Foreign Identities in the Austrian E-Government

Mario Ivkovic, Klaus Stranacher

Foreign Identities in the Austrian E-Government

Mario Ivkovic and Klaus Stranacher

E-Government Innovation Center (EGIZ), Austria,
mario.ivkovic@egiz.gv.at, klaus.stranacher@egiz.gv.at,
WWW home page: http://www.egiz.gv.at

Abstract. With the revision of the Austrian E-Government Act [8] in the year 2008, the legal basis for a full integration of foreign persons in the Austrian e-government, has been created. Additionally, the E-Government Equivalence Decree [1] has been published in June 2010. This decree clarifies which foreign electronic identities are considered to be equivalent to Austrian identities and can be electronically registered within the Austrian identity register. Based on this legal framework a concept has been developed which allows non-Austrian citizens to log in to Austrian online administrative procedures using their foreign identity. A solution resting upon this concept has been developed and successfully tested. This solution has become operative in July 2010.

Keywords: E-Government, Interoperability, Electronic Identities

1 Introduction

Electronic identities (eID) are gaining more and more importance and are a fundamental component of many e-government applications. Due to the mobility of citizens, cross-border interoperability in the European eID landscape has become a key topic. Based on the Directive 1999/93/EC of the European Parliament for digital signatures [7], Member States have developed individual and partly diverging e-government strategies and solutions. Thus, cross-border interoperability turned out to be a challenging issue.

A project dealing with this challenge is STORK (Secure idenTity acrOss boRders linKed), an ICT Policy Support and Competitiveness and Innovation Program (CIP) of the EU with the aim "to establish a European eID Interoperability Platform that will allow citizens to establish new e-relations across borders, just by presenting their national eID"[1]. The results of the work described in this paper, are presently being integrated into the Austrian STORK implementation.

The rest of this paper is structured as follows. The next sub section outlines the Austrian eID concept. The second section gives an overview about the legal basis for foreign identities in Austria. The next section presents an approach for the integration of foreign eIDs into the Austrian e-government. This includes the login to Austrian online administrative procedures as well as the electronic

[1] https://www.eid-stork.eu/

registration in the Austrian identity register. Based on this approach existing components have been extended and new components developed. Therefore the fourth section comprises the implementation. In the last section, we finalize the paper with some conclusions.

1.1 Identification in the Austrian E-Government

In the following sections we give an overview about identification and authentication in the Austrian e-government. Legal basis for identification in Austria is the Austrian E-Government Act[8].

SourcePIN All persons that are registered in Austria (having a permanent or a non-permanent residence in Austria) are listed in the Central Register of Residence (CRR). To each person in this register a unique number, the CRR number[2], is assigned. Due to data protection laws it is not allowed to use this CRR number for e-government applications. Therefore, the so-called *SourcePIN*, which is derived from the citizen's CRR number by using strong cryptographic means (Triple-DES encryption), has been introduced. The SourcePIN may only be stored on a Citizen Card and is thus under the sole control of the citizen. However, even the SourcePIN may never directly be used as identifier in e-government services. Instead, a sector-specific personal identifier has to be derived from the SourcePIN.

For people who want to use Austrian e-government applications but do not have a residence in Austria, the Supplementary Register for natural persons has been established. Similar to the CRR number, all persons in the supplementary register have a unique number. This number is then used to derive a SourcePIN for natural persons without a residence in Austria.

Sector specific PIN From the very beginning data protection was an integral component of the Austrian e-government strategy. Therefore, the use of cross-departmental identifiers has been avoided. Rather than using the SourcePIN directly, sector specific PINs that are derived from the SourcePIN (applying cryptographic hash functions), must be used. A sector specific PIN (ssPIN) in contrast to a SourcePIN may be stored for further processing. With ssPINs it should be prevented to link a person across different administrative procedures from different departments.

Citizen Card The Citizen Card is an essential part of the Austrian e-government strategy. A Citizen Card is used for unique identification and authentication of citizens in online procedures of the public administration.

In the Austrian E-Government Act[8] a Citizen Card is defined as a logical unit independent of its technical implementation, which combines a qualified

[2] http://www.epractice.eu/en/cases/crraustria

electronic signature with an *Identity Link*. The Identity Link provides a means for identification by linking a qualified certificate with the citizen's SourcePIN.

A Citizen Card can be e.g. a smart card, a mobile phone, or any other device fulfilling the following requirements:

Electronic Signature: A Citizen Card must support qualified electronic signatures as defined in the Austrian Signature Act [2]. Therefore, at least one certificate, which is used for the creation of a qualified electronic signature, is stored on a Citizen Card. Additionally, a further certificate that can be used for signature creation or data encryption may be stored on a Citizen Card.

Identification: With the Identity Link, an XML structure containing the SourcePIN, it is possible to uniquely identify a citizen in an e-government procedure.

Data Storage: A Citizen Card must provide data storage divided into so-called *Info Boxes*. In one of the Info Boxes, the above mentioned Identity Link is stored.

The Identity Link uniquely assigns a Citizen Card to a citizen. This is done by signing an XML structure that contains the citizen's public key(s) and the SourcePIN. The signature is created by the SourcePIN Register Authority[3]. By doing this, the public keys are unambiguously linked to a particular person.

Citizen Card Environment The Austrian e-government strategy introduced the concept of a Citizen Card Environment (CCE) in order to ease the access to a Citizen Card. The CCE, also referred to as Citizen Card Software (CCS), is thus the middleware between e-government applications and Citizen Cards. A CCE offers functionalities for electronic signature creation and verification, data encryption and decryption, and provides access to the Info Boxes. Currently several different forms of CCEs are available, ranging from software applications running on a client computer to Java-Applets embedded in an e-government web site[4].

Basic Services In order to kick-start e-government in Austria, the Austrian Federal Chancellery has developed some software components, called Modules for Online Applications (MOA-Modules), which offer useful basic functionalities for e-government application operators. The MOA-Modules are open source and can be used free of charge. At the present time the following modules are available:

MOA-SS: This module provides functionalities for the creation of electronic signatures. Supported are XML signatures according to XMLDSIG [4].

[3] The SourcePIN Register Authority is an authority conducted by the Austrian Data Protection Commission, http://www.stammzahlenregister.gv.at/

[4] http://www.buergerkarte.at/en/index.html

MOA-SP: This module offers functionalities for the validation of electronic signatures. Supported is the validation of XMLDSIG signatures as well as CMS signatures [5].

MOA-ID: This module provides means for secure identification and authentication of citizens within e-government applications. The unique identification is achieved by reading the Identity Link and the creation of a qualified signature.

2 Foreign Identities

In the year 2008 the Austrian E-Government Act [8] has been amended. With this revision the acceptance of foreign identities has been enabled. §6(5) states:

> Data subjects who are not registered in the Central Register of Residents nor in the Supplementary Register may be entered in the Supplementary Register in the course of an application for the issue of a Citizen Card without proof of the data in accordance with paragraph 4 if the application is provided with a qualified electronic signature which is linked to an equivalent electronic verification of that person's unique identity in his or her country of origin. The Federal Chancellor shall lay down by Order further conditions for equivalence. The SourcePIN Authority shall, upon application of the data subject, provide the SourcePIN of the data subject directly to the Citizen Card enabled application where the official procedure is carried out. The SourcePIN may be used by the SourcePIN Register Authority only to calculate ssPINs."

As a result foreign electronic identities are fully integrated in the Austrian e-government in case they are associated with qualified electronic signatures. As a requirement, if the citizen is not already registered in the Central Register of Residents (person has a registered residence in Austria), the foreign citizen must be registered in the Supplementary Register. The SourcePIN Authority is then able to derive a SourcePIN. So a temporary Identity Link, temporary because this Identity Link is repeatedly generated and not permanently stored on an eID card, can be forwarded to an e-government application. The e-government application uses the Identity Link only for the computation of the sector specific PIN.

With §6(5) of the Austrian E-Government Act the possibility to register a person electronically has been given. For the concrete usage it must be determined which electronic identity is considered to be equivalent. This is done by the so called E-Government Equivalence Decree [1]. The decree has been published in June 2010. Thereby it is determined which identification attributes from a foreign identity must be used. Table 1 gives an overview about the electronic identities which are considered to be equivalent. All this countries have in common that they have a unique identifier which can be used for identifying persons. Depending on the country this number is e.g. the tax number, social

insurance number, health care user number or the personal identification number. Usually this identifier is stored in the certificate (as serial number), except Liechtenstein. In this case a national register query must be performed to get the national identifier (see section 4.2 for details).

Country	Unique identifier in the country of origin	Name of the eID card
Belgium	RRN number (Rijksregister-Registre National)	Belgian Personal Identity Card (Elektronische identiteitskaart BELPIC)
Estonia	PIC number (Personal Identification Code)	Estonian ID Card (Isikutunnistus ID-kaart ESTEID)
Finland	FINUID number (Finnish Unique Identifier)	Finnish Electronic Identity Card (FINEID)
Iceland	SSN number (Social Security Number)	Icelandic bank card
Italy	Tax identification number	Electronic Identity Card (Carta d'identità elettronica)
		National Service Card (Carta nazionale dei servizi)
Liechtenstein	Serial number of the certificate in conjunction with PEID number (Personal Identification Number)	lisign
Lithuania	Personal ID code	Lithuanian Personal Identity Card (Asmens Tapatybės Kortelė)
Portugal	Personal identification number Social insurance number Tax number Healthcare user number	Personal Identity Card (Cartão do Cidadão)
Sweden	Personal ID number	Nationellt id-kort
Slovenia	Serial number of the certificate in conjunction with PRN number (Personal Registration Number) or tax identification number	SIGOV Card
	Tax identification number	Halcom ONE FOR ALL!
	Tax identification number	Postarca smart card
Spain	Personal ID number	DNI electronic (DNI electrónico)

Table 1. Equivalent foreign electronic identities [1]

For the login to an Austrian online application the foreign person must be identified via the Central Register of Residents or the Supplementary Register. For this purpose the available identification attributes are read from the eID card. Based on these attributes, persons can be search in the registers. Additionally,

to get registered in the Supplementary Register it is currently needed to go to the local department.

In this paper we will show the concept and implementation of identifying foreign persons in the Austrian e-government. The focus is on the electronic registration in the Supplementary Register according to §6(5) of the Austrian E-Government and the E-Government Equivalence Decree.

3 Concept

This section describes the realized concept that enables the login to an Austrian e-government application using a foreign eID card. The following functional description covers the login to a foreign person in case he or she is already registered in the Supplementary Register as well as the person must be registered in the Supplementary Register previously.

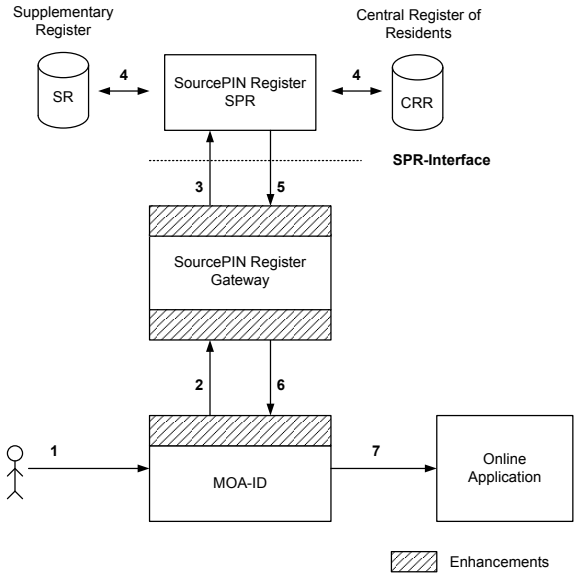

Fig. 1. Foreign Identities in the Austrian E-Government

Figure 1 shows the process consisting of following steps:

1. A foreign citizen wants to log in to an Austrian e-government application using an eID card. For accessing the application the citizen must be identified and authenticated via the basic service MOA-ID.
   If the citizen wants to login, MOA-ID tries to read the Identity Link from the eID card (via the Citizen Card Environment). This attempt fails, because only Austrian eID cards hold an Identity Link. So MOA-ID detects that the inserted eID card is a foreign one, a non activated Austrian Citizen Card or an unknown signature card. For the following it is assumed that the inserted eID card is a foreign card. This is checked by MOA-ID anyway.
   To get the identification data from the foreign person (e.g. first name, family name and national eID number) the card holder is requested to create a signature. Therefore, a request is sent to the CCE which creates the qualified signature using the actual eID card. This signature is sent back to MOA-ID. Next MOA-ID sends this signature to the SourcePIN Register Gateway

(SPR Gateway). This gateway provides a simple access to the SourcePIN Register.
2. The SPR Gateway gets the foreign signature from MOA-ID and verifies it. Thereby also the signatory certificate is checked if it is qualified. In case the certificate is qualified the necessary identification data is extracted. This data are first name, family name, national eID number and information about the certificate (validity, issuer, public key, etc.). For Liechtenstein an additional register query must be performed to get the current national identifier. After collecting all required data a request to the SourcePIN Register is sent.
3. The gateway forwards the request (containing the person data) to the SPR to get the Identity Link of the foreign person.
4. The SPR searches the Central Register of Residents (CRR) and the Supplementary Register (SR). Now the following two cases are distinguished:
   (a) If the foreign person is already registered in one of the two registers an Identity Link can be generated for this person on the fly.
   (b) The foreign person is neither registered in the CRR nor in the SR. In this case the person is electronically registered in the SR based on §6(5) of the E-Government Act. If the registration was successful (the person is now registered in the SR), an Identity Link can be generated. In case the registration failed an appropriate error message is produced.
5. Depending on the prior steps the generated Identity Link or the error message is sent back to the SPR Gateway.
6. Based on the received Identity Link, MOA-ID creates a security token (SAML artifact). Alternatively, if an error message has been received, the message is shown to the person.
7. The person is granted access to the e-government application.

4 Implementation

The concept described has been realized in the course of a project. Therefore existing services (MOA-ID and SPR Gateway) have been extended. In the following sections these enhancements are described. Furthermore, the realization of the register query for Liechtenstein is depicted.

4.1 MOA-ID Enhancements

For the MOA-ID enhancements the current release has been adapted. These adaptions contain following enhancements regarding the integration of foreign eID cards:

- *Foreign eID card*: MOA-ID has been adapted to support foreign eID cards. MOA-ID is now able to detect and support foreign eID cards. This is done via sending a request to the Citizen Card Environment to read the Identity Link from the card. In case of an activated Austrian Citizen Card the Identity Link is returned and the login process proceeds as usual. If a foreign card is

in the card reader, an Identity Link could not be found and so an appropriate error message is sent back to MOA-ID. Based on this error message MOA-ID detects, that the inserted card is a foreign one.
- *Signature creation*: To get the signature certificate from the foreign citizen, MOA-ID has been amended to send a request to the Citizen Card Environment. Via this request the citizen is asked to create a signature using his or her qualified certificate. After creation of the signature the Citizen Card Environment sends the signature back to MOA-ID. Finally MOA-ID sends the signature to the SPR Gateway to get the temporary Identity Link of the foreign citizen.
- *Configuration*: The last enhancement concerns the configuration of MOA-ID. In the context of the enhancement new configuration parameters must be defined to enable the access to the SourcePIN Register Gateway.

4.2 SourcePIN Register Gateway

The main purpose of the SourcePIN Register Gateway is to enable a simple and secure access to the SourcePIN Register. Following enhancements have been made: The gateway has been extended by an additional request that can be sent to the SourcePIN Register. This request contains the foreign signature. This signature is then used to get the signatory certificate and so to get the identification data of the foreign citizen. The response of the SPR Gateway contains the generated Identity as result.

In the following the process from receiving the request from MOA-ID till sending back the Identity Link is described in more detail:

1. MOA-ID sends the request to get the Identity Link to the gateway. This request contains the signature of the foreign person.
2. After receiving the signature the SPR Gateway verifies the signature. Additionally a certificate check is executed to check if the certificate is qualified.
3. In case the certificate is qualified the gateway extracts following person data from the certificate:
   (a) First name
   (b) Family name
   (c) Date of birth (optional): Only if available from certificate
   (d) Sex (optional): Only if available from certificate
   (e) Public key
   (f) Travel document:
      i. Document number: This number corresponds to the unique identifier of the country. Usually this identifier is encoded in the certificate, except Liechtenstein (see following sub section for details).
      ii. Document type: Hard coded string *ELEKTR_DOKUMENT* (which means *electronic document*)
      iii. Issue date
      iv. Issuing authority
      v. Issuing country

4. Using the extracted person data a SOAP request (according to the SPR interface specification [3]) is created and sent to the SourcePIN Register. The register evaluates the request and querires the Central Register of Residents and the Supplementary Register. As search criteria only first name, family name, unique identifier and - if available - the date of birth are used. If the person can be found in one of these registers a temporary Identity Link is created and sent back to MOA-ID. In case the person could not be found, the SourcePIN register adds the person to the Supplementary Register according to §6(5) of the E-Government Act. Thereby, all available person data are stored in the Supplementary Register. After a successful registration an Identity Link can be produced and sent back to the gateway.
5. The gateway forwards the Identity Link, or the error message if an error occurred during the registration process, to MOA-ID.

Liechtenstein The certificate of Liechtenstein does not contain a unique identifier. Instead the identifier is stored in a central identity register. Together with the federal administration of Liechtenstein we developed a SOAP interface to this register (see also Figure 2). Using this interface the SPR Gateway is able to request for the unique identifier. Thereby the request is an *AttributeQuery* according to the SAML specification [6]. This request contains the qualified certificate of the citizen and is sent to the identity register of Liechtenstein. Based on this certificate the identity register is able to find the person. Then the identity register creates a response containing the unique identifier and additionally the first name, family name and date of birth. This response is sent back to the Austrian SPR Gateway. After receiving the response, the SPR Gateway extracts the person data. Using this data the person can be searched for within the Austrian registers or can be added to the Austrian Supplementary Register.

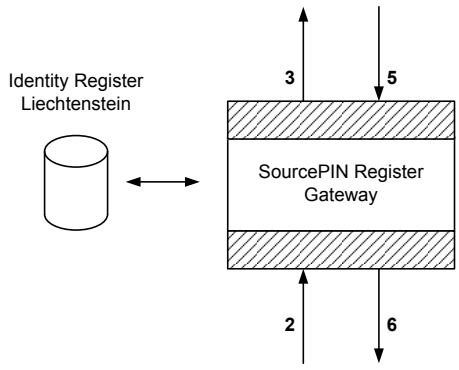

Fig. 2. Register query for Liechtenstein

5 Conclusions

This paper describes how foreign identities are handled within the Austrian e-government. Based on an updated legal framework a solution has been developed which allows non-Austrian citizens to log in to an Austrian online service using their foreign eID. The implementation has been successfully tested and was launched in July 2010.

The presented concept fits very well to the pan-European approach of interoperable electronic identities. Foreign citizen can directly use Austrian e-government services without the need of a prior on-site registration.

However, although the Equivalence Decree currently lists 14 eID cards which are considered to be equivalent, not all off them can be actually used at the present time. This is because not all of these eID card are already implemented in the available Citizen Card Environments. The CCE that mostly supporting foreign eID cards is MOCCA[5]. MOCCA supports the Belgian BELPIC, the Estonian ESTID, the eID card from Liechtenstein and two different eID cards from Italy. The MOCCA team will integrate further eID cards in the near future. Nevertheless, the developed system has already been started.

Future work touches the SIGOV cards of Slovenia. As with the certificate of Liechtenstein, the Slovenian SIGOV card does not contain the national identifier (tax or PRN number). Additionally, in this case no national register can be queried for the identifier. However, the Slovenian government conducts a Web service[6] which is able to verify a given tax or PRN number. Based on this Web service a concept for identifying persons is currently under development.

References

1. Austrian Federal Law Gazette (BGBl) Nr. 170/2010. E-Government Equivalence Decree, Decree of the Federal Chancellor laying down conditions for equivalence under Section 6(5) of the E-Government Act, 2010.
2. Bundesgesetzblatt (BGBl) Teil I Nr. 190/1999. Bundesgesetz über elektronische Signaturen (Signaturgesetz – SigG), 1999. available in German only, http://www.ris.bka.gv.at.
3. Bundesministerium fuer Inneres, Sektion IV - Support Unit ZMR. SZR 2.0 Anwendungsdokumentation, November 2009. Version 1.0.
4. D. Eastlake 3rd, J. Reagle, and D. Solo. (Extensible Markup Language) XML-Signature Syntax and Processing, March 2002. http://www.ietf.org/rfc/rfc3275.txt.
5. R. Housley. Cryptographic Message Syntax (CMS), July 2004. http://www.ietf.org/rfc/rfc3852.txt.
6. OASIS. Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0, March 2005.

[5] http://mocca.egovlabs.gv.at/

[6] Slovenian Web service for verifying a tax or PRN number, https://storitve-ca.gov.si/avtentikacija.htm

7. European Parliament and Council. Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, December 1999. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:EN:HTML.
8. Austrian Federal Law Gazette (BGBl) part I Nr. 10/2004. The Austrian E-Government Act, Federal Act on Provisions Facilitating Electronic Communications with Public Bodies, entered into force on 1 March 2004; amended by BGBl I Nr. 7/2008 (amendments entered into force on 1 January 2008) including the Corrigendum in BGBl I Nr. 59/2008, 2008.