Using Anonymous Credentials for eID Authentication in the Public Cloud

Bernd Zwattendorfer
E-Government Innovation Center (EGIZ), Graz University of Technology, Inffeldgasse 16a, 8010 Graz, Austria

Keywords: eID, Electronic Identity, Citizen Card, Anonymous Credentials, Privacy, Authentication, Public Cloud.

Abstract: Unique identification and secure authentication are important processes in several security-sensitive areas of applications such as e-Government or e-Health. Within Europe, electronic IDs (eIDs) are the means to securely support these processes. In Austria, the Austrian citizen card is used by citizens for identification and authentication at online applications. Identification in Austria is based on a special data structure including multiple personal attributes stored on the citizen card. However, in the current situation it is only possible to disclose the complete identity of a citizen and not only parts of it. To bypass this issue and to increase privacy, in this paper we propose a security architecture which uses anonymous credentials for Austrian eID authentication to enable minimum/selective disclosure. Due to the use of anonymous credentials, our proposed architecture also allows the migration of important components of the Austrian eID system into a public cloud. A public cloud deployment has several advantages, in particular with respect to scalability and cost savings. While public cloud deployment brings up new issues relating to privacy, the use of anonymous credentials can mitigate these issues as they can ensure privacy with respect to the cloud provider.

1 INTRODUCTION

Unique identification and secure authentication are important processes when access to protected data needs to be regulated. In particular, in security-sensitive areas of applications such as e-Government these processes are essential. For protecting citizen access to public and also private sector applications Austria relies on the Austrian citizen card, the official eID in Austria (Leitold et al., 2002). The Austrian citizen card is capable of unique identification and qualified signature creation, which is further used for authentication at service providers (applications).

Using the Austrian citizen card, identification is based on a special data structure stored on the citizen card. In the current situation it is only possible to disclose the complete identity of a citizen (the complete special data structure) to a service provider. However, in some situations it might be favorable to disclose only some parts or even just derived attributes from this identity (e.g. age instead of date of birth).

To achieve this, in this paper we propose a security architecture which uses anonymous credentials for Austrian eID authentication. Anonymous credentials particularly preserve users' privacy and ensure only minimum data disclosure, hence it's not necessary for citizens to reveal their complete identity anymore. Moreover, our proposed architecture also allows the migration of important components of the Austrian eID system into a public cloud. Comparing all cloud deployment models, the public cloud offers the highest benefits in terms of scalability and cost savings with respect to all other cloud models (Alford, 2009). However, the public cloud also has the highest privacy concerns (Pearson and Benameur, 2010). Deploying the Austrian eID system in a cloud-based setting could take advantage of the public cloud benefits, but requires the need of privacy preservation at the same time. This can be achieved by adopting our proposed architecture, which is able to ensure privacy with respect to the cloud provider under the assumption that the cloud provider is acting *honest but curious* (Nuñez and Agudo, 2014).

The paper is structured as follows. Section 2 briefly describes the Austrian citizen card concept. Section 3 elaborates on anonymous credentials and overviews different technologies. In Section 4 we describe our proposed architecture on using anonymous credentials for a public cloud deployment of the Austrian eID system, explain an identification and authentication process in detail, suggest technologies for implementing the proposed architecture, and discuss it in Section 5. The paper is round up by a drawing conclusions in Section 6.

Zwattendorfer B..
Using Anonymous Credentials for eID Authentication in the Public Cloud.
DOI: 10.5220/0005494901560163
In *Proceedings of the 11th International Conference on Web Information Systems and Technologies* (WEBIST-2015), pages 156-163
ISBN: 978-989-758-106-9
Copyright © 2015 SCITEPRESS (Science and Technology Publications, Lda.)

2 THE AUSTRIAN eID SYSTEM

The Austrian eID system, handling in particular unique identification and secure authentication of citizens, constitutes a main pillar within the Austrian e-Government infrastructure. The core component of the Austrian eID system is the so-called Austrian citizen card (Leitold et al., 2002). In the following subsections we briefly describe the Austrian citizen card concept and explain how the Austrian citizen card is used for identification and authentication at online applications.

2.1 The Austrian Citizen Card Concept

The Austrian citizen card constitutes the core component of the Austrian eID system. The Austrian citizen card is rather a concept than one concrete implementation, hence different technological approaches for implementing a citizen card may exist. Currently, two implementations are rolled-out in the field, one relying on smart cards and the other one using a mobile phone. In more detail, the citizen card has three main functions as many other European eIDs according to (Arora, 2008):

1. Unique identification
2. Secure authentication
3. Qualified signature creation

Unique identification of the Austrian citizen card is based on a special data structure (so-called *identity link*), which is directly stored on the card. This special data structure contains personal data for identifying a citizen. The personal data consists of a unique identifier, first and last name, and date of birth of the citizen. To ensure integrity and authenticity of the identity link, it is digitally signed by a trusted authority, the so-called SourcePin Register Authority.

Unique identification at online applications is mainly based on the unique identifier included in the identity link, which is called *sourcePIN*. The sourcePIN is solely stored on the citizen card and must not be stored in any other location according to Austrian law (Federal Chancellery, 2008). Hence, due to these legislative restrictions and further privacy reasons, for identification at online applications the sourcePIN is not used directly but rather a derived identifier by using a one-way hash function. Derivation of this identifier, which is called sector-specific PIN - *ssPIN*), is based on the governmental sector (e.g. tax, finance, etc.) the online application belongs to.

Secure authentication at online applications is based on creating a qualified electronic signature. By verifying the created signature at the online application, the citizen can prove the authenticity of her identity data. However, qualified signature creation can be seen as separate process for the Austrian citizen card. Hence, the creation of qualified electronic signatures, which are equivalent to handwritten signatures according to the EU signature directive (European Parliament and Council, 1999), defines the third main function of the citizen card.

2.2 Identification and Authentication at Online Services

Identification and authentication at Austrian online applications using the Austrian citizen card is based on the following architecture illustrated in Figure 1.

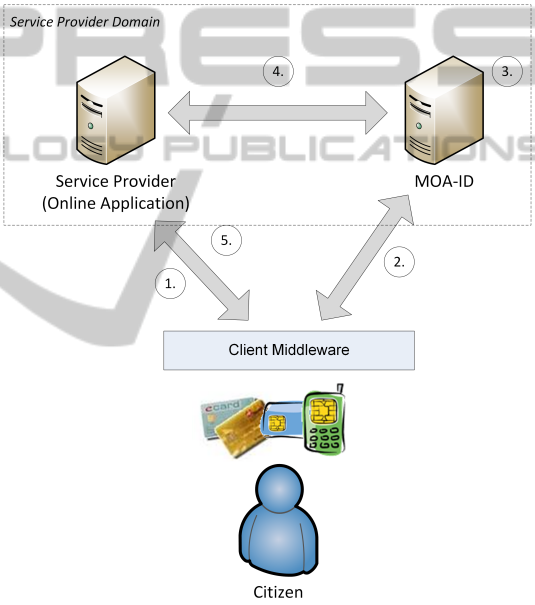

Figure 1: The basic Austrian eID system Architecture.

The following entities are involved in an identification and authentication process:

Citizen. A citizen wants to access a protected resource at the service provider.

Service Provider. The service provider is operated by the public or the private sector and offers protected services to citizens .

MOA-ID. MOA-ID (Lenz et al., 2014) is an open source software module which enables the usage of the Austrian citizen card for accessing protected services at the service provider. In this context, MOA-ID can be seen as identity information provider according to (ISO/IEC JTC 1, 2011). On the one hand, MOA-ID communicates with the

client middleware to access citizen card functionality. On the other hand, MOA-ID provides the service provider identity and authentication information of the citizen in a structured way, which is based on SAML (Cantor et al., 2009). Regarding the operation of MOA-ID, the current Austrian eID system foresees a local (de-centralized) deployment of MOA-ID in every service provider's domain.

Client Middleware. The client middleware can be a piece software either installed locally in the citizen's domain or on a remote server. In fact, the client middleware is an implementation of an abstract layer (Hollosi et al., 2014). This layer allows accessing citizen card functionality in a standardized way without the need of knowing any details on the underlying citizen card implementation.

According to Figure 1, an identification and authentication process using this architecture comprises the following steps:

1. A citizen wants to access a certain protected service at the service provider. Assuming that the citizen is not authenticated yet, the service provider sends an authentication request to MOA-ID.
2. MOA-ID verifies this authentication request and initiates the authentication process by invoking the citizen's client middleware. In a first step, the citizen's identity link is read and verified from the client middleware and the citizen card respectively. In a second step, the creation of a qualified electronic signature from the client middleware is requested by MOA-ID. The received signature is then verified by MOA-ID again.
3. Following the sector-specific identification concept outlined in the previous section, MOA-ID derives the sourcePIN extracted out of the identity link according to the sector the service provider belongs to. This results in the generation of the ssPIN.
4. Finally, MOA-ID puts all identification and authentication data into a standardized data structure (SAML assertion) and transmits it to the service provider.
5. Based on the received data the service provider can decide to either grant or deny access.

3 ANONYMOUS CREDENTIALS

Anonymous credential systems allow authentication of users based on authentic anonymous attributes. Hence, only a certain attribute or a part of an identity and not the complete identity must be revealed during an authentication process. For instance, anonymous credentials allow authentication based on a certain age, without revealing the full date of birth of the authenticating user. Anonymous credential systems are not particularly new (Brands, 2000; Camenisch and Lysyanskaya, 2001), however, in the past years they transform from theoretical and scientific concepts to practically applicable solutions.

Basically, anonymous credentials can be differentiated into one-show (Brands, 2000) and multi-show credentials (Camenisch and Lysyanskaya, 2001). Using one-show anonymous credentials, always the same mathematically computed attribute value is disclosed to a verification entity. Due to that, persons might be somehow linkable, since the re-occurring attribute value allows recognition over several authentication processes. In contrast to that, when disclosing a mutli-show credential to a verifier, for every disclosure always a different mathematical attribute value is calculated, which avoids linkability. In the following, we briefly introduce the actual most important anonymous credential systems.

3.1 U-Prove

U-Prove[1] constitutes an anonymous credential system invented by (Brands, 2000), which is further developed and improved by Microsoft. The central component of U-Prove is a so-called U-Prove Token, which includes authentic and cryptographically protected attributes. This U-Prove token is used during interactions with a service provider for proving certain attributes (Paquin, 2013). The U-Prove Token and its included attributes are thereby verified by a service provider. U-Prove Tokens are usually issued to and for a user by a trustworthy entity (issuer), which verifies the authenticity of claimed user attributes before they are stored in the U-Prove Token.

Revocation of issued U-Prove Tokens is done by using blacklists. Usually, a unique identifier is encoded into an issued U-Prove Token, which is put on the blacklist if the token needs to be revoked. U-Prove Tokens can be revoked either by the user herself or by a service provider.

The main features of U-Prove are unlinkability and selective attribute disclosure. In that case, unlinkability means that there exists no relationship between two U-Prove Tokens, which have been issued to one and the same user. Nevertheless, users - even anonymous – are still linkable when using just one U-Prove Token at different service providers. The reason is

[1] http://research.microsoft.com/en-us/projects/u-prove/

that always the same mathematical value is disclosed to the service provider, which makes U-Prove a one-show credential system. However, users are still able to decide themselves which attributes should be disclosed to a service provider and which should not.

3.2 Idemix

Identity Mixer[2] (Idemix) is an anonymous credential system developed by IBM. Similar to U-Prove, a user gets issued a credential containing different attributes from an issuer, which asserts the authenticity of the attributes. If one of these attributes is needed as proof for authentication at a service provider, the issued credential is transformed into a new credential, which only contains a subset of attributes to be used for authentication at the service provider. Thereby, the user can convince the service provider that she possesses certain attributes or fulfills certain properties without revealing her complete identity. In contrast to U-Prove, such a credential transformation can be carried out any number of times and the user still stays unlikable. Hence, Idemix can be seen as a multi-show anonymous credential system.

Revocation in Idemix - in contrast to U-Prove - is mostly based on whitelists. If a user needs to verify that her credential has not been revoked, she just needs to prove that a certain identifier of the credential is listed on the whitelist. However, a couple of other revocation mechanisms exist in Idemix, e.g. also blacklists. An overview of different revocation mechanisms for Idemix credentials is given by (Lapon et al., 2011).

3.3 ABC4Trust

ABC4Trust[3] (Attribute-based Credentials for Trust) was an EU co-funded project of the framework programme 7, which was lasting for 4 years and ended in 2014. The aim of ABC4Trust was the development and piloting of a framework, which is capable of combining different anonymous credential systems. Currently, ABC4Trust supports in its framework U-Prove and Idemix as underlying technologies. The following Figure 2 illustrates the general architecture of the ABC4Trust framework and its interactions between involved entities (Camenisch et al., 2012).

[2]http://idemix.wordpress.com/

[3]https://abc4trust.eu/

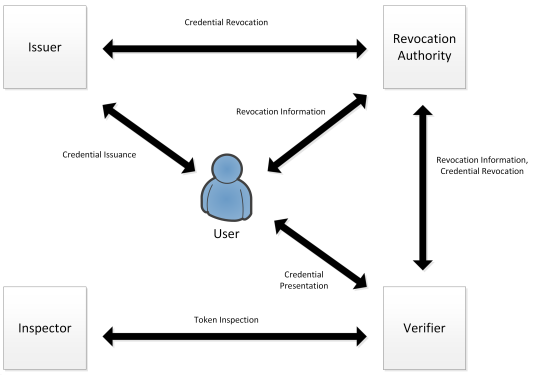

Figure 2: ABC4Trust Framework Architecture. (Camenisch et al., 2012)

4 USING ANONYMOUS CREDENTIALS FOR PUBLIC CLOUD DEPLOYMENT

In the following sub-sections we explain how the Austrian eID system can be made more privacy-friendly by using anonymous credentials and why it is possible to deploy the eID system in a public cloud.

4.1 Motivation

Currently, the Austrian eID system requires the deployment of MOA-ID in every service provider's domain. While this current deployment approach in fact ensures high scalability, having a centralized deployment approach may be advantageous. Having a single central instance would take away much burdensome work from service providers (e.g. installation and deployment of MOA-ID, maintenance efforts, etc.). In addition, during an authentication process citizens would always be presented the same user interface of one central MOA-ID instance instead of always different user interfaces of multiple MOA-ID instances.

A central MOA-ID instance operated under normal settings would be less scalable than the decentralized approach. Nevertheless, this scalability issue could be easily mitigated by moving MOA-ID into a public cloud, which provides the best advantages in terms of scalability. However, a move of a trusted service such as MOA-ID into a public cloud brings up new obstacles, particularly relating to privacy (Pearson and Benameur, 2010). This is now where anonymous credentials come into play, which have strong privacy capabilities.

In the following we present an architecture on how the Austrian eID system can be securely moved into

the cloud by still preserving citizen's privacy with respect to the cloud provider operating MOA-ID.

4.2 Architecture

In this section an architectural design is presented on how the Austrian eID system can be moved into a public cloud by using anonymous credentials. Applying this architecture, the main advantage for citizens is that it is not necessary to reveal their complete identity to MOA-ID and subsequently the service provider as it is done now. To achieve this, the Austrian citizen card and its containing attributes of the identity link must be modeled as anonymous credentials. This can be seen as prerequisite when applying the following cloud-based architecture. Figure 3 illustrates this architecture. From the general architectural point of view, there are no big differences to the existing architecture in Figure 1. However, one new component is added (Revocation Authority), which will be queried during the identification and authentication process.

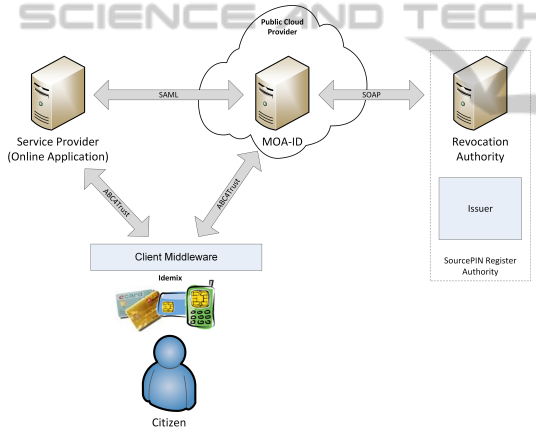

Figure 3: Cloud-based Architecture using Anonymous Credentials.

Using the proposed architecture, the citizen card supports the functionality of selective attribute disclosure because the citizen card is modeled based on anonymous credentials now, which are still issued by the trusted SourcePIN Register Authority. Verification of the validity of citizens credentials is done by MOA-ID. To do that, MOA-ID contacts on-the-fly the revocation authority (similar to requesting revocation information for traditional X.509 certificates using OCSP (RFC 6960, 2012)). If the credential has not been revoked, access for citizens to the service provider can be granted. In more detail, proofs of credentials are exchanged between the citizen and the service provider.

The following entities are involved in this architecture. A *Citizen* wants to access a protected service using her citizen card. This time, the attributes of the citizen card are modeled as anonymous credentials. The *Service Provider* requires just a minimum of data for authentication, e.g. the citizen's age. *MOA-ID* takes over the identification and authentication process for the service provider. In particular, MOA-ID does the revocation checking. The *Revocation Authority* stores a blacklist according to (Lapon et al., 2011). The blacklist contains a list on all revoked credentials. The revocation authority is operated by the *SourcePIN Register Authority*. In our setting, the SourcePIN Register Authority is also acting as *Issuer* and also takes over the issuance of anonymous credentials. The *Client Middleware* regulates access to credentials on the citizen card. In addition, the client middleware is responsible for any credential transformation.

4.3 Used Technologies

In the following we briefly describe the technologies which are feasible for implementing the architecture.

Idemix. Idemix was selected as a possible anonymous credential system because it is a multi-show credential system, supported by ABC4Trust, and Java libraries are freely available. When implementing our architecture, Idemix should be used for modeling the Austrian citizen card and its attributes as anonymous credentials.

Idemix supports different approaches for revocation checking (Lapon et al., 2011). In this concrete architecture we rely on verifiable encryption (Lapon et al., 2011) in combination with blacklists. Verifiable Encryption means that a citizen can actually proof an attribute although the attribute is encrypted. In our architecture, a unique identifier of the citizen's credentials is encrypted. Thereby, the citizen can proof the correctness of the unique identifier without disclosing the identifier to a verifier.

ABC4Trust. ABC4Trust will be used as XML-based communication protocol between service provider and client middleware, and MOA-ID and client middleware. Thereby, between both entities a presentation policy and a presentation token according to the ABC4Trust specification will be exchanged. The presentation policy defines which attributes or credentials, respectively, are required from the citizen and need to be read out from the citizen card via client middleware. The client middleware calculates and creates the requested credentials and returns them included in a presentation token to the requesting entity.

SAML. The Security Assertion Markup Language (SAML) (Cantor et al., 2009) is an XML-based framework for the secure exchange of identification and authentication data. The current MOA-ID implementation already relies on SAML for the secure data exchange between MOA-ID and the service provider. Hence, we will also rely on SAML for this communication flow. However, in our proposed scenario no real data will be transferred but rather revocation information.

SOAP. SOAP (W3C, 2007) is an XML-based protocol for simple data exchange between entities using web service technology. SOAP messages can include arbitrary XML documents for message transfer. For our approach, a web service was defined to exchange revocation information between MOA-ID and the revocation authority.

4.4 Process Flow

In this sub-section the detailed identification and authentication process using the proposed architecture and technologies is described. The individual steps are illustrated in the sequence diagram in Figure 4.

The process steps are as follows:

1. A citizen wants to access a protected resource of an online application (service provider).
2. Since we assume that the citizen has not successfully authenticated yet, the service provider sends a SAML AuthnRequest to MOA-ID.
3. MOA-ID verifies the SAML AuthnRequest and creates a presentation policy, which requests from the user that her credentials are valid and not revoked. The presentation policy is transmitted by MOA-ID to the client middleware.
4. To prove that the citizen's credential is not revoked, verifiable encryption (VE) as revocation mechanism will be used. The unique identifier of the credential will be encrypted by the user (VE-Attribute) and together with the actual credential included into a presentation token. The presentation token is then returned to MOA-ID.
5. MOA-ID extracts the VE-Attribute out of the presentation token and verifies it. However, MOA-ID can only verify the validity, more precisely the calculated proof, of the VE-Attribute but not its value, since the value is encrypted.
6. To verify the validity of the citizen's credential, the VE-Attribute is transmitted via SOAP web service to the revocation authority.
7. The revocation authority decrypts the VE-Attribute[4] and extracts the containing unique identifier of the citizen's credential.
8. The revocation authority checks whether the identifier is listed on its maintained blacklist. All credential identifiers, which are on the blacklist, are revoked.
9. The revocation authority returns the revocation information as a web service response. More precisely, it is sufficient to just return a boolean value indicating whether the credential is revoked or not. In our presented scenario we assume that the presented credential is still valid.
10. MOA-ID includes the presented citizen's credential as well as the corresponding revocation information into a SAML assertion. The SAML assertion is wrapped in a SAML response, which is signed.
11. MOA-ID returns the SAML assertion (SAML response) to the service provider, as it is done in the current Austrian eID system architecture.
12. The service provider verifies the SAML response and SAML assertion.
13. The service provider assembles a presentation policy (including the requested attributes (proofs) required for authentication) and sends it to the client middleware. For instance, this could be the age of the citizen.
14. The client middleware calculates the proofs according to the presentation policy and transmits them together with the credential wrapped in a presentation token to the service provider.
15. The service provider verifies the presented attributes/proofs. Additionally, it is checked whether the credential presented to the service provider in this step and the credential included in the SAML assertion, which has been previously presented to MOA-ID in step 4, are identical.
16. If both verification processes are successful, the service provider can grant the citizen access to the protected resource.

5 DISCUSSION

In this section we briefly discuss our architecture according to selected criteria.

[4]The revocation authority is able to decrypt the VE-Attribute since it is part of the SourcePIN Register Authority, which was responsible for credential issuance.

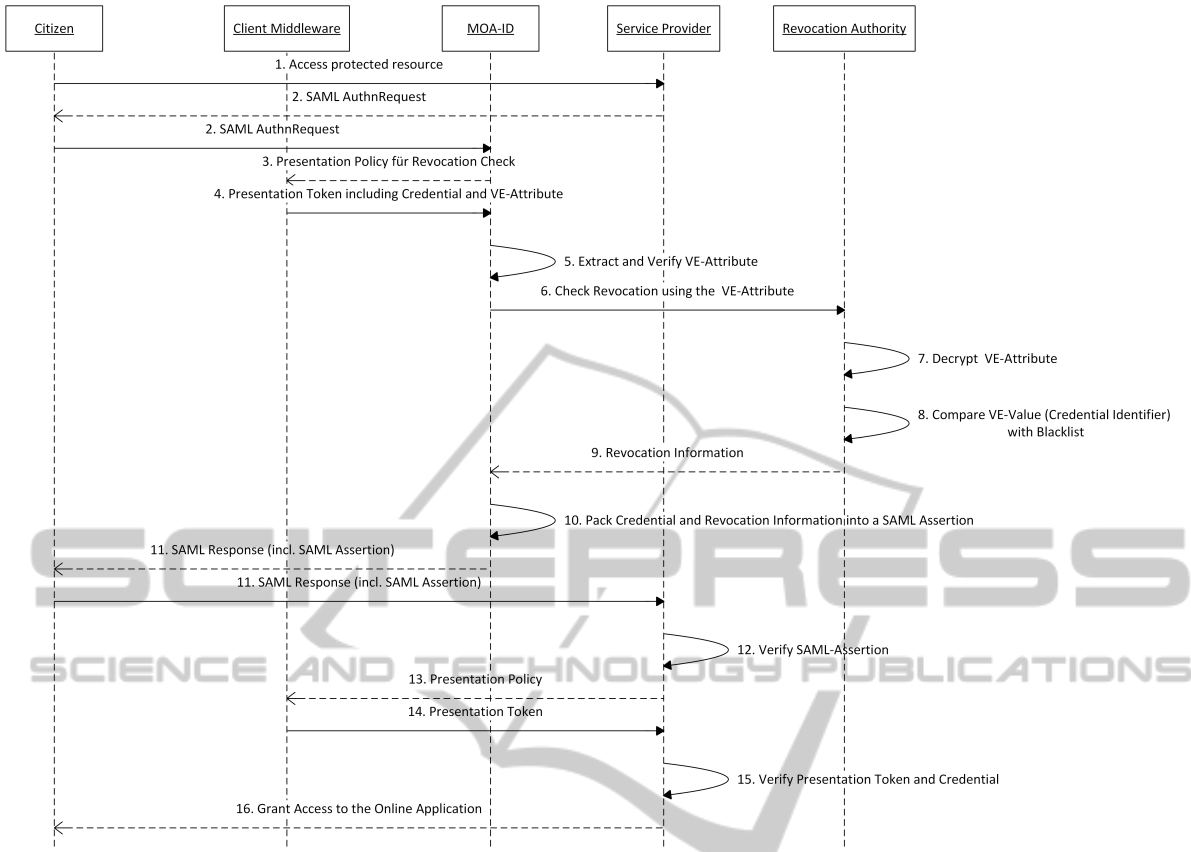

Figure 4: Identification and Authentication Process using Anonymous Credentials for the Austrian eID.

Re-use of Existing Infrastructure. The use of anonymous credentials requires a complete exchange of the identity link since a completely different technology is used. Sector-specific PINs (ssPINs) can be either modeled for all sectors as credential attributes or by using scope-exclusive pseudonyms (Camenisch et al., 2011), which are supported by ABC4Trust. Additionally, both MOA-ID and the service provider need to support the communication protocol (presentation policy and token exchange) of ABC4Trust.

Compliance to the Current Process Flow. The process flow described in Figure 4 using anonymous credentials is a bit different to the process flow of the current situation as illustrated in Figure 1. In our proposed architecture MOA-ID just verifies if a presented credential is revoked or not. The actual verification of attributes and corresponding proofs is done by the service provider.

Scalability. Revocation checking of anonymous credentials is very complex and computational intensive, especially for multi-show credentials such as Idemix. In particular, for a high number of users – such as the Austrian population – computation power demand increases. However, a movement of certain components in the cloud (e.g. MOA-ID) can lower this burden.

Practicability. Proof computation for certain attributes in multi-show credential systems is also very computational intensive (Lapon et al., 2011). According to our architecture, this is done on the client middleware. Hence, due to that there may be longer waiting times during the authentication process.

Extensibility. Extensibility heavily depends on the option chosen for modeling sector-specific PINs. If every ssPIN is modeled as separate attribute in the credential, then any additional sector or ssPIN would require a new issuance of the citizen's credential. In contrast to that, if sector-specific PINs are modeled using the scope-exclusive pseudonym approach as described in (Camenisch et al., 2011), a similar concept as it is done is available. Scope-exclusive pseudonyms can be seen similar to the current approach having a sourcePIN and then deriving ssPINs based on different sectors.

SCITEPRESS
SCIENCE AND TECHNOLOGY PUBLICATIONS

Changes in the Client Middleware. For using anonymous credentials the complete functionality of the client middleware needs to be changed. On the one hand, the client middleware needs to deal with anonymous credentials stored on an underlying token and, on the other hand, needs to implement the ABC4Trust protocol for communication.

Trust in MOA-ID. Applying the proposed architecture, MOA-ID requires no full trust. MOA-ID never sees any personal citizen data in plain. The only data MOA-ID sees is the citizen's credential but not its included attributes. Hence, MOA-ID can be easily deployed in a public cloud. However, our assumption is based on the *honest but curious* cloud attacker model, which means that the cloud provider works correctly but may want to inspect processed data.

6 CONCLUSIONS

Anonymous credentials are a valuable technology to protect citizen's privacy. One of the main features is unlinkability, avoiding user tracking during multiple different identification and authentication processes. In addition, anonymous credentials allow the disclosure of only a subset of a complete identity still in an authentic fashion. Moreover, even derived attributes can be used for authentication (e.g. age instead of date of birth). This makes anonymous credentials also interesting in the eID context.

In this paper we proposed an architecture showing how anonymous credentials can be integrated into the Austrian eID system. Thereby, anonymous credentials can be used for identification and authentication at service providers, still following the existing privacy concept based on sector-specific identifiers. Moreover, the proposed architecture even allows a deployment of MOA-ID in a public cloud, enabling higher scalability end elasticity features. In addition, concrete technologies were identified for a possible upcoming implementation. The implementation can be considered as future work.

An implementation of the proposed architecture can clearly show its practicability. The main bottleneck for that might be the client middleware, which needs to run complex and power intensive computations for credential proof generation. A detailed analysis of an implementation would deliver deeper insight if citizens loose usability in terms of performance when using anonymous credentials. Nevertheless, for the near future anonymous credentials are a valuable and promising means for ensuring data protection and privacy when applied in an eID context.

REFERENCES

Alford, T. (2009). The Economics of cloud computing. *Booz Allen Hamilton*.

Arora, S. (2008). National e-ID card schemes: A European overview. *Information Security Technical Report*, 13(2):46–53.

Brands, S. A. (2000). *Rethinking Public Key Infrastructures and Digital Certificates - Building in Privacy*. PhD thesis, MIT.

Camenisch, J., Krontiris, I., Lehmann, A., Neven, G., Paquin, C., and Rannenberg, K. (2012). H2.1-ABC4Trust Architecture for Developers.

Camenisch, J., Krontiris, I., Lehmann, A., Neven, G., Paquin, C., Rannenberg, K., and Zwingelberg, H. (2011). D2.1 Architecture for Attribute-based Credential Technologies Version 1.

Camenisch, J. and Lysyanskaya, A. (2001). An efficient system for non-transferable anonymous credentials with optional anonymity revocation. In Pfitzmann, B., editor, *EUROCRYPT*, pages 93–118.

Cantor, S., Kemp, J., Philpott, R., and Maler, E. (2009). Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2 .0.

European Parliament and Council (1999). DIRECTIVE 1999/93/EC on a Community framework for electronic signatures.

Federal Chancellery (2008). The Austrian E-Government Act. *Austrian Federal Law Gazette I*, 7:1–11.

Hollosi, A., Karlinger, G., Rössler, T., and Centner, M. (2014). Die österreichische Bürgerkarte.

ISO/IEC JTC 1 (2011). ISO/IEC 24760-1:2011 - A framework for identity management - Part 1: Terminology and concepts.

Lapon, J., Kohlweiss, M., Decker, B. D., and Naessens, V. (2011). Analysis of Revocation Strategies for Anonymous Idemix Credentials. In *CMS*, pages 3–17.

Leitold, H., Hollosi, A., and Posch, R. (2002). Security architecture of the Austrian citizen card concept. In *ACSAC*, pages 391–400.

Lenz, T., Zwattendorfer, B., Stranacher, K., and Tauber, A. (2014). Identitätsmanagement in Österreich mit MOA-ID 2.0. *eGovernment Review*, 13:20–21.

Nuñez, D. and Agudo, I. (2014). BlindIdM: A privacy-preserving approach for identity management as a service. *International Journal of Information Security*, pages 1–17.

Paquin, C. (2013). U-Prove Cryptographic Specification V1.1.

Pearson, S. and Benameur, A. (2010). Privacy, Security and Trust Issues Arising from Cloud Computing. In *IEEE CloudCom*, pages 693–702.

RFC 6960 (2012). X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP.

W3C (2007). SOAP Version 1.2 Part 1: Messaging Framework (Second Edition).

SCITEPRESS SCIENCE AND TECHNOLOGY PUBLICATIONS