Approaching the Challenge of eID Interoperability: An Austrian Perspective

eGovernment is a key enabler for efficient public administrations and user-friendly governmental procedures. Electronic identities (eID) are crucial for any eGovernment infrastructure as they allow for the remote identification of citizens during online processes. Most EU Member States have already rolled out eIDs for their citizens on a national level. Due to country-specific legal, social, and technical requirements, existing national eID solutions are usually not interoperable. In a converging European society, cross-border applicability of eID based services is of increasing importance. To overcome existing limitations, the European Commission has launched the large scale pilot STORK, which aims to establish an eID interoperability layer based on existing national solutions. Integration of this interoperability layer into existing national eID infrastructures raises various challenges on a technical, organisational and legal level. In this article we focus on the Austrian situation and show how the faced challenges have been overcome. We discuss both the Austrian national eID infrastructure and the STORK interoperability layer and show how these two components have been smoothly combined in order to open the Austrian eGovernment landscape for European citizens.

Arne Tauber

EGIZ - eGovernment Innovation Center, an initiative of Austrian Federal Chancellery, and Graz University of Technology, Austria

Thomas Zefferer

IAIK - Institute for Applied Information Processing and Communications Graz University of Technology - Inffeldgasse

Bernd Zwattendorfer

eGovernment Innovation Center (EGIZ)

Keywords

eID, eGovernment, Austrian Citizen Card, STORK, interoperability, cross-border authentication.

> “Challenges that arise during achieving compatibility with the STORK interoperability layer have been successfully overcome by Austria, which guarantees access to Austrian eGovernment services for European citizens.”

1. Introduction

Inspired by the private sector and its customer-oriented philosophy, national governments endeavour to improve administrative and governmental processes in terms of efficiency and usability. Nowadays, Information and Communication Technologies (ICT) represent key enablers of these efforts and facilitate the mapping of paper based administrative procedures to the digital world. eGovernment – the incorporation of ICT into governmental processes – allows public authorities to reduce bureaucracy and enables citizens to carry out administrative procedures conveniently over the Internet. As such procedures usually comprise privacy sensitive data, the application of appropriate security mechanisms is a crucial requirement for eGovernment services. The reliable identification and secure authentication of remote users is one important pillar, which the overall security of eGovernment services is based on. An elaborated infrastructure for electronic identities (eID) is therefore crucial for any eGovernment service requiring secure user authentication.

During the past years, national governments and public administrations have met this demand by setting up national eID infrastructures. In most cases, national eIDs are nowadays based on smart cards being issued to citizens. Due to country-specific legal, social, and technical requirements and because of varying historical evolutions, Europe is currently facing a heterogeneous ecosystem of isolated eID infrastructures and solutions.

In a converging European society, the importance of national borders decreases while cross-border applicability of online services is an increasing issue. This is also manifested by the Digital Agenda for Europe (European Commission, 2010) and the related eGovernment Action Plan (European Commission, 2010a), explicitly emphasising the importance of electronic means to increase the mobility of citizens and businesses within the Community and to ensure the four freedoms towards a Digital Single Market: free movement of goods, capital, services and people. Unfortunately, the lack of interoperability between different national solutions renders the development of eID based cross-border applications difficult. To leverage interoperability efforts, the European Commission has launched several large scale pilots (LSP). These pan-European projects aim to achieve interoperability of eGovernment services in different fields of application such as eHealth or eProcurement. The corresponding LSPs are epSOS [1] (eHealth) and PEPPOL [2] (eProcurement). The topic eID interoperability is considered by the LSP Secure *Identity Across Borders Linked* [3] (STORK). The fundamental goal of STORK is to achieve interoperability between country-specific eID infrastructures and to facilitate the development and adoption of eID based cross-border applications.

Given the existing heterogeneous ecosystem of national eID solutions, STORK does not try to re-invent the wheel by proposing a common eID solution for all European countries that would replace established approaches. Instead, STORK aims to establish an interoperability layer that is based upon existing country-specific eID solutions. This way, existing approaches that usually perfectly satisfy given national requirements can be maintained while at the same time interoperability with foreign eID infrastructures is assured. Needless to say this approach requires national eID infrastructures to implement an interface to the STORK interoperability layer to support cross-border identification and authentication. Due to national specifics, achieving compatibility between national eID solutions and the STORK interoperability layer can be difficult. Challenges in both the technical and the legal domain have to be overcome in order to integrate existing eID infrastructures into STORK.

In this paper we elaborate on this issue by providing a more detailed insight into the Austrian situation. We discuss the Austrian national eID infrastructure and show which challenges had to be overcome

1 http://www.epsos.eu-
2 http://www.peppol.eu
3 https://www.eid-stork.eu

to achieve compatibility with the STORK interoperability framework. We start our explanations by introducing the Austrian national eID concept and key components of the underlying infrastructure in Section 2. Section 3 emphasises on the STORK project and introduces core features of the developed interoperability framework. Details on the integration of STORK functionality into the Austrian eID infrastructure are discussed in Section 5. Finally, conclusions are drawn in Section 6.

2. The Austrian eID Concept

Reliable identification of citizens is a crucial factor of governmental or administrative procedures. In the traditional scenario, in which citizens personally show up at administrative offices, identity is usually proven by showing an identity card, passport, or similar identity documents. In the digital world things are more complicated as citizens interact with public administrations remotely over the Internet. An elaborate eID and authentication concept is therefore crucial for any interactive eGovernment service that requires certainty on users' identities. In this section we discuss the Austrian eID concept and introduce core components of the Austrian eID and eGovernment infrastructure.

The Austrian Citizen Card (Leitold et al., 2002) represents the key component of the Austrian eID concept. The Citizen Card is an abstract definition of an eID token that belongs to the user and provides the following functionalities:

- Identification and secure authentication
- Creation of electronic signatures
- Storage of additional identity-related information

To allow for the creation of electronic signatures, the Citizen Card concept foresees the secure storage of private signature keys and corresponding public signature certificates. The Austrian Citizen Card concept fulfils the requirements of Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures (Signature Directive) (Council of the European Union, 2000). Due to the equivalence to traditional ID documents and handwritten signatures, citizen cards rely on qualified certificates and Secure Signature Creation Devices (SSCD) as defined by the Signature Directive.

Secure authentication is achieved by requesting the citizen to apply an electronic signature over given identification data. The identification data is stored on the Citizen Card within a special XML-based data structure called Identity Link. This data structure links the citizen's unique identity to the previously mentioned signature certificates that are also stored on the Citizen Card. The citizen's identity is represented by a unique identifier, first and last name, as well as the citizen's date of birth. All this data is encapsulated in the Identity Link data structure. The unique identifier is called sourcePIN and is derived from the user's unique national identification number that is available in Austria's Central Residents Register (CRR). The derivation is based on a 3DES encryption and carried out by the Austrian SourcePIN Register Authority, which is part of the Austrian Data Protection Commission [4]. The SourcePIN Register Authority is in sole possession of the required secret derivation key and therefore the only party in the Austrian eGovernment infrastructure that is able to compute citizen-specific sourcePINs.

Due to existing privacy legislations, neither public nor private sector applications are allowed to store citizens' sourcePINs directly. Hence, the Austrian eID concept follows a sector-specific identification approach. In the public domain, there are for instance predefined sectors for health, finance,

4 http://www.dsk.gv.at/DesktopDefault.aspx?alias=dsken

justice, education and research, agriculture and employment. If the national eID concept is used in the private domain, each company represents an own sector. For each sector in the public or private domain, a unique sector-specific ID is derived from the user's personal sourcePIN. This is achieved by applying a non-invertible hash function over the concatenation of the user's sourcePIN and the particular sector. This way, user activities cannot be traced across different sectors. This enhances the preservation of users' privacy. Figure 1 illustrates the most important steps of the eID derivation process and shows involved parties and components.

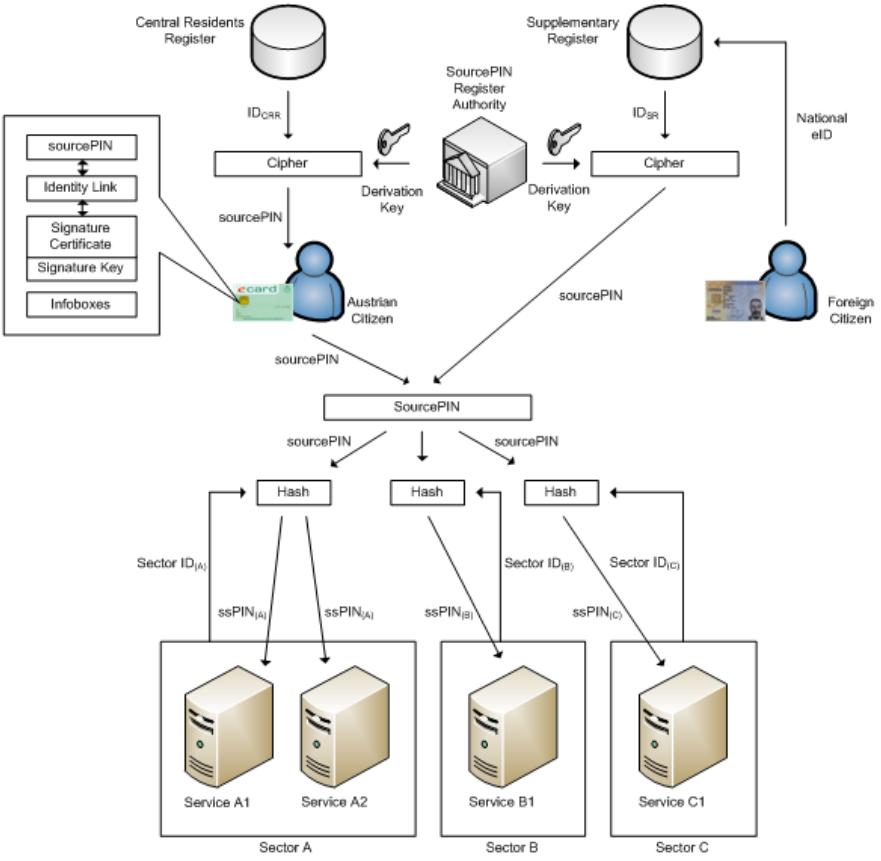

Figure 1: Derivation of electronic IDs

As the entire eID concept relies on the unique identifier stored in Austria's CRR, this solution is basically restricted to citizens listed in this register. In general, this applies only to citizens having their residence in Austria. To overcome this limitation, the Austrian eID concept foresees an additional register, the so called Supplementary Register (SR). Persons not listed in the CRR (e.g. foreign citizens or Austrian citizens currently residing in a foreign country) can register at the SR to become part of the Austrian eID infrastructure. The integration of persons over the SR is also shown in Figure 1.

The Austrian Citizen Card concept is technology neutral. Although its name might suggest the usage of smart cards, the concept is not limited to this technology at all as stated in the Austrian eGovernment Act (Republik Österreich, 2004). In general, Citizen Cards can be implemented by any technology that is able to meet the predefined requirements regarding security and functionality. Currently, Austrian citizens can use smart cards such as their health insurance card, bank cards, or mobile phones to carry out eGovernment procedures.

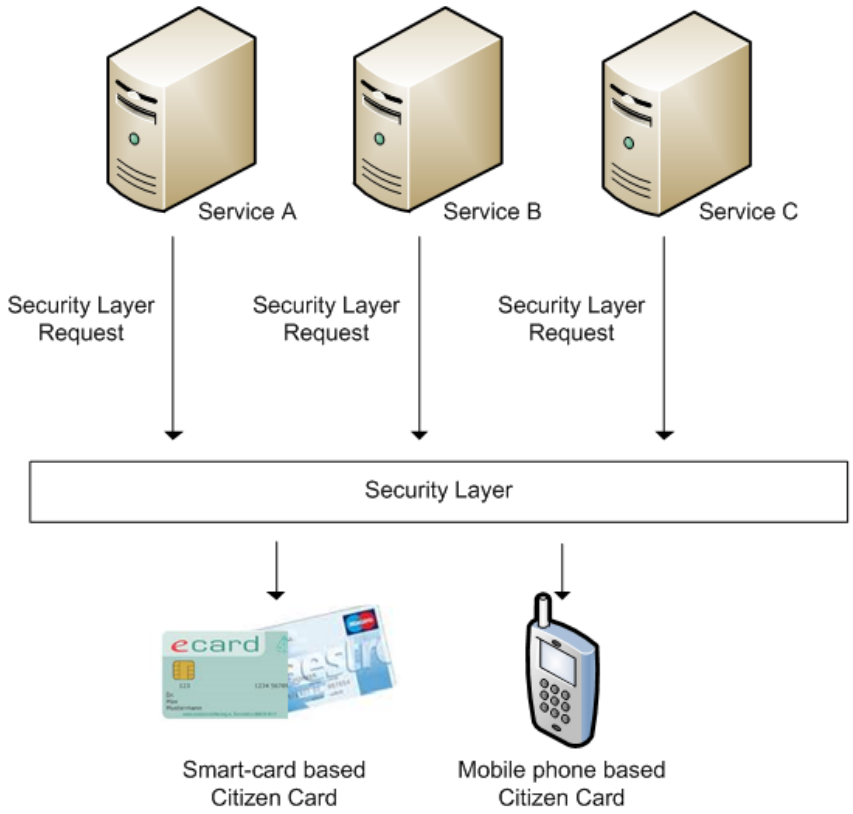

Figure 2: Security Layer concept

To facilitate the integration of the Citizen-Card functionality into eGovernment applications, the Austrian eID concept defines an abstract access layer called Security Layer (Leitold et al., 2002). Figure 2 illustrates the basic concept of the Security Layer Interface. This interface is implemented by the Citizen Card Software (CCS), which on the one side handles access to different Citizen Card implementations (e.g. smart cards) and on the other side provides their functionality to eGovernment services and applications through an abstract XML based interface. Hence, eGovernment services can use a standardised interface to access Citizen Card functionality irrespective of the underlying Citizen Card implementation.

Since the Security Layer specifications are open, various CCS implementations from different vendors are already available [5]. Most implementations follow a client-side approach, which requires users to install the CCS on their local computer. As mandatory software installation and maintenance tasks may harm usability, a minimal footprint solution has also been introduced in Austria. The MOCCA Online CCS (Centner et al., 2009) follows a Java Applet-based approach and does only require minimal local software installations. Since experience has shown that smart cards are a general barrier in terms of usability, an appropriate mobile-phone based alternative is also available in Austria. The A-Trust Mobile Phone Signature[6] combines a central hardware security module (HSM) and the citizen's mobile phone to provide means for secure user authentication and the creation of electronic signatures according to the Austrian Citizen Card and Security Layer specifications. Architecture and security features of this approach have been discussed in detail by Orthacker et al. (2010).

5 http://www.buergerkarte.at/index.en.php
6 https://www.handy-signatur.at

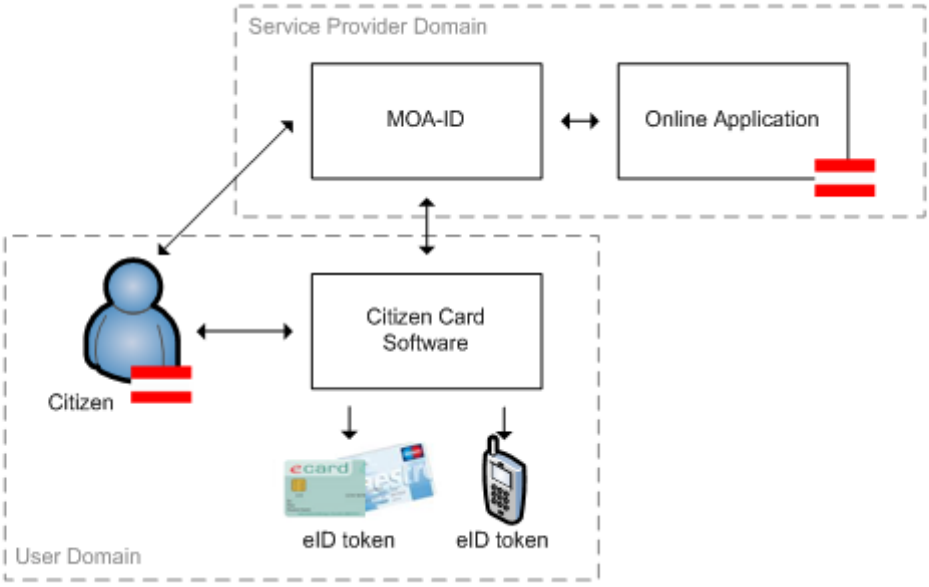

Figure 3: Austrian eID based user authentication process

Although the Security Layer concept facilitates access to Citizen Card functionality, the development of Citizen Card based applications is still a challenging task. To further ease the integration of Citizen Card functionality into eGovernment applications, the Austrian eGovernment infrastructure provides several basic open source modules that encapsulate frequently used Citizen Card functions. For instance, the module MOA-ID[7] implements all required functionality for a Citizen Card based secure user identification and authentication and offers this functionality to external eGovernment applications through a web-service based interface. Hence, eGovernment applications can employ MOA-ID to securely authenticate citizens instead of implementing interaction with the Security Layer interface and underlying eID tokens on their own. Figure 3 illustrates the interaction of the different components. Citizens interact with MOA-ID in order to authenticate and to gain access to online applications. During the authentication process, MOA-ID interacts with the Citizen Card Software through the standardised Security Layer interface in order to access the citizens' eID tokens. In subsequent sections we will show how this basic set-up has been extended in order to achieve compatibility with the STORK interoperability framework.

The MOA-ID module encapsulates most functionalities that are required for the secure eID based authentication of citizens. However, authentication is not the only key feature in eGovernment. Hence, similar to MOA-ID additional modules exist which facilitate the creation and verification of electronic signatures (MOA-SP/SS[6]) or the secure delivery of electronic documents with the quality of certified electronic mail (MOA-ZS[6]).

The Austrian eGovernment strategy foresees various sophisticated concepts that assure both security and privacy preservation within eGovernment. Various publicly available open source components facilitate the integration of eID and eSignature functionality in public and private sector applications. While the Austrian eID and eGovernment infrastructure has already proven to perfectly meet national requirements, the growing demand for cross-border applicability raises various new issues. Key challenges and requirements of eID interoperability will be discussed in the following section.

7 http://egovlabs.gv.at/

3. The EU Large Scale Pilot STORK

3.1 The STORK Background

Electronic identification has become a natural part of our digital life. People are used to authenticating themselves at online shops, mail providers, social networks, or public sector applications. In some cases a high-quality eID is necessary to prevent identity theft or digital twins. This is particularly true in the case of eGovernment applications. Therefore, in the last years, several governmental eID projects have been launched within Europe. Popular examples are the Finish eID card (FINEID) (December 1999), the Estonian eID card (January 2002), the Austrian Citizen Card (2003, mass-rollouts in 2005), the Italian Carta d'Identitá Elettronica (CIE) and Carta Nazionale dei Serivizi (CNS) cards (2003), and the Belgian eID card (2nd half of 2003). All these solutions evolved as national islands and are heterogeneous in various dimensions on a technical, operational and legal level. On technical level many different solutions are used for authentication. These range from username/password and software certificates to mobile eIDs or smart cards based on the use of qualified electronic certificates. From an operational point of view, many different issuers can be found. eID tokens may be issued by the public sector or the private sector, at federated, local or regional level. Legal issues often concern the inclusion and application of unique national identifiers in a flat, sectoral or combined manner.

With vanishing borders and the evolvement of the Internal Market, citizen's mobility within the EU is steadily increasing. This asks for cross-border qualified authentication and identification in equal measure. Some examples are migrant workers, exchange students, social security cases, moving house, eHealth for medical treatments abroad, or even eJustice in cross-border legal proceedings. For this purpose, the European Commission (EC) has launched the European LSP STORK with the aim to provide a technical framework for the cross-border mutual recognition of eIDs. The STORK consortium consists of 32 partners from 17 EU/EEA MS. The project has a total budget of 26.5 million Euro (50% co-financed by the EC), started in May 2008 and runs until December 2011.

Since STORK is a pan-European interoperability project and thus follows the guidelines of the European Interoperability Framework (EIF) (European Commission, 2010b), it respects the European Union principle of subsidiarity and does not change the situation in participating Member States (MS). In contrast, it rather aims at providing an interoperability framework for cross-border recognition of eIDs on top of existing solutions. Naturally, such an ambitious target bears several challenges. First, a consensus between the participating MS is needed on the applied common authentication and identification framework. Existing solutions are quite heterogeneous in their technical nature. Some MS have decentralised or user-centric authentication models, others have centralised models. Solutions also differ in their authentication quality (username/password, software certificates, smart cards, etc.). Second, legal issues may be an obstacle in terms of limiting the use of national identifiers abroad or preventing other cross-border transactions due to different national data privacy regulations. Third, other questions arise concerning liability and trust. Who is responsible if a cross-border data transfer goes wrong or according to what policy can identity sources be trusted? Those are questions and issues that had to be tackled by STORK.

3.2 The STORK Methodology

Regarding eID interoperability, STORK was not faced with a green-field situation. In the course of the IDABC [8] programme, several projects and studies already worked on eID and interoperability.

8 IDABC = Interoperable Delivery of European eGovernment Services to public Administrations, Businesses and Citizens

Examples are the study on eID interoperability (European Commission, 2009), MODINIS [9], FIDIS [10] or the Porvoo Group [11].

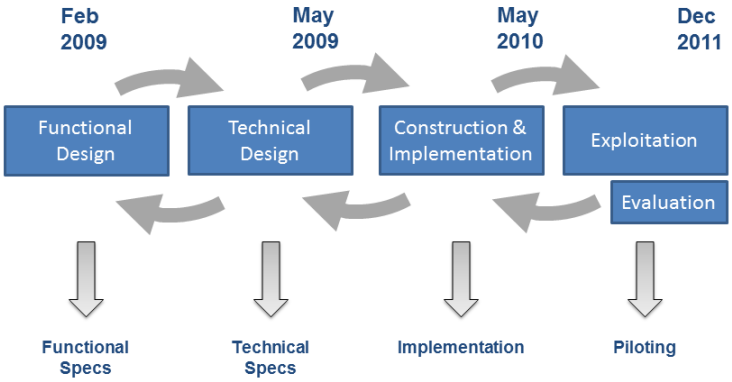

Figure 4: STORK Methodology

Figure 4 illustrates the STORK approach of developing an eID interoperability framework for the participating countries. Each phase is tightly related to a STORK work package (WP). STORK has seven work packages. WP1 deals with project management and WP7 with dissemination, respectively. WP2-6 are technical work packages.

All these work packages contributed to the production of the STORK common specifications and their deployment and demonstrations in the single pilots. WP2 investigated the legal situation in each partner MS and defined a framework mapping of technical and organisational issues to a quality scheme. A survey on state-of-the-art eID and Identity Management (IdM)-related technologies was made by WP3. WP4 sketched the basic process flows of all interoperability model combinations for all by STORK identified use cases: authentication, attribute transfer and certificate validation. The input of WP2 was particularly important to validate whether the process flows were compatible with data protection restrictions in each country. Based on the input of WP3 and WP4, WP5 was in charge of generating the STORK common specifications, main building blocks and architectural models. To validate, demonstrate, and evaluate the developed concepts and components, WP6 has established an interoperability framework across the participating countries and integrated its cross-border authentication components into several operational services. The STORK piloting phase started in summer 2010 with 21 service provider applications.

3.3 The STORK Architecture

A first project milestone – especially carried out by WP2 - was the development of the Quality Authentication Assurance (QAA) framework (Hulsebosch et al., 2009). eIDs in different MS are based on different technologies and have different security levels. This leads to the necessity of a common understanding and standardised way to deal with authentication across the participating countries. A harmonised classification into four well-defined QAA levels allows MS to map national authentication

9 The MODINIS programme was launched in the course of the eEurope 2005 Action Plan and has been continued in the i2010 initiative. Further details are available at http://ec.europa.eu/information_society/eeurope/i2010/archive/modinis/index_en.htm .

10 FIDIS (Future of Identity in the Information Society) was a five-year project in the 6th Framework Programme (FP 6) dealing with Identity Management (IdM) in the European Information Society.

11 The Porvoo Group is a forum for discussion to promote eID interoperability. The group also meets twice a year. Information about the group is available at http://ec.europa.eu/idabc/en/document/4491/5584.html .

levels to the common STORK QAA levels and vice versa. In this way, authentication levels of different MS can implicitly be mapped between each other via the defined QAA scheme. A QAA level integrates several aspects of authentication: registration, credential issue, authentication quality and strength.

Besides the QAA levels, STORK has defined three basic use cases, which built the fundamental basis for the further development of the interoperability model architecture. Those use cases are:

1. **Authentication** - This use case constitutes the cross-border authentication process at service providers in other countries.
2. **Attribute Transfer** - STORK supports the attribute transfer of personal identification attributes (national ID number, name, date of birth, qualification, etc.). These are either retrieved from the eID credential or - if necessary - from an attribute provider (governmental source).
3. **Certificate Verification** - Defines the secure and reliable verification process of electronic signatures.

STORK investigated two interoperability models (Leitold & Zwattendorfer, 2010; Koulolias et al., 2011; Leitold, 2011). The first is the so-called Middleware (MW) model, which provides a user-centric approach for authentication. The second is the so-called Pan-European Proxy Services (PEPS) model, which uses a federated identity approach to delegate the authentication process to the respective national infrastructure. Both models and their combinations are discussed in more detail in the following sections.

3.3.1 MW Model

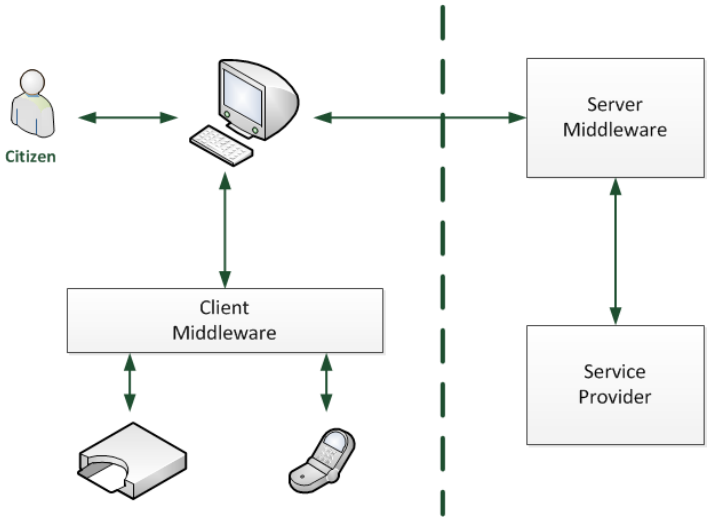

Figure 5: MW Model

Figure 5 illustrates the so-called Middleware (MW) model. This authentication model is user-centric and the identity data is usually stored on or accessed with tokens being in the sole possession of the user, for example a smart card or a mobile phone. The communication with the token is usually provided through a client MW allowing the user to confirm the authentication process with a Personal Identification Number (PIN) or Transaction Number (TAN). In the MW model, service providers aiming to integrate cross-border authentication support must set up a server MW within their operational environment. This software is in charge of handling the authentication process with the user and

the client MW. Therefore, the server-side MW must integrate the authentication mechanisms for all token types it supports, e.g. for different countries.

3.3.2 PEPS Model

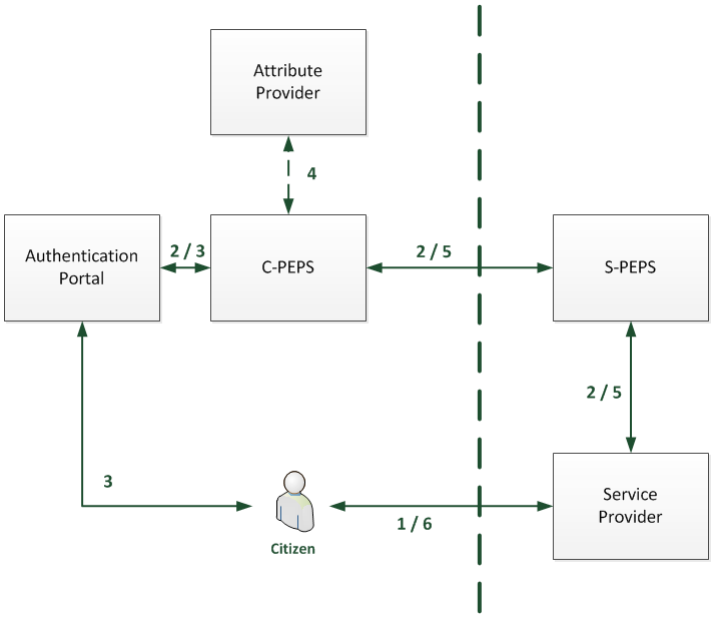

Figure 6: STORK logical PEPS model

In contrast to the user-centric MW model, the PEPS interoperability model uses a federated and proxy-based approach. According to Majava & Graux (2007), any European interoperability framework has to perform a number of basic functions. These include the identification of a local identity provider, the retrieval of identity attributes and the transport of these attributes to a trusted service provider across countries. A service implementing these functionalities is called Pan-European Proxy Services (PEPS). A PEPS can be seen as a single gateway, which on the one side hides national infrastructural complexities and on the other side implements the protocol for cross-border communication. Figure 6 illustrates the cross-border PEPS authentication process from a logical point of view. In detail, the data flow between the involved entities actually runs through the user's browser as bearer. Hence, the STORK authentication protocol has been designed in such a way that identity data between different entities is exchanged and forwarded using HTTPs POSTs conducted by the user's browser.

Consider the scenario where a user from MS A wants to authenticate at a service provider residing in MS B. Both MS host a national single PEPS instance. The PEPS instance of MS A is called C-PEPS (PEPS residing in the citizen's home country) and the PEPS instance of MS B is called S-PEPS (PEPS in the service provider country). Both the C-PEPS and the S-PEPS have a trust relationship with each other. The same holds for the S-PEPS and the service provider. The authentication process is as follows. If a user wants to access a protected resource of the service provider (1), the service provider delegates the authentication process to its corresponding S-PEPS (2), which delegates the process to the C-PEPS of the user's home country (2). The actual authentication is carried out at the C-PEPS or another national identity provider behind it (3). The C-PEPS may also retrieve additional identity information from an attribute provider (4). The authentication and identity information are transferred from the C-PEPS back to the S-PEPS (5), which finally transfers it to the authentication requesting service provider (5). The user is now granted access to the requested resource (6). According to Majava & Graux (2007), this decentralised model can also be compared with a generalised MW approach where

[. . .] a fully decentralised PEPS model can essentially be implemented as a so-called middleware approach, where the PEPS basically functions as a middleware emulator that presents a commonly understood middleware to all SPs, regardless of the authentication method being used.

3.3.3 Comparison of Both Models

When comparing the MW and the PEPS model, several differences become evident. In the MW model, authenticating foreign users directly communicate with the service provider. There are no intermediaries between the user and the service provider, which allows for end-to-end security. Since the authentication data is retrieved from the user's eID, the user remains the data owner; the service provider is the data controller. This authentication model is thus user-centric. Even if this model has a high degree of privacy and security, the major drawback is the dependency on eID token maintenance.

In contrast to the MW model, the PEPS model involves third parties. Since PEPS instances act as intermediary between the user's identity data source and the service provider, a PEPS inevitably becomes an identity data processor and controller. In contrast with the MW model, there is a liability shift from the service provider to the PEPS. Moreover, the MW end-to-end security is replaced with segmented trust relationships in the PEPS model. Even if this model provides a good way to hide complexities of the national authentication infrastructures, the degree of privacy and security is not the same as for the MW model.

Nevertheless, preserving privacy is a major aspect in both models. To be compliant with the EU Data Protection Directive (Council of the European Union, 1995) in both models users must give their consent that their data is used abroad.

3.3.4 Combining Both Models – The V-IDP

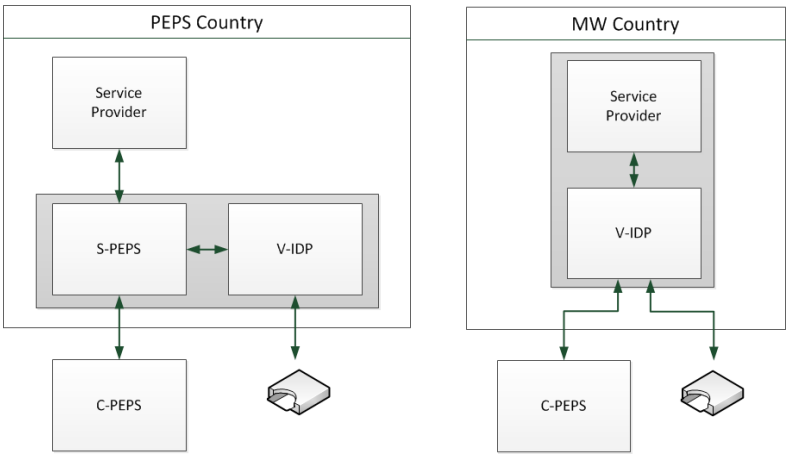

Figure 7: STORK Virtual identity provider

In the discussions above only two scenarios have been sketched. The MW-MW and PEPS-PEPS cross-border scenario. This means that a user from a MW country can only authenticate at a service provider having a server-side middleware installed. In turn, a user coming from a PEPS country can only authenticate at a service provider of a PEPS country. Even if the two interoperability models are quite different, STORK aims for a common interoperability architecture which combines both models

in order to support all possible scenarios. This means

- A user from a MW country can authenticate at a service provider located in another MW country.
- A user from a MW country can authenticate at a service provider located in a PEPS country.
- A user from a PEPS country can authenticate at a service provider located in a MW country.
- A user from a PEPS country can authenticate at a service provider located in another PEPS country.

Even though MW and PEPS have completely different operational models, they can be combined with the concept of a V-IDP, which is illustrated in Figure 7. A V-IDP is a server MW with a PEPS interface so that both instances can communicate with each other. The STORK common specifications have been designed in such a way that major components operate on the same protocols, irrespective of the model or its combinations.

According to Figure 7, a PEPS country may install the V-IDP in the S-PEPS environment so that users from PEPS countries are delegated to their national PEPS and users from middleware countries can directly be authenticated at the V-IDP. The authentication data is then returned back to the service provider over the same interface. In a middleware country a service provider may install the V-IDP so that users from PEPS countries are delegated to their national PEPS and users from middleware countries can directly be authenticated at the V-IDP. In this way both the MW-PEPS and PEPS-MW scenarios can be realised.

4. Implementation and Integration Considerations

The main aim of the STORK project was the provision of an interoperability framework for secure cross-border identification and authentication based upon the various national eID solutions of the participating countries. As previously described, this was not a trivial task as the eID landscape in Europe is very heterogeneous. Having a look at the STORK architecture in Section 4, on the one side the STORK framework had to deal with the implementation of the cross-border identification and authentication protocol for cross-border data exchange and, on the other side, it had to provide appropriate interfaces for integrating different national eID models and concepts. The first challenge had been overcome by implementing the common specification developed by WP5. For the second challenge – the integration of national eID concepts into the STORK framework – no common solution could be provided for all individual national concepts. However, the STORK framework provided well-defined interfaces for integration in both the PEPS and the MW model. This section describes the challenges as well as implementation and integration considerations of the Austrian eID concept into the STORK architecture. As the Austrian eID infrastructure relies on the middleware approach because of liability and privacy reasons, we focus on the middleware model in the remainder of this section.

Although the STORK framework already provided interfaces for the integration of the national infrastructure there were still a lot of challenges that had to be overcome on technical, legal, and organisational level. During integration of STORK functionality into the Austrian eID infrastructure, two different use cases had to be considered. The first use case covers the identification and authentication of Austrian citizens in foreign Member States, while the second use case concerns the acceptance of foreign citizens at Austrian online applications. On a technical level, for both use cases the approved Austrian eID module MOA-ID, which has been introduced in Section 2, built the fundamental technical basis. This module had been further enhanced to meet the requirements for achieving cross-border interoperability for the Austrian eID concept.

The main challenges that had to be faced during the integration of the Austrian eID concept were as follows:

- Technical integration of the Austrian eID concept into the STORK framework
- Mapping between national and common STORK attributes
- Treatment of electronic identifiers
- Authentication Levels
- Privacy Preservation
- User Consent
- Legacy Support

The next two subsections describe in more detail how these challenges were met, distinguishing between the two different use cases on user identification and authentication.

4.1 Authentication of Austrian citizens in foreign Member States

The Austrian eID concept follows a middleware approach. Hence, for this use case the STORK interoperability framework foresees the installation and deployment of a common server-side middleware (Virtual Identity Provider – V-IDP) in the foreign country. Depending on the national interoperability model to be used the V-IDP is either directly installed in the service provider domain (if the MW approach is followed) or in the PEPS domain (if the foreign country relies on the PEPS approach). However, in both scenarios the V-IDP is responsible for the communication with the Austrian eID modules and manages the integration of the Austrian national eID solution.

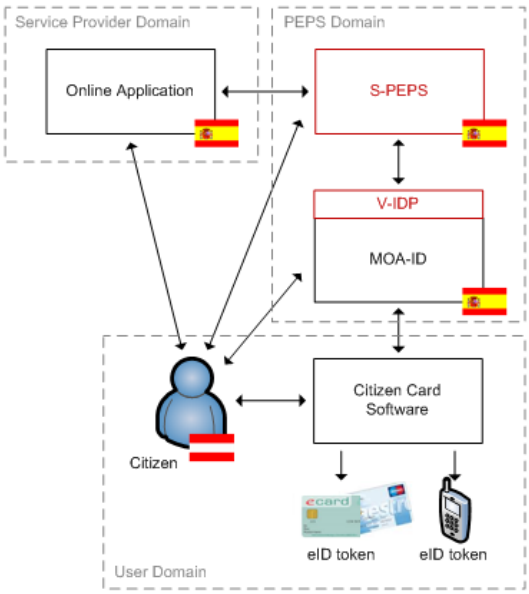

Figure 8: Authentication of Austrian citizens in foreign Member States

In general, the V-IDP defines a server-side middleware solution developed together by Austria and Germany (Leitold & Zwattendorfer, 2010). The V-IDP is set up on a modular architecture and defines

lightweight interfaces for easy integration of national eID modules. Austria has implemented these interfaces by connecting the V-IDP to the Austrian open-source middleware module MOA-ID. In this case, core components of MOA-ID remained unchanged while only the interfaces to the V-IDP needed to be implemented. The implementation of these interfaces on the one hand triggers the authentication process with MOA-ID and on the other hand receives the identification and authentication data from this Austrian module after successful authentication. Figure 8 illustrates the sample scenario of authenticating an Austrian citizen (Middleware country) at a service provider in a foreign country such as Spain (PEPS country). In this example, an Austrian citizen wants to access a protected resource at a Spanish service provider. It is assumed that the user hasn't been authenticated before and thus is redirected to the corresponding national Spanish S-PEPS. After providing information on the respective home country, the user is redirected to the installed V-IDP as Austria follows the MW approach. The V-IDP is responsible for triggering the authentication process at MOA-ID and the user runs through the same authentication process as used when authenticating at Austrian service providers. After having received the identity and authentication information from MOA-ID, the V-IDP returns this information back to the requesting S-PEPS and service provider respectively.

Moreover, after having received the data from MOA-ID the VIDP is responsible for mapping the national Austrian eID attributes (national identifier, first and last name, date of birth) to the according STORK attributes. The exact mapping has been already specified in the design phase. However, as STORK follows the minimal data disclosure principal according to the European Data Protection Directive, only requested attributes are transmitted. Although a user may have consented to the transmission of all his/her identity data only required attributes are transferred to the requesting service provider by the V-IDP. At this point it is important to mention that the user gives his/her consent for the transmission of identity attributes by providing a qualified digital signature. This behaviour is completely equal to a traditional authentication process when authenticating at an Austrian service provider.

A special attribute acts as the user's national electronic identifier which allows unique identification of Austrian citizens in foreign countries. As described in Section 2, each Austrian citizen is assigned a unique identification number (sourcePIN) which is stored on the Austrian Citizen Card. Preserving privacy equally to the domestic Austrian requirements also across borders, this unique identifier must not be transferred to service providers of foreign countries. Therefore, MOA-ID can be configured in such a way that the unique identifier is specifically derived for one single country only by using one-way hash functions. This derived identifier remains unique per country and can be further derived or used regarding the needs and requirements of the destination country. Within the European Union there are no common legal agreements or regulations on how citizen identifiers are treated in a cross-border context. STORK tried to take up this gap and had defined ways and possibilities on how identifiers are used in cross-border scenarios. However, although STORK had provided common recommendations on identifier treatment and usage the national regulations are so heterogeneous that it was decided to leave the responsibility of identifier usage to each Member State.

Another challenge STORK had to tackle was the quantification of the various existing national authentication possibilities. Therefore, WP2 has defined four different authentication levels to get a common understanding on security for the various authentication mechanisms used across countries. The Austrian eID concept is based on qualified electronic signatures and thus allows secure and reliable authentication with the highest authentication level of four in the STORK context.

4.2 Acceptance of foreign citizens in Austria

The acceptance of foreign citizens at online applications using an enhanced Austrian eID framework defines the second relevant cross-border use case. Austria is currently the only country out of the 17 Member States participating in STORK that has a nation-wide legal basis for the acceptance of foreign citizens at domestic governmental applications. Correct interpretation and implementation of these legal requirements is the main challenge to bear in mind when technically implementing the communication with the STORK framework on a national level.

Since the Austrian eID concept is based on qualified electronic signatures, for identification and authentication of foreign citizens, the same level of security is required for granting foreigners access to domestic applications. To achieve this, the create-signature functionality of the STORK protocol is used. By using this functionality, foreign users are requested to give their consent for accessing an online application by creating a qualified electronic signature. Taking the V-IDP - PEPS interoperability model as an example, the V-IDP located in the service provider environment initiates the signature-creation process within the authentication request being sent to the desired C-PEPS. The C-PEPS is responsible for users' signature creation and further returns the created signature to the requesting service provider or V-IDP, respectively. In this scenario, the V-IDP constitutes the module MOA-ID enhanced by STORK functionality. This enhancement includes the implementation of the STORK protocol as well as specifics for foreign citizen treatment according to the Austrian law defined in the Austrian Republic (Republik Österreich, 2010). According to this regulation, European citizens can be equally treated as Austrian citizens in governmental as well as commercial online processes. To achieve this, foreign citizens must be registered in the Austrian supplementary register as described in Section 2. The registration is based on foreign citizens' consent expressed by a qualified electronic signature. The identity data to be used for registration covers the foreign unique identifier, first and last name of the citizen, and the date of birth if present in the citizen's qualified certificate. However, in order to protect privacy, the foreign unique identifier himself is stored but a special derivation of it. Due to that, foreign users experience the same privacy protection as Austrian citizens. Even if foreign citizens want to access certain services of different sectors, the unique identifier stored in the supplementary register is uniquely derived for every target sector as it is currently done for all Austrian citizens.

Figure 9 illustrates the implemented architecture for accessing the STORK framework. In this sample scenario, a Spanish citizen wants to access certain protected resources at an Austrian service provider. The online application of the service provider is protected by the STORK-enabled version of MOA-ID (V-IDP) which enables cross-border authentication. In our example, via a country selection template, the user can select his/her original nationality and hence is redirected through the enhanced MOA-ID module to the Spanish C-PEPS. The authentication request also contains a signature creation request as Austrian governmental service providers require a qualified signature for authentication. The Spanish C-PEPS manages the complete authentication and identification process. There may be other national specific services involved in this process but these details have been omitted for the sake of clarity. However, the C-PEPS is also responsible for creating a qualified electronic signature of the citizen. If successfully authenticated, the C-PEPS transmits a message including identification, authentication as well as citizen signature data back to the requesting V-IDP. The V-IDP verifies this message and registers the foreign user in the supplementary register based on the data received. The registration takes place completely on the fly, no further user interaction is required. If the user has successfully been registered, identification and authentication data is transferred to the online application and access to the protected resource is granted.

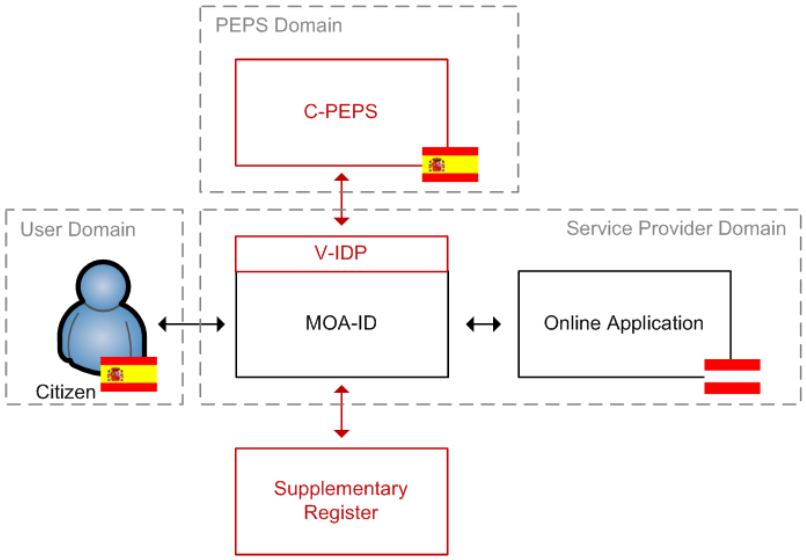

Figure 9: Acceptance of foreign citizens in Austria

To support foreign citizen identification and authentication, MOA-ID was amended by the integration of connectors to the STORK framework. However, STORK also defines its own communication possibilities for service providers to start an authentication process. One main requirement before enhancing the MOA-ID module was the support for legacy applications. Therefore, MOA-ID implements a mapping between the national authentication protocol and the STORK protocol. Due to that, existing applications can remain untouched but still can experience the features of cross-border authentication possibilities.

5. Conclusions

Information and Communication Technologies penetrate more and more our daily life. This also holds for the governmental sector as eGovernment aims to improve efficiency, usability and cost reductions. The advantages of transforming traditional, paper-based processes into fully-fletched electronic processes apply to all involved parties, pertaining public authorities, citizens, and businesses. As such online services become more and more sophisticated and due to the processing of sensitive data, security and privacy are important topics to be concerned about when designing and developing eGovernment applications. Therefore, secure identification and authentication of citizens play a major role in such online applications.

Although username/password authentication schemes currently still represent the dominant authentication approach on the Internet, several weaknesses are known to this mechanism. Thus this approach cannot provide the high level of security required in governmental applications when processing sensitive data. Because of that, several Member States have already rolled-out national eID solutions relying on stronger two-factor authentication mechanisms (e.g. based on smart-cards or mobile phones) which provide a higher level of security. Austria was an early adopter in this field and has already introduced its Citizen Card concept in 2002. However, many other countries have secure and established eID solutions in place too.

Nevertheless, all of these eID concepts have been mostly designed and developed to satisfy domestic needs only. Therefore, a very heterogeneous eID landscape can be found across Europe on a technical, legal and organisational level. All these solutions usually lack on cross-border applicability, which makes it impossible for citizens to authenticate themselves at online applications of foreign countries using their own national eIDs. STORK tried to fill this gap by developing and implementing an eID

interoperability framework for secure identification and authentication of citizens across EU Member States. STORK depicts one of the four EU large scale pilot projects co-funded by the European Commission and aims to achieve interoperability between the various eID infrastructures that are currently in place across Europe. In other words, with the help of STORK, acceptance of foreign citizens at domestic online applications becomes possible.

Although STORK produced precise specifications and architectural descriptions for the cross-border interoperability framework, integration and connection of national eID infrastructures was an open issue. Austria took this challenge by enhancing well-approved and widely deployed national eID modules such as MOA-ID to achieve STORK compatibility. Nevertheless, as Austria is currently the only country having a legal basis for acceptance of foreign eIDs in online processes, several national legal requirements had to be taken into account during the integration of the STORK functionality. Respecting the Austrian law, foreign citizens are registered in the so-called supplementary register by the means of qualified certificates and are treated equally like local residents.

STORK has already demonstrated its functionality and applicability in several pilot applications. Due to its acceptance in the European scientific and business communities, the STORK project can be seen as a success. However, there are still some open questions, which require further investigations and discussions. Examples are the missing legal framework for EU cross-border scenarios, the unregulated treatment of foreign identifiers or liability and accountability issues. The project STORK ended in the year 2011. However, the successor project "STORK 2" is already in the starting blocks and will try to tackle these issues left open.

6. References

Centner, M., Orthacker, C. & Bauer, W. (2009). Minimal-Footprint Middleware for the Creation of Qualified Signatures. In: Proceedings of the 6th International Conference on Web Information Systems and Technologies, 64-69.

Council of the European Union (1995). DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

Council of the European Union (2000). DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures.

European Commission (2009). Study on eID Interoperability for PEGS: Update of Country Profiles Analysis & assessment report.

European Commission (2010). A Digital Agenda for Europe. In COM(2010) 245 final/2.

European Commission (2010a). The European eGovernment Action Plan 2011-2015 - Harnessing ICT to promote smart, sustainable & innovative Government. In: COM(2010) 743.

European Commission (2010b). European Interoperability Framework (EIF) for European public services. In: COM(2010) 744 final.

Hulsebosch, B., Lenzini, G. & Eertink, H. (2009). STORK Deliverable D2.3 Quality authenticator scheme.

Koulolias, V., Kountzeris, A., Crespo, A., Leitold, H., Zwattendorfer, B. & Stern, M. (2011). STORK e-Privacy and Security. In: Proceedings of 5th International Conference on Network and System

Security (NSS 2011), 234-238.

Leitold, H., Hollosi, A. & Posch, R. (2002). Security Architecture of the Austrian Citizen Card Concept. In: 18th Annual Computer Security Applications Conference (ACSAC 2002), 391-402.

Leitold, H. & Zwattendorfer, B. (2010). STORK: Architecture, Implementation and Pilots. In: ISSE 2010 Securing Electronic Business Processes: Highlights of the Information Security Solutions Europe 2010 Conference, 131-142.

Leitold, H. (2011). Challenges of eID Interoperability: The STORK Project. In: Privacy and Identity Management for Life - IFIP Advances in Information and Communication Technology, 144-150.

Majava, J. & Graux, H. (2007). Common specifications for eID interoperability in the eGovernment context.

Orthacker, C., Centner, M. & Kittl, C. (2010). Qualified Mobile Server Signature. In: Proceedings of the 25th TC 11 International Information Security Conference, SEC 2010.

Republik Österreich (2004). Erlassung eines eGovernment-Gesetzes sowie Änderung des Allgemeinen Verwaltungsverfahrensgesetzes 1991, des Zustellgesetzes, des Gebührengesetzes 1957, des Meldegesetzes 1991 und des Vereinsgesetzes 2002.

Republik Österreich (2010). Verordnung des Bundeskanzlers, mit der die Voraussetzungen der Gleichwertigkeit gemäß § 6 Abs. 5 des eGovernment-Gesetzes festgelegt werden (eGovernment-Gleichwertigkeitsverordnung).

Authors

Arne Tauber
EGIZ - eGovernment Innovation Center
An initiative of Austrian Federal Chancellery, and
Graz University of Technology, Austria
arne.tauber@egiz.gv.at
http://www.epractice.eu/en/people/258625

Thomas Zefferer
IAIK - Institute for Applied Information Processing and Communications
Graz University of Technology - Inffeldgasse
thomas.zefferer@iaik.tugraz.at
http://www.epractice.eu/en/people/tzefferer

Bernd Zwattendorfer
eGovernment Innovation Center (EGIZ)
bernd.zwattendorfer@egiz.gv.at
http://www.epractice.eu/people/bzwattendorfer