A Shared Certified Mail System for the Austrian Public and Private Sectors

Arne Tauber[1], Bernd Zwattendorfer[1], Thomas Zefferer[1]

[1] E-Government Innovation Center, Inffeldgasse 16/a,
8010 Graz, Austria
{Arne.Tauber, Bernd.Zwattendorfer, Thomas.Zefferer}@egiz.gv.at

Abstract. It is vital for public administrations and private businesses to send important documents such as bids or subpoenas in a secure and reliable way. Therefore, many countries have put various certified mail systems in place on the Internet. Due to the low number of official deliveries, it is reasonable to search for synergies with the private sector to guarantee the economic success of such widely-deployed systems. Opening a governmental system to the private sector inevitably raises challenges and security requirements in terms of qualified identification, data privacy protection, and trust. Privacy issues may arise when national (governmental) identification numbers are used. Trust issues may arise when trusted third parties are involved. Even if trusted third parties do not conspire with senders or recipients concerning a fair message exchange, they may cheat when financial interests come into play, e.g. in a per-message payment scheme. In this paper we present a solution addressing these issues from a practical viewpoint. Our solution distributes trust among different domains and introduces a scheme for qualified authentication and identification of recipients using the Austrian national electronic ID card to meet the requirements for data privacy protection.

Keywords: Certified E-Mail, Non-Repudiation, Semi-TTP, Trust Distribution, Domain Separation, Qualified Identification.

1 Introduction

Registered mail is a useful tool in administrative procedures and business processes. We are accustomed to send deeds, bids and other important documents in a secure and reliable way. In contrast to standard letters, registered mail guarantees the sender that a document has been delivered to the recipient at a certain point in time. Certified mail provides a further proof by having receipts signed by the recipient. Standard mailing systems such as e-mail are a frequent tool of choice for both official and business communications. However, they do not have the same evidential quality as registered mail has in the paper-based world. Pure e-mail without any additional measures can rather be compared to sending a postcard, which lacks integrity, confidentiality, and non-repudiation.

In the last two decades, the research community has provided a number of secure messaging mechanisms in order to fill these gaps. These mechanisms have been published as fair non-repudiation protocols (see e.g. survey of Kremer et al [1] and Onieva et al. [2]). We talk about certified electronic mailing (CEM) and refer to communication and mailing systems implementing these protocols as certified mail systems (CMS). There is no common view, which security properties a CMS has to fulfill and which services it has to provide. However, Ferrer-Gomilla et al [5] (pp. 2) consider that in related literature there is the agreement that certified electronic mailing should be the fair exchange of items. Official activities are more strongly bound to legal regulations than in civil law. Particularly in the justice sector administrative deliveries often require recipients to be unambiguously identified. Based on the results of the research community and on national legal regulations, various countries have already put domestic CMS in place on the Internet. Popular examples of governmental systems are the Italian Posta Elettronica Certificata (PEC) [6], the German De-Mail system [7] and the Austrian Electronic Document Delivery System (DDS) [8]. The Austrian Ministry of Justice has deployed a CMS for the justice sector called ERV (Elektronischer Rechtsverkehr). We can find a similar system in Germany with the eJustice system EGVP (Elektronisches Gerichts- und Verwaltungspostfach) and in the Netherlands with the JUBES (Justitie Berichten Service).

The Austrian governmental CMS (DDS) has a steadily increasing number of users. However, the low number of official deliveries per year has raised the demand for synergies with the private sector to guarantee the economic success of this widely-deployed system. A governmental system, which is going to be shared with the private sector, inevitably raises additional demands in terms of trust and privacy. This is particularly true for CMS using governmental national identification numbers to uniquely identify and address recipients. All CMS in place fully rely on the trustworthiness of trusted third parties (TTP). However, TTPs may cheat, even if approved and organizationally supervised by regulatory bodies. Trust concerns especially arise for TTPs operated by private businesses, because they usually do not enjoy the same public confidence as governmental institutions.

In this paper we discuss security issues of privacy and trust in a governmental CMS, which is going to be shared and used by both the public and private sectors. We show how a governmental addressing scheme based on national identification numbers may also be used in a privacy-preserving manner by the private sector. To achieve this, we make use of an additional trust domain, which is fully supervised by the government. This trust domain ensures privacy by hiding the national identification number from business entities. Moreover, we show how this model can be exploited to provide a technical supervision of TTPs concerning the reliable charging. We achieve this by means of cryptographic tokens serving as digital postmarks. Even if the presented approach is specific to the Austrian CMS, the model may be applied to similar systems as well. The remaining sections of the paper are organized as follows. Section 2 introduces the main CMS concepts and definitions we consider relevant for systems provided on the Internet. Additionally, we discuss the architecture and protocol of the Austrian governmental CMS. In Section 3 we discuss privacy issues and threats that arise when opening that system to the private sector. Based on these considerations, we identify the needed security requirements to tackle these issues. In Section 4 we present the security extensions we made to the governmental system in order to satisfy the requirements stated. Related work is discussed in Section 5. Finally, conclusions are drawn.

2 Background

Many CMS security properties are just considered from a theoretical viewpoint. In this section we give a brief overview of practical CMS security properties. Interestingly, in some aspects these properties differ from the security properties most frequently found in research literature. They rather match the properties of physical certified mail. Based on the terminology of CMS security properties, we introduce the architectural model and the protocol flows of the Austrian governmental CMS. This should serve as a basis to discuss our extensions for a CMS shared between public and private sectors.

2.1 CMS provided on the Internet

Numerous CEM protocols have been proposed in the last years. Most are designed for efficiency and are just considered from a theoretical point of view. There are few protocols that also take practical aspects of certified mail into account. Ferrer-Gomilla et al. [5] review in detail many CEM security properties that have been defined in the literature so far. We discuss in more detail the following three security properties we consider as relevant for CMS when actually being deployed on the Internet.

- ***Strong fairness***. This is a core property stating that either all entities (sender and recipient) receive the expected items (message, proof of receipt, etc.) or no one gets what is expected.

- ***Trusted Third Party***. Existing CMS have many similarities with postal systems in terms of infrastructure and security. This also applies to delivery agents acting as TTP. Many theoretical approaches try to increase efficiency and thereby decrease the needed amount of trust by reducing the involvement of TTPs. This often leads to so-called optimistic approaches, where TTPs are only involved in dispute resolution processes, e.g. when a recipient denies of having received a message. Oppliger [9] (pp. 6) states that such protocols are hard to deploy in practice and that the more pragmatic approaches are online TTPs, which are involved in all protocol executions, but not in all protocol steps. Thus they do not have to process the entire message. In fact, all systems and protocols provided on the Internet make use of inline TTPs. Inline TTPs act as intermediary (proxy) between senders and recipients and process the entire message. This inevitably leads to a higher need for computational and communicational resources and to a higher amount of required trust in these TTPs. However, especially in large-scale environments inline TTPs facilitate the fair exchange and enable the full control of message flows. Inline TTPs are usually implemented as delivery agents and similar to Internet e-mail providers, they often provide some sort of mail handling services (MHS) with mail transfer agents (MTA) for senders and mail delivery agents (MDA) for recipients.

- ***Non-repudiation services***. Evidences are essential for CMS. Evidences are usually signed data structures attesting particular events. Most systems provide at least a non-repudiation of delivery (NRD) evidence. This evidence is usually generated and signed by the MDA and attests that a message has arrived at the recipient's domain. In some systems, the stronger version, a non-repudiation of receipt (NRR) evidence, has to be electronically signed and to be provided by the recipient herself. In some systems, MTAs attest the acceptance of messages (by senders) with a signed non-repudiation of submission (NRS) evidence. Senders may ensure the authenticity of a message by providing a signed non-repudiation of origin (NRO) evidence. Usually evidences are transferable, i.e. they can be used by recipients or senders in dispute resolution processes without the need to involve a TTP.

2.2 The Austrian Governmental CMS

We sketch the architecture and the certified mail protocol of the Austrian governmental system according to the security properties discussed above, before we continue to discuss the privacy- and trust-based security requirements we have to meet when sharing it with the private sector.

In order to facilitate communications with public bodies, the Austrian eGovernment Act came into force in March 2004. Together with the "General Administrative Process Law" [3] and the "Law on the Delivery of Official Documents" [4] it regulates the policies and general requirements for serving official documents.

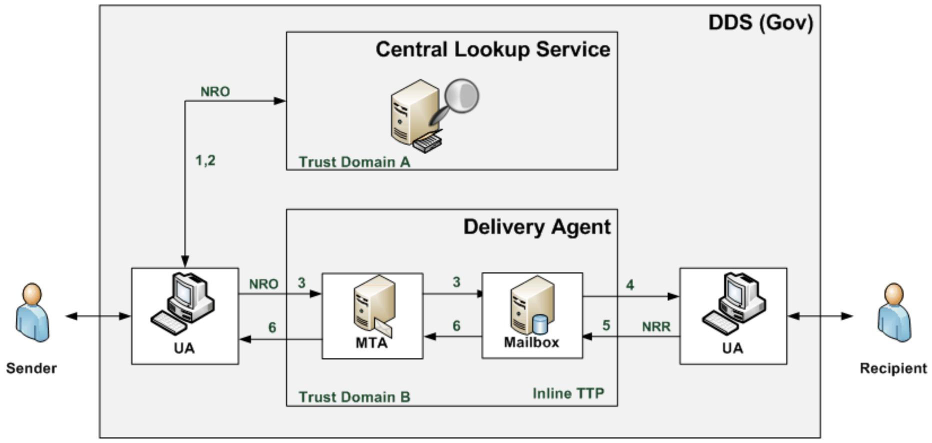

Fig 1. Architecture and protocol flows of the Austrian governmental CMS

In contrast to CMS such as the German De-Mail or the Italian PEC, the Austrian DDS is not purely based on the e-mail communication protocol. It is rather a hybrid system with a web-service based architecture conveying e-mail compatible MIME containers. This approach results from the fact that Austrian laws permit senders to address recipients in different ways. The e-mail protocol just allows the use of the standard e-mail address format. However, public authorities may want to address an Austrian citizen using an identifier based on the national ID as well, e.g. if the recipient's e-mail address is not available.

Fig 1 illustrates the architecture of the Austrian governmental DDS. This system has two separated trust domains. Imaginarily excluding trust domain A, this system would have many similarities with existing CMS using web servers acting as inline TTPs. Trust domain B consists of several so-called delivery agents acting as TTPs to ensure the fair exchange of messages between senders and recipients (strong fairness). All delivery agents are approved and organizationally supervised by the Federal Chancellery. Delivery agents provide MTAs for senders and MDAs (in terms of a mailbox) for recipients and can best be described with the CEM security properties of weak-stateless, verifiable, and inline TTPs providing well-defined non-repudiation services (see [5] for further details on CEM properties). Senders have to authenticate with delivery agents using TLS/SSL client authentication. This operation has to be logged in order to provide a non-repudiation of origin (NRO) service - a non-transferable evidence generated by the delivery agent.

Trust domain A is represented by the central lookup service (CLS) operated by the Federal Chancellery. The CLS can be seen as a directory holding the data of all registered recipients. It is a trusted source providing the list of delivery agents a recipient is registered with. In contrast to domain-name based addressing mechanisms such as e-mail, senders of the Austrian CMS do not know, with which delivery agent a recipient is actually registered with. A recipient may be registered with the same address (derived from the national ID) with multiple delivery agents. Apart from that unique ID to identify the recipient, no personal details are exposed to registered senders. Austrian laws require all senders to query the CLS before delivering messages to delivery agents. For the sake of efficiency, the CLS is designed as lightweight online TTP providing one non-transferable evidence only. Senders have to authenticate against the CLS using TLS/SSL client authentication exactly in the same manner as with delivery agents. The CLS provides a NRO service by logging each request for later potential dispute resolution processes. No other non-repudiation services are provided. It is therefore not a TTP in terms of providing transferable non-repudiation services, but rather being a trusted source of information. Although the CLS is actively involved in each delivery execution, the processing of entire messages is not required due to the property of an online TTP.

The protocol flow of the Austrian governmental CMS is as follows: **(1)** Senders query the CLS using search parameters such as demographics (name, date of birth, etc.) or the recipient's CMS sector-specific personal identification number (ssPIN). We call this value the recipient's unique identification number Id_R. The value is calculated by applying a SHA-1 hash function to the concatenation of the national ID number (sourcePIN[1]) and a two-character sector string code as follows:

$$Id_R = ssPIN\ (CMS) = \text{SHA-1}\ (\text{sourcePIN} \parallel \text{'ZU'}) \qquad \textbf{(1)}$$

where || denotes the concatenation operation and sourcePIN denotes a recipient's unique national identification number in e-Government procedures. Usually, this unique identifier is stored on the recipient's Austrian citizen card. More details on this approach, the concepts and the security architecture of the Austrian citizen card are described in detail in [11]. **(2)** The CLS returns a list of delivery agents the recipient is registered with. **(3)** The sender selects a delivery agent from the list and delivers the message to the MTA web service of the selected agent. This is done by using SSL client authentication. If desired by the recipient, confidentiality is ensured through end-to-end encryption (E2EE) using the S/MIME Cryptographic Message Syntax standard. Based on this authentication procedure, the delivery agent generates a non-transferable NRO evidence, which remains in trust domain B for later potential dispute resolution processes. The delivery agent stores the message into the recipient's mailbox and **(4)** sends a notification e-mail informing the recipient that a new message is ready to be retrieved. **(5)** The recipient logs in at the web site of the delivery agent using her citizen card, the Austrian national electronic identification (eID) card. The citizen card allows for creating qualified electronic signatures (QES) conforming to the EU Signature Directive [9] and thus being legally equivalent to handwritten signatures. By creating a QES, the recipient generates an NRR evidence, which **(6)** is countersigned by the delivery agent using an advanced electronic signature (AdES) conforming to the Signature Directive. The NRR evidence is then returned to the sender (either through a sender's web service or via regular e-mail).

Having introduced the security architecture of the Austrian governmental CMS, in the next section we discuss arising challenges and requirements when opening this governmental system to the private sector. A shared public-private system not only asks for high security provisions and data privacy protection, but is faced with stringent requirements of underlying legal regulations as well.

3 Security Requirements

The public sector usually enjoys more public confidence than the private sector. When opening a governmental system to the private sector, several challenges and requirements regarding privacy must be taken into account. Additionally, mandatory redesigns may also pose new security threats. In the Austrian case, we identified privacy issues concerning the use of national identifiers as well as the threat of potential cheating parties when business entities come into play. These issues are discussed in the following subsections.

[1] Source Personal Identification Number

3.1 Privacy

In Austria, only public administrations are allowed to use the national identification number (or a derivation of it). In case of the Austrian governmental CMS, this also affects the recipient's unique identification number Id_R. It would seem reasonable to introduce a new fictional identifier scheme for business entities or to redesign the protocol so that Id_R is not used in case of business entities. Even if business entities are not allowed to use one of the identifiers above and thus are not able to query the CLS using Id_R, there are still two strong arguments for using a national ID number based scheme also for the private sector.

First, Austria and many other countries such as Italy, Spain, Finland, Belgium, or Estonia store the citizen's unique identifier on the national eID card. Usually, such cards have the same legal value as traditional ID documents, by virtue of using qualified electronic signatures having legal equivalence to handwritten ones. The national ID number on the eID allows the identification of citizens even if eID tokens and certificates have expired or get replaced. Binding the eID to a citizen's mailbox thus ensures a qualified identification and authentication even if for instance the eID token has changed. Some administrative and judicial procedures require such a degree of reliable authentication to ensure that a delivery is handed over to just the intended recipient and no other affiliated person. Besides subpoenas, a typical example is the delivery of official documents in divorce proceedings where both partners are still living in the same household. However, qualified identification may be of keen interest for the private sector as well. As an example scenario, postal operators offer value-added services, where a postman identifies the recipient by checking her personal ID. In this way, customers can e.g. enter into a subscription-based contract for a mobile phone, without having ever been in a mobile shop. Delivery agents may offer such high value-added services to private customers if and only if recipients can be identified and authenticated in a qualified way.

A second argument for the use of a national ID number based scheme is the linkage between a recipient's different mailboxes. We stated that a recipient may be registered with multiple delivery agents. If a sender searches for a particular recipient, the CLS must thus know all delivery agents a recipient is registered with and return them in the search answer. The governmental system requires all mailbox accounts to be linked with the recipient's Id_R. If a recipient has accounts with multiple delivery agents, all accounts can easily be linked together. In case of a private business delivery agent, the use of Id_R is not allowed. In a public-private system, however, it is essential that all mailbox accounts are linked to the same person so that the CLS can return to senders a complete list of delivery agents a recipient is registered with. This is only feasible if mailbox accounts of private business delivery agents are also bound to the recipient's national ID number.

Based on these considerations, we have identified two major privacy-related security requirements in case of a private business involvement. First, in any case the recipient's sourcePIN must not leave the recipient's domain. This is regulated by law, which only allows the use of the sourcePIN in the recipient's and the public sector domain. Second, in case of a unique business ID (based on the sourcePIN), this ID must not be exposed to any involved party other than the recipient and her delivery agent. This prevents the tracking of recipients' activities.

3.2 Threats

There is a heightened risk of cheating parties when financial aspects come into play and profit-oriented businesses are involved. The use of the Austrian CMS is free of charge for recipients, but senders have to pay delivery agents for each delivered message. Therefore, we can identify two potential cheating parties: senders and delivery agents acting as TTPs. Cheating senders may claim to have not sent a message so as to refuse payment. This issue can usually be addressed by a NRS service. In systems with inline TTPs, such a measure fully relies on the trustworthiness of TTPs. However, TTPs may not be completely trustworthy. TTPs may be fully trusted with respect to a fair message exchange and not conspire with other parties by e.g. retaining messages. Nevertheless, a cheating TTP may generate fictive and forged messages, which may appear to originate from a specific sender. By creating associated NRS evidences, a TTP could claim the provision of rendered services and demand payment from senders. In CMS where senders have to create transferable NRO evidences, e.g. a digital signature attesting data-origin authentication, a TTP may not make such a claim. For usability reasons, in practice many CMS make use of standard authentication mechanisms for senders, e.g. username/password based on TLS/SSL (client) authentication without the need for senders to digitally sign messages. In this case a sender does not have a transferable NRO evidence and a dispute resolution process is hard to carry out. This also applies to the Austrian system. For our proposed security architecture, we introduce the notion of a semi-trusted third party (semi-TTP) for the reliable charging of rendered message services. Even if in most governmental systems (Italy, Germany, Austria, etc.) TTPs are accredited and organizationally supervised by regulatory authorities, no one may hinder them from changing software or hardware components afterwards. Therefore, it is vital and a major security requirement to technically supervise semi-TTPs.

4 Security Architecture

Based on the considerations made so far, we present the security extensions of the Austrian approach of a shared system for the public and the private sector. The most significant feature of this system is the enhancement of trust for senders in semi-TTPs using a domain separation model. The legal regulations for a shared delivery system are laid down by the law on “The Delivery of Official Documents” that allows the private sector to take part in the Austrian governmental DDS with several limitations. Due to Austrian data protection legislations, registered recipients are free to decide whether they want to accept private deliveries or official deliveries only. If they are willing to accept deliveries from private businesses, they must give their explicit consent. Moreover, recipients must be addressable and identified in a qualified way. For this purpose, we introduce a sector-specific personal identifier (ssPIN) for the private sector that we discuss in subsection 4.1. In subsection 4.2 we present our approach that allows the transmission of this PIN from the CLS to senders and then to delivery agents in a way that senders never come in touch with the PIN. At the same time, an additional trust layer ensures the technical supervision of delivery agents by providing a non-repudiation service for both senders and delivery agents.

4.1 Qualified Identification

In Section 3 we discussed the requirement of unique identifiers corresponding to the eID for the private sector to ensure that recipients can be identified in a qualified way, i.e. having an electronic equivalent to other official IDs. The governmental system requires that a unique identifier of a recipient must be assigned with a delivery agent using the citizen card upon registration. In the governmental context, a recipient has a unique ID Id_R across all delivery agents. Even if a recipient is registered with more delivery agents, the lookup service has to include just this value in a search result.

Only the public sector is allowed to access Id_R. In a shared public-private system, data privacy legislations prohibit delivery agents to make use of Id_R in case of business senders. If a delivery agent does not support administrative deliveries, thus acting as pure private service provider, it is not allowed to access the sourcePIN stored on the recipient's eID and to further derive an Id_R. The Austrian eGovernment Act has met this concern by defining unique identifiers for the private sector (further denoted as private ssPIN). By law, such identifiers must be calculated in the recipient's domain in a way that private businesses – in our case delivery agents acting purely private - will never come in touch with and will never be able to access the sourcePIN.

Delivery agents must communicate their own business identifier, i.e. the commercial register number, to the recipient's domain in order to obtain the private ssPIN. The calculation is carried out by the recipient's citizen card environment, a publicly available software to communicate with and access the functionality of the Austrian citizen card (see [11]). A recipient's private ssPIN (Id_{RB}) is calculated as follows.

$$Id_{RB} = ssPIN_{private}\ (CMS) = \text{SHA-1 (sourcePIN || BUSINESS\_ID)} \qquad \textbf{(2)}$$

Id_{RB} is derived by applying a one-way SHA-1 hash function to the concatenation of the sourcePIN and the business ID of the delivery agent. This hash function makes it impossible to determine the sourcePIN on the basis of the resulting private ssPIN. In contrast to the public ssPIN, a recipient's private ssPIN is different for each delivery agent due to different business IDs.

4.2 Trust Domain Separated Security Model

Based on the considerations made in Section 3, we are faced with two basic security requirements. The first is a non-repudiation service assuring that delivery agents may not cheat and generate fictive NRD evidences to demand payment from senders. The second requirement concerns the privacy of unique identifiers in the context of business senders, i.e. Id_{RB} we introduced in Section 4.1. Senders must use this ID to uniquely identify recipients when delivering messages to delivery agents, but they are never allowed to come in direct touch with it.

Our approach exploits the existing security architecture by extending the CLS from a trusted information source to a more feature-rich and lightweight online TTP providing non-repudiation services for both senders and delivery agents. Trust Domain A is operated by the Federal Chancellery and thus already provides the basis for a technical supervision of Trust Domain B. Although efficiency was a major concern of our approach from the beginning, additional security measures should not be a bottleneck when thousands or even millions of messages are being delivered within a short time frame. In order to minimize complexity and not to downgrade efficiency too much, we decided to introduce one additional non-repudiation service only. In order to address all issues considered so far, we developed a lightweight version we call Compact Digital Postmark (CDPM).

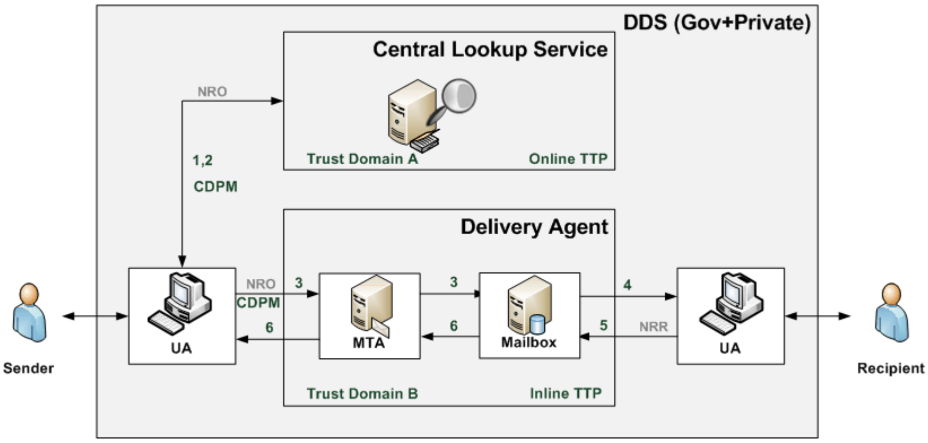

Fig 2. Trust domain separated security architecture of the Austrian public-private CMS.

Fig 2 illustrates the extended security architecture of the shared system for the public and private sectors using trust domain separation and the non-repudiation service CDPM.

CDPMs can only be generated by Trust Domain A in a reliable way so that neither senders nor delivery agents are able to reproduce them. The CDPM is calculated as follows

$$\mathrm{CDPM}_{(enc)} := \mathrm{RSA}_{pub}\ (\ \mathrm{Id}_S \parallel \mathrm{BT} \parallel \mathrm{TS} \parallel \mathrm{Id}_{RB}) \qquad \textbf{(3)}$$

The CDPM conveys a concatenation of the sender's identity Id_S, a billing token (BT), a time-stamp (TS) and the recipient's unique business ID Id_{RB}. Each approved delivery agent being part of the system is equipped with a custom RSA private key in an out-of-band process. The CDPM is encrypted using the corresponding RSA public key (RSA_{pub}). We have shown in Section 4.1 that in contrast to the governmental Id_R, the value of Id_{RB} differs for each delivery agent. Therefore, if a sender's search request results in a recipient registered with multiple delivery agents, the lookup service has to generate the equal number of CDPMs. This non-repudiation service thus prevents both senders and delivery agents from denying of being related to a particular CDPM. Due to the strong encryption, the recipient's Id_{RB} and the billing token remain hidden from senders. CDPMs are not message-bound and may be used for the delivery of any message. Such a binding is not necessary for the purpose of billing. It would rather downgrade efficiency due to the entire processing of messages. When delivering a message to a delivery agent, a sender is required to convey the CDPM along with the message. A delivery agent has to decrypt the CDPM and extract all values contained. The Id_{RB} is the link to the recipient's mailbox account bound to this value. The billing token is a nonce intended for delivery agents and must be used to validate genuineness when demanding payment from senders. A sender may decide to not deliver a message after querying the lookup service. Therefore, the CLS uses a secure random algorithm so that generated billing tokens are not guessable and reproducible by cheating delivery agents. Domain policies define that a CDPM has an expiration date of two days. The CDPM time-stamp must conform to the ISO-8601§5 extended format ("YYYY-MM-ddThh:mm:ss").

Delivery agents must validate each CDPM against the lookup service before demanding payment from senders. This operation must not immediately be carried out online upon message receipt. An online verification would be a potential bottleneck and could result in latencies or message queues and lead to rejection of messages. This may be the case when large-scale enterprises like insurance companies are delivering messages in bulk. However, billing tokens are unique and delivery agents can thus detect if a dishonest sender is trying to reuse such a token in a replay attack. Validation of CDPMs can hence be carried out offline at a later point in time. In the course of this, a delivery agent has to communicate the decrypted CDPM to the lookup service, which checks if a billing token is genuine and not reused and if the billing token has been issued to the indicated sender and is belonging to the requesting delivery agent.

4.3 Security Considerations

In this section, we check the fulfillment of the security requirements we stated in Section 3. Assuming that the CLS in trust domain A is a fully-trusted third party, we classify our discussion into four cases: (1) the exposure of Id_{RB} to unauthorized parties; (2) cheating sender and honest TTP; (3) honest sender and cheating TTP; (4) cheating sender and cheating TTP.

Case 1. *The exposure of* Id_{RB} *to unauthorized parties*. Only the concerned recipient, the related TTP and the CLS are allowed to be in the possession of Id_{RB}. Senders and other TTPs must not see this value at any stage of the protocol flow. During a recipient's registration or authentication process, Id_{RB} remains in the recipient's and the related TTP's domain. Upon registration, this value is transmitted only to the CLS. The CLS is thus responsible for not revealing Id_{RB} to unauthorized parties. By encrypting this value with the related TTP's public key RSA_{pub}, resulting in *CDPM* = RSA_{pub} (Id_S || Id_{RB} || BT || TS), only the related TTP but no sender and no other TTP is able to see the value of Id_{RB}.

Case 2. *Cheating sender and honest TTP*. To refuse payment, a cheating sender may deny to have sent a message provided with a particular CDPM. The CLS binds each CDPM to the sender's identity Id_S. This dispute can be resolved by the CLS. A sender, however, may claim that the CDPM was lost and used by some other sender. This case is covered by honest TTPs checking the authenticating sender's identity Id_S (SSL authentication) against the Id_S value contained in CDPM before accepting a message. If the values do not match, the message must be rejected.

A cheating sender may also try to reuse CDPMs to pay only once. However, TTPs are required to check whether BT is used twice in order to prevent replay attacks. If so, the message must be rejected.

Case 3. *Honest sender and cheating TTP*. To demand payment from senders, a TTP must send BT to the CLS acting as clearing center. BTs are not guessable. They can also be used only once. After being validated by the CLS, BT is devaluated.

Case 4. *Cheating sender and cheating TTP*. This is the case where a sender uses a (stolen) CDPM of another sender. A cheating TTP may skip the sender's identity (Id_S) check and validate the stolen BT to demand payment from the cheated sender. This issue is somewhat mitigated by the timestamp TS, which makes BTs only valid for a short period of time. However, case 4 is currently not completely covered by our architecture. This could e.g. be solved by including an encrypted version of Id_S within CDPM, which can only be decrypted by the CLS. A TTP would have to provide this sender identity token to validate BT. However, we assume this cheating case is unlikely to happen.

4.4 Implementation

Efficiency was a major concern of our approach and hence a huge amount of messages sent during a short time frame should not force our solution to its knees. In order to achieve this, our approach uses a non-repudiation service based on just one encryption operation. The deployed solution currently uses the RSA algorithm for encryption and decryption of CDPMs. Before going into productive operation, a Java-based prototype with the functionality of trust domain A was implemented to evaluate the performance under real conditions. For security reasons and to accelerate the computation of CDPMs, we employed a SafeNet LunaPCI 3000 hardware security module (HSM) as cryptographic unit. We achieved a throughput of nearly 250.000 CDPMs / hour with a single off-the-shelf server and one application server. The gained results were more than sufficient for going into productive operation. Our concept has been taken up by the market and was implemented in both trust domains. Software solutions for delivery agents exist from several vendors. Currently, three delivery agents are part of the system and provide the service: two private sector implementations[2] and the Federal Computing Centre[3].

[2] http://www.meinbrief.at, http://zustellung.telekom.at

[3] http://www.brz-zustelldienst.at

5 Related Work

Our approach has analogies to the paper-based world, where postage stamps and postmarks ensure trust and a reliable postage charge handling. Similar technologies and concepts can also be found in the electronic world where Electronic Postal Certification Marks (EPCM) ensure non-repudiation and certainty of date and time for arbitrary documents. Several international postal operators – Italy, Portugal, France, Canada and the United States – already provide a common framework of EPCM services [12]. EPCMs are a meaningful trust vehicle in open systems. They ensure non-repudiation of submissions by applying digital signatures and providing time-stamp services. EPCMs are not suitable for online TTPs as they are based on digital signatures and thus require the entire processing of messages. Our encrypted "postage mark" CDPM is used within a closed system and in conjunction with an online TTP, i.e. we do not bind the token to a particular message. In contrast to our approach, EPCMs operate on the basis of a prepaid model, i.e. you have to pay for the non-repudiation of submission services even if you don't deliver the message to the recipient.

We introduced a security architecture based on two separated trust domains, which provides a realistic trust model for senders and integrates well in the existing infrastructure. The term "semi-TTP" has first been introduced by Franklin and Reiter [13]. However, this notion was referring to TTPs ensuring the fair exchange of messages. The idea of distributing trust to prevent cheating has been tackled by various researchers. There have been proposed schemes for distributing trust among a group of TTPs using cryptographic threshold schemes (see [14] and [15]), so that a single TTP is not able to compromise the security of the entire system. However, these approaches highly increase complexity, downgrade efficiency and are hard to deploy. For the fair message exchange problem, more pragmatic approaches have been proposed to distribute trust among different types of TTPs. Most of the proposed approaches are optimistic (i.e. offline) protocols. A first approach is described by Micali [16] in a U.S. Patent (already flawed [17]). Ateniese extended this approach in his TRICERT system, which uses a fully-trusted offline TTP and several less-trusted inline TTPs [18]. We transferred that idea from the fair message exchange problem to meet our requirements, resulting in an online based approach ensuring privacy and a technical supervision of (semi-)TTPs. From a practical viewpoint, the CLS acting as fully-trusted online TTP has the benefit that senders are not burdened with cryptographic operations and that future (security) protocol changes are easier to deploy.

6 Conclusions

In this paper we discussed the solution of an extended security architecture that became necessary when opening the Austrian governmental CMS to the private sector. Even if TTPs may be considered as fully-trusted in the context of a fair message exchange between senders and recipients, they may only be semi-trusted in other aspects, e.g. when financial interests come into play. If all non-repudiation services are generated by inline TTPs, these entities may cheat and generate fictive non-repudiation services in order to demand payment from senders. We presented a practical approach to technically supervise (semi-) TTPs, i.e. delivery agents, by distributing trust using domain separation. The existing security architecture was extended to a fully-trusted lightweight online TTP providing a non-repudiation service for both senders and semi-TTPs.

We realized this non-repudiation service by implementing an efficient CDPM, which is bound to the sender and to a delivery agent. In addition to a billing token, the CDPM conveys the recipient's business ID, so that senders can uniquely identify the recipient when delivering messages. Besides providing non-repudiation services, the CDPM fulfills the requirement of data privacy, so that senders do not come in touch with this unique ID derived from the national ID. The concept has been taken up by the market and has been implemented by both the CLS and all delivery agents.

References

1. Kremer, S., Markowitch, O., Zhou, J., An intensive survey of fair non-repudiation protocols, Computer Communications, Elsevier, vol. 25, no. 17, 2002, pp. 1606—1621
2. Onieva, J., Zhou, J., Lopez, J, Multiparty Nonrepudiation: A survey, ACM Computing Surveys 2008, vol. 41 no. 1.
3. Gesamte Rechtsvorschrift für Allgemeines Verwaltungsverfahrensgesetz 1991, Fassung vom 23.05.2011, http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10005768, last visited on 23.05.2011.
4. Gesamte Rechtsvorschrift für Zustellgesetz, Fassumg vom 23.05.2011, http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10005522, last visited on 23.05.2011.
5. Ferrer-Gomilla, J., Onieva J., Payeras, M., Lopez, J., Certified electronic mail: Properties revisited, In: Computers & Security (2009), Elsevier.
6. Gennai, F., Martusciello, L., Buzzi, M., A certified email system for the public administration in Italy, In: IADIS International Conference WWW/Internet, 2005, vol. 2, pp. 143—147
7. Dietrich, J., Keller-Herder, J., De-Mail — verschlüsselt, authentisch, nachweisbar, Datenschutz und Datensicherheit – DuD 2010, vol. 34, no. 5, pp. 299-301
8. Tauber A., Requirements for Electronic Delivery Systems in eGovernment – An Austrian Experience, IFIP I3E 2009, vol. 305, pp. 123-33
9. Oppliger, R., Providing Certified Mail Services on the Internet, In: IEEE Security and Privacy, vol. 5, no. 1, pp. 16-22
10. European Parliament and Council, Directive 1999/93/EC on a Community framework for electronic signatures.
11. Leitold, H., Hollosi, A., Posch, R., Security Architecture of the Austrian Citizen Card Concept, Proceedings of 18th Annual Computer Security Applications Conference, 2002.
12. Miranda J.P., Melo J., EPM: Tech, Biz and Postal Services Meeting Point, ISSE 2004 - Securing Electronic Business Processes: 259-267, 2004
13. Franklin, M., Reiter, M., Fair exchange with a semi-trusted Third Party, In: Proceedings of 4th ACM conference on Computer and Communications Security, 1997, pp. 1-6
14. Kothari, S.C., Generalized linear threshold scheme, In: Proceedings of Crypto'84, pp. 231-241.

15. Shamir, A., How to share a secret, Communications of the ACM, vol. 22, no. 11, pp. 612-613.
16. Micali, S., Simultaneous electronic transactions, US Patent 5666420, 1997.
17. Fao, B., Wang, G., Zhou, J., Zhu, H., Analysis and Improvement of Micali's Fair Contract Signing Protocol, Information Security and Privacy, ACISP'04, 2004, pp. 176-187,
18. Ateniese, G., Medeiros, B., Goodrich, M., TRICERT: A Distributed Certified E-Mail Scheme, In: Proceedings of the Network and Distributed System Security Symposium, NDSS 2001, San Diego, California, USA 2001.