Requirements for Electronic Delivery Systems in eGovernment – an Austrian Experience

Arne Tauber

IAIK, Graz University of Technology
Arne.Tauber@iaik.tugraz.at

Abstract. Electronic mailing systems are the dominant communication systems in private and business matters. Public administrations deliver documents to citizens and businesses – subpoenas, legal verdicts, notifications, administrative penalties etc. However, official activities are more strongly linked to legal regulations than in civil law. Delivery of crucial and strictly personal documents raises the demand for qualified identification and non-repudiation services as featured by registered mail in the paper world. Legal requirements for electronic delivery carried-out by public administrations (eDelivery) cannot be fulfilled by standard certified mailing systems. Although the requirements for eDelivery systems may differ due to national legal regulations, this paper discusses common requirements and challenges on an abstract level. Moreover, we show how these requirements have been addressed by introducing the Austrian eDelivery system for eGovernment applications.

Keywords: eGovernment, Registered Mail, Certified Mail, Electronic Delivery

1 Introduction

Electronic mail (e-mail) has become the most popular communication method in our daily life – we are used to write and receive e-mails when communicating with friends, families, relatives or even in business matters when submitting contracts or invoices. This has been confirmed by a survey [1] reporting that about 90% of active internet users in Austria are using the internet for communication purposes.

Electronic communication is of great importance not only in the private and business sector. The delivery of documents such as notifications, administrative penalties, permits or laws, is a fundamental and resource-intensive task for governments and public administrations. For instance, the Austrian Treasury and Ministry of Justice deliver more than 44 million documents each year. The transition to electronic delivery systems (further denoted as eDelivery systems) is a key requirement towards service-oriented architectures in eGovernment. Electronic delivery has still to be considered as a value-added service and will not replace paper-based delivery at least for the next decades. Reduced costs associated with delays and saving paper, 7 x 24 availability and improved accessibility are the promises. Delivery is one of the last steps in public proceedings and raises the demand for an

electronic counterpart in order to avoid media-breaks for processes carried-out fully electronically.

Due to the high penetration rate e-mail seems to be the first choice when looking for communication media serving different kind of transactions – from citizens to administrations (C2A), administrations to citizens (A2C), businesses to administrations (B2A), administrations to businesses (A2B) as well as administrations to administrations (A2A). However, official activities are more strongly bound to legal regulations than in civil law and applied tools and technologies have to be almost legally regulated. Especially the justice sector requires a receiver to prove her identity in a qualified way when delivering crucial documents. A typical example is a subpoena, a written command to a person to testify before a court. A signed proof of receipt further guarantees that a receiver has picked-up the delivery at a certain point of time and thus are a valid evidence in public proceedings.

Several EU member states have already recognized the need for legal regulations concerning administrative deliveries. A number of domestic laws and regulations have been enacted in the last years providing the basis for qualified eDelivery systems. Austria has introduced its eDelivery system early in 2004. Looking at the national level of other EU member states there are similar initiatives such as DE-Mail [2] in Germany, Posta Elettronica Certificata (PEC) [3] in Italy or Secure Mailbox in Slovenia. From a local point of view, several Austrian ministries have launched a closed mailing system, e.g. the Austrian eDelivery system for legal relations (ERV) [4] provided by the Ministry of Justice or the eDelivery system for communications with tax authorities (FinanzOnline[1] - DataBox) provided by the Austrian Treasury.
Although the mentioned eDelivery systems are based on different national legal regulations and thus are implemented in different ways, this paper discusses common requirements on an abstract level. In the remainder of this paper we identify these requirements, discuss technologies backing qualified eDelivery systems and practical experiences gained in the Austrian case. In section 2 requirements and challenges to eDelivery systems are discussed. Although these requirements and challenges are specific to the public sector, some can be found in the private sector as well. In section 3 we discuss the common eDelivery architecture and addressing approaches from an abstract point of view. We continue in section 4 with discussing the Austrian electronic delivery system for eGovernment applications to show how requirements, challenges and security technologies have been implemented nationwide on the large scale. Synergies with the private sector to make eDelivery systems economic and initiatives towards cross-border delivery reducing barriers to EU member states are briefly discussed in section 5. Finally, conclusions are drawn.

2 Requirements and Challenges to eDelivery Systems

Registered mail is a fundamental vehicle in traditional means of carrying out public administration. In many cases subpoenas, legal verdicts, notifications, permits or administrative penalties are served by registered mail. In the private sector we are

[1] https://finanzonline.bmf.gv.at

used to serve submits for bidding processes, contracts, dismissals etc. by registered mail. Registered mail gives the sender the guarantee of having sent a delivery at a certain point of time. Depending on the case, public authorities may require a qualified proof of receipt to have legal evidence that a receiver picked-up a delivery at a certain point of time. This is determinant, e.g. for the commencement of the period for appeal. Deliveries may further be strictly personal meaning only the receiver herself can pick-up the delivery. Standard deliveries can usually be picked-up by families, relatives or neighbors as well. Qualified identification and a signed proof of delivery give evidence to public authorities on who has picked-up a delivery.

Based on the considerations made so far we can sketch the basic requirements for qualified eDelivery systems:

1. ***Qualified identification*:** qualified identification is a fundamental requirement for public administrations when delivering documents strictly personal. Usually receivers prove their identity by showing their passport, identity card, driver's license or another official ID. EDelivery systems must therefore guarantee that receiver registration is based on a reliable identification procedure. Most certified mail systems provide non-repudiation concerning a particular address or mail-box. This does not apply to eDelivery systems where qualified identification is a fundamental requirement.

2. ***Non-repudiation services***: legal provisions may force an eDelivery system to provide a delivery confirmation and/or a qualified proof of delivery. The former gives evidence to public authorities of having sent the delivery at a certain point of time. The latter gives evidence to public authorities that a receiver has picked-up the delivery at a certain point of time. EDelivery systems must thus provide non-repudiation services offering protection against false denial of involvement as described in RFC 2828 [5]. These services must include "non-repudiation with proof of origin" and "non-repudiation with proof of receipt" to provide an electronic delivery confirmation and/or a digital proof of receipt containing a timestamp and an electronic signature of the receiving unit (either the receiver herself or her service provider). Implementation guidelines concerning non-repudiation protocols are given in [6][7].

3. ***Trust***: citizens shall innately trust the eDelivery system they are using. Therefore, entities acting as trusted third party (TTP) must be approved by governmental controlling institutions.

Standard communication systems such as e-mail have their limitations and cannot provide qualified identification or qualified proofs of receipt. Even in most certified mailing systems there is a lack of qualified identification. In the remainder of this section we discuss further requirements that may be part of eDelivery systems depending on legal regulations. Several requirements can already be partially handled by standard or certified mailing systems:

4. ***Privacy, integrity, confidentiality and authenticity***: analogous to the privacy of correspondence in the paper world, eDelivery systems must ensure that the content of deliveries cannot be altered and can be solely disclosed to the receiver. It should be evident that the delivery origin is authentic backed by security technologies on the transport or application layer.

5. ***Delivery quality***: legal regulations may provide different quality levels concerning administrative deliveries. These levels could range from standard deliveries with no further requirements to qualified deliveries offering non-repudiation services. Delivery qualities may further define dedicated receiver groups, e.g. that a delivery can only be picked-up by the receiver herself or even by an authorized representative.

6. ***Representation***: an eDelivery system must support communications between citizens and administrations (C2A, A2C) as well as communications between businesses and administrations (B2A, A2B). It must be ensured in a technical or organizational way that deliveries to businesses can only be picked-up by authorized representatives, e.g. the registered manager of a company or other authorized business employees.

7. ***Look-up service***: if allowed by legal regulations, a look-up service could facilitate the search for a particular receiver. Such a service could be useful in heterogeneous or federated delivery systems featuring a broad range of delivery service providers.

8. ***Interoperability***: service architectures and protocols must be standardized to ensure interoperability between all entities of the eDelivery system. Open standards should be used for transparency, freedom of choice and to facilitate interoperability, also in terms of cross-border on the large scale.

9. ***Absence***: citizens may not be able to pick-up deliveries, e.g. when being on vacation or being hospitalized. EDelivery systems should therefore allow the absence of receivers concerning commencements of the period for appeal.

10. ***Accessibility***: eDelivery systems should be designed for ease of access by enabling participants to use commodity products such as e-mail clients or web browser. The installation of additional software on the client side should be minimized wherever applicable.

3 Architectural and Technical Considerations

In this section we discuss architectural and technical issues of eDelivery systems on an abstract level. We aim to identify the main entities of such a system and to address requirements for a qualified identification. From an abstract point of view qualified

eDelivery systems can be seen as a closed communication system providing different services for its participants. Technical, organizational and legal policies are usually defined by legal regulations on a local, regional or national level.

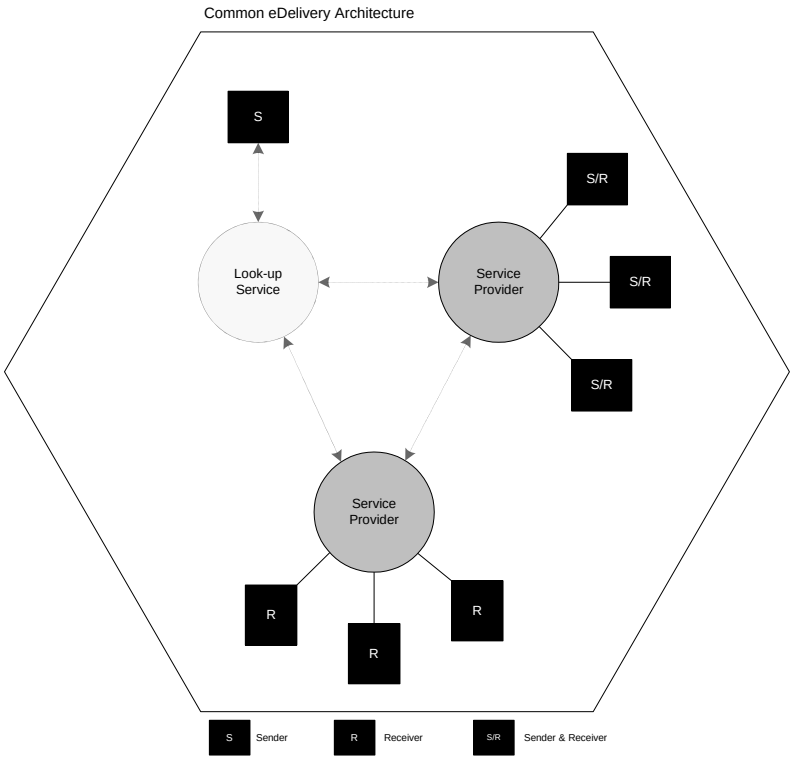

Fig. 1. Common architecture of an eDelivery system for eGovernment applications

The common architecture of eDelivery systems for eGovernment applications is illustrated in fig. 1. This architecture has been sketched on a very high abstraction level and identifies four types of entities: service providers, receivers, senders and an optional look-up service.

Similar to standard mail providers, *service providers* run communication services allowing the transmission of qualified deliveries. It is practically impossible to provide a qualified delivery system on the large scale without trusted third parties (TTP). TTPs must follow legal provisions and are usually approved by governmental controlling institutions. *Receivers* have to register with at least one service provider and can receive deliveries depending on their identification quality. This means that receivers should only be able to pick-up "strictly personal" deliveries if and only if they are registered based on an official ID. Standard deliveries could even be picked up using a pretended identity like in standard mailing systems. Following the EU Signature Directive [8], many EU member states have already introduced electronic

IDs (eID) based on qualified signature certificates. Such eIDs have the same legal impact as traditional official IDs in the context of public services. It is obvious that eDelivery systems for eGovernment applications are supposed to enable eIDs in order to be carried-out fully electronically. This applies to registration processes as well as the qualified identification of receivers when picking-up of deliveries.

Depending on legal provisions *senders* must not necessarily register with a service provider. However, authenticity of senders should be ensured in some way. Digital Signatures or SSL/TLS client authentication are e.g. technologies backing an adequate authentication on the transport layer. On the application layer electronic signatures could guarantee authenticity of senders. If a service provider supports the feature of sending deliveries, receivers could act as senders and vice versa.

There are a number of approaches ensuring a reliable addressing of receivers. Unique identifiers are a common way to address entities in communication systems. DE-Mail in Germany and PEC in Italy make use of identifiers based on the common e-mail address format, e.g. givenname.familyname@systemprovider.it. In this way citizens can provide their eDelivery address when applying for public services. Another approach is to use a unique national ID as a basis for reliable addressing a receiver. Austria introduced a so called delivery specific personal identification number – a derivation of a citizen's assigned unique identification number held in the base registers – the Central Residents Register (CRR) and the Supplementary Register for persons who do not have a registered address in Austria. For data protection reasons public authorities are not allowed to use the CRR number in public proceedings. The delivery specific PIN is therefore a derivation using strong cryptography by applying a Triple-DES encryption with a following one-way SHA-1 hash function. Austrian citizens are not necessarily obliged to provide identification information in order to be addressable. A central look-up service – the so called *delivery head* – holds all essential information of all receivers registered with approved service providers.

Secure and reliable communication in standard communication systems is typically based on end-to-end encryption. Due to the diversity of software products and cryptographic tools, complexity is rapidly increasing with the number of participants. This circumstance hinders the dissemination of secure systems as can be seen in the case of standard mailing systems. Several protocols for certified e-mail communications have been proposed so far [9][10] including TTPs[11][12]. EDelivery systems are usually designed in a way that receivers shall not get in touch with cryptographic functions such as signature creation, signature verification, non-repudiation services and end-to-end encryption. These operations are carried-out by service providers acting as TTP. Even if entity communication between senders and service providers or an intra-provider communication has to fulfill a number of requirements in terms of software and protocol security, the receiver should not be burdened with such complex processes. An eDelivery infrastructure should rather ease the access to the system allowing the use of commodity products such as e-mail clients or web browsers. This could be achieved by enhancing standard mailing system in order to meet the requirements discussed in section 2. For instance, Posta Elettronica Certificata (PEC) in Italy followed this approach.

The considerations made so far are on an abstract level and may quite differ by means of implementation issues for different member states. Questions arise when

addressing legal, technical and organizational barriers for a delivery of cross-border eDelivery services for public administrations. Section 5 gives a brief overview of an ongoing EU project addressing these issues.

4 The Austrian Delivery System for eGovernment Applications

In this section we discuss how the considerations made so far have been implemented on a national level by introducing the Austrian eDelivery system for eGovernment applications. Policies and general requirements are laid down by the Austrian eGovernment Act – enacted on 1st March 2004 – which provides the legal basis to facilitate electronic communications with public bodies. In the remainder of this section we discuss architectures, main process building blocks, open standards and security technologies backing the Austrian eDelivery system.

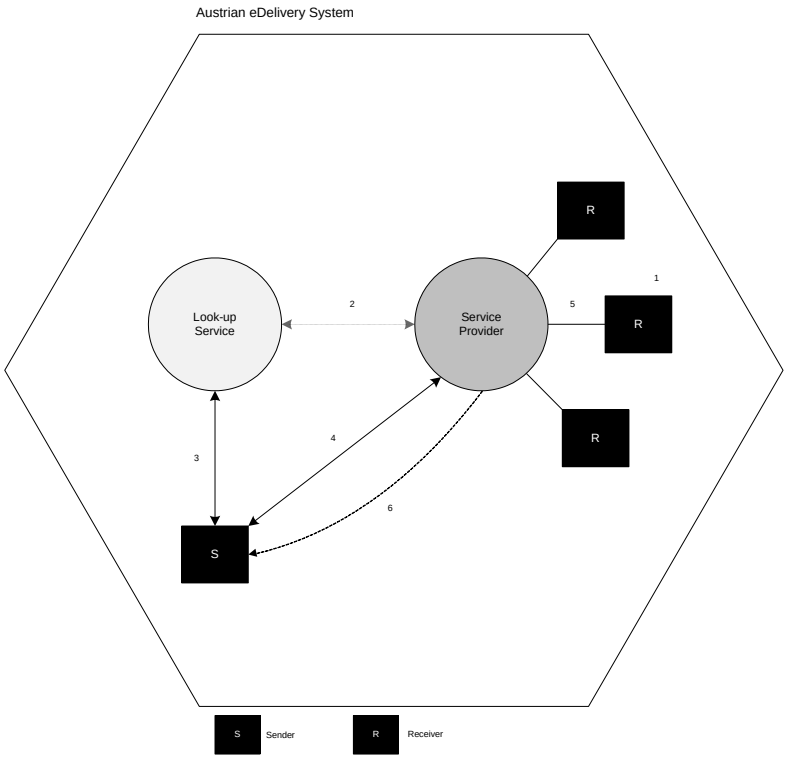

Fig. 2. Architecture of the Austrian eDelivery system

Fig. 2 shows the architecture of the Austrian eDelivery system for eGovernment applications. From an abstract point of view the main entities are as follows:

1. ***Service providers***: as long as legal, technical and organizational provisions are fulfilled, any public body or business can operate as service provider. A service provider can only be approved by the Federal Chancellor and must offer a number of basic services such as the receipt of administrative deliveries and several non-repudiation services.

2. ***Receivers***: all Austrian citizens and businesses can register with any service provider. Once the citizen or business is registered, all public administrations can address the receiver by electronic means. Electronic delivery is free of charge for receivers.

3. ***Senders***: all Austrian public bodies are allowed to deliver documents to registered receivers.

4. ***Look-up service***: the main look-up service (so called *delivery head*) can be seen as a register holding the data of all receivers. Service providers are therefore required to communicate all registered receivers to the look-up service.

(1) Registration with service providers can only be carried-out with the Austrian citizen card, the official electronic identification (eID) of citizens for online public services. Moreover, the citizen card offers the option of creating qualified electronic signatures. As stated by the EU Signature Directive, qualified signatures have the same legal impact as handwritten signatures. The security architecture of the Austrian citizen card is described in detail in [13]. Registration with service providers is explicitly voluntary as electronic delivery can be seen as an add-on service to traditional means of carrying-out delivery of printed documents. Registration of corporate bodies is based on so called electronic mandates. As citizen cards are only issued to physical persons, the Austrian eGovernment movement has developed an XML-scheme [14] for electronic mandates, the technical vehicle for acting on someone else's behalf. Electronic mandates are digitally signed XML structures and can be stored on a citizen's eID. For instance, a registered manager of a company can apply for an electronic postal mandate and accordingly act on behalf of the company when registering with a service provider. Postal mandates are available for representation of both corporate bodies and physical persons. (2) Service providers must communicate the receiver's registration data to the look-up service in order to be found by public authorities. Among personal data like delivery specific PIN, given name, family name, date of birth, e-mail address, a service provider has to communicate an optionally supplied X.509 encryption certificate for end-to-end encryption, the receiver's preferred document formats - e.g. PDF or MS-Office - and declared absence times. End-to-end encryption between senders and receivers is only applied if the receiver explicitly wishes this additional security layer by providing an X.509 encryption certificate in order to receive encrypted e-mails.

(3) In order to search for particular receivers, public authorities are forced to register with the central look-up service. The registration process is based on SSL/TLS X.509 client certificates having an appropriate attribute (Austrian eGovernment OID [15]) to assure that only public authorities can register with the look-up service. Using object identifiers to define appropriate attributes (OID) is a common practice in public key infrastructure (PKI). The supplied certificate must be used for searching receivers at the look-up service as well as for transmission of deliveries to a service provider. Public authorities are allowed to search for receivers using particular parameters such as given name, family name, date of birth and the e-mail address. Public authorities are not always aware of the citizen's e-mail address, e.g. in the case of traffic offence penalties. They are therefore recommended to use the encrypted unique delivery specific PIN for searching receivers that can be obtained by querying a frontend service of the Central Residents Register (CRR). For data protection reasons public authorities are never in the possession of the plain delivery specific PIN, it is rather protected using strong cryptography (RSA 1024bit) and can only be decrypted by the look-up service. Requests to the look-up service are sent using a HTTPs GET request based on SSL client authentication. Search parameters are passed as HTTP GET encoded parameters. Returned search results are based on an XML structure containing all service providers a receiver is registered with. For data protection reasons the look-up service must provide a limited result set only - the web service location of the service provider, preferred document formats and an optional encryption certificate, if the receiver has supplied one. In case of absence or a receiver has never registered with a service provider, a *not found* answer will be returned by the look-up service.

(4) If a receiver could be found, the public authority transmits the delivery to the web service location of the service provider returned by the look-up service. SSL client certificates with a public authority OID assure authenticity of senders on the transport layer. Public authorities are advised to electronically sign documents before delivery to assure authenticity on application layer. By 2011 all administrative processes bound to the General Administrative Process Law [16] are obliged to digitally sign official copies. The transmission of electronic deliveries is based on the Soap with Attachments (SwA) protocol supplying a MIME container. The SOAP part contains particular data to identify the receiver's delivery account such as the encrypted delivery specific PIN as well as additional metadata concerning unique reference numbers or delivery qualities. Attached binary documents are supplied within the MIME part of the SwA message. If a receiver has supplied a certificate for end-to-end encryption, a SMIME container is supplied respectively. The use of (S) MIME containers ensures the interoperability with standard e-mail clients. Service providers can either provide the MIME container in a well structured form through a web-interface or forward the container to the receiver's standard e-mail account.

(5) After having accepted a delivery, service providers must notify the receiver by electronic means, e.g. e-mail or SMS that a delivery is ready to be picked-up. If the delivery will not be picked-up within 48 hours, a second notification is sent-out. The receiver can pick-up the delivery logging in at the web interface of the service provider with her citizen card and sign a delivery confirmation with her qualified signature certificate. The delivery confirmation is as an XML document and must be signed following the XMLDSIG [17] standard. Receivers can optionally login using a

standard mail client based on SSL client authentication. In this case the delivery confirmation must be signed by the service provider. The Austrian eDelivery system distinguishes between two delivery qualities - qualified deliveries (RSa) and standard deliveries.

(6) RSa requires a service provider to return the signed confirmation back to the sending public authority either by e-mail or a SOAP based web service. If a receiver does not pick-up the delivery in time an appropriate non-delivery confirmation is returned as well.

So far not all Austrian citizens are registered for electronic delivery and printed documents are still dominating the world of delivery. In order to encourage public authorities to integrate their services into the eDelivery system, the Austrian eGovernment movement has developed the concept of *dual delivery*. This concept follows the *fire-and-forget* pattern allowing all kinds of deliveries to be carried-out over one single interface. If a receiver cannot be found querying the look-up service, the document will be printed out and delivered using conventional channels, e.g. by post.

5 Ongoing and Future Work

The low frequency of electronic deliveries a year raises the demand for synergies with the private sector to make systems deployed on the large scale economic. Registered mail is a fundamental vehicle in the private sector when delivery of crucial documents asks for a qualified proof of receipt. Legal provisions allow businesses to make use of the Austrian eDelivery system with limitations. By using national and international standards a specification meeting the requirements for shared use of both governmental and business processes has been published this year. A service following this specification has recently been put into practice by an approved service provider and other providers are encouraged to follow suit.

With the introduction of the EU Service Directive [18] cross-border eGovernment gets on the agenda of all EU member states. The ongoing EU Large Scale Pilot "STORK" [19] aims to achieve interoperability by bridging public services based on different legislations. Austria has the lead of Pilot 4, the so called eDelivery pilot[2] focused on coupling eDelivery systems of different Member states.

6 Conclusions

Registered mail is a fundamental vehicle in the paper world. With respect to electronic communications, standard mailing systems do not meet the requirements for an adequate qualified delivery. Several EU member states have already delivered eDelivery services based on domestic legal regulations. Even if at first sight these systems seem to quite differ from each other, common requirements such as qualified identification and non-repudiation services can be identified. Furthermore, this paper

[2] The author of this paper is involved in this pilot.

discusses common architectural characteristics of eDelivery systems on an abstract level by identifying the main entities and requirements. Considerations regarding reliable identification, authentication and confidentiality are made and discussed.

As an example the Austrian eDelivery system facilitating electronic communications with public bodies is discussed. This use case demonstrates how requirements stated so far have been implemented on basis of Austrian legal regulations. Open standards and security technologies backing the Austrian eDelivery system are discussed as well. Ongoing work regarding the demand for synergies with the private sector in order to make such a system deployed on the large scale economic is briefly noted. Finally, a short outlook to the EU large scale pilot STORK is given, addressing cross-border interoperability by coupling eDelivery domains of different member states.

References

1. STATISTIK Austria, ICT Usage in Households, 2008. (in German).
2. DE-Mail: Richtlinie für Bürgerportale, Version 0.98, 03.02.2009. (in German).
3. PEC: Regole tecniche del servizio di trasmissione di documenti informatici mediante posta elettronica certificata. (in Italian).
4. Ornetsmueller G., WEB-ERV – ERVService, Version 1.1, 15 March 2007.
5. Shirey R., RFC 2828, Internet Security Glossary, May 2000.
6. ISO/IEC 13888, Information technology - Security techniques - Non-repudiation.
7. ISO/IEC DIS 10181, Information technology - Open systems innterconnection - Security framework in open systems.
8. European Parliament and Council, Directive 1999/93/EC on a Community framework for electronic signatures.
9. Schneider B., Riordan J., A Certified E-Mail Protocol, Proceedings, of 14th Annual Computer Security Applications Conference, 1998.
10. Al-Hammadi, B.; Shahsavari, M, Certified exchange of electronic mail (CEEM), Southeastcon '99. Proceedings. IEEE.
11. Oppliger R., Stadlin P., A certified mail system (CMS) for the Internet, Computer Communications, vol. 27, 2004.
12. Puigserver, M.M.; Gomila, J.L.F.; Rotger, L.H., Certified e-mail protocol with verifiable third party, EEE '05. Proceedings.
13. Leitold. H, Hollosi A., Posch R., Security Architecture of the Austrian Citizen Card Concept, Proceedings of 18th Annual Computer Security Applications Conference, 2002.
14. Rössler T., Hollosi A., Elektronische Vollmachten Spezifikation 1.0.0, 2006. (in German).
15. Hollosi A., Leitold H., Rössler T., Object Identifier der öffentlichen Verwaltung, 2007. (in German).
16. General Administrative Process Law 1991 – AVG. BGBl. 1991/51 idF BGBl. 2004/10. (in German).
17. Eastlake D., Reagle J., Solo D., XML Signature Syntax and Processing, W3C Recommendation, 2002.
18. Directive 2006/123/EC of the European Parliament and of the Council, of 12 December 2006 on services in the internal market.
19. STORK: STORK – An overview, as seen on, 12 March 2009.