# From National Certified Email Systems to European Registered Email Systems: a Case Study

Marina Buzzi

IIT-CNR, Institute of Informatics and Telematics, National Research Council, Italy, marina.buzzi@iit.cnr.it

Francesco Gennai

ISTI-CNR, Institute of Information Science and Technologies, National Research Council, Italy, francesco.gennai@isti.cnr.it

Loredana Martusciello

IIT-CNR, Institute of Informatics and Telematics, National Research Council, Italy, loredana.martusciello@iit.cnr.it

Alessandra Antolini

AgID, Agency for Digital Italy, Roma, Italy, antolini@agid.gov.it

Giuseppe Mancinelli

AgID, Agency for Digital Italy, Roma, Italy, giuseppe.mancinelli@agid.gov.it

Claudio Petrucci

AgID, Agency for Digital Italy, Roma, Italy, petrucci@agid.gov.it

Roberto Reale

AgID, Agency for Digital Italy, Roma, Italy, roberto.reale@agid.gov.it

Since 2006 the European Union has addressed the problem of the interoperability of Certified eMail Systems of Member States, in order to promote data and document exchange among Member States and to foster economic growth, as well as simplify administrative tasks within the Digital Single Market. In the last twenty years EU Member States introduced their own national certified email systems such as Posta Elettronica Certificata (PEC) in Italy, but cross-border interoperability is still lacking. In 2019, ETSI defined the Registered EMail (REM) Specifications. This implies migrating from the current EU national certified email system to the new REM architecture. This paper discusses how the Italian government is approaching this transition process, presenting the main differences between the national certified email system (PEC) and the REM. Based on the experience gained, a few suggestions are proposed for policy makers who need to address similar challenges.

**CCS CONCEPTS** • Certified email system • **Interoperability** • Registered EMail

**Additional Keywords and Phrases:** Certified email, Interoperability, Registered EMail (REM), EU

**ACM Reference Format:**

Marina Buzzi, Francesco Gennai, Loredana Martusciello, Alessandra Antolini, Giuseppe Mancinelli, Claudio Petrucci, Roberto Reale, From National Certified Email Systems to the European Registered Email Systems: a Case Study, In *Proceedings of ICEGOV Conference '22. ACM, Guimarães, Portugal (PT), 4 pages.* https://doi.org/10.1145/3560107.3560256

# 1 Introduction

As digitalization became increasingly pervasive, EU Member States started to create their own national certified email systems such as Incamail (Switzerland), Posta Elettronica Certificata or PEC (Italy), and De-Mail (Germany). This fueled the development of services relying on certified email at a national level, but cross-border interoperability was still lacking. Indeed, due to a lack of coordination at the European level, these systems are not interoperable, hampering the development of the Digital Single Market. The EU project "Pan-European Public Procurement Online" paved the way for the definition of the European Registered Email (REM) through its seminal Work Project (WP8), which developed a "secure and reliable transport of electronic business documents" [1]. The ETSI REM specifications include a set of four documents, the suite ETSI EN 319 532 1-4 (https://www.etsi.org/).

In Italy, AGID (Agenzia per l'Italia Digitale), the public body in charge of planning, implementing, and monitoring the Public Administration digitalization process, has coordinated the evolution of certified email systems to ensure compliance with technical and legal requirements. In October 2019, AGID established a Working Group (WG) with the aim of defining the new Technical Rules compliant with the functional requirements for a qualified and certified electronic delivery service addressed by the eIDAS (electronic IDentification, Authentication and trust Services) Regulation. This enabled Italian operators to operate not only in the internal market, but also in the territorial scope of application of the eIDAS Regulation, benefiting from the legal presumptions provided therein. The WG on the basis of the ETSI REM standards selected a transport architecture based on SMTP, in order to safeguard the investments carried out at a national level by institutions, providers, and user communities since the introduction of the PEC. This paper is organized into five sections. Section 2 introduces Related Work, section 3 discusses REM vs PEC, section 4 analizes interoperability issues, and section 5 proposes some guidelines for policy makers and conclusion.

# 2 RELATED WORK

A review of certified email systems was carried out in [2]. Tauber [3] introduced a set of definitions and a set of properties of certified email systems: a) Non-repudiation of origin (NRO) if it gives evidence against the false denial of having originated the message b) Non-Repudiation of Receipt (NRR) if it gives evidence against the false denial of having received the message. Moreover, the protocol 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. If the TTP is actively involved in each protocol step, it is called inline TTP. If it is only involved in a dispute resolution process, it is called offline TTP. Many studies focusing on certified email protocols relying on TTP propose new protocols for improving efficiency, fairness and security features [4],[5],[6] but the implications of migration due to transborder interoperability in the EU have not yet been analyzed. This paper compares the main features of REM systems vs the Italian certified email system PEC and provides several suggestions for helping governments customize the general policy and define instances meeting their national requirements, and for organizing and managing migration to the new standards. Systems such as Incamail and De-Mail, relying on email protocols, in their migration process towards the REM standard, would face issues analogous to those experienced by the Italian Government in the PEC migration. In contrast, certified delivery systems relying on http protocols such as DDS (Austria) have to address different problems that need further investigation.

# 3 PEC ARCHITECTURE

From a legal point of view, the Italian government has created the legal substrate for laying down the rules that endow an e-mail with legally *erga omnes* validity. The PEC provides digital evidence (digitally signed files with associated timestamps) attesting the sending and delivery of electronic documents from the sender to the receiver's mailbox. The service is based on a set of PEC providers, enabled by legal requirements that are certified by Agid. Figure 1 shows the logical schema of the PEC architecture. More details are described in the Informational RFC [7].

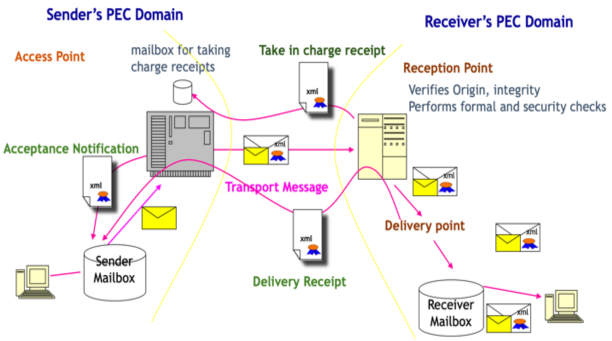

**Figure 1: The flow of a PEC message**

The sender creates or selects one or more electronic documents. The PEC operates as a transport layer without worrying about the transferred content (payload). After the authentication and authorization phases, the sender composes and sends the message via email client interface. "When the user sends the message, the PEC server of the sender's PEC provider performs a set of tests to verify the formal correctness of the message and the absence of viruses" [7]. If these checks reveal a critical issue, the system discards the message and sends a signed receipt to the sender, notifying them of this event. "If no critical aspects emerge, the sender's PEC provider includes the message created by the sender as an attachment in a "transport envelope", and digitally signs it to ensure the integrity of the message during delivery. Next, the message is forwarded through the network to the PEC provider of the receiver" [7].

The receiver's PEC provider, in turn, performs a series of tests designed to check the source and the integrity of the received message, to verify the integrity and non-alteration of the message during transit between PEC providers. "The receiver's PEC provider also checks for the presence of any virus that would block the forwarding of the message. This event causes the sender's PEC provider to emit a non-delivery PEC notification to the sender. Otherwise, the receiver's PEC provider delivers the message to the mailbox of the recipient" [7]. At the conclusion of this operation, the recipient's PEC provider will send the delivery PEC notification. This receipt confirms that the message sent by the sender has been delivered to the mailbox of the receiver (while no evidence is ever returned on the "read" status) and can also highlight the transmission content (original message), depending on the chosen configuration. "The PEC delivery notification is electronically signed by the recipient's PEC provider to further guarantee the legal validity of that notification" [7]. The recipient can access the message in their mailbox as in a traditional mail system.

A fundamental point in this architecture is related to the identity of the PEC Providers and the PEC domains. To this end, a PEC provider is registered in the public list of PEC service providers maintained by Agid, including its managed domains (IGPEC file). This centralized solution is not necessarily scalable but provides an authoritative list of PEC Trust Providers and domains. In the following section we will discuss how REM addresses this point.

The last difference is related to the signature created and added during the message flow from the sender to the receiver. PEC utilizes S/MIME digital signature while REMS exploit both Cades and Xades signatures.

# 4 REM vs PEC Architecture

REM is part of the *Electronic Registered Delivery Services (ERDS)* based on Store&Forward (relying on the email transport architecture). From a functional point of view, the flow of a message into the REM architecture is similar to the PEC. This is very important since it implies that for the final user the migration from PEC to REM is transparent; i.e., it does not impact on senders or receivers on REM messages. The main differences are a) the format of evidence (receipts), b) applied signatures, c) the mechanism for the trust identification of REM Service Providers (REMSP) and REM domains. The REM server R-REMS indicates the server of the Recipient's REMS and S-REMS indicates the server of the Sender's REMS. Analogously to PEC, a REM system implements the following macro-functions:

1. Acceptance of an email from its users, after having performed the (mandatory) formal validity checks
2. Forwarding of the original email wrapped in an email in REM format (dispatch) (if the checks carried out by the primary acceptance module are successful)
3. Taking charge of a REM email (dispatch) from other REM providers
4. Delivery of a REM email (dispatch type)
5. Creation of notification when the following events occur: (non/) acceptance of original message, (non/) delivery to the recipient, (non/)acceptance, timeout expiration.

Main differences between PEC and REM impact on:

- Formats of the XML files. There are minor changes in names, attributes, and semantics. The XML structure is signed with the XADES-B-T signature (which derives from the W3C XML dsig with a few minor changes).
- Mechanisms for enabling identity between REM Providers and REM domains.

The Agid WG in January 2020 produced the document “REM Services - Criteria for the adoption of ETSI standards - Policy IT”, updated in 2021, after various interactions with the ESI committee that oversees the ETSI-REM standards. The collaboration with the ESI Committee highlighted the need to integrate the ETSI-REM standards with a new document (introducing the Common Service Interface), which is currently in the form of a draft and is in the ETSI public inquiry.

Key REM components are CSI (Common Service Infrastructure) and the Trust List. The CSI is the mechanism enabling the a trust identification of the REM Providers. Another essential component is the Capability & Security Information, an XML structure that extends the Trusted List structure through which a Provider publishes its capability metadata, including the X.509v3 certificate, presented by the Provider in SMTP-TLS sessions. In this scenario, AgID acts as a control and certification authority, identifies the Providers, and ensures that the relevant membership rules are respected. In the new scenario, REM domains are discovered through DNS.

## 4.1 Trust identification of the REMSP

The ETSI specification is very broad and introduces functions that can be mandatory or optional (REM baselines) [8]. The REM Policy IT instantiates these functions to define their attributes (mandatory or optional) necessary for REMSP to implement their systems.

The European eIDAS Regulation on electronic identification and trust services is a key enabler for secure cross-border transactions that ensures that services can exploit their own national electronic identification schemes (eIDs) to access digital public services in other EU countries (https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation).

eIDAS requires Providers of Qualified Services to be inserted into the European Trusted List. This also means that REMSPs have to be inserted into a trusted list (XML file) as well. The EU Trusted List declares the Providers for every kind of functionality (digital signature, time stamp, etc.) and includes the Provider X509 certificate. It is accessible at https://webgate.ec.europa.eu/tl-browser/#/.

In the case of REMSP, it is necessary to introduce a new entry for each REM Provider in the Trusted List for Italy. To ensure interoperability, the REM provider must be added to this list. Thus, in the REM architecture, when sending an email via SMTP, to be sure of the identity of the service supply point, i.e., to avoid MITM (Man in The Middle) attacks the S-REMS has to access the capability&management interface, to retrieve X.509v3 certificate of the R-REMS.

## 4.2 Trust identification of the REM Domains

The current PEC architecture, based on the LDIF-IGPEC file, allows the identification of a Provider and of the PEC domains that belong to it. Thus, for the PEC there is no mechanism in place that allows a Provider to have the necessary guarantees to identify the remote Provider when opening an SMTP-TLS session; it makes use of the simple opportunistic TLS, therefore it is not protected from a MITM attack that directs the SMTP-TLS session to a compromised Provider.

On the other hand, PEC allows the certified identification of a PEC domain. Considering the specifications of the REM and the related REM Policy IT, we can identify the “Certification of a Provider” within the scope of the Common Service Interface, while the definition of a security mechanism to certify a REM domain is left to Member States. An Internet email domain presents itself to the REM system (as well as to the PEC system) via an MX record inserted in a name server, that may be out of the applicability of a centralized control policy if it is managed by external organizational units (organizations, individuals).

While PEC has adopted a centralized management solution, which by avoiding the management of non-controllable components, certifies in a reliable way a domain as a PEC domain, a centralized LDIF - IGPEC file may in principle pose operational challenges, even though no scalability issues have been experienced in the production environment. For the REM, which is based on a distributed management model, it is possible to exploit DNS (DANE) or the web (MTA-STS), two solutions involving external organizational units and maintenance activities (certificate renewal, etc.). Indeed, the best scalability of a system is obtained at the cost of distributing configurations and related maintenance activities among multiple organizational units. The distributed solutions (DANE, MTA-STS) guarantee the necessary safety/certification even in case of incorrect operations or configurations by the individual external operating units. In these cases, a single unit may be subject to outages, without however compromising security and/or certification functionalities outside its DNS namespace.

# 5 GUIDELINES AND CONCLUSION

The complex transition of the national certified email systems to qualified certified delivery services compliant with the eIDAS regulation requires a long, resource-consuming process. Policymaking faces two main challenges: (1) Introducing the new interoperable REM protocols while safeguarding the investments performed by PEC Providers over time and (2) Keeping a path between legal constraints and system requirements for making technical solutions easily applicable. Relevant findings from our experience are suggested:

- Create a multidisciplinary and inclusive policy-making Working Group, including all stakeholders. It is crucial that policy makers work with technicians to adopt secure and reliable solutions.
- Schedule weekly meetings to keep attention focused on the WG discussions
- Set up technical thematic focus groups to resolve any difficulties encountered over time
- Act to minimize the risk of disruption associated with migration
- Ensure continuity with legacy processes and user experience, as far as possible.

This paper discusses the impact of the introduction of the REM in an operational environment where certified email was already extensively used by citizens, organizations, and public administrations. The format differences between PEC and REM architectures do not impact on the functional flow of the certified message, hence a migration will be transparent for the final user. On the other hand, advanced users that have developed ad-hoc tools to exploit the XML format for extracting (and processing) data will be required to update such tools. The main difference between the two architectures is related to certification of REM Providers and REM domains. REM adopts a new mechanism for guaranteeing interoperability between REM Providers, namely the Common Service Interface, while REM domains are detected via DNS. Based on the ongoing experience, some guidelines are proposed to support policy-makers addressing similar challenges. Future work will complete steps required for the qualification of REMSPs and the migration toward interoperable REM systems.

# REFERENCES

<bib id="bib1"><number>[1]</number>Ruggieri, F. 2010. Registered e-mail.Reliable e-mail for everybody. Datenschutz und DatensicherheitDuD, 34(5) 314-317.</bib>
<bib id="bib2"><number>[2]</number>Tauber, A. 2011. A survey of certified mail systems provided on the Internet. *Computers & Security*, *30*(6-7), 464-485.</bib>
<bib id="bib3"><number>[3]</number>Tauber, A., Kustor, P., & Karning, B. 2013. Cross-border certified electronic mailing: A European perspective. *Computer law & security review*, *29*(1), 28-39.</bib>
<bib id="bib4"><number>[4]</number>Cederquist, J., Dashti, M. T., & Mauw, S. 2007. A certified email protocol using key chains. *Int. Conf. on Advanced Information Networking and Applications Workshops* pp. 525-530. IEEE.</bib>
<bib id="bib5"><number>[5]</number>Liu, Z., Pang, J., & Zhang, C. 2010. Extending a key-chain based certified email protocol with transparent TTP. *IEEE/IFIP Int. Conf. on Embedded and Ubiquitous Computing* (pp. 630-636).</bib>
<bib id="bib6"><number>[6]</number>Ferrer-Gomila, J. L., Hinarejos, M. F., Draper-Gil, G., & Huguet-Rotger, L. 2018. Optimistic protocol for certified electronic mail with verifiable TTP. *Computer Standards & Interfaces*, *57*, 20-30.</bib>
<bib id="bib7"><number>[7]</number>Petrucci, C., Gennai, F., Shahin, A., Vinciarelli, A. 2011. Italian Certified Electronic Mail RFC 6109, April, 2011.</bib>
<bib id="bib8"><number>[8]</number>Réti, K., Foti, S., Boldrin, L., Cruellas Ibarz, J. C., Fiedler, A., Tauber, A., ... & LLaneza, P. 2017. ETSI EN 319 532-1 v0. 0.4.</bib>