Architectures and Protocols for Secure Information Technology Infrastructures

Antonio Ruiz-Martínez
University of Murcia, Spain

Rafael Marín-López
University of Murcia, Spain

Fernando Pereñíguez-García
University of Murcia, Spain

A volume in the Advances in Information Security, Privacy, and Ethics (AISPE) Book Series

Information Science REFERENCE
An Imprint of IGI Global

Managing Director: Lindsay Johnston
Editorial Director: Joel Gamon
Production Manager: Jennifer Yoder
Publishing Systems Analyst: Adrienne Freeland
Development Editor: Monica Speca
Assistant Acquisitions Editor: Kayla Wolfe
Typesetter: Travis Gundrum
Cover Design: Jason Mull

Published in the United States of America by
Information Science Reference (an imprint of IGI Global)
701 E. Chocolate Avenue
Hershey PA 17033
Tel: 717-533-8845
Fax: 717-533-8661
E-mail: cust@igi-global.com
Web site: http://www.igi-global.com

Library of Congress Cataloging-in-Publication Data

Architectures and protocols for secure information technology infrastructures / Antonio Ruiz Martinez, Rafael Marin-Lopez and Fernando Pereniguez Garcia, editors.
pages cm
Includes bibliographical references and index.
ISBN 978-1-4666-4514-1 (hardcover) -- ISBN 978-1-4666-4515-8 (ebook) -- ISBN 978-1-4666-4516-5 (print & perpetual access) 1. Information technology--Security measures. 2. Computer networks--Security measures. I. Martinez, Antonio Ruiz, 1976-, editor of compilation. II. Marin-Lopez, Rafael, 1977-, editor of compilation. III. Garcia, Fernando Pereniguez, 1984-, editor of compilation.
QA76.9.A25A73 2014
005.8--dc23
2013020692

This book is published in the IGI Global book series Advances in Information Security, Privacy, and Ethics (AISPE) (ISSN: 1948-9730; eISSN: 1948-9749)

British Cataloguing in Publication Data
A Cataloguing in Publication record for this book is available from the British Library.

Chapter 11
The Austrian Identity Ecosystem:
An E-Government Experience

Klaus Stranacher
Graz University of Technology, Austria

Thomas Zefferer
Graz University of Technology, Austria

Arne Tauber
Graz University of Technology, Austria

Bernd Zwattendorfer
Graz University of Technology, Austria

ABSTRACT

Architectures and protocols for secure information technology are crucial to satisfy security requirements of current e-government solutions. Identity plays a central role in most e-government solutions, as users typically need to be reliably identified and authenticated. User identification and authentication approaches usually rely on complex cryptographic methods and sophisticated technical solutions. Additionally, these solutions need to be backed by appropriate organizational and legal frameworks that assure the legal validity of provided identification and authentication approaches. In this chapter, the authors introduce the Austrian identity ecosystem that represents one of the main pillars of the Austrian e-government infrastructure. They discuss underlying concepts and main building blocks of this comprehensive ecosystem and show how architectures and protocols for secure information technology are employed to assure the security of user identification and authentication processes. By discussing concrete use cases, the authors illustrate the applicability of the Austrian identity ecosystem for both Austrian and foreign citizens.

DOI: 10.4018/978-1-4666-4514-1.ch011

INTRODUCTION

Identity is an important concept of various scientific disciplines and has also become common in popular discourse (Fearon, 1999). Due to its frequent use, the term 'identity' is often used without any further explanations and definitions, ignoring its multiple meanings. Given the complexity of the term and concept of identity, it is unsurprising that various different definitions can be found in literature. Hogg et al. (1988) define identity as '*people's concepts of who they are, of what sort of people they are, and how they relate to others*'. According to Katzenstein (1996), '*the term [identity] (by convention) references mutually constructed and evolving images of self and other*'. White (1992) states that '*identity is any source of action not explicable from biophysical regularities, and to which observers can attribute meaning*'. The different definitions of the term 'identity' emphasize the multiple meanings and interpretations of this term and its relevance for many scientific disciplines.

Identity plays also a central role for governments and public administrations. Usually, such institutions have a rather pragmatic view on the abstract term identity. For these institutions, identity is basically a necessary concept that facilitates the implementation of governmental and administrative procedures. Each person that participates in such a procedure is assigned a unique identifier (e.g. a number) that unambiguously distinguishes this person from others. This concept is applied to both natural and legal persons in the same way. The use of abstract numbers is necessary as in large administrative districts (such as states or nations) the name and date of birth of citizens are usually not sufficient to allow for an unambiguous distinction of users.

Identity has played an important role in the accomplishment of governmental and administrative procedures for a long time. Citizens have become used to identify themselves by showing an ID or passport when participating in official procedures or applying for official services. During the past years, Information and Communication Technologies (ICT) have significantly changed the way administrative procedures are conducted by both public administrations and citizens. Attempts to leverage ICT in order to improve the efficiency of governmental procedures are subsumed under the term e-Government. E-Government allows citizens to carry out administrative procedures over the Internet without the need to personally show up at administrative offices. One of the biggest challenges in e-Government is the development and deployment of appropriate means to reliably identify persons that actively participate in Internet-based e-Government procedures. This typically involves the deployment of an electronic ID (eID) that is linked to the person's identity and is used to unambiguously identify this person in electronic governmental procedures.

Many European countries have rolled-out electronic IDs to their citizens on national level since years. In the special case of Austria, the so called Citizen Card represents the national eID that allows citizens to securely identify and authenticate at online procedures. The Austrian Citizen Card concept has already been introduced in 2002 and has been designed to be applicable in both the public and the private sector. Public administrations use the Citizen Card concept to reliably identify and authenticate citizens in e-Government procedures. At the same time, the Citizen Card concept is also used by the private sector to protect access to security sensitive applications such as e-Banking. This way, the Citizen Card has emerged being a key concept and core component of various security sensitive online services in Austria.

During the past ten years, a complex and powerful ecosystem of Citizen Card related concepts and components has evolved to address emerging challenges such as integration of legal identities, electronic mandates, or interoperability with

foreign eID solutions. In this article we introduce the Austrian identity ecosystem in detail. Starting from the Citizen Card concept, which represents the key element of the entire ecosystem, related concepts and components of the Austrian identity ecosystem are introduced and discussed. We show how the set of well-established concepts and components is used to securely authenticate national and foreign citizens and how advanced concepts such as legal identities and electronic mandates are considered. We will especially elaborate on security and privacy requirements of electronic identities and discuss how these issues are addressed by the Austrian identity ecosystem.

E-GOVERNMENT IN AUSTRIA

Austria has been working on appropriate e-Government solutions for a couple of years and has invested significant effort in their development. The main aim of these efforts is to support Austrian citizens and businesses in online procedures and thereby facilitating access to public authorities or public administrations with the help of ICT. Austria follows a well-defined and sustainable e-Government strategy, which is aligned along several initiatives and regulations of the European Union. The main strategy dates back to the year 2000 and is based on agreements achieved in the EU summit in Feira (European Parliament, 2000a) and Lisbon (European Parliament, 2000b). In this summit, common objectives such as online availability of main governmental services by the year 2005 had been agreed. These agreements have been anchored in the Austrian government program to join forces and to spur e-Government in Austria. Several EU initiatives dealing with e-Government agreements to strengthen the European internal market have followed. Examples of such European initiatives are the European Union action plan "eEurope" (European Commission, 2002) or the "i2010" initiative of the European Commission (European Commission, 2006), representing a successor initiative of this action plan. Currently, the European Commission has published new guidelines in its "Digital Agenda for Europe 2020" (European Commission, 2010). These guidelines especially focus on strengthening the digital European internal market by providing faster Internet connections and interoperable online services.

All these directives and regulations have yielded according amendments of the Austrian e-Government strategy and implementations based on well-established information and communication technologies. However, the main vision for successful and sustainable e-Government in Austria, which has been elaborated in the year 2000, is still valid. This vision envisages that all Austrian citizens and businesses must be able to conduct all governmental processes and transactions electronically, fast and in a simply manner, and without any special or detailed knowledge on technology (Federal Chancellery of Austria, 2010a). This vision foresees a simple, secure, and transparent implementation of e-Government services by means of modern information and communication technologies.

Basic Objectives

From this overall vision and from the general Austrian e-Government strategy, the following basic objectives of e-Government solutions in Austria can be derived:

- Assure trust in provided services by appropriately informing citizen on the security-, privacy-, and transparency-preserving features of provided solutions.
- Include all relevant authorities to avoid silo solutions, i.e. separated solutions of different authorities, which hinder interoperability between them.
- Iteratively transform services to achieve complete transactional services without media-breaks.

One major aim of the Austrian e-Government strategy is to inform citizens about the availability and the maturity of electronic governmental services. This way, citizens should be able to recognize the added value such as higher comfort and flexibility, and should also gain an appropriate level of trust in these services. Therefore, it is important that e-Government applications are easily accessible and follow common and approved approaches to assure an adequate degree of usability. Moreover, e-Government applications should be easily locatable by citizens and any existing barriers that threaten to aggravate access to services should be removed. The use of existing and well-established standards helps to decrease such barriers. Another important criterion with respect to citizen information is security. Security and privacy are essential to assure trust in governmental online services that usually transfer or process sensitive data. Citizens must believe and give credit to the same level of trust for online services as they do for traditional paper-based procedures. Citizens must be appropriately informed about the strengths and security features of used technologies.

Another main pillar of the Austrian e-Government strategy constitutes the inclusion of all relevant authorities. This requirement involves the implementation of e-Government on different public administrative levels. This means that e-Government should be implemented on national, regional, and local level involving federal states, municipalities, and cities. All levels must cooperate with each other to guarantee consistency and to avoid silo solutions. Existing infrastructures should be conjointly re-used to benefit as much as possible from the advantages offered by e-Government.

Existing e-Government infrastructures and solutions should not be abandoned, but moreover integrated into new and emerging services. The aim is to develop fully-fledged transactional solutions and services without media breaks. This means that citizens should be able to electronically apply for governmental procedures and at the same time receive the results without the need for paper-based post mail. To achieve this goal, governmental services should be transformed iteratively to electronic pendants. This means to set up simple and pure informational services at the beginning and to steadily increase the complexity and sophistication of these services. The final goal is to roll out complete transactional services in the end. The step-wise transformation necessitates continuous amendments that are facilitated by fast technological improvements. The fulfillment of this requirement can be facilitated by a modular design of services and by the definition of appropriate interfaces.

Besides the definition of technological concepts and solutions, the realization of a comprehensive e-Government strategy requires the implementation of long-term and fundamental structures in several areas. By the help of an e-Government strategy, concepts and guidelines are worked out, which need to be further implemented step-wise. To implement those concepts, a general framework, not only on technical but also on organizational and legal level, has to be implemented. This guarantees the necessary basis for a successful and sustainable e-Government infrastructure.

The following sub-sections briefly describe the organizational, legal, and technical frameworks that have been defined to guarantee successful e-Government solutions in Austria.

Organizational Framework

To achieve the ambitioned objectives defined by the Austrian e-Government strategy, efficient and collaborative organizational structures are required. Therefore, Austria relies on a dynamic and flexible organizational model. The most important entities of this organizational model are the:

- E-Government Platform
- E-Cooperation Board

- Platform Digital Austria
- E-Government Innovation Centre

The *E-Government Platform* consists of the Austrian vice chancellor, several ministries, the president of the Austrian Federal Economic Chamber, the presidents of social insurance carriers, and governing actors of e-Government working groups, which have strong relations to the federal states in Austria. The major objective of this platform is the organization of e-Government initiatives and activities in Austria on political level.

The *E-Cooperation Board* is combined of ministries, federal states, associations of Austrian cities and towns, and advocacy groups. The E-Cooperation Board coordinates ongoing work in the field of e-Government and determines the responsibility for carrying out e-Government implementation plans.

The *Platform Digital Austria* constitutes the coordination and strategy council of the federal government for e-Government in Austria. All e-Government projects converge in this council. Hence, this council represents one of the central entities of the Austrian e-Government strategy.

The *E-Government Innovation Centre* has been founded in parallel to the Platform Digital Austria. It is responsible for technology observation and technical innovations with respect to e-Government. Furthermore, federal states, cities, or municipalities are supported in their e-Government activities. In addition, the E-Government Innovation Centre has been a partner in several European-wide e-Government projects, such as STORK[1] (Secure Secure idenTity acrOss boRders linKed) or SPOCS[2] (Simple Procedures Online for Cross- Border Services).

Legal Framework

Besides a mature organizational structure, a consistent legal framework represents a relevant factor for successful and sustainable e-Government in Austria. The main pillar of the Austrian legal framework for e-Government constitutes the Austrian E-Government Act (Federal Chancellery of Austria, 2004), which has been especially stipulated according to the Austrian e-Government strategy. However, the legal framework is not based on the Austrian E-Government Act only, but includes several additional relevant laws and regulations. Basically, the main legal framework components of the Austrian e-Government are the:

- E-Government Act
- Signature Act
- General Administrative Procedures Act
- Service of Documents Act

Within the European Union, Austria is one of the first Member States that has adopted a comprehensive e-Government law. The Austrian E-Government Act has come into force on March 1, 2004 and has been amended on January 1, 2008. The three main principles of the Austrian E-Government Act are freedom of choice regarding citizens' interaction with the government and public authorities, guaranteeing security and data protection, and assurance of barrier-free access to e-Government services for all citizens.

The Austrian Signature Act (Federal Chancellery of Austria, 1999) constitutes the implementation of the EU Signature Directive (European Union, 1999), which was published by the European Commission in 1999. This directive specifies a common legal framework for electronic signatures in the European Union. In general, the Austrian Signature Act distinguishes between simple, advanced, and qualified electronic signatures. Qualified electronic signatures are legally equivalent to hand-written signatures according to the EU Signature Directive. Qualified electronic signatures play a major role in the Austrian eID concept, as they are also used for secure electronic authentication of citizens in online procedures.

The General Administrative Procedures Act (Federal Chancellery of Austria, 1991) regulates procedures of nearly all public administrations

and authorities in Austria. For instance, this act regulates how citizens can contact public authorities. In electronic processes, this can be done e.g. via e-mail or Web forms.

The Service of Documents Act (Federal Chancellery of Austria, 1982) defines the postal and electronic delivery of authoritative documents to citizens. Similar to the paper-based world, in electronic delivery a differentiation between verifiable and non-verifiable delivery exists. In a verifiable delivery scenario the recipient confirms the receipt of a document by his or her signature. In Austria, verifiable deliveries can be also carried out using electronic means.

Technical Framework

The technical framework to be applied for e-Government in Austria is based on modern and approved information and communication technologies. By the help of these technologies, data and message exchange between citizens, businesses, and public authorities can be organized in a secure and transparent way. The technical core component within the Austrian e-Government strategy constitutes the Austrian Citizen Card concept. The Austrian Citizen Card is an electronic ID (eID), which allows for secure and reliable authentication of citizens in online procedures and enables citizens to create qualified electronic signatures.

Smart cards are currently a popular technology that can be used to practically implement the Austrian Citizen Card concept. National health insurance cards, which are applicable as Citizen Card, have been rolled-out nation-wide. However, the Austrian Citizen Card concept is technology agnostic, hence alternative implementations are also possible. An increasing number of citizens use the Austrian Mobile Phone Signature (Orthacker et al., 2010). In this solution, Citizen Card functionality is not implemented by a smart card but by a central server with attached hardware security module (HSM). Citizens authorize access to personal data stored and processed in the central HSM by means of a two-factor authentication with the help of their mobile phones.

In general, Austria tries to guarantee technology neutrality in its e-Government solutions. This neutrality is guaranteed by open interfaces and easy exchangeability of single modules. One major aspect thereby is the use of international standards (e.g. well-known standards SOAP/WSDL Web services, SSL, SAML[3] or electronic signature standards such as XMLDSIG[4] or XAdES[5]). On the one hand, such standards ensure interoperability between cross-domain applications of public authorities. On the other hand, well-established and proven standards ascertain a high level of security and privacy for citizens.

THE AUSTRIAN E-ID CONCEPT

The Austrian eID concept aims to achieve the basic goals of the Austrian e-Government strategy that have been discussed in the previous section. To achieve these goals, the Austrian eID concept has been based on the organizational, legal, and technical frameworks provided by the Austrian e-Government strategy. In this section we discuss the Austrian eID concept in detail. We do so by discussing the Austrian Citizen Card concept, which represents the backbone of the Austrian eID concept, first. We then introduce different concepts and components that are based on the Austrian Citizen Card concepts and that build the Austrian identity ecosystem.

The Austrian Citizen Card Concept

The Austrian eID concept (Federal Chancellery of Austria, 2008) constitutes one of the key concepts of the Austrian e-Government strategy. The Austrian Citizen Card, in turn, defines the key concept of the Austrian eID concept. Representing the official eID in Austria, the Citizen

Card is basically an abstract definition of a secure eID token that is in possession of the citizen. Its main capabilities are secure identification and authentication of citizens as well as the creation of qualified electronic signatures according to the EU Signature Directive (European Union, 1999).

As mentioned above, the Citizen Card concept is a technology-neutral concept that allows for several different implementations. Currently, smart cards and mobile phones can be used as Citizen Card. However, the technology neutral approach guarantees that also alternative approaches and implementations can be developed and deployed in the future.

Citizen Card Functions

Irrespective of the actual implementation of the Citizen Card concept, the Austrian Citizen Card provides a well-defined set of functionality. We elaborate on the supported features in the following.

Identification and Authentication of Citizens

Unique identification and secure authentication are essential components of governmental processes. In e-Government processes, the Citizen Card provides technical means for carrying out identification and authentication electronically. By using the Citizen Card in online applications, user identification is based on the so-called *Identity Link*. The Identity Link is a special data structure including the citizen's first name, last name, date of birth, and a unique identifier. Although the included identifier is unique, it must not be used directly for identification at online applications due to legal privacy restrictions. Therefore, the unique identifier is derived for a specific sector the application belongs to. On the one hand, this derivation still guarantees uniqueness; on the other hand, applications are not able to track citizens. This way, the concept of sector-specific identifiers assures privacy preservation. The sector specific identification approach followed in Austria is discussed in more detail later in this article.

The unique identifier stored on the Citizen Card allows for a unique identification of users in online procedures. However, security sensitive applications usually require user not only to identify but to also authenticate. Identification and authentication are actually related processes. The claim to be a person is typically referred to as identification, while the proof of this claim is referred to as authentication. In Austria, the Citizen Card is not only used for identification but also for electronic authentication. In online processes, authentication is carried out by creating an electronic signature by applying Citizen Card functionality. The functionality to create electronic signatures using the Austrian Citizen Card is described in the following.

Secure and Qualified Electronic Signatures

Besides proofing his or her identity, citizens often need to express a written declaration of intent in governmental processes or transactions. This requirement can occur, for instance, when applying for a governmental process or at the end of such a process, when confirming the receipt of results. In traditional paper-based processes, a written expression of declaration of intent is carried out through hand-written signatures. In electronic processes, the hand-written signature needs some equivalent.

According to the Austrian Signature Act, which constitutes the Austrian implementation of the EU Signature Directive, the electronic pendants to hand-written signatures are qualified electronic signatures. Qualified electronic signatures are fully equivalent to hand-written signatures by law. In general, electronic signatures are cryptographic mechanisms to express a declaration of intent

electronically. According to the EU Signature Directive, qualified electronic signatures are created by using a qualified digital certificate and by invoking a Secure Signature Creation Device (SSCD). A qualified digital certificate needs to include some specific information according to the EU Signature Directive. All requirements for qualified digital certificates are defined in this directive. An SSCD is usually a cryptographic hardware token that needs to fulfil several requirements also defined in the EU Signature Directive.

Data Storage

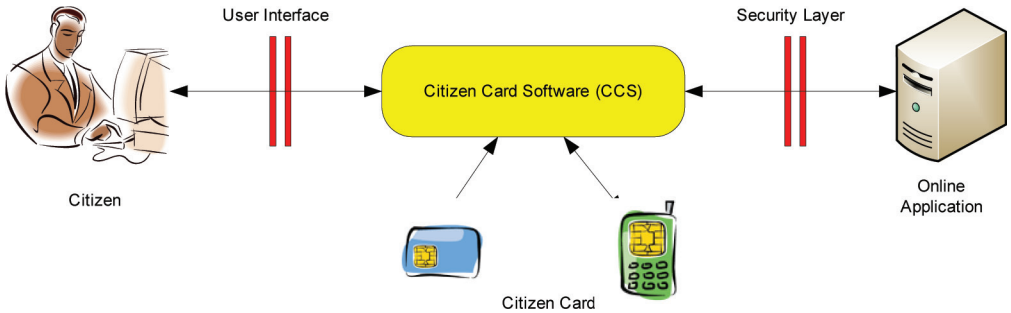
The third functionality of the Austrian Citizen Card constitutes simple data storage. The Citizen Card provides a readable and writeable data storage. The data storage is divided into logical entities, which are irrespective of the physical storage location. Possible physical storage locations are the Citizen Card itself, the citizen's hard drive, or data storage accessible over the Internet, e.g. cloud storage solutions. Data to be stored can be of arbitrary format, such as other digital certificates, XML data, or similar data formats.

Citizen Card Model

Figure 1 illustrates the general Citizen Card model (Federal Chancellery of Austria, 2008) and shows all participating parties and components in Citizen Card-based transactions. The central component of the Citizen Card model is the so-called *Citizen Card Software (CCS)*, which constitutes a middleware residing between the citizen and the online application. All involved entities are briefly described below.

- **Citizen:** A citizen is a natural person who wants to access a governmental application by using Citizen Card functionality. The Citizen Card functionality is invoked through the Citizen Card software.
- **Online Application:** This as a governmental or business application offering specific services to citizens, which may require Citizen Card functionality. For instance, restricted access to services is protected through Citizen Card authentication.
- **Citizen Card Software:** The Citizen Card Software constitutes a software, which is either locally installed on the citizen's computer or provided remotely on server-side. This software provides Citizen Card functionality to the citizen. Amongst others, Citizen Card functionality includes identification, authentication, or the creation of electronic signatures. The Citizen Card Software is the core component of this model, facilitating access to Citizen Card functions and operations.
- **User Interface:** The user interface is the interface between the user and the Citizen Card Software. Required credentials to au-

Figure 1. The Austrian citizen card model (Federal Chancellery of Austria, 2008)



thorize access to Citizen Card functionality are collected from the user through this interface.

- **Security Layer:** The *Security Layer* is a well-defined interface between the online application and the Citizen Card Software. Via this interface, applications are able to access Citizen Card functionality. This interface can be used without paying attention to the underlying Citizen Card implementation. Implementation specifics are encapsulated by the Citizen Card Software.

The Identity Ecosystem in Austria

Based on the Austrian Citizen Card concept, that has been discussed above in more detail, a complex ecosystem of related concepts and solutions has evolved during the past years. We give an overview of this ecosystem in the following.

As elaborated above, secure identification and authentication are key features of the Austrian Citizen Card. The Citizen Card representing the Austrian national eID relies on existing unique identifiers that are further used to derive sector-specific identifiers. Unique identifiers are essential as identification based on first name, last name, and date of birth may be ambitious, especially when the number of users increases. Therefore, in Austria all citizens are registered in the *Central Register of Residence (CRR)* and have a unique number assigned (*CRR Number*). The CCR Number acts as unique identifier.

Due to data protection restrictions, the CRR Number must not be directly used in e-Government processes. Therefore, the CRR Number is encrypted to derive a new unique identifier. This new identifier is created by the *SourcePIN Register Authority*, a subdivision of the *Austrian Data Protection Commission*. The derived identifier is named *sourcePIN* and is also unique for all citizens. In addition, the sourcePIN is stored on the Citizen Card together with other identity related data such as first name, last name, and date of birth. Those identification data and the corresponding citizen's qualified certificate are wrapped within a special XML-based data structure. This data structure, which has already been briefly mentioned above, is called *Identity Link* and is electronically signed by the SourcePIN Register Authority. This signature establishes and certifies a link between the identity data and the qualified certificate stored on the Citizen Card. The Identity Link can be further used for unique identification at online applications.

According to the Austrian E-Government Act, the unique identifying sourcePIN requires special protection to preserve citizen's privacy. A permanent storage of this identifier is only allowed within the Identity Link stored on the Citizen Card. Hence, for identification at online applications it is forbidden to use the sourcePIN directly. Because of this restriction - due to data protection reasons - the Austrian e-Government strategy foresees a sector-specific model for identification at online applications. Instead of using the sourcePIN directly, a sector-specific identifier is derived from the sourcePIN. This so-called *sector-specific PIN (ssPIN)* is derived from the combination of the sourcePIN and a governmental sector identifier (e.g. finance, tax, etc.) by using cryptographic one-way hash functions. The use of cryptographic hash functions allows for special privacy protection, as the sourcePIN cannot be calculated from a given ssPIN. In addition, an authority from a specific governmental sector is not able to calculate the ssPIN of another sector, e.g. the ssPIN of the finance sector differs from the ssPIN of the tax sector.

Hence, within the Austrian eID concept the ssPIN constitutes the identifier to be finally used for identification at online applications.

The entire Austrian eID concept for natural persons relies on the unique identifier stored in Austria's Central Register of Residence. Austrian citizens living in Austria, and hence being

registered in the CRR, are usually the typical use case and basic assumption when developing e-Government strategies and concepts in Austria. However, the Austrian eID concept also foresees e-Government applications for persons not listed in the CRR (e.g. foreign citizens or Austrian citizens currently residing in a foreign country). Such persons are not registered in the CRR but can be registered in the so-called *Supplementary Register for Natural Persons (SR)*. The Supplementary Register for Natural Persons constitutes an additional register for foreign citizens or Austrian citizens living abroad. Through the Supplementary Register for Natural Persons, these persons become part of the Austrian eID infrastructure and thus get the possibility to use e-Government applications in Austria. In more detail, by registering in the Supplementary Register for Natural Persons, they also get a unique sourcePIN assigned. This way, foreign citizens can be treated equivalently to domestic Austrian citizens in online e-Government applications. In fact, foreign citizens get the same rights in online applications and e-Government processes as Austrian citizens. The legal basis for that is the so-called *E-Government Equivalence Decree* (Federal Chancellery of Austria, 2010b), which was published and became law in 2010. This decree specifies which foreign electronic IDs can be treated equally to the Austrian eID, i.e. the Austrian Citizen Card.

Another main pillar of the Austrian eID ecosystem is the usage of electronic mandates. Electronic mandates can be used as electronic representations for natural and legal persons, or for professional representatives. In case of representation of natural persons, the sourcePIN of both the representative and the represented person are taken for modelling the mandate process electronically. However, also legal persons such as companies get a unique number for governmental processes in Austria. This unique number of a legal person and the sourcePIN of the representative (natural person) are used for mandate generation. We will discuss the use case on electronic mandates in more detail below.

The Austrian identity ecosystem allows unique identification and secure authentication for both natural and legal persons. To ease an integration of the rather complex Austrian eID ecosystem into security sensitive applications, a set of software modules has been developed, which cover most functionality and hide complex details. Figure 2 illustrates main components and entities of the Austrian identity ecosystem. We skip a full description of the individual components in this section. However, we are going to describe the individual organizations interacting with each other as well as basic technical building blocks in more detail in the following section.

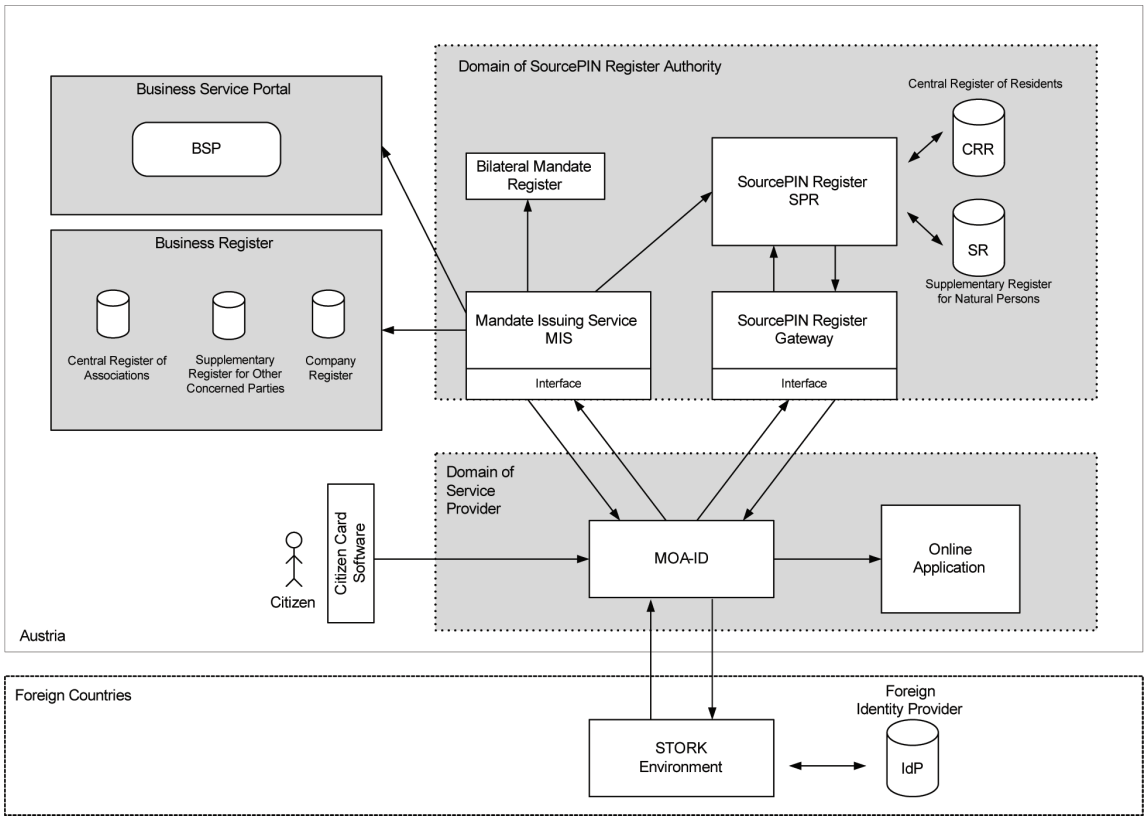
USE CASES FOR IDENTIFICATION AND AUTHENTICATION

To better illustrate the practical application of the various components of the Austrian identity ecosystem, several concrete use cases, in which different users are securely identified and authenticated, are discussed in this section.

Figure 2 provides a general overview of the Austrian identity ecosystem by showing relevant involved components and their relations to each other. Irrespective of that actual use case, a citizen wants to log in to an online application, which runs in the domain of a service provider. The central element to grant access to the online application is the component *MOA-ID* (Federal Chancellery of Austria, 2003). MOA-ID provides secure identification and authentication of citizens based on the Austrian eID concept. In addition to MOA-ID, several other components exist, which are needed to cover all uses cases within the Austrian identity ecosystem. In general, the Austrian identity ecosystem distinguishes three use cases:

- Identification and Authentication of Austrian citizens
- Identification and Authentication of foreign citizens

Figure 2. The identity ecosystem in Austria



- Identification and Authentication of legal identities and electronic mandates

In the following subsections, these use cases are explained in detail, involved components are introduced, and interaction between these components is discussed.

Identification and Authentication of Austrian Citizens

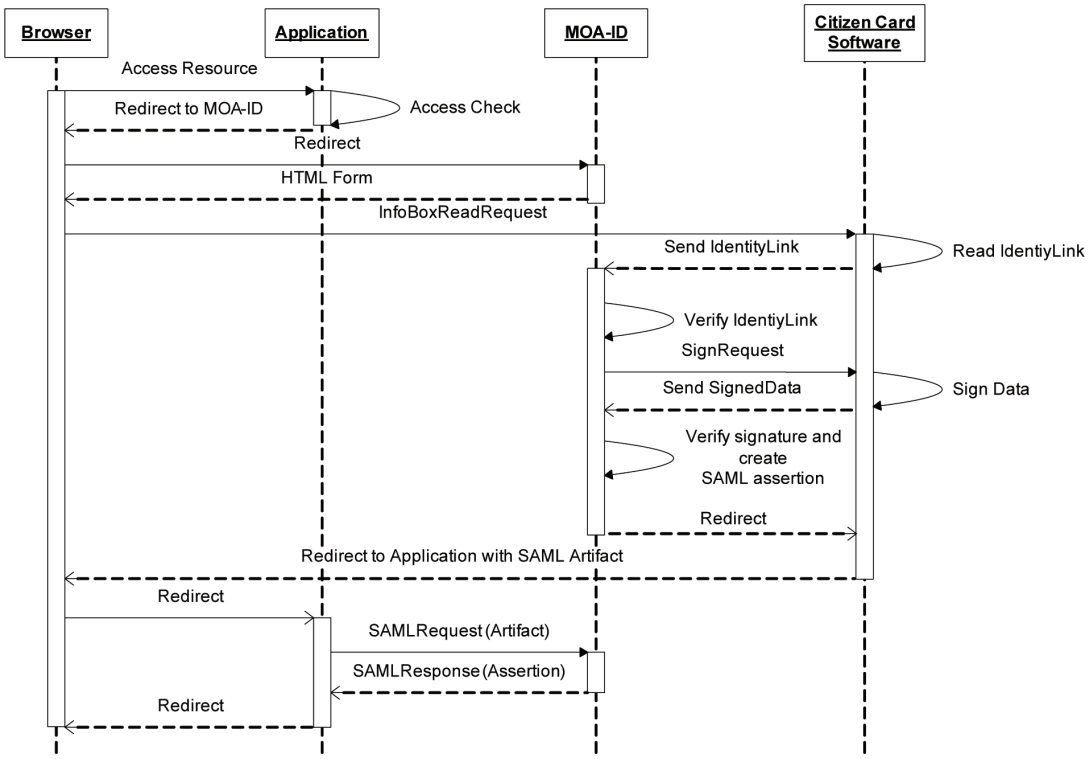
The Austrian e-Government concept foresees user identification based on sector-specific identifiers. This concept guarantees uniqueness while preserving privacy. Authentication of citizens is based on the creation of qualified electronic signatures to state the willingness to access protected services provided by online applications.

As shown in Figure 2, the central component MOA-ID plays a major role for identifying and authenticating citizens, who want to access protected services of an online application. In general, the entire process is divided into two steps, identification, and authentication of the citizen. For identification, the Identity Link of the citizen is used. For authentication, the citizen needs to apply an electronic signature.

Figure 3 shows the sequence diagram for this use case in detail. Secure authentication of a citizen consists of the following steps:

1. The citizen wants to access an application, which is run by a service provider. The application performs an access check and – if has not been successfully authenticated yet

Figure 3. Sequence diagram showing relevant steps to be carried out by Austrian citizens for identification and authentication at online applications



- redirects the citizen to MOA-ID for identification and authentication.

2. MOA-ID returns an HTML form, which includes an XML request to read the Identity Link from the citizen's Citizen Card (InfoBoxReadRequest). This request is sent to the Citizen Card Software.
3. The Citizen Card Software reads the Identity Link and returns it to MOA-ID.
4. MOA-ID verifies the Identity Link as the Identity Link is signed by the SourcePIN Register Authority. At this stage the citizen is successfully identified.
5. Based on the information gathered from the Identity Link, MOA-ID sends an XML request to create an electronic signature to the Citizen Card Software.
6. The citizen is requested to sign the data included in the XML request. The data basically textually describes the willing to intend to authenticate at the applications. After this step, the Citizen Card Software returns the signed data to MOA-ID.
7. MOA-ID verifies the signed data, creates a SAML assertion, and redirects the citizen to the online application (via the Citizen Card Software and the citizen's Web browser). This redirect also includes a SAML artifact, a pointer to the SAML assertion temporally stored at MOA-ID.
8. The online application uses the SAML artifact as a reference to gather the SAML assertion from MOA-ID.
9. Based on the information in the SAML assertion, the online application decides whether the citizen is granted access or not. Finally, the citizen is redirected to the requested protected resource.

Identification and Authentication of Foreign Citizens

In 2008, the Austrian E-Government Act (Federal Chancellery of Austria, 2004) was amended. This revision allows foreign citizens to be treated equally to Austrian citizens in Austrian e-Government processes by amending the following statement:

[…] 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 […]

Based on this statement, foreign electronic identities are fully integrated in the Austrian identity ecosystem. As a requirement, foreign citizens must be registered in the Supplementary Register for Natural Persons (SR) in case they are not already registered in the Central Register of Residents (CRR). Based on that registration, the SourcePIN Register Authority is able to derive a sourcePIN from the information extractable of the foreign eID. Additionally, a temporary[6] Identity Link can be created and further used for identification of foreign citizen at Austrian online applications.

For the integration of foreign citizens into the Austrian identity ecosystem, the respective foreign eID needs to provide an appropriate level of equivalence to the Austrian eID. This equivalence is stated in the *E-Government Equivalence Decree* (Federal Chancellery of Austria, 2010b), which has come into force in June 2010. All countries listed in this decree have in common that they rely on a unique identifier for identifying persons and store this identifier in the citizen's digital certificate. This identifier can be, depending on the country, the tax number, the social insurance number, the health care user number, or an arbitrary personal identification number. Table 1 lists all foreign electronic identities that are equivalent to the Austrian eID according to the E-Government Equivalence Decree.

The identification and authentication process for foreign citizens is based on the identification and authentication use case for Austrian citizens. Therefore, the foreign citizen to be authenticated must be identified via the Central Register of Residents or the Supplementary Register for Natural Persons. Each foreign citizen, who wants to become part of the Austrian eID ecosystem, needs to undergo a registration process. During this registration process, identification attributes are read from the foreign eID card. The foreign citizen is automatically registered in the Supplementary Register during the first login. The registration is based on the citizen's qualified certificate and the data included in this certificate. The registration process is conduced completely online. Hence, personal presence of foreign users in public administrations is not required.

Regarding the identification and authentication of foreign users, two scenarios are distinguished (Login via SourcePIN Register Gateway and Login via STORK). Both scenarios base on the same legal framework, but differ (partly) in the technical implementation. The two scenarios are discussed in more detail in the following subsections.

Table 1. Equivalent foreign electronic identities (Federal Chancellery of Austria, 2010b)

Country	Unique Identifier	Name of eID Token
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	Personal Identity Card (Cartão do Cidadão)
	Social insurance number	
	Tax number	
	Healthcare user number	
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!
		Postarca smart card
Spain	Personal ID number	DNI electronic (DNI electrónico)

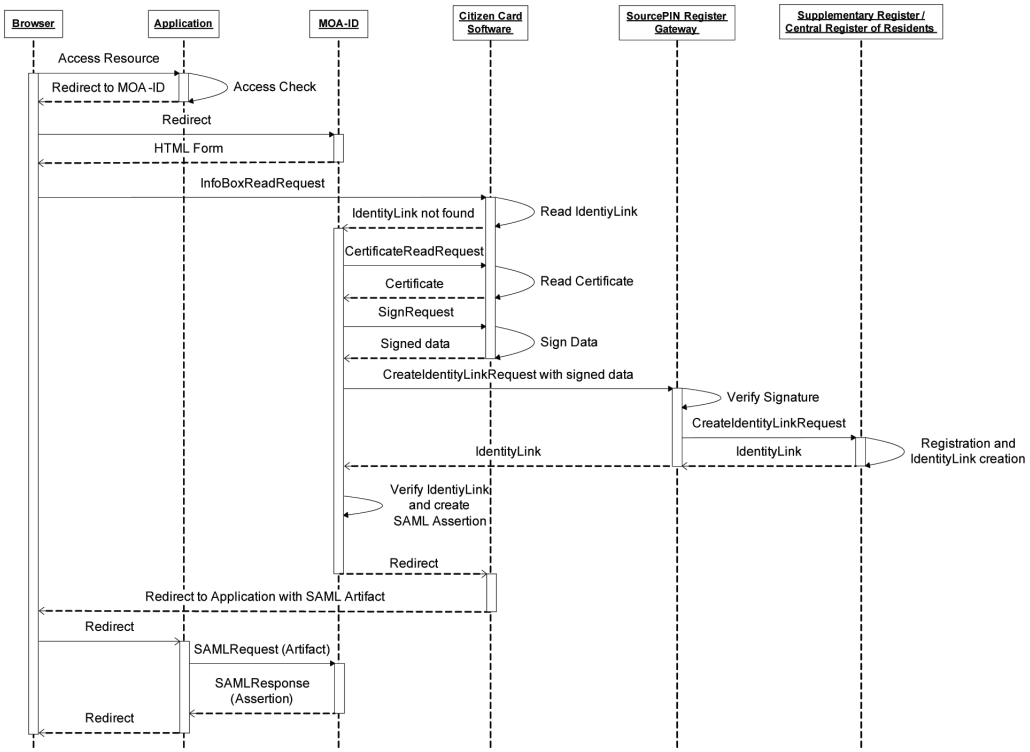
Login via SourcePIN Register Gateway

Basically, the login for foreign citizens is based on the login for Austrian. For the registration of a foreign citizen in the Supplementary Register for Natural Persons, a so called SourcePIN Register Authority Gateway is used. This gateway is contacted by MOA-ID during the authentication process and provides simple access to the SourcePIN Register Authority, which is responsible for the registration of foreign citizens and the creation of the temporary Identity Link. As a basic requirement, foreign eID token specifics must be integrated in the Citizen Card Software. Amongst others, the open source Citizen Card Software MOCCA[7], which represents another key component of the Austrian identity ecosystem, supports eID tokens from the following countries: Belgium, Estonia, Finland, Italy, Liechtenstein, Lithuania, Portugal, and Sweden.

Figure 4 illustrates the sequence diagram for this login scenario. The following process steps need to be carried out to successfully identify and authenticate a foreign citizen according at an Austrian online application:

1. The start of the authentication process is equal to the steps 1-2 from the authentication process for Austrian citizens (see section *Identification and Authentication of Austrian Citizens*). There, an XML request for retriev-

Figure 4. Sequence diagram showing relevant steps to be carried out for foreign citizen authentication through the SourcePIN register gateway



ing the Identity Link is sent via HTTP Post to the Citizen Card Software.

2. The Citizen Card Software tries to read the Identity Link. As a foreign eID token is used instead of an Austrian Citizen Card, this read process fails. A well-defined error message is sent back to MOA-ID.
3. Instead reading the Identity Link, MOA-ID creates an XML request to get the qualified certificate from the foreign citizen's eID token. This request is sent to the Citizen Card Software, which reads the certificate form the citizen's eID token and returns the certificate to MOA-ID.
4. Based on the information within the signer certificate, MOA-ID sends an XML request (to create an electronic signature) to the Citizen Card Software.
5. The foreign citizen is requested to sign the data, which textually states the willingness for authentication at the online application. The Citizen Card Software returns the signed data to MOA-ID.
6. MOA-ID creates an XML request including the signed data and sends this request to the SourcePIN Register Gateway.
7. The gateway verifies the signature and forwards the request to the SourcePIN Register.
8. The SourcePIN Register searches the Central Register of Residents and the Supplementary Register for Natural Persons in order to find the entry of the foreign citizen. At this point, two scenarios need to be distinguished:
   a. The foreign citizen is already registered in one of the two registers. Therefore, an Identity Link can be generated and returned to the gateway.

b. The foreign citizen is not registered in one of the registers. In this case, the citizen is automatically registered in the Supplementary Register for Natural Persons. After completion of the registration process, an Identity Link can be generated and returned to the gateway.

9. The gateway receives the Identity Link from the SourcePIN Register and sends it to MOA-ID.
10. MOA-ID verifies the electronic signature of the Identity Link, creates a SAML assertion including citizen's identity and authentication information, and redirects the citizen to the online application. This redirect also includes a SAML artifact, being a point to the SAML assertion temporally stored at MOA-ID.
11. These process steps are equal to the steps 8-9 from the authentication process for Austrian citizens (see section *Identification and Authentication of Austrian Citizens*).

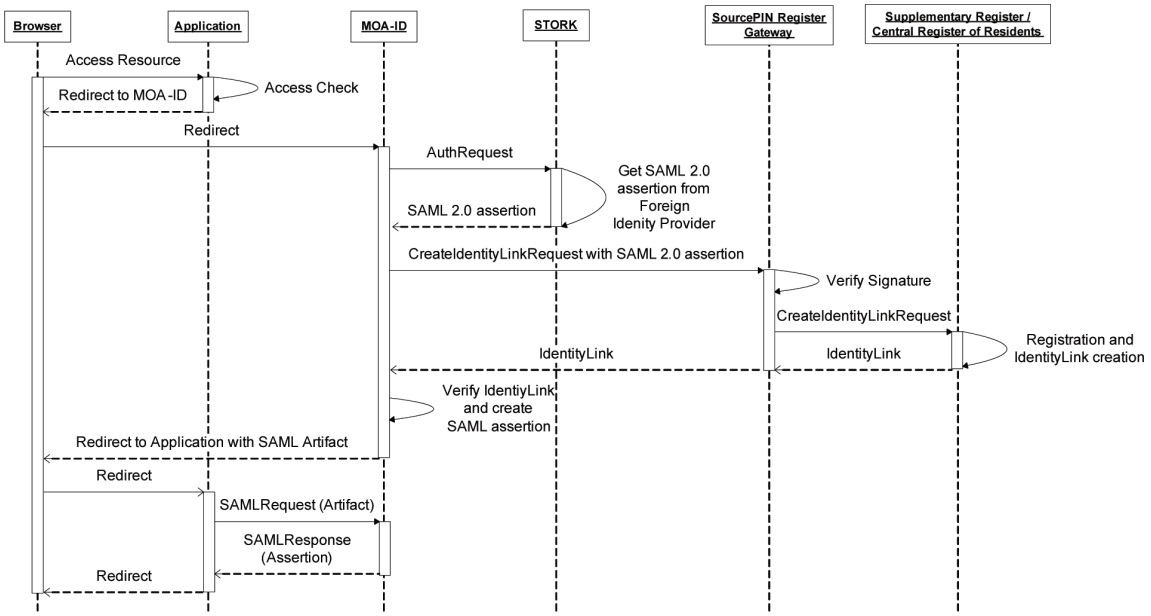
Login via STORK

STORK was an EU large scale pilot project aiming on the interoperability of national eID solutions in cross-border scenarios. During the STORK project, a framework has been developed, which enables citizens to log in at foreign applications using their national eID and domestic infrastructure.

In contrast to the scenario shown above, the Citizen Card Software is not involved in the authentication process. Therefore, this scenario does not require foreign eID tokens to be integrated in Citizen Card Software solutions. Figure 5 shows the sequence diagram for this scenario. The following process steps need to be carried out to successfully identify and authenticate a foreign citizen according to this scenario:

1. See process step 1 from the authentication process for Austrian citizens (see section *Identification and Authentication of Austrian Citizens*).

Figure 5. Sequence diagram showing relevant steps to be carried out for foreign citizen authentication through the STORK framework



2. In this step, the citizen selects his or her home country. MOA-ID sends a well-defined authentication request to the STORK environment of the selected home country.
3. The STORK environment contacts the national identity provider to get a SAML 2.0 assertion. The citizen identifies at the identity provider using his or her national eID infrastructure. The SAML 2.0 assertion includes several requested citizen identity information. In particular, the assertion contains a citizen's signature representing the willingness to login at the Austrian online application.
4. The identity provider returns the SAML 2.0 assertion to the national STORK environment and sends it back to MOA-ID.
5. MOA-ID creates an XML request based on extracted data out of the SAML 2.0 assertion (including the citizen's signature) and sends this request to der SourcePIN Register Gateway.
6. The gateway verifies the signature of the citizen, which is part of the SAML 2.0 assertion, and forwards the request to the SourcePIN Register.
7. See process step 9-11 of the scenario for foreign citizens discussed above (see section *Login via SourcePIN Register Gateway*).

Legal Identities and Electronic Mandates

Representation and mandates are important vehicles in public procedures and business processes. We usually use mandates to empower other persons to act on behalf of ourselves. Typical examples are health care proxies or mandates to carry out bank transactions on behalf of another person. Particularly in e-Government processes many contacts are initiated by companies or other organisations whereby a natural person, e.g. a company manager, is representing the legal person. Another use case is professional representation. Lawyers, notaries, clerks, or tax consultants are representing their clients in various matters.

The Austrian e-Government initiative considered representation from the very beginning. Art. 5 of the Austrian e-Government Act (Federal Chancellery of Austria, 2004) states that

[…] where the Citizen Card is to be used for submissions by a representative, a reference to the permissibility of the representation must be entered in the Citizen Card of the representative. This occurs where the sourcePIN Register Authority having been presented with proof of an existing authority to represent or in cases of statutory representation, enters in the Citizen Card of the representative, upon application by the representative, the sourcePIN of the principal and a reference to the existence of an authority to represent, including any relevant material or temporal limitations […]

and

[…] in cases of professional representation in which no particular proof of authority to represent is required, enters in the Citizen Card of the representative, in a form which can be verified electronically, a reference to the fact that he has been authorised to act as professional representative […]

Since professional representatives may represent hundreds or thousands of clients, it is inconvenient to enter the power of representation for each client in the Citizen Card environment. Further, it does not match practice in traditional proceedings or business processes where - due to their professional license - professional representatives may just claim to represent a particular client. Therefore, in Austrian e-Government professional representatives are identified with a special object identifier (OID), which is included in the qualified certificate of their Citizen Card. Each occupational group has a different value, so different types of

professional representatives can be distinguished according to the OID in their certificate.

For all other types of representations the Austrian e-Government initiative has published a specification for electronic mandates. This specification is based on XML and aims for creating an electronic image of traditional mandates. One might think that representation and electronic mandates might not be a complex task. Popular existing approaches for representation are the permission-based delegation model (PBDM) in role-based access control (RBAC) (Khambhammettu et al., 2006) or delegation in RBAC (Zhang et al., 2003). These models are intra-organisational and do not meet the requirements for an identity management system on a national scale. Attribute certificates used in Public Key Infrastructures (PKI) are also often used for representation. However, representation is usually not limited to a single role, but might be more complex as discussed by Rössler (2009). Representation can be categorised into

- **Bilateral Representations:** Where a mandator empowers the proxy to act in her name.
- **Substitution:** Where an intermediary is indirectly empowered by the mandator to delegate the power of representation to a proxy.
- **Delegation:** Which is similar to substitution, but in this case the proxy does not act in the intermediary's name, but the mandator's name.

The Austrian specification for electronic mandates is able to model all mentioned representation scenarios. The XML structure of an electronic mandate is illustrated in Figure 6. An electronic mandate holds the following core information:

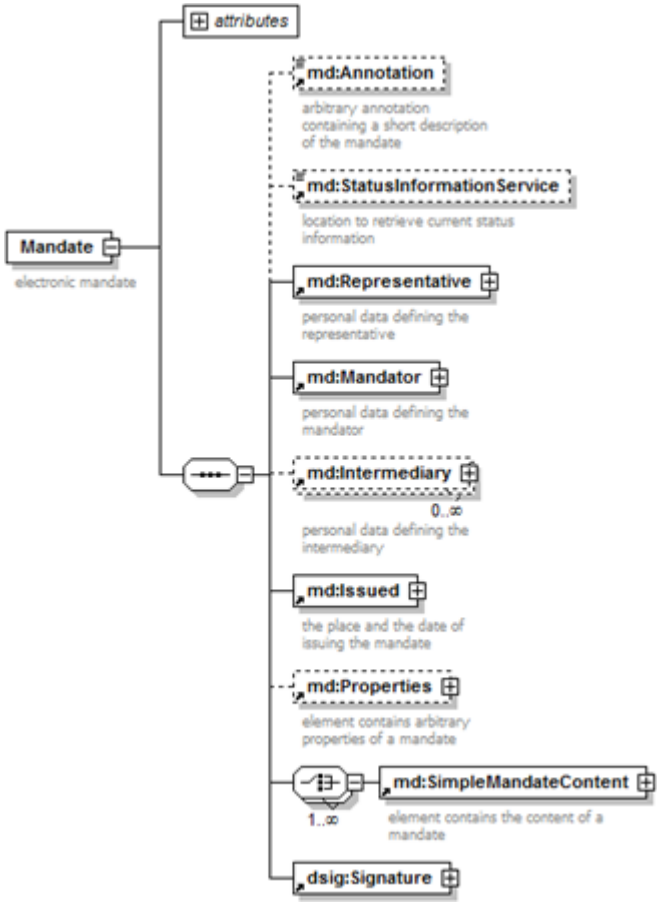
- The proxy's (representative) identification data. This includes the sourcePIN, name, and date of birth.
- The mandator's identification data. In case of natural persons these are the sourcePIN, name, and date of birth. In case of legal persons the full name (e.g. company name) and the register number (e.g. company number) are included.
- In case an intermediary (delegate or substitute) is involved, the according identification data are included.
- Date and time of issuance of the mandate.
- Mandate content as a textual description defining the scope of application, e.g. that the mandate can only be used for certain bank transactions.
- Financial or timely constraints, e.g. that a mandate is only valid up to a certain date or that a transaction can only be carried out up to a certain amount.

This XML structure must be electronically signed by the SourcePIN Register Authority. For authenticity, only mandates signed by this authority are valid mandates in the context of Austrian e-Government.

The Austrian mandate management system is illustrated in Figure 2. The system can be characterized as a central system with just-in-time generation of electronic mandates on the basis of live information retrieved from constitutive registers. The core of the system is the so-called Mandate Issuing Service (MIS). It handles most process steps in the mandate management workflow. The main duties are:

- To accept incoming requests by identity providers, e.g. MOA-ID. Requests have to contain the proxy's identity link and a set of mandate identifiers. In case of professional representative the proxy's certificate has also to be provided. Mandate identifiers are a kind of search filter. For example, an identity provider may only want to accept mandates for bank transactions or tax affairs.

Figure 6. XML structure of an electronic mandate



- To search for a proxy's mandates. The MIS distinguishes between bilateral mandates, i.e. mandates between natural persons, and mandates for legal persons. The SourcePIN Register Authority provides a central service for bilateral mandates. Mandators can access this service with their Citizen Card and register a new mandate, i.e. empower another person. In case of legal persons several (constitutive) registers are accessed. For example, the service searches the company register, the central register for associations, or the supplementary register for legal persons whether the proxy is authorized to solely represent a legal person or not. By using the business service portal, authorized persons of a company can designate certain persons to carry out specific transaction on behalf of the company, e.g. to accept certified electronic mail items. This mandate source is also queried by the MIS.
- Retrieve the mandator's sourcePIN. In case of a bilateral mandate, the mandator's identification data has to be provided in the mandate. This also includes the sourcePIN. Since the register only stores the ssPIN to identify a mandator's mandate, the MIS has to retrieve the mandator's sourcePIN from the SourcePIN register.

How does the authentication process in case of a proxy work? We assume that access to a particular e-Government resource is restricted to certain persons and protected by MOA-ID. When a proxy is trying to access the resource on behalf of another person, the following steps are carried out by MOA-ID and the mandate management system:

- MOA-ID reads the Identity Link from the proxy's Citizen Card.
- The proxy creates a qualified electronic signature and signs a statement (including a unique reference value) that she wants to act on behalf of another person.
- MOA-ID submits the Identity Link, the signature certificate, and a list of mandate identifiers as search filters to the MIS.
- The MIS searches all sources for mandates belonging to the proxy by considering the search filters.
- The MIS returns a URL to MOA-ID, which redirects the proxy to this URL.
- The proxy selects a mandate from the list of available mandates from the sources.
- The MIS electronically signs the selected mandate and redirects the proxy back to MOA-ID.
- MOA-ID fetches the selected mandate from the MIS and finishes the proxy's authentication.

In comparison to the standard MOA-ID authentication without representation (see section *Identification and Authentication of Austrian Citizens*), the proxy is faced with only one more single step.

In case of professional representatives, the MIS presents the proxy a further option when selecting a mandate. The professional representative can choose to represent either a natural or legal person. In case of a natural person, the representative has to enter the client's name and date of birth. The MIS fetches the sourcePIN from the SourcePIN Register and creates the electronic mandate. In case of legal persons, the professional representative can search the constitutive register for company information. For example, by entering the company's name or the company number, the MIS searches the company register for this specific company and creates a dedicated mandate for this company.

CONCLUSION

The Austrian identity ecosystem and its core concepts and building blocks support a broad spectrum of different use cases regarding the secure and reliable identification and authentication of users. Austrian citizens are authenticated by means of their personal Citizen Card, which can be implemented by means of smart cards or mobile phones. Additionally, foreign citizens can make use of the Austrian identity ecosystem to securely authenticate at Austrian e-Government services. Finally, the Austrian identity ecosystem also provides appropriate concepts for the integration of legal identities and electronic mandates.

The comprehensive Austrian identity ecosystem allows for a secure and reliable identification and authentication of national and foreign citizens. Identification and authentication of users are key requirements of most transactional e-Government services. By providing well-designed solutions for various use cases, the Austrian identity ecosystem facilitates the fulfillment of these requirements.

The Austrian identity ecosystem and its core concepts and building blocks is a prime example of a successful application of secure information technology to establish appropriate solutions for security sensitive applications. By relying on approved protocols and architectures, the Austrian identity ecosystem contributes to the overall security of the Austrian e-Government strategy and assures the future success of e-Government in Austria.

REFERENCES

ETSI TS 101 903. (2010). *Electronic signatures and infrastructures (ESI), XML advanced electronic signatures (XAdES) V1.4.2*.

European Commission. (2002). *eEurope 2005: An information society for all*. Geneva, Switzerland: European Commission.

European Commission. (2006). *i2010 eGovernment action plan: Accelerating eGovernment in Europe for the benefit of all*. Geneva, Switzerland: European Commission.

European Commission. (2010). *A digital agenda for Europe*. Geneva, Switzerland: European Commission.

European Parliament. (2000a). *Santa maria de feira European Council. Conclusions of the Presidency*. Geneva, Switzerland: Author.

European Parliament. (2000b). *Lisbon European council. Presidency Conclusions*. Geneva, Switzerland: Author.

European Union. (1999). *Directive 1999/93/EC of the European parliament and of the council of 13: December 1999 on a community framework for electronic signatures*. Brussels, Belgium: European Union.

Fearon, J. D. (1999). *What is identity (as we now use the word)?* Palo Alto, CA: Stanford University.

Federal Chancellery of Austria. (1982). *Service of documents act*. Federal Law Gazette No. 200/1982 as amended by: Federal Law Gazette I No. 5/2008.

Federal Chancellery of Austria. (1991). *General administrative procedure act 1991 – AVG*. Federal Law Gazette No. 51/1991 as amended by: Federal Law Gazette I No. 135/2009.

Federal Chancellery of Austria. (1999). *The Austrian signature act*. Federal Law Gazette I No. 190/1999.

Federal Chancellery of Austria. (2003). *Module for online applications (MOA) - Identification (ID)*. Retrieved from https://joinup.ec.europa.eu/software/moa-idspss/description

Federal Chancellery of Austria. (2004). The Austrian egovernment act: Federal act on provisions facilitating electronic communications with public bodies, entered into force on 1 March 2004, last amended part I, Nr. 111/2010. *Austrian Federal Law Gazette (BGBl) part I Nr. 10/2004*.

Federal Chancellery of Austria. (2008). *The Austrian citizen card*. Retrieved from http://www.buergerkarte.at/konzept/securitylayer/spezifikation/aktuell/

Federal Chancellery of Austria. (2010a). *Implementation of the i2010 initiative in Austria*. Retrieved from http://www.bka.gv.at/DocView.axd?CobId=16635

Federal Chancellery of Austria. (2010b). E-government equivalence decree, decree of the federal chancellor laying down conditions for equivalence under section 6(5) of the e-government act, 2010. *Austrian Federal Law Gazette (BGBl) Nr. 170/2010*.

Hogg, M., & Abrams, D. (1988). *Social indentifications: A social psychology of intergroup relations and group processes*. London: Routledge.

Katzenstein, P. (1996). *The culture of national security: Norms and identity in world politics*. New York: Columbia University Press.

Khambhammettu, H., & Crampton, J. (2006). Delegation in role-based access control. [ESORICS.]. *Proceedings of ESORICS*, *2006*, 174–191.

OASIS. (2012). *Security assertion markup language (SAML), OASIS security services (SAML) TC*. Retrieved from http://www.oasis-open.org/committees/tc_home.php?wg_abbrev= security

Orthacker, C., Centner, M., & Kittl, C. (2010). Qualified mobile server signature. In Meyer, H. M., & Turner, J. A. (Eds.), *IFIP Advances in Information and Communication Technology Series*. Springer.

Rössler, T. (2009). Empowerment through electronic mandate – Best practice Austria. In *Proceedings of 9th IFIP WG 6.1 Conference on e-Business, e-Services and e-Society, I3E 2009*, (vol. 305, pp. 148-160). Berlin: Springer.

White, H. C. (1992). *Identity and control: A structural theory of social action*. Princeton, NJ: Princeton University Press.

World Wide Web Consortium. (2008). *XML signature syntax and processing* (2nd ed). Retrieved from http://www.w3.org/TR/xmldsig-core/

Zhang, X., Oh, S., & Sandhu, R. (2003). PBDM: A flexible delegation model in RBAC. In *Proceedings of the Eighth ACM Symposium on Access Control Models and Technologies SACMAT 2003*, (pp. 149-157). ACM.

ENDNOTES

1 http://www.eid-stork.eu/

2 http://www.eu-spocs.eu/

3 SAML (OASIS, 2012) is a widely used XML standard and framework for the secure exchange of identity and authentication information.

4 XMLDSIG (World Wide Web Consortium, 2008) is a recommendation of the World Wide Web Consortium for XML digital signature processing rules and syntax.

5 XAdES (ETSI TS 101 903, 2010) is an open standard for XLM based advanced electronic signatures.

6 The identity link is repeatedly generated and not permanently stored on a foreign eID card.

7 https://joinup.ec.europa.eu/software/mocca/description