Austrian citizen card, MOA-ID

I. INTRODUCTION

These days, more and more protected information and resources are continuously put online on the Internet. People are accustomed to authenticate against various applications or online services. All these services are usually set up on different user databases. Therefore, many portals rely on the mechanism of Single Sign-On (SSO), which allows users to authenticate once and gain access to protected resources of multiple systems in a distributed computing environment. Basically, SSO enables the sharing of user authentication data between different applications. Recent and state-of-the-art SSO web-technologies are SAML [1] or OpenID [2].

Austrian e-Government is based on a secure, user-centric and privacy-preserving identification and authentication concept where the Austrian citizen card plays a major role. The citizen card is the Austrian national electronic identification (eID) solution, which allows for creating qualified electronic signatures in conformance with the European Union (EU) Signature Directive [3]. Besides that, focus is on data-privacy protection and on the prevention of tracking of citizens' activities. Therefore, Austrian governmental identity management (IdM) relies on a so-called sectoral identification model. This means that a citizen's unique national identification number cannot be stored as identification key in governmental databases, but must rather be securely derived for each different sector or domain a governmental application belongs to. To ease the take-up of the Austrian IdM solution by public-sector service providers, the Austrian e-Government initiative provides the open-source module MOA-ID [4]. MOA-ID is an identity providing middleware that can be used by service providers to protect their resources with citizen card access. However, MOA-ID is not SSO-capable and citizens accessing applications of different administrative sectors (e.g. finance, justice) must re-authenticate every single time they are changing applications or switching contexts.

In this paper we present a security architecture that fills this gap by enabling SSO between different administrative sectors using MOA-ID still as identity provider (IdP). We achieve this by enhancing MOA-ID and by transforming sectoral identifiers using an additional attribute provider (SourcePIN Register Authority) hosted by the Austrian Data Protection Commission. The remainder of this paper is structured as follows. In Section II we introduce the concept of Single Sign-On and give a brief overview of the Austrian governmental IdM solution Related work is discussed as well. We identify and discuss security- and data-privacy protection requirements in detail in Section III. Architecture and protocol flows of our user-centric and cross-sector IdM solution are presented in Section IV. Thereafter we continue to discuss how we met the stated security requirements and comply with data-privacy protection demands. Besides benefits, potential risks are discussed as well. Finally, conclusions are drawn

II. BACKGROUND

A. The Austrian Citizen Card Concept

The Austrian Citizen Card [5] defines a major component within the Austrian e-Government strategy and eID concept. Currently, most Austrian citizen cards are based on smart cards such as bank cards or health insurance cards. However, due to its concept of technology neutrality, the implementation of a citizen card is not limited to smart cards only. A second approach using mobile phones for authentication gets well established at the moment. The concept of this approach has been described in detail by Orthacker et al. [6].

Similar to traditional processes, it's essential to uniquely identify citizens in online processes. Therefore, the citizen card contains a special data structure where the citizen's identity data are stored. These identity data consist of a unique identifier, first name, last name, and date of birth. Additionally, in online governmental processes citizens sometimes need to express a declaration of intent. For this, the signature creation

functionality of the citizen card can be used which are based on a qualified electronic certificate fulfilling the requirements of the EU Signature Directive [3]. Such signatures are legally equivalent to hand-written signatures across the whole EU as stated by the Austrian Signature Law [7].

In Austria, the citizen card concept is legally based upon the so-called e-Government Act [8]. This law constitutes topics such as identification, authentication, delegate management, etc. The most important background part for our work is citizen identification. Each Austrian citizen listed in the Central Residents Register (CRR) is assigned a 12-character (40-bit) unique national identification number, the CRR number Id_{CRR}. This number cannot be directly used in e-Government processes. An encrypted version called *sourcePIN* must be used instead. The sourcePIN is calculated by the SourcePIN Register Authority (a subdivision of the Austrian Data Protection Commission) by encrypting the concatenation of Id_{CRR} and a 1-byte seed value "s" with a 168-bit secret Triple-DES ($3DES_{ADPC}$) key as follows.

$$sourcePIN = 3DES_{ADPC}\ (Id_{CRR} \,||\, s \,||\, Id_{CRR} \,||\, Id_{CRR}) \quad (1)$$

where || denotes the concatenation operation. The resulting 128-bit sourcePIN must only be stored on the citizen card. Due to data privacy legislations it is neither allowed for public sector applications nor for private sector applications to store the sourcePIN or use it directly for identification. Hence, the Austrian e-Government concept foresees identification based on a sectoral model, which on the one hand preserves privacy because the sourcePIN itself cannot be used to track citizens' activities across different administrative sectors and on the other hand still allows unique identification because the sourcePIN is securely derived for each sector using a one-way SHA-1 hash function. The derived identifier is named sector-specific PIN (ssPIN) [9]. The resulting 160-bit ssPIN value is calculated as follows.

$$ssPIN_{(A)} = SHA\text{-}1\ (sourcePIN \,||\, SC_A) \quad (2)$$

where SC_A denotes the two-character administrative sector code of an application of sector *(A)*. Due to the cryptographic one-way derivation it is not possible to re-generate the sourcePIN from a given ssPIN. Moreover, it is not possible to calculate an ssPIN of another sector from a given ssPIN. However, in some cases public authorities belonging to different sectors still may need to exchange data of the same user. For this purpose, the Austrian e-Government Act defines the notion of an *encrypted ssPIN* [10], i.e. a public authority may use an ssPIN of a different administrative sector only in encrypted form.

For supporting user identification and authentication based on the Austrian citizen card, service providers usually integrate the so-called open source IdP module MOA-ID into their applications. This server-side middleware handles the communication with the client-side middleware (CCS) and provides the user identification data to the application in a standardized format. In a first step the user is requested to provide her identity data (identification step). This is achieved through MOA-ID by sending appropriate commands [11] to the CCS, which in turn reads the identification data (sourcePIN, name and date of birth) from the citizen card. MOA-ID then calculates the ssPIN for unique identification at the sectoral online application. In a second step, the user is asked to give her consent to authenticate at the respective application (authentication step). This is done by digitally signing a special text. After that, MOA-ID assembles the retrieved identity information into a certain format (based on SAML [1]) and transfers these data to the corresponding online application.

B. Single Sign-On (SSO)

In many cases, access to services is offered through a web portal where various services of different providers are bundled. In general, the portal does not support a central user repository. Thus, mostly each service provider needs to manage its user data separately. This can lead to a situation at the portal where users want to access several services of different vendors at the same time but have to authenticate at each service provider separately. If the services are protected by username/password schemes, users also tend to use the same password for all services which heavily decreases security.

To avoid such an issue, the concept of *Single Sign-on* (SSO) has been developed. Jan De Clercq defines Single Sign-On as *"the ability for a user to authenticate once to a single authentication authority and then access other protected resources without reauthenticating."* [12] Using SSO, the access to other resources happens automatically, seamlessly, and more or less transparent (depending on the SSO implementation) to the user.

On the one side, Single Sign-On saves time and costs because users just need to run through one authentication process only. Security is usually increased because authentication takes place on a single place which should be particularly protected. Users e.g. do not need to remember several different passwords anymore but can just use a strong one only. However, on the other side this leads to one main disadvantage of Single Sign-On systems: if an attacker figures out the identity and authentication data of the SSO system, she will be able to gain access to all services protected by the SSO system.

C. Related Work

Single Sign-On is not a new topic. Hence, various systems based on different methodological approaches do already exist. This sub-section briefly describes two different ticket-based SSO solutions which are supporting cross-domain SSO.

a) Security Assertion Markup Language (SAML)

SAML [1] is currently the most well-known standard for SSO across multiple domains. SAML specifies an XML-based standard especially designed for the secure exchange of identification, authentication and authorization data. In general, SAML tokens (so-called SAML assertions) contain information on who has authenticated at what time by using which means. Those information including additional user data such as identifiers or other personal properties are exchanged between parties who trust each other.

b) OpenID

OpenID [2] defines a decentralized authentication system for web-based and OpenID enabled services. Users just need to

authenticate once at so-called OpenID providers for accessing multiple protected resources or services. OpenID relies on URL-based identities. Thus, the usernames follow the syntax of URLs. One advantage is that users do not need to rely on a specific OpenID provider but can use the particular provider of their choice.

III. REQUIREMENTS

The Austrian eID concept is mainly used in security- and privacy-sensitive fields of application such as e-Government or e-Banking. Hence, the Austrian eID concept has been designed such that privacy-sensitive data is protected appropriately and can be accessed by authorized parties only as discussed in Section II. Unfortunately, there is often a trade-off between the level of security, privacy protection and the achievable usability. In the Austrian eID infrastructure, this trade-off becomes apparent when users attempt to authenticate at multiple service providers belonging to different sectors. As users are identified by different ssPINs in each sector, separate authentication processes have to be carried out for each sector.

In this paper we therefore propose a Single Sign-On approach that bases on the existing Austrian eID infrastructure. The basic objective of our proposed solution is the preservation of the provided level of security and privacy, and to increase usability at the same time. The SSO solution may under no circumstances violate the requirement for perpetuation of the ssPIN concept. To further improve usability, the applied SSO functionality shall also be completely transparent to the user. This means that the Single Sign-On authentication process must not significantly differ from common eID based authentication processes. Optionally, the user might be notified about the available SSO feature during the authentication process. Due to the continuously growing Austrian e-Government infrastructure, scalability is an important issue, too. Ideally, the Single Sign-On approach to be developed should allow for the seamless integration of new identity providers into an existing SSO enabled infrastructure. The integration of new identity providers therefore requires at least the establishment of trust between the new entity to be integrated and the existing infrastructure and the administrative efforts for integration should be minimal.

In the Austrian e-Government infrastructure, user-centric approaches are followed wherever possible. This basically means that users should always remain in control of their own personal data. For instance, if user related data has to be exchanged between two server components, users should always be aware of personal data being exchanged or transmitted. During the extension of this framework by SSO capability, its user-centric characteristic should be preserved.

Cross-sector applicability, transparency, scalability, and user-centricity have been identified as basic requirements for the SSO solution to be developed. These requirements shall be fulfilled such that usability is improved while at the same time security and privacy protection is preserved. In the following, we introduce the architecture of our solution and show how the identified requirements have been met by our approach.

IV. SSO SECURITY ARCHITECTURE

In this section we describe the architecture and protocol flows of our proposed privacy-preserving cross-sector SSO solution for Austrian citizens.

A. Architecture

Currently, if users want to access two or more applications, which belong to different sectors, they have to authenticate separately at each application. For instance, consider the scenario illustrated in Figure 3. If an online application *(A)* belongs to the sector *(A)*, users have to authenticate at the according MOA-ID *(A)* which protects application *(A)*. MOA-ID *(A)* calculates $ssPIN_{(A)}$ (on the basis of the user's sourcePIN) for sector *(A)* and makes it available for identification at application *(A)*. Since MOA-ID *(A)* is processing $ssPIN_{(A)}$, it is only allowed to run in sector *(A)*. If the same user wants to access another application *(B)* which belongs to sector *(B)*, she needs to authenticate again by running through the citizen card authentication process. Thus, MOA-ID *(B)* protecting application *(B)* calculates $ssPIN_{(B)}$ for identification at online application *(B)*.

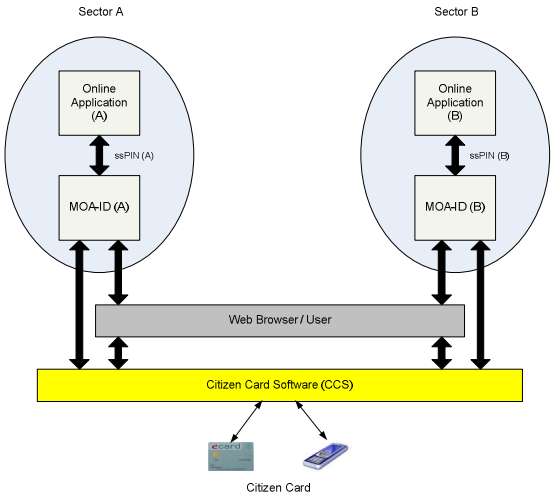

Figure 1. Current Cross-Sector Authentication

Frequent authentication processes actually do not encourage usability. Therefore, we have enhanced MOA-ID in such a way that Single Sign-On can be supported but still keeping the same level of security by using the Austrian citizen card. This means for users the ability – if already successfully authenticated for one sector - to authenticate at applications belonging to other sectors without re-authenticating. For instance, assume a user has been successfully authenticated at application *(A)* via MOA-ID *(A)*. Furthermore, application *(A)* links to applications of other sectors, e.g. the application *(B)* of sector *(B)*. With the help of the MOA-ID SSO enhancements, users are able to seamlessly authenticate at application *(B)* without re-authentication. MOA-ID *(B)* protecting application *(B)* can grant access because an appropriate trust relationship between MOA-ID *(A)* and MOA-ID *(B)* exists. All required authentication and identification data are transferred from MOA-ID *(A)* to MOA-ID *(B)* in a user-centric way. Figure 4 illustrates this Single Sign-On scenario.

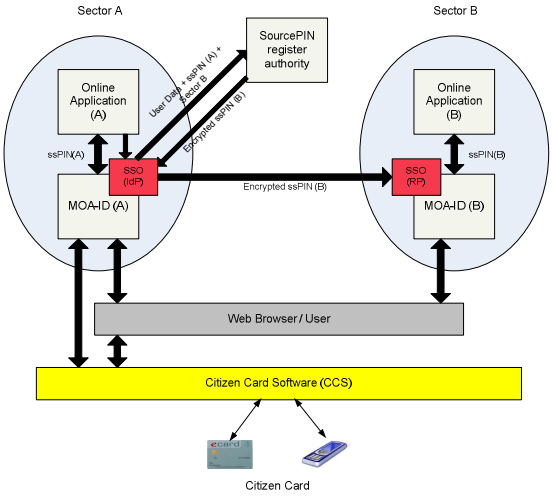

Figure 2. Single Sign-On Cross-Sector Authentication

Redirection from application *(A)* and subsequent identification at application *(B)* requires $ssPIN_{(B)}$ for sector *(B)*. However, during authentication at application *(A)* only $ssPIN_{(A)}$ for sector *(A)* has been calculated. Hence, for seamless authentication at online application *(B)* a prior calculation of $ssPIN_{(B)}$ must take place. This calculation is conducted by using the concept of *encrypted ssPINs*. Encrypted ssPINs are defined by the Austrian E-Government Law [8] to allow applications the processing of ssPINs of foreign sectors without disclosing the actual ssPIN value. An encrypted ssPIN of sector *(B)* is calculated by encrypting the concatenation of a timestamp TS, the sector code SC_B and $ssPIN_{(B)}$ as follows.

$$ssPIN_{enc(B)} = RSA_{pub(B)}(TS \mid SC_B \mid ssPIN_{(B)}) \qquad (3)$$

where $RSA_{pub(B)}$ denotes the official RSA public key of sector *(B)*. Key lengths of public keys must be at least 1024 bits (2048 bit recommended). The timestamp *TS* ensures that each calculated value of $ssPIN_{enc(B)}$ is different and thus prevents the tracking of citizens' activities in a different sector. To calculate $ssPIN_{enc(B)}$ within sector *(A)*, we make use of the SourcePIN Register Authority (SRA). The SRA holds a registry of the public keys of all sectors and provides a web service to transform own ssPINs to encrypted ssPINs of other sectors. This transformation requires as input the user's identity data (first name, last name, date of birth), the $ssPIN_{(A)}$ of sector *(A)*, as well as the desired sector code SC_B of sector *(B)*. In this way, the SRA can search for the user in the central residents register and calculate the user's sourcePIN and $ssPIN_{enc(B)}$, respectively.

B. *SSO Protocol*

The sequence diagram in Figure 3 illustrates our SSO protocol in more detail. The process has four main steps which are further discussed in more detail. Furthermore, we assume that the user has already been successfully authenticated once using her citizen card at MOA-ID *(A)*. For that, we enhanced MOA-ID in such a way that a user's authentication session isn't immediately discarded upon ticket devaluation by the online application.

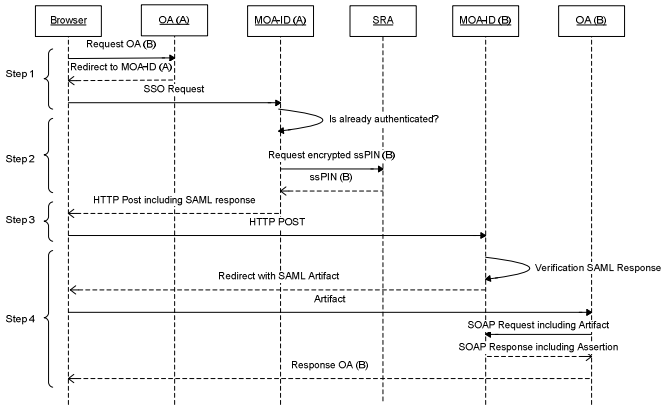

Figure 3. Sequence Diagram

Step 1: In this step, the user wants to access a particular service of sector *(B)* although currently interacting with an application of sector *(A)*. Instead of being directly forwarded to application *(B)* the user is redirected to MOA-ID *(A)* in order to check if she has been already successfully authenticated before, i.e. if the authentication session is still valid. MOA-ID *(A)* further checks if MOA-ID *(B)* and consequently also application *(B)* is trusted.

Step 2: If the requirements of Step 1 are fulfilled, MOA-ID *(A)* submits the user's identification data (name, date of birth), $ssPIN_{(A)}$ and SC_B to the SRA for the calculation of $ssPIN_{enc(B)}$ [13]. The communication with the SRA is secured with Transport Layer Security (TLS) client authentication.

Step 3: In this step the actual SSO process takes place. Since the user has been successfully authenticated before, the information of this previous authentication including $ssPIN_{enc(B)}$ is packed into a SAML assertion and digitally signed. This assertion is based on SAML 2.0 and assembled according to the Web SSO profile. The signed assertion is then conveyed by the user through HTTP-POST to MOA-ID *(B)*. By this assertion MOA-ID *(A)* asserts MOA-ID *(B)* the trustworthiness of the previous authentication at application *(A)*.

Step 4: After having verified the assertion, MOA-ID *(B)* decrypts $ssPIN_{enc(B)}$ with its private key $RSA_{priv(B)}$ and prepares the identification data to be sent to the protected application *(B)*. The communication between MOA-ID *(B)* and application *(B)* is based on the SAML Browser/Artifact Binding 1.0. Although the SAML assertion transmitted between MOA-ID *(A)* and MOA-ID *(B)* is based on SAML version 2.0, the identification data sent from MOA-ID *(B)* to application *(B)* is still included in SAML 1.0 assertions. The reason for that is the support of legacy services because currently most Austrian (governmental) online applications are capable of processing SAML 1.0 assertions only. After this process step, the user is successfully and seamlessly authenticated at application *(B)* without re-authentication at MOA-ID *(B)*. Online applications experience no difference whether users have been authenticated via normal citizen card authentication or via SSO. Hence, legacy applications do not need to modify their authentication environment for supporting SSO.

V. SECURITY AND PRIVACY DISCUSSION

In this section we evaluate if and how the different requirements that have been defined in Section III are met by our proposed solution. We also revisit the security and privacy protection capabilities of the Austrian eID-based authentication framework and analyze if they have been compromised by the applied modifications.

The basic objective of our efforts, i.e. the development of a cross-sector Single Sign-On concept for the Austrian eID infrastructure, has been achieved. As discussed in Section IV and illustrated in Figure 3, the implemented SSO capability requires additional communications between the involved identity providers. To guarantee the confidentiality of the exchanged data, the connection, over which the authentication data is transmitted, has to be secured appropriately. This is achieved by means of TLS encryption and the usage of the HTTPS protocol. It is also important to note that SSO authentication can take place between trusted identity providers only. This is guaranteed by the fact that each identity provider signs the SSO authentication data before transmitting it to another identity provider.

To meet the requirements for cross-sector applicability our SSO solution also requires an interaction between the involved identity provider and the Austrian SourcePIN Register Authority. As the data being exchanged between these entities is privacy-sensitive, again this channel is secured employing approved protocols such as TLS and HTTPs. The protection of the transmitted privacy sensitive data is also strengthened by the fact that the requested ssPIN is encrypted by the Austrian SourcePIN Register Authority using the intended recipient's public key. Furthermore, the applied encryption assures that only the intended recipient is actually able to decrypt the ssPIN. To further improve the usability of the eID-based log-in process, also the requirement for transparency has been considered by our implementation. Basically, neither security nor privacy is actually compromised by a completely transparent SSO authentication process. Nevertheless, we have provided an optional notification message that informs the user that SSO-related authentication data are to be sent to other trustworthy identity providers if desired by the user.

According to the Austrian e-Government policy that recommends the implementation of user-centric approaches, SSO authentication data is exchanged between identity providers via the user's web browser. By employing the SAML HTTP POST binding for this purpose, users remain in control of the data being transmitted to other identity providers. Unfortunately, putting users' web browsers into the communication path also raises new risks such as man-in-the-middle attacks, where the transmitted authentication data can potentially be intercepted. A direct connection path between the two identity providers would minimize this kind of threats. Also the adoption of the so-called *Holder-of-Key Web Browser SSO Profile* [14] could further increase the security of our solution.

VI. CONCLUSIONS

The Austrian eID infrastructure relies on a secure and privacy-preserving concept that makes use of sector-specific identifiers (ssPIN) to identify users. This prevents public agencies and private businesses belonging to different sectors from exchanging and synchronizing collected private data of certain citizens or customers. While this approach improves privacy and security, it cab have various negative effects on the usability of authentication processes.

In this paper thus we have introduced an enhancement of Austrian eID infrastructure core components allowing for secure and privacy-preserving cross-sector SSO user authentications. This has basically been achieved by implementing a secure exchange of ssPINs between trusted identity providers. The applied modifications and improvements do not harm the security and privacy-preservation capabilities of the Austrian eID based authentication framework. At the same time, the developed solution satisfies also the predefined requirements for scalability, transparency, and user centricity.

The practical applicability of our solution has been already been verified. The circular resolution database management system that has been discussed in [15] has been enhanced by our SSO authentication solution in a first piloting phase. So far, no severe issues have been faced. The incorporation of gained experiences of this piloting phase and the integration of our solution in further productive applications is regarded as future work.

REFERENCES

[1] OASIS, „Security Assertion Markup Language (SAML)", http://www.oasis-open.org/committees/security/

[2] OpenID Foundation, http://openid.net/

[3] European Parliament and the Council. Directive 1999/93/ec on a community framework for electronic signatures, December 1999

[4] ARGE Spezifikation MOA, „Spezifikation Module für Online Applikationen – ID", August 2007

[5] H. Leitold, A. Hollosi, and R. Posch, "Security Architecture of the Austrian Citizen Card Concept" in Proceedings of the 18th Annual Computer Security Applications Conference (ACSAC '02)

[6] C. Orthacker, M. Centner, C. Kittl, "Qualified Mobile Server Signature", In: IFIP Advances in Information and Communication Technologies Series (SEC 2010).

[7] Bundesgesetz über elektronische Signaturen (Signaturgesetz - SigG)

[8] Bundesgesetzblatt für die Republik Österreich BGBl. I Nr. 10/2004. The Austrian, E-Government Act. 2004.

[9] A. Hollosi, R. Hörbe, "Bildung von Stammzahl und bereichsspezifischem Personenkennzeichen (bPK)", 2006

[10] O. Ehrenmülller, „Dokumentation zur Entschlüsselung von Fremd-bPK", 2007

[11] Federal Chancellery Austria. The Austrian Citizen Card, http://www.buergerkarte.at/konzept/securitylayer/spezifikation/aktuell/index.en.html, May 2004

[12] J. D. Clercq, "Single Sing-On Architectures" in Infrastructure Security, G. Davida, Eds. InfraSec 2002 Proceedings, vol. 2437, October 2002, pp. 40–58

[13] Ministery of Interior, "Technische Informationen zum SZR", http://portal.bmi.gv.at/ref/portref/szr_technisches.html

[14] H. Lockhart and T. Hardjono, "SAML V2.0 Holder-of-Key Web Browser SSO Profile Version 1.0", OASIS, August 2010

[15] T. Zefferer and T. Knall, "An Electronic-signature Based Circular Resolution Database Management System", In: Proceedings of the 25th Annual ACM Symposium on Applied Computing, 2010, pp. 1840-1845