Karl Christian Posch, Reinhard Posch, Arne Tauber, Thomas Zefferer, and Bernd Zwattendorfer - "Secure and Privacy-preserving eGovernment - Best Practice Austria" - Rainbow of Computer Science, Volume 6570, 2011, pp. 259-269
URL: http://link.springer.com/chapter/10.1007/978-3-642-19391-0_19
The original publication is available at www.springerlink.com

Secure and Privacy-preserving eGovernment – Best Practice Austria

Karl Christian Posch, Reinhard Posch, Arne Tauber, Thomas Zefferer, and Bernd Zwattendorfer

Institute for Applied Information Processing and Communications, Graz University of Technology, Inffeldgasse 16a, A-8010 Graz, Austria

Abstract. In the past, contact with public authorities often appeared as winding way for citizens. Enabled by the tremendous success of the Internet, public authorities aimed to react on that shortcoming by providing various governmental services online. Due to these services, citizens are not forced to visit public authorities during office hours only but have now the possibility to manage their concerns everywhere and anytime. Additionally, this user friendly approach also decreases costs for public authorities.
Austria was one of the first countries that seized this trend by setting up a nation-wide eGovernment infrastructure. The infrastructure builds upon a solid legal framework supported by various technical concepts preserving security and privacy for citizens. These efforts have already been awarded in several international benchmarks that have reported a 100% online availability of eGovernment services in Austria.
In this paper we present best practices that have been followed by the Austrian eGovernment and that have paved the way for its success. By virtually following a traditional governmental procedure and mapping its key stages to corresponding online processes, we provide an insight into Austria's comprehensive eGovernment infrastructure and its key concepts and implementations. This paper introduces the most important elements of the Austrian eGovernment and shows how these components act in concert in order to realize secure and reliable eGovernment solutions for Austrian citizens.

Keywords: eGovernment, Austrian citizen card, eID

1 Introduction

The Austrian eGovernment has been awarded with top ranks in several European-level eGovernment studies during the past couple of years. Among the key concepts for this success were the solid treatment of the citizen's right for privacy and data protection, together with best-practice procedures for identification when necessary. It is thus no surprise that Austria's eGovernment has influenced the European development to a significant extent. The advances with the Digital Agenda prove that this avenue was rightly taken. eID and electronic signature play an outstanding role within this new European Commission effort now.

In this paper, we look at the overall scope of Austria's eGovernment services. We will virtually follow an eGovernment process from the application stage towards back-office processing and final delivery. Moreover, we will also point out typical potential security risks and measures taken to counter these risks to guarantee a secure and reliable eGovernment process. It becomes apparent that the quality of administrative services can be significantly improved with eGovernment processes while, at the same time, these services can also be delivered at a much lower cost than with traditional procedures.

Most often in the past, contact with public authorities has typically been tedious for citizens. People were often forced to spend hours queuing in front of counters or filling complex forms without helping assistance. More recently, public authorities have been positively influenced by the private sector, where customer friendliness is key for success. By improving traditional procedures in terms of efficiency and customer orientation, citizens have developed from pure suppliants to emancipated customers. In this context, public authorities have evolved to customer-oriented service providers satisfying the needs of their customers.

In parallel to this development we could observe significant advances in information technology. Especially the success story of the Internet has had a significant impact on various areas of life during the past decades. Public authorities reacted to this trend and started to offer different online services for citizens too. Driven by the aspiration to continuously improve existing procedures in terms of efficiency and customer friendliness, public authorities aimed to employ the Internet in order to spare citizens personal visits at administrative offices.

The online processing of procedures involving citizens and public authorities has the potential to improve common paper-based procedures significantly. Austria was one of the first countries that recognized this potential and started to build a comprehensive eGovernment infrastructure early on. Nevertheless, the new electronic approach also raised many new challenges. Considering the fact that various procedures are potentially dealing with data which are sensitive with respect to privacy and security, it is crucial that they are at least as reliable and as secure as their traditional non-electronic pendants. In order to guarantee the integrity and security of eGovernment infrastructures, these aspects need to be defined not only on technical level, but also on legal level. Therefore, in Austria the E-Government Act [7], which has come into effect in 2004 and has been amended in 2008, defines the legal framework for all eGovernment procedures in Austria.

Basing on the given legal framework, Austria has taken the challenge to develop a comprehensive and future-proof eGovernment framework. Austria's early investments in eGovernment and future technologies have already paid off: In the past years, several international benchmark [5] [4] [3] have reported a 100% online availability of eGovernment services in Austria.

In this article, we describe key components of the Austrian eGovernment. We present best practices which have contributed to its success. The article

guides the reader through a typical eGovernment procedure and introduces basic concepts and building blocks of the Austrian eGovernment infrastructure. By reading this paper, the reader will get an understanding of the overall technical setup that has paved the way for the success of the Austrian eGovernment.

In section 2 we describe an exemplary procedure and identify its three basic stages. With this we briefly introduce a typical administrative procedure. In subsequent sections we provide details on these three fundamental stages and show how their different requirements have been met. In this way, we provide the reader with an overview of the Austrian eGovernment with its relevant core components and basic concepts, as well as concrete implementations. Finally, we draw conclusions and give a brief outlook towards future developments and trends.

2 Common Structure of Administrative Procedures

Procedures at public administrative offices have been purely paper-based for centuries. Those procedures involving citizens and public authorities can generally be subdivided into three basic stages, as illustrated in Figure 1. These stages are *Application*, *Back-office processing* and *Delivery*. In this section we identify these main stages by looking in some detail at the issuance of a criminal-record certificate.

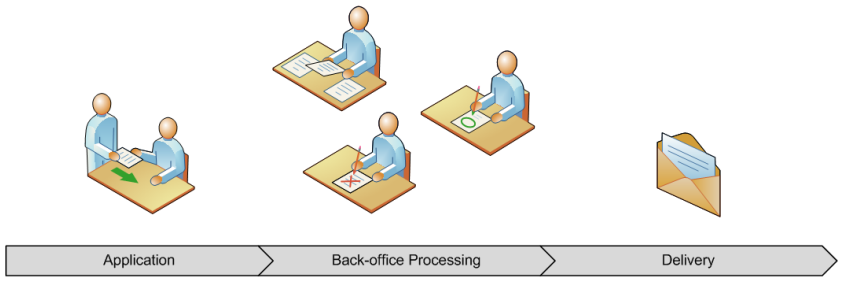

Fig. 1. Three stages of administrative procedures

Administrative procedures are guided by legal requirements. When mapping traditional paper-based administrative procedures to electronic web-based services, basically the same requirements as for paper-based approaches hold true. In the remainder of this section we identify some key requirements relevant for each of these three stages.

In order to request the issuance of a criminal-record certificate, a citizen has to formally apply in order to trigger the adequate administrative procedure. Thus, *Application* is the initial phase of many governmental processes. In traditional governmental processes, usually a paper-based application form has to be

filled by the applicant. This is quite often only possible during office hours of the responsible public authority. The case officer in charge verifies the provided application data and the citizen's identity by checking an ID document presented by the citizen. Authentication of the applicant and verification of the citizen's application data are thus the key elements of this first stage.

Then follows *Back-office processing*. In this phase, case officers manage all necessary processes for responding to the applicant's request. In order to issue a criminal-record certificate, for instance, the case officer has to examine whether there are any crimes registered for the particular citizen. When all required data has been collected, an appropriate paper-based criminal-record certificate is finally generated. In order to prove the authenticity of this certificate, the document is signed by the public authority. The key elements of this second stage are thus the efficient and reliable processing of internal files and data records, and the signing of documents by the public authority.

In the final phase, *Delivery*, the case officer in charge delivers the requested certificate to the applying citizen. In traditional paper-based procedures, the certificate is usually delivered either directly to the citizen during office hours or via registered mail. Thus, reliable and evidential delivery of documents is of major importance in order to close the electronic process in a proper manner.

Depending on the service and the degree of user interaction, eGovernment services are usually subdivided according to a maturity model consisting of five classes: *Information*, *one-way interaction*, *two-way interaction*, *transaction*, and *targetisation/automation*. This model has also been applied by Capgemini for the eGovernment benchmark reports [5]. The example procedure discussed in this paper—Issuance of a Criminal-Record Certificate—is a fully transactional service, and thus falls into the class *transaction*.

In the following sections, we show how the three phases of classical administrative procedures have been implemented within the Austrian eGovernment. In doing so, we describe the core elements, the key concepts, and some methods of the awarded Austrian eGovernment.

3 Electronic Application

Similar to traditional governmental processes, identification, authentication and signatures play an important role within electronic government, too. When applying for certain services, for instance, a citizen often needs to be uniquely identified. This holds true for traditional paper-based procedures as well as for their electronic equivalents. Austria's eGovernment solution for mapping identification, authentication, and signatures into the digital world is the so-called *Austrian citizen-card concept* [8]. The idea behind this concept is to provide both, citizens as well as administrative online-service providers, secure and reliable means for identification and authentication in online eGovernment processes. Generally, this concept is independent from technology and platform, and supports various functions such as the creation and verification of electronic signatures or the encryption and decryption of electronic documents.

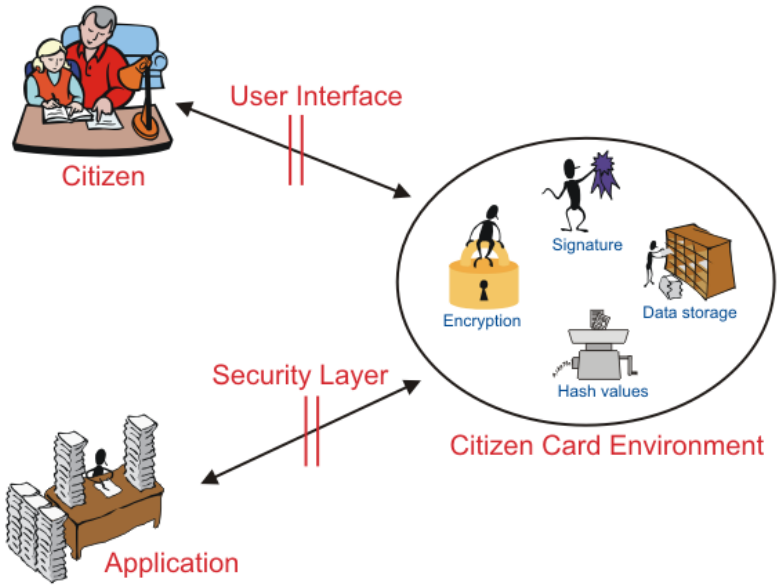

Fig. 2. The Austrian Citizen Card Concept [1]

Figure 2 illustrates the Austrian citizen-card concept. Basically, three parties are involved in this concept: The citizen who wants to use a certain service, the relying party and—acting as intermediary—the so-called citizen-card environment (CCE). The citizen-card environment decouples all security-related functions from the underlying citizen-card technology. For example, the citizen card can be a smartcard, e.g. bank card, student card or health-insurance card[1] or also a mobile phone. Thus, applications that want to access a certain functionality of the citizen card just need to communicate with the citizen-card environment. The citizen-card environment handles all technology-specific operations, e.g. secure smartcard communication. The communication between the application and the citizen-card environment is based on a defined interface, the so-called security-layer interface [1]. This interface is XML-based and its protocol messages can be transported over HTTP or TCP.

According to the citizen-card concept, the citizen-card environment can either run on the citizen's local computer or on a remote server accessible via the Internet. Currently, several proprietary and open-source implementations for a local citizen-card environment exist. An open-source implementation based on Java-Applet technology for a server-based citizen-card environment has been discussed in [6]. In this case, only a minimal piece of software needs to be installed on the local system to handle the communication with the smartcard –

[1] Currently, each Austrian citizen possesses such a health-insurance card where the citizen-card functionality can be simply activated.

namely the Java Applet in the user's web browser. An alternative for server-side signature creation uses mobile phones as secure devices for authentication. This option has been discussed in [11]. In this latter approach, security functions are implemented by a server-side hardware security module, but authorized via a mobile transaction number (mobile TAN) sent via SMS to the user.

In 1999 the European Union has published the so-called EU Signature Directive [12] which focuses on qualified electronic signatures. Such qualified electronic signatures are legally equivalent to hand-written signatures. Thus, almost any governmental process where a citizen's signature is required can also be processed online. Qualified signatures according to this directive can be generated by an Austrian citizen card. However, qualified electronic signatures can also be used for secure authentication in eGovernment processes. Authentication is an important process to verify that a citizen is the certain person she claims to be. To simplify the authentication process for online-service providers, an open-source module for identification and authentication has been developed. A server-side middleware named MOA-ID (Module for Online Applications – Identification) [10] acts as intermediary between the citizen-card environment and the actual online application. In this way, the online application does not need to communicate directly with the citizen-card environment, but instead receives all data required for identification and authentication via a standardized interface (SAML [15]). Initially, MOA-ID reads the citizen's identification data via the citizen-card environment from the citizen's smartcard or another equivalent device. This identification data is stored within an XML data structure. After this first step, i.e. identification, the citizen is asked to sign an appropriate text to confirm her authentication request towards the online application. Finally, the citizen's signature is verified and an authentication token containing relevant identification and authentication information is assembled and transmitted to the online application.

An fundamental aspect of authentication in administrative processes is delegation. Austria is the only country in Europe having automated mechanisms for delegation. In paper-based procedures, mandates are used to attest that a person is empowered to represent another person. We can find the application of mandates in several scenarios, e.g. in court proceedings. Other examples are the procuration in commercial transactions when acting on behalf of a company, or a postal mandate when receiving deliveries on someone else's behalf. Electronic mandates belong to the core of the Austrian eGovernment strategy. Empowerment is established through electronic mandates based on XML structures stored on the citizen card. This approach has been discussed in detail in [14]. In the course of an identification process based on MOA-ID, electronic mandates are read out and validated together with the citizen's electronic signature.

After completion of the *Application*, the citizen-related information that has been collected in this first step is handed over to appropriate *Back-office processes*.

4 Back-office Processes

Citizens trigger administrative procedures by making a formal application. In Austrian eGovernment services, this is usually done by means of appropriate web forms in connection with the citizen card. The applicant's citizen card allows a secure and reliable remote user authentication and it allows the citizen to sign applications online. As soon as the electronic application form is transmitted to the responsible public authority, related back-office processes are started. The objective of these processes is the appropriate processing of the applicant's request. In case of our example process here, i.e. issuance of a criminal-record certificate, back-office processes involve the collection of the particular applicant's criminal records and the preparation of an electronically signed criminal-record certificate.

The *efficient* processing of back-office processes is an important requirement for public authorities not only in Austria, but in the entire European Union. According to the Services Directive [13], which has been published by the European Parliament and the Council on 12 December 2006, and which had to be implemented by EU Member States by 28 December 2009, procedures and formalities need to be simplified. In this way, the establishment of businesses and the provision of services within the European Union is aimed to be facilitated for both, natural and legal persons.

In the remainder of this section, we show how efficient back-office processing according to the requirements defined by the EU Service Directive is accomplished within the Austrian eGovernment. Thereby, we put the focus on the internal processing of electronic files and data records, and the application of electronic signatures by public authorities.

The internal processing of files and data records is one of the key challenges of administrative back-office processes. While paper-based files have built the basis of such processes until now, information technologies have significantly enhanced theses processes in terms of efficiency during the past decades. In Austria, public authorities make use of the so-called electronic file system (Elektronischer Akt, ELAK) that allows for processing of electronic records free of media breaks. The ELAK is a key element of the Austrian eGovernment strategy. As a workflow management system for internal work processes, it supports a seamless cooperation free of media breaks between different administrations and enables a one-stop administration for citizens. All Austrian ministries are connected to the electronic file system of the federal administration (ELAK im Bund, EiB). The EiB is operated by the Federal Data Processing Center and, since its start in 2001, about 9500 workstations have been connected to this system. Both, public administrations and citizens, benefit from the electronic file system. Besides the benefits mentioned, case officers can easily access, search for, and timely edit documents. Since all documents are digital, there are no unnecessary delivery delays when sharing or disseminating them. Citizens can thus receive documents and notifications 24 hours a day, 7 days a week.

Besides the efficient internal processing of files and data records, the preparation of electronic documents is the second key requirement for back-office pro-

cesses in the Austrian eGovernment. In order to ensure data-origin authentication, for example in official notifications, documents being issued by public authorities need to be signed. Signatures applied by public authorities are usually referred to as *official signatures*.

The Austrian solution for electronic official signatures has been discussed in [9] and addresses two basic objectives. First, Austrian official signatures allow citizens to reliably verify that the signer actually is a public authority or a public official. This has been achieved by defining an registered X.509 object identifier (OID) as extension to the signature certificate. The OID reliably identifies signatures being applied by public authorities, and allows citizens to verify whether or not obtained documents originate from public authorities.

The second objective that has been addressed by the Austrian solution for official signatures is resistance against media breaks. This means that the electronic signature of digital documents remains verifiable even if this document has been printed to paper. This objective has been achieved by relying on pure text-based electronic signatures. This means that all signed content needs to be based on text and must be visible on the document in order to allow a manual reconstruction from printouts. Furthermore, all information covered by the applied electronic signature must be printed out on the document as well. Amongst others, this includes the signature value, information about the signatory, and a link to a signature verification service that can be used to verify the document's signature.

Another key benefit of the Austrian official signature is its technology independence. The method used is applicable to various document formats including XML, PDF, and Microsoft Office documents. This allows for a widespread and flexible use of official signatures according to the needs of the particular application.

The electronic file system and official signatures represent the basic building blocks of back-office processes in the Austrian eGovernment. By guaranteeing an efficient processing of digital data records and allowing for reliable data-origin authentication, these two concepts contribute to the awarded quality of Austrian eGovernment.

5 Electronic Delivery

Governments and public administrations deliver important documents (e.g. subpoenas) in a reliable and evidential way. Registered and certified mail are useful vehicles serving this purpose in the postal world. Registered mail gives senders extended tracking possibilities and evidence of having submitted a particular delivery at a certain point in time. Certified mail provides a further proof of receipt signed by the recipient or a delegate. Document delivery is usual the last phase of an administrative procedure. Within eGovernment, an electronic equivalent is required to ensure a process free of media breaks. Standard mailing systems like e-mail have a poor evidential quality. They can rather be compared to send-

ing a postcard, which lacks integrity, confidentiality, sender-identity information, authenticity, and non-repudiation.

In the Austrian eGovernment a certified mail system (CMS) is being used. As one of the first systems, the Austrian *document delivery system* (DDS) has been established in 2004 to facilitate reliable and evidential communications with public bodies over the Internet. The legal basis of this system is laid down by the Law on the Delivery of Official Documents [2]. The Austrian DDS defines four types of participants: Senders, recipients, delivery agents, and a central lookup service (CLS). Delivery agents operate certified mail services by providing the following two mail handling functionalities: Mail delivery agents (MDA) for senders, and mail transfer agents (MTA) for recipients. Delivery agents must be approved by the Federal Chancellery for compliance with technical, organizational and legal requirements. So far, three providers have been approved. Two private sector companies[2] and the Federal Data Processing Center[3]. The system is free of charge for all recipients. Recipients can register with any delivery agent, even with multiple. Registration is based on the Austrian citizen card. This ensures qualified authentication and identification procedures in order to provide a high service quality for senders. A hallmark of the Austrian DDS is its communication architecture. In contrast to e-mail-based architectures, senders are not required to register with delivery agents. They must register with the central lookup service (CLS) instead. The CLS is a register, operated by the Federal Chancellery, holding the data of all recipients registered with any delivery agent. This is necessary because the Austrian DDS has no domain-based communication architecture like e-mail. It is not possible to determine a recipient's delivery agent just on the basis of the recipient's address data. The main delivery process steps are as follows:

1. Senders query the CLS to find out with which delivery agent a recipient is registered with. Due to data privacy protection the CLS returns only a minimalistic set of data sufficient to correctly address a recipient: an encrypted delivery token holding the recipient's unique identifier, the URLs of recipient's delivery agent(s), supported MIME types by the sender and an optional encryption certificate.
2. Senders directly transmit a delivery to the recipient's delivery agent. The communication protocol is based on web-services technology using the simple object access protocol (SOAP).
3. The delivery agent informs the recipient that a delivery is ready for pick-up.
4. The recipient authenticates at the delivery agent and confirms the reception of a new delivery by creating a qualified electronic signature (QES) using her citizen card.
5. As a result, the delivery agent returns this non-repudiation of receipt (NRR) evidence back to the sender.

[2] https://www.meinbrief.at, https://zustellung.telekom.at
[3] https://www.brz-zustelldienst.at

The Platform Digital Austria has developed an open-source module called MOA-ZS (Modules for Online Applications – ZuStellung) to facilitate the integration of the certified-mail functionality into senders' back-office applications. MOA-ZS defines a middleware implementing the four key functionalities required for using the Austrian DDS: CLS query, payload encryption, document delivery, and reception of returning NRR evidences. The module is provided as an open-source module to foster the take-up by public administrations and the adoption and extension by private businesses. With some minor restrictions, the Austrian DDS can also be used by private businesses to deliver documents with the quality of certified mail. Security and privacy for recipients have been strengthened in the case of private senders to ensure a high level of trust in this system. With this public-private sector shared system, the Austrian DDS has demonstrated its abilities on a national level to be deployable on the large scale. A next challenge for the Austrian DDS, especially within the context of the European service, is interoperability on the European level. The use of open standards, interfaces and technologies is a key factor for a sustainable system and facilitates upcoming interoperability efforts. Due to its openness and flexibility, the Austrian DDS is well prepared to face this challenge.

6 Conclusions and Outlook

In the past years, information technologies have increasingly made their way into traditional adminstrative procedures. Favored by the success of the Internet, eGovernment has improved many of these procedures in terms of efficiency and usability. In this paper we have introduced the Austrian way to overcome the various challenges of eGovernment. We have introduced the basic building blocks of the Austrian eGovernment infrastructure that are used to build up secure and reliable solutions for both, citizens and public administrations.

While this paper has primarly focused on Austrian approaches, similar attempts to enhance eGovernment have been made in other EU Member States as well. Since these solutions are most often specific to the particular Member State, they are usually able to satisfy the needs of the particular country only. Thus, interoperability between these systems is often an issue. To bear this challenge, several international research projects have been launched in order to support the ecosystem of key policy areas like eID, eHealth, eProcurement, and the Services Directive. Austria participates in several of these large scale pilots and contributes its experiences in design and implementation of secure and reliable eGovernment infrastructures to the development of cross-border solutions on an European level.

References

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

2. Bundesgesetz. Bundesgesetz über die Zustellung behördlicher Dokumente. http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10005522, April 1982.
3. Capgemini. *EU eGovernment-Studie 2006*. 2006.
4. Capgemini. *EU eGovernment Report 2007*. 2007.
5. Capgemini. *eGovernment Benchmark 2009*. 2009.
6. Martin Centner, Clemens Orthacker, and Wolfgang Bauer. Minimal-Footprint Middleware for the Creation of Qualified Signatures. In INSTICC Institute for Systems, Control Technologies of Information, and Portugal Communication, editors, *Proceedings of the 6th International Conference on Web Information Systems and Technologies*, pages 64 – 69. INSTICC - Institute for Systems and Technologies of Information, Control and Communication, Portugal, 2010.
7. Bundesgesetzblatt für die Republik Österreich BGBl. I Nr. 10/2004. *The Austrian E-Government Act*. 2004.
8. Herbert Leitold, Arno Hollosi, and Reinhard Posch. Security Architecture of the Austrian Citizen Card Concept. In *ACSAC '02: Proceedings of the 18th Annual Computer Security Applications Conference*, page 391, Washington, DC, USA, 2002. IEEE Computer Society.
9. Herbert Leitold, Reinhard Posch, and Thomas Rössler. Media-break resistant eSignatures in eGovernment: an Austrian experience. In Javier Lopez Dimitris Gritzalis, editor, *Emerging Challenges for Security, Privacy, and Trust - 24th IFIP SEC*, volume IFIP AICT 297 of *IFIP Advances in Information and Communication Technologies*, pages 109 – 118. Springer, 2009.
10. ARGE Spezifikation MOA. Spezifikation Module für Online Applikationen - ID. http://egovlabs.gv.at/projects/moa-idspss, Aug 2007.
11. Clemens Orthacker, Martin Centner, and Christian Kittl. Qualified Mobile Server Signature. In Hinchey M. Meyer B. et al. Turner, J.A., editor, *IFIP Advances in Information and Communication Technology Series*. Springer, 2010. in press.
12. European Parliament and the Council. Directive 1999/93/ec on a community framework for electronic signatures, Dec 1999.
13. The European Parliament and the Council of the European Union. *Directive 2006/123/EC of the Eurpean Parliament and of the Council on services in the internal market*. 2006.
14. Thomas Rössler. Empowerment through Electronic Mandates - Best Practice Austria. In S. Sharma G. Canals C. Godart, N. Gronau, editor, *Software Services for e-Business and e-Society : Proceedings of the 9th IFIP WG6.1 Conference*, volume 305 of *IFIP AICT*, pages 148 – 159. Springer, 2009.
15. OASIS Security Services (SAML) TC. Security Assertion Markup Language (SAML). http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security.