2015 IEEE/ACM 1st International Workshop on TEchnical and LEgal aspects of data pRivacy and SEcurity

Introducing New Technology into Italian Certified Electronic Mail: A Proposal

Marina Buzzi, Luca Ferrucci, Francesco Gennai, Claudio Petrucci

{IIT,ISTI}-CNR - Area della Ricerca di Pisa - Italy
Email: {gennai,ferrucci}@isti.cnr.it, marina.buzzi@iit.cnr.it

Agid - Agenzia per l'Italia Digitale - Roma - Italy
Email: petrucci@agid.gov.it

***Abstract*—Over the last decade, an increasing number of Certified E-Mail systems (CEM) have been implemented in Europe and worldwide, but their diffusion and validity are mainly restricted in a national arena. Despite the effort of European Union (EU) that recently defined a specification for guaranteeing interoperability of CEM systems between Member States, its adoption has not be not yet fuelled, mainly since any CEM system receives a legal value by its State legislation. It is difficult to extend the legal value of CEM security mechanisms, e.g. receipts with timestamps which are considered evidences and legal proofs in disputes that may arise from different Parties inside a State, unless a common political and legal agreement will be created. At this aim, recently EU introduce the new Regulation on Electronic Identification and Trust Services (eIDAS) , to address this issue. We believe that the first step for encouraging a more large adoption between communities is to implement CEMs using standard worldwide recognized solutions.**

In this paper we propose a technical evolution of the Italian CEM, called Posta Elettronica Certificata (PEC) moving from a close mechanisms to the adoption of a more standardized, distributed solution, based on DNS Security Extensions (DNSSec). This proposal would have a minimal impact on the legislation, restricted to the annex that defines PEC technical rules.

I. Introduction

One of the main objectives of EU is to accelerate the adoption of the eEurope plans, filling the gap between different degrees of ICT penetration in the Member States.

The Digital Agenda is a priority of the Italian government, with the goal of improving service, while reducing costs. Established by the Development Decree of June 22, 2012 [1], the Agency for Digital Italy (AGID) has the task of implementing the objectives defined by the Italian government, acting as a supervisor and coordinating the development of ICT in the public administration and promoting goals and challenges conforming to the **Digital Agenda for Europe** (DAE). DAE was presented by the European Commission (EC) in 2010 with the aim of exploiting the potential of ICT to promote innovation, economic growth and competitiveness. The main goal of the Agenda is to promote solid socio-economic benefits thanks to a single digital market based on high-speed Internet and interoperable applications. DAE is one of the seven main initiatives identified in the **EU 2020 Strategy**, for promoting a smart and sustainable UE. The spread of digital technologies would favour employment and simplify administrative procedures, thus offering citizens a better quality of life, with more efficient health services, simpler access to public services and cultural resources. DAE also identifies the main problems that may undermine the diffusion of ICT and indicates an European common strategy to overcome these obstacles by identifying actions required of Member States for bridging the Digital Divide and providing accessible services for any EU citizen. Each member state has to absorb the European guidelines, implementing its own strategy for reaching the goals of the DAE, defining priorities and strategy based on national context and resources.

The Agency is the organization responsible for coordinate and monitoring the progress and quality of this process in Italy. The Italian PEC is a system that provides legal evidence attesting the sending and delivery of electronic documents to the sender, with associated timestamps. It offers a complete, usable and reliable solution for the secure transmission of documents. The Italian Government assigned to AGID as the organization of reference for PEC. Broadly speaking, the institutional activities of AGID include receiving and assessing applications for subject candidates to play the role of PEC provider (as defined in the circular CNIPA CR/49 of November 24, 2005 [2]) supervising the activity of the PEC provider (maintenance of requirements, service levels, usage statistics) and supervising the interoperability test (according to the circular CNIPA CR/51 of December 7, 2006 [3]).

In this paper we describe a possible technical evolution of the PEC system, also discussing its impact on the current legislation that regulates the PEC services and control its quality and interoperability. The paper is organized as follows: section II describes the actual functional schema of the Italian PEC, after a brief introduction on the main properties a CEM should satisfy. Section III introduces other european CEMs, analysing what properties they actually satisfy and the level of interoperability. Then, section IV gives an overview of the above mentioned proposal of Italian PEC and section V draws conclusive remarks and focus on future developments.

II. Italian Certified Electronic Mail

In this section we illustrate the architecture of the Italian PEC [4]. In [5] are described a set of properties that CEM

978-1-4673-7097-4/15 $31.00 © 2015 IEEE
DOI 10.1109/TELERISE.2015.14

systems should satisfy. A protocol provides **Non-repudiation of origin** (NRO) if it gives evidence against the false denial of having originated the message and **Non-repudiation of receipt** (NRR) if it gives evidence against the false denial of having received the message. Moreover it provides **Non-repudiation of submission** (NRS) and **Non-repudiation of delivery** (NRD) if it gives evidence against the false denial of having submitted or delivered the message, respectively. In a CEM protocol, Trusted Third Parties (TTPs) may be involved in addition to sender and receiver. In the case it is involved actively in each protocol step it is called **inline TTP**; this type of TTP usually has to process the entire message as a proxy. Instead, if it is only involved in a dispute resolution process, it is called **offline TTP**.

Figure 1 shows the functional schema of the PEC system.

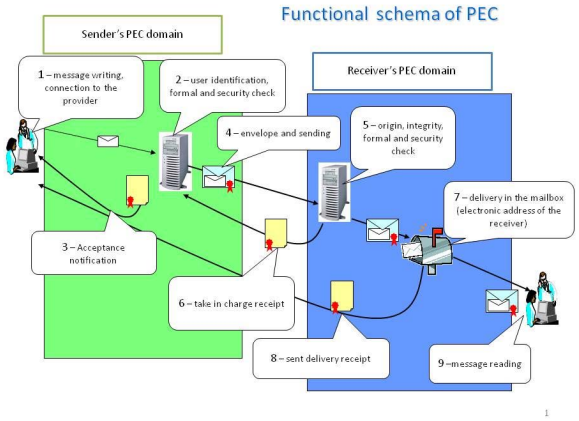

Fig. 1. Functional schema of PEC

The system is layered on top of the e-mail architecture based on the SMTP protocol to ensure compatibility with standard e-mail client and to guarantee interoperability with traditional e-mail systems. Delivery agents, called **PEC providers**, act as an inline TTP between senders and recipients. They have to be accredited by AGID for compliance with given technical and legal requirements, as requested in [6]. Both senders and recipients must register a mailbox with a PEC provider. The PEC technical rules do not make any assumptions about the communication protocol between end user and his PEC provider. They only define the minimum security requirements for authentication and confidentiality, e.g., with username/password combined with a TLS connection. PEC providers must sign all messages and evidences according to the S/MIME v3 standard [7], with an x.509 v3 certificate [8].

The usage of end-to-end cryptography, e.g. using a national eID document to uniquely identify users, has several advantages as NRO and sender's authentication, but implies an extensive penetration of technology in society, requiring a high degree of user technical knowledge. To mask a user from the complexity of cryptographic applications and its legal implications, it may be applied server-to-server, privileging usability against security, as the case for PEC.

Now we describe the phases of the PEC functional protocol. First of all, the sender's UA authenticates against the **Sender's Access Point** (S-AP) and submits the message to the S-AP Message Transfer Agent (MTA). The S-AP performs validity checks on the messages and stores an NRS evidence into the sender's Message Store (MS), if they pass. Otherwise, a non-acceptance evidence (negative NRS) is generated and stored into the sender's MS including the reason of the failure. Then, the S-AP wraps the message into a new, signed S/MIME v3 envelope with his x509 v3 certificate and forwards it to the **Recipient's Reception Point** (R-RP) using SMTP. If the R-RP does not acknowledge this message with a take-in-charge evidence within the next 12 h, the S-AP stores a non-delivery-to-RP evidence (negative NRD) into the sender's MS. If this operation was successful, the R-RP verifies the digital signature of the S-AP. If it is, R-RP returns a take-in-charge evidence to the S-RP, which is forwarded to the **Sender's Delivery Point** (S-DP) and stored into the sender's MS. Then, the R-RP forwards the message to the R-DP, returning a non-take-in charge evidence to the S-RP in case of an error, which is forwarded to the S-DP and stored into the sender's MS. If the R-DP operation was successful, an NRD evidence is returned by the R-DP to the S-RP and forwarded to the S-DP, which stores the message into the sender's MS. In all other cases, a non-delivery evidence (negative NRD) is returned.

III. Certified E-Mail systems

For more than a decade the EC has supported initiatives and projects in order to ensure economic growth. Some of these projects aim to create interoperability frameworks for the mutual recognition of electronic documents and delivery. According to the targets of each project, cross-border interoperability must not require a completely new communication infrastructure, rather it should be achieved by bridging existing systems. This section, after an overview of the architecture of two of the most important European CEMs and the introduction of a recent standard, **Registered Electronic Mail** (REM), discusses their interoperability on a technical and organizational level. In [5] is possible to find more details.

A. Austrian DDS

Requirements for the Austrian CEM, called **Document Delivery System** (DDS) [9], are laid down by the "Law on the Delivery of Official Documents" [10]. DDS defines the following main types of entities: (1) **senders**: all public entities can register as sender, (2) **delivery agents** (DA): they act as inline TTP and have to be accredited by the Federal Chancellery, (3) **recipients**: all physical persons and corporate bodies can register with one or more DAs, and (4) **Central lookup service** (CLS): the Austrian Federal Chancellery operates a lookup service holding the address data of all recipients registered with a DA. Only recipients have to register with DAs, while senders are required to register and authenticate themselves with the CLS using an

X509v3 certificate. Recipient's registration is based on the Austrian national electronic ID card, which complies to the EU Signature Directive [11].

Senders addresses recipients with an unique ID, derived from the national identification number. First of all, the sender's user agent (UA) must query the CLS to determine with which DA(s) a recipient is registered, using an HTTPs GET request based on SSL client authentication. Each DA list entry contains a unique billing token, generated using strong RSA encryption. Then, the sender's UA chooses a DA from the list and submits the message to the web service endpoint of the recipient's DA, using the SOAP transport protocol. Senders are recommended to electronically sign documents to provide an NRO evidence. The DA takes the message in charge and stores it into the recipient's MS. The recipient's UA authenticates himself with his DA using a web-browser or e-mail client and generates an NRR evidence by signing an XML-based proof of receipt using his citizen card, then the message can be retrieved by the recipient's UA from the MS. The DA timestamps and digitally countersigns the NRR evidence and returns it to either the sender's e-mail address or a web service provided by the sender's UA. If a recipient does not pick up the message within two weeks, the DA returns a non-delivery evidence (negative NRR) back to the sender.

B. German DeMail

De-Mail is a project of the German government with the aim of providing a reliable and legally binding communication infrastructure for administrations and citizens [12]. De-Mail is layered on top of the SMTP protocol. The main types of entities are similar to the ones of DDS. DAs act as inline TTPs and have to be accredited by the BSI for compliance with given technical and organizational requirements. Both senders and recipients have to register a mailbox with a DA, using an official ID document or the national eID, which complies to the EU Signature Directive. The technical concept distinguishes between two types of communication channels having different security requirements: the communication between end-entities and their DAs and the intra-provider communication between DAs, which is based on SMTP and a secure TLS connection. Also user authentication is required to be based on encrypted channels, e.g., a TLS - based connection. The system architecture provides consistent encryption between all communication nodes. On a voluntary basis, recipients may list their own encryption certificate in a public directory. De-Mail provides two basic delivery qualities for senders: standard mail and certified mail. Standard mail only ensures message integrity and confidentiality between the sender and the recipient throughout the whole communication channel. In the following, we describe De-Mail system.

First of all, the sender's UA authenticates itself with his DA and submits the message to the DA's MTA using a secured channel, e.g. a TLS channel. The message may also be encrypted for the recipient and/or digitally signed, e.g. using x.509v3 certificates, to provide an NRO evidence. The sender's DA checks the message for correctness (existing recipient, headers, etc.) and stores an NRS evidence into the sender's MS, including the hash value of the original message and a timestamp. The NRS evidence must be signed by the sender's MTA. The sender's provider encrypts the message with its own private key and the public key of the recipient's provider and forwards the message to the recipient's MTA, where it is decrypted, checked for correctness and stored into the recipient's MS. Finally, the recipient's MTA generates an NRD evidence containing the hash value of the original message and a timestamp. This evidence is returned to the sender's MTA, which stores it into the sender's MS. Like the NRS evidence, the recipient's MTA must sign the NRD evidence.

C. Registered Electronic Mail Standard

In 2008, ETSI published a first version of the REM standard [13]. REM is primarily intended as an evidence standard to establish interoperability between different certified e-mail domains operating under different policies and countries. Now, we briefly discuss the five parts of the REM standard:

1) **Part 1: Architecture**: it describes the logical model of an REM system, introducing roles, styles of operation, interfaces and main evidence types. An REM system is called **REM Management Domain** (REM-MD) and acts as an inline TTP between senders and recipients. A REM-MD consists of at least three core components: an MTA, a **message store** (MS) and an **evidence provider** (EP). REM supports two basic styles of operation: **store and forward** (S&F) where messages are directly forwarded to the recipient, and **store and notify** (S&N), where the recipient is only notified and must retrieve the message from the sender's REM-MD MS.
2) **Part 2: Data requirements, Formats and Signatures for REM**: it deals with the specification of REM-MD envelopes, REM dispatches and REM evidences. A REM-MD envelope is defined as a MIME message encapsulating both REM dispatches and REM evidences. A REM dispatch holds the delivery content as payload. REM evidences are well-structured containers holding all evidence-related data. The standard specifies three evidence formats and the corresponding signature types. It also describes in detail the mechanisms for trust establishment between different REM-MDs with the **ETSI Trust-service Status List** (TSL) (ETSI, 2009) standard for mutual recognition of trusted REM services.
3) **Part 3: Information Security Policy Requirements for REM Management Domains**: it specifies the assessment of security requirements of REM-MDs being compliant to ISO/IEC 27001 (ISO/IEC, 2005a). Controls to mitigate security risks have to be selected according to the ISO/IEC 27002 (ISO/IEC, 2005b). It also defines the authentication mechanisms and their quality levels for senders and recipients, and restricts the type of signatures to be used to increase interoperability.
4) **Part 4: REM-MD Conformance Profiles**: it introduces two conformance profiles and specifies the mandatory

requirements a REM-MD has to meet to be compliant with each profile.

5) **Part 5: REM-MD Interoperability Profiles**: it profiles the standard to ease interoperability between different SMTP-based REM-MDs, for both REM dispatches and REM evidences.

Now, we describe the REM protocol steps in case of the S&F style. First of all, the sender's UA submits a message through the **sender message submission interface** (S-MSI) to the MTA of the sender's REM Management Domain (S-REM MD), which may create an NRS evidence and store it into the sender's MS. The S-REM MD MTA forwards a REM dispatch through the **MD relay interface** (MD-RI) to the MTA of the recipient's REM Management Domain (R-REM MD). The REM dispatch includes the sender's original message and may include also the aforementioned NRS evidence. The R-REM MD MTA stores the message into the recipient's MS. Then, the R-REM MD EP creates an NRD evidence and returns it back to the S-REM MD MTA through the MD-RI, which stores it into the sender's MS.

Depending on the REM implementation, several other actors, evidence types and message flows may be involved. Third parties, such as system components, TTPs, arbiters or other users, may retrieve evidences from MS through the so-called **third-party evidence retrieval interface** (TP-ERI).

D. CEMs properties and interoperability

In this section, we describe which of the properties reported in section II are actually applied by the CEMs described above, summarized in figure 2: a black circle represents a property which is satisfied, a white one represent an optional property which is satisfied only under particular conditions, while the absence of a circle means that the property is not satisfied. We also discuss the findings and impact in the context of interoperability.

CMS Name	DDS	PEC	De-Mail	REM
Country	AUT	ITA	DEU	ETSI
NRO	○	○	○	●
NRR	●			●
NRS		●	●	●
NRD		●	●	●

Fig. 2. Classification of CEMs according to satisfied security properties

Figure does not report properties which are universally applied by CEMs discussed above. In particular, all solutions use inline TTPs, whereas actual research is focusing on offline solutions. In fact, inline TTPs may become a bottleneck because of the amount of communicational and computational power needed, but we can note that certified email traffic is limited respect to traditional email traffic due to lack of spam and the cost of the service. Instead, to reduce the need of computational power, especially for cryptographic operations, the most part of inline TTPs use off-the-shelf components, such as Hardware Security Modules (HSM). Finally, inline TTPs request that all entities completely trust them; in practice, this seems to be mitigated by the fact that TTPs are required by law to undergo a technical and organizational accreditation. There are also some benefits: first of all, inline TTPs allow the full control of message flows, facilitating the CEM deployment; then, they allow asynchronous communication, decoupling sender and recipients from each other, avoiding direct interaction; finally, since they take in charge the most part of protocol operations such as notification of evidence and authentication of messages, end users can use traditional email clients or web browsers.

Another common property for all the CEMs is the use of standard electronic signatures for the generation of evidences or to guarantee authenticity and integrity of the exchanged electronic documents, as in Italian PEC.

For non-repudiation services, we do not see a common approach. Senders have to authenticate against inline TTPs, which seems to be sufficient for most CEMs to ensure some kind of NRO, so NRO evidences are not seen as necessary. NRS evidences appear to be essential in provider-based systems where messages may leave the sender's provider domain. However, there is a consensus on the usage of NRD evidences, which seems to be a core property. Using inline TTPs, an NRR evidence is not necessarily needed, because TTPs can preserve messages and return a delivery receipt to the sender even if the recipient has not yet retrieved the message.

Actually, most CEMs are closed systems, and do not provide interfaces to other CEM to interoperate. For example, end users have to register with multiple CEM to address different recipients, increasing costs, so there is the need for a global certified electronic mail system. The EC, as discussed at the beginning of this section, lunched several initiatives and projects to increase interoperability. ETSI tried to fill this gap by introducing the REM standard, described in section III-C, but it has been rarely used so far and has not been widely adopted by governments or industries; for example, the Italian PEC and the German De-Mail are fully compatible with the **Part 5** of REM, since it deals with SMTP-based CEMs, while Austrian DDS is not compatible due to the use of HTTP. So, recently, a **Large Scale Pilot** (LSP) european project, called **Simple Procedures Online for Crossborder Services** (SPOCS), have been started to address this issue. SPOCS is based on an appropriate framework on top of existing systems, applying the design principles of the European Interoperability Framework [14]. The main idea behind the concept is a gateway solution making CEMs interoperable with a multilateral approach on different layers, including technical, semantic and procedural interoperability.

Independently, AGID published the PEC technical rules as an Informational Request for Comment (RFC6109) in April 2011 [15] to the **Internet Engineering Task Force** (IETF). The idea of the Italian Government was to share this experience with the international community and receive feedback in order to encourage the development and consolidation of a common standard.

As mentioned in the abstract, recently EU introduced the eIDAS Regulation [16], which replaces the EU Signature Directive [11]. Its main purpose is to leverage the LSPs as a pillar for the development of interoperability of cross-border eID and trust, by forcing Member States to a mutual recognition and acceptance of electronic identification, to give legal effect to trust services and to provide a legal cross-border framework for electronic seals, time stamping and electronic document acceptability and delivery. AGID is now investigating if PEC technical rules are full compliant with the Regulation, to plan changes to the legislation and the specifications accordingly.

As part of this process, in the next section we introduce a possible evolution of the PEC, which purpose is to increase interoperability and standardization level of the CEM solution.

IV. Evolution of the Italian PEC

In this section, we introduce a possible evolution to Italian PEC technical specifications to increase standardization and interoperability of the actual solution.

In the actual solution, PEC providers must sign all messages and evidences according to the S/MIME v3 standard with an x.509 v3 certificate. This certificate, and the list of the accredited PEC providers, are stored in a centralized directory based on Lightweight Directory Access Protocol (LDAP), managed by AGID; the access to this directory is limited to PEC providers only. This mechanism is not interoperable with other CEMs, is not scalable and based on a proprietary LDAP directory schema; our idea is to substitute it with a distributed solution based on the publication of a PEC provider's certificate in the Distributed Name System (DNS) [17], [18]. DNS is a worldwide distributed database which associates various information with domain names. In this paper, we use the DNSSec and the recent TLSA standard, which are described in the next section.

A. DNS Security Extension

DNSSec [19]–[21] is an extension of the DNS that provides authentication of data to DNS clients, authenticated denial of existence, and data integrity, but not availability or confidentiality. DNSSec is perfectly backward compatible with DNS and it inherits the same hierarchy, so that a DNSSec server can resolve DNS query and viceversa, in a best-effort way. For this purpose it adds new Resource Records(RRS):

- **RRSIG Record**: contains digital signature to authenticate a set of RRs
- **DNSKEY Record**: contains the public key used to verify RRSIG's record signature
- **DS Record**: contains the hash of the public key of the delegated zone digitally signed by the private key of the parent zone
- **NSEC Record**: contains a link of the following domain name in the zone to authenticate the denial of existence

The DANE IETF working group aims to develop protocols and techniques to enable internet applications to establish cryptographically secure communications based on DNSSec, to replace the traditional model based on Public Key Infrastructure [8]. With RFC6698 [22] DANE specifies a new RR, called **TLSA**, to embed in an authoritative DNSSec zone the authentication information for a x.509 v3 certificate (or part of it). The TLSA RR links the x.509 v3 certificate or public key with its domain name, thus forming a **TLSA certificate association**. The certificate embedded in this way is authenticated by the DNSSec trust chain.

B. Architecture of the proposed evolution

In this section, we describe briefly the logical architecture of the proposed evolution of the Italian PEC.

To distribute responsibility and to increase scalability, the proposal required that each PEC provider must create and manage its own authoritative DNSSec zone, with a unique and well-known domain name. Each PEC provider must publish at least two RRs:

1) a TLSA RR, which embeds the x.509 v3 certificate of the PEC provider. The TLSA standard allows an entity to release and revoke autonomously its own certificates, avoiding the use of a Certification Authority (CA).
2) a TXT RR, which contains a unique string signed with a private key managed by AGID. This record is useful to identify an accredited PEC provider.

The set of all TXT RRs published by PEC providers substitutes the list of accredited PEC providers previously maintained in the centralized LDAP directory. To authenticate such records, the proposal required AGID to create its own DNSSec zone to publish a TLSA RR which embeds the needed public key.

Figure 3 shows the flow of a PEC message from a Sender to a Receiver, limited to the modifications involved by this proposal. S-DNS and R-DNS are the DNSSec zone of the PEC providers which manage the PEC domains of the Sender and the Receiver, respectively.

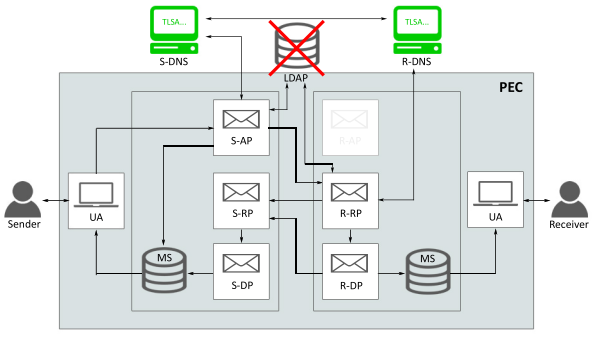

Fig. 3. Functional schema of the evolution of PEC

To check if the PEC provider of the recipient is accredited, the S-AP submits a DNSSec query to retrieve the TXT RR of the Receiver's PEC provider and the TLSA RR of the public key managed by AGID. If these RRs are present and validated, than the Receiver's PEC provider is accredited. In case of a DNS system error (DNS request timeout, one of the RRs

is not present or cannot be validated, etc...), the Receiver's PEC provider is safely considered not accredited, to prevent possible Internet attacks to the DNS system.

When the R-RP receives the certified e-mail, it must perform a check on the Sender's PEC provider similar to the one performed by the S-AP. After it, R-RP submits a DNSSec query to retrieve the TLSA RR which embeds the x.509 v3 certificate of the Sender's PEC provider to verify the digital signature of the S-AP. In case of a DNS system error (DNS request timeout, the TLSA RR is not present or not validated, etc...), the email is safely considered not a PEC message and a negative NRD evidence is returned by the R-RP to the S-RP.

In the following, we describe the main benefits of this proposal. First of all, we must note that the use of DNSSec guarantees a high level of security in the retrieval of information from an insecure communication channel such as Internet, allowing the protection of the answer to DNS query against Man in the Middle (MITM) attacks. Moreover, it guarantees the integrity and authenticity of the data contained in the DNSSec zones, ensuring the bind with the origin and allowing the generation of NRO, NRS and NRD evidence. Other benefits are (1) an increased scalability in terms of a possible growth in the number of PEC providers and mailboxes, (2) the limited number of changes to the actual PEC technical rules; in fact, the new proposal impacts only on the algorithm and the way to store, access and retrieve information about the x.509 v3 certificates of the PEC providers, (3) an increased standardization degree, which led to an increase in interoperability with other CEMs. For instance, a De-Mail provider, which is based on the same transport protocol, could authenticate a PEC message by retrieving the x.509 v3 certificate of a PEC provider from its DNSSec zone.

V. Conclusions and future work

In the process of dematerialization of physical documents, CEMs have been created in order to introduce certification of electronic communication with legal validity, analogously to the surface certified mail, which usually provides both sender and receiver with sending and delivery receipts. Those evidences are commonly used in civil administrative cases or disputes and rely on the existence of a TTP that is not involved/interested in the content of communications, and carried out the services, such as Postal Entities or a CA, e.g. to build a Trust Chain in electronic document protocol.

Being the electronic mail an open, interoperable and insecure tools, it needs to be adapted by increasing its level of certification. Introducing certification elements in the Internet mail, also if supported by the adoption of standards, fall down into the introduction of a Third Trust Part. This requires agreements between Service Providers inside and outside Country boundaries, a process that would also involve Government, difficult to be pursued worldwide.

In conclusion, this proposal does not impact substantially on the current Italian legislation, requiring only to change the technical rules that are annex of the law, maintaining the same security level but moving from PKI to the DNSSec hierarchy with great advantages in term of adoption of a standardized distributed solution and cost reduction. As a future work, we will complete the modification to the PEC technical specifications, starting a complete set of functional tests to validate the practical application of the new proposal. Furthermore, we will investigate about the introduction of Security Assertion Markup Language (SAML) [23] as authentication mechanism to authorize and uniquely identified PEC end-users, to fill the gap in the PEC technical rules mentioned in section II, in order to achieve a better complain with eIDAS requirements.

References

[1] I. Government, "Decreto sviluppo 22-06-2012," http://www.leggioggi.it/allegati/decreto-sviluppo-testo-dl-83-2012-convertito-legge-134-2012/, 2012.

[2] CNIPA, "Circolare cnipa cr/49," http://archivio.cnipa.gov.it/site/_files/-CIRCOLARE2005.

[3] ——, "Circolare cnipa cr/51," http://archivio.cnipa.gov.it/site/_content-files/01384500/1384506_circolare2006.

[4] C. Petrucci, F. Gennai, M. Buzzi, and A. Vinciarelli, "Italian standard certified electronic mail: Posta elettronica certificata (pec)," in *MeT 2011*, 2011, pp. 1–12.

[5] A. Tauber, "A survey of certified mail systems provided on the internet," *Computers & Security*, vol. 30, no. 67, pp. 464 – 485, 2011.

[6] CNIPA, "Regole tecniche del servizio di trasmissione di documenti informatici mediante posta elettronica certificata," http://www.agid.gov.it/sites/default/files/leggi_decreti_direttive/pec_regole_tecniche_dm_2-nov-2005.pdf, 2005.

[7] IETF, "Rfc5751 - secure/multipurpose internet mail extensions (s/mime) version 3.2: Message specification," https://www.ietf.org/rfc/rfc5751.txt, 2010.

[8] ——, "Rfc5280 - internet x.509 public key infrastructure certificate and certificate revocation list (crl) profile," https://www.ietf.org/rfc/rfc5280.txt, 2008.

[9] P. Reichstadter, A. Tauber, and A. Hollosi, "Modell und prozesse der elektronischen zustellung," 2008.

[10] ZustG, "Zustellgesetz. bundesgesetz uber die zustellung behordlicher dokumente," 2004.

[11] E. Parliament, "Directive 1999/93/ec on a community framework for electronic signatures," http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31999L0093, 1999.

[12] BSI, "De-mail, technische richtlinie fur burgerportale," 2009.

[13] ETSI, "Etsi ts 102 640-1: electronic signatures and infrastructures (esi) - registered eletronic mail," 2010.

[14] E. Union, "European interoperability framework (eif) for european public services," http://ec.europa.eu/isa/documents/isa_annex_ii_eif_en.pdf, 2010.

[15] IETF, "Rfc6109 - la posta elettronica certificata - italian certified electronic mail," http://tools.ietf.org/html/rfc6109, 2011.

[16] E. Parliament, "Regulation 910/2014 on electronic identification and trust services," http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG, 2014.

[17] IETF, "Rfc1034 - domain names - concepts and facilities," https://www.ietf.org/rfc/rfc1034.txt, 1987.

[18] ——, "Rfc1035 - domain names - implementation and specification," https://www.ietf.org/rfc/rfc1035.txt, 1987.

[19] ——, "Rfc4033 - dns security introduction and requirements," https://www.ietf.org/rfc/rfc4033.txt, 2005.

[20] ——, "Rfc4034 - resource records for the dns security extensions," https://www.ietf.org/rfc/rfc4034.txt, 2005.

[21] ——, "Rfc4035 - protocol modifications for the dns security extensions," https://www.ietf.org/rfc/rfc4035.txt, 2005.

[22] ——, "Rfc6698 - the dns-based authentication of named entities (dane) transport layer security (tls) protocol: Tlsa," https://www.ietf.org/rfc/rfc6698.txt, 2012.

[23] ——, "Saml enhanced client sasl and gss-api mechanisms draft-ietf-kitten-sasl-saml-ec-12," https://tools.ietf.org/html/draft-ietf-kitten-sasl-saml-ec-12.txt, 2014.