Computer Standards & Interfaces 34 (2012) 452–466

Contents lists available at SciVerse ScienceDirect

Computer Standards & Interfaces

journal homepage: www.elsevier.com/locate/csi

An interoperability standard for certified mail systems

Arne Tauber [a,*], Jörg Apitzsch [b,1], Luca Boldrin [c,2]

[a] Institute for Applied Information Processing and Communications, Graz University of Technology, Austria
[b] Bremen online services GmbH, Am Fallturm 9, D-28359 Bremen, Germany
[c] InfoCert S.p.a, C.so Stati Uniti, 14, I-35127 Padova, Italy

ARTICLE INFO

Article history:
Received 2 January 2012
Accepted 9 March 2012
Available online 17 March 2012

Keywords:
Certified electronic mail
Registered electronic mail
Interoperability
Standard
Security

ABSTRACT

A large number of certified mail systems have been put into operation on the market over the last years. In contrast to standard mailing systems like e-Mail, certified mail systems provide the secure, reliable and evidential exchange of messages with the quality of traditional postal registered or certified mail. Most of these systems are tailored to national laws, policies, needs and technical requirements and are thus closed and only accessible by certain user groups. However, the ongoing globalization and opening of the markets, especially in the European Union, ask for global certified mailing as already known from e-Mail. Interoperability of certified mail systems is a new and challenging research field. This article presents a framework and standard to make arbitrary certified mail systems interoperable. The presented approach uses a federated trust network of so-called electronic delivery gateways for seamless certified mailing across systems. This is achieved by converting protocols and system specifics on different layers using a harmonized interoperability protocol. The presented framework has been standardized by the European Telecommunications Standards Institute (ETSI) as Registered Electronic Mail specification for interoperable certified mail systems.

1. Introduction

People are accustomed to sending valuable documents in a secure and reliable way. This includes documents like deeds, contracts, bids, subpoenas, summons, etc. Regular mail has no security provisions and senders rely on the assumption of a correct and successful delivery. This is where *Registered Mail* and *Certified Mail* come into play. Registered mail is a useful vehicle in the postal world for secure mail delivery by providing extended tracking possibilities. The certified mail service provides the sender additional proofs of submission and receipt.

Nowadays, more and more people are using electronic communication means. However, standard communication systems like Internet electronic mail (e-Mail) have a poor evidential quality. They can rather be compared to sending a postcard, which lacks confidentiality, authenticity, integrity and non-repudiation. Extensions like S/MIME (Secure Multipurpose Mail Extensions) or PGP (Pretty Good Privacy) enhance the e-Mail protocol with additional cryptographic functionalities like confidentiality, integrity and authenticity. Nevertheless, the shortcoming of a non-repudiable fair exchange still remains. The Internet community tried to address this issue by introducing the four receipting mechanisms of Message Disposition Notifications (MDN) specified by RFC 3798 [17], Delivery Status Notifications (DSN) specified by RFC 3461 [25], SMTP service extensions for message tracking specified by RFC 3885 [1] and signed S/MIME receipts specified by RFC 2634 [18]. Due to the open nature of Internet e-Mail, all these extensions rely on the assumption of a fairly acting recipient. This means the recipient actually returns a receipt after having received the message.

Due to this gap, the research community has provided many protocols for secure messaging over the last two decades. They have been published as fair non-repudiation protocols. The aim was to design security extensions for asynchronous communications providing similar added value as registered or certified mail do in the postal world. The terms certified mail systems (CMS) or certified electronic mailing (CEM) are used when applying such protocols in the context of electronic mailing systems, for example Internet e-Mail. CEM is a quite young research discipline starting in the early 1990s.

Due to an increasing demand by governments, postal operators and the industry, various CMS have been put into operation over the last five years. Popular examples of governmental systems are the Italian Posta Elettronica Certificata (PEC) [16], the Austrian Document Delivery System (DDS) for the public sector [34] and the German De-Mail system [7]. Particularly the justice sector relies on the secure and evidential document delivery and started to introduce such systems several years ago with the Austrian ERV (Elektronischer Rechtsverkehr) [31] or the German EGVP (Elektronisches Gerichts- und Verwaltungspostfach) [32], which is based on the Online Services Computer Interface (OSCI) standard [2]. In the private sector mainly postal operators, which are continuously shifting their postal services into the electronic world, have identified a gap in the market and provide certified electronic

* Corresponding author. Tel.: +43 316 8735533.
E-mail addresses: Arne.Tauber@iaik.tugraz.at (A. Tauber), ja@bos-bremen.de (J. Apitzsch), Luca.Boldrin@infocert.it (L. Boldrin).
[1] Tel.: +49 421 2049539.
[2] Tel.: +39 49 8288093.

0920-5489/$ – see front matter © 2012 Elsevier B.V. All rights reserved.
doi:10.1016/j.csi.2012.03.002

mailing as value-added service. The Belgian CertiPost,[3] the German E-Postbrief,[4] the Swiss IncaMail[5] or the Slovenian Secure Mailbox[6] are popular representatives of European postal operator CMS. CMS are also largely deployed within enterprises, mainly for certified communications with external entities. These systems are mostly based on commercial off-the-shelf products.

All mentioned CMS are closed systems and thus only accessible by certain user groups. In order to address a particular recipient, senders have to be registered in the same system. It is currently not possible to send certified mailings from one system to another one. Especially businesses, which operate in multiple countries and take part in competitive tendering procedures or communicate with foreign public agencies, are forced to register accounts with multiple CMS. Like accustomed to e-Mail, users may want to have one mailbox and not to be faced with additional costs or getting familiar with new systems serving the same purpose. As being normal for e-Mail communications, there is a strong need for global certified electronic mailing. This issue has become more important with the expansion of the European Economic Area (EEA) and the creation of a European Digital Single Market aiming at increasing the growth potential within the European Union (EU) by removing legal and administrative barriers for businesses when they want to provide services abroad. A major objective in this context is to establish interoperability across different EU Member States, so that citizens and businesses can use domestic infrastructures abroad. This also includes CMS infrastructures.

CMS interoperability is a new and challenging research field. Even if some initiatives like the European Telecommunications Standards Institute (ETSI) or the Universal Postal Union (UPU) have recently started to standardize CEM communications, both research and practice lack solutions how to make existing systems interoperable. This article presents and discusses a new approach, which fills this gap by providing an interoperability framework and standard being able to couple arbitrary CMS. The remainder of this article is organized as follows. First, the topic of CEM is introduced by discussing basic concepts and security properties. Next, an overview of recent initiatives trying to achieve CMS interoperability is given. It is argued why these initiatives cannot be used to achieve interoperability between existing CMS. Following this, the main problem of CMS interoperability is sketched and requirements and challenges of an interoperability standard are discussed. That followed, the core architecture of the interoperability concept is discussed. The main idea behind the concept is a gateway solution making CMS interoperable with a multilateral approach on different layers. This includes technical, semantic, and procedural interoperability. From a technical point of view, gateways act as entry or exit point of a CMS and interface with other CMS operating on a different CEM protocol. The idea is that each CMS has at least one gateway and gateways communicate with each other using the harmonized *Interconnect Protocol* (ICP), which represents a metadata layer being able to map CMS aspects to a unified metadata protocol on a technical and semantic layer. This article also discusses the standardization of the ICP by ETSI as a new *Registered Electronic Mail* (REM) standard for bridging CMS based on different protocols. Finally, security and legal aspects are discussed and conclusions are drawn.

2. Certified electronic mail

An interoperability framework or standard usually requires a deep understanding of underlying technologies and architectural models. This also applies to the subject of CEM, which has much more aspects beyond the communicational part. Basically, a CMS operates on an underlying communication system like Internet e-Mail or Web services technologies and extends this system with several architectural concepts and security properties. To get a deeper understanding of the topic of CEM, this section introduces the general communication model and briefly discusses the most relevant practical CEM security properties.

2.1. Security properties

Certified electronic mailing is a quite young research field that started to evolve in the early 1990s. Certified mail is part of the fair exchange problem family and has thus adopted many results from the research area of fair non-repudiation protocols. Interestingly there is no consensus among researchers on the security properties a certified electronic mail protocol has to fulfill and what services it has to provide. The large number of proposed protocols having different properties confirms that view. Nevertheless, the fair and evidential exchange of messages is considered vital for certified electronic mailing.

In 2000 a first detailed overview paper was published by Kremer et al. [22], which provides a comprehensive survey of fair non-repudiation protocols. The paper also briefly reviews security properties that a fair non-repudiation protocol must respect. Oppliger [30] discussed several CEM security properties from a practical perspective. An informal analysis assesses the impact in terms of performance, level of interaction, trust and infrastructural requirements when a CEM protocol is actually deployed on the Internet. Onieva et al. [29] published a comprehensive survey of multiparty non-repudiation protocols. This means there are more parties involved than just the sender and the recipient. A recent work by Ferrer-Gomilla et al. [15] summarizes definitions, properties and requirements related to CEM. The paper features the most complete overview of security properties found in literature so far, shows the dependencies between single properties and analyzes why some of these properties are mutually exclusive. This research structure has been taken up by the authors [37], who identified and discussed practical security properties on the basis of an assessment, comparison and evaluation of existing CMS. Many CEM properties found in literature are, however, only considered from a theoretical point of view. This article only focuses on practical CEM properties, which are as follows.

2.1.1. Fairness

Fairness is a core property and makes a CEM protocol practical. Consider the scenario where an e-Mail sender signals the intention for the exchange of a message for a receipt. The recipient confirms that with a receipt and a malicious sender in the end does not send the message. Or the sender transmits the message to the recipient and a malicious recipient does not acknowledge with a receipt. Such scenarios lead to a disadvantageous position for one entity and possibly to a dispute. Fairness originates from traditional postal certified mail, where postal employees release the delivery if and only if the recipient signs a receipt. The literature defines the following flavors of fairness in the context of CEM and other non-repudiation protocols: strong, weak, true, light and probabilistic (cf. [15]). Only *strong fairness* is acceptable and implemented in practical systems. This kind of fairness denotes that all entities, this means sender and recipient, get the expected items (message content or receipt) or no one gets what is expected.

2.1.2. Trusted third parties

Each CMS has at least one trusted third party (TTP) ensuring the (strong) fair exchange of messages. Many approaches in literature have tried to minimize the trust in TTPs and to increase efficiency by reducing the involvement of TTPs. Approaches without TTP are hard to realize and emerged as being impractical. In *offline* or so-called *optimistic* approaches, TTPs are only involved in dispute resolution processes. However, offline and even *online* approaches, where a TTP is involved in each protocol run, but not in each protocol step, are hard to deploy in practice. For this reason all existing systems use *inline* TTPs, which are involved in each protocol step and act as intermediary

[3] http://www.certipost.be.
[4] http://www.epost.de.
[5] http://www.incamail.ch.
[6] http://moja.posta.si.