Cross-Border Certified Electronic Mailing

A Scalable Interoperability Framework for
Certified Mail Systems

Arne Tauber

Cross-Border Certified Electronic Mailing

A Scalable Interoperability Framework for Certified Mail Systems

Ph.D. Thesis

at

Graz University of Technology

submitted by

Arne Tauber

Institute for Applied Information Processing and Communications (IAIK),
Graz University of Technology
A-8010 Graz, Austria

April 2012

Assessors
Prof. Reinhard Posch
Prof. Antonio Lioy
Advisor
Herbert Leitold

Grenzüberschreitende Elektronische Zustellung

Ein Interoperabilitätsframework für elektronische Zustellsysteme

Doktorarbeit

an der

Technischen Universität Graz

vorgelegt von

Arne Tauber

Institut für Angewandte Informationsverarbeitung und Kommunikationstechnologie (IAIK),
Technische Universität Graz
A-8010 Graz

April 2012

Diese Arbeit ist in englischer Sprache verfasst.

Begutachter
Prof. Reinhard Posch
Prof. Antonio Lioy
Betreuer
DI Herbert Leitold

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 with the Digital Single Market, ask for global certified mailing as one is already accustomed to e-Mail. This demand is also emphasized by the ongoing implementation of the EU Services Directive.

Interoperability of certified mailing is a new and challenging research field. This thesis presents a framework to make arbitrary certified mail systems interoperable. The presented approach is aligned to the European Interoperability Framework (EIF) and reaps the benefits from best-practice concepts of other European interoperability initiatives. The concept 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 with a multilateral approach using a common certified mail language. These core elements provide a scalable interoperability framework ensuring autonomy and transparency by leaving existing systems untouched.

To demonstrate its applicability, the framework has been implemented, tested and deployed in real environments and under real conditions in two European large scale pilots. The concept presented in this thesis has been standardized by ETSI as a new Registered E-Mail (REM) standard. Even if the main objective of this thesis is to show the technical feasibility of certified mail interoperability, legal and governance aspects are vital for sustainable pan-European or global certified mailing and are thus discussed as well.

Kurzfassung

Eine Vielzahl an elektronischen Zustellsystemen ist in den letzten Jahren am Markt erschienen. Im Gegensatz zu herkömmlichen Kommunikationsmedien wie E-Mail garantieren elektronische Zustellsysteme den sicheren, verlässlichen und beweiskräftigen Austausch von Nachrichten, der mit der Qualität eines postalischen Einschreibens vergleichbar ist.

Die meisten dieser Systeme sind auf nationale Gesetze, Richtlinien oder technische Anforderungen zugeschnitten und nur bestimmten Nutzerkreisen zugänglich. Die fortschreitende Globalisierung und Öffnung der Märkte, vor allem in Hinblick auf Europa mit seinem digitalen Binnenmarkt, verlangt nach einer globalen elektronischen Zustellung so wie man sie von E-Mail Kommunikationen kennt. Dieses Bestreben wird durch die aktuelle Umsetzung der EU Dienstleistungsrichtlinie zudem verstärkt.

Interoperabilität von elektronischen Zustellsystemen ist ein neuer und herausfordernder wissenschaftlicher Forschungsbereich. Diese Arbeit präsentiert ein Rahmenwerk, um beliebige elektronische Zustellsysteme miteinander interoperabel zu machen. Der verwendete Ansatz orientiert sich an dem Europäischen Interoperabilitätsframework (EIF) und verwendet Best-Practice Konzepte von anderen europäischen Interoperabilitätsinitiativen. Das Herzstück des Frameworks ist ein föderiertes Vertrauensnetzwerk von sogenannten Zustellgateways für eine nahtlose, grenzüberschreitende elektronische Zustellung. Dies wird erreicht, indem Protokolle und Systemeigenheiten auf unterschiedlichen Ebenen über eine gemeinsame Zustellsprache konvertiert werden. Diese Kernkonzepte ermöglichen ein skalierbares Interoperabilitätsframework, welches Autonomie und Transparenz garantiert, indem bestehende Systeme unangetastet bleiben.

Um seine Anwendbarkeit zu demonstrieren, wurde das Interoperabilitätsframework in zwei Großpilotprojekten auf EU-Ebene implementiert, getestet und in operativen Umgebungen eingesetzt. Das in dieser Arbeit präsentierte Konzept wurde von ETSI als neuer Registered E-Mail (REM) Standard spezifiziert. Wenngleich das Hauptziel dieser Arbeit das Aufzeigen der technische Machbarkeit ist, so sind rechtliche Aspekte und Koordinierungsaufgaben essentielle Aspekte für ein nachhaltiges, europaübergreifendes oder globales Interoperabilitätsframework für elektronische Zustellung und werden daher ebenso diskutiert.

Statutory Declaration

I declare that I have authored this thesis independently, that I have not used other than the declared sources / resources, and that I have explicitly marked all material which has been quoted either literally or by content from the used sources.

Signature Value	h+1gBZOEE1Z1B+SKGcS0CATQbSWJ6I5qVddjPr0WpnZRaAdhTNRWJIuCb6imchKZF+f+1wu02+6/3HlILTNp4A==	
SIGNATURE INFORMATION	**Signatory**	Arne Tauber
	Issuer-Certificate	CN=a-sign-Premium-Sig-02,OU=a-sign-Premium-Sig-02,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
	Serial-No.	532347
	Method	urn:pdfsigfilter:bka.gv.at:binaer:v1.1.0
	Parameter	etsi-bka-1.0@1334233341-623139115@19754-2307-0-11535-13851
Verification	Signature verification at: http://www.signature-verification.gv.at	
Note	This document is signed with a qualified electronic signature. According to section 4 para 1 of the Signature Act it in principle is legally equivalent to an handwritten signature.	
Date/Time-UTC	2012-04-12T12:22:21Z	

Eidesstattliche Erklärung

Ich erkläre an Eides statt, dass ich die vorliegende Arbeit selbstständig verfasst, andere als die angegebenen Quellen/Hilfsmittel nicht benutzt, und die den benutzten Quellen wörtlich und inhaltlich entnommenen Stellen als solche kenntlich gemacht habe.

Signature Value	ye2A+dU7Ol9IAtQA092A9NnsN5pBo7mtYylA0YQffKaq55f47wQItptTP4iw9WGdM4woTWYdR4hTqB9vXGNDHg==	
SIGNATURE INFORMATION	**Signatory**	Arne Tauber
	Issuer-Certificate	CN=a-sign-Premium-Sig-02,OU=a-sign-Premium-Sig-02,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
	Serial-No.	532347
	Method	urn:pdfsigfilter:bka.gv.at:binaer:v1.1.0
	Parameter	etsi-bka-1.0@1334233399-623196758@21671-25773-0-15627-2688
Verification	Signature verification at: http://www.signature-verification.gv.at	
Note	This document is signed with a qualified electronic signature. According to section 4 para 1 of the Signature Act it in principle is legally equivalent to an handwritten signature.	
Date/Time-UTC	2012-04-12T12:23:19Z	

Contents

List of Figures

List of Tables

Acknowledgements

First of all, I want to thank my colleague Thomas Rössler for his great contributions to the first version of the interoperability concept, which has evolved over time in numerous fruitful discussions in the course of the STORK Large Scale Pilot. Further, I want to thank Jörg Apitzsch and Luca Boldrin for bringing in new great ideas and pushing the improvement of the concept in the course of the SPOCS Large Scale Pilot to its actual shape. I also want to thank all people - particular my co-advisor Herbert Leitold - being of great help in revising my publications and this thesis.

Both Large Scale Pilots formed a basis and a testbed for this thesis. Therefore, I also want to thank the countless people being involved in these Large Scale Pilots for helping to put the framework presented in this thesis into operation.

Last but not least, without the support and understanding of my family and my girlfriend Iris, this thesis would not have been possible.

Arne Tauber
Graz, Austria, January 2012

List of Acronyms

A2A	Administration to Administration
A2B	Administration to Business
A2C	Administration to Citizen
AdES	Advanced Electronic Signature
ADPC	Austrian Data Protection Commission
AP	Access Point
APE	Apartado Postal Electrónico
API	Application Programming Interface
ARPANET	Advanced Research Projects Agency Network
AS	Applicability Statement
ASC	Administrative Sector Code
ASN.1	Abstract Syntax Notation One
AU	Access Unit
ASCII	American Standard Code for Information Interchange
B2A	Business to Administration
B2B	Business to Business
B2C	Business to Citizen
BCG	Business Client Gateway
BGBl	Bundesgesetzblatt
BGP	Border Gateway Protocol
BII	Business Interoperability Interfaces
BSI	Bundesamt für Sicherheit in der Informationstechnik
BusDox	Business Document Exchange Network
C-PEPS	Citizen PEPS
CAdES	Cryptographic Message Syntax Advanced Electronic Signature

C2A	Citizen to Administration
C2B	Citizen to Business
C2C	Citizen to Citizen
CA	Certification Authority
CC	Clearing Center
CCITT	Comité Consultatif International Téléphonique et Télégraphique
CCP	Code of Civil Procedure
CEM	Certified Electronic Mail
CERT	Computer Emergency Response Team
cf	confer (compare)
CIE	Carta d'Identitá Elettronica
CLS	Central Lookup Service
CIP	Competitiveness and Innovation Framework Programme
CIQ	Customer Information Quality
CMS	Certified Mail System
CNS	Carta Nazionale dei Servizi
COD	Certificate of Delivery
COP	Certificate of Posting
CORBA	Common Object Request Broker Architecture
CRL	Certificate Revocation List
CRR	Central Residents Register
CSP	Certification Service Provider
DARPA	Defense Advanced Research Projects Agency
DDS	Document Delivery System
DGP	Delivery Gateway Protocol
DNS	Domain Name System
DOD	Designated Operator of Destination
DOM	Document Object Model
DOO	Designated Operator of Origin
DOS	Denial of Service
DP	Delivery Point

DPM	Digital Postmark
DSN	Delivery Status Notification
DSS	Digital Signature Service
e-Business	Electronic Business
e-Catalogue	Electronic Catalogue
e-Commerce	Electronic Commerce
e-CODEX	e-Justice Communication via Online Data Exchange
e-Delivery	Electronic Delivery
e-Document	Electronic Document
e-Filing	Electronic Filing
e-Government	Electronic Government
e-Health	Electronic Healthcare
e-Inclusion	Electronic Inclusion
e-Invoicing	Electronic Invoicing
e-Justice	Electronic Justice
e-Learning	Electronic Learning
e-Law	Electronic Law
e-mail	Electronic Mail
e-Ordering	Electronic Ordering
e-Payment	Electronic Payment
e-Prescription	Electronic Prescription
e-Procurement	Electronic Procurement
e-Safe	Electronic Safe
e-Signature	Electronic Signature
EAS	European Administrative Space
EBCDIC	Extended Binary Coded Decimal Interchange Code
ebMS	Electronic Business Message Service Specification
EDG	Electronic Delivery Gateway
ebXML	Electronic Business XML
eID	Electronic Identity
E2EE	End-to-End Encryption

EC	European Commission
ECAS	European Commission Authentication Service
ECM	Extended Certified Mail
EDI	Electronic Data Interchange
EE	Enterprise Edition
EEA	European Economic Area
EGVP	Elektronisches Gerichts- und Verwaltungspostfach
EHIC	European Health Insurance Card
EIAG	European Interoperability Architecture Guidelines
EIF	European Interoperability Framework
EIIS	European Interoperability Infrastructure Services
EIP	Entrepreneurship and Innovation Programme
EIS	European Interoperability Strategy
EJN	European Judicial Network
ENISA	European Network and Information Security Agency
EOD	Evidence of Delivery
EOO	Evidence of Origin
EOR	Evidence of Receipt
EOS	Evidence of Submission
EP	Evidence Provider
EPCM	Electronic Postal Certification Mark
epSOS	Smart Open Services for European Patients
ERV	Electronic Legal Communications
ES	Evidence Store
etc.	et cetera
ETSI	European Telecommunications Standards Institute
EU	European Union
EUPL	European Union Public License
EVS	European VCD System
FCC	Federal Computing Center
FTP	File Transfer Protocol

GeL	Government eLink
GDP	Gross Domestic Product
GUI	Graphical User Interface
HSM	Hardware Security Module
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPs	Hypertext Transfer Protocol Secure
IAF	Integrated Architecture Framework
ICM	Ideal Certified Mail
ICP	Interconnect Protocol
ICT	Information and Communication Technologies
ICT-PSP	ICT-Policy Support Programme
IDA	Interchange of Data across Administrations
IDABC	Interoperable Delivery of European eGovernment Services to public Administrations, Businesses and Citizens
IdM	Identity Management
IE	Internet Explorer
IEC	International Electrotechnical Commission
IEE	Intelligent Energy Europe Programme
IETF	Internet Engineering Task Force
IIS	Internet Information Server
IM	Instant Messaging
IMI	Internal Market Information System
IMAP	Internet Message Access Protocol
IP	Internet Protocol
IPR	Intellectual Property Right
ISA	Interoperable Solutions for European Public Administrations
ISO	International Organization for Standardization
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
ISMS	Information Security Management System
IT	Information Technology

ITU	Internet Telecommunication Union
ITU-T	Internet Telecommunication Union (ITU) Telecommunication Standardization Sector
JAB	Justitiestandaard Asynchrone Berichtenuitwisseling
JAX-B	Java Application Programming Interface (API) for Extensible Markup Language (XML) Binding
JAX-WS	Java API for XML Web Services
JCA	Java Cryptography Architecture
JCE	Java Cryptography Extension
JUBES	Justitie Berichten Service
LIME	Lightweight Message Exchange Profile
LSP	Large Scale Pilot
MAAWG	Messaging Anti-Abuse Working Group
MDN	Message Disposition Notification
MD-RI	Management Domain Relay Interface
MHE	Message Handling Environment
MHS	Message Handling System
MIME	Multipurpose Internet Mail Extensions
MOA-ID	Modules for Online Applications - Identification
MOA-SP	Modules for Online Applications - Signature Verification
MOA-SS	Modules for Online Applications - Signature Creation
MOA-ZS	Modules for Online Applications - Electronic Delivery
MOTIS	Message Oriented Text Interchange System
MS	Message Store
MsgBox	Message Box Service Relay
MSH	Message Service Handler
MTA	Message Transfer Agent
mTAN	Mobile Transaction Number
MTOM	Message Transmission Optimization Mechanism
MTS	Message Transfer System
MW	Middleware
NCP	National Contact Point

NDR	Non-Delivery Report
NGN	Next Generation Network
NIF	National Interoperability Framework
NRD	Non-Repudiation of Delivery
NRO	Non-Repudiation of Origin
NRR	Non-Repudiation of Receipt
NRS	Non-Repudiation of Submission
NRT	Non-Repudiation of Transport
NVS	National VCD System
OASIS	Organization for the Advancement of Structured Information Standards
OCSP	Online Certificate Status Protocol
ODF	Open Document Format
OID	Object Identifier
OSCI	Online Services Computer Interface
OSI	Open Systems Interconnection
OSOR	Open Source Observatory and Repository
P2P	Peer-to-Peer
PAdES	PDF Advanced Electronic Signature
PC	Personal Computer
PDAU	Physical Delivery Access Unit
PDF	Portable Document Format
PDS	Physical Delivery System
PEC	Posta Elettronica Certificata
PEGS	Pan-European e-Government Services
PEPPOL	Pan-European Public Procurement Online
PEPS	Pan-European Proxy Service
PGP	Pretty Good Privacy
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure Exchange

PoC	Point of Care
POO	Proof of Origin
POP3	Post Office Protol v3
POR	Proof of Receipt
PReM	Postal Registered eMail
PRESTO	Protocole d'Echanges Standard et Ouvert
PSC	Point of Single Contact
QAA	Quality Authentication Assurance
QC	Qualified Certificate
QES	Qualified Electronic Signature
RASP	Reliable Asynchronous Secure Profile
REM	Registered Electronic Mail
REM-MD	REM Management Domain
R-MSRI	Recipient Message Store Retrieval Interface
RP	Reception Point
RRR	Return Receipt Requested
S-PEPS	Service Provider PEPS
SAFE	Secure Attached File Encryption
SAML	Security Assertion Markup Language
SDK	Software Development Kit
SE	Software Engineering
SePS	Secure electronic Postal Services
SEPA	Single Euro Payment Area
SLA	Service Level Agreement
SME	Small and Medium-sized Enterprises
S/MIME	Secure / Multipurpose Internet Mail Extensions
SMS	Short Message Service
S-MSI	Sender Message Submission Interface
S-MSRI	Sender Message Store Retrieval Interface
SMTP	Simple Mail Transfer Protocol
SOA	Service Oriented Architecture

SOAP	Simple Object Access Protocol
sourcePIN	Source Personal Identification Number
SP	Signature Provider
SPOCS	Simple Procedures Online for Cross-border Services
SPRA	SourcePIN Register Authority
SSCD	Secure Signature Creation Device
ssPIN	Sector Specific Personal Identification Number
SSL	Secure Sockets Layer
START	Secure Trusted Asynchronous Reliable Transport
STF	Specialist Task Force
STORK	Secure Identity Across Borders Linked
STS	Security Token Service
SwA	SOAP Messages with Attachments
TAN	Transaction Number
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TP-ERI	Third Party Evidence Retrieval Interface
TSA	Time-Stamping Authority
TSL	Trust-service Status List
TTP	Trusted Third Party
UA	User Agent
UBL	Universal Business Language
UML	Unified Modeling Language
UN/CEFACT	United Nations Centre for Trade Facilitation and Electronic Business
UPU	Universal Postal Union
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
URN	Uniform Resource Name
US	United States
USPS	United States Postal Service
UTF	UCS Transformation Format

VAL	Virtual Access Layer
V-IDP	Virtual Identity Provider
VCD	Virtual Company Dossier
VPN	Virtual Private Network
VoIP	Voice over IP
WLAN	Wireless Local Area Network
WOT	Web of Trust
WP	Work Package
WS	Web Services
WSDL	Web Services Description Language
WS-Addressing	Web Services Addressing
WS-Federation	Web Services Federation Language
WS-ReliableMessaging	Web Services Reliable Messaging
WS-Security	Web Services Security
WS-Transfer	Web Services Transfer
WS-Trust	Web Services Trust Language
XAdES	XML Advanced Electronic Signature
XKMS	XML Key Management Specification
XML	Extensible Markup Language
XMLDSig	XML Digital Signature
XOP	XML-binary Optimized Packaging
XSLT	Extensible Stylesheet Language Transformations

Chapter 1

Introduction

> *" Beginning is not only a kind of action. It is also a frame of mind, a kind of work, an attitude, a consciousness. "*
>
> [Edward Said, Literary Theorist, 1935–2003]

Communication in human interaction is a key activity with the aim to exchange information. The Oxford Dictionary[1] defines communication as "*[. . .] the imparting or exchanging of information by speaking, writing, or using some other medium [. . .]*". Communication can be seen as a human interaction where a sender exchanges information with a recipient. The communication is called synchronous if both sender and recipient are present at the same time (not necessarily at the same location). If the recipient responds or receives the information at a later point in time, the communication is called asynchronous. Postal mail delivery is one of the oldest forms of asynchronous communications. Postal systems date back to the invention of writing (2400 BC) where written documents by Pharaohs were delivered using a courier service [Wikipedia, 2011a].

Traditional mail has a long history. Postal systems have improved their services and offered more and more additional services over time. This also includes security services like certified mail delivery. With the increasing use of modern communication technologies, particularly Internet Electronic Mail (e-mail), traditional postal services including certified mail are continuously going to be shifted to the electronic world. This thesis treats Certified Electronic Mail (CEM) as an Information Technology (IT) security and Electronic Government (e-Government) discipline. The remainder of this chapter discusses the motives behind this thesis, the resulting concept and its underlying methodology.

1.1 Motivation and Problem

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 delivery.

Nowadays, more and more people are using electronic means to communicate with each other. However, standard communication systems like Internet 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 Secure / Multipurpose Internet Mail Extensions (S/MIME) or Pretty Good

[1] `http://oxforddictionaries.com/definition/communication`

Privacy (PGP) 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 with several Internet e-mail security service extensions. 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 the 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 traditional registered or certified mail do in the postal world. The terms Certified Electronic Mail (CEM) or Certified Mail System (CMS) are used when applying fair non-repudiation protocols in the context of electronic mailing systems, for example Internet e-mail. CEM is a quite young research field starting in the early 1990s. Due to an increasing demand in the public and private sectors, various CMS have been put into operation in the last decade by governments, postal operators and private businesses. Popular examples of governmental systems are the Italian Posta Elettronica Certificata (PEC), the Austrian Document Delivery System (DDS) for the public sector and the German De-Mail system. Particularly the justice sector relies on the secure and evidential document delivery and started to introduce such systems several years ago with the Austrian Electronic Legal Communications (ERV) and the German Elektronisches Gerichts- und Verwaltungspostfach (EGVP). In the private sector mainly postal operators, which are continuously shifting their postal services to the electronic world, have identified a gap in the market and provide certified electronic mailing as value-added service. The Belgian CertiPost, the German E-Postbrief, the Swiss IncaMail or the Slovenian moja.posta.si system are popular representatives of European postal operator systems. CMS are also largely deployed within enterprises, for internal communications or 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 particular user groups. In order to address a particular recipient, senders have to be registered with the same system. It is currently not possible to send certified electronic mailings from one system to another. 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 single 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 the European Single Market[2]. This circumstance has led the European community to enact the Directive on services in the internal market [The Council of the European Union, 2006a]. The so-called Services Directive was approved on 12 December 2006 and is a European Union (EU) law with the aim to increase the growth potential within the EU by removing legal and administrative barriers for businesses when they want to provide services abroad. One of the main objectives of the Services Directive is to establish interoperability across services of different EU Member States towards a European Administrative Space (EAS), so that citizens and businesses can use domestic e-Government infrastructures abroad. This also includes CMS infrastructures. A typical CMS scenario in the context of the Services Directive would be an Italian pizza baker who wants to establish a new business in the city of Vienna. The formalities shall be carried out electronically. In is assumed that the Italian citizen has already registered a mailbox in the own national CMS, the PEC system. After having processed the application of the Italian citizen, Austrian public agencies may need to send the final official notification by means of certified electronic mail. In this case the Services Directive asks for interoperability between the Austrian DDS and the Italian PEC, so

[2]The Single Market is often also referred to as Internal Market. More information about the Single Market can be found at the Web site of the European Commission, see http://ec.europa.eu/internal_market/index_en.htm.

that Austrian public agencies can deliver documents from the domestic DDS to the Italian citizen's PEC mailbox.

Even if the scenario described above is a desired state, it cannot be realized due to a missing interoperability basis. 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 and CMS communications, both research and practice lack solutions how to make existing systems interoperable. This thesis presents a concept, which fills this gap by proposing a CMS interoperability framework being able to couple arbitrary CMS. The concept has been developed by the author of this thesis in the course of the two European Large Scale Pilots (LSPs) Secure Identity Across Borders Linked (STORK)[3] and Simple Procedures Online for Cross-border Services (SPOCS)[4]. Both LSPs are also going to be discussed later in this thesis.

1.2 Concept

This thesis introduces and presents a multilevel CMS interoperability concept. The interoperability *Level 1* concept allows users to access foreign CMS with their domestic authentication and identification credentials. This is achieved with the STORK cross-border authentication framework for the mutual recognition of eIDs. However, this means that users still need to deal with multiple and (foreign) mailboxes. Like accustomed to e-mail, people may want to have one single mailbox for global certified electronic mailing. This is where interoperability *Level 2* comes into play. The interoperability *Level 2* concept is able to couple arbitrary CMS (and even other communication systems). The concept incorporates best practice by relying on the interoperability design principles of the European Interoperability Framework (EIF) and by building upon the architecture of Pan-European e-Government Services (PEGS). 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. Legal interoperability is still a missing piece and requires a political driver. This kind of interoperability is not directly covered by the concept presented in this thesis, but nevertheless discussed as well.

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 a harmonized protocol, which is a kind of "lingua franca". This protocol represents a metadata layer, which is able to map all CMS protocols to a unified meta protocol on a technical and semantic layer. Alignment of different CMS procedures is implemented directly in each gateway's business logic. By using Web services technologies, different CMS can thus communicate with each other through their gateways using this harmonized protocol. Besides communicational interoperability, trust establishment between different CMS is another important aspect for a CMS interoperability concept. Entities of one system have to implicitly trust entities of other CMS when sending messages across different CMS. The concept proposed in this thesis uses a trust mechanism based on the ETSI Trust-service Status List (TSL) standard.

The main concept has been developed by the author of this thesis in the course of the STORK Electronic Delivery (e-Delivery) pilot[5] and has been improved in WP3 of the LSP SPOCS[6].

[3] STORK is a European Commission (EC) co-financed Type-A project with the aim to develop an interoperability framework for cross-border authentication and Electronic Identity (eID) recognition. One STORK Work Package (WP) deals with CEM. For more details, see `https://www.eid-stork.eu`.

[4] SPOCS supports the implementation of the Services Directive and aims to provide seamless electronic procedures by building cross-border interoperability based on existing systems and solutions. One WP deals with interoperable CMS infrastructures. For more details, see `http://www.eu-spocs.eu`.

[5] The author of this thesis was leading the STORK e-Delivery pilot from July 2010 to June 2011.

[6] The author of this thesis has largely contributed to this process.

1.3 Methodology

The development, implementation and evaluation of the CMS interoperability framework presented in this thesis follows a well-defined methodology, which is segmented into concrete chapters. Therefore, this thesis has been structured as follows: Chapter 2 gives a brief overview of the topic of registered and certified mail in traditional postal systems. This helps to understand the basic mechanisms and principles behind these security services. The aspect of hybrid mail is introduced in this chapter as well. Hybrid mail is a first step incorporating modern communication technologies into traditional mail delivery. Nevertheless, in many parts of our everyday life electronic communication technologies have already replaced paper-based communications. Internet e-mail is a popular example. Equally to traditional postal mail delivery, there is a need for a fair and evidential document exchange for electronic communications as well. Since standard communication systems like Internet e-mail do not have this degree of evidential quality, the research community is working on CEM protocols since two decades. Therefore, Chapter 3 introduces and reviews the CEM scientific background. By drawing on the literature, CEM security properties are classified and reviewed according to their practical relevance. This helps to classify and review existing CMS, which are currently deployed on the Internet. Even if CEM research already exists since the early 1990s, only in the last decade governments, postal operators and private businesses have started to put CMS into operation on the Internet. Since this thesis proposes an interoperability framework for such systems, Chapter 4 reviews many existing CMS by drawing on the CEM security properties discussed in Chapter 3 and by classifying major systems according to practical CEM properties. Such an assessment and classification is vital for the development of a CMS interoperability framework. All the reviewed CMS are closed and standalone systems and are not interoperable with each other. Chapter 5 discusses the motives behind this thesis and the need for interoperable CMS, particularly against the background of recent developments like the Digital Single Market in the European Community. The development of a an appropriate CMS interoperability framework is not a straightforward task. Chapter 6 thus makes an analysis to identify essential requirements, which a prospective interoperability framework has to fulfill. The chapter also discusses challenges, which have to be tackled when developing such a framework. The discussion in this chapter draws on the interoperability groundwork of Chapter 5 and on the CEM security properties reviewed in Chapter 3. The concept proposed by this thesis is presented in Chapter 7. It introduces and discusses step-by-step the main architectural model starting from an abstract viewpoint to a more detailed view. Chapter 8 continues to introduce the process model of the interoperability framework. Both Chapter 7 and 8 present and discuss the interoperability framework, which has been developed by the author of this thesis in the course of the STORK e-Delivery pilot. Several improvements of this concept have been made in the course of the LSP SPOCS. These improvements are discussed in detail in Chapter 9. Chapter 10 highlights selected details of the implementation of this framework made in SPOCS. The focus thereby is on the implementation of a gateway for the Austrian DDS, which has been developed by the author of this thesis during the SPOCS project. Besides cross-border CMS interoperability, the STORK e-Delivery pilot has demonstrated authentication and identification interoperability in different national CMS. Chapter 11 gives a brief overview of this kind of interoperability[7]. The CMS interoperability framework is evaluated according to requirements compliance, testing, governance structure, standardization impact and legal context in Chapter 12. Finally, conclusions are drawn.

[7] As STORK e-Delivery pilot leader the author has supervised the integration of the STORK interoperability framework in selected CMS.

Chapter 2

Traditional Certified Mail

"Trust opens up new and unimagined possibilities."

[Robert C. Solomon, Professor of Continental Philosophy , 1942–2007.]

Certified electronic mailing has adopted many aspects from traditional postal registered and certified mail. This chapter thus introduces the basic principles and security concepts of traditional certified mail. Most people have already come across postal registered mail at some time in their life. *Registered Mail* is an adequate and useful vehicle in the postal world to send important documents in a reliable and evidential way. Postal services and the handling procedures that they use provide value-added service, such as extended tracking possibilities and evidence of having sent a particular delivery at a certain point in time. Depending on the country and postal service several other value-added security services are offered. These services range from delivery confirmations to signature confirmations and return receipts and are discussed in detail in the first part of this chapter. A postal service offering one of these confirmations or receipts is usually called *Certified Mail*. Since registered and certified mail have a long history, the first part also briefly describes the evolution of these services over time as well as the characteristics of these services provided by postal services nowadays. This chapter concludes with a discussion on hybrid certified mail services, the link between the postal and the electronic world.

The remainder of this chapter is structured as follows. Section 2.1 introduces the main idea behind registered mail. However, registered mail is just one basic value-added service. Postal services offer some more security services to meet customer needs. They cover insurance, proof of delivery as well as restricted delivery to a particular circle of recipients. Section 2.2 discusses each of them in detail. Registered mail services have a long history and Section 2.3 exemplarily describes the evolution of registered mail in Germany and the United States (US) over the last centuries. The state of play of mail security services of four major postal services is briefly introduced in Section 2.4. This overview illustrates that although services are called and used differently in each country, the underlying security principles are the same. In the last years postal services are reaping the benefits of Information and Communication Technologies (ICT) and are continuously replacing parts of their delivery processes by electronic means. This particularly affects the submission of mail items and is called *Hybrid Mail*. Section 2.5 discusses the benefits of hybrid registered and certified mail.

2.1 Introduction

Since centuries, regular mail is used to deliver documents, letters, postcards, parcels or other postal items to their designated recipients. The actual delivery is usually conducted by postal services like the United States Postal Service (USPS), Canada Post, Deutsche Post AG, etc. With regular mail, senders hand their delivery item over to the postal service assuming that it will be correctly delivered to the designated

recipient. If recipients do not provide any feedback, the sender will never know whether the item has actually been delivered or not. Therefore, regular mail is basically a matter of trust in postal services' processes. Senders act on the assumption that their item:

- is actually delivered
- is delivered to the designated recipient (or to relatives or neighbors in case of absence)
- is not opened, read or inspected by any intermediary (except for example by the customs control)
- does not suffer any physical damage
- does not get lost and
- does not get stolen

In the majority of cases regular mail meets these assumptions. However, postal services do not guarantee that. For example the sender will not receive any compensation if mail gets lost. The same may apply to any damages. In this case the sender may have the burden of proof and show that the item was not damaged in any way before delivery. For standard items with no particular value people usually accept the risks of loss, theft, damage or delivery to wrong recipients. However, when sending sensitive documents or valuable or irreplaceable items, there may be the need for higher safety and security. Examples of valuable delivery items are tax returns for the internal revenue service, issued passports being submitted to their holders, contracts and deeds, summons or subpoenas to appear before court, jewelry, paychecks or money. For this purpose many postal services offer value-added services with a higher security. Depending on the postal service, these services are referred to as *Registered Mail*, *Registered Post*, *Secure Delivery* or *Certified Mail*. Even if being based on different legislations, provided under different terms and conditions and called differently, they all share the feature of an extended delivery process tracking. Tracking means that the delivery item is recorded by the postal service in a registry. The term "Registered mail" has been derived therefrom.

Registered mail items get a unique tracking or routing number when being recorded the first time. The format of this tracking number is specified by the UPU according to the S10c-5 data definition and encoding standards "Identification of postal items - Part C: 13 character identifier for special letter products" [UPU, 1996]. Examples of fictive tracking numbers could be as follows:

- RR 123 45678 9 US
- RO 123 45678 9 AT
- RR 123 45678 9 DE

The tracking number has four main parts. The first two characters denote the service indicator. For example, RO means "rush order". That follows an eight-digit serial number to be chosen by the postal service. The UPU recommends the inclusion of a check digit to ease the detection of errors in the code. The last two characters denote the ISO-3166-1 [ISO, 2006] country code. The 13-digit tracking number is usually accompanied by a bar-code, which is put as label on the delivery for automated processing. Tracking is not the only registered mail feature. Senders usually get a kind of receipt (so-called proof of submission). This receipt is issued by the postal service and contains the tracking number so that senders may contact the postal service to determine the current location of the delivery. This is possible because at each point on the delivery route the delivery status is recorded and updated in the tracking database.

2.2 Mail Security Services

The properties and basic processes of registered mail are pretty similar in most countries. Depending on legal regulations or general terms and conditions, registered mail may have different flavors and offer additional security services. Basically these are the mail security services of insurance, delivery confirmation, signature confirmation, collect on delivery, restricted delivery and return receipt.

- ***Insurance***: in case of valuable or irreplaceable items like jewelry, money or security papers, the registered mail delivery may be insured. The additional price of this service usually depends on the value of the insured item. Such mail is often transmitted sealed in a security box to prevent unwarranted access and on its route to the recipient the item is continuously monitored.

- ***Delivery Confirmation***. The delivery confirmation service is a receipt to document the final delivery step. It usually contains the date, time and address of delivery. The confirmation has a reference to the tracking number to be able to match it with the corresponding mail item. Not just the successful delivery is documented. Even in case of failed delivery attempts it is generated, for example if the address does not exist. It must be noted that the delivery confirmation only documents the delivery to a given address. It is not evident if the item has been dropped into the recipient's mailbox or if it has been personally handed over to the recipient. This is covered by the *Signature Confirmation* security service described below.

- ***Signature Confirmation***. In contrast to a delivery confirmation, a signature confirmation documents and attests the handover of the delivery to the final recipient. The process is usually as follows. The sender fills out a form by inserting the sender's and the recipient's address data and eventually some other necessary information. This form is delivered together with the mail item to the recipient. The recipient has to sign the form before actually receiving the mail item. Like a delivery confirmation, a signature confirmation is also recorded in the registry of the postal service. If the recipient is absent, for example because of illness or due to vacation or an in-existing address, a negative signature confirmation is generated.

  It has to be noted that in most cases a signature confirmation only attests that a postal employee handed an envelope over to the recipient. This confirmation is not anyhow related to the actual content of the mail item. This is reasoned by the security principle of secrecy of correspondence, which is part of the constitution of several European countries and guarantees that the content of a delivery is not revealed to any intermediary on the delivery route. In case of a signature confirmation covering the mail content, postal employees would have to witness the hand over the content. This would violate the secrecy of correspondence.

- ***Collect on Delivery***. The collect on delivery service is a special security service where postal service employees collect the payment and postage of an item upon delivery. It is often provided in conjunction with the signature confirmation service.

- ***Restricted Delivery***. Usually postal employees must not deliver the mail item to the person imprinted on the letter cover. They may also hand it over to a relative being present or a neighbor. However, there may be cases where only particular persons or delegates on behalf of these persons should be allowed to receive a delivery. There may even be cases where only the recipient and no other person, not even a delegate must receive the delivery. Especially in the justice sector this is a frequent requirement. The personal delivery of subpoenas is a typical example. Consider the case where father and son have the same given name and family name and are living in the same household. They can basically just be distinguished by their date of birth. It is important that the right person receives the subpoena to appear before court. Another example is the delivery of documents in divorce proceedings to married people still living in the same household. It is crucial that the right person receives the mail and that this circumstance is appropriately documented. The

requirement of qualified identification for recipients is taken into account by the restricted delivery service. With this service senders can restrict the circle of people being allowed to pick up a delivery. Postal services usually offer two basic restricted delivery services. The first allows both the recipient and an authorized delegate to sign for and receive a delivery. The second allows just the recipient to receive the delivery.

Since postal employees must verify the recipient's identity, this service is often used by postal services to provide additional value-added services. For example, the German Post offers a service called "Postident", which verifies and documents the recipient's identity by a postal service employee. In this way people can for example enter a subscription-based mobile phone contract without ever having been in a mobile shop.

- ***Return Receipt***. Both the delivery and signature confirmation services are recorded into internal postal service databases. By this means the information has no transferable evidential value. This means that if a dispute arises because a recipient denies of having received an item, the sender or a court is forced to involve and consult the postal service as Trusted Third Party (TTP) to retrieve and release the necessary information from the database. The return receipt service provides the sender the signed confirmation including all related data so that it can be retained by the sender as evidence of a successful or failed delivery attempt.

So far only the term *Registered Mail* has been used and several additional services covering different security aspects have been introduced. Postal services offer the registered mail service in conjunction with a variety of these additional security services. For example, the USPS call their combination of registered mail with a signature confirmation as *Certified Mail*. The service is provided with or without return receipt. In the latter case it is called Return Receipt Requested (RRR). In order to simplify the usage of terms, for the remainder of this thesis the term *Registered Mail* is used if a service provides just a proof of submission and the term *Certified Mail* if a service additionally provides either a delivery confirmation, a signature confirmation or a return receipt.

2.3 A Brief History of Registered and Certified Mail

Registered mail has a long history and its security services evolved over time. A first reference dates back to the reign of Mary Tudor. According to Joyce [1893, page 234], an Order in Council from 1556 had ordained:

> *"[...] that the poste between this and the Northe should eche of them keepe a booke and entrye of every letter that he shall receive, the tyme of the deliverie thereof unto his hands with the parties names that shall bring it unto him, whose handes he shall also take to his booke, witnessing the same note to be trewe."*

In 1841 Great Britain introduced registered mail as it is known today. A green sheet (later replaced by blue crossed lines) was sent along with the registered mail item to the recipient's post office. This sheet served as receipt and was returned to the sender's post office. Great Britain was not the only territory having registered mail at that time. For example, the German *Affidavit of Service* was introduced quite early and is still used today. The same applies to the USPS registered mail service. This section exemplarily describes the evolution of both services from its beginning down to the present day.

2.3.1 Germany

This section gives an overview of the chronological development of the German certified mail service called *Zustellungsurkunde* (Affidavit of Service) as described in [Wikipedia, 2011b]. The affidavit of

service is defined by the Code of Civil Procedure (CCP) [Bundesrepublik Deutschland, 2005] as a means to provide evidence of delivery. Today the service is offered by the German Post and is also provided by several private companies since the deregulation of the postal market in 1997. The service can only be used by public bodies and according to the CCP evidences must be issued by postal services to document and attest a successful or failed delivery attempt.

- **1793**. The concept of the affidavit of service dates back to 1793 where Prussian states' letters could already be sent with "acknowledgment of receipt". Courts received a "receipt" in terms of a delivery confirmation, which had to be signed by mailmen to document a successful or failed delivery attempt.
- **1869**. The service was renamed to "Schreiben mit Behändigungsschein".
- **1871**. The service was opened to private individuals. The *Deutsche Reichspost* (name of the German Post at that time) charged twice the standard postage rate for this service. Registered mail was available, but in this case the delivery could only be handed over to the recipient or an authorized delegate.
- **1872**. An additional "delivery fee" was introduced. Now the postal service charged twice the standard postage rate plus this "delivery fee". The additional fee was twice as much for private individuals than for courts.
- **1879**. The service was renamed from "Schreiben mit Behändigungsschein" to "Briefe mit Zustellungsurkunde" (letters with affidavit of service). From now on no more differentiation was made between courts and private customers. However, the service was now available in two different qualities. With the standard quality the recipient got a copy of the delivery confirmation. The simple quality just documented the delivery date on the confirmation.
- **1900**. Registered mail was now detached from the affidavit of service and people could use it now also in private matters.
- **1963**. Changes in the CCP had several consequences on the delivery process. Up to that point in time an affidavit of service delivery was sent just like a standard letter. From now on a delivery with affidavit of service had to contain the item itself plus an additional form sheet.

2.3.2 United States

Since its founding in 1775 by Benjamin Franklin, the USPS made a rapid progress in establishing new (security) services for its customers.

- **1855**. On 3rd March 1885 the U.S. Congress authorized the *Registered Mail* service. According to John [1998, page 78], the general post office only introduced a rudimentary registered mail service with postage prepayment. It was announced as great innovation, but only offered an account checking and no insurance for any lost money. The practicability of the service was doubted and even 20 years later most people were not aware of its existence. However, the establishment of new additional security services was rapidly growing in the following years, as an article documenting the USPS American history [USPS, 2006] reports.
- **1863**. Introduction of uniform postage rates, regardless of the distance.
- **1864**. Creation of the postal money order system.
- **1869**. International money orders.

- **1885**. Introduction of the *Special Delivery* service, which is the expedited delivery of items for an additional fee.
- **1911**. Start of the postal savings system.
- **1913**. Introduction of the *Collect on Delivery* service.
- **1955**. The *Certified Mail* service based on the idea of U.S. postmaster General Joseph Cooper was introduced.

2.4 Examples of Selected Certified Mail Services

The registered and certified mail security services have not evolved uniformly across the world. Over the last centuries, each country and each postal service has introduced its own registered or certified mail services tailored to particular national needs. Nevertheless, their rendered services are basically a combination of the security services introduced above (cf. Section 2.2). To illustrate this, this section gives a brief overview of selected registered and certified mail services from different countries, how they are called and what security services they provide.

2.4.1 United States - USPS

The USPS[1] is the U.S. government-owned universal postal service and responsible for serving all U.S. citizens. The USPS provides the following security services:

- ***Registered Mail*** provides by default the security services insurance, proof of submission and delivery confirmation. The service can optionally be combined with the security services of signature confirmation, collect on delivery, return receipt and restricted delivery.
- ***Certified Mail*** provides by default the same security services as *Registered Mail* and additionally provides a signature confirmation. The certified mail service can be combined with the security services of return receipt and restricted delivery.

2.4.2 United Kingdom

Royal Mail[2] is the U.K. government-owned universal postal service and provides the following security services:

- ***First and Second Class Mail*** guarantee that items are delivered the next day (first class) or the third day (second class) after submission. Both services provide a proof of submission, which is called *Certificate of Posting*.
- ***Special Delivery*** is intended for urgent and valuable items to be delivered within a certain timeframe. Besides insurance a signature confirmation (called *Electronic Proof of Delivery*) is also provided.
- ***Sameday*** guarantees delivery of urgent items on the same day. Besides insurance, it provides a delivery confirmation returned by e-mail.

[1] http://www.usps.com
[2] http://www.royalmail.com

- ***Royal Mail Tracked Services*** allows the detailed tracking of items and provides a delivery confirmation either by e-mail or Short Message Service (SMS) and, additionally, a signature confirmation (*Electronic Proof of Delivery*).
- ***Recorded Signed For*** is the highest Royal Mail security service and provides insurance, proof of submission, delivery confirmation and a return receipt.

2.4.3 Austria - Österreichische Post

Österreichische Post AG[3] is the universal postal service serving all Austrian citizens. It offers several security services for both the private and public sectors. Private individuals can use the registered mail service *Einschreiben* with the security services of insurance and signature confirmation. It can be combined with return receipt, restricted delivery and collect on delivery.

Public agencies and courts use special services that are regulated by the *Service of Documents Act* [Republik Österreich, 1982][4]. This law defines the following two certified mail services:

- ***RSa-Brief***. An "RSa" letter is sent as certified mail with the security services of return receipt and restricted delivery. Senders can choose between two restricted delivery options. With the "normal" option both the recipient or an authorized delegate can pick up the delivery. The option "Nicht an Postbevollmächtigte" allows just the recipient to pick up the delivery. In both cases the receiving person must sign a return receipt for the sender.
- ***RSb-Brief***. An "RSb" letter is almost identical to "RSa" but has no restricted delivery limitations.

2.4.4 Italy - Poste Italiane

Poste Italiane[5] is the government-owned universal postal service serving all Italian citizens and provides the following security services related to letters:

- ***Posta Raccomandata*** is a certified mail service providing a return receipt service plus optionally the collect on delivery service.
- ***Posta Raccomandata 1*** guarantees the service delivery of Posta Raccomandata within one working day and provides a further electronic signature confirmation.
- ***Posta Assicurata*** has the same security services as Posta Raccomandata but provides an additional insurance for the delivery item.

2.5 Hybrid Certified Mail and Electronic Security Services

The increasing penetration and use of ICT has led postal services and other private businesses to improve and offer value-added services for customers with the aim to increase efficiency and to reduce costs. Even if mail delivery is still dominant, parts of the delivery route, associated services and side products have been replaced by electronic means. First of all, this concerns the multi-channel delivery from the sender to the recipient. This kind of service is called *Hybrid Mail*. Hybrid mail is a Pre-Internet technology dating dating back to the 1970s.

McMillan [2001] gives an overview of hybrid mail and its benefits. The main concept is illustrated in Figure 2.1. Mail items are submitted by electronic means from senders to a multi-channel delivery hub.

[3] http://www.post.at

[4] The Service of Documents Act was last amended in 2010 with the law BGBl. I Nr. 111/2010.

[5] http://www.poste.it

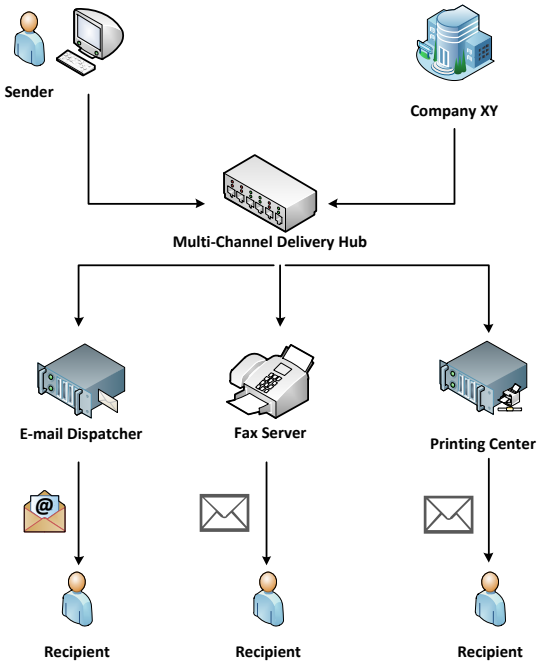

Figure 2.1: The concept of multi-channel or hybrid mail delivery.

According to the available address data the hub routes the delivery to an appropriate delivery channel. In case of an electronic address this could be an e-mail dispatcher forwarding the document to the recipient's e-mail account. Otherwise the item is forwarded to a fax server or a local printing center for regular mail delivery. Today hybrid mail is mainly offered as outsourced service. The benefits for both customers and hybrid mail providers are at hand as discussed by McMillan [2001]:

- ***Economy of time.*** Hybrid mail can usually be submitted anytime and is only one click away from the printing center. This reduces the time needed for driving to the post office or to a mailbox. The delivery time can thus be calculated more precisely.
- ***Economy of scale.*** Due to the high capacity of an outsourced service, hybrid mail providers can more effectively buy and employ necessary hardware like printers and envelopers.
- ***Load balancing.*** Peaks of multiple customers can be better balanced and more effectively used across the available hardware components.
- ***New technology.*** Since the expenses of new technologies are implicitly distributed over multiple customers, hybrid mail providers can usually purchase and adopt new technologies much earlier.
- ***Off-loading non-core activity.*** Customers can off-load printing and enveloping jobs to the hybrid mail provider and concentrate on their revenue-making tasks. Without outsourcing, efforts include hardware costs for printers and personnel costs for printing, enveloping, stamping and posting, assumed that the latter steps are carried out manually.
- ***Address verification.*** Hybrid mail providers can check the recipient's address prior to printing. Undeliverable mail may thus be returned to the sender to save costs.
- ***Distribution to regional hub.*** If the delivery is forwarded to a local printing center close to the recipient, the route of regular mail delivery is much shorter and helps to save transport and logistics costs. Hybrid mail has thus become important in countries that are too large for one-day delivery, for example Australia or Canada.

- CO_2 ***reduction.*** Hybrid mail saves transport costs and thus directly reduces the CO_2 footprint.

Hybrid mail is still mainly used by Small and Medium-sized Enterprisess (SMEs), public agencies or large enterprises like insurance companies to send invoices or marketing information. However, the hybrid mail market for private individuals is currently being conquered. Many service providers offer interfaces for senders to deliver electronic mail items by regular mail. They range from sophisticated interfaces for bulk mailings by business solutions to simple browser-based Graphical User Interfaces (GUIs) for private individuals. Last not least, hybrid mail has not only benefits. Especially from a data protection perspective it raises some issues. The secrecy of correspondence for regular mail is preserved by envelopes. Even when strong cryptographic technologies are applied, hybrid mail items are opened at the time when the media changes and the item is printed on paper.

With hybrid mail, postal services use ICT to improve the delivery process from the sender to the recipient. At the same time traditional security services are continuously replaced by electronic ones. This mainly concerns the evidential-based security services proof of submission, delivery confirmation, signature confirmation and return receipt. For example, the USPS *Return Receipt* service not only offers the receipt as green postcard. Senders may also get the receipt as scanned image in terms of a Portable Document Format (PDF) file by e-mail. This service is called *Return Receipt Electronic*. With the USPS *Delivery Confirmation* service customers can access the delivery confirmation online using the USPS *Track & Confirm* tool. In case of the *Signature Confirmation* service, customers can request to receive a copy of the recipient's signature by e-mail. The Royal Mail *Recorded Signed For* security service is also available online via their *Track & Trace* service. However, the USPS is not the only postal service shifting their paper-based security service to the electronic world. Similar services are provided by many other postal services on the world.

Although hybrid mail improves mail delivery by replacing parts of the regular mail process with electronic counterparts, they do not unleash the full potential of ICT. Electronic communications like e-mail are continuously replacing regular mail and registered or certified security services should thereby be taken into account and not fall by the wayside. The next chapter discusses the topic of CEM, the counterpart of traditional registered and certified mail security services in the electronic world.

Chapter 3

Certified Electronic Mail

"The new electronic independence re-creates the world in the image of a global village."

[Marshall McLuhan, Canadian Communications Theorist, 1911–1980.]

This section continues with the review of pure electronic certified mailing. A clear understanding of the concepts behind certified electronic mailing is vital to facilitate the design of a CMS interoperability framework. Since a couple of decades, ICT are continuously replacing paper-based communication and collaboration systems in our society. Particularly the increasing penetration of the Internet and mobile phones in our everyday's life contributes to that trend. Today we are accustomed to communicate via e-mail, social networks, SMS, Instant Messaging (IM), chats, Voice over IP (VoIP), microblogs and other modern communication media. Even if these means are pretty convenient and easy to use, they have a poor evidential quality. For example, the sender of an e-mail does not know whether the recipient has received or even read a message, as long as there is no feedback. A malicious recipient could simply claim of not having received the message. Equally a sender could claim of not having sent the message. Pure e-mail without any additional measures has no security provisions. It can be compared to sending a postcard, which lacks confidentiality, authenticity, integrity and non-repudiation services. Even though several security extensions enhance e-mail with confidentiality, authenticity and integrity, the lack of fair non-repudiation still remains. Usually a missing evidential communication is no problem at all, because it is assumed that most recipients are acting honestly. Nevertheless, the need for certified mail and its security services not only concerns regular mail, but electronic communications as well. Particularly in advanced business and governmental communication scenarios it is a desired feature. For example, consider public agencies sending subpoenas and other important official notifications or businesses sending bids, deeds or contracts using electronic communication means. They still want to enjoy the benefits, quality and security services of traditional postal certified mail delivery.

This section investigates the evolution, security services and properties of Certified Electronic Mail (CEM). First an overview of the general electronic mail handling architecture and model is given. This model is based on X.400 [ITU-T, 1988]. X.400 has never enjoyed the popularity of Internet e-mail, but is still used to some extent in Europe, South America and Asia, particularly for Electronic Data Interchange (EDI) services. X.400 defines the generic system architecture of Message Handling Systems (MHSs) and its generic architectural model can be used to describe many existing mailing systems, including Internet e-mail. Besides a brief overview of the X.400 model, common terms are introduced to serve as a basis for discussing attempts to evidential e-mail and subsequently for introducing the security services and properties of CEM. Several Internet Engineering Task Force (IETF) standards tracks have been published with the aim to extend the e-mail Simple Mail Transfer Protocol (SMTP) protocol with the evidential quality of certified mail. These approaches are discussed in detail in Section 3.2. Even if these services are a nice added value and are often used in today's e-mail conversations, from a security point of view the evidential value is still missing. Therefore, since two decades the research community

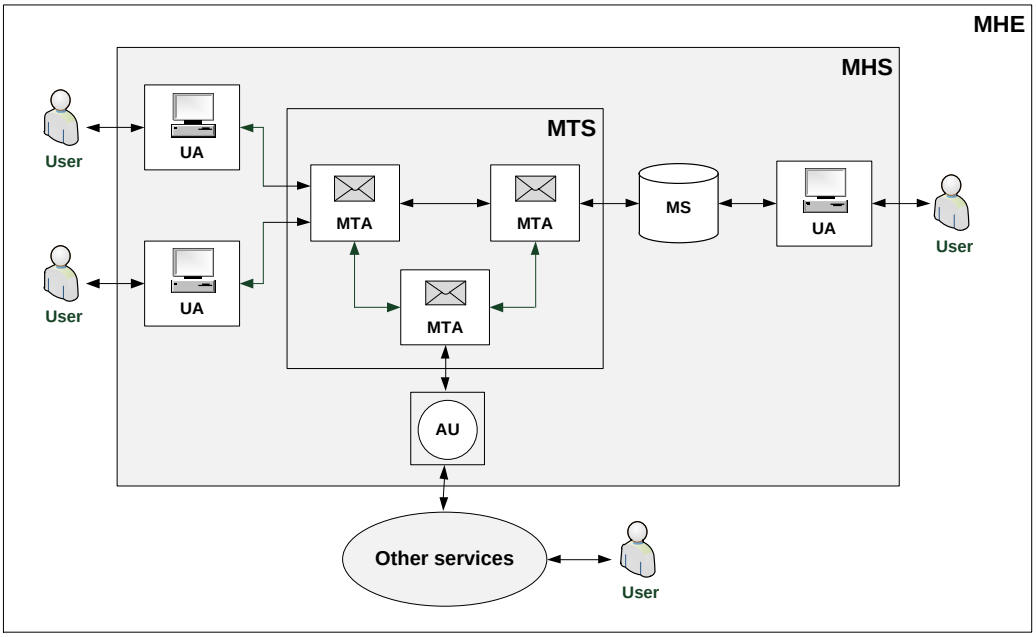

Figure 3.1: System architecture of the generic X.400 MHS

is continuously working on and publishing new security protocols meeting the requirement of fair non-repudiation. Interestingly the research community has no common view on what security properties a CEM protocol has to provide. In the course of years the community published a large number of protocols with security properties having different flavors. These properties and their evolution in research are discussed in Section 3.3. This thesis focuses on actually deployed systems, particularly on the Internet. Therefore, each property is discussed in detail with respect to its practical relevance.

3.1 General Mail Handling Model

Published in 1984 and revised in 1988, X.400 [ITU-T, 1988] is a suite of recommendations by the standardization sector Comité Consultatif International Téléphonique et Télégraphique (CCITT) of the Internet Telecommunication Union (ITU) for MHS in data networks and open systems communications. The CCITT was renamed in 1993 to ITU Telecommunication Standardization Sector (ITU-T). The ITU-T is in charge of elaborating all kinds of norms, standards and recommendations in the field of telecommunication on international level. The International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) has standardized X.400 as "ISO/IEC 10021-1 - Information technology – Message Handling Systems (MHS) – Part 1: System and Service Overview" [ISO/IEC, 2003a], published in 1999 and last revised in 2003. ISO/IEC 10021, which is also called Message Oriented Text Interchange System (MOTIS), consists of 11 parts, each of them standardizing different MHS aspects.

3.1.1 Architecture and Functional Model

The recommendations X.400 and X.402 "Message Handling Systems: Overall Architecture" [ITU-T, 1999a] (see also [ISO/IEC, 2003b]) specify the overall architecture and functional model of the generic X.400 MHS as illustrated in Figure 3.1. X.400 defines an architectural model with three main layers. The Message Handling Environment (MHE) is the outermost layer and describes the concept of message

handling with the primary objects of users (persons or computers) and the MHS. The MHS is a functional means of conveying messages (information objects) from a user to another user or a group of users (distribution list). The recommendation defines two types of users: direct and indirect users. A direct user is directly communicating with the MHS, an indirect user is connected through another communication system to the MHS, for example through regular mail delivery.

The MHS is the second layer of the X.400 architectural model and defines the following objects:

- ***User Agents***. Users can either act as sender (denoted as originator in X.400 terminology) when submitting messages or as recipient when receiving messages. Senders prepare and submit messages with a User Agent (UA), which is an application to process and transmit messages between the user and the Message Transfer System (MTS) or a Message Store (MS). The MTS can either deliver messages directly to the recipient's UA or the user can make use of the MS functionality to retrieve delivered messages with the UA at a later point in time. The UA may also have notification provisions for the sender and is usually tailored to an application-specific messaging context. X.400 does not restrict the number of allowed UAs.

- ***Message Transfer System***. The MTS is a store-and forward system and the backbone of the MHS. This means the MTS consists of one or more Message Transfer Agents (MTAs), accepts messages from a sender's UA and delivers messages to the recipient's UA, an Access Unit (AU) or a MS. The MTS concept is specified in detail in ITU-T [1999b].

- ***Message Stores***. A MS is an infrastructural component acting as intermediary between a user and an MTA. It provides storage of delivered or submitted messages for later retrieval by the user. Each MS is associated with a UA (for message retrieval), but not each UA must be associated with a MS, for example in case of submitting-only agents. The MS concept is specified in detail in ITU-T [1999c].

- ***Access Units***. An AU connects other communication systems (indirect users) to the MHS, for example regular mail delivery. AUs are usually no general-purpose docking modules, but rather connect dedicated external communication systems. X.400 defines the Physical Delivery Access Unit (PDAU), which converts electronic messages to physical ones (called physical rendition) and delivers the converted message to a Physical Delivery System (PDS), for example regular mail.

The MTS defines the third layer of the X.400 architectural model and only consists of MTAs, the single links in the store-and-forward chain of the MHS. The MTA is basically defined as general-purpose module to serve all kinds of communications. However, it could also serve concrete scenarios, for example to convert messages. X.400 does not restrict the number of MTAs within an MTS.

3.1.2 Messaging

X.400 messages consist of two parts: a transport envelope and the message content. The content is the actual information the sender wants to deliver to the recipient, for example a document. The envelope contains the control information for the MTS to correctly deliver the message from the sender's UA to the recipient's UA or MS. This control information consists of the sender's and recipient's address data and any necessary information provided by previous transmission hops on the delivery route.

X.400 defines three basic interactions between UAs, MSs, AUs and MTAs. In the so-called *submission interaction*, content and envelope are submitted by the sender's UA, MS or AU to the sender's MTA. The *transfer interaction* describes the transmission of a message (content plus envelope) between MTAs on the delivery route. The content remains unchanged by the MTS on its delivery route, whereas the envelope may be modified, for example to update routing information. An exception is the conversion or transformation of messages by MTAs. In this case also the content may be altered. The so-called *delivery*

Security services	Sender	MTS	Recipient
Message origin authentication	P	U	U
Report origin authentication	U	P	-
Proof of delivery	U	-	P
Proof of submission	U	P	-
Content integrity	P	-	U
Content confidentiality	P	-	U
Message flow confidentiality	P	-	-
Non-repudiation of origin	P	-	U
Non-repudiation of submission	U	P	-
Non-repudiation of delivery	U	-	P

P = The MHS component is a provider of the service
U = The MHS component is a user of the service

Table 3.1: X.400 security services related to certified mailing according to [ITU-T, 1988, page 25].

interaction denotes the process in which the final MTA delivers the message (content plus envelope) to the recipient's UA, MS or an AU for delivery to external communication systems.

In contrast to Internet e-mail, which uses the addressing format defined in RFC 5322 [Resnick, 2008], X.400 uses directory names as specified in the ITU-T X.500 series (see also ISO/IEC [2008]). For example, the SMTP-based e-mail address `john.doe@department.organization.us` is expressed in X.500 annotation as `G=John,S=Doe,OU=Department,O=Organization,C=US`. Both formats implement a hierarchical, unique and component-based addressing scheme. However, the attribute-based X.500 scheme is longer and harder to remember for people. This is probably also one of the reasons why X.400 has never reached the popularity of Internet e-mail.

3.1.3 Security Services

Since the distributed MTS concept has a segmented communication path between sender and recipient, X.400 provides several security features to reduce potential threats like:

- ***Access threats***. Unauthorized access by invalid users.
- ***Inter-message threats***. Masquerade, message modification, replay attacks, eavesdropping and traffic analysis.
- ***Intra-message threats***. Repudiation of messages and security level violation.
- ***Data-storage threats***. Modification of routing information and replay attacks.

A detailed discussion of these threats can be found in [ITU-T, 1988, page 24]. Even if X.400 has security measures to cover many of the above threats, this section only focuses on the measures related to certified mailing. Besides messages, X.400 support so-called *reports* to report the delivery or acceptance status of a message. However, these reports are basically not protected by any security measures and thus X.400 defines several security messaging elements. Table 3.1 lists the MHS security messaging elements related to the provision of certified mail services. They are defined as follows [ITU-T, 1999a, page 25]:

- ***Message origin authentication***. The Message Origin Authentication service enables the corroboration of the source of a message.

- ***Report origin authentication***. The Report Origin Authentication security service enables the corroboration of the source of a report.
- ***Proof of submission security service***. This security service enables the originator of a message to obtain corroboration that it has been received by the MTS for delivery to the originally specified recipient(s).
- ***Proof of delivery security service***. This security service enables the originator of a message to obtain corroboration that it has been delivered by the MTS to its intended recipient(s).
- ***Data Confidentiality security services***. These security services provide for the protection of data against unauthorized disclosure.
- ***Content Confidentiality security service***. The Content Confidentiality security service provides assurance that the content of a message is only known to the sender and recipient of a message.
- ***Data Integrity security services***. These security services are provided to counter active threats to the MHS.
- ***Content Integrity security service***. This security service provides for the integrity of the contents of a single message. This takes the form of enabling the determination of whether the message content has been modified.
- ***Non-Repudiation security services***. These security services provide irrevocable proof to a third party after the message has been submitted, sent, or delivered, that the submission, sending, or receipt did occur as claimed.
  - ***Non-Repudiation of Origin security service***. This security service provides the recipient(s) of a message with irrevocable proof of the origin of the message and its content.
  - ***Non-Repudiation of Submission security service***. This security service provides the originator of the message with irrevocable proof that the message was submitted to the MTS for delivery to the originally specified recipient(s).
  - ***Non-Repudiation of Delivery security service***. This security service provides the originator of the message with irrevocable proof that the message was delivered to its originally specified recipient(s).

3.2 Approaches to Secure and Reliable Electronic Mailing

Even if social networks and its communication features are used by more and more people, e-mail is still increasing in popularity and is the “de-facto” standard for all kinds of electronic communications. This includes communications from

- Administration to Administration (A2A)
- Administration to Business (A2B)
- Administration to Citizen (A2C)
- Business to Administration (B2A)
- Business to Business (B2B)
- Business to Citizen (B2C)
- Citizen to Administration (C2A)

- Citizen to Business (C2B)
- Citizen to Citizen (C2C)

The e-mail technology dates back to the early 1970s where it has been used for communications in the Advanced Research Projects Agency Network (ARPANET), a network funded by the Defense Advanced Research Projects Agency (DARPA) of the United States Department of Defense. At that time, e-mail messages were carried over the File Transfer Protocol (FTP). Later, when the ARPANET was replaced by the Internet Protocol Suite named TCP/IP (Transmission Control Protocol (TCP) and Internet Protocol (IP)), transferring e-mail over FTP was replaced by using the SMTP protocol [Postel, 1982] in 1982. By default, e-mail has no security provisions. This concerns both the basic security features of integrity, confidentiality, authenticity and accountability as well as the certified mail features ensuring an evidential document exchange. Section 3.2.1 first discusses the basic e-mail security protocols and mechanisms to ensure integrity, confidentiality and authenticity. Due to the lack of evidence, several receipting mechanisms have been proposed and are regularly used in e-mail communications. Section 3.2.2 discusses their basic functionality and explains why they do not have the evidential quality of certified mail.

3.2.1 Basic e-mail Security Mechanisms

The Internet community has addressed the lack of e-mail security with the S/MIME and OpenPGP standards. S/MIME is an IETF standard specified in RFC 5751 [Ramsdell and Turner, 2010] to send and receive secure Multipurpose Internet Mail Extensions (MIME) data. It supports two content types; one for digital signatures[1] and one for data encryption. S/MIME signatures ensure authenticity, data integrity and non-repudiation with proof of origin. An S/MIME signed message has two MIME parts: the first part holds the message content plus its MIME headers. The second part holds the signature itself plus any additional information to verify the signature. An S/MIME encrypted message has also two MIME parts. The first one holds the necessary information to decrypt the message. The second one holds the encrypted data. S/MIME operates on the Cryptographic Message Syntax standard [Housley, 2009] and makes use of X.509 certificates as defined in the IETF's Public Key Infrastructure Exchange (PKIX) and Certificate Revocation List (CRL) profile [Cooper et al., 2008].

An alternative to S/MIME is OpenPGP, which is a signature and encryption standard based on PGP and is specified in RFC 4880 [Callas et al., 2007]. It uses the PGP/MIME method for signature and encryption. PGP/MIME superseded the outdated PGP/INLINE method and allows for signing and encrypting all file attachments.

3.2.2 Receipting Mechanisms for e-mail

Even if e-mail security protocols like S/MIME or OpenPGP provide the basic security features of integrity, authenticity and confidentiality, lack of evidence still remains. Senders do not know whether the intended recipient has read or even received a message. This has been addressed by the Internet community with four receipting mechanisms, namely Message Disposition Notifications (MDNs), Delivery Status Notifications (DSNs), SMTP service extension for message tracking and S/MIME receipts. These mechanisms are introduced in the next sections. However, from a security perspective, they still cannot address the lack of evidence. This is subsequently discussed.

Message Disposition Notification

[1] The notions of digital and electronic signature are used synonymously throughout the remainder of this thesis.

MDNs are receipting or acknowledgment mechanisms for the e-mail protocol and are specified in RFC 3798 [Hansen and Vaudreuil, 2004] for the Post Office Protol v3 (POP3) and in RFC 5303 [Melnikov, 2003] for the Internet Message Access Protocol (IMAP). MDNs are requested by the sender by including a `Disposition-Notification-To` header in the message. The purpose of MDN is to report the final delivery status (success or failure) of messages. Most e-mail clients already implement the MDN mechanism. They usually provide several options to customize the acknowledgment behavior, for example "Ignore", "Ask", "Reject" and "Always Send" options. The recipient's client sends the MDN report back to sender using a MIME container message. This container has at least two parts: the first part contains a human-readable description of the report. The second part contains a machine-readable version for automated processing by e-mail clients. If the original message has to be returned along with the report, it can be included in the third MIME part.

MDN does not have any security provisions to ensure the integrity and authenticity of reports. Therefore, the Internet community has published a secure MDN mechanism known as *Applicability Statement (AS)*. MDN is used as basic receipting mechanism in the three AS standards, which specify the secure Peer-to-Peer (P2P) exchange of structured business data for EDI, Extensible Markup Language (XML) or other data. AS1 describes the transport using SMTP and is specified in RFC 3335 [Harding et al., 2002]. AS2 describes the Hypertext Transfer Protocol (HTTP) transport and is specified in RFC 4130 [Moberg and Drummond, 2005]. AS3 describes the FTP transport and is specified in RFC 4823 [Harding and Scott, 2007]. In contrast to the insecure MDN variant, AS requires the recipient's environment to provide an adapter for processing MDN requests before forwarding the message to the recipient's inbox. Furthermore, the returning MDN must be signed and must contain a hash value over the original message.

Delivery Status Notification

DSN is an SMTP service, which allows the sender or the sender's mail provider to request a report on the delivery status of a message. A DSN error report message is also called Non-Delivery Report (NDR) or *bounce message*. DSN success reports have to be explicitly requested by the sender, whereas DSN error reports are automatically returned to the sender. DSN is specified by the following conventions:

- ***RFC 3461*** - SMTP Service Extension for Delivery Status Notifications DSNs - see Moore [2003].
- ***RFC 3462*** - The Multipart/Report Content Type for the Reporting of Mail System Administrative Messages - see Vaudreuil [2003a].
- ***RFC 3463*** - Enhanced Mail System Status Codes - see Vaudreuil [2003b].
- ***RFC 3464*** - An Extensible Message Format for Delivery Status Notifications - see Moore and Vaudreuil [2003].
- ***RFC 5337*** - Internationalized Delivery Status and Disposition Notifications - see Newman and Melnikov [2008].

In contrast to the NDR, which is widely implemented as de-facto e-mail "bouncing" mechanism to report a failed delivery attempt, the functionality to request a success delivery status report is not supported and implemented by all mail servers.

SMTP Service Extension for Message Tracking

RFC 3888 [Hansen, 2004b] describes active and passive tracking mechanisms on the basis of DSN or MDN. These mechanisms are the standard way of tracking e-mail messages. However, MTAs may

not have implemented these standards or recipients may have MDN disabled. There may be cases where DSN or MDN do not provide any tracking information. In this particular case the IETF has published specifications for a last additional mechanism to determine the message status. The SMTP service extension for message tracking is specified by the following standards tracks:

- ***RFC 3885*** - SMTP Service Extension for Message Tracking (see Allman and Hansen [2004])
- ***RFC 3886*** - SMTP Service Extension for Message Tracking (see Allman [2004])
- ***RFC 3887*** - SMTP Service Extension for Message Tracking (see Hansen [2004a])

S/MIME Receipts

Another receipting standard are S/MIME-signed receipts as defined in RFC 2634 [Hoffman, 1999]. The standard aims to to provide the sender a proof of delivery and to demonstrate the sender that the recipient was able to verify the S/MIME signature of the original message. The concept of signed receipts is as follows:

1. The sender creates a signed S/MIME message, which includes an attribute indicating the request for a signed receipt. This is achieved by adding the `receiptRequest` attribute to the `signedAttributes` field of the S/MIME signature.
2. The sender submits the final message to the intended recipient(s).
3. The recipient receives the message, validates the signature and checks if there is any request for a signed receipt.
4. The recipient creates a signed receipt. A signed receipt is an Abstract Syntax Notation One (ASN.1) `signedData` object.
5. The recipient returns the signed receipt to the sender.
6. The sender receives the message and validates if it contains a signed receipt. This validation requires particular data of the original message. Therefore, the sender has to keep a copy of these data either by extracting it from the original message or by keeping the whole original message.

Security Considerations

The four mechanisms MDN, DSN, SMTP service extension for message tracking and S/MIME signed receipts have been briefly reviewed. Even if these mechanisms provide added value to the standard e-mail protocol, the evidential security level does not increase. No one can prevent the recipient from configuring the receiving environment in such a way that MDN, DSN, S/MIME receipt requests or SMTP tracking requests are completely ignored. All the discussed mechanisms act on the assumption of fairly acting infrastructural entities, meaning that all entities including the recipient actually return the expected receipt or status notification.

Furthermore, none of the mentioned mechanisms except S/MIME receipts employs any cryptographic technologies to ensure message tracking or receipting. Even if S/MIME ensures confidentiality, authenticity and integrity, it still lacks mechanisms to ensure the fair and non-repudiable exchange of a message for a receipt. Recipients can still deny having received the message.

According to Oppliger [2007] all of these tracking and receipting mechanisms are relatively new and SMTP already exists since 1982. The mechanisms require infrastructural changes and this means they

have to be deployed along the message delivery path. For example, MTAs need to be updated to process DSNs and UAs are required to understand MDN requests. Even if all infrastructural components would be able to process the mentioned mechanisms, the open and heterogeneous nature of the Internet and the lack of appropriate cryptographic technologies allow to spoof messages and to deny the participation in a message exchange.

3.3 CEM Research and Security Properties

Even with the tracking services defined by the IETF standards tracks, e-mail has no electronic counterpart to traditional postal certified mail. In the last two decades the research community has tried to fill this gap by proposing and publishing a number of non-repudiation protocols for secure, reliable and evidential messaging meeting the requirements for certified mail. 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. By looking at regular mail delivery, certified mail is:

1. ***fair***. Due to physical presence of postal employees, a delivery is only handed over to the recipient if and only if a receipt is signed in exchange. Therefore, the postal service acts as TTP to ensure that the exchange of a delivery for a receipt between the sender and the recipient is fair.

2. ***non-repudiable***. The recipient has to sign a receipt, which is returned to the sender (a carbon copy may be filed for a certain period of time by the postal service). With this signature the recipient cannot deny having not received a certain delivery. This is more stringent if the delivery is restricted and the recipient's identity is verified with an official document, for example a driver's license, passport or identity card.

Postal certified mail delivery can thus be defined as the fair exchange of a message for a signed receipt. Zhou and Gollmann [1996b] follow this approach and define CEM as the fair exchange of a message for a Non-Repudiation of Receipt (NRR) evidence. An NRR evidence is linked to the message content, whereas postal certified mail only acknowledges a message envelope. In contrast to Zhou and Gollmann [1996b], not all researchers follow this definition. Ferrer-Gomilla et al. [2010] start their definition of CEM as a service, which provides exchange of a message plus a Non-Repudiation of Origin (NRO) evidence for an NRR evidence. The NRO evidence guarantees the sender's authenticity and ensures that the sender cannot deny of having participated in a communication. This is not the case for regular mail delivery, where the sender's identity is usually not verified by the postal service.

According to Ferrer-Gomilla et al. [2010], there is the agreement that certified electronic mail should be a fair exchange of items and that there is no agreement regarding the exchanged items. Based on these considerations, they have identified the following combinations of possible CEM definitions:

1. Exchange of message and NRO for NRR linked to the message.
2. Exchange of message and NRO for acknowledgment of receipt.
3. Exchange of message for NRR linked to the message.
4. Exchange of message for acknowledgment of receipt.
5. Exchange of envelope and, if possible, NRO for NRR, if possible, linked to the message.
6. Exchange of envelope and, if possible, NRO for acknowledgment of receipt.
7. Exchange of envelope for NRR, if possible, linked to the message.
8. Exchange of envelope for acknowledgment of receipt.

This list only concerns the exchanged items and illustrates the room for interpretation of the CEM service. A large number of CEM security properties can be found in the literature and authors of CEM protocols choose different properties they consider to be important. In this section these properties are discussed by reviewing common definitions and requirements. The focus is on core CEM security properties with practical applicability. Many protocols have been designed with the aim to increase efficiency by reducing the amount of computational and communicational power and to decrease the needed trust in third parties by proposing protocols where TTPs are only involved in exceptional cases, for instance in dispute resolution processes. However, these protocols and their properties are often questionable whether they are actually convenient and practicable when being deployed in real environments and under real conditions.

To obtain a detailed overview of all properties, several survey documents on non-repudiation protocols and certified electronic mail have been examined. A first work, which gives an overview of the evolution of protocols and techniques to achieve fair non-repudiation with TTPs, was published by Zhou et al. [1999]. Even if this work not explicitly addresses CEM, its findings can be applied to CEM as well. This result from the fact that CEM is part of the fair exchange family. Other typical fair exchange applications can be found in the areas of Electronic Commerce (e-Commerce) and contract signing. Vendors ship their goods to consumers expecting to receive the outstanding amount of money in exchange. In case of contract signing, one party submits a signed contract to the other party in expectation of receiving the countersigned contract. Particularly in the latter case not only the fair exchange, but also non-repudiation plays an important role. So when talking about non-repudiation protocols, the provided security services can be applied to all types of protocols being part of this family. This also includes CEM.

In 2000 a first detailed overview paper was published by Kremer et al. [2002], which provides a comprehensive survey of fair non-repudiation protocols. The paper briefly reviews some security properties that a fair non-repudiation protocol must respect. This review is limited to some core properties including the definition of different flavors of non-repudiation services, communication channels and timeliness (deadlines). Like Zhou et al., Kremer et al. discuss the evolution of TTP involvement. This ranges from protocols without TTP to protocols with a heavy involvement of TTPs. According to this TTP classification, their work discusses selected fair non-repudiation protocols.

Oppliger [2004] discusses the lack of evidence of Internet e-mail and a way to deal with CEM on the Internet. Like the previous surveys, the author discusses potential technologies and solutions classified according to the involvement of TTPs. In 2007, Oppliger extended his paper with a more elaborated version [Oppliger, 2007]. The paper discusses in detail the different approaches of TTP involvement, their benefits and drawbacks. 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.

So far only the two-party scenario has been considered. This means that exactly two entities, the sender and the recipient, agree to use a non-repudiation protocol. In the multiparty scenario, n entities, where $n > 2$, agree to use a non-repudiation protocol. Onieva et al. [2008] published a comprehensive survey of multiparty non-repudiation protocols. Like Kremer et al. [2002], they review in detail the non-repudiation fundamentals by defining requirements and security properties with a strong focus on evidences, the involvement of TTPs and the evidence lifecycle (non-repudiation phases). The focus of this work is on the definition of CEM security properties in the context of multiparty communication scenarios by discussing several multiparty non-repudiation protocols for contract signing and CEM.

Ferrer-Gomilla et al. [2010] recently published a work summarizing definitions, properties and requirements related to CEM. The paper features the most complete overview of security properties defined by the literature so far, shows the dependencies between single properties and analyzes why some of these properties are mutually exclusive.

In the following subsections, the following CEM security properties are reviewed in more detail:

- Non-repudiation services and evidences

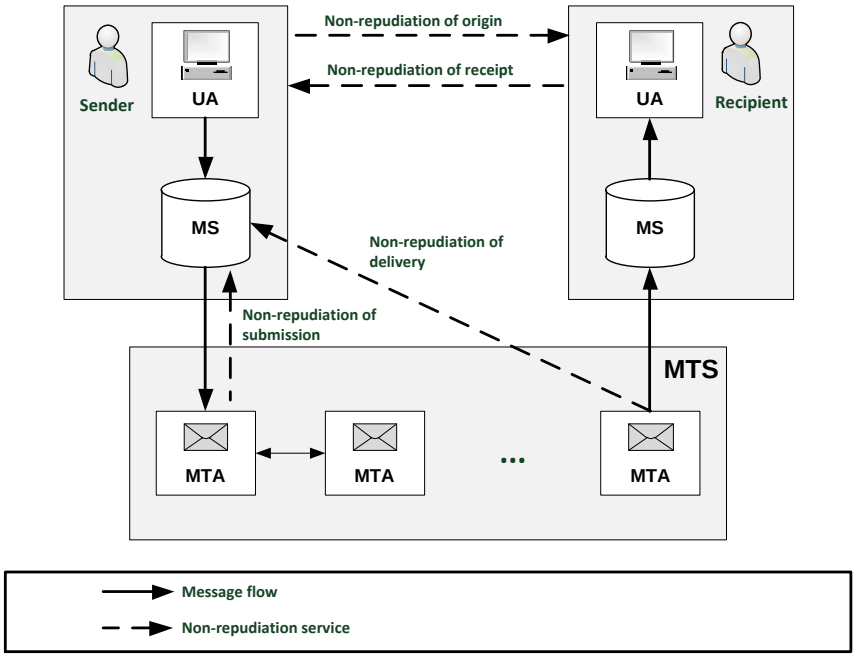

Figure 3.2: Flow of messages and evidence relations according to the model described in ISO/IEC [2009a].

- Fairness
- Trusted third parties
- Communication channel
- Timeliness
- State storage
- Confidentiality, integrity and authenticity
- Performance
- Policy

3.3.1 Non-Repudiation Services and Evidences

A communication between different entities may lead to a dispute. Senders may claim not having submitted or sent a message. They may also claim not being the originator of a message. Recipients on the other side may claim not having received, read, retrieved or downloaded a message. Even TTPs may cheat and deny the execution of particular operations or services. This is why non-repudiation is a core property of CEM protocols. It ensures that none of the involved parties can cheat and deny their participation in a communication.

The following international standards define non-repudiation mechanisms as a guideline for implementers:

- ***ISO/IEC-10181-4*** [ISO/IEC, 1997] extends and refines the non-repudiation services defined by ISO [1989] and the ITU-T Recommendation X.813 [ITU-T, 1996]. It defines a general framework

for the development and provision of non-repudiation services and describes policies and how they may be applied to open systems. The standard does not go into technical details and does not describe any protocol details.

- ***ISO/IEC-13888-1*** [ISO/IEC, 2009a][2] provides a general model for the other two parts of the ISO-13888 family [ISO/IEC, 2010, 2009b]. It defines non-repudiation mechanisms for the following evidence phases: generation, transfer, storage, retrieval and verification. The general model describes:
  - the entities involved in a non-repudiation exchange
  - the basic requirements for these entities
  - the involvement of TTPs in each evidence phase
  - evidence generation and verification using symmetric cryptography (secure envelopes) or using asymmetric cryptography (digital signatures)
  - non-repudiation tokens (evidences)
  - specific non-repudiation services (non-repudiation of origin, delivery, submission, and transport)
- ***ISO/IEC-13888-2*** [ISO/IEC, 2010][3]. The second part of the standard extends the general model of ISO/IEC 13888-1 with concrete mechanisms using symmetric cryptography. These mechanisms rely on so-called *Secure Envelopes* created by TTPs with a secret key. The TTP is also in charge of verifying these non-repudiation tokens. The standard specifies the specific non-repudiation mechanisms for NRO and Non-Repudiation of Delivery (NRD) as well as a mechanism for obtaining a time-stamping token.
- ***ISO/IEC-13888-3*** [ISO/IEC, 2009b][4]. This part extends the general model of ISO/IEC 13888-1 with concrete non-repudiation mechanisms using asymmetric cryptography. The specified non-repudiation security services are based on digital signatures and may be created both with or without the involvement of a TTP. The standard addresses evidences produced by end entities (NRO, NRR) as well as evidences produced by TTPs (Non-Repudiation of Submission (NRS), NRD). Figure 3.2 illustrates the abstract communication model highlighting the message flows and evidence relations between the single entities. ISO-13888-1 calls the NRD service Non-Repudiation of Transport (NRT) and the NRR service NRD. The exact definitions of these services are discussed below. Since certificates for creating digital signatures may expire, the standard further specifies mechanisms to ensure that a non-repudiation token was signed before a certain point in time. This is covered by the time-stamping and time-marking mechanisms.
- ***X.400*** [ITU-T, 1988, page 25]. X.400 already provides the non-repudiation services NRO, NRS and NRD (cf. Section 3.1.3).
- ***RFC 2828*** [Shirey, 2000, page 111]. This IETF standards track provides a Internet security glossary and defines the non-repudiation service as

  > *"A security service that provide protection against false denial of involvement in a communication."*

  The standard defines the two basic mechanisms "non-repudiation with proof of origin" (NRO) and "non-repudiation with proof of receipt" (NRR). Like ISO/IEC 13888, RFC 2828 defines the different evidence lifecycle phases of request, generation, transfer, verification, archival and possible dispute resolution.

[2] Revises the ISO-13888-1 standard from 2004
[3] Revises the ISO-13888-2 standard from 1998
[4] Revises the ISO-13888-3 standard from 1997

All introduced standards deal with the following four non-repudiation services:

- Non-Repudiation of Origin (NRO)
- Non-Repudiation of Receipt (NRR)
- Non-Repudiation of Submission (NRS)
- Non-Repudiation of Delivery (NRD)

These services are illustrated in Figure 3.2 and are defined in detail below. Most non-repudiation protocols found in the literature consider the following two services as necessary [Ferrer-Gomilla et al., 2010].

Definition 1 *Non-Repudiation of Origin (NRO). A protocol provides non-repudiation of origin if and only if it gives evidence against the false denial of having originated the message.*

The NRO service is addressed to the recipient and usually provided on an end-to-end basis, this means directly between the sender and recipient. The most common method to provide NRO are signatures based on digital certificates. For example, S/MIME or PGP are common standards to digitally sign e-mails. With the digital certificate belonging to the originator, recipients can verify whether the sender has signed a message with the corresponding private key and thus is the legitimate originator. But how do recipients know whether the sender is the claimed person and can be trusted? This could be ensured by TTPs. In the case of S/MIME the TTP is represented by a Public Key Infrastructure (PKI) [Cooper et al., 2008] providing a public directory holding the necessary verification information like Certification Authority (CA) certificates and status information like CRLs or Online Certificate Status Protocol (OCSP) responders. In contrast to the centralized PKI trust model, trust in PGP is established through a decentralized Web of Trust (WOT) where public signature keys are signed and asserted by people who know the owner of an identity certificate. This is usually done at so-called key signing parties. Independent from the used mechanisms, the quality of the provided NRO service depends on the quality of the used digital signature. This circumstance and its impacts are discussed in detail in next chapter (cf. see Section 4.4.1).

The non-repudiation token generated by the NRO service is called Evidence of Origin (EOO). Depending on the protocol, the evidence is generated by the sender or by an MTA on behalf of the sender. The latter may be the case when a sender has no own cryptographic infrastructure for creating digital signatures or the sender authentication method does not provide any means for transmitting an EOO to the recipient. Consider for example a sender using a Secure Sockets Layer (SSL) or Transport Layer Security (TLS) client authentication instead of generating a digital signature. A digital signature is usually part of the message and can be transmitted without problems to the recipient. A client authentication does not produce a transferable EOO. In this case an MTA may generate the EOO on behalf of the sender. If generated by a TTP, this evidence may also be created using symmetric cryptography, for example with secure envelopes as specified in ISO-13888-2 [ISO/IEC, 2010].

Definition 2 *Non-Repudiation of Receipt (NRR). A protocol provides non-repudiation of receipt if and only if it gives evidence against the false denial of having received the message.*

Like the NRO service, the NRR service is also provided on an end-to-end basis between the sender and the recipient. The resulting non-repudiation token is called Evidence of Receipt (EOR). The NRR service can be compared with the signature confirmation or return receipt service applied in postal certified mail. ISO-13888-1 calls this service Non-Repudiation of Delivery (NRD). Depending on the protocol, the EOR is generated by the recipient or by an MTA or MS on behalf of the recipient and is

addressed to the sender. There are different approaches to implement an NRR service. Some protocols require the recipient to just acknowledge the reception of a message envelope as done in postal systems. Most CEM protocols, however, require the recipient to acknowledge the reception of the message content. As discussed, most protocols thus consider Definition 1 and 2 as essential properties. Zhou and Gollmann [1996b] follow the postal certified mail model and consider just the NRR service as essential for CEM protocols.

In the context of the NRR service many protocols prevent a so-called *Selective Receipt*. This means that if the sender knows the message content before the receipt is generated, the sender can refuse to sign the receipt. This is a known problem in X.400. Therefore, CEM protocols usually require the sender to sign an EOR before getting access to the message content. Another type is *Author-Based Selective Receipt*. Author-based selective receipt is a problem that can also be found in postal certified mail delivery. For instance, if a person is in debt and receives a certified mail from a court or debt collecting agency, it may guess the content of the delivery beforehand and thus refuse its acceptance. The problem of author-based selective receipt, this means the author is revealed before the recipient has signed the receipt, was first addressed by Kremer and Markowitch [2001] presenting two CEM protocols taking this property into account. Further CEM protocols with no author-based selective receipt have been proposed by González-Deleito [2005] and Payeras-Capella et al. [2009].

Usually both NRO and NRR services are provided on an end-to-end basis where evidences are created by the sender and recipient without the intervention of a third party. In case MTAs or a MS are involved in the communication flow, disputes between these entities and senders or recipients may arise. No system is perfect. In the real world trusted parties may not work flawlessly or they may cheat. Examples are bribed cops or biased judges. The same may happen in the electronic world. TTPs may not work flawlessly or they may cheat. Therefore, protocols often provide the following two non-repudiation services as defined by Onieva et al. [2008, page 3].

Definition 3 *Non-Repudiation of Submission (NRS). A protocol provides non-repudiation of submission if and only if it gives evidence against the false denial of having submitted the message.*

The service only attests that a sender submitted a particular message to a certain MTA. It cannot be used to draw any conclusions on the remaining delivery process. The resulting non-repudiation token is called Evidence of Submission (EOS) and is usually generated by the sender's MTA and addressed to the sender. This security service is also provided by postal registered mail delivery giving the sender a proof of submission receipt with the tracking number of the delivery.

Definition 4 *Non-Repudiation of Delivery (NRD). A protocol provides non-repudiation of delivery if and only if it gives evidence against the false denial of having delivered the message.*

The service only attests that an MTA has delivered a particular message into the recipient's MS for later retrieval. It cannot be used to draw any conclusions on the remaining delivery process. This means the service does not give evidence if the recipient actually received, read or downloaded the message. The NRD service can be compared with the *delivery confirmation* security service of postal certified mail. ISO-13888-1 calls this service NRT. The resulting non-repudiation token is called Evidence of Delivery (EOD). This evidence is usually generated by the recipient's MTA or MS and is addressed to the sender.

Thus far the term evidence has been used to describe products or tokens of non-repudiation services. As discussed, digital signatures based on asymmetric cryptography as well as secure envelopes based on symmetric cryptography may be used. Each of them has its benefits and drawbacks. Digital signatures require a trust infrastructure like a PKI or a WOT. However, in contrast to secure envelopes they are less critical in terms of trust in the TTP. A NRO service based on digital signatures not only guarantees non-repudiation of origin, but ensures message integrity as well. A TTP processing a sender's message

may still read the content if it is not encrypted, but it is not able to modify the message content without being detected (provided that the recipient verifies the NRO signature). In contrast to digital signatures, secure envelopes require full trust in the TTP since evidences are both generated and verified by the TTP. They further require the online availability of the TTP to validate the evidence. If these conditions are not fulfilled, a malicious TTP may be able to modify the message content without being detected. One benefit of secure envelopes is the better performance. This results from the use of symmetric cryptography, which requires less computational power than asymmetric cryptography relying on longer keys.

Evidences usually consist of a set of data signed by the issuing entity to identify the transaction and the involved parties. The kind of data depends on the protocol and implementation but may comprise:

- Event code and reason
- A unique evidence identifier
- A reference to the message the evidence is bound to
- Entity details of sender or recipient
- Entity authentication details of sender or recipient
- Information about delegates acting on behalf of an entity
- Date and time of evidence issuance
- Policy IDs
- Evidence issuer details
- Digital signatures

A time-stamp is considered as important evidence part, at least when digital signatures are used. As discussed, (X.509) certificates have certain validity periods and may expire. In case of a dispute it is essential to know when the evidence was signed and thus if the used public key was valid at that point in time. It is therefore recommended to add a time-stamp to the evidence information to know whether an evidence was generated before a certain date. Evidence issuers can either add the system time or send the evidence data to a so-called Time-Stamping Authority (TSA), which creates a digital signature over the evidence data, a time-stamp of a synchronized clock and a unique TSA identifier.

Onieva et al. [2008, page 6] discussed the general evidence lifecycle specified in ISO-13888-1 [ISO/IEC, 2009a] with its five different phases: generation, transfer, verification, storage, retrieval and dispute resolution. In addition to the mentioned phases, the Internet security glossary (RFC 2828 [Shirey, 2000]) defines an initial evidence request phase. The seven evidence lifecycle phases are as follows:

1. ***Phase 1 - Request Service***. This is the initial phase where the requester asks for the evidence to be generated. Usually CEM protocols have a predefined set of evidences that are not generated on request but rather generated automatically at certain steps in the protocol.

2. ***Phase 2 - Generate Evidence***. In this phase an evidence generator generates an evidence on behalf of an evidence subject, a TTP or upon request by an evidence requester. This phase involves the potential repudiator and eventually a TTP. A TTP can be directly involved as online authority when secure envelopes are used or as inline evidence generator. It can also be indirectly involved as token generation authority, digital signature generation authority, time-stamping authority, monitoring authority or offline authority providing public key certificates.

3. ***Phase 3 - Transfer Evidence***. The transport of evidences to the requester is one of the most crucial parts of the protocol and heavily depends on the quality of the communication channel (see also cf. Section 3.3.4).

4. ***Phase 4 - Verify Evidence***. The evidence is verified by the requester to check its validity and if it meets all requirements for later potential dispute resolution. This procedure is closely related to the evidence generation phase. In case of secure envelopes the verifier has to contact the responsible TTP, which may cause additional delays.

5. ***Phase 5 - Store Evidence***. Evidences may be stored by different entities. Evidence requesters may store the evidence in a local store for later dispute resolution. Based on legal regulations, TTPs may also retain evidences for long-term archival.

6. ***Phase 6 - Retrieve Evidence***. Evidences may be retrieved from a store for several reasons. One reason is a dispute resolution process.

7. ***Phase 7 - Dispute Resolution***. This phase is only activated in case a dispute arises. An adjudicator is involved to arbitrate the dispute according to the given evidences and an agreed policy. Depending on the protocol and implementation, other parties may be involved in this phase as well.

The mentioned evidence phases are just considered from an abstract viewpoint. During the execution of a CEM protocol not all phases may be activated and different entities may be involved. This heavily depends on the applied non-repudiation policy based on agreements or a given legal regulation.

Regarding the verification of evidences in dispute resolution processes, the following definition is considered to be a compulsory property for protocols to be practical.

Definition 5 *Evidence transferability. Evidences are transferable if and only if they can be used independently by senders and recipients without the need to request input from other entities.*

Evidence transferability is usually a desired property and avoids the involvement of multiple entities. In this way evidences can be stored by requesters for later potential dispute resolution. For example, digitally signed evidences having a structured data format are well suited for exchange with entities. Nontransferable evidences pose the risk that TTPs or other entities would have to be consulted, logs to be evaluated, etc.

3.3.2 Fairness

Besides non-repudiation, fairness is also 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. However, no system is perfect. Cheating parties may not be the only reason for a dispute. Other factors may also lead to disadvantageous situations for one or more entities. Consider for example a network failure during the transmission of a receipt from the recipient to the sender. This is what fairness should prevent. Fairness originates from postal certified mail, where postal employees release the delivery if and only if the recipient signs a receipt. We can find similar scenarios for e-Commerce where customers receive goods only in exchange for money. No involved party should be in an advantageous position at the end of the exchange process. The literature defines the following flavors of fairness in the context of CEM and other non-repudiation protocols:

- Strong fairness
- Weak fairness
- True fairness
- Light fairness
- Probabilistic fairness

Asokan et al. [1998b] has defined the two notions of strong and weak fairness.

Definition 6 *Strong fairness. A protocol fulfills strong fairness if and only if all entities get the expected items, or none of the entities gets what is expected.*

It has to be noted that the use of the term "fairness" (without any prefix) usually means strong fairness.

Definition 7 *Weak fairness. A protocol fulfills weak fairness if and only if just one entity gets the expected item, and the other party has proof of this situation.*

The latter definition does not mean fairness is actually weak but rather verifiable. In each case one entity can prove to an arbiter that the other entity has received (or can still receive) the expected item. The practicality of weak fairness is questionable because user acceptance of such a property will probably be low.

Another interesting definition of fairness can be found in Kremer et al. [2002].

Definition 8 *True fairness. A protocol fulfills true fairness if and only if it fulfills fairness as defined in Definition 6, and in case of success, generated evidences are independent of how the protocol is executed.*

True fairness means that one cannot distinguish if a TTP intervened or not and that evidences are generated independently from that fact. Evidences generated by TTPs look the same as they would have been generated by senders or recipients. The same also applies vice versa. This property is equivalent to having a transparent TTP (as discussed later in this chapter).

A often cited practical use case of this property is e-Commerce. The scenarios of a cheating customer or a network failure during money transfer are theoretically impossible to distinguish. This circumstance may eventually lead to a bad customer reputation. For a protocol implementing true fairness it would thus not be evident if a TTP intervened or not. However, as Ferrer-Gomilla et al. [2010] argue, a single intervention of a TTP in e-Commerce scenarios must not immediately lead to a bad reputation. Only if a TTP must continuously intervene, the reputation of a vendor or customer can be questioned. Reputation schemes based on user ratings like applied by eBay seem to be better solutions than a protocol implementing true fairness.

Another practical use case for true fairness is legacy support. For example, if a CEM protocol without TTP is upgraded to a better protocol with TTP involvement, signatures created by TTPs may eventually not be recognized or processable by the other entities. True fairness ensures that the TTP in the upgraded protocol remains transparent.

Another interesting property, even if just from a scientific point of view, is probabilistic fairness.

Definition 9 *Probabilistic fairness. A protocol is probably fair with a probability ϵ if and only if it fulfills fairness as defined in Definition 6 and the probability that a cheating party is in an advantageous position is $< \epsilon$.*

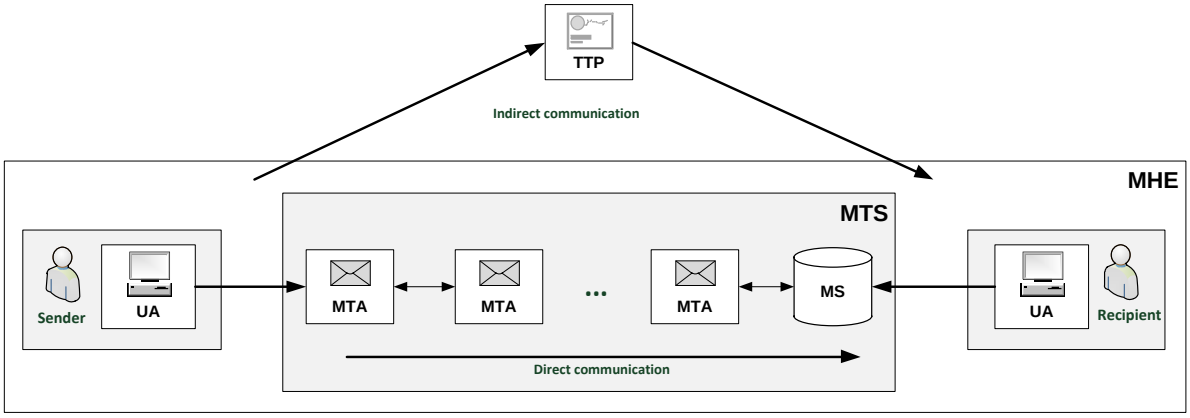

Figure 3.3: Models of message transfer according to Onieva et al. [2008, page 3].

Probabilistic fairness can usually be found in protocols not having any trusted third party. Markowitch and Roggeman [1999] proposed such a non-repudiation protocol. However, this fairness property is not really interesting in practice as entities get their items only with a certain probability and user acceptance of such a non-repudiation protocol will certainly be low.

Another special case of strong fairness was introduced by Onieva et al. [2009] in the context of multi-party non-repudiation protocols.

Definition 10 *Light fairness. A protocol fulfills light fairness if and only if sender and recipient get an NRR and an NRO evidence, respectively, or none of them gets an evidence.*

This property ensures just the fair exchange of evidences. This means that the recipient may receive the message, whereas the sender may not get any evidence. This would put one entity in a more advantageous position with respect to the fair exchange of a message for a receipt. Therefore, this property is not really applicable in the context of CEM.

3.3.3 Trusted Third Parties

Fairness is a core CEM property. The literature defines two ways how this basic requirement can be met. As illustrated in Figure 3.3, sender and recipient can either directly or indirectly communicate with each other and exchange messages and evidences. In the latter case a TTP is involved to ensure the fair exchange. When TTPs are involved, a major classification criterion of CEM protocols is the extent of a TTP's involvement in the protocol.

First approaches addressing the fair exchange problem actually required no TTP (direct communication). Basically all protocols for simultaneous secret exchange may be used to achieve fairness. The gradual exchange of information is such a method. Blum [1983] and Tedrick [1983, 1985] proposed protocols for the exchange of (secret) keys between two parties, whereby no party trusts the other.

However, these kinds of protocols are not practical. One shortcoming is the fact that these protocols make the assumption of communication partners having the same computational power, which is not realistic. Consider the disparity between a single standalone computer versus large enterprises. A huge number of computational rounds further worsen the applicability of these protocols.

In the 1990s the first fair protocols, which do not require a TTP and are independent from each party's computational power, were presented. Ben-or et al. [1990] presented a contract signing protocol that is fair in the sense that the conditional probability that one party can sign the contract for both parties is close to zero. Markowitch and Roggeman [1999] presented the first non-repudiation protocol without

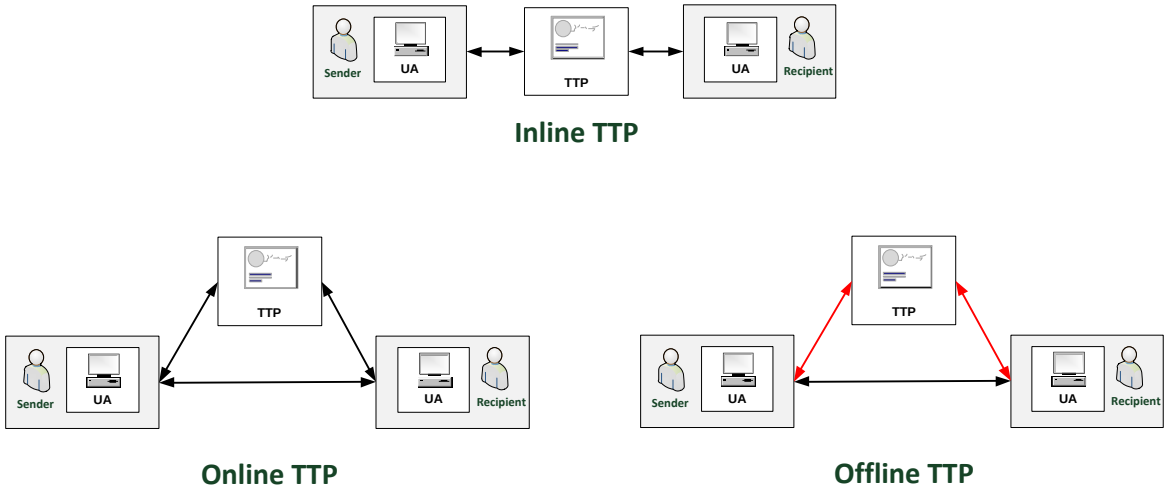

Figure 3.4: Involvement of TTPs according to Oppliger [2007, page 18,19].

TTP. Like Ben-or et al., this protocol has a probabilistic fairness. Even if the fairness of the protocol does not depend on the computational power of the participating entities, it depends on the number of protocol rounds. The protocol can be parameterized according to the more powerful entity and no entity is in an advantageous position until the last round. In 2001 a similar protocol was published by Mitsianis [2001]. In contrast to the approach of Markowitch and Roggeman, which allows a dynamic reconfiguration of the number of protocol rounds, Mitsianis's protocol has a fixed number of rounds being initially chosen by the sender.

Nevertheless, even if approaches without TTP have improved over the years, they can only ensure probabilistic fairness. This circumstance is not accepted by most users. Moreover, since these protocols usually require high interactions to increase fairness, they are not well suited for asynchronous protocols like e-mail. For the rest of this thesis, approaches without TTP are not taken into account because they are not practical. Several definitions are now introduced, which distinguish between the extent of a TTP's involvement. In the literature the following definitions can be found:

- Inline TTP
- Online TTP
- Offline TTP

Figure 3.4 illustrates the three models of TTP involvement in a two-party CEM communication scenario between a sender and a recipient.

Definition 11 *Inline TTP. A TTP is said to be "inline" if it is involved in each protocol step.*

As illustrated in Figure 3.4, an inline TTP acts as intermediary (mediator or message proxy) between the sender and recipient to ensure fairness. Therefore, sender and recipient do not directly communicate with each other. A possible CEM scenario with an inline TTP could be as follows. The sender's UA submits a message to the TTP. The TTP then starts the fair exchange. For example, the recipient may get notified that a message is ready to be retrieved. The recipient subsequently generates an EOR, transmits it to the TTP, which thereupon releases the message. Finally the TTP returns the receipt to the sender.

The advantages of the "inline" approach are first of all the simple concept. Since inline TTPs act as message proxy, they could for instance be implemented as part of existing infrastructural components

like MTAs or MSs. This allows to easily deploy this concept into existing infrastructures without the need to change client components on the sender's or recipient's side. Besides that and if desired, for example to avoid selective receipts, an inline TTP may also completely hide a sender's identity. Since the inline TTP acts as message proxy, it allows the full control of message flows and can completely decouple the sender from the recipient.

Inline TTPs have to process the entire message. Their disadvantage is that they may thus become a communicational and computational bottleneck, especially in large-scale environments. They may further need a large storage to preserve messages, logs and time-stamps. Besides higher infrastructural requirements, all entities must completely trust inline TTPs. This is why Bahreman and Tygar [1994] call protocols with inline TTPs the *believer's CEM*. Without appropriate security measures, a cheating inline TTP may read or modify messages. In each case, a dishonest inline TTP may withhold or discard messages. For example, this may be crucial in tendering processes and lead to an advantageous situation of a certain client or group. The trust in the whole system thus depends on the trust in the TTP. If a system has just one inline TTP it may pose a single point of failure, which leads to a heightened security risk.

The concept of inline TTPs first appeared in the context of CEM. In 1994 Bahreman and Tygar [1994] presented one of the first protocols using an inline TTP. Besides a CEM protocol without TTP, which uses cryptographic techniques like bit-commitment and zero-knowledge interactive proofs, they proposed a new protocol using an inline TTP called *postmaster*. Two years later Coffey and Saidha [1996] proposed an approach with a so-called non-repudiation server acting as a TTP intermediary providing NRO and NRR evidences signed by an additional TSA. Coffey and Saidha call their evidences Proof of Origin (POO) and Proof of Receipt (POR), respectively. Zhou and Gollmann [1996b] proposed a protocol where the message is transmitted from the sender to the recipient through a set of inline TTPs handling both the message delivery and the receipt collection. Their protocol provides both an NRS evidence and a NRD evidence, which are called Certificate of Posting (COP) and Certificate of Delivery (COD), respectively. Micali's Ideal Certified Mail (ICM) protocols [Micali, 1996, 1997c] are further examples of CEM protocols ensuring fairness with an inline TTP. The ICM protocols encrypt their messages in a way that the TTP is not able to access the content. A recent protocol using an inline TTP was published in 2005 by Cimato et al. [2005].

Definition 12 *Online TTP. A TTP is said to be "online" if it is involved in each protocol run but not in each protocol step.*

An online TTP is not required to process the entire message. Sender and recipient directly communicate with each other, but with the intervention of an online TTP (cf. Figure 3.4). A typical scenario with an online TTP could be as follows: a sender contacts the online TTP and submits a session key, which is used to encrypt the message. The sender directly sends the encrypted message to the receiver. The receiver contacts the online TTP, which releases the decryption key only in exchange for a receipt. After that the recipient can decrypt the message and the online TTP returns the receipt to the sender. The responsibilities and operations an online TTP has to carry out depend on the protocol. An online TTP usually does not process the entire message like an inline TTP, but carries out just message-related operations, for instance the provision of decryption keys or evidences.

Due to the lesser involvement of the TTP, online protocols require lesser communicational and computational power and are thus more efficient than protocols having an inline TTP. Even if online protocols have a greater performance, the trust problem is not automatically solved. However, in contrast to inline TTPs, an online TTP cannot discard or remove messages. It may still be able to delay the message delivery and it may eventually be able to read or modify a message in case it processes the message content. This may also be the case when the online TTP has the decryption key and gets the message from elsewhere. This problem can be solved with an additional End-to-End Encryption (E2EE) layer. Nevertheless, there is lesser trust needed in online TTPs than in inline TTPs. Like inline TTPs, even online TTPs may keep a database for a certain period of time in case of disputes.

The online TTP concept first appeared in 1984 in a US patent with the name "Method and apparatus providing registered mail features in an electronic communication system" by Mueller-Schloer [1984]. In 1995 Cox et al. [1995] published the *NetBill* security and transaction protocol in the context of e-Commerce. The system ensures the fair micropayment for information goods on the Internet with the NetBill system acting as online TTP. Zhou and Gollmann [1996a] proposed a CEM protocol with an online TTP. The main goal of this work is to minimize the involvement of the TTP in the protocol execution. Deng et al. [1996] proposed a protocol with an online TTP satisfying the requirements of fairness, NRO and NRD evidences. The protocol is suboptimal, because the message content has always to be carried through the online TTP. In 1996, Zhang and Shi [1996] presented another protocol with an online TTP. The sender submits a session key to the TTP, which is used to encrypt the message. To ensure that no other entity, even the TTP, cannot read the message, the content is further encrypted under the recipient's public key. At the right moment the TTP publishes the session for the recipient in a publicly accessible way. One drawback of this protocol is that the TTP must store the key information for potential disputes for an unknown amount of time. Franklin and Reiter [1997] were the first to introduce the notion of a semi-trusted TTP. In their protocol the TTP can fail or misbehave, but it cannot conspire with any other party. Their protocol relies on the assumption that at most one party cheats. This means, if for instance the recipient cheats, both the sender and the TTP must be honest. The protocol is designed in such a way that the cheating party cannot retrieve any useful new information about the message. In 2002, Abadi et al. [2002] presented a protocol with a so-called "light" online TTP. The main goals of the protocol are minimal infrastructural requirements, this means that it can be implemented without any special requirements for the recipient. The recipient can participate with a standard e-mail client and a web browser. A more recent protocol was proposed by Oppliger and Stadlin [2004], which uses an online TTP and dual signatures to cryptographically link the message keys to the message. The protocol is designed such that it can be deployed on the Internet.

Definition 13 *Offline TTP. A TTP is said to be "offline" if it is only involved in a dispute resolution process.*

An offline TTP is not involved in the communication between sender and recipient. It only intervenes in exceptional situations when a dispute arises (cf. Figure 3.4). This may be the case when a sender claims not having received a receipt, a recipient claims not having received the message or simply due to a network failure so that the message or receipt do not reach its destinations. Offline TTPs are the most used design pattern in today's CEM protocols. Offline protocols are said to be "optimistic" because they rely on the assumption that in most cases all entities are acting honestly and no transmission error occurs. Only in cases where an entity claims that it is in a disadvantageous position, the TTP intervenes and finishes the protocol to ensure fairness. This means that in the end either no items are exchanged or the protocol is finished and all entities receive their expected items.

From a performance perspective, offline approaches require the least communicational and computational power and due to their efficiency they are well-qualified for real-time applications. Compared to inline or online approaches, lesser trust is needed in a TTP, since it only intervenes in exceptional cases.

The disadvantages are that offline solutions usually have an increased message size and that they need a higher interaction between the sender and the recipient. However, this is not a desired property in asynchronous protocols like e-mail. Nevertheless, from a research viewpoint optimistic approaches are the most efficient ones and only require minimal trust in TTPs. Therefore, both Oppliger [2007] and Ferrer-Gomilla et al. [2010] recommend to focus research on this kind of solutions.

The offline TTP concept was first mentioned in 1983 by DeMillo and Merritt [1983]. Micali's Extended Certified Mail (ECM) protocols [Micali, 1997b] are very efficient. They require only three messages to be exchanged between the sender and the recipient. Micali proposed also variations of this protocol where trust is distributed among different TTPs in order to the reduce the needed trust in a single TTP. Another optimistic protocol was presented by Micali at the RSA conference in 1997 [Micali, 1997a]. Amongst the first non-repudiation protocols with offline TTPs were also those of Asokan

[Asokan et al., 1997, 1998a,b]. In 1997 Zhou and Gollmann [1997] published a more efficient version of their former CEM protocol [Zhou and Gollmann, 1996a]. They replaced the online TTP with an optimistic solution. Other protocols in the late 1990s were the ones presented by Chen [1998], which enables the fair exchange of digital signatures over the Internet, a digital contract signing protocol published by Pfitzmann et al. [1998] and a secure and fair non-repudiation protocol published by Zhou et al. [1999]. Zhou et al. give also a brief overview of the evolution of non-repudiation protocols with TTPs. In 2000, Kremer and Markowitch [2000] improved the protocol of Zhou and Gollmann [1996a], which was the most efficient one at that time. They identified the weaknesses and presented two solutions: one with an active offline TTP and one with a passive TTP. The TRICERT protocol by Ateniese and Goodrich [2001] bases upon the idea of semi-trust first introduced by Franklin and Reiter. Their solution makes use of an efficient offline TTP and several semi-trusted inline TTPs. More recent protocols have been presented by Nenadić et al. [2004] and Gürgens et al. [2005].

As discussed in the context of true fairness (see Definition 8), in some cases it may not be desired to know whether a TTP was involved or not. An often cited use case is reputation in e-Commerce scenarios. The property of true fairness can be ensured in offline CEM protocols with a so-called transparent TTP, which is defined as follows.

Definition 14 *Transparent TTP. A TTP is said to be "transparent" if it is not possible to decide whether an evidence was issued by the TTP itself or by some other involved entity.*

The TTP property of transparency is thus equivalent to having true fairness. The concept was first mentioned in a protocol proposed by Micali [1997a] where the TTP is called "invisible". Bao et al. [1998] and Asokan et al. [1998a] presented optimistic protocols for the fair exchange of digital signatures ensuring true fairness. Further examples are the protocols presented by Markowitch and Kremer [2001] and Markowitch and Saeednia [2002]. They allow the transparent signature recovery and are efficient in terms of communication and computation.

TTPs may misbehave like in the real world and may thus not be trusted. Therefore, some protocols require the involvement of TTPs to be provable. This means that that the TTP has to generate some kind of evidence that allows to demonstrate its participation. Ferrer-Gomilla et al. [2010] distinguish between "online" and "offline" verifiability, which are defined by Puigserver et al. [2005, page 1] as follows.

Definition 15 *Online Verifiability. A service is "on-line" verifiable when a user can immediately know whether the TTP misbehaved by checking the evidences received from the TTP. In case of problems the user can start a dispute to correct the situation.*

Definition 16 *Offline Verifiability. The verifiability of a security service is "off-line" when the evidences received from the TTP are not enough to know if it has been provided properly or not. But if a dispute arises between the parties involved in the protocol, then the evidences can be used to prove whether the TTP misbehaved.*

From the definitions above it is evident that an online-verifiable service requires an additional infrastructure besides the TTP to independently verify whether the TTP misbehaved or not. The properties of a transparent and verifiable TTP are mutually exclusive [Ferrer-Gomilla et al., 2010].

Another property, which is not directly related to the involvement of a TTP but more to confidentiality, can be found in Kremer et al. [2002].

Definition 17 *Neutral TTP. A TTP is said to be "neutral" if its correct operation is not conditioned by its knowledge of the message content.*

A neutral TTP is content-agnostic and its operations are just based on and affect only the message envelope. This means that also end-to-end encrypted messages can be processed by a neutral TTP.

3.3.4 Communication Channel

A crucial aspect of fair non-repudiation protocols and in particular CEM is the quality of the underlying communication channel. The quality and reliability of how data is transmitted from the sender to the recipient heavily determines and influences other security properties. Particularly if the protocol termination depends on deadlines, fairness may be threatened. Consider the following scenario. A CEM policy defines that if after a certain time period t the recipient has not returned an NRR evidence, the protocol is automatically terminated by the TTP. If, however, the data transmission of the receipt from the recipient to the TTP is somehow delayed due to a network failure or congestion, the protocol may be terminated and the sender never receives the receipt. On the contrary the recipient has received the message and is in an advantageous position. In this scenario strong fairness cannot be ensured anymore. The communication channel property is thus strongly related to the security property of timeliness, which is discussed in the next section.

The non-repudiation literature defines the following three types of communication channels:

- Operational communication channel
- Unreliable communication channel
- Resilient communication channel

Definition 18 *Operational channel. A communication channel is said to be "operational" if the transmitted data arrives after a finite and known amount of time.*

Operational channels require that a message arrives correctly to the recipient after a finite and known amount of time. They are rather unrealistic, especially in heterogeneous and distributed networks like the Internet. Even if the communication channel is designed such that data definitely reaches its destination, the time factor is hard to control and it usually cannot be guaranteed that the data arrives after a finite amount of time. The following definition of a communication channel makes no assumptions.

Definition 19 *Unreliable channel. A communication channel is said to be "unreliable" if transmitted data may get permanently lost.*

The Internet can be seen as an unreliable communication channel. Since it is an interconnection of networks operated by different providers and based on different technologies, this heterogeneity cannot guarantee a constant quality throughout the whole network. Several circumstances may cause the permanent loss of data. Internet providers do not guarantee a 100% online availability and may occasionally disconnect entities from the Internet. Other typical examples are malware like trojan horses or viruses, which modify network traffic or disconnect an entity from the Internet or (distributed) Denial of Service (DOS) attacks causing the temporary non-availability and disconnection from the Internet. Ferrer-Gomilla et al. [2010, page 172] claim that there may exist protocols to recover from these situations such that messages get not permanently lost. This could be achieved for instance through replay and acknowledge messages, computer viruses disinfection, firewalls, redundant network links, etc. This leads to the following definition.

Definition 20 *Resilient channel. A communication channel is said to be "resilient" if the transmitted data arrives after a finite and unknown amount of time.*

In a resilient channel, temporary disconnections, either resulting from Internet provider blackouts or attacks, do not lead to permanently lost data. The situation of lost messages is recognized and can be recovered from by re-sending the corresponding data. Messages are just delayed but they definitely arrive at their destination at a later unknown point in time.

3.3.5 Timeliness

Another useful property is timeliness, which is defined as follows.

Definition 21 *Timeliness. A protocol fulfills the timeliness property if and only if honest entities can stop the protocol execution in a finite amount of time while keeping fairness.*

This property is of practical relevance. Without this property entities would not be able to stop the protocol. For example, if recipients deny to sign a receipt, senders would eventually have to wait endlessly for the receipt and the protocol would never terminate. In practice this is a non-acceptable circumstance. Therefore, many protocols use deadlines to automatically terminate a protocol. However, Ferrer-Gomilla et al. [2010, page 175] state that the use of deadlines in combination with unreliable or resilient communication channels may threat the compulsory fairness property. This situation has been described in Section 3.3.4 where a recipient receives the message but the transmission of the receipt not happens in time and finally leads to an unfair situation. In this case a synchronized clock and an operational communication channel is needed to meet the deadline. However, TTPs may preserve evidences and adapt deadlines. For instance, if a receipt exchange between the TTP and the recipient has already started, the deadline could be postponed.

Ferrer-Gomilla et al. [2010, page 6] thus distinguish between the following two definitions.

Definition 22 *Synchronous timeliness. A CEM protocol is said to respect synchronous timeliness if all honest entities are able to terminate the protocol in a finite and known amount of time without loosing fairness.*

This kind of timeliness uses deadlines to terminate the protocol. All involved entities are required to keep their clock in sync with the TTP's reference clock. By using deadlines, TTPs have to preserve evidences only for a certain period of time. This property is called stateless state storage and is introduced in the next section.

Definition 23 *Asynchronous timeliness. A CEM protocol is said to respect asynchronous timeliness if all honest entities are able to terminate the protocol at any time without loosing fairness.*

The latter definition is not bound to any deadlines. This implies that a TTP may be forced to preserve (evidence) data for an unknown (infinite) amount of time or at least until evidences expire. In case the TTP is in charge of delivering the evidences, it may try as long as each entity acknowledges its receipt. Then the protocol would also be terminated. But in contrast to synchronous timeliness there is no deadline for this process.

3.3.6 State Storage

Depending on the protocol design, TTPs may need to store certain data and information to ensure fairness and to provide all required services. The literature defines four types of TTP state storage:

- Strong stateless
- Weak stateless
- Weak stateful
- Strong stateful

Definition 24 *Strong stateless. A TTP is said to be "strong stateless" if and only if it never needs to store any data to accomplish its tasks.*

From a practical viewpoint, the property of strong stateless is desired. However, this property is hard to realize in practice. At least not without complex and probably impractical protocol designs and increased message sizes. All the state information about evidences and related message items must be stored within the items itself. This also applies to any other protocol-related state information.

Definition 25 *Weak stateless. A TTP is said to be "weak stateless" if and only if it needs to store data for a finite and known amount of time to accomplish its tasks.*

In contrast to a strong stateless TTP, a weak stateless TTP can store data and it knows the period of time for how long state data must be stored. It is assumed that solutions provided on the Internet are all weak stateless. This is the case when policies or agreements regulate applied deadlines. After deadline or evidence expiration all related data can be permanently deleted.

Definition 26 *Weak stateful. A TTP is said to be "weak stateful" if and only if it needs to store data for a finite and unknown amount of time to accomplish its tasks.*

A weak stateful TTP also deletes state storage data. But in contrast to a weak stateless TTP it does not know when this will happen. This makes protocols impractical, because the period of time for state storage may be quite long and if data needs to be stored for many items the needed storage capacity cannot be estimated in advance.

Definition 27 *Strong stateful. A TTP is said to be "strong stateful" if and only if it needs to store data forever to accomplish its tasks.*

Strong stateful is the "worst" state storage property for practical protocols, because stored data will never be deleted. This implies that protocols will have to provide for a steadily increasing unlimited storage capacity. This is virtually impossible to realize. From the four state definitions only strong stateless and weak stateless are practical and desired properties. Since strong stateless is hard to realize, in practice protocols most likely will be weak stateless.

3.3.7 Confidentiality, Integrity and Authenticity

Another communication-related security property is confidentiality, which is defined by [ISO/IEC, 2009c, page 2] as follows:

Definition 28 *Confidentiality. Property that information is not made available or disclosed to unauthorized individuals, entities, or processes*

where processes is defined as "set of interrelated or interacting activities which transforms inputs into outputs". If this definition relates to a TTP, the TTP is called neutral (cf. Definition 17). Confidentiality can be provided between two points on the message route. A message may be encrypted between the sender's UA and the MTA, between MTAs, between MTAs and a MS or between a MS and a UA. A point-to-point encryption between the sender's UA and the recipient's UA is called End-to-End Encryption (E2EE). For Internet e-mail E2EE can easily be implemented with given standards like S/MIME or OpenPGP. E2EE may lead to systems where recipients can only acknowledge the receipt of a message envelope. Since TTPs cannot access the message content, the resulting NRR evidence may thus only be bound to the message envelope.

Besides non-repudiation and protecting confidentiality, data integrity and authenticity are further information security key concepts. ISO/IEC [2009c, page 4] defines integrity as follows:

Definition 29 *Integrity. Property of protecting the accuracy and completeness of assets*

where asset is defined as "anything that has value to the organization". This includes information ("knowledge or data that has value to the organization"), software, such as a computer program, physical, such as computer, services, people, and their qualifications, skills, and experience, and intangibles, such as reputation and image. At the bottom line, integrity ensures that any modification of communication data can be detected. ISO/IEC [2009c, page 2] defines authenticity as follows:

Definition 30 *Authenticity. Property that an entity is what it claims to be.*

Authenticity ensures that both data and communications are genuine. Authentication is the process to validate that entities (sender, recipient, TTPs) are who they claim to be and may be executed on several layers. For example, senders may provide an NRO evidence on the document level with a digital signature and may additionally authenticate against the MTS on the transport layer using SSL client authentication. Authentication levels may vary from low levels (username/password) to high levels using two-factor mechanisms like mobile-Transaction Numbers (TANs) or smart-cards based on national eIDs. It has to be stressed that a CEM protocol, which provides NRO evidence cannot hide a sender's identity at the same time. The authentication level is crucial to ensure a certain quality for providing value-added services like restricted delivery known from regular mail. The delivery to particular persons or authorized delegates in the electronic world can only be ensured if the authentication or registration has the same quality as an official ID used in the real world.

Interestingly, only non-repudiation and confidentiality are explicitly mentioned as security properties in the literature. Practice shows that data integrity and (sender) authenticity are apparently considered as intrinsic CEM properties. This does not apply to confidentiality. Particularly so-called notary systems try to add an additional security layer on top of the e-mail system by ensuring NRS, sender authentication and message integrity through digital signatures. However, confidentiality in these systems is left untouched, at least on the recipient's side. These kinds of CEM protocols and systems are reviewed in the next chapter.

3.3.8 Performance

Efficiency (performance) may also be a factor of interest when comparing and evaluating different CEM protocols. In the literature, efficiency is most often considered from a theoretical viewpoint and determined by the number of steps needed to execute a protocol. There exists no CEM protocol with less than three steps. A two-step protocol would mean that the sender sends the message to the recipient, which in turn sends the receipt back to the sender. In this case fairness cannot be guaranteed, because the recipient could always refuse to send the receipt. The most efficient protocols are optimistic protocols requiring at least three steps to finish, whereas protocols with online TTPs require at least four steps.

However, it is hard to estimate the efficiency of systems in place just on the basis of protocol steps. Depending on the process, a system may have to execute different flows and thus need a different number of steps to finish the protocol. For example, this may be the case when errors occur or deadlines expire and TTPs have to execute different procedures. By taking into account all conceivable scenarios, complete CEM protocol flows from sender to recipient (and vice versa) can be illustrated as decision graph in a tree structure. Even when just taking into account best-case or worst-case scenarios, the efficiency of deployed systems not only depends on the number of protocol steps but on deployment strategies, infrastructure, software, hardware and other factors that also determine efficiency.

3.3.9 Policy

Another interesting property is the applied policy or governance structure, because infrastructural characteristics are often determined by policy requirements. Policies usually determine the applied security

properties. They also regulate the procedures for dispute resolution and the designated judges.

National or Electronic Justice (e-Justice) systems are typically governed by “de jure” policies. Domestic laws regulate the types, requirements and accreditation procedures for TTPs, the communication infrastructure, evidences, timeliness, etc. In case of private businesses, a “de facto” policy may be defined by general business terms or on some other contractual basis between the service provider and its customers.

3.3.10 Dependencies and Incompatibilities

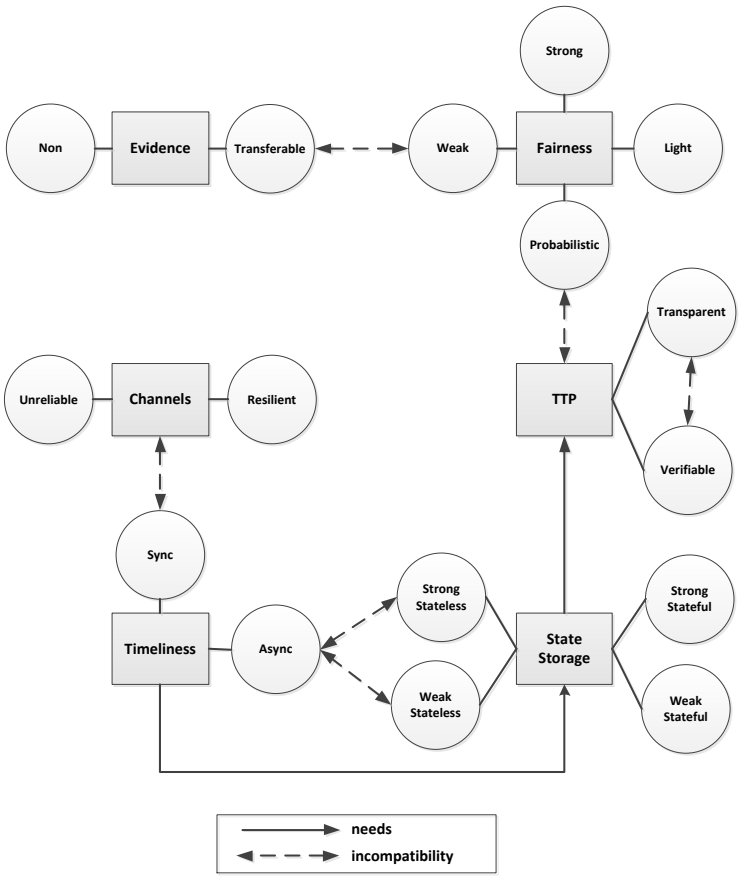

Figure 3.5: CEM security properties dependencies graph (according to Ferrer-Gomilla et al. [2010, page 11]).

Figure 3.5 illustrates the CEM security properties dependency graph defined by Ferrer-Gomilla et al. [2010, page 177]. The graph illustrates the discussed CEM security properties, their dependencies between each other and what properties are mutually exclusive, this means that cannot be used together.

From the graph the following dependencies can be deduced:

1. State storage requires a TTP.
2. Timeliness requires state storage.

Storing a protocol’s state means storing crucial information like process flow status, acknowledgement status, etc. Since this data determines the further process flow and eventually the content of resulting evidences, TTPs are required to preserve this information. The dependency of timeliness on state storage

results from the discussion on the Definitions 22 and 23 on synchronous and asynchronous timeliness. To ensure timeliness, TTPs are required to store evidences for a known (synchronous timeliness) and unknown (asynchronous timeliness) amount of time.

Ferrer-Gomilla et al. [2010, page 175] have identified the following incompatible properties:

1. ***Transparent TTP versus verifiable TTP***. Verifiable means that one can check whether the TTP misbehaved or not. According to Definition 14, one cannot determine whether the TTP was involved in the protocol run or not. Therefore, both properties are mutually exclusive.

2. ***Asynchronous timeliness versus strong stateless***. As discussed for Definition 23, asynchronous timeliness requires state storage for an unknown amount of time. This is incompatible with strong stateless.

3. ***Asynchronous timeliness versus weak stateless***. As discussed for Definition 23, asynchronous timeliness requires state storage for an unknown amount of time. This is incompatible with weak stateless.

4. ***Transferable evidences versus weak fairness***. According to Definition 5, with transferable evidences entities can show that a message was sent or received without involving other entities. However, this is not guaranteed with weak fairness.

5. ***Synchronous timeliness versus unreliable and resilient communication channels***. By using particular deadlines, synchronous timeliness (cf. Definition 22) requires a synced clock and that messages and evidences are transmitted in a known amount of time. This property is thus only compatible with an operational communication channel.

Having reviewed and discussed CEM research security properties according to their practical relevance, the next chapter continues to give an overview of systems, which implement CEM protocols and are deployed on the Internet. The systems are reviewed according to the terminology introduced in this chapter. Besides demonstrating the similarity of CEM systems to their traditional postal counterparts, a comparison of these systems also demonstrates that certain properties are indeed incompatible as discussed above.

Chapter 4

Certified Mail Systems Provided on the Internet

"To effectively communicate, we must realize that we are all different in the way we perceive the world and use this understanding as a guide to our communication with others."

[Anthony Robbins, American Self-Help Author.]

More and more people are using the Internet as a means to retrieve or to share information or to communicate with each other. The number of Internet users has increased from about 360 million in 2000 to 2 billions by the end of March 2011[1], which corresponds to 30% of the world population. Even if in the last years the usage of microblogs, IM tools or social networks rapidly increased, e-mail is still the fastest growing communication media. According to Radicati [2010], 2,9 billion e-mail accounts are currently registered. This corresponds to about 1,6 e-mail accounts per person. It is assumed that this number will increase to 3,8 billion in 2014, whereby the number of e-mail accounts per person will remain about the same. Most accounts are for private use (75%) and this number will only slightly change in the next four years. In 2014 corporate e-mail accounts will increase to a total of 26%. However, in contrast to private users, corporate users receive 110 messages a day on average.

By looking at the benefits of shifting traditional certified mail services to hybrid certified mail (cf. Section 2.5), it is reasonable to think one step further and to provide certified mail as fully electronic service. As discussed in Chapter 3, standard communication systems like e-mail do not meet the requirements for electronic certified mailing. In the last two decades the research community has thus tried to fill this gap by proposing and publishing a number of non-repudiation protocols for secure and reliable messaging. Besides Certified Electronic Mail, the expression Certified Mail System (CMS) is used when talking about protocols in the context of electronic mailing systems[2], for example e-mail.

Due to an increased demand from the public and private sectors and based on the results of the research community, the CMS ecosystem has significantly grown in the last decade. Governments, postal services and private businesses have put into operation a number of CMS on the Internet. Governmental systems are usually based on specific legislation, have well-defined policies and are usually supervised by regulatory authorities. They are thus often called "de jure" systems. Private sector systems are normally not based on legal regulations but rather on a contractual basis or agreement between the service provider and its customers. In the private sector especially, postal operators aim to compensate for the shift from paper to electronic communications by providing value-added services on the Internet. One such value-added service is the provision of Certified Electronic Mail (CEM). Besides the fair and non-repudiable exchange, further obvious benefits are as follows:

[1] Source: Internet World Stats - `http://www.internetworldstats.com/stats.htm`

[2] The terms CEM and CMS can be used synonymously to denote either the action of certified electronic mailing, a CEM protocol or a certified mail system.

- ***Economy of time***. Senders can enjoy the same time-saving benefits like hybrid mail users. No more time must be spent on printing, enveloping, stamping. Hybrid mail still requires a last printing and traditional mail delivery step. This is probably the most time-consuming part. CEM delivery is completely electronic and the delivery from the sender to the recipient usually takes no more than a few seconds or minutes. However, not only senders benefit from a time-saving electronic delivery. In case of traditional certified mail, the delivery is often deposited at the nearest post office, if the recipient is not present. The recipient must then go to the post office to pick up the delivery. With CMS provided on the Internet, messages are always delivered into the recipient's mailbox, which can usually be accessed online and anytime from home.

- ***Cost-savings***. One of the main reasons for senders to switch from paper-based mailings to electronic ones are the tremendous cost savings. Besides personnel costs for enveloping and stamping, printing costs can be enormously reduced. This is manifested by the Austrian Electronic Law (e-Law) work flow, process and production management system as an example. The system was introduced by the Austrian Federal Chancellery and the Parliament in 2000. It provides a work flow system where all federal ministries are connected together to simplify the single steps of law making in a fully electronic way. Besides time savings, the paper consumption was enormously reduced [Engeljehringer, 2004]. Initially there was a paper consumption of 60 million tons a year. Through this electronic workflow management system yearly costs of more than 1 million € could be saved. This example can not be directly mapped to CEM but illustrates the potential savings of printing costs (and the implicit reduction of the CO_2 footprint).

  Besides personnel and printing costs, the delivery costs for CEM are usually vastly reduced. This is emphasized by a market study evaluating the potential of certified electronic mail in Austria [Füll, 2005][3]. According to this study, public administrations are sending 130 million deliveries a year. Most of them are delivered by the Austrian universal postal service, the Österreichische Post AG[4]. 17 millions (13%) are certified mail items. This corresponds to 90% of the total volume of certified mail items (public + private). Even if certified mail items make up 13% of all public sector deliveries, the portion of costs is about 47%. This is reasoned by the quintuplicate price. A certified mail costs on average € 3,5 compared to € 0,66 for regular letters. Most of the certified mail items are sent by either the Ministry of Justice (>50%) and the Treasury (˜30%). Based on estimated investment and maintenance costs for a CMS infrastructure, the study calculated potential cost savings of about 80-90% compared to traditional mail delivery. This calculation assumes that all deliveries are sent electronically. However, the break-even for a CMS infrastructure in Austria would already be reached with a volume of 180.000 CEM items per year.

- ***Location-independency***. Hybrid mail provides a certain location-independency for senders. Deliveries can be sent from everywhere, for example from automated applications, from the office or even from home. All deliveries are bundled in printing centers. CEM provides the same comfort for senders, but enables location-independency also for recipients. Access possibilities with Web browsers or e-mail clients allow recipients to retrieve and read messages from almost everywhere, even when being on vacation far away from the workplace (or from home).

- ***24x7 Availability***. Traditional mail delivery is bound to the service hours of postal services. Postmen usually deliver mail items only at daytime. The same applies to post offices when recipients have to pick up a deposited delivery there. Like e-mail, CEM has no constraints like business hours, but rather provides operating times of 24 hours a day and 7 days a week.

- ***Media-break free***. Nowadays business applications and processes are almost completely electronic. This starts from data collection or data input and covers automated processing of this

[3] Even if the study was conducted in 2005, most information, data, statements and results are still valid today.
[4] http://www.post.at

data across different departments or organizations. Delivery is usually the last step in public proceedings or business processes. Public agencies and courts send verdicts or other notifications as a result of an ongoing or completed proceeding. Insurances send the result of a case to the concerned parties. Even if business applications and processes are fully automated, traditional mail delivery is still widely used, which inevitably causes a media break. This media break is particularly problematic in case of hybrid certified mail where the evidence returns as paper-based receipt. This format must then be converted back to its electronic version so that the result can be processed by the application. A CMS, however, allows the bidirectional electronic processing of messages and evidences for a seamless integration into existing business applications and processes.

- ***SPAM free***. According to the Messaging Anti-Abuse Working Group (MAAWG) report for the third and fourth quarter 2010 [MAAWG, 2011], 88% - 91% of all e-mail traffic can be classified as "abusive" e-mail. Abusive e-mail are defined as communications, which seek to exploit the end user. In many regions this kind of communications, this means unsolicited or unwanted e-mail by the user, is called SPAM. The number of roughly 90% relates to the unfiltered e-mail traffic, which is about 90 trillion e-mails per year, these are 250 billion e-mails per day or 2.9 million e-mails per second. Even though today's SPAM filtering mechanisms are quite advanced and have a good detection rate, according to MAAWG [2011] 18% of all incoming e-mails are still SPAM. This number includes both actual SPAM and graymail, which also comprises newsletter and other informational mail. It is assumed that this number of SPAM mails causes costs of about $ 3 million per year for a 1000-person organization.

  A major benefit of CMS is their closed nature. Most CMS are just accessible by certain user groups. Usually each participant has to be registered in a qualified way using an official ID document or an eID. By default, the system is protected with strong authentication mechanisms. This makes it easy to track down and eventually prosecute malicious users. Moreover, many systems have a per-message payment scheme. In this case each sent message produces a multiple of expenses compared to standard e-mail.

Despite these common advantages, CEM has nevertheless many flavors. System architects and standard designers may put emphasis on different aspects of certified mail, which is observed in the diversity and heterogeneity of deployed systems. As discussed in Chapter 3, also the research community has no common view on the security properties that a CMS has to provide. As long as systems are autonomous and remain closed, this is not a significant issue. However, an increasing demand for interoperable CMS can currently be observed, for both global reliable business communications and public sector systems. An assessment and classification of existing solutions would facilitate an alignment of different CMS towards interoperability.

The goal of this chapter is to give an overview of existing systems and standards and to assess and evaluate applied security properties. Many certified mail protocols found in literature are only considered from a theoretical point of view. Practical aspects are often left out. For example, most published protocols have been designed for efficiency. This leads to design decisions in which it is questionable whether they are deployable under real conditions. This sections aims at getting a clearer view of the CEM security properties that are actually applied in practice. It is based on two previous publications of the author. The first work [Tauber, 2011] provides a detailed survey of today's CMS landscape by taking both deployed systems and standards into account. In contrast to this survey, which covers systems from all over the world, the second work [Tauber et al., 2011a] focuses on deployed systems in the countries Austria, Germany and Switzerland. The remainder of this chapter is organized as follows. In the preceeding chapter the security properties defined so far by the research community have been reviewed by discussing common definitions, requirements and their practical relevance. Using this terminology, this chapter reviews five major national CMS and three CMS standards. Other existing systems and standards are also briefly discussed. Finally, applied security properties are assessed and evaluated by discussing the decision of system architects and standard designers of just using particular properties.

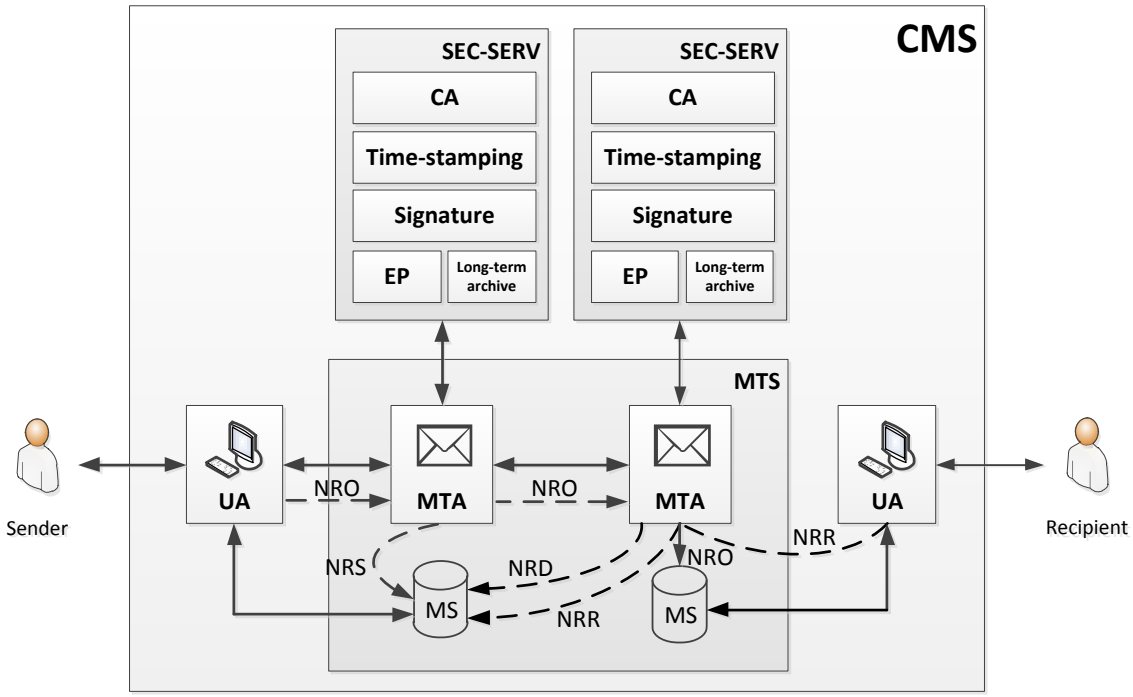

Figure 4.1: General X.400-based architecture of certified mail systems

4.1 General CMS Architecture

The general X.400 mail handling model discussed in the preceeding chapter (cf. Section 3.1) is used to describe CMS architectures and protocol flows and to label CMS entities in this chapter. Most CMS operate on the same architectural and communicational model. Cryptographic primitives are intentionally not discussed in detail.

Figure 4.1 illustrates the general architecture of today's CMS according to the X.400 model. In contrast to the X.400 model introduced in the preceding chapter (cf. Figure 3.1), this model extends the X.400 architecture with two aspects. First, the evidence process flows according to ISO-13888-1 (cf. Figure 3.2) are indicated with dotted lines. This illustrates, which entities are the originator, intermediary and final consumer of certain evidences. Second, the figure shows what typical additional security services may extend the X.400 architectural model to form a CMS. These are as follows:

- ***Evidence Provider***. Evidences are generated and eventually also verified by a so-called Evidence Provider (EP). This service may be provided by a third party as standalone instance or may also be an integral part of the MTS, for example as additional feature of an MTA or a MS. The EP services are usually accessed by TTPs to generate NRS and NRD evidences. However, smaller instances of EPs may also be found in the sender's and recipient's UAs to generate NRO and NRR evidences.

- ***Long-term archive***. Based on legal requirements or a system's policy, evidences may have to be preserved for a long time in order to resolve a potential upcoming dispute. Like the EP, a long-term archive may be provided by a third party or implemented as integral part of the MTS acting as TTP.

- ***Signature Provider and TSA***. Both components, the EP and the long-term archive, usually rely on cryptographic technologies using digital signatures and timestamps. A Signature Provider (SP)

provides means to create and verify signatures based on different formats. The TSA attaches a timestamp to an evidence signature so that the signature time remains evident and the signature can be verified at a subsequent time. Both the SP and the TSA usually rely on PKI technology to establish trust of their provided services throughout the whole CMS.

According to the X.400 terminology, a message consists of two parts: a transport envelope and the actual message content. In case of CEM the content could either be a so-called *Dispatch Message*, for example a document for the recipient, or an *Evidence Message*. In contrast to an evidence message, the dispatch message is created and submitted by the sender and addressed to the final recipient. Depending on the CMS, evidence messages may be created by various entities and have various recipients. Possible evidence messages could be:

- NRR evidence created by the recipient for the sender.
- NRD evidence created by the recipient's MS for the sender.
- NRS evidence created by the sender's MTA for the sender.
- NRS evidence created by the sender's MTA for the recipient.

4.2 Certified Mail Systems

Based on the core CEM security properties discussed in the preceding chapter (cf. Section 3.3), this section continues to discuss several CMS systems according to this terminology. Even if a number of systems have emerged in the last years, many of them are operated by postal services and other private businesses, have closed and proprietary specifications and do not provide any external interfaces. Therefore, this section investigates the following five national CMS, which are deployed nationwide on a large scale and have publicly available specifications.

1. The Austrian Document Delivery System (DDS)
2. The Italian Posta Elettronica Certificata (PEC)
3. The German De-Mail system
4. The Austrian e-Justice system Electronic Legal Communications (ERV)
5. The Slovenian moja.posta.si

For each system, some general and, if available, legal background information are provided. Both the architecture and the standard CMS protocol flows are discussed on an abstract level. Moreover, main building blocks, roles and relationships between the system entities are shown to reflect the security properties. Besides the five systems discussed in detail, other CMS are described and discussed as well.

4.2.1 DDS (Austria)

Policies and requirements for the Austrian Document Delivery System (DDS) - the CMS for the public sector - are laid down by the "Service of Documents Act" [Republik Österreich, 1982][5], which provides the legal basis to facilitate communications with public bodies. The Austrian DDS was put into operation on the Internet in 2004. The technical specifications [Reichstädter and Tauber, 2008] are maintained by the Austrian Federal Chancellery.

[5]The law was amended in 2004 [Republik Österreich, 2004] by defining certified electronic mailing and electronic communication systems as second delivery channel besides traditional mail delivery. In 2008, the law was last amended by introducing minor changes to the procedures related to electronic delivery [Republik Österreich, 2008].

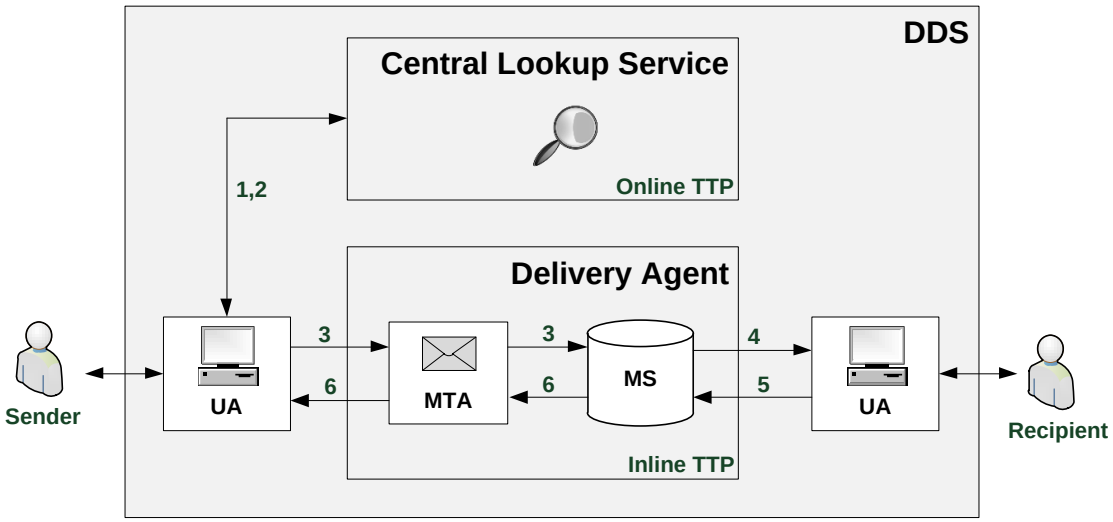

Figure 4.2: Architecture and protocol steps of the Austrian Document Delivery System (DDS)

Architecture Figure 4.2 illustrates the architecture of the Austrian DDS, which has been discussed in detail by Tauber [2009, 2010], Reichstädter [2003] and [Posch et al., 2011, 2012]. The Austrian DDS defines the following main types of entities:

- ***Senders***. All public bodies can register as sender.
- ***Delivery agents***. Delivery agents act as inline TTP to ensure strong fairness between senders and recipients. They provide an MTA for senders and a MS for recipients. Delivery agents have to be accredited by the Federal Chancellery. So far, the following three providers have been officially accredited[6].
  1. Österreichische Post AG[7]
  2. Federal Computing Center (FCC)[8]
  3. Telekom Austria TA AG[9]
- ***Recipients***. All natural and legal persons can register with one or more delivery agents.
- ***Central Lookup Service (CLS)***. The Austrian Federal Chancellery operates a lookup service holding the address data of all recipients registered with a delivery agent.

A hallmark of the Austrian architecture is that only recipients have to register with delivery agents. Senders are required to register with the CLS. All Austrian citizens and corporate bodies may register as recipient with any delivery agent. They are free to register with multiple delivery agents. Registration with delivery agents is based on the Austrian citizen card, the national eID, which is legally equivalent to standard ID documents and allows for creating Qualified Electronic Signatures (QESs) in conformance with the EU Signature Directive [The Council of the European Union, 2000b].

[6] An official and up-to-date list of accredited delivery agents can be found at `https://www.bka.gv.at/zustelldienste`

[7] `https://www.Meinbrief.at`

[8] `https://www.brz-zustelldienst.at`

[9] `https://zustellung.telekom.at`

The communication between the citizen card and applications is based on an open protocol specification called "Security Layer". This protocol hides the complexities of citizen card tokens with an abstract interface layer. This was necessary, because so far there are no standardized platform-independent or vendor-independent mechanisms for Web browsers to access hardware tokens in a custom way. Standard mechanisms provided by Web browsers are mostly limited to SSL client authentication. The Security Layer protocol provides functions for the Austrian citizen card to create Advanced Electronic Signature (AdES) and QES and to access particular data structures on the card. The protocol is based on Hypertext Transfer Protocol Secure (HTTPs) carrying well-defined XML requests and responses. Software implementing the Security Layer protocol may hence be accessible from any network location. So far, there are Security Layer implementations to access smart-card tokens using local software or Java applets embedded in the browser[10]. Recently, software has been provided to access server-side Hardware Security Module (HSM) tokens using a Mobile Transaction Number (mTAN)[11]. The concept of the mobile citizen card has been discussed in detail by Orthacker et al. [2010]. The security architecture of the Austrian citizen card is discussed in detail by Leitold et al. [2002].

Registration for legal persons as recipient is based on the citizen card together with an electronic mandate. Representation of legal entities has been considered by the Austrian e-Government strategy from the beginning and is an integral part of the Austrian e-Government law [Republik Österreich, 2004]. On this basis Austria has built an infrastructure for legal identity management using the concept of "electronic mandates".The concept of empowerment through electronic mandates in Austrian e-Government has been discussed in detail by Rössler [2009a] and Tauber and Rössler [2009a]. Mandate management based on this concept, which enables access for professional representatives like lawyers, notaries, etc. is discussed in detail by Tauber and Rössler [2009b]. In 2010, the Austrian e-Government initiative adapted the concept of electronic mandates towards an online, systematic and token-independent approach[12] enabling legal identity management on the basis of the citizen card and fresh information from constituent registers. Tauber and Leitold [2011] discuss the evolution of the Austrian electronic mandate infrastructure, the experiences gathered and the necessary adaptations from local mandate management to an online, systematic and token-independent approach.

In the Austrian DDS, senders have to provide an X.509 SSL client certificate for registration. This certificate must be used by the sender to authenticate against both the CLS and delivery agents. The certificate must have a particular X.509 Object Identifier (OID) extension [Rössler, 2009b]. This identifier is called the Austrian e-Government OID, which certifies that the authenticating party belongs to a public body.

The CLS is a directory holding the data of all registered recipients (registration data is provided by delivery agents). It is a trusted source providing the information with which delivery agents a recipient is registered. This is necessary, because the Austrian system has no domain-name based addressing model such as Internet e-mail. The Austrian system is based on the Simple Object Access Protocol (SOAP) and uses a national ID number based scheme to address recipients. This number is called Id_R and is the recipient's unique ID number in the context of CEM. Delivery agents bind a recipient's electronic mailbox to Id_R and register the mailbox by sending this value along with associated demographics (name, date of birth, etc.) to the CLS. Senders are not able to determine a recipient's delivery agents just on the basis of this number and must thus query the CLS.

[10]More general information about the citizen card and technical specifications can be found at `http://www.buergerkarte.at`. The site also provides a support forum and several tools for signing and verifying e-mails and PDF documents (online).

[11]More information about the features, registration procedure and usage of the mobile signature solution can be found under `https://www.handy-signatur.at`

[12]The mandate management system for bilateral mandates between physical persons can be found under `https://vollmachten.stammzahlenregister.gv.at`. The site also provides some further general information about the systematic mandate management solution.

CMS protocol The protocol steps of the Austrian DDS are illustrated in Figure 4.2.

1. The plain Sector Specific Personal Identification Number (ssPIN) can only be used by delivery agents or the CLS, as both operate in the domain of CEM. Senders usually operate in different administrative sectors and thus have to use an encrypted form of the ssPIN. They can calculate the encrypted ssPIN for CEM by sending the ssPIN together with the recipient's name and date of birth to the SourcePIN Register Authority (SPRA), which determines the corresponding Source Personal Identification Number (sourcePIN) and calculates the encrypted ssPIN for certified electronic mail by encrypting a concatenation of the plain ssPIN and a timestamp with the RSA[13] public key of the CLS. As discussed, senders cannot address recipients with a domain-name based scheme. Recipients can only be addressed by means of demographics (name, date of birth, etc.) or the encrypted ssPIN. Therefore, in a first step, the sender's UA must query the CLS to determine with which delivery agent(s) a recipient is registered. This operation is performed using an HTTPs GET request based on SSL client authentication.

2. The CLS searches in its internal database for recipients matching the given search parameters. If a recipient has successfully been found, the CLS returns the complete list of delivery agents the recipient is registered with. Each delivery agent list entry contains the following data.

   - ***Unique identifier***. The CLS encrypts Id_R (plus a timestamp) with the RSA public key of the associated delivery agent. Due to the unique nature of this encrypted token it also serves as billing token. Delivery agents have to validate this token at the CLS after having received a delivery. In this way, the CLS acts as an online TTP (not in terms of fairness) to ensure a correct billing procedure.
   - ***Uniform Resource Locator (URL) of the delivery agent***. This URL defines the Web service interface of the delivery agent's MTA where senders can submit messages to.
   - ***Supported document formats***. Recipients can define at each delivery agent the document formats they support. The delivery agent list entry contains a list of MIME types defining the supported document formats.
   - ***Optional encryption certificate***. If the recipient has provided an X.509 encryption certificate for E2EE, it is also part of the result list.

3. The sender's UA chooses a delivery agent from the list and submits the message to the Web service endpoint of the recipient's delivery agent MTA. This operation is based on the SOAP Messages with Attachments (SwA) over HTTPs transport protocol [Barton et al., 2001]. SwA defines a mechanism to carry SOAP messages within a MIME multipart message together with a set of attachments encoded as single MIME parts. All attachments can be referenced from within the SOAP messages using a specific Uniform Resource Name (URN) identifier. The CMS protocol of the Austrian DDS carries all metadata within the SOAP message. This data comprises

   - The recipient's unique identifier.
   - An electronic address where NRR evidences have to be returned. This may either be an e-mail address or a Web service, which must be reachable by the delivery agent.
   - The sender's and recipient's demographics (name, date of birth, etc.).
   - A reference or application number, which uniquely identifies the delivery.
   - The delivery quality. Senders can deliver a message with either standard quality or with CEM quality called "RSa". RSa requires the recipient to provide an NRR evidence, whereas

[13] RSA stands for Rivest, Shamir and Adleman who first described this algorithm as a method for obtaining digital signatures and public-key cryptosystems [Rivest et al., 1978]

from a security perspective the standard quality can be compared to e-mail. If the delivery quality is followed by a "+" sign (for example RSa+), the delivery is restricted and postal representatives are not allowed to retrieve a delivery with an electronic mandate on behalf of the recipient.

In case of E2EE, the whole MIME container including the SOAP request is encrypted with the recipient's X.509 certificate using the S/MIME standard. In this way, delivery agents can forward the encrypted message to the recipient's S/MIME-capable e-mail client, which can take the message as is and easily decrypt it with the corresponding private key. Senders are recommended to electronically sign documents to provide an NRO evidence on the document level. Transferable NRO evidences on the transport layer are not foreseen. The delivery agent checks if the sender's SSL client certificate is valid and has the Austrian governmental OID. If the message passes all checks, the delivery agents takes the message in charge and stores it into the recipient's MS.

4. The delivery agent sends out an e-mail or SMS notification to inform the recipient that a message is ready for retrieval. If the recipient does not retrieve the message within 48 hours, a second notification is sent. A third reminding notification is sent after another 24 hours by regular mail, if and only if the recipient has defined a postal address.

5. The recipient's UA authenticates against the MS using a Web browser and generates an NRR evidence by signing an XML-based proof of receipt using the citizen card. This signature is created by the recipient with the help of the Security Layer interface. The NRR evidence consists of a QES certifying the acceptance of the message content. The message itself can now be retrieved by the recipient's UA from the MS. Recipients may alternatively use standard e-mail clients supporting SSL client authentication to retrieve messages from the MS.

6. The delivery agent timestamps and countersigns the NRR evidence with an AdES. It the returns the evidence to either the sender's e-mail address or a Web service provided by the sender's UA. If a recipient does not retrieve the message within one week, the delivery agent returns a non-delivery evidence (negative NRR) back to the sender.

To ease the take-up of certified electronic mail delivery by public agencies, the Austrian e-Government initiative provides the application Modules for Online Applications - Electronic Delivery (MOA-ZS)[14]. MOA-ZS is a middleware, which has well-defined Web service interfaces and can thus easily be integrated into existing governmental back-end applications to connect to the Austrian DDS. The main task of MOA-ZS is to bundle the following complex tasks into one single interface.

- Addressing of recipient(s) by querying the CLS.
- Optional signing of documents (implicit provision of an NRO evidence).
- Optional encryption of the MIME container on the transport layer (if the recipient has defined an X.509 encryption certificate).
- Delivery of (encrypted) message to the delivery agent of choice.
- Processing of incoming NRR evidences.

The Austrian governmental 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 such a widely-deployed system. A governmental system, which is going to

[14]Software and documentation of MOA-ZS are published as open source and are freely available from the open source platform "Digital Austria". See `http://egovlabs.gv.at` for more information.

be shared with the private sector, inevitably raises additional requirements 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 TTPs. 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. Tauber and Rössler [2010b] and Tauber et al. [2011b] have discussed security issues of privacy and trust in the Austrian governmental CMS, which is shared and used by both the public and private sectors. They show how a governmental addressing scheme based on the national identification number may also be used in a privacy-preserving manner by the private sector. To achieve this, the CMS defines an additional trust domain, which is made up of the CLS and is fully supervised by the government. This trust domain ensures privacy by hiding the national identification number from business entities. Moreover, this model can be exploited to provide a technical supervision of TTPs concerning reliable charging. This is achieved by means of cryptographic tokens serving as digital postmarks. A brief overview of the rationale behind this shared system is given by the author in [Tauber and Reichstädter, 2010].

So far, just a small portion of Austrian citizens is registered for electronic delivery and printed documents are still dominating the world of delivery. In order to encourage public agencies to connect their services to the Austrian DDS, the Austrian e-Government initiative has developed the hybrid mail concept of "Dual Delivery". This concept follows the fire-and-forget pattern allowing all kinds of deliveries to be carried out over one single interface. If a recipient cannot be found querying the CLS, the document will be printed out and delivered using other channels, for example postal mail delivery. Dual delivery is an integral component and functionality of the middleware MOA-ZS.

4.2.2 PEC (Italy)

The Posta Elettronica Certificata (PEC) is the Italian national CMS for both the public and private sectors. The legal basis for the PEC is laid down by the presidential decree °68 [Il Presidente della Repubblica, 2005a], which was enacted on 11th February 2005[15]. A decree of 6th May 2009 [Il Presidente del Consiglio dei Ministeri, 2009] provided the basis for the allocation of free PEC mailboxes for all Italian citizens[16]. With law °2 [Parlamento Italiano, 2009], which was enacted on 28th January 2009, the registration of a PEC mailbox was rendered compulsory for all companies, freelancers and public administrations. The decree °266 of 2th November 2005 [Repubblica Italiana, 2005a] provides the basic technical rules of all aspects of the PEC system. Its annex [Repubblica Italiana, 2005b] provides the detailed technical specifications for all PEC communications. These technical specifications are maintained by the national IT center of the public administration (DigitPA)[17].

Architecture Figure 4.3 illustrates the PEC architecture, which has been discussed by Gennai et al. [2005]. The system is layered on top of the Internet e-mail architecture and operates according to the e-mail standard IETF Standards Track RFC 2822 [Resnick, 2001]. So-called PEC providers ensure strong fairness by acting as an inline TTP between senders and recipients. PEC providers have to be accredited by DigitPA for compliance with given technical and organizational requirements. So far, 25 providers have been officially accredited[18]. The PEC terminology defines three main services that a provider has to implement: Access Point (AP), Reception Point (RP) and Delivery Point (DP). The AP provides an MTA to forward submitted messages to other MTAs. The RP and DP can be seen as two

[15] With decree °82 [Il Presidente della Repubblica, 2005b] of 7th March 2005 all public agencies were commanded to use PEC as for communications with citizens, businesses and administrations. A directory of all public agencies having a PEC mailbox can be found under `http://www.paginepecpa.gov.it`.

[16] Italian citizens can apply for a free PEC mailbox at `https://www.postacertificata.gov.it`.

[17] `http://www.digitpa.gov.it`.

[18] The public directory of accredited providers can be found at `http://www.digitpa.gov.it/pec_elenco_gestori`

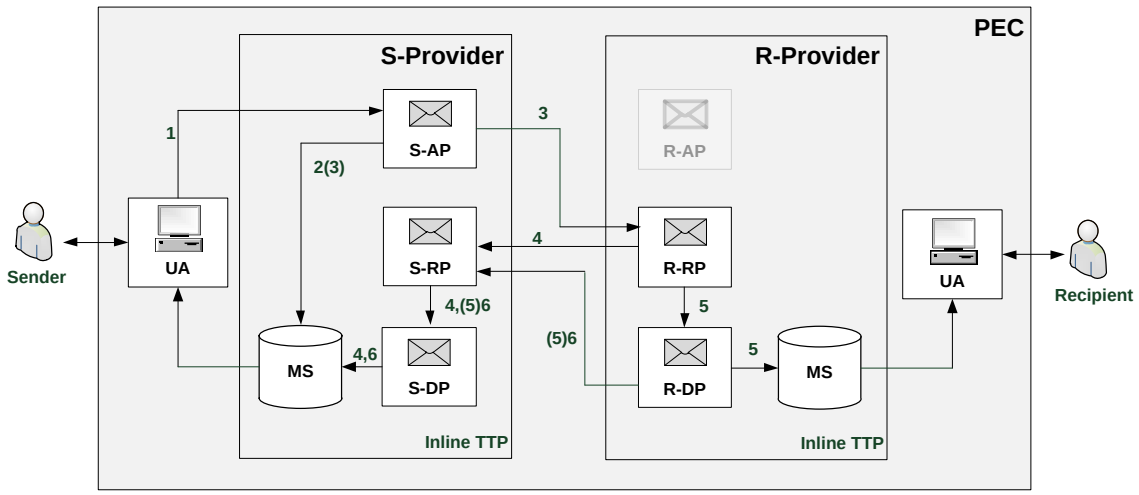

Figure 4.3: Architecture and protocol steps of the Italian Posta Elettronica Certificata (PEC) system

logical units of the recipient's MTA, where the RP accepts the message from the sender's MTA and the DP stores the message into the recipient's MS.

In contrast to the Austrian DDS, both senders and recipients must register an account with a PEC provider. The PEC standard does not make any assumptions about the communication protocol between senders/recipients and providers. However, most providers have interfaces that are accessible by standard mail clients or Web browsers. For such interfaces, the standard defines the minimum security requirements for authentication and confidentiality, for example, username/password combined with a TLS connection. However, the inter-provider communication, evidence signatures and formats are specified in detail by the PEC specifications. Providers must sign all messages and evidences according to the S/MIME v3 Cryptographic Message Syntax standard as defined in Housley [2009] using (at least) an AdES according to the EU Signature Directive. For the following protocol description, all provider services are preceded by a prefix indicating if the service is related to the sender's or recipient's provider, for example, S-AP, R-DP, etc.

CMS protocol The PEC protocol steps are illustrated in Figure 4.3.

1. The sender's UA authenticates against the S-AP and submits the message to the S-AP (MTA). The message may optionally be signed by the sender to provide an NRO evidence, for example, by applying an S/MIME signature.

2. The S-AP performs validity checks on the message, for example, to see if all recipients are PEC participants. If all checks pass, the S-AP stores an NRS evidence into the sender's MS. In all other cases, for example, if the message contained a malicious software or did not conform to the RFC 2822 format, a non-acceptance evidence (negative NRS) is generated and stored into the sender's MS for later retrieval.

3. The S-AP wraps the sender's original message together with some additional meta-data (in XML format) into a new, signed RFC 2822 envelope and forwards it to the R-RP using SMTP as defined in RFC 2821 [Klensin, 2001]. If the R-RP does not acknowledge this message with a take-in-charge evidence (see next step) within the next 12 hours, the S-AP stores a non-delivery-to-RP evidence (negative NRD) into the sender's MS for later retrieval.

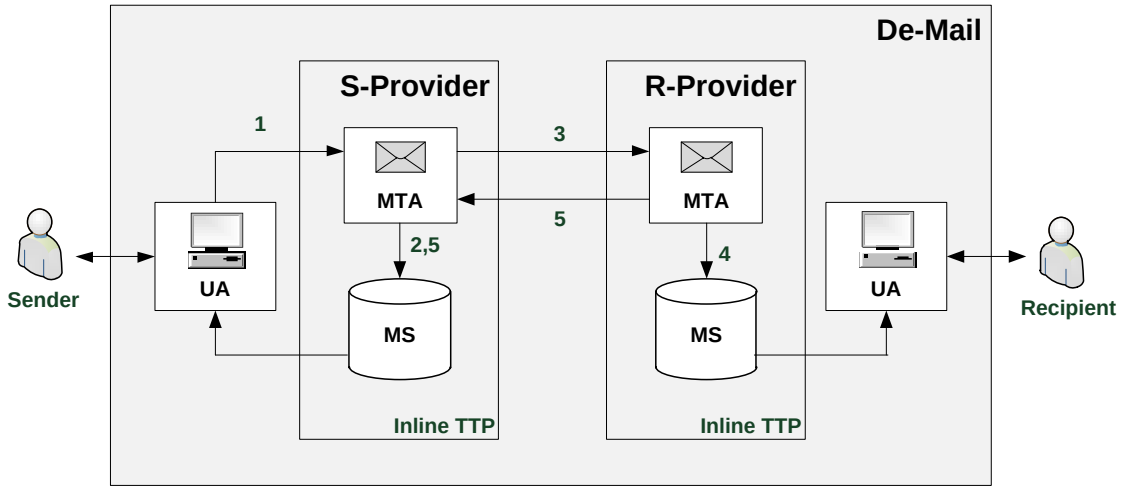

Figure 4.4: Architecture and protocol steps of the German De-Mail system

4. The R-RP checks the incoming envelope for formal correctness and verifies the digital signature of the S-AP. If the message is valid, a take-in-charge evidence (a kind of pre-NRD) is returned to the S-RP, forwarded to the S-DP and stored into the sender's MS for later retrieval.

5. Then, the R-RP forwards the message to the R-DP. In case of an error, for example, the R-DP detects malicious software within the message, a non-take-in-charge evidence is returned to the S-RP, forwarded to the S-DP and stored into the sender's MS for later retrieval. The R-DP unpacks the original message and stores it into the recipient's MS for later retrieval.

6. If this 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 for later retrieval. In all other cases, a non-delivery evidence (negative NRD) is returned.

4.2.3 De-Mail (Germany)

De-Mail is a recent project of the German government with the aim of providing a reliable, evidential and legally binding communication infrastructure for administrations, businesses and citizens. A prototype of the system was successfully piloted in the German city of Friedrichshafen between October 2009 and March 2010[19]. The "De-Mail law" (also called Citizen Portals Law) was enacted on 2th May 2011 and defines the organizational and legal regulations for the provision of De-Mail services. The technical specifications of De-Mail are published and maintained by the Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik (BSI)) [BSI, 2011].

Architecture Security aspects of the De-Mail architecture are discussed by Dietrich and Keller-Herder [2010] and Rossnagel et al. [2009]. Like the Italian PEC, De-Mail is also layered on top of the Internet e-mail protocol. So-called De-Mail providers ensure strong fairness by acting as inline TTP between senders and recipients. De-Mail providers have to be accredited by the BSI for compliance with given technical and organizational requirements to ensure a high level of reliability, data security and privacy. Both senders and recipients have to register a mailbox with a De-Mail provider. Like other "de-jure" systems, De-Mail puts emphasis on highly authenticated and identified participants. Registration

[19] http://www.fn.de-mail.de

is thus based on a qualified identification procedure, for example with an official ID document or the national eID. A De-mail address having the format givenname.familyname.number@providername.de-mail.de is assigned to each registered participant. Usage of clearly recognizable pseudonyms is also allowed.

The technical concept distinguishes between two types of communication channels having different security requirements: the communication between end-entities and their De-Mail provider and the inter-provider communication between De-Mail providers. Inter-provider communication is based on SMTP and a secure TLS connection. User authentication must be based on encrypted channels, for example a TLS-based connection. De-Mail defines two authentication levels: normal and high. The normal level corresponds to username/password based authentication. High-level authentication must be based on two-factor mechanisms like an additional mTAN or a smartcard, for instance the German eID. Providers have to offer at least Web-based access (HTTPs) in terms of a Web mailbox. They may also provide access for mail clients as a value-added service. The system architecture provides encryption between all communication nodes, but E2EE is not compulsory. This is an often criticized aspect (cf. Lapp [2009] and Lechtenbörger [2010]). 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. For the CMS protocol description only the certified mail quality is considered.

CMS protocol Figure 4.4 illustrates the protocol flow of the De-Mail certified mail quality.

1. The sender's UA authenticates at it's De-Mail provider and submits the message to the MTA using a secured channel. If the sender authenticates with the highest quality, this circumstance may be expressed by instructing the provider to flag the message accordingly. The message may also be encrypted for the recipient (E2EE) and/or digitally signed using a Qualified Certificate (QC) to provide an NRO evidence.

2. The sender's De-Mail provider checks the message for correctness (existing recipient, headers, meta-data, etc.) and stores an NRS evidence into the sender's MS for later retrieval. This evidence includes the hash value of the original message and a timestamp. The De-Mail standards recommends to sign NRS evidences with an HSM.

3. The sender's provider encrypts the message with its own public key and the public key of the recipient's provider and forwards the message to the recipient's MTA.

4. The recipient's MTA takes the message in charge, decrypts and checks the message and puts the message into the recipient's MS for later retrieval. If the sender has flagged the message as "restricted delivery", the recipient can fetch the message only with the highest authentication quality.

5. 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 for later retrieval. Like the NRS evidence, the recipient's MTA is recommended to sign the NRD with an HSM.

4.2.4 moja.posta.si (Slovenia)

Moja.posta.si is a private business CMS operated by the Slovenian Post. It aims at serving all kinds of secure and reliable transactions between public administrations, businesses and citizens. Because Slovenia does not have a dedicated law for CEM, the system is based on a contractual basis between the

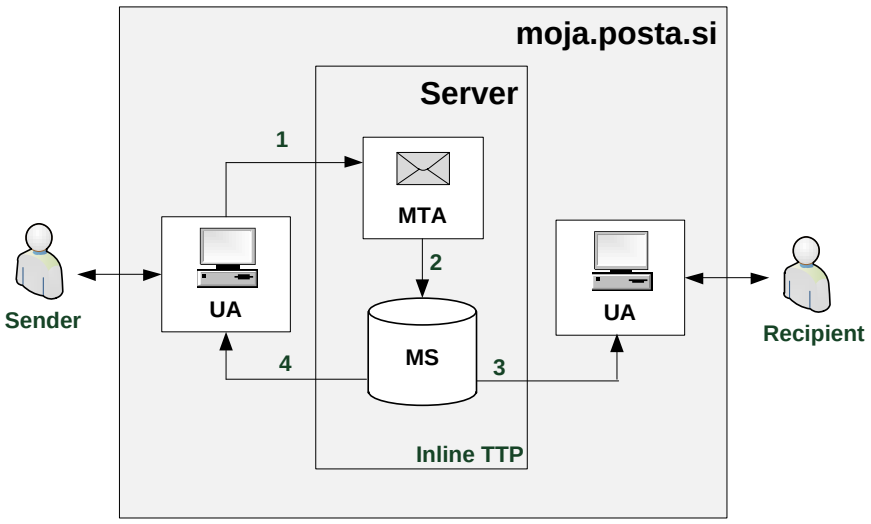

Figure 4.5: Architecture and protocol steps of the Slovenian CMS moja.posta.si

operator and its customers. A certain legal binding is established through the use of QCs by means of binding mailboxes to physical persons as a result of the legal equivalence between QES and handwritten signatures.

Architecture The architecture of moja.posta.si is illustrated in Figure 4.5. The CMS is operated on a single Web server acting as an inline TTP between senders and recipients. This is the simplest kind of architecture one can find in today's CMS ecosystem. Due to the single provider system, there is no need for message routing and inter-provider exchange of messages and evidences. Moja.posta.si runs on a platform based on Internet Information Server (IIS) and ActiveX technology. Therefore, only Microsoft Internet Explorer (IE) is supported as a UA so far. Authentication of senders and recipients is based on SSL client authentication with QCs. Certificates are issued by the Posta®CA, the official CA of the Slovenian Post, which meets national and European regulations for issuing QCs. Besides browser-based UA access, the system provides a Web service interface for business access to enable the automated submission and retrieval of messages. This interface is based on standardized Web Services (WS) technologies using SOAP. In contrast to most other CMS, moja.posta.si allows recipients to be addressed in multiple ways: either with the official Slovenian tax number or with the recipient's "@moja.posta.si" mailbox account address.

CMS protocol Figure 4.5 illustrates the protocol flow of a standard delivery transaction within the Slovenian CMS.

1. The sender's UA submits a message to the central MTA. In case of end users, this is conducted by authenticating at the Web site using Microsoft IE with SSL client authentication. The message must be signed with an ActiveX plugin using the QCs before it can be submitted. In case of sending applications, Web service clients acting as UA may submit messages to the Web service interface of the central MTA. Authentication is hereby ensured through SSL client authentication and NRO evidences by requiring sending applications to sign the message content using an AdES.

2. The MTA checks the incoming message, adds a timestamp by signing the message with an AdES and stores the message into the recipient's MS.

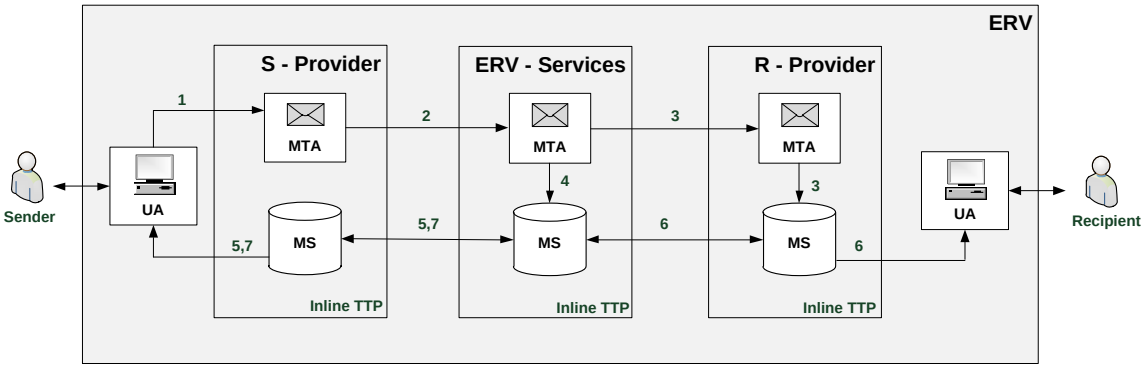

Figure 4.6: Architecture and protocol steps of the Austrian ERV

3. In case the recipient has provided a notification address, for example a standard e-mail address, a notification informs the recipient that a message is ready to be retrieved. The recipient's UA authenticates against the MS in the same way as the sender with the MTA in step 1 and retrieves the message. From a GUI perspective, the MTA and the MS run within the same environment.

4. If the sender has requested an NRR evidence, the MS creates an XML NRR evidence upon message retrieval and adds a timestamp by signing the evidence with an XML Advanced Electronic Signature (XAdES) signature. This evidence is stored into the sender's MS for later retrieval.

4.2.5 ERV (Austria)

The Electronic Legal Communications (ERV) is the official Austrian e-Justice system providing a secure, reliable and legally-binding communication infrastructure in judicial matters between end users, courts and the departments of public prosecution, respectively. The ERV is based on the official decree Bundesgesetzblatt (BGBl) 481/2005 [Republik Österreich, 2005], which was enacted on 30th December 2005[20]. The technical specifications [Ornetsmüller and Dreer, 2011] are maintained by the Austrian FCC.

Architecture The architecture of the Austrian ERV is illustrated in Figure 4.6. Core parts of the ERV architecture are the so-called ERV Services. This is a collection of MHS Web services, which are centrally operated by the FCC and act as inline TTP between ERV providers. ERV providers ensure strong fairness by acting as inline TTP between senders and recipients. The conceptual model of the ERV is very similar to the Austrian DDS. The lack of a domain-name based addressing model and the application of a numeric values-based addressing scheme requires a central instance to establish the mapping between users and ERV-providers. In contrast to the Austrian DDS, where the central lookup service acts as a kind of online TTP, the ERV services instance act as completely inline TTP by providing an MTA and a MS. ERV providers must be accredited by the FCC for compliance with given technical and organizational requirements. Several private businesses have been accredited as ERV providers for end users like lawyers and notaries. Other ERV providers are hosted by the Ministry of Justice to connect Austrian courts and the departments of public prosecution to the ERV. The ERV services platform also hosts an internal ERV provider so that other end users like police stations, which are not registered with an official ERV provider, can use and participate in the system.

[20]The decree was last amended in 2009 with BGBl 343/2009 [Republik Österreich, 2009]

CMS protocol Figure 4.6 illustrates the protocol flow of a standard ERV delivery transaction.

1. The sender's UA submits a message (either an XML document or binary content) to the MTA of its ERV provider.
2. The MTA proofs the message for correctness, adds a timestamp and forwards the message to the MTA of the ERV services platform.
3. Like in the step before, the ERV services MTA also proofs the message for correctness and checks whether the recipient has a valid account. The MTA then forwards the message to the MTA of the recipient's ERV provider, which stores the message into the recipient's MS.
4. Depending on the result of this operation and the checks in the previous step, the MTA of the ERV services generates a positive or negative NRD and stores it into the ERV services MS of the sender's ERV provider.
5. The sender's ERV provider pulls its ERV services MS in regular intervals and stores a fetched NRD evidence into the sender's MS for later retrieval.
6. As soon as the recipient retrieves the message from her MS, the ERV provider generates an NRR evidence and forwards it to the ERV services MS.
7. Like in step 5, the sender's ERV provider pulls its ERV services MS in regular intervals and stores a fetched NRR evidence into the sender's MS for later retrieval.

4.2.6 Other CMS

In the European and international context, several other CMS have been provided on the Internet by public administrations, postal operators and private businesses. A brief overview of selected systems is given in the remainder of this section. Specifications and details about the architecture and functionality of the described CMS are not publicly available. An exception is the German e-Justice system, which is based on the Online Services Computer Interface (OSCI) standard that is discussed in detail below. The following list of systems makes no claim of being complete, because there are most likely systems out there, which are operated by private businesses and not known to the author of this thesis.

4.2.6.1 Systems Provided by Postal Operators

This section briefly reviews the following CMS:

1. The German E-Postbrief
2. The Swiss IncaMail
3. The Spain Apartado Postal Electrónico
4. The Canadian PosteCS

Germany: E-Postbrief

Since July 2010, the German Post provides a CMS called "E-Postbrief"[21]. The E-Postbrief architecture is almost equal to moja.posta.si. The service can be accessed using standard Web browsers and

[21] http://www.e-post.de

runs on a central Web server acting as inline TTP between senders and recipients. Recipients can register a certified mail address ending with "@epost.de". Businesses can register a respective subdomain. Like De-Mail, the system supports two different authentication levels. Standard authentication is based on username and password. Authenticated users are required to use a two-factor mechanism based on username, password and an mTAN. Senders can choose between two delivery qualities. The registered mail quality provides the sender an NRS and an NRD evidence. The certified mail quality provides the sender an NRS evidence and requires the recipient to generate an NRR evidence. Recipients can decide whether to accept or reject a message. To accept a message with certified mail quality, recipients must be authenticated with an mTAN. In case a recipient rejects the acceptance of a message, the message will immediately be deleted from the server and a corresponding (negative) NRR is stored into the sender's MS. E2EE is not foreseen. Users can, however, provide a public key so that messages are stored in an encrypted form within the MS. The key may also be made available through an address register, so that senders may use encryption on a document level. The use of QES is currently not supported. However, the integration of that functionality is foreseen in the near future. Like the moja.posta.si Web service interface for business access, E-Postbrief provides a so-called Business Client Gateway (BCG), which can tunnel corporate e-mail services based on Microsoft Exchange or Lotus Notes through a Virtual Private Network (VPN) to the E-Postbrief system. A major hallmark of the system is its hybrid registered mail functionality. In case the recipient is not registered with the system, the document is printed out and delivered using regular mail. Data privacy aspects of the German E-Postbrief are discussed in detail by Schulz [2010].

Switzerland: IncaMail

The Swiss Post operates a CMS service called "IncaMail"[22]. INCA is the abbreviation for Integrity, Non-repudiation, Confidentiality, and Authentication. The CMS architecture is very similar to moja.posta.si and E-Postbrief and runs on a central Web server acting as inline TTP between senders and recipients. In contrast to the CMS reviewed so far, IncaMail also allows for sending certified mails to standard e-mail users. Senders must be registered with the IncaMail system and may use the Web mail GUI or standard mail clients with an IncaMail plugin. In case the recipient is a registered IncaMail user, the process is the same as for E-Postbrief and the sender receives an NRS and NRR evidence by means of a signed PDF file. However, if the recipient is a standard e-mail user, IncaMail applies its patented Secure Attached File Encryption (SAFE) technology to provide the NRR evidence. SAFE encrypts the message with a secret key stored on the IncaMail server, creates a notification message for the recipient and embeds the encrypted data within the Hypertext Markup Language (HTML) content of the notification. In this way, the sender's message must not be temporarily stored on the IncaMail servers. The recipient opens the attached HTML file, which posts the encrypted message data to the IncaMail servers for decryption. Now the recipient can decide whether to accept or reject the message, and the NRR evidence is returned to the sender. Besides access for end-users, IncaMail provides both a Web services (SOAP) and an SMTP gateway functionality for business customer access.

Spain: Apartado Postal Electrónico

The Spain postal operator Correos runs a CMS for its customers, which is called Apartado Postal Electrónico (APE)[23]. The service uses a central Web server acting as inline TTP between senders and recipients. The architecture is thus very similar to the postal systems discussed so far. However, the focus of the system is on digital signatures and encryption rather than on delivery evidences, such as NRD or NRR. Because this is a closed system, senders can visually see whether a message has been sent, but

[22] http://www.incamail.ch
[23] https://cep.correos.es

they do not actually receive any kind of transferable NRS evidence. NRO can be ensured by optionally signing the message with the own eID card or a software certificate using XAdES or Cryptographic Message Syntax Advanced Electronic Signature (CAdES) signature.

Canada: PosteCS

Canada Post offers, with its PosteCS system[24], a CMS that is similar to the Swiss IncaMail. The system runs on a central Web server acting as inline TTP between senders and recipients. Senders must be registered with PosteCS to submit messages to any recipient having a standard e-mail address. For each submitted message, the system generates a timestamp and provides the sender with an NRS evidence. In contrast to the IncaMail SAFE technology, PosteCS temporarily stores the sender's message on the server and only sends a notification mail to the recipient including a download link for the message. The download is time-limited, and the sender may protect the download with a password, which must be shared between the sender and recipient out-of-band. If the message has been successfully downloaded, PosteCS generates an NRR evidence, which is returned to the sender.

4.2.6.2 Private Business Systems

This section briefly reviews the following CMS:

1. The Belgian CertiPost
2. The US RPost

Belgium: CertiPost

The "e-Delivery service" of the Belgian Certipost[25] is a CMS with legal value for both private businesses and public administrations. Certipost uses a similar architecture as the previously reviewed postal operator systems. A central Web server acting as inline TTP provides the fair, secure and reliable exchange of administrative and business documents between senders and recipients. The platform is going to soon implement the Registered Electronic Mail (REM) standard for interoperability. REM is a standard specified by the European Telecommunications Standards Institute (ETSI), which is discussed in the next sections. Only senders registered with the Certipost system can submit certified mail messages. After submission, the Certipost platform generates an NRS evidence, which is stored into the sender's MS. If the recipient is not a Certipost user, the system offers the hybrid mail option where the document is printed out and delivered to the recipient using traditional registered mail. In case the recipient is a registered Certipost user, the message is delivered into the recipient's MS. Recipients can decide whether to accept or reject a message. An NRR evidence certifying the recipient's decision is sent back to the platform, countersigned and timestamped by Certipost and stored into the sender's MS for later retrieval.

US: RPost Registered Mail

The RPost Registered Email system[26] is a CMS, which has a similar architecture as the postal operator systems introduced so far, this means, it uses a central Web server acting as an inline TTP. RPost holds the US patents 6182219, 6571334, 7240199, 7660989, 7693558, 7707624 and 7865557, which

[24] https://cpc.postecs.com
[25] http://www.certipost.be/ddsolutions/en/e-delivery-overview.html
[26] http://www.rpost.com

cover technologies of proof of submission and delivery. As in all other systems, senders must be registered with the RPost server. The service mainly focuses on confirming the delivery to standard e-mail users. After having submitted a message, the system generates a signed NRS evidence, which is returned to the sender. The RPost server delivers the message to the recipient and returns a signed NRD evidence to the sender by creating a delivery audit trail. This audit trail consists of transaction metadata of the communication between the RPost mail server and the recipient's mail server or user agent. It has to be noted that this is not an NRD evidence in terms of the CMS non-repudiation services, because the service relies on the assumption that the data provided by the recipient's mail system is correct.

4.2.6.3 Notary Systems

This section briefly reviews the following CMS:

1. The EuroNot@ries eWitness
2. The Norwegian eNotarius eNmail
3. The Spanish Certimail

EU: EuroNot@ries eWitness

The secure and reliable data processing service "eWitness" [27] was created by EuroNot@ries, an association of several notaries from different European countries. The goal of this system is the trustful notarial certification of electronic online transactions. eWitness provides the same functionality as RPost Registered Mail, this means it mainly takes care of the outbound communication. Besides a strong SSL client authentication of senders, eWitness provides a certified tracking record of submitted content and submission time. This record is signed by the eWitness server and returned to the sender as an NRS evidence. In a similar manner as RPost, eWitness tracks the SMTP traffic (audit trail) and returns an NRD evidence by means of a signed PDF document back to the sender. The evidential value of the NRD evidence is also questionable for the eWitness system. However, it is a core feature of this system that recipients should not notice the tracking of the e-mail conversation.

Norway: eNotarius eNmail

The eNotarius "eNmail"[28] service is a CMS having the same architecture and providing the same services as eWitness. A central Web server acting as inline TTP ensures strong fairness between senders and recipients. Besides the NRS and the "NRD evidence" by tracking the SMTP communication, eNmail provides, if requested by the sender, an NRR evidence with the same mechanism as the Canadian PosteCS system. The system can be used with standard e-mail clients and an additional plugin.

Spain: Certimail

The Spanish Certimail[29] service is a CMS having the same architecture and providing the same services as the Canadian PosteCS system. A central Web server acting as an inline TTP ensures strong fairness between senders and recipients by providing NRS and NRR (after successful download) evidences to the sender. The system can be used with standard e-mail clients.

[27] http://www.ewitness.eu
[28] http://www.enotarius.com
[29] http://www.certimail.es

4.2.6.4 e-Justice Systems

This section briefly reviews the following CMS:

1. The German EGVP
2. The Dutch Justitie Berichten Service (JUBES)
3. The Spanish Notificaciones Electronicas

Germany: EGVP

The German e-Justice system Elektronisches Gerichts- und Verwaltungspostfach (EGVP)[30] provides a reliable messaging infrastructure for law courts, public administrations, companies, lawyers and notaries. The system is based on the OSCI standard. OSCI ensures fairness by returning NRD and NRR evidences in exchange for a message. The OSCI standard is discussed in detail in the next sections.

Netherlands: JUBES

The Netherlands Justitie Berichten Service (JUBES)[31] is the official Dutch e-Justice system ensuring the reliable communication between administrative units of both the justice sector and police organizations. JUBES uses the Dutch Justice Standard for Asynchronous Messaging JAB (Justitiestandaard Asynchrone Berichtenuitwisseling), which is a profile of the Organization for the Advancement of Structured Information Standards (OASIS) Electronic Business Message Service Specification (ebMS) standard. ebMS is based on SOAP or SwA and provides an NRD evidence for the communication between two so-called Electronic Business XML (ebXML) Message Service Handlers (MSHs). Justitiestandaard Asynchrone Berichtenuitwisseling (JAB) extends ebMS with several security functions like digital signatures, encryption, NRO and NRR evidences. JAB can be carried over both HTTP and SMTP transport protocols.

Spain: Notificaciones Electronicas

The Spain Ministry of Public Administrations operates a CMS called "Notificaciones Electronicas"[32]. It is a Web portal acting as inline TTP and providing a certified mail service with legal value. Citizens can register a mailbox for free. However, the service can only be used to receive notifications from public administrations, not to send messages. Due to the legal binding, citizens can only register with their eID based on a QC. Because a recipient's mailbox is only accessible through a Web browser, an e-mail is sent to inform that a new notification is ready to be retrieved. After successful download or in case the notification is not retrieved within a certain period of time, a negative NRR evidence is returned to the sending public administration.

4.3 CMS Standards

To avoid the description of only concrete implementations, three international CMS standards are reviewed in order to evaluate the applied definitions and security properties considered necessary by standard designers. The following standards are reviewed:

[30] http://www.egvp.de
[31] http://www.justid.nl/images/JUBES_Informatievoorwaarden_v1%205_tcm54-306421.pdf
[32] https://notificaciones.060.es

1. ETSI Registered Electronic Mail (REM)
2. UPU Postal Registered eMail (PReM)
3. Online Services Computer Interface (OSCI)

4.3.1 ETSI Registered Electronic Mail (REM)

In 2008, ETSI published a first version of the REM standard TS 102 640 to ease interoperability and to prevent a heterogeneous CMS landscape across Europe. REM is primarily intended as an evidence standard to establish interoperability between different certified (Internet) e-mail domains operating under different policies. The five parts of the REM standard, which have also been discussed by Ruggieri [2010], are as follows:

1. ***Part 1*** - Architecture [ETSI, 2010b]. This part describes the logical model of REM systems from an abstract point of view. It introduces roles, styles of operation, interfaces and main evidence types. A single REM system is called REM Management Domain (REM-MD) and acts as inline TTP between senders and recipients. A REM-MD consists of at least three core components: an MTA, a MS and an EP. REM supports two basic styles of operation: Store and Forward (S&F) and Store and Notify (S&N). Under the S&F style, messages are directly forwarded to the recipient (or the recipient's REM-MD MS), whereas the S&N style means that 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 [ETSI, 2010c]. The second part of the standard 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 like IDs, evidence event, version, timestamps, policy ID, issuer details, sender details and recipient details. To ease interoperability between different REM-MDs, the standard maps REM evidences to basic messaging-related events like submission/acceptance/rejection by a REM-MD (classifiable as NRS), relay to remote REM-MD, delivery/non-delivery to recipient (classifiable as NRD) or retrieval/non-retrieval/download/non-download by recipient (classifiable as NRR). The standard specifies three evidence formats: ASN.1, XML and PDF evidences. For each of these formats, the corresponding signature types are applied: Cryptographic Message Syntax signatures for ASN.1, XAdES for XML and PDF Advanced Electronic Signature (PAdES) for PDF. Part 2 of the specification also describes in detail the mechanisms for trust establishment between different REM-MDs with the ETSI TS 102 231 TSL standard [ETSI, 2009] for mutual recognition of trusted REM services.

3. ***Part 3*** - Information Security Policy Requirements for REM Management Domains [ETSI, 2010d]. Part 3 specifies the assessment of security requirements of REM-MDs being compliant to the ISO/IEC 27001 standard [ISO/IEC, 2005a]. Controls to mitigate security risks have to be selected according to the ISO/IEC 27002 standard ISO/IEC [2005b]. This part of the REM standard also defines the authentication mechanisms for senders and recipients. Authentication qualities may range from low levels (basic authentication using TLS) to high levels using QES based on Secure Signature Creation Devices (SSCDs) in conformance with the EU Signature Directive. To ease interoperability and the cross-border mutual recognition of evidences, signatures should be either an AdES or a QES.

4. ***Part 4*** - REM-MD Conformance Profiles [ETSI, 2010e]. The fourth part of the specification was added with the first revision of the standard in January 2010. It introduces two conformance profiles (basic and advanced) and specifies the mandatory requirements a REM-MD has to meet to be compliant with each profile.

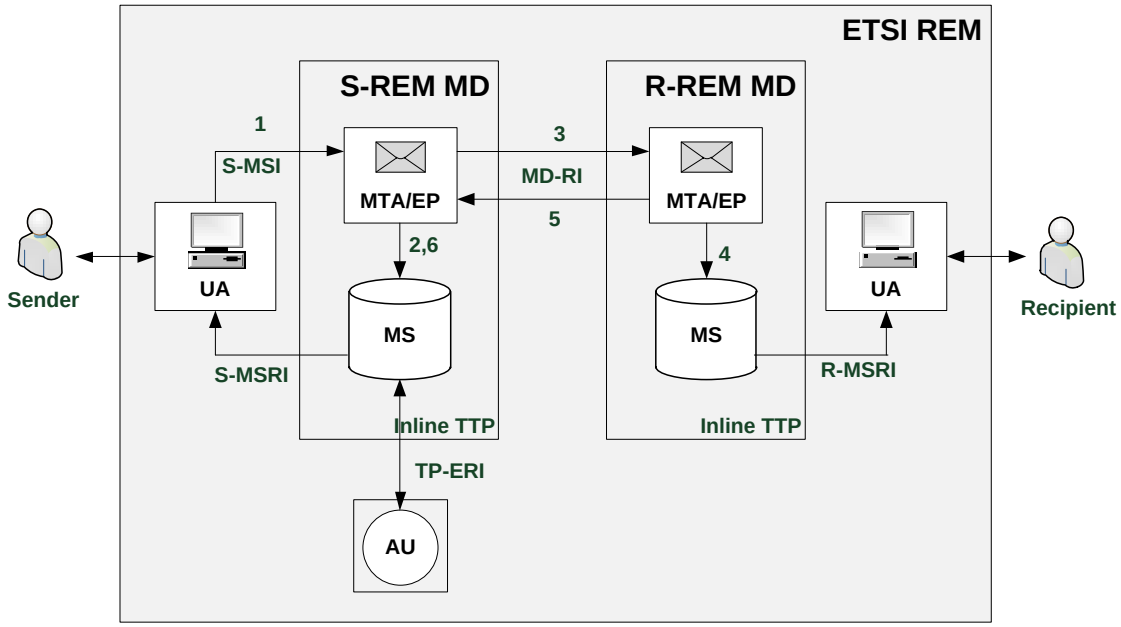

Figure 4.7: Architecture and protocol steps of the ETSI REM standard

5. ***Part 5*** - REM-MD Interoperability Profiles [ETSI, 2010f]. Part 5 of the specification profiles the standard to ease interoperability between different SMTP-based REM-MDs. Interoperability profiles for both REM dispatches and REM evidences are specified in detail.

Figure 4.7 illustrates the basic REM transport architecture. For simplification, the REM EP is shown together with the MTA. REM has a particular terminology for communication interfaces between entities, which is explicitly denoted in Figure 4.7.

CMS protocol The REM protocol steps in case of the S&F style of operation are illustrated in Figure 4.7.

1. 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).

2. The S-REM-MD EP may create an NRS evidence and store it into the sender's MS for later retrieval by the senders' UA through the Sender Message Store Retrieval Interface (S-MSRI).

3. The S-REM-MD MTA forwards a REM dispatch through the Management Domain Relay Interface (MD-RI) to the MTA of the recipient's Management Domain (R-REM-MD). The REM dispatch includes the sender's original message and may include also the aforementioned NRS evidence.

4. The R-REM-MD MTA stores the message into the recipient's MS for later retrieval by the recipient's UA through the Recipient Message Store Retrieval Interface (R-MSRI).

5. The R-REM-MD EP creates an NRD evidence and returns it back to the S-REM-MD MTA through the MD-RI.

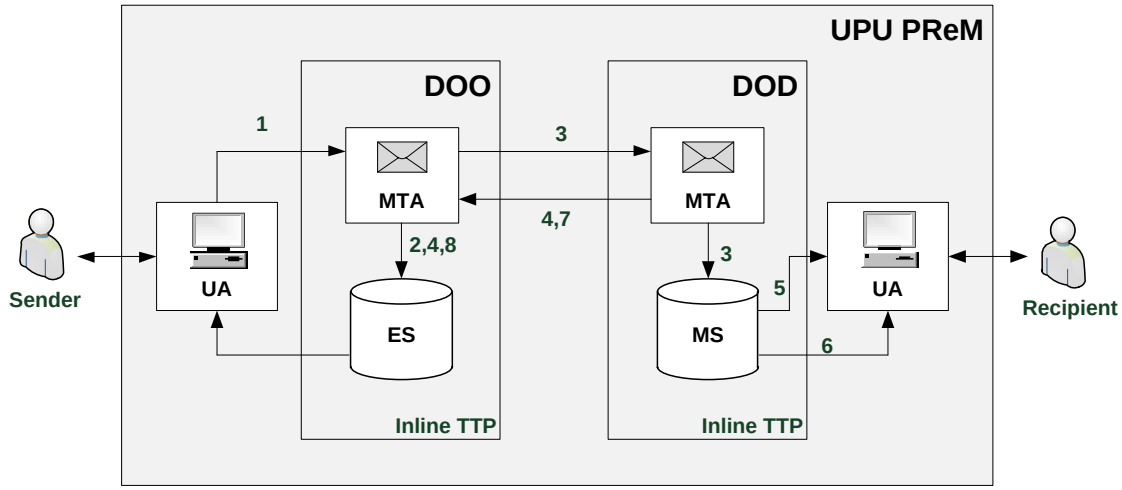

Figure 4.8: Architecture and protocol steps of the UPU PReM standard

6. The S-REM-MD MTA stores the evidence into the sender's MS for later retrieval by the sender's UA through the S-MSRI.

The discussed protocol flow illustrates the typical REM S&F style of operation. Depending on the REM implementation, several other components, actors, evidence types and message flows may be involved. Third parties, such as system components, TTP, arbiters or other users, may retrieve evidences from the MS through the so-called Third Party Evidence Retrieval Interface (TP-ERI).

4.3.2 UPU Postal Registered eMail (PReM)

To keep pace with the shift from traditional postal services to electronic communications, the UPU has published the specification for Postal Registered eMail (PReM) [UPU, 2008] to provide value-added REM services on the Internet.

Architecture A simplified version of the PReM architecture is illustrated in Figure 4.8. PReM services must be provided by designated operators, this means governmental or non-governmental entities officially designated by a UPU member country to operate postal services. Designated operators ensure strong fairness by acting as inline TTP between senders and recipients. PReM extends the UPU Secure electronic Postal Services (SePS) interface specifications [UPU, 2003]. The SePS standard was published in 2004 and specifies the application of Digital Postmarks (DPMs) [Miranda and Melo, 2004]. The term DPM was later renamed to Electronic Postal Certification Mark (EPCM). SePS is a SOAP-based protocol allowing clients to send documents to a postal operator, which signs and timestamps the document with an electronic signature. EPCMs can be verified by sending the "postmarked" document to a trusted postal operator supporting SePS. Concepts, schemas, operations and the SePS EPCM service are standardized under CEN/TS 15121 [CEN/TS, 2010a,b]. EPCMs only ensure integrity and authenticity of documents. The exchange of documents between different entities is out of scope of the specification. PReM extends SePS by specifying an additional layer for the fair and evidential document exchange. For this purpose, PReM adopts the ETSI REM XML evidence format and introduces five additional SePS SOAP operations to exchange messages and evidences between end-entities and postal operators.

CMS protocol The PReM protocol steps are illustrated in Figure 4.8.

1. The sender's UA submits a message to its Designated Operator of Origin (DOO) MTA using the XML-based SePS protocol. The UA can either be a Web browser or e-mail client with a PReM plugin. The UA may sign (NRO evidence) and optionally encrypt (E2EE) the message.
2. The DOO checks the message and verifies if the recipient's operator - the Designated Operator of Destination (DOD) - is trusted, this means it is a UPU member. The acceptance/rejection status of the message is stored as NRS evidence into the sender's Evidence Store (ES) for later retrieval.
3. The DOO MTA creates a PReM dispatch holding the sender's original message, generates an EPCM for proof of receipt and signs it for proof of origin. The DOO MTA authenticates against the DOD MTA and delivers the dispatch. The DOD MTA verifies the signature, generates an EPCM for proof of receipt and stores the dispatch into the recipient's MS.
4. The DOD MTA creates a take-in-charge evidence and returns it to the DOO MTA, which stores it into the sender's ES.
5. The recipient is notified that a new message can be retrieved from the MS.
6. The recipient's UA authenticates against the DOD MS and retrieves the message.
7. If the recipient does not retrieve the message within a certain period of time, the DOD MTA returns a "message expiration evidence" (negative NRR) back to the DOO MTA. Otherwise, an NRR evidence is returned back to the DOO MTA.
8. The DOO MTA stores the incoming evidence into the sender's ES for later retrieval.

4.3.3 Online Services Computer Interface (OSCI)

OSCI is a standard for secure and reliable messaging. The standard is primarily used in the context of e-Government applications by German virtual post offices [Planitzer and Weisweber, 2007; Maseberg et al., 2008] to reliably exchange encrypted and digitally signed messages between public administrations. One of the most popular examples is the German e-Justice system called Elektronisches Gerichts- und Verwaltungspostfach (EGVP). OSCI was designed for interoperability and to serve arbitrary business scenarios. The technical specifications are maintained by the OSCI Steering Office [OSCI Steering Office, 2009].

Architecture The OSCI communication architecture is based on Web services. The message structure conforms to SOAP (version 1.2), and attachments are carried using the SOAP Message Transmission Optimization Mechanism (MTOM). OSCI mainly operates on the SOAP header block, the communication data. The content data (SOAP body) is encrypted and out of scope of the specification. Figure 4.9 illustrates the architecture of the OSCI standard. The standard defines the secure messaging between delivery agents (so-called OSCI gateways) acting as inline TTP between senders and recipients to ensure the fair, secure, reliable and traceable message exchange [Apitzsch, 2007]. The communication between end-entities (sender, recipient) and OSCI gateways is out of scope of the standard. Gateways act as SOAP endpoints and inter-gateway authentication is based on X.509 certificates, PKI, Web Services Trust Language (WS-Trust) [Nadalin et al., 2007] and Web Services Federation Language (WS-Federation) [Lockhart et al., 2006]. The authentication strength depends on the concrete business scenario. Gateway policies and supported functionalities must be exposed in a formal description using the Web Services Description Language (WSDL) standard [Chinnici et al., 2007]. OSCI supports both synchronous and asynchronous communications between senders and recipients. As synchronous communications are hard to carry out (sender and recipient have to stay always online), OSCI defines so-called Message Box

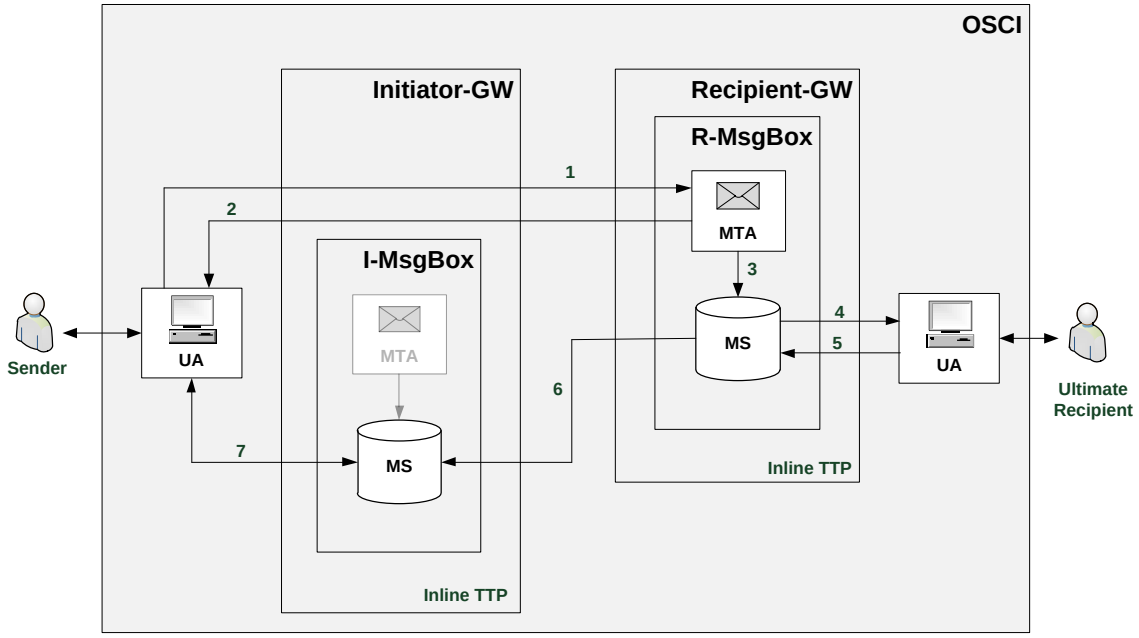

Figure 4.9: Architecture and protocol steps of the OSCI standard

Service Relays (MsgBoxs) to preserve messages for end-entities in an asynchronous communication. A MsgBox also serves as an MTA to enable the communication between end-entities and other OSCI gateways. In case of the sender's MsgBox, the gateway is called "Initiator", and in case of the recipient's MsgBox, it is called "Recipient". The OSCI standard has thus defined the nomenclature ultimate recipient, which is aligned to the definition of the ultimate receiver defined in the SOAP 1.2 specification. Because synchronous and asynchronous message flows only differ in the intermediary MsgBox nodes, this thesis only reviews the asynchronous mode. The discussion is simplified by just taking the case with two gateways into consideration and omitting message exchanges with other third parties, for example, security token services. An OSCI message exchange may include additional intermediary gateway nodes between the sender's and the recipient's gateway. However, this does not affect the basic protocol flow.

CMS protocol The OSCI protocol steps are illustrated in Figure 4.9.

1. The sender's UA wraps the content of the message into a SOAP body and transmits the message directly to the MTA of the Recipient MsgBox. E2EE may be chosen to enable confidentiality. Identification and authentication takes place using WS-Trust and Security Token Services (STSs).

2. The UA can request an NRD evidence, which has to be returned synchronously in the network backchannel by the recipient's MsgBox MTA in the SOAP header. This evidence consists of an XML Digital Signature (XMLDSig) [Bartel et al., 2008] with a reference to the SOAP body block, the signature time and any address data.

3. The recipient's MsgBox MTA stores the message into the recipient's MS for later retrieval.

4. The ultimate recipient's UA pulls the message from the MsgBox service.

5. If requested by the sender, the ultimate recipient's UA returns a signed NRR evidence to the recipient's MsgBox MS. This evidence is structurally similar to the NRD evidence. The main difference is that it must contain a reference to the decrypted content.

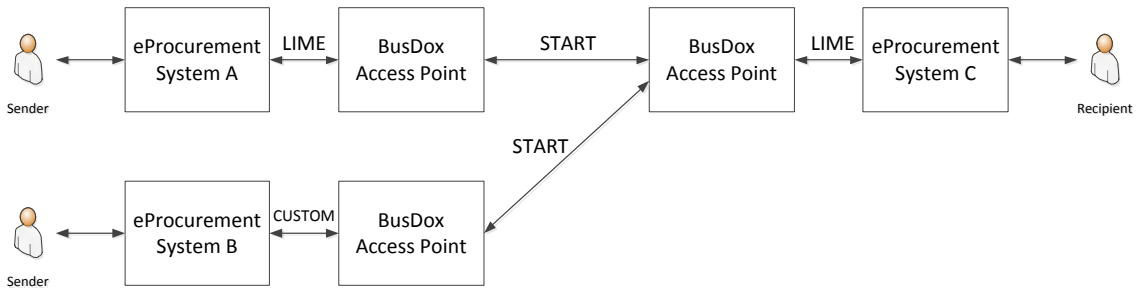

Figure 4.10: Four corner model of the BusDox architecture

6. The evidence is forwarded by the recipient's MsgBox MS as SOAP payload to the sender's MsgBox MS.

7. The sender's UA can subsequently pull the NRR evidence from its MsgBox MS.

4.3.4 Other Standards

In the European context, several other standards have emerged in the last several years. They are all used in the context of business document exchange and profile the WS-* protocol family to provide secure and reliable messaging on the transport level. They do not have the classic evidential transferability based on digital signatures as it is known for most CMS provided on the Internet. This section briefly reviews the following standards:

1. The Danish Reliable Asynchronous Secure Profile (RASP)

2. The Pan-European Public Procurement Online (PEPPOL) Business Document Exchange Network (BusDox)

3. The French Protocole d'Echanges Standard et Ouvert (PRESTO)

4. The Estonian X-Road

4.3.4.1 Reliable Asynchronous Secure Profile (RASP)

RASP is a profile of the WS-* standards family developed by the Danish National IT and Telecom Agency [2007]. This agency provides and controls a national service registry so that RASP is already broadly used in Denmark. The primary goal of RASP is to provide a platform for the reliable and secure business document exchange. Besides the synchronous messaging using SOAP over HTTPs, RASP supports an asynchronous reliable messaging based on SMTP and the Web Services Reliable Messaging (WS-ReliableMessaging) standard [Davis et al., 2009]. As a consequence, RASP only provides reliable messaging on the transport level and does not support transferable evidences as known from other CMS.

4.3.4.2 Business Document Exchange Network (BusDox)

One of the aims of the European LSP PEPPOL is to establish an exchange platform for the pan-European public Electronic Procurement (e-Procurement). SMEs, in particular, should benefit from a harmonized way to communicate with European governmental institutions. For this reason, the PEPPOL consortium published a set of specifications for a pan-European communication network called BusDox. The specifications are based on a so-called "four corner model", which defines national APs for cross-border

communication. The four corners are: sender, sender's AP, recipient's AP and recipient. This model is illustrated in Figure 4.10. Within the national scope, companies and governmental agencies communicate with the APs either via proprietary interfaces or via the PEPPOL Lightweight Message Exchange Profile (LIME) protocol [Fremantle, 2009a]. AP communicate with each other via the Secure Trusted Asynchronous Reliable Transport (START) protocol [Fremantle, 2009b]. START is based on the Web Services Transfer (WS-Transfer) [Davis et al., 2010] and WS-ReliableMessaging technology and has many similarities with the Danish RASP. This results from Danish experts bringing in experience from RASP and contributing to the BusDox specification. With the four corner model, a local company can reliably transmit a document to a foreign governmental institution through the AP network without having to care about protocols and interfaces in the foreign Member State. Like RASP, BusDox also does not provide transferable evidences as known from most other CMS.

4.3.4.3 Protocole d'Echanges Standard et Ouvert (PRESTO)

The French PRESTO is a specification profiling several Web service specifications of the WS-* protocol family. Like RASP and BusDox, also PRESTO uses WS-ReliableMessaging to provide the secure and reliable message delivery [DGME, 2006]. A first version of PRESTO was based on HTTPs only. Meanwhile the standard also supports other bindings like SMTP and FTP.

4.3.4.4 X-Road

The Estonian X-Road [X-Tee, 2005] standard was published in 2001 with the aim at connecting different national governmental databases, institutions and individuals. Like the data exchange standards presented before, X-Road is also based on Web services standards. Authenticity, integrity and confidentiality are implemented as basic security mechanisms. Transferable evidences are also not supported. However, all transactions within the X-Road system are logged and cryptographically secured if needed for dispute resolution.

4.4 Evaluation

This section evaluates which CMS properties found in the literature are actually applied in practice. Several CMS standards and systems are evaluated according to their architecture and protocol flows to identify the classification properties. Below, findings in relation to the design decisions of system architects versus the current trends in research are discussed.

4.4.1 Evaluation Criteria

In the preceding chapter most CEM security properties have been introduced and discussed regarding their practical relevance. Therefore, the following CEM security properties have been selected as evaluation criteria when comparing different systems and standards.

1. Non-repudiation services (NRO, NRR, NRS, NRD and evidence transferability)
2. Fairness (strong, weak, true, light, probabilistic)
3. TTPs (inline, online, offline, no TTP, transparency, verifiability)
4. Communication channel (operational, resilient, unreliable)
5. State storage (strong stateless, weak stateless, weak stateful, strong stateful)
6. Confidentiality (regarding E2EE)

7. Timeliness (asynchronous)

8. CMS policy (de-Jure, de-facto)

Most protocols are published from a conceptual and scientific viewpoint and do not actually refer to certain implementation-specific details. However, especially for interoperability efforts, implementation-specific criteria and aspects may be of interest. For evaluation purposes, the criteria of transport protocols, certificate qualities and signature formats are also taken into account.

Transport Protocols CEM protocols usually just specify security properties, process flows and architectural building blocks from the message layer upwards. The CEM itself can be operated on top of any messaging or communication system. However, by nature CEM protocols are often associated with the e-mail protocol, which is based on SMTP. Even when having the same security properties and residing on the same network layer, for example TCP/IP, many CMS are not based on SMTP. A popular alternative is the use of Service Oriented Architectures (SOAs) to facilitate the automated processing of messages and evidences. The most prominent SOA implementation standard is SOAP over HTTPs. Systems and standards are also classified according to this criterion because different approaches may have different infrastructural requirements and are thus of interest when evaluating systems towards interoperability.

Certificate Qualities and Signature Formats Trust in systems and standards increases with a higher security level. Furthermore, it is highly recommended to increase trust in systems by increasing security rather than using trusted software (security by obscurity). This also holds for the application of electronic signatures. For instance, the same signature created with a HSM is more secure than a signature created with a software token since the private key is securely protected by an appropriate hardware layer. But how can the signature quality be classified? Even if evidence signatures applied in different CMS may have the same purpose and meaning on a semantic level, they are incompatible due to different formats, qualities and requirements. Few references provide a common understanding of electronic signatures. One of them is the EU Signature Directive 1999/93/EC [The Council of the European Union, 2000b], which provides a legal framework for the mutual recognition by defining AdESs and QESs. According to Article 2 of the Signature Directive, an AdES is an electronic signature, which meets the following requirements:

1. it is uniquely linked to the signatory;

2. it is capable of identifying the signatory;

3. it is created using means that the signatory can maintain under his sole control; and

4. it is linked to the data to which it relates in such a manner that any subsequent change of the data are detectable.

QES are defined as AdES based on a QC and created by an SSCD. The Signature Directive defines the requirements for QCs (Annex I), CAs issuing QCs (Annex II) and SSCDs (Annex III), respectively. According to the Directive, QES are legally equivalent to handwritten signatures throughout the EU. Therefore, when comparing different CMS, especially with respect to interoperability, certificate qualities and signature formats should be classified and evaluated. A clear definition of harmonized certificate qualities and signature formats is vital to ease the mutual recognition of evidences. Therefore, this section evaluates existing CMS and standards according to the used signature quality (AdES or QES).

CMS Name	DDS	PEC	De-Mail	SI-Moja	ERV	REM	PReM	OSCI
Country	Austria	Italy	Germany	SI Post	Austria	ETSI	UPU	OSCI
Standardization Body								Leitstelle
Non-repudiation services								
NRO	$\bullet_o$	$\bullet_o$	$\bullet_o$	•	$\bullet_o$	$\bullet_i$	•	•
NRR	•			•	•	$\bullet_i$		•
NRS		•	•			$\bullet_i$	•	
NRD		•	•		•	$\bullet_i$	•	•
Evidence Transferability	•	•	•	•	•	•	•	•
Fairness								
strong	•	•	•	•	•	•	•	•
weak								
true								
light								
probabilistic								
TTP								
Inline TTP	•	•	•	•	•	•	•	•
Online TTP								
Offline								
No TTP								
Transparent								
Offline Verifiability								
Online Verifiability	•	•	•	•	•	•	•	•
Communication Channel								
operational								
resilient								
unreliable	•	•	•	•	•	•	•	•
State Storage								
Strong Stateless								
Weak Stateless								
Weak Stateful	•	•	•	•	•	•	•	•
Strong Stateful								
Confidentiality (E2EE)	$\bullet_o$	$\bullet_o$	$\bullet_o$	$\bullet_o$	$\bullet_o$	$\bullet_o$	$\bullet_o$	•
Timeliness	•	•	•	•	•	$\bullet_i$	$\bullet_i$	$\bullet_i$

•= applied/supported $\bullet_o$ = optional $\bullet_i$ depending on the implementation

Table 4.1: Classification of CMS according to the security properties defined in literature

4.4.2 CMS Security Properties

Table 4.1 summarizes the properties of national CMS and standards according to different classification criteria. There seems to be a consensus on strong fairness being an essential requirement for CMS provided on the Internet. As in traditional postal systems, this appears to be a decisive acceptance criterion for users. Even if, in some e-Commerce scenarios, it might not be desirable to see the involvement of a TTP, there is the broad agreement that weak fairness is not acceptable and that true fairness is not desired. This is strongly related to the desired properties of TTP verifiability and evidence transferability, as is discussed below.

It is notable that all solutions - even those briefly discussed - use inline TTPs, whereas the research community is more and more focusing on offline solutions. Starting with inline TTPs in the early 1990s, research has moved to online TTPs in the mid-1990s and finally tended toward offline TTPs in the late 1990s. This trend remained unchanged up to the present day. So why do system architects and standard designers rely on inline solutions, although the research community tends to the contrary? To answer this question, first the drawbacks of inline TTPs should be highlighted and discussed how they are relativized in practice. The literature often argues that inline TTPs may become a bottleneck because of the amount of communicational and computational power needed. Of course, in practice, almost any amount of data can be processed with an appropriate infrastructure. For example, one just has to look at the most-frequented Internet sites, such as Facebook, Google or YouTube. From a communicational point of view, in practice, a CMS with inline TTPs does not need the full range of bandwidth of a traditional e-mail provider. Due to cost reasons, the number of certified mail messages is kept within limits, compared with standard e-mail. Moreover, CMS are usually free from SPAM, which often makes up more than 90% of regular e-mail traffic. In the case of inline TTPs, computational power is needed for cryptographic operations, such as message encryption or evidence signature generation. However, even in the case of hundreds of thousands or millions of CMS items a day, this can today be managed with off-the-shelf components. Most proposed protocols prefer online or offline solutions due to the reduced amount of trust that must be put in TTPs. In practice, this seems to be mitigated by the fact that de-jure systems require TTPs by law to undergo a technical and organizational accreditation. In many cases, this is emphasized by requiring an ISO 27001 Information Security Management System (ISMS) [ISO/IEC, 2005a] certification. In de-facto systems, the trust issue is somewhat mitigated by the fact that predominant CMS service providers are postal services, which usually enjoy a certain amount of trust from their regular postal handling procedures. However, what are the benefits that induce service providers to use inline TTPs? First, they allow the full control of message flows and thus facilitate the CMS deployment. Additional properties, such as timeliness based on deadlines, are also easier to implement. As in the case of traditional mail or e-mail, asynchronous communication is also the preferred way and is often a requirement for CMS to be practical. It is not desired that sender and recipient directly interact with each other. This requires an online or inline TTP to decouple senders and recipients from each other. In this case, and if supported by a CMS, senders may remain completely anonymous. Another benefit is usability. If all evidences are generated and signed by inline TTPs, senders and recipients do not necessarily need any additional cryptographic tools and can use the system with off-the-shelf components, such as e-mail clients or Web browsers. In such a case, a PKI for end-entities is not needed at all and reduces infrastructural requirements.

With respect to non-repudiation services, a common approach among the reviewed CMS cannot be observed. NRO evidences are generally not seen as necessary but can optionally be provided by senders in all systems. In each system, senders have to authenticate against inline TTPs, which seems to be sufficient for most CMS to ensure some kind of NRO, even if not transferable. NRS evidences appear to be essential in provider-based systems (PEC, De-Mail, REM, PReM) where messages may leave the sender's provider domain. In OSCI, this evidence type is out of scope of the specification, and in the Austrian CMS, it is not really meaningful as senders directly deliver messages to the recipient's provider. However, there is a consensus on the usage of NRD evidences, which seems to be a core property of CMS

CMS Name	DDS	PEC	De-Mail	SI-Moja	ERV	REM	PReM	OSCI
Country	Austria	Italy	Germany	SI Post	Austria	ETSI	UPU	OSCI
Standardization Body								Leitstelle
Transport protocol								
HTTP	•			•	•		•	•
SMTP		•	•			•		
Message protocol								
SOAP	•			•	•		•	•
e-mail		•	•			•		
Signature quality								
AdES	•	•	•	•		$\bullet_i$	$\bullet_i$	•
QES	•		•	•		$\bullet_i$	$\bullet_i$	•
Policy								
de-jure	•	•	•		•	$\bullet_i$	$\bullet_i$	$\bullet_i$
de-facto				•		$\bullet_i$	$\bullet_i$	$\bullet_i$

•= applied/supported $\bullet_i$ depending on the implementation

Table 4.2: Classification of CMS according to other CMS properties

provided on the Internet. By using inline TTPs, an NRR evidence is not necessarily needed, because TTPs can ensure strong fairness by preserving messages and returning a delivery receipt to the sender even if the recipient has not yet retrieved the message. NRR evidences, the stronger version of NRD, are mostly used in case of particular legal requirements, as in Austria (DDS and ERV) or in the German OSCI based e-Justice system EGVP. However, there is no consensus as to whether NRR evidences should certify the reception of the message content or the message envelope, as used in traditional mail delivery. Evidence transferability appears to be a common requirement. All systems and standards use electronic signatures for that purpose. In addition to the long-term archival ability enabled by electronic signatures, transferable evidences certainly increase trust when using the system.

In all of the discussed systems, timeliness is fully maintained by inline TTPs, and in all governmental systems, evidences are preserved by TTPs for a certain period of time. This allows all participating entities to finish the protocol in a finite and known amount of time, for instance by re-requesting evidences that have been lost due to a network failure. Timeliness is not explicitly defined for standards, because this property, in the end, depends on system policies and the chosen implementation. Finally, E2EE is not deemed to be a core property of CMS but is supported as an optional feature in most systems.

To summarize, in practice, systems are not aligned to newer (optimistic) design patterns proposed by the research community. Systems provided on the Internet are heavily aligned to the equivalent traditional postal certified mail service. One reason is definitely the increased user acceptance by providing known services and process flows from traditional postal services. In all cases, inline TTPs ensure strong fairness between senders and recipients by handling the exchange of a message for a transferable NRD (or NRR) evidence.

4.4.3 Other Properties

AdES and QES signatures are supported by almost all systems. Austria requires QES for recipients' NRR signatures, and delivery agents are recommended to sign evidences using an AdES. PEC does not specify the signature quality of evidence signatures. It simply has the requirement that applied signatures must be recognizable in the European and international context, which in the end leads to an AdES or a QES. De-Mail recommends evidence signatures to be a QES. Signatures of other entities may be of lower quality. Moja.posta.si requires QES on the recipient side and uses AdES for evidence signatures

and timestamps. Signature requirements for the Austrian ERV are not specified. OSCI does not make any restrictions on the signature quality and REM recommends the usage of at least an AdES. Even if there is no consensus on transport protocols, there seems to be a broader agreement on the application of certain signature formats and qualities, this means to be conformant with the EU Signature Directive and thus be mutually recognizable within the European context.

Table 4.2 shows a diverse choice of transport protocols between WS technologies (SOAP) and e-mail (SMTP). The technology comparison refers to the inter-provider communication, which in case of inline TTPs is transparent to senders and recipients. End-entity access for senders and recipients is, in most systems, supported for multiple technologies: mail clients, Web browsers or Web service clients. SMTP is a somewhat outdated technology, especially when dealing with structured data. Many CMS have thus chosen newer Web services technologies to transport messages, evidences, and electronic signatures in a structured way. As long as all systems are closed and autonomous, this is not a significant issue. This is currently the case. However, when thinking towards interoperable systems, this might become an issue. This implication is discussed in the next chapter.

Chapter 5

Need for Interoperability

"In the long history of humankind (and animal kind, too) those who learned to collaborate and improvise most effectively have prevailed."

[Charles Darwin, English Naturalist, 1809–1882.]

The ongoing globalization reduces barriers to bring together economies, cultures, languages and people. Vanishing borders not only boost international trade of goods, services and money, but also increase people's mobility. Particularly in Europe with its high diversity of countries and regions having different legislations, languages and cultures, the European Community is pushing the development of the Internal (or Single) market[1] since 1993. The single market has its foundations in the Treaty of the European Union [European Union, 2008][2]. The main goal of the single market is to reduce barriers and to simplify the rules for citizens and businesses to ensure the "four freedoms" within the EU: free movement of goods, services, capital and people. This means that EU citizens should be able to live, work and study in any EU Member State. Consumers should have the possibility to buy their products in other Member States without any bigger fiscal hurdles. The same should hold for businesses selling their products in other Member States. A single market automatically increases competitiveness and efficiency. More suitable manufacturing locations can be chosen to shorten transport routes, expand the trade area and save costs. Most legislations (internal market directives) have an international aspect and do not only focus on the European context in order to reap the benefits from a worldwide collaboration.

One cornerstone of a single market is a European Administrative Space (EAS) in terms of integrated administrative procedures on a local, national and pan-European level. Particularly e-Government plays a key role towards the accomplishment of this goal. Today, e-Government is manifested by a modern and efficient administration. By means of ICT and thereby especially the Internet, administrative processes are often reorganized and executed more efficiently. Service delivery, information sharing and communications with citizens and businesses are also improved. Besides better services for citizens and businesses, the promises are transparency, 24x7 availability, reduced red tape, efficiency, accessibility and reduced costs. A "digital" single market and a common administrative space can only be established with interoperable e-Government infrastructures. But what exactly is interoperability? The EIF [European Commission, 2010b, page 2] defines interoperability as follows:

[1] `http://ec.europa.eu/internal_market/`

[2] Article 3 (3) of the Treaty of the European Union

> "*The Union shall establish an internal market. It shall work for the sustainable development of Europe based on balanced economic growth and price stability, a highly competitive social market economy, aiming at full employment and social progress, and a high level of protection and improvement of the quality of the environment. It shall promote scientific and technological advance.*"

> "*Interoperability, within the context of European public service delivery, is the ability of disparate and diverse organisations to interact towards mutually beneficial and agreed common goals, involving the sharing of information and knowledge between the organisations, through the business processes they support, by means of the exchange of data between their respective ICT systems.*"

A working paper by the EC [European Commission, 2003] has discussed the importance of interoperability for e-Government services in this field. The paper dates back to the beginnings of European interoperability initiatives and discusses why European policy objectives like the single market freedoms, industrial policy, sustainable development and security across Europe can only be achieved with interoperable e-Government services. These services should be as efficient and effective as in the private sector and not stop at national borders. This means the public sector should be able to conduct cross-border governmental transactions in a likewise efficient manner as when purchasing goods in an online store residing in a foreign Member State. This requires interoperability within and across organizational and administrative boundaries. e-Government must be understood as an overarching term and comprise several levels: local, regional, national and pan-European and include both public administrations and the private sector in equal measure.

This chapter discusses the importance and need for interoperability by casting light on the political drivers aiming to achieve the European policy objective of a European digital single market. This process has started about a decade ago and due to missed targets this matter is becoming more and more important. All political commitments have been accompanied by several interoperability initiatives on a European level, mostly coordinated by the EC. Surveys, studies, strategy papers, frameworks and architecture guidelines were the outcome of these "programmes". Recently the EC has started to launch several interoperability projects on a European level to speed up the achievement of the goal of a EAS and a digital single market and to boost the competitiveness in Europe's digital economic area. These projects are also referred to as Large Scale Pilots (LSPs). CEM is a key aspect of e-Government and plays an important role in the secure and evidential document exchange between citizens, business and administrations. In a digital single market this communication does not stop at national borders. CMS interoperability is thus getting on the agenda of a digital Europe with no borders. Therfore, this chapter also discusses a major motive behind the work of this thesis, in particular the need for CMS interoperability and what scenarios and degree of interoperability should be achieved.

5.1 A History of Political and Strategic Commitments

Policy makers are a strong driver and strategic stimulus to push on the achievement of interoperability through common policies. Thereby one important aspect is the inclusion of pan-European ideas in national e-Government strategies. National e-Government services must be open and citizens, businesses and administrations should have access to other EU services. In the last decade, the European Community has thus made a number of political and strategic commitments towards the achievement of pan-European interoperability. Starting with the eEurope and i2010 initiatives, which missed their targets, the EC is now running a new strategy with the EU 2020 initiative to achieve the goal of a digital single market by the end of 2020. The work presented in this thesis was conducted and piloted in EU projects supporting the EC's policy initiatives. Therefore, this section gives a brief overview of these three major political commitments.

5.1.1 eEurope (2000-2005)

In a special meeting in Lisbon on 23-24 March 2000, the European council agreed on a strategy[3] with the goal

> "*to become the most competitive and dynamic knowledge-based economy in the world, capable of sustainable economic growth with more and better jobs and greater social cohesion.*"

It was set to reach this goal by the end of 2010. As one of the main key actions was defined the creation of an information society for all with the shift to a digital knowledge-based economy, access to world-class communications infrastructure by businesses and citizens and unleashing the full potential of e-Commerce.

In 1999, the EC has launched the eEurope initiative [European Commission, 2000] to bring Europe online. The start of this initiative was accompanied by the publication of the eEurope 2002 Action Plan [Council of the European Union and European Commission, 2000] at the Feira European Council in June 2002. The action plan had the aim to reach the targets set by the Lisbon strategy by defining necessary measures and relied on urgent actions by defining 64 targets to be achieved by the end of 2002. Most of the targets have been successfully achieved within its targeted timeframe. With the conclusion of eEurope 2002, it was clear that further appropriate actions need to be taken to foster the shift to a knowledge-based economy and information society. Therefore, in 2005 the eEurope 2005 Action Plan [European Commission, 2002] endorsed by the Barcelona European Council was published to succeed the eEurope 2002 Action Plan. The eEurope initiative ended in 2005. From 2001 to 2003 eEurope was accompanied by the eEurope+ initiative, which had the same objectives and targets as eEurope, but was focusing on EU candidate countries. The results of the eEurope initiative have been reflected in the Information Society Benchmarking Report [European Commission, 2005b], which reported that the roll-out of broadband access was a success story, online availability of public services was continuously growing, digital divide was still a problem and that disparities between Member States had not been reduced between the start of the initiative and 2004.

5.1.2 i2010 (2005-2010)

With i2010, the EC has launched a successor programme of the eEurope initiative. The programme was officially announced in a communication of the EC [European Commission, 2005a]. i2010 is a strategic framework, which defines guidelines for an Information Society. ICT is seen as a powerful driver for economic growth and employment throughout the EU and thus i2010 puts emphasis on the following priorities:

1. ***A single European information space***, which promotes an open and competitive internal market for information society.

2. ***Innovation and investment in ICT***. Research and innovation are major drivers for economic growth and the creation of new jobs. However, research alone is not enough and the results must be transfered into products to boost the economy. Therefore, the EC has launched two research programmes in the context of i2010. The Seventh Research Framework Programme (FP7)[4] runs from 2007 until 2013 and has total budget of over € 50 billion.

   The second research programme is the Competitiveness and Innovation Framework Programme (CIP)[5] targeting at SMEs to foster the take-up of ICT. The CIP has total budget of € 3621 million and runs from 2007 until 2013. The CIP has the following three sub-programmes.

[3] The presidency conclusions of the Lisbon European Council on 23 and 24 March 2000 are available at `http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/00100-r1.en0.htm`

[4] `http://ec.europa.eu/research/fp7/understanding/fp7inbrief/home_en.html`

[5] `http://ec.europa.eu/cip/`

(a) The Entrepreneurship and Innovation Programme (EIP)

(b) The ICT-Policy Support Programme (ICT-PSP)

(c) The Intelligent Energy Europe Programme (IEE)

Each of these sub-programmes has its own objectives. Particularly the ICT-PSP focuses on harmonizing ICT services through research in interoperability.

3. ***Inclusion, better public services and quality of life***. It is particularly important for economic growth and competitiveness to make ICT available to all people, whether they are living in areas, which have easy access to ICT, or not.

In order to set concrete actions for the realization of the i2010 goals, the EC has published the i2010 Action Plan [European Commission, 2006] including the aim to accelerate e-Government in Europe for the benefit of all. This action plan draws on the Manchester Ministerial Declaration, which was approved on 24 November 2005, which aims for widespread and measurable benefits from e-Government by 2010.

i2010 was accompanied by annually reports in 2006, 2007, a mid-term review report in 2008 and Europe's Digital Competitiveness Reports in 2009 and 2010 , which serve as evidence base for the Digital Agenda, the follow-up programme of i2010, which is going to be introduced in the next section. The final report in 2010 [European Commission, 2010c] states that i2010 has not reached all of its objectives. Even if broadband access is widespread throughout the EU, high-speed broadband is not that widely available as in other countries like Korea and Japan. The provision and consumption of cross-border services, particularly in the e-Commerce and Electronic Business (e-Business) sectors is quite low. This is reasoned by a low consumer trust and legal barriers for service providers. Last not least, even if the availability of public online service is quite high[6], take-up of public services by citizens is lagging behind.

5.1.3 Digital Agenda 2020

Europe 2020[7] is the EU's growth strategy for this decade. Economy growth should be smart, sustainable and inclusive. EU 2020 addresses the five targets of employment, R&D (innovation), climate change (energy), education and poverty (social exclusion).

The EC has launched seven flagship initiatives to address these targets. One of these flagship initiatives is the Digital Agenda for Europe [European Commission, 2010a] with the aim to use ICT as a driver for social benefits and to ensure economic growth and higher employment. The Digital Agenda points out the weaknesses in the European ICT area, for example that markets are still fragmented to a large extent. This not only applies to e-Commerce, but also to invoicing or payment. Interoperability between public services is also lagging behind the targeted goals and administrations of different Member States are not working or cannot work together as they should. Another item on the agenda is cybercrime. European citizens and businesses are more and more faced with cyber attacks when being on the Internet. Identity theft targets like online banking fraud (phishing) or social networks, industrial espionage or military attacks are steadily increasing. And in the R&D sector there is still a huge need to catch up with other countries like the US or Japan. European businesses, particularly SMEs, should get better access to R&D resources to invent and develop quality products, which will be highly in demand on the market. Last not least, the Digital Agenda points out the shrinking number of ICT experts in Europe and the deficiency of digital literacy, this means that many people are still suffering from the disadvantage of little knowledge in digital technologies (digital divide).

In the light of these weaknesses, the Digital Agenda has defined a set of concrete actions to deliver economic growth and to bring social benefits to the EU and the Member States:

[6] The ranking of full online availability of each Member State is also reflected in the 8^{th} benchmark measurement [European Commission, 2009c]

[7] http://ec.europa.eu/europe2020/

1. ***A vibrant digital single market***. The European online market is still widely fragmented. This concerns the content sector, cross-border transactions, eID and authentication and the telecommunication sector. A high priority is thus to facilitate cross-border transactions. Besides cross-border Electronic Signatures (e-Signatures), this also includes authentication. Even if username/password is the most used authentication scheme on the Internet, there is a need for authentication services with a higher quality like eIDs, particularly for e-Government services. This agenda item will work towards interoperable eID services throughout Europe.

2. ***Interoperability and standards***. Interoperability will be better promoted by a review of the European standardization policy and driving forward the adoption of the EIF under the Interoperable Solutions for European Public Administrations (ISA) programme. Both the EIF and ISA will be introduced in the next section.

3. ***Trust and security***. Security and trust in the Internet and online applications will be strengthened by a modernized European Network and Information Security Agency (ENISA) and creating a Computer Emergency Response Team (CERT) for EU institutions.

4. ***Fast and ultra fast Internet access***. Fast Internet for citizens and businesses is considered as a key driver for a growing economy. Therefore, actions will be taken to fund high-speed broadband access and to invest in Next Generation Networks (NGNs).

5. ***Research and innovation***. The EU spends about 40% of the costs of the US for research and innovation. Therefore, a new "Innovation Union" flagship will provide a research and innovation strategy until 2020. Investments in R&D should be doubled by 2020 and particularly SMEs should get easier access to research funds.

6. ***Enhancing digital literacy, skills and inclusion***. Another major action is to increase the number of ICT-skilled people, this also includes the higher participation of women in this area. About 30% of all people in Europe have never used the Internet. It is highly important that citizens get e-Business skills since many parts of our daily life are steadily becoming digital.

7. ***ICT-enabled benefits for EU society***. Healthcare can improve the quality of life. Therefore, ICT should be used to provide European citizens online access to their medical records. Within the Community, where an increasing mobility of citizens is expected, cross-border access to health data should be realized through interoperable systems. However, not only Electronic Healthcare (e-Health) asks for cross-border capability. Also in the area of e-Government public services should work across borders. The Community already provided a legal instrument for cross-border e-Government with the Services Directive [The Council of the European Union, 2006a]. However, further actions must be taken to ensure seamless cross-border procedures regarding e-Procurement, e-Signatures and authentication. e-Government services should become fully interoperable.

Following the i2010 e-Government Action Plan from 2006 [European Commission, 2006], the EC has recently published the new e-Government Action Plan 2015 [European Commission, 2010d] with the aim to implement the vision of the Malmö Ministerial Declaration[8]:

> "*whereby European governments are recognised for being open, flexible and collaborative in their relations with citizens and businesses. They use eGovernment to increase their efficiency and effectiveness and to constantly improve public services in a way that caters for users' different needs and maximises public value, thus supporting the transition of Europe to a leading knowledge-based economy.*"

[8] Malmö Declaration on e-Government, available online at `http://www.egov2009.se/wp-content/uploads/Ministerial-Declaration-on-eGovernment.pdf`

The Action Plan aims to realize two key actions set by the Digital Agenda. First, by 2015, the mobility of citizens and businesses should be highly enabled by providing a number of important cross-border services online. Second, by 2015, 50% of all European citizens should use e-Government services.

5.2 Interoperability Activities in the EU

Strategic commitments on a political level are a very important driver to select the direction of where interoperability has to go and how it should be achieved. Nevertheless, the development of appropriate concepts, technical frameworks and the launch of concrete projects showing their feasibility are of utmost importance to push their take-up by the public and private sectors. Therefore, the EC has launched their interoperability programmes quite early. This section discusses these programmes and their contribution in more detail and gives an overview of recent larger projects co-funded by the EC, which have the aim to develop and demonstrate interoperability frameworks for concrete application areas.

5.2.1 Programmes

The EC has already started early to launch concrete interoperability programmes with the aim to develop concepts and technical frameworks for the delivery of cross-border e-Government services to citizens and businesses. Moreover, the collaboration between public administrations of different Member States should be intensified. In 1995, the EC started the Interchange of Data across Administrations (IDA) programme, which was superseded by the Interoperable Delivery of European eGovernment Services to public Administrations, Businesses and Citizens (IDABC) programme running in the context of the i2010 initiative. Recently, the IDABC follow-up programme ISA was launched. This section gives an overview of these programmes, their contributions and achievements.

5.2.1.1 IDA (1995-2004)

The first phase of the Interchange of Data across Administrations (IDA) programme[9] started in 1995 with the aim to foster interoperability efforts in the context of telematic networks. Major objectives were to create a common interface from the Community to Member States and to reap its benefits for all citizens and businesses. Last not least, a publicly available best practice guide should help developing and taking up solutions in single Member States.

Some major achievements and contributions of the IDA programme are as follows:

- ***Architecture guidelines (1999)***. The European Interoperability Architecture Guidelines (EIAG) [European Commission, 2004a] provide an architectural description for the provision of interoperable cross-border telematic services and networks. They should be used as a reference when building or accessing cross-border services. Promises are shorter implementation times, better manageability and reduced costs due to economy of scale and that administrations can concentrate on their core business. These guidelines provide the technical basis for the EIF, which is going to be discussed in the next section.

- ***eLink middleware (1999)***. eLink was a middleware developed under the IDA programme to provide a generic solution for the interoperable information exchange between public administrations. The middleware should serve as a gateway between heterogeneous systems. The basic idea behind eLink is to bridge different messaging systems via a unified format, the eLink message format. Each system provides a gateway, which converts the local format to the eLink message format and

[9] Some (legal) background information on the IDA programme is available at http://europa.eu/legislation_summaries/information_society/strategies/l24147a_en.htm

vice versa. eLink has adopted some aspects from the German OSCI standard and the Swedish Government eLink (GeL) standard [Statskontoret, 2003]. Aspects adopted from GeL are the service identification process and OSCI provides the messaging format based on SOAP, XML signatures and encryption. The specifications [European Dynamics SA, 2004] are publicly available.

- ***ePractice.eu (2002)***. ePractice.eu is an online portal provided by the EC to share information about projects and strategies in the areas of e-Government, e-Health and Electronic Inclusion (e-Inclusion). Practitioners from all Member States can contribute and provide articles on several areas of interest.

- ***Architecting the delivery of PEGS (2004)***. The architecture for Pan-European e-Government Services (PEGS) [Capgemini, 2004] guideline provides a basic concept to make different solutions interoperable on pan-European level. PEGS is based on the Integrated Architecture Framework (IAF), which divides architectures into four levels of abstraction: contextual, conceptual, logical and physical. Similar to the eLink approach, PEGS introduces a network interconnect infrastructure using so-called PEGS gateways. These gateways convert different systems on each of the four mentioned defined layers.

The IDA programme officially ended with 31 December 2004.

5.2.1.2 IDABC (2005-2009)

Interoperable Delivery of European eGovernment Services to public Administrations, Businesses and Citizens (IDABC)[10] is the follow-up programme of IDA and extends the scope from administrations to citizens and businesses with the goal of promoting the digital single market. Therefore, like its predecessor, IDABC has regularly published recommendations, studies and other material on interoperable solutions as well as provided solutions for the cross-border link-up of public services. Among the major achievements and contributions of IDABC are:

- ***European Interoperability Framework (2003)***. The conception of the EIF [European Commission, 2004b] already started in 2003 in the course of the IDA programme and is currently in a revision process. The EIF defines itself as a reference document to support interoperability efforts. The main objectives are to support National Interoperability Frameworks (NIFs) as a "meta framework" and to provide a framework for establishing interoperability between public services for administrations, businesses and citizens. The underlying interoperability principles of the EIF are accessibility, multilingualism, security, privacy (personal data protection), subsidiarity, the use of open standards, assessment of benefits of open source software and the use of multilateral solutions. The framework further outlines the basic interaction types between administrations, citizens and businesses, this means the basic interoperability scenarios A2A, A2B and A2C (even in the cross-border case). Another major contribution of the EIF are the recommendations for interoperability on the specific layers introduced by PEGS: organizational, semantic and technical interoperability. The EIF limits itself on these three aspects. The contextual layer, for example legal or political issues, are explicitly left out of consideration. The first version of the EIF (1.0) appeared in November 2004. However, a revised version of the framework has recently published as annex of a communication of the new ISA programme [European Commission, 2010b].

- ***European Interoperability Strategy (EIS) (2008-2010)***. With the European Interoperability Strategy [European Commission, 2009f], IDABC sets a number of actions as a driver to improve the interoperability of public services. The EIS will play a key role in ISA, IDABC's follow-up programme. The main tasks of the EIF are to define a strategy based on a vision and the definition of

[10] A general description of the IDABC programme and its goals is available at `http://ec.europa.eu/idabc/en/chapter/3.html`

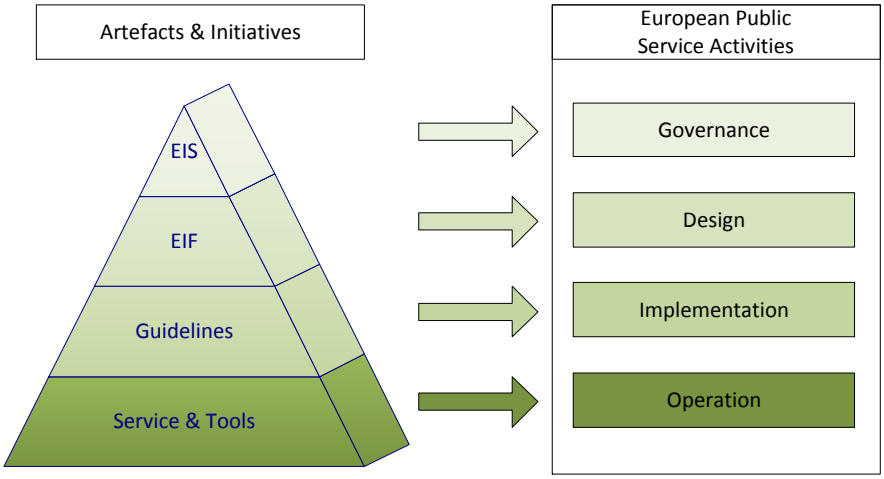

Figure 5.1: Interoperability governance pyramid as defined by the (Draft) European Interoperability Framework 2.0. The EIS builds the top of the pyramid and defines the main interoperability strategy (governance layer). Based on this strategy the EIF defines the recommendations and principles on how to establish interoperability (conception layer). Concrete implementations should be developed with the help of architectural guidelines (implementation layer). The lowest layer is defined by services and tools, which have been developed by several initiatives and should be reused as building blocks to achieve interoperability (operational layer).

priorities and objectives. It therefore sits on top of the interoperability governance pyramid. The interoperability governance pyramid and the relation of the EIS to the EIF and guidelines like the European Interoperability Architectural Guidelines defined by IDA are illustrated in Figure 5.1.

- ***Studies***

  - ***European Interoperability Infrastructure Services (EIIS) (2009-2010)***. In 2009 the EC has conducted the EIIS study on the potential reuse of system components [European Commission, 2009b]. The main goal of this study was to identify and describe common interoperability infrastructure services of existing systems or system in development. Nine services have been defined: Audit Trail and Log, Service Registry, Identity and Access Management, Document Storage, Workflow Management, Data Certification, Data Transport, Data Translation and Structured Data Storage. The study recommends to use the promising SOA approach in order convey and exchange information in a structured way. The EIIS finds itself on the lowest layer of the interoperability governance pyramid (cf. Figure 5.1).

  - ***eID interoperability for PEGS (2005-2009)***. Many public services are only accessible by eIDs as a means for qualified identification and authentication. In the past decade, many Member States have rolled out custom eID solutions. eID interoperability is therefore considered as a key enabler for accessing public services abroad. In 2009, IDABC has thus conducted a study on eID interoperability [European Commission, 2009d], which is based

on the previous works in this area by Modinis[11], FIDIS[12] or the Porvoo Group[13]. The outcome of this study was a detailed analysis and assessment report with eID profiles of 32 countries.

- ***Preliminary study on mutual recognition of e-Signatures for e-Government applications (2005-2009)***. Even if electronic signatures are regulated to some extent by the EU Signature Directive [The Council of the European Union, 2000b], application and formats are still heterogeneous throughout the EU. This is a massive barrier for the cross-border use of e-Signatures. Therefore the EC has conducted a study on the mutual recognition of e-Signatures for e-Government, e-Health, e-Procurement and e-Justice applications [European Commission, 2009e]. The main findings of this study are that most signature solutions are tailored to national needs and thus not cross-border capable. Legal frameworks in some countries also lead to requirements, which cannot be met by foreign solutions. This may be reasoned by the Signature Directive, which in several aspects leaves some room for interpretation. Therefore, a more precise and complete legal framework on European level is required.
- ***Study on electronic documents and electronic delivery and study on the implementation of Art. 8 of the Services Directive (2007-2009)***. In preparation for the implementation of the Services Directive, which will facilitate the cross-border provision of services and the creation of a new business in a foreign Member State, the EC has conducted two studies to facilitate the achievement of this goal. Electronic Documents (e-Documents) and e-Delivery[14] are key elements of e-Government to ensure the secure, reliable and evidential exchange of authentic documents. A study on electronic documents and electronic delivery [Siemens and Timelex, 2009] assesses in detail the application of e-Documents and e-Delivery in all 27 EU Member States. The study further analyzes problems and identifies challenges with respect to legal, policy, technical and infrastructural issues. A second study [Siemens and Timelex, 2008] assesses the state of implementation of Art. 8 of the Services Directive in each Member State. Further details on the Services Directive are discussed later in this chapter in the context of the European SPOCS project.

IDABC has officially ended in 2009.

5.2.1.3 ISA (2010-2015)

In 2010, the EC has launched Interoperable Solutions for European Public Administrations (ISA), the follow-up programme of IDA and IDABC. ISA's major goal is to create a better communication between public administrations across Europe. The programme runs until 2015 and has a total budget of € 164.1 million.

A mission statement of the EC[15] says

> "*In order to provide user-friendly public services to citizens and businesses, public administrations work together and exchange information, not only within countries but increasingly*

[11] The MODINIS programme was launched in the course of the eEurope 2005 Action Plan and has been continued in the i2010 initiative. Further details are available at `http://ec.europa.eu/information_society/eeurope/i2010/archive/modinis/index_en.htm`

[12] FIDIS (Future of Identity in the Information Society) was a five-year project in the 6^{th} Framework Programme (FP 6) dealing with Identity Management (IdM) in the European Information Society.

[13] The Porvoo Group is a forum for discussion to promote eID interoperability. The group also meets twice a year. Information about the group is available at `http://ec.europa.eu/idabc/en/document/4491/5584.html`

[14] The term e-Delivery denotes the service of documents whether it is certified or not. CEM can thus be considered as e-Delivery sub-category.

[15] `http://ec.europa.eu/isa/index_en.htm`

across borders. Such cross border collaboration touches many aspects of life, including security, justice, the environment, job offers and studying abroad, but also doing business in the single market and the correct spending of EU funds. The ISA programme supports cross-border electronic cooperation between public administrations at national, regional and local level, leading to cost-effective delivery of public services, facilitating the implementation of EU legislation and supporting the single market."

The main activities and actions of ISA are defined as follows[16]:

- Common frameworks in support of interoperability (policies, strategies, specifications, methodologies, guidelines and similar approaches and documents)
- Reusable generic tools (demonstrators, reference, shared and collaborative platforms, common components and similar building blocks for user needs across policy fields)
- Common services (operational applications and infrastructures of a generic nature to meet user requirements across policy areas)
- Analysis of the ICT side in the implementation of new EU legislation

ISA will heavily align to the EIS and the EIF by supporting both the Digital Agenda and the e-Government Action Plan 2011-2015 in realizing some of its goals and planned action items. The work programme focuses on interoperability, common frameworks and ICT architectures and last not least information exchange.

5.2.2 Large Scale Pilots

With the ICT-Policy Support Programme (ICT-PSP) the EC has started to launch so-called Pilot Type A projects[17]. A Type A project is also called Large Scale Pilot (LSP), is driven by Member States and addresses cross-border interoperability aspects. Its main goals are to make existing systems or services in development interoperable through an appropriate framework. These projects are intended to run for at least 36 months and to produce architectural concepts and common specifications to achieve interoperability. For sustainability reasons these specifications should be presented to standardization bodies. The outcome of LSPs is usually validated, demonstrated and evaluated in a 12 month piloting phase at the end of the project. In the last three years, the EC has launched five LSPs to develop cross-border interoperability solutions for different key areas towards a digital single market. These are as follows.

1. Secure Identity Across Borders Linked (STORK) - eID
2. Pan-European Public Procurement Online (PEPPOL) - e-Procurement
3. Simple Procedures Online for Cross-border Services (SPOCS) - Services Directive
4. Smart Open Services for European Patients (epSOS) - e-Health
5. e-Justice Communication via Online Data Exchange (e-CODEX) - e-Justice

Parts of the work presented in this thesis have been conducted in the course of the two LSPs STORK and SPOCS. The next sections give an overview of the objectives and work of each LSP, which has also been briefly reflected by the author in [Tauber et al., 2011d].

[16] http://ec.europa.eu/isa/strategy/index_en.htm
[17] http://ec.europa.eu/information_society/activities/ict_psp/faq/pilots_a/index_en.htm

5.2.2.1 STORK

Electronic identification has become a natural part of our digital life. People are used to authenticate at online shops, mail providers, social networks or public sector applications. In some cases a high-quality (e)ID is necessary to prevent identity theft or digital twins. This is particularly true in the case of e-Government applications. Therefore, in the last years, several governmental eID projects have been launched. Popular examples are the Finish eID (FINEID) card (December 1999), the Estonian eID card (January 2002), the Austrian citizen card (2003, mass-rollouts in 2005), the Italian Carta d'Identitá Elettronica (CIE) and Carta Nazionale dei Servizi (CNS) cards (2003) and the Belgian eID card (2^{nd} half of 2003). All these solutions evolved as national islands and are heterogeneous in various dimensions. On a technical level many different tokens are used for authentication. Ranging from username/password and software certificates to mobile eIDs or smartcards. From an operational point of view many different issuers can be found. Tokens may be issued by the public sector or the private sector, at federated, local or regional level. Legal issues often concern the inclusion and application of unique national identifiers in a flat, sectoral or combined manner. With the increasing mobility within the EU, the cross-border need for qualified identification is increasing in equal measure. Some examples are migrant workers, exchange students, social security cases, moving house, e-Health for medical treatments abroad or even e-Justice in cross-border legal proceedings.

For this purpose, the EC has launched the European LSP STORK with the aim to provide a technical framework for the cross-border mutual recognition of eIDs. The STORK consortium consists of 32 partners from 17 EU/EEA Member States[18]. The project has a total budget of € 26.5 million (50% co-financed by the EC). The project started in May 2008 and finished in December 2011.

From the very beginning, STORK had to tackle several issues. First, a consensus between the participating Member States was needed on the applied authentication and identification framework. In some Member States legal issues posed an obstacle in terms of limiting the use of national identifiers abroad or preventing other operations due to data privacy regulations. But also other questions arised concerning liability and trust. Who is responsible if a cross-border transaction goes wrong or how can identity sources be trusted?

Entity Authentication Assurance A first project milestone was the development of the Quality Authentication Assurance (QAA) framework [Hulsebosch et al., 2009]. eIDs in different Member States are based on different technologies and have different security levels. This leads to the necessity of a common understanding and standardized way to deal with authentication. A harmonized classification into four well-defined QAA levels allows Member States to map national authentication levels to the QAA levels and vice versa. In this way authentication levels of different Member States can implicitly be mapped between each other via the QAA scheme. A QAA level integrates several aspects of authentication: registration, credential issuance, authentication quality and strength.

Authentication Framework STORK has defined three basic use cases, which are as follows:

1. ***Authentication*** - in an online access to a service provider
2. ***Attribute Transfer*** - STORK supports the attribute transfer of personal identification attributes (national ID number, name, date of birth, qualification, etc.). These are retrieved form the eID credential and if needed from an attribute provider (governmental source)
3. ***Certificate Verification*** - for electronic signatures

[18]These are Austria, Belgium, Estonia, Finland, France, Germany, Greece, Italy, Island, Lithuania, Luxembourg, Portugal, Sweden, Slovenia, Spain, The Netherlands and The United Kingdom.

The developed interoperability framework features two basic models [Leitold and Zwattendorfer, 2010; Leitold, 2011]:

1. ***Middleware (MW)***. In the MW model, service providers, which aim to integrate cross-border authentication support, set up an authentication software (MW) within their operational environment. Therefore, this MW must integrate all the necessary eID authentication components. In this scenario authenticating foreign users directly communicate with the service provider. There are no intermediaries between the user and the service provider, which enables end-to-end security. Since the authentication data is retrieved from the eID, the service provider remains the data controller. This authentication model is called "user-centric".

2. ***Pan-European Proxy Service (PEPS)***. In contrast to the MW model, the PEPS interoperability model uses a federated approach. A PEPS can be seen as a gateway, which hides national infrastructural complexities. Consider the cross-border authentication scenario where a user from Member State A wants to authenticate against a service provider residing in Member State B. Both Member States host an own PEPS instance. The PEPS instance of Member State A is called Citizen PEPS (C-PEPS) and the PEPS instance of Member State B is called Service Provider PEPS (S-PEPS). Both the C-PEPS and the S-PEPS have a trust relationship. The same holds for the S-PEPS and the service provider. The authentication process is as follows. The service provider redirects the user to the S-PEPS, which redirects the user to the C-PEPS of the user's home country. The actual authentication is carried out at the C-PEPS or another national identity provider behind. The C-PEPS may also retrieve additional identity information from an attribute provider. The authentication information and additional identity attributes are transfered by the C-PEPS back to the S-PEPS, which finally transfers it to the service provider. In contrast to the MW model, third parties are involved in the PEPS model. Since PEPS instances become identity data processors or controllers, there is a liability shift from the service provider to the PEPS. Nevertheless, in both models, users must give their consent that their data is used abroad.

Even though MW and PEPS have completely different operational models, they can be combined (MW-MW, MW-PEPS, PEPS-MW, PEPS-PEPS) with the concept of a Virtual Identity Provider (V-IDP). A V-IDP is a MW with a PEPS interface so that both instances can communicate with each other. The STORK common specifications have been designed in such a way that major components operate on the same protocols, irrespective of the model or its combinations. Technical details of the STORK interoperability framework and its models are introduced and reviewed in detail in Chapter 11.

To validate, demonstrate and evaluate its concepts and components, STORK has established an interoperability framework across the participating countries and integrated its cross-border authentication components into several operational services. The applicability in real environments and under real conditions is demonstrated in a 18-month piloting phase in the following six pilot applications.

1. ***Pilot 1 - Cross-border authentication***. Pilot 1 integrates cross-border authentication into citizen portals.

2. ***Pilot 2 - Saferchat***. Pilot 2 builds an online platform for safer communications between students. Only students between a certain age are allowed to authenticate at the platform.

3. ***Pilot 3 - eID student mobility***. Pilot 3 facilitates student's mobility by enabling cross-border authentication at universities. Students can thus carry out the whole enrollment or pre-enrollment phase for the Erasmus exchange program online from home.

4. ***Pilot 4 - eID electronic delivery***. Pilot 4 provides cross-border authentication at CMS Web frontends. Foreign senders and recipients can thus be identified and authenticated in all phases of a CEM process. The pilot also enables the cross-border signing of NRR evidences and provides a

cross-border interoperability framework for the qualified exchange of documents between different CMS.

5. ***Pilot 5 - EU citizen change of address***. Pilot 5 integrates cross-border authentication at e-Government applications supporting the change of address. This facilitates the process of moving house abroad.

6. ***Pilot 6 - ECAS integration***. European Commission Authentication Service (ECAS) is the central authentication system of the EC and serves more than 250 applications[19], for example CIRCABC[20] and the Internal Market Information System (IMI)[21]. Pilot 6 extends the existing username/password-based authentication system with eID support.

The author has discussed Pilot 2 (Saferchat) and Pilot 4 (eID electronic delivery) in detail in two publications [Tauber et al., 2011c; Knall et al., 2011]. The STORK piloting phase started in Summer 2010 with 21 service provider applications. Although STORK can be considered as a success story, there are still some open issues, for example the support for legal persons. STORK has demonstrated a technical concept for a cross-border authentication framework and proven its feasibility, but a missing legal basis including aspects of certification, liability, supervision, data protection, accreditation is currently preventing a wide-spread take-up by both governments and the industry. Only a few Member States have a legal regulation for eIDs in place. Austria is one of them (cf. Rössler [2008]).

The EC has recognized the importance of cross-border authentication and has explicitly announced two authentication-related actions in the Digital Agenda [European Commission, 2010a]:

- ***Key Action 3***

  > "*In 2011 propose a revision of the eSignature Directive with a view to provide a legal framework for cross-border recognition and interoperability of secure eAuthentication systems;*"

- ***Key Action 16***

  > "*Propose by 2012 a Council and Parliament Decision to ensure mutual recognition of e-identification and e-authentication across the EU based on online 'authentication services' to be offered in all Member States (which may use the most appropriate official citizen documents - issued by the public or the private sector);*"

5.2.2.2 PEPPOL

With 16% of the EU's Gross Domestic Product (GDP), public administrations are amongst the greatest contractors of private sector service providers. The traditional procurement process requires a lot of paperwork for tendering, ordering, invoicing, etc. Therefore, in many European countries e-Procurement solutions have been built to save costs and to reduce the administrative burden by leading the modern administration into the digital era. However, most of these solutions are isolated applications and many countries even have one at all. To increase the competitiveness within the EU it is thus necessary to establish EU-wide interoperability by connecting existing e-Procurement infrastructures.

Therefore, the EC has launched the European LSP Pan-European Public Procurement Online (PEPPOL)[22] with the aim to create EU-wide standards to foster transparency and competitiveness in the EU, save time and reduce costs with estimated savings of € 50 billion per year. The PEPPOL consortium consists of

[19] http://ec.europa.eu/isa/actions/01-trusted-information-exchange/1-4action_en.htm
[20] https://circabc.europa.eu
[21] http://ec.europa.eu/internal_market/imi-net/index_en.html
[22] http://www.peppol.eu

18 project partners from 12 countries[23]. The project is coordinated by the Norwegian Agency for Public Management and e-Government and has a total budget of € 30.1 million (50% co-financed by the EC). The official start was in May 2008 and the project is planned to run for 48 months until 2012. The piloting phase started in November 2010. Eight contracting public administrations and seven suppliers participate in this phase.

PEPPOL provides the following building blocks, which cover both the tendering (pre-award) and procurement (post-award) process.

Virtual Company Dossier (VCD) A powerful tool for the tendering phase is the VCD. Suppliers usually must provide evidence, for example by means of a certificate, to prove that they are qualified enough for a selected service. However, as of today there is a considerable heterogeneity of such evidences across Europe. They have different formats, languages and unknown issuers as from a point of view of another country. WP2 has thus defined the VCD as a standardized structure for evidences. The PEPPOL VCD tools provide a set of instruments to handle evidences. The National VCD System (NVS) helps businesses and administrations to create electronic evidences with the VCD builder. Each created evidence can subsequently be uploaded to the VCD. The European VCD System (EVS) is a decision support system in call for tenders to help public administrations select and validate evidences of tenderers. Single VCDs can be examined with the VCD viewer tool.

e-Catalogue WP3 has developed another instrument for the tendering phase, the Electronic Catalogue (e-Catalogue). With this tool suppliers are able to describe the goods and services they offer, this means single products and its prices. Common data structures and classification schemes enable the seamless cross-border exchange of these information. The e-Catalogue specification is based on the CEN Business Interoperability Interfaces (BII) for Public procurement in Europe [24]. CENBII is a specification with the aim to facilitate cross-border e-Procurement in Europe and provides an agreement on business and semantic models. On the syntactic and technical level, CENBII profiles of the United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT) technical specifications[25] and of the Universal Business Language (UBL) [Bosak et al., 2006] are used.

e-Catalogue components are also used in the procurement phase when a contract has been awarded to a supplier.

Electronic Ordering (e-Ordering) and Electronic Invoicing (e-Invoicing) The procurement process starts with the issue of an order and is tightly related to the topics of e-Catalogue and invoicing. It saves time and costs if ordering information can be provided and updated automatically. WP4 has thus provided tools for the e-Ordering phase, which are also based on CENBII.

A number of national solutions can be found for invoicing. WP5 has defined a standardized way to exchange invoicing information across borders. The common specifications are also based on CENBII.

e-Signature Validation e-Procurement documents may be signed by the issuer to ensure authenticity and integrity in all phases of procurement. The signature certificate may be issued by some accredited CA, some other authority on national, regional or local level or by some private business. Cross-border recognition of e-Signatures and validation of certificates is thus important to facilitate the exchange and cross-border acceptance of e-Documents. For this purpose, WP1 has specified a federated network of validation services, which can recognize both QCs and non-QCs as long as the latter are accepted in some

[23] These are Austria, Denmark, Finland, France, Germany, Greece, Hungary, Italy, Norway, Portugal, Sweden and the United Kingdom

[24] The CENBII specification is available at `http://www.cen.eu/cwa/bii/specs/`

[25] The UN/CEFACT technical specifications are available at `http://www.unece.org/cefact/codesfortrade/CCTS_index.htm`

e-Procurement domain. This cross-border validation system uses a classification system for eIDs and e-Signatures [Olnes et al., 2010] and utilizes the XML Key Management Specification (XKMS) [Hallam-Baker and Mysore, 2001] and the OASIS Digital Signature Service (DSS) [OASIS Digital Signature Services TC, 2007] standard.

Transport The secure, reliable and evidential document exchange is ensured by BusDox, which has been discussed in detail in the preceding chapter (cf. Section 4.3.4.2).

5.2.2.3 SPOCS

In order to increase the growth potential of the services market within the EU, the EU Services Directive [The Council of the European Union, 2006a] was approved on 12 December 2006. The main goal of the "Directive on services in the internal market" is to establish a single market for services within the EU by removing legal and administrative barriers for businesses when they want to provide services abroad. The Services Directive asks Member States to simplify administrative procedures for service providers when they either want to establish a business in a foreign Member State or when they want to provide services abroad. For this purpose, Member States must provide so-called Point of Single Contacts (PSCs) acting as intermediaries between service providers and the national public administrations (competent authorities). PSCs are designed to allow businesses to gather all the necessary information and to complete all the relevant administrative procedures electronically, for example obtaining authorizations to start an activity. The current national implementations of the EU Services Directive are first but important steps ahead. However, in order to bring a real benefit to European Service Providers, a better electronic support is needed. This would help to strengthen European businesses and to strengthen the business location Europe tremendously. Consequently, the Services Directive asks to build up on existing e-Government infrastructures as the Service Providers' domestic e-Government elements. For example, eID tokens, CMS accounts, etc. should work abroad as well. Therefore, an advanced interoperability concept is needed to bridge the various national e-Government elements like CEM, e-Document sources etc. While the cross border use of eIDs is already tackled by the LSP STORK, the interoperability in other areas of e-Government is not well developed yet. Therefore, the EC has launched the European LSP Simple Procedures Online for Cross-border Services (SPOCS)[26], which takes up this challenge and provides an interoperability framework for those e-Government areas which are required to conduct typical Services Directive related processes fully electronically. The SPOCS consortium consists of 33 partners from 16 Member States[27]. The project is coordinated by Capgemini Netherlands and has a total budget of € 24 million (50% co-financed by the EC). The project started in June 2009 for a 3-year journey until June 2012.

The following description of SPOCS is based on a work of the author of this thesis (cf. Rössler and Tauber [2010b]). Considering a real cross-border e-Government application, many aspects are touched, for example the cross-border use of eIDs, e-Documents, CMS or Electronic Safe (e-Safe) applications. In order to foster the interoperability of national e-Government services and infrastructures, the European Commission has launched several LSPs in the past. Usually, each LSP addresses specific aspects and use-cases. Unlike the other LSPs, the new LSP SPOCS has a much broader scope. The scope of SPOCS is to develop the infrastructure for future PSCs in accordance with the Services Directive. In other words, SPOCS aims to prepare a framework which enables service providers, this means the users in terms of the Services Directive, to use their national e-Government infrastructure and elements, such as their eIDs, CMS portals, e-Safe applications, e-Documents etc. , in front of foreign services provided by foreign PSCs. Thus, SPOCS results will support Member States to

[26] http://www.eu-spocs.eu

[27] These are Austria, France, Germany, Greece, Italy, Lithuania, Luxembourg, Malta, Norway, Poland, Portugal, Romania, Slovenia, Sweden, The Netherlands and The United Kingdom

> "*[. . .] ensure that all procedures and formalities relating to access to a service activity and to the exercise thereof may be easily completed, at a distance and by electronic means, through the relevant point of single contact and with the relevant competent authorities*"
>
> (Article 8, EU Services Directive [The Council of the European Union, 2006a])

Although the Services Directive focuses on foreign service providers considered from the point of view of the country offering electronic services, the resulting interoperability framework should be applicable to other areas as well. Especially the private sector could and should benefit from the solutions developed by SPOCS. Solutions and especially interoperability frameworks can only achieve impact on the market if they are used by a critical mass. Moreover, SPOCS intends to adopt and adapt (if necessary) interoperability solutions provided by other interoperability projects wherever possible. For instance, the interoperability framework provided by STORK for authenticating physical persons is going to be used in SPOCS scenarios as well. On the other hand, the SPOCS interoperability framework for e-Documents will base on results provided by PEPPOL. From this perspective SPOCS is the most integrative LSP of all.

The primitive principles of the SPOCS vision can be briefly summarized as follows:

1. Provide access to all foreign services by electronic means.
2. Enable service providers to use their existing domestic e-Government infrastructure in connection with services abroad.
3. The solutions to be developed should be versatile and open for other sectors as well (for example the private sector)
4. Adopt or adapt existing interoperability solutions.

The work of the LSP SPOCS is structured in so-called work packages. Work packages 1 to 4 develop common technical specifications for the interoperability solutions and implement them as open source software modules. Following main objectives for these work packages exist:

- ***WP1***. Enable content syndication, related to glossaries and to multilingual reality.
- ***WP2***. Enable understanding and recognition of electronic documents (e-Documents), as well as the authentication and validation of e-Documents.
- ***WP3***. Enable understanding and recognition of CMS and e-Safe systems in different Member States.
- ***WP4***. Enable definition and description of services to form a better understanding and recognition of electronic services, which are provided in different national service directories.

In addition, in WP5, Member States participating in the piloting, integrate the open source modules developed by SPOCS in their national e-Government systems and keep the solutions operational for at least twelve months. The overall objective of WP5 is to experiment with the provision of services related at least to the three professions of travel agents, real estate agents and master builder. The candidate countries for these pilot professions are Austria, Germany, Greece, Italy and Poland.

5.2.2.4 epSOS

With vanishing borders within the EU, citizens' mobility has highly increased and a larger number of tourists, business travelers or exchange students can be recorded. Healthcare and treatment abroad is not that effective and often poses a risk due to missing patient data. Even if e-Health has progressed in the last years, it is still a local, regional or national matter. The EC has recognized the need to improve cross-border electronic healthcare services and the treatment for traveling citizens with electronic patient data.

Therefore, the EC has launched the European LSP epSOS[28] with the aim to build, demonstrate and evaluate a cross-border framework for e-Health services. The epSOS consortium consists of 47 project partners from 23 countries (20 EU Member States and three non-EU countries)[29]. The project is coordinated by the Swedish Association of Local Authorities and Regions and has a total budget of € 36 million (50% co-financed by the EC). The official start was in July 2008 and the project is expected to run until December 2013. The involved healthcare infrastructure counts 3445 entities of which are 183 hospitals, 2149 pharmacies and 1113 Point of Care (PoC). The PoC concept is introduced below.

epSOS has structured its project into the following five major domains[30]:

1. Analysis and evaluation
2. Legal and regulatory issues (policy)
3. Specification and implementation
4. Field testing
5. Project management

The project cuts into two major phases. The first phase deals with the patient summary and Electronic Prescription (e-Prescription). e-Prescription denotes the electronic prescribing of medication. The patient summary should facilitate the quick access to patient's health data and reduce errors made by healthcare professionals and is a standardized format that contains all relevant data for a patient's healthcare treatment abroad.

The second project phase deals with the integration of the 112 emergency service and the European Health Insurance Card (EHIC) as well as patients' access to their health data. The latter requires qualified identification, which is an important building block throughout the whole project. Since e-Health data are highly personal, it must be guaranteed that only authorized persons can access certain data.

The epSOS system architecture consists of the following two building blocks:

- ***epSOS interface***. The communication layer between healthcare systems of different countries is called epSOS interface. It has both an inbound and outbound communication endpoint (either called *Inbound Protocol Terminator* or *Outbound Protocol Terminator*). The communication is based on Web services.
- ***National Contact Point (NCP)***. A NCP is a gateway, which acts as national entry and exit point and communicates with foreign healthcare system via the corresponding NCP using the epSOS interface. NCPs have a national interface to communicate with the national infrastructure and national portals via so-called National Connectors and Portal Adapters.

[28] http://www.epsos.eu

[29] These are Austria, Belgium, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Italy, Malta, Norway, Poland, Portugal, Slovenia, Slovakia, Spain, Sweden, Switzerland, The Netherlands, Turkey and The United Kingdom.

[30] See http://www.epsos.eu/fileadmin/content/pdf/epSOS_Project_Structure_Overview.pdf

5.2.2.5 e-CODEX

A higher mobility in the EU inevitably leads to an increasing number of cross-border (legal) procedures. Currently 10 million people are involved in cross-border civil proceedings. To ensure efficiency and transparency and to reduce time, costs and red tape it is necessary to improve the cross-border access to legal means by citizens and businesses. It is also necessary to improve the interoperability between legal authorities within the EU. Recently, the EC has launched the European LSP e-CODEX with the aim to establish a European e-Justice system to help implement the EU legal framework and the e-Justice action plan [European Union, 2009] and achieve cross-border interoperability in criminal, civil and commercial matters. The e-CODEX consortium consists of 18 partners from 15 countries[31]. The project is coordinated by the German ministry of justice of Northrhine-Westphalia and has a total budget of € 14.04 million (50% co-financed by the EC). The project started in December 2010 and runs for 48 months until November 2013.

At the time of writing, e-CODEX was still in an assessment phase and thus no results were available. Nevertheless, from the beginning the project is focusing on the following topics:

- ***Identity and e-Signatures***. Qualified identification is an important aspect in legal proceedings. WP4 aims to build federated identity services, which rely on existing eID infrastructures. New solutions should only be built where necessary and unavoidable. A challenge of this task will be the assignment of corresponding roles in terms of semantics and mappings to new foreign users. Empowerment and mandate management, for example natural persons representing legal entities, are also on the agenda since this a frequent instrument used in legal proceedings. The work package also wants to make provisions for public administrations to search for message recipients. Last not least, the recognition of e-Signatures will be addressed by this work package to ensure that documents remain authentic also abroad. Like for eID, the verification of signatures will be carried out by a federated signature verification service.

- ***Exchange of documents/data, Electronic Filing (e-Filing) and Electronic Payment (e-Payment)***. WP5 deals with the reliable and evidential cross-border document exchange. Therefore, it is assessing already from the beginning existing standards and results of other LSPs serving this purpose.

- ***Document Standards and Semantics***. WP6 provides a cross-border framework for the mutual recognition of e-Documents. This includes both the document content as structured data and document metadata as interpretable semantics.

- ***Pilot and Experimenting***. The results - specifications and common modules - are validated, demonstrated and evaluated in a piloting phase. This is conducted by WP3.

5.2.2.6 Synergies between LSPs

e-Government building blocks like eID, CEM, e-Documents or e-Signatures are key aspects of several LSPs. It only seems natural to search for synergies between the single LSPs. In the course of cross-pilot activities and collaborations, main building blocks are identified for reuse and eventually extended and adapted according to the needs of each LSP (see Figure 5.2). The use of synergies definitely brings the vision of a digital single market one step closer. Synergies between the LSPs STORK and epSOS are discussed by the author in [Zwattendorfer et al., 2011b].

[31] These are Austria, Belgium, Czech Republic, Estonia, France, Germany, Greece, Hungary, Italy, Malta, The Netherlands, Portugal, Romania, Spain and Turkey.

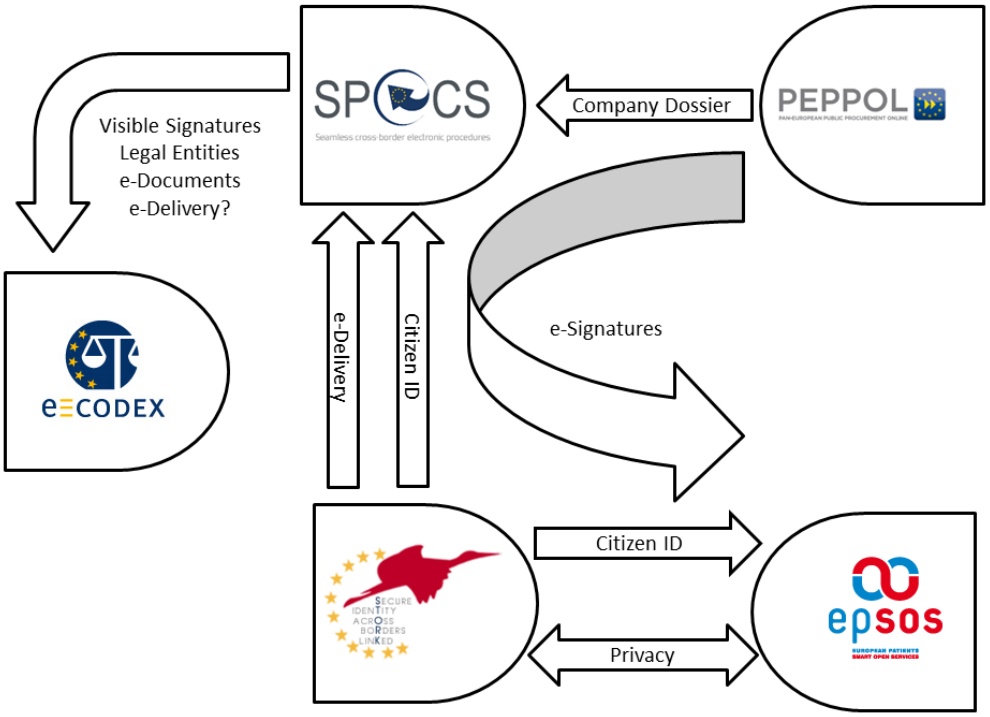

Figure 5.2: Synergies between different LSPs by reusing main building blocks

5.3 CMS Interoperability

Interoperability has been identified as a key enabler for economic growth and social cohesion. This not only concerns the key areas of eID, e-Signatures and e-Documents, but in particular also CEM. The secure, reliable and evidential document exchange is deemed as main building block and core transport component of several LSPs. PEPPOL, SPOCS, epSOS and e-CODEX - all of them require a communication infrastructure with the quality of CEM. According to the targets of each LSP, this should not be a completely new communication infrastructure, but should rather enable cross-border interoperability between existing systems.

But what is the state of play in terms of CMS interoperability? By having a look at all CMS, which have been introduced in Chapter 4, most systems are closed. Those CMS, which allow to send messages to arbitrary e-mail recipients, are not completely closed. Even if arbitrary recipients can be reached, senders still have to register with the system. This means that, in general, CMS are only accessible by particular user groups. Registration in some system is restricted to certain eIDs, which requires a certain citizenship or residence in a particular country. Other systems are restricted to certain occupation groups. Typical examples are e-Justice systems where only legal entities - courts, public prosecution departments, lawyers, notaries, etc. - can participate. In order to address a particular recipient in a closed CMS, senders have to be registered in the same system. It is currently not possible to send certified mailings from one closed CMS to another one. Even systems of the same country are not interoperable. For example, De-Mail and the OSCI-based EGVP or the Austrian DDS and the ERV. Even if they serve the same purpose of providing CEM services, they have completely different user groups and different technical specifications, organizational and business aspects as well as legal frameworks.

The diversity of isolated solutions results in a large heterogeneity in the current CMS ecosystem. 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 if they want to reach their communication partners. However, the registration in a foreign system, particu-

larly if it resides in a foreign country, may be problematic and raise several technical, organizational and legal challenges.

- ***Technical challenges***. The CMS registration or authentication procedure may be restricted to certain technologies, which are not available abroad. For example, one can only register with and authenticate at the Austrian DDS and Moja.posta.si using the Austrian citizen card or the Slovenian eID, respectively. Not only authentication poses a technical hurdle. Users must get familiar with new GUIs and country-specific terms and functionalities. This particularly applies to trust relationships. For example, security tokens like SSL server certificates or signature certificates may be issued by (certification) authorities, which are only known in the country hosting the CMS.
- ***Organizational challenges***. A major problem may definitely be the linguistic barrier. Conversations with communication partners may be in an agreed language like English. However, the CMS the communication partner is using for delivering documents is often operated by some third party, which may host the CMS frontend in the official country language. This must not necessarily be the agreed language. Registration may not only fail due to technical incompatibilities, but also because of organizational hurdles. For example, one can register with the German E-Postbrief in an official post office of the German Post or via a restricted delivery security service (Post-Ident) where a postman verifies the recipient's identity. However, both options are only available in Germany, which renders the registration of foreign users difficult. Last not least the registration with a new CMS may lead to additional costs. Particularly in CMS with flat rates, where the price has to be paid annually in advance, the costs for sending one or a few messages may be extremely high compared to the rendered services.
- ***Legal challenges***. Even if the registration of a foreign user would be technically and organizationally feasible, legal barriers may prevent it. For example, policies and regulations may restrict the registration to certain user groups, people having their domicile in a particular country or people belonging to particular occupation groups.

Like accustomed to e-mail or traditional mail delivery, users may want to have one mailbox and not to be faced with additional costs and getting familiar with new systems serving the same purpose. As already being normal for e-mail communications, there is a strong need for pan-European and global certified electronic mailing. This issue has become more important with the expansion of the EEA and the creation of the digital single market. Each LSP asks for cross-border CEM where citizens, businesses and administrations can send certified mailings between the different national infrastructures.

Particularly in SPOCS CEM plays a key role. CEM gains in importance, because the Services Directive introduces the principle of tacit authorization.

> "*Failing a response within the time period set or extended in accordance with paragraph 3, authorisation shall be deemed to have been granted.*"
>
> (Article 13 (4) of the Services Directive)

The PSC (or competent authority) has the burden of proof and the response mentioned in Article 13 should thus has evidential value. Since the application procedure is an asynchronous process, the response should be sent to the applicant by using certified mail. In conjunction with Article 8, this means when the application is carried out fully electronically, PSCs should communicate with applicants using a CMS infrastructure. This includes the use of domestic CMS infrastructures abroad. Consider the case of an Italian pizza baker who wants to open a new branch in the Austrian city of Vienna. The Services Directive renders possible to handle the communication with all involved agencies through a PSC in the foreign Member State. The Italian pizza baker wants to carry out the application according to Article 8 of the Services Directive in a fully electronic way. The pizza baker is registered with an

Italian PEC provider and has an Italian eID card that will be accepted in Austria. After having handled the application, the Austrian PSC authority has to send the final official notification back to the applicant with the requirement for a proof of delivery. Because the Italian service provider is already registered within the PEC system, it is not desirable to also register with the Austrian DDS. Because the Austrian PSC authority is a legitimate sender of the Austrian DDS and the Italian pizza baker is a legitimate recipient of the Italian PEC system, this scenario asks for two interoperable CMS, even if both systems are based on completely different technical, legal and organizational policies.

CMS interoperability is a new and challenging research field. In Chapter 4 several promising standards have been discussed. But can one of these standards fill the gap of CMS interoperability? ETSI tried to fill this gap by introducing the REM standard in 2008. Even though ETSI has enhanced the standard with conformance and interoperability profiles, REM, as for the present status of specifications, is tailored to SMTP. In a scenario where only half of existing CMS are based on SMTP, this seems a serious obstacle for REM to become a widely adopted standard. This is also manifested by the fact that REM has been rarely used so far and has not been widely adopted by governments nor by industries. PReM is still in draft status. However, PReM seems not to become an international standard for all CMS. It is primarily intended for UPU postal operators, this means governmental or non-governmental entities designated by a UPU member to operate postal services. Even if the standard would be adopted in the near future, it raises the same interoperability discussion as for REM. What about BusDox? Even if PEPPOL provides a good approach to achieve interoperability between existing systems, it is only applicable in the context of non-evidential document exchange. However, certified electronic mailing concerns far more aspects than just the reliable technical delivery of documents. Certified mailing deals with various non-repudiation services, signatures, authentication qualities, etc. Moreover, the running PEPPOL infrastructure requires all participants to be registered in a central lookup directory. Besides the additional technical and organizational efforts, data protection considerations make this a non-acceptable circumstance for CMS interoperability.

Standards are clearly the first choice to achieve a homogeneous CMS ecosystem in the long term. However, there are so many different CMS out there that a single standard will probably not become prevalent in the near future. Even if standards have been published, it is assumed that in the midterm existing investments will remain. It can be argued that at this point in time interoperability should rather be achieved through an appropriate framework on top of existing systems like it has demonstrated PEPPOL for e-Procurement or STORK for authentication and identification. The fact that CMS interoperability is currently a hot topic is manifested in the European e-Government Action Plan 2011-2015 [European Commission, 2010d] where the EC identifies CMS interoperability as driving force for citizens' mobility.

> "*[. . .] The envisaged actions should ensure the development of interoperable services enabling citizens to communicate, perform transactions, and send and receive electronic documents and information to and from public administrations across the EU. These will allow for delivering secure cross-border exchange and safe storage of electronic information (eDelivery of documents and information). [. . .]*"
>
> (Section 2.2.2 Personal Mobility, page 10)

The following two actions have been defined.

> "*The Commission will support exchanges of best practice and coordinate the efforts of Member States to jointly develop and set up interoperable eDelivery services.*" (2012-2014)

> "*Member States will provide cross-border and interoperable eDelivery services for citizens, for example so that they can study, work, reside, receive health care and retire anywhere in the European Union.*" (2015)

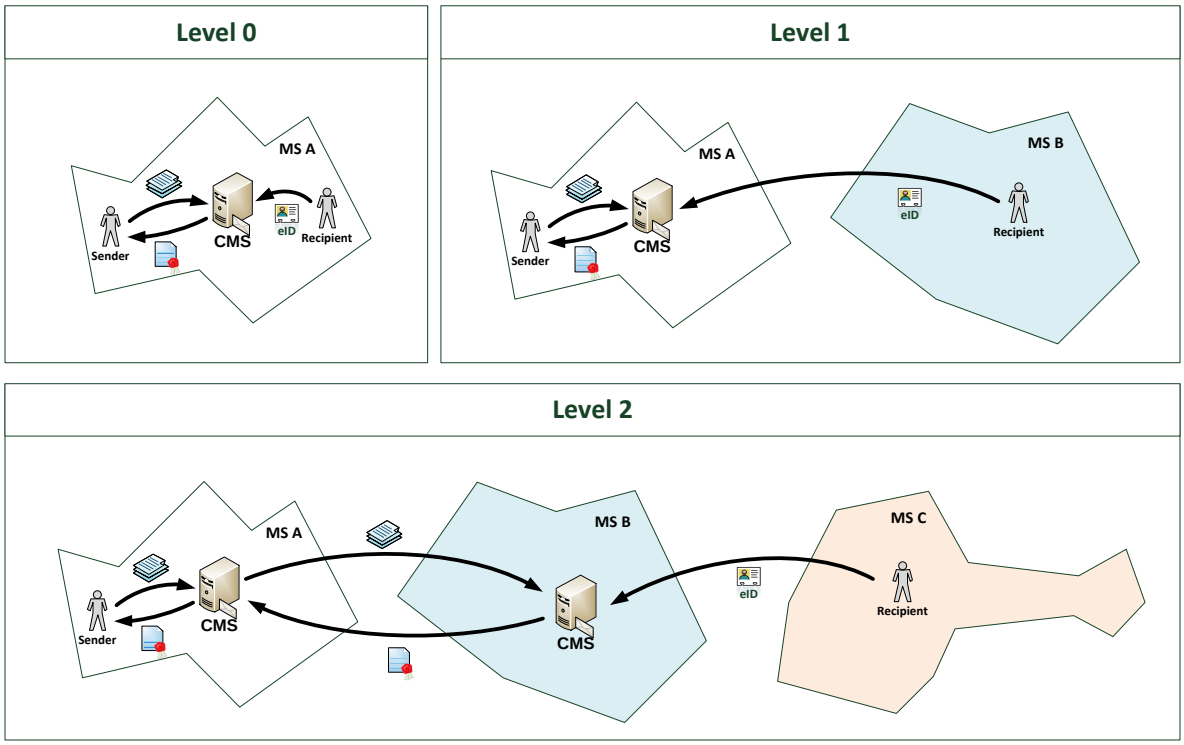

Figure 5.3: The three basic CMS interoperability levels

Recently, initiatives within two European LSPs have been started to address the issue of cross-border CMS interoperability. Besides the qualified identification and authentication of senders and recipients, Pilot 4 (e-Delivery pilot) of the LSP STORK also provides a concept for an interoperable CMS framework. At the same time, and in strong collaboration with STORK, WP3 of the LSP SPOCS develops a specification for a pan-European CMS interoperability framework. The work presented in this thesis has been conducted by the author in the course of these two LSPs. Before continuing to discuss in detail the requirements for such a framework, its concept, process flows, improvements and evaluation, the basic CMS interoperability levels are introduced.

Considering cross-border CMS use cases, the following scenarios can be identified being the basic CMS interoperability scenarios. The scenarios are illustrated in Figure 5.3 and are sorted following increasing complexity. By way of illustration systems residing in different Member States are used to emphasize the location difference. However, the location of a CMS is irrelevant. Interoperability could also be achieved between different regional or local systems.

The lowest interoperability level denotes the domestic scenario, currently the only possible scenario in most systems (due to the fact that most systems are closed). The level number "0" emphasizes the fact that this scenario has nothing to do with interoperability. It can be formally described as follows.

Definition 31 ***Interoperability Level 0****. A recipient of Member State A registers with a CMS of Member State A, for example by using an eID. As a result, the recipient is able to receive messages from senders of Member State A through the CMS of Member State A. The sender receives in exchange an NRD or NRR evidence from the CMS of Member State A.*

In case the recipient's country does not have an own CMS, it is meaningful that the recipient registers with the sender's CMS. Since the complete message delivery is conducted in the sender's territory, only the sender's CMS policies apply. The recipient could further act as sender (if supported) and reach all users registered with this CMS. It can be formally described as follows.

Definition 32 ***Interoperability Level 1****. A recipient of Member State B registers with a CMS of Member State A, for example by using an eID. As a result, the recipient is able to receive messages from senders of Member State A through the CMS portal of Member State A. The sender receives in exchange an NRD or NRR evidence from the CMS of Member State A.*

Level 1 enables authentication at foreign CMS, but has nothing to do with the exchange of documents and direct interactions between different CMS. This is covered by Level 2, which denotes real cross-border CMS interoperability. It can be formally described as follows.

Definition 33 ***Interoperability Level 2****. A recipient of Member State C registers with a CMS of Member State B, for example by using an eID. As a result, the recipient is able to receive messages from senders of any participating Member State (for example A) through the CMS of Member State B. The sender receives in exchange an NRD or NRR evidence from the CMS of Member State B. The envelope content of messages, for example a document, must not be altered on its way from the sender to the recipient.*

This thesis proposes and presents a cross-border CMS interoperability framework for both Level 1 and Level 2 interoperability in the remaining chapters. Before doing so, the requirements and challenges for such a framework are discussed in detail in the next chapter.

Chapter 6

Requirements and Challenges

"A powerful idea communicates some of its strength to him who challenges it."

[Marcel Proust, French Novelist, 1871–1922.]

This thesis focuses on interoperability level 2, which means that two arbitrary CMS are made interoperable so that a sender from CMS A can deliver a message to a recipient from CMS B and in turn evidences are returned from CMS B to CMS A. So far, CMS interoperability has been used as a general term on an abstract level to describe the link-up of two different systems according to this basic scenario. However, CEM has many facets. This is also evident from the numerous CEM properties, which have been discussed in detail in Chapter 3. Their diversity in practice has been confirmed by comparing CMS provided on the Internet in Chapter 4. Both facts make it harder to achieve CMS interoperability.

CMS interoperability can be achieved by several means and to several extents. Before designing an interoperability framework it is thus of utmost importance to define the main requirements, which have a significant influence on the resulting design and architecture. Policies usually regulate and define the (security) properties of a CMS. The diversity and heterogeneity of the CMS ecosystems inevitably raises challenges on different levels when trying to make different CMS interoperable and not violating any (security) property at the same time. This chapter discusses the requirements a prospective interoperability architecture has to meet and what challenges it has to tackle.

6.1 Requirements

From an abstract point of view, existing systems are heterogeneous in various dimensions. The EIF [European Commission, 2010b, chapter 4] describes these dimensions as the four levels of technical, semantic, procedural and legal interoperability. Each of these levels has to be taken into account when aiming for interoperability. The objective of the work described in this thesis is to build an interoperability framework on top of existing systems. Therefore, the main goal is to achieve seamless interoperability by leaving existing systems untouched. This concerns at least the technical, semantic and procedural levels. As will be discussed below in the evaluation chapter (cf. Chapter 12), for certain kinds of deliveries, for example serving administrative documents, changes in the legal environment will be unavoidable for CMS interoperability.

To achieve the goal of seamless CMS interoperability, several requirements have to be met. The following requirements are considered as vital for a CMS interoperability framework.

- Scalability
- Autonomy

- Transparency
- Security and Privacy
- Preservation of Information
- Open Standards
- Design Reuse
- Multilingualism
- Interoperability Agreement

While identifying these requirements, the EIF's underlying principles of European public services have been taken into account. The purpose of the EIF is to help designing European public services and its underlying principles are a good guideline in helping to achieve this goal. Since an interoperability framework acts as a "bridge" between different CMS and end-users like senders or recipients reside in their accustomed systems, the underlying EIF principle of *Accessibility* does not apply. The author of this thesis has already briefly discussed the requirements of scalability, autonomy and transparency in a previous work [Tauber and Rossler, 2010, page 11]. The following section deepens this discussion and introduces six further requirements mentioned above.

6.1.1 Scalability

Requirement 1 *The CMS interoperability framework must use a multilateral solution and support administrative scalability.*

Today a manageable number of CMS can be found on the market. Several governmental systems based on legal regulations can be found in Europe. Postal operator systems and private business CMS are spread all over the world. Some countries have one or a few systems and many countries even have a system at all. However, the trend of a steadily increasing number of systems in today's CMS ecosystem can be observed. Particularly private business CMS offering both hybrid mail and CEM functionalities are springing up like mushrooms. An interoperability framework should be inclusive. This means that every system should be able to reap the benefits from services offered through such a framework. We may think of an interoperability framework on European level under the wings of the EC or even an international framework governed by the UPU. Even CMS clusters should be easily made interoperable. It is conceivable that an interoperability framework could link up a UPU cluster of PReM postal services systems with a European network of national CMS systems. Even systems on a regional or local level, for example custom solutions of private businesses or public agencies like e-Justice systems, should be made interoperable through this framework.

By taking this into account, a first essential requirement is administrative scalability. Administrative scalability means that the interoperability framework is able to handle an increasing number of systems in a single environment. This kind of scalability is often confused with load scalability, which denotes the effective handling of an increasing amount of data either by dynamically reconfiguring the system, applying some load-balancing mechanisms or dynamically increasing hardware resources.

The EIF suggests the use of multilateral solutions to achieve interoperability. A framework with bilateral agreements results in an architecture where each system has as many communications as there are other participants. This induces less efficiency and higher costs. Figure 6.1 illustrates the difference between bilateral and multilateral solutions.

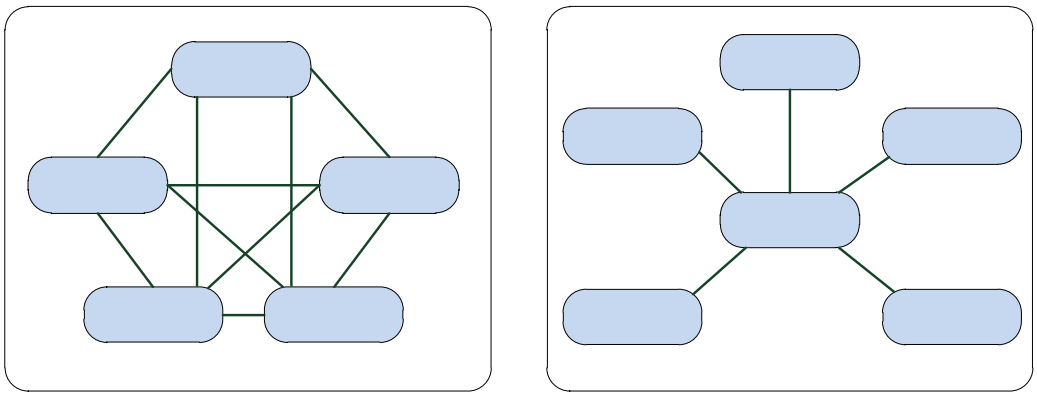

Figure 6.1: Bilateral versus multilateral interoperability solutions. Taken from the EIF 1.0 [European Commission, 2004b, page 10]. The depiction on the left shows an interoperability architecture based on bilateral agreements. Each system is directly connected with each other system. The depiction on the right shows a multilateral solution.

6.1.2 Autonomy

Requirement 2 *The CMS interoperability framework must support the loose coupling of autonomous systems.*

Subsidiarity is one of the underlying principles of the EIF. The Oxford English Dictionary[1] defines subsidiarity as

> "*[. . .] the principle that a central authority should have a subsidiary function, performing only those tasks which cannot be performed at a more local level.*"

This means that in case of a collaboration between national solutions the EU leaves the greatest possible freedom to national solutions. Only unavoidable actions are made on EU level. The principle of subsidiarity may not only be applied at the national level, but may also hold on a regional level within a country or even on local level. Subsidiarity thus implies the most decentralized level of control which is appropriate. The least degree of standardization is the result and orchestration is only needed and applied in case no transparent inter-working is possible.

Subsidiarity grants systems the highest degree of autonomy. This means that the interoperability framework and single CMS should not have any mutual dependencies. Consider a CMS, which wants to join a cluster or network of other CMS coupled by some kind of interoperability framework. In no case the joining of a single system must lead to modifications or adaptions in other CMS or the interoperability framework itself. Moreover, changes in the internal behavior of a system must have absolutely no effect on the overall interoperability framework. If this requirement is not met, it may lead to a chain of reactions in single systems and cause huge efforts and costs. From a technical point of view, autonomy means that in the best case the joining of a single system is not noticed by other systems. Thus it can be stated that a loose coupling is necessary so that systems joining or leaving the interoperability framework can easily be coupled and decoupled. This is a great benefit because autonomy is tightly related to scalability and eases to meet this requirement.

Autonomy should be realized by requiring no or only minimal changes to systems joining the interoperability framework. In no case other systems must be affected. Open and standardized interfaces for the integration of single systems into the framework definitely facilitate the goal of autonomy and reduce complexity and implementation efforts.

[1] `http://oxforddictionaries.com/definition/subsidiarity`

6.1.3 Transparency

Requirement 3 *The CMS interoperability framework must be able to transparently couple different systems.*

Transparency depends on autonomy and is a desired requirement. In the best case, different systems can be bridged without affecting their own infrastructures. Transparency means that national complexities are hidden by the interoperability infrastructure and that in the best case system entities are not aware of the fact that the CMS is connected to another one. In this context, location transparency is very important. Location transparency implies that senders and TTPs should not care if a recipient resides in the own system or in a foreign one. As an example scenario, a transparent architecture would allow an Italian sender to enter the Belgian registered e-mail address in the PEC client software instead of the address of an Italian recipient. The sender has not to care where exactly the recipient resides. Depending on the recipient's location, a transparent architecture routes the message to the correct destination.

Transparency is desired in the various dimensions of technical, semantic, procedural and legal transparency. This implies that a CMS should not care about the technical characteristics of other systems. System technologies should remain as they are and systems should be made interoperable even if they operate on totally different communication protocols, for example SMTP and Web services. An interoperability framework should be payload-agnostic and be generic enough to serve all kinds of documents and business scenarios. Transparency also concerns the semantic level. Meanings must remain the same for non-repudiation services, authentication levels, signatures, etc. On an organizational and procedural level, transparency should ensure the automated establishment of trust between different CMS. Entities of one domain must not be aware of trust instances of other domains, for example TTPs or PKIs. Moreover, a transparent architecture does not require users to be registered in additional central directories. This may lead to data privacy violations and prevent certain systems to join the interoperability framework. Even fairness and timeless, which have different characteristics in any system, must be transparently preserved. Fairness and timeliness between two different systems in the bridged state may not be ensured anymore, because in most systems the number and types of evidences as well as delivery deadlines are defined by policies and are thus different. In "de jure" systems they are actually regulated by law. Last not least, a legal or political consensus is needed to set up a transparent governance structure. Even if the latter requirement is out of scope of this thesis, this aspect is discussed in more detail in the evaluation chapter (cf. Chapter 12).

6.1.4 Security and Privacy

Requirement 4 *The CMS interoperability framework must respect security and privacy provisions of single systems and provide an overarching framework with well-defined security policies.*

This is a "horizontal" requirement and takes into account the security design principles of confidentiality, integrity, availability, authenticity and accountability when building an interoperability framework. It is important to not just secure single components, but consider the security of the overall framework. A clear and understandable security policy is also vital. Such a security policy must cover the need of single systems. This means that the security and privacy requirements of single systems must not be threatened by integrating the system into an interoperability framework. This requires well-defined interfaces between systems and the interoperability framework. Interfaces must be clearly defined and regulated by appropriate security policies. Consider the scenario where the Italian PEC and the Austrian DDS are somehow coupled through an interoperability framework. The Italian PEC is not a completely closed system and under certain circumstances allows that standard e-mail users may send regular e-mails to a PEC account. Even if these kinds of e-mails are clearly marked as "non-PEC", the Austrian DDS is a closed system and only accepts messages from registered CMS (in this case PEC) users. This security policy must in no case be violated by a PEC system, which forwards incoming "non-PEC" messages to

the foreign DDS. Another cross-border scenario would be authentication. For example, the German De-Mail system binds certain certified mail qualities and delivery options to the recipient's authentication level and quality. Even if in the cross-border scenario the recipient resides in a different system, De-Mail should be able to enforce its security policy. This requires a common understanding of authentication and identification across borders, the publication of supported authentication levels by the foreign system and the enclosure of authentication information within cross-border CMS messages. Summarizing, the interoperability framework must be a trusted environment, which respects national, regional or local regulations.

Besides security, privacy must also be taken into account. Each CMS may have its own data privacy regulations, which must be respected. An interoperability framework must not require the exposure of data that may violate local data privacy regulations. A good example is the exposure of recipients' personal or address data. Some CMS operate central lookup directories in terms of white pages. The registration in such directories is compulsory in some CMS. In others it is done on a voluntary basis. For data privacy considerations some CMS explicitly do not have such lookup provisions. Even if a system operates a lookup directory, the access of foreign systems and use of data abroad may not be allowed. The privacy regulations of single systems must be respected. Nevertheless, for natural persons a central lookup directory might be questionable like it has been done by PEPPOL for BusDox for legal persons or is going to be provided by e-CODEX. For these projects, using central registries is reasoned by the fact that recipients in PEPPOL and e-CODEX are mainly legal entities where information about these entities is already publicly available from constituent registers like the commercial register. Standard CMS systems, however, not only serve administrations and businesses, but have large user databases of physical persons where data privacy is a crucial issue.

6.1.5 Preservation of Information

Requirement 5 *The CMS interoperability framework must support the generation of a customizable audit trail for cross-border transactions.*

Most CMS provided on the Internet have transferable evidences. This means that sender and recipient receive (signed) evidences, which can be archived and used in arising disputes on demand. However, users may forget to archive evidences, unintentionally delete evidences or evidences may even get permanently lost due to a computer breakdown. For this reason many CMS operators have policies that force their TTPs - in most cases delivery agents - to preserve evidential information for a certain period of time. For example, the law of the Italian PEC renders the preservation of transactional information for all PEC providers obligatory. PEC providers must keep an audit trail of evidential log information regarding the messages (not the message content) for 30 months. According to the PEC specifications [Repubblica Italiana, 2005b, page 9], the following message information has to be preserved:

- Message-ID
- Timestamp
- The sender's PEC address
- The recipient's PEC address
- The message subject
- The log event (acceptance, retrieval, error, etc.)
- Related message-IDs
- The sender's PEC provider

This example illustrates the variety of potential log data. In addition to the data mentioned above, other systems preserve evidences or further information about electronic signatures, non-repudiation services, timestamping services, etc. According to the principle of subsidiarity and by taking into account autonomy and transparency, an interoperability framework should respect a system's data processing regulations and policies. An interoperability framework must have provisions to document cross-border transactions. The granularity of information, this is the type and amount of information, must be customizable by each system.

6.1.6 Open Standards

Requirement 6 *The CMS interoperability framework must use open standards to facilitate autonomy and scalability.*

The use of open standards is vital for a flexible, effective and sustainable interoperability framework. "Open" usually means that a standard is publicly available and has undergone a development process, which has not been dominated by some interest group. If an open standard contains parts, which are subject to a patent, licensing fees must be "reasonable and non-discriminatory".

The benefits of open standards in an interoperability environment are its technology and product independence. Independent from the underlying implementation, software components can smoothly interact. Particularly in today's global networking, communications not based on open standards are unimaginable. Regardless if someone sits in a coffee shop with a tablet Personal Computer (PC) connected to the Internet through a Wireless Local Area Network (WLAN) hotspot or someone sits in the train and is connected to the Internet through a notebook and a 3G access, both can seamlessly communicate with each other because all components from the hardware layer up to each single software part involved in the communication operate on open standards like WLAN a/b/g/n or TCP/IP. With open standards, users can freely choose, which products they want to use. Today this is a major user demand and firms not using open standards often have problems establishing themselves on the market, because proprietary solutions usually create a vendor lock-in and users are bound a product's lifetime to a particular firm.

At the bottom line, particularly for CMS joining an interoperability framework, open standards provide flexibility, choice and efficiency and they foster the requirements of autonomy and scalability and allow for an easier integration of new systems into the framework.

6.1.7 Design Reuse

Recommendation 1 *The CMS interoperability framework should reuse existing components to ensure a faster and cheaper development by relying on best-practice and components tested for reliability and robustness.*

This is rather a recommendation than a strong requirement. By integrating existing standards and components like building blocks or software parts in a larger context, the development of an interoperability framework would be faster and cheaper. Moreover, it can rely on components tested for reliability and robustness. For example, this is eased by using open standards not being protected by any Intellectual Property Rights (IPRs) in a component-based service model by reusing components through SOAs like Web services. Regarding reusability, particularly on EC level, ISA and formerly the IDABC and IDA programmes are very active in this field and have already made numerous contributions. Many recommendations, guidelines and architectural frameworks have been elaborated by these programmes. The most relevant publications include the EIF, the EIAG and the EIIS report. Last not least, the European LSPs like PEPPOL and STORK have elaborated basic interoperability building blocks for standard cross-border processes in the context of e-Procurement and eID. PEPPOL, as already discussed, creates

an interoperability framework for public e-Procurement. As a result, PEPPOL has developed BusDox (cf. Section 4.3.4.2), a transport infrastructure for reliable exchanging documents between heterogeneous e-Procurement environments. STORK provides an interoperability framework for the mutual recognition of eIDs across Europe and upon its completion hands over a set of common specifications and open modules, which are licensed under the European Union Public License (EUPL) in order to be integrable in other open source projects without any problems. It is thus beneficiary to use the outcome of all the mentioned initiatives when designing a CMS interoperability framework.

6.1.8 Multilingualism

Requirement 7 *The CMS interoperability framework must support multilingualism for control information on the message level.*

The use and support of multiple languages is a crucial success factor for cross-border services, because if not implemented correctly it may pose a great barrier for foreign users. This is particularly a challenge in the EU with the large number of 23 official languages.

CEM is operating on the message level and as discussed, a CMS interoperability framework should be payload-agnostic. This means that message contents must not be touched in any way. Therefore, multilingualism on document level is not a CMS interoperability framework's business. This is out of scope and depending on the use case and context it must or should be provided by the sender. However, control information like errors, notifications or success messages are very well subject to an interoperability framework. Since this kind of information is often displayed to senders or recipients by means of evidences, multilingualism is a particular matter of interest. This could, for example, be solved by introducing a harmonized set, a common language of control information used to map between the languages used in the single CMS.

6.1.9 Interoperability Agreement

Recommendation 2 *The CMS interoperability framework should have an interoperability agreement regulating all cross-border relevant aspects.*

A good interoperability framework needs an agreement, a policy which regulates several behavioral aspects like the exchange of messages, security, privacy, trust, dispute resolutions, etc. Even if many CMS can directly be mapped by the framework itself, some have to be regulated by an agreement. The next section discusses challenges for an interoperability framework on the technical, semantic and procedural level and identifies what aspects could be mapped by the framework itself and what aspects should or could be solved by an interoperability agreement.

6.2 Challenges

In the domestic (closed) CMS scenario all entities deal with the same regulations, policies, business processes, semantics and technologies. This means that different entities communicate over common interfaces, they know the meaning of each CMS object like exchanged messages and evidences or other infrastructural parts and they know potential process flows within the system. Entities communicate in a trusted environment. Even if sender and recipient do not know each other, they are faced with well-defined and well-known TTPs and trust relationships. All these assertions are only valid within the CMS boundaries. By crossing the CMS boundaries all the assertions made are not valid anymore. When thinking of two or even more systems being somehow coupled, one may encounter different policies, business processes, semantics and technologies. Crossing the own system boundaries also leads to unknown TTPs and trust relationships.

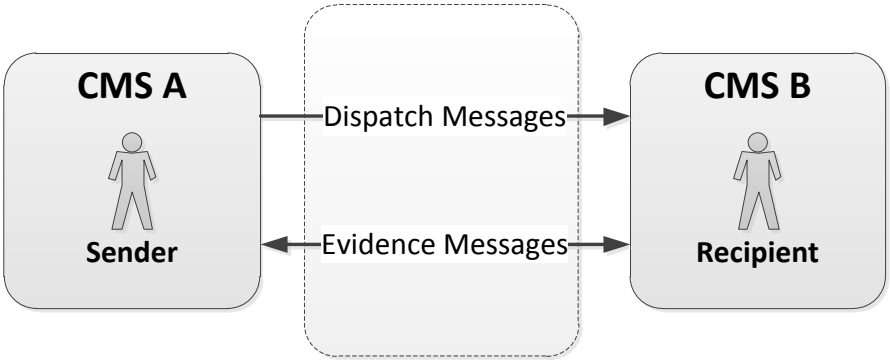

Figure 6.2: Abstract CMS interoperability scenario between two systems.

Figure 6.2 illustrates this coupled state model where two systems are made interoperable. This visualization is made from a very abstract point of view to illustrate the two basic message flows. In the cross-border scenario some entities reside in different domains. As illustrated in Figure 6.2, this applies at least to the sender (CMS A) and the recipient (CMS B). This model does not make any further assumptions about the number of TTPs, where they are located and how the message is transmitted from the sender to the system's boundaries. It is assumed that between CMS A and CMS B there is some kind of interoperability framework, which is illustrated as "black box". As discussed in Chapter 4, all CMS have two message types: dispatch messages and evidence messages. Dispatch messages are just unidirectional. They straightly proceed from the sender to the recipient. Evidence messages may flow in both directions. Even if most evidences flow from the recipient or the recipient's MTA or MS towards the sender, there are some exceptions like an NRO evidence. Bearing in mind this abstract conceptual interoperability model, the "black box" interoperability framework is faced with numerous challenges. According to the EIF's interoperability levels, a framework may be faced with technical, semantic, procedural and legal challenges. Even if overcoming legal challenges and hurdles is a very important issue to achieve interoperability also in operational environments, it is out of scope of this thesis. Nevertheless, the current legal situation of cross-border CEM and missing pieces are discussed in detail below in the evaluation chapter (cf. Section 12.5).

The author of this thesis has discussed the challenges of cross-border document exchange in depth in [Tauber and Rössler, 2010c] and [Tauber and Rossler, 2010]. The following sections deepen the identified multi-dimensional challenges on a technical, semantic and procedural level.

6.2.1 Technical Challenges

Technical challenges arise when trying to make systems interoperable on the technical level. But what means achieving interoperability on the technical level?

The EIF 1.0 [European Commission, 2004b, page 16] describes the dimension of technical interoperability as follows:

> "*This aspect of interoperability covers the technical issues of linking computer systems and services. It includes key aspects such as open interfaces, interconnection services, data integration and middleware, data presentation and exchange, accessibility and security services.*"

This kind of interoperability can be classified into technical and syntactical interoperability. The first denotes the link-up of hardware or software components to achieve end-to-end communication so that

datagrams or packets can be sent between hosts. This includes all layers of the Open Systems Interconnection (OSI) model from the physical, data link, network, transport up to the session, presentation and application layer. Syntactical interoperability means that systems communicating with different data formats can seamlessly exchange data. For example, Web services data formats comprise XML, SOAP or HTTP. Other data formats are for example ASN.1 or programming language formats like JAVA, C, etc. Provided that two different CMS communicate over the Internet and are thus linked up on the same network and transport layer with respect to the OSI layered model, an interoperability framework may carry out conversions on the session, presentation and application layer. A typical conversion on the presentation layer is character encoding and decoding, for example between American Standard Code for Information Interchange (ASCII), Extended Binary Coded Decimal Interchange Code (EBCDIC), ISO-8859-1 (Latin alphabet No. 1) and UCS Transformation Format (UTF)-8. Others include data conversions for newline data codes (CR/LF to CR), encoding schemes like Base64 and Quoted-printable or even encryption and decryption of sensitive data.

The evaluation and comparison of CMS (cf. Section 4.4.2) shows a uniform distribution of systems, which make use of the e-mail communication protocol and Web services technologies. An example would thus be the protocol conversion on the application layer from Web services based architectures using the SOAP family - SwA, MTOM, etc. to e-mail based architectures using the SMTP protocol family. This technical and syntactical link-up is obviously rather straightforward and easy to accomplish.

Things get more complicated when cryptographic protocols are involved. In most CMS, evidences are electronically signed. Data modifications, actually already a single bit modification, invalidate a signature. However, since character and protocol conversions are necessary for interoperable systems to communicate with each other, provisions must be made that an interoperability framework does not remove any inbuilt or inherent security functionalities. So how to deal with that? One solution for this problem are signature transformation services. They convert a signature format into another one, for example e-mail based signatures (Public Key Cryptography Standards (PKCS) #7, S/MIME or the Cryptographic Message Syntax) to XML digital signatures used in Web services and vice versa. Such an approach is described by Stranacher and Zwattendorfer [2009]. In this way the signature transformation service acts as TTP by validating the original signature and applying a signature to the new format. An attestation is attached to document the signature validity of the original format for long-term archival (in case disputes arise). Even when signature transformations seem feasible from a technical point of view, electronic signatures have several semantics, which risk to get lost or wrongly translated. This issue is discussed in more detail in the next section.

The only interoperability knock-out criterion would be the CEM confidentiality property. This does not effect point-to-point encryption as SSL or TLS on the presentation, but rather E2EE on the protocol layer, comprising the encryption of the whole payload and the message envelope (metadata). In this case a conversion cannot be carried out on the application layer by an interoperability framework. Two different systems featuring an identical or similar transport protocol and E2EE mechanism could potentially be coupled, even if E2EE is applied. However, this depends on the degree of similarity and applied domain policies. A possible scenario would be the coupling of two e-mail-based CMS where no essential information are included in the e-mail headers. Both CMS would operate on the same protocols and the dispatch content could be seamlessly delivered to the foreign recipient. The similarity considerations made so far just apply to dispatch messages. Evidences have more system-specific semantics and may need an appropriate translation (unless a common standard like ETSI REM is shared between two systems).

6.2.2 Semantic Challenges

Even if systems are successfully linked up on the technical level, exchanged information must be correctly interpreted by the receiving system.

The EIF 1.0 [European Commission, 2004b, page 16] describes the dimension of semantic interop-

erability as follows:

> "*This aspect of interoperability is concerned with ensuring that the precise meaning of exchanged information is understandable by any other application that was not initially developed for this purpose. Semantic interoperability enables systems to combine received information with other information resources and to process it in a meaningful manner.*"

Of course seamless semantic interoperability is a desired state where no knowledge is required of how the information was produced. A common understanding should be achieved through appropriate mappings in the context of an interoperability agreement rather than standardizing it. Standardization inevitably leads to modifications in systems. This should whenever possible be avoided. Mappings may be employed by producing so-called interoperability assets, specifications based on dictionaries, thesauri, ontologies, registries or taxonomies.

By looking at CMS, messages may not only differ at the protocol level. Their information having the same meaning may be structured differently and is thus at risk of being wrongly interpreted. This concerns dispatch and evidence messages in equal manner.

Dispatch Messages

Dispatch messages contain routing information and data uniquely addressing the recipient. This dataset may range from unique identifiers (e-mail address or national identification number) to other personal information (name, date of birth, residence, etc.). A misinterpretation may eventually lead from wrongly routed messages with legal consequences to a recipient who has never seen the message. Message IDs are an integral part to uniquely identify dispatch messages. Such IDs are used as references in messaging threads, for example to group messages in client applications, or to uniquely assign evidence messages to their related dispatch message. A wrong interpretation of such IDs may lead to evidences attesting events of wrong or even not existent dispatch messages. The (legal) consequences would be grave and security and trust of the whole framework would be at risk. Last but not least, timeliness is another property that has to be carefully interpreted as it is often bound to (legal) deadlines, for example a period for appeal. Consider the case where an interoperability framework wrongly interprets the date or timezone of a dispatch message expiration time whereupon the message is automatically deleted too early.

Evidence Messages

Evidence messages also have several elements, which may be subject to misinterpretation. Especially the event of an evidence is affected by that. Assuming that two different systems describe their evidences as "delivery confirmation" attesting a final delivery event, the evidences may yet have completely different meanings. On the one hand, CMS A may produce an NRD evidence upon the message has been stored into the recipient's MS and call it "delivery confirmation". On the other hand, CMS B may produce an NRR evidence as soon as the recipient has accepted and retrieved the message from the MS and call it "delivery confirmation". Both evidences attest completely different events and may thus have different legal consequences. Since evidences are often regulated by public law, such a distinction is vital. It is therefore meaningful to bind evidences to messaging-related events like delivery, acceptance, rejection, retrieval, download, etc. A taxonomy of such events certainly helps to create a common understanding of evidences across different systems.

Authentication is also an important CMS aspect. We can find various authentication mechanisms in existing CMS. They range from weak password-based authentication to secure methods based on two-factor mechanisms like mTANs or smartcards. Many countries have already recognized the need

for qualified eID and have rolled out solutions on the national scale. These eIDs usually have the same quality as official ID documents and often provide additional electronic signature functionalities with the same legal value as a handwritten signature. Each CMS benefits from using such a qualified eID. NRR evidences have a stronger legal binding or CMS providers may offer value-added services based on qualified eIDs. For example, the German E-Postbrief offers a so-called "Post-Ident" service, which allows recipients to be identified online so that they can for example enter a subscription-based contract for a mobile phone or open a bank account by electronic means. Governmental CMS often bind certain delivery qualities to a recipient's authentication quality to deliver personal documents to the right person. De-Mail is such an example. Like for evidences, it is also important to have a classification and common understanding of authentication and identification qualities across CMS as wrong interpretations may have legal consequences. In conjunction with authentication, delegation is also an important aspect. CMS processes are in many cases carried out by a proxy. Deliveries are often taken in charge by relatives or neighbors (having a postal mandate or not). Systems may want to know this circumstance and document it accordingly. A CMS may also state that certain messages cannot be retrieved by a delegate. Therefore, mandate management is also an important cross-border aspect to consider.

A similar discussion arises for electronic signatures. CMS policies often require evidences to be signed with a certain quality, for example with a HSM. There are few references providing a common understanding of signature qualities. As discussed in detail in Chapter 4 (cf. Section 4.4.1), one example is the EU Signature Directive, which defines the requirements for the creation of AdES and QES. According to the Signature Directive, QES must be created using an SSCD and are legally equivalent to handwritten signatures. However, existing CMS use many variants of electronic signatures that are not covered by the Signature Directive. This issue is also discussed in a publication by the author of this thesis [Zefferer et al., 2011]. Like for the evidence and authentication discussion, it is thus vital to have a common understanding of electronic signatures, either on a technical level or regulated by an appropriate interoperability agreement.

6.2.3 Procedural Challenges

Besides technical and semantic challenges, interoperability also has to deal with different business processes when trying to couple different CMS. The EIF 1.0 [European Commission, 2004b, page 16] describes the dimension of procedural interoperability as follows:

> "*This aspect of interoperability is concerned with defining business goals, modeling business processes and bringing about the collaboration of administrations that wish to exchange information and may have different internal structures and processes. Moreover, organizational interoperability aims at addressing the requirements of the user community by making services available, easily identifiable, accessible and user-oriented.*"

From a communication perspective, it is obvious that only the Store & Forward (S&F) messaging style (cf. Section 4.3.1) is supported. This means that the message must be forwarded from the sender's CMS to the recipient's CMS. In order to meet the requirement of transparency, the Store & Notify (S&N) messaging style cannot be supported by an interoperability framework. On procedural level, CMS mainly differ in their evidence process flows. Evidences are issued by entities at different instants of time and their number and types heavily vary from system to system. Chapter 4 (cf. Section 4.4.2) discussed the disagreement regarding evidences by implementers and standard designer. Even if an agreement on the semantic level can be reached regarding the exact meaning, what happens if certain evidences are simply not available in foreign CMS? The lack of certain evidences may lead to interrupted process flows and eventually threaten the core CEM security property of strong fairness. It is not desired that a system's policy will be violated this way with possible legal consequences. To prevent this scenario, the requirement of transparency has thus to be met. As discussed above, fairness will be maintained this way.

Besides preserving fairness, trust is another challenge. The transparency requirement asks for implicit trust relationships between different systems. Entities of one system should not care about bilaterally establishing trust with single entities of another system. So how can a sender or TTP trust the issuer of an evidence coming from a foreign system? With respect to scalability and autonomy, it has been stated that systems should seamlessly integrate into the interoperability framework without affecting other systems. Thus, if new systems join an interoperability framework, how can already integrated systems trust the new system or entities within? These questions will not only have to be solved on a technical, semantic and procedural layer, but will definitely deserve some kind of interoperability agreement.

Another CEM security property, which is affected by procedural disagreements, is timeliness. Several systems have well-defined timeframes and deadlines for the forwarding, delivery, retrieval and expiration of messages. When deadlines expire, an evidence is usually generated to terminate the CMS protocol execution. But what if another system has different deadlines or even no deadlines? This issue is particularly crucial since many administrative and judicial procedures have a period for appeal, starting with the legally effective delivery, which may start after expiration of a deadline for retrieval. Without tackling this issue, system policies will be violated and disputes may arise. This has to be solved in a similar manner as for the fairness issue, this means on the procedural level together with an appropriate interoperability agreement.

Cross-border addressing of recipients and other entities is one of the most challenging parts when coupling different CMS. Recipients can either be addressed with unique identifiers or other data related to the recipient's identity, for example given name, family name, date of birth or postal addresses. The dominating addressing schemes in existing systems are unique identifiers, either unique national identifiers or regular e-mail addresses. National IDs like resident numbers or tax numbers have one advantage over the e-mail address format. If a CMS does not have some kind of directory or lookup service, the recipient's e-mail address may not be at hand. A national ID, however, may be determined through central registers. This kind of addressing scheme can thus be of help when public proceedings are not initiated by the citizen, for example in the case of traffic offense penalties. Interoperability efforts are faced with both national data privacy protection legislations and technical protocol limitations. Legal regulations may prohibit the use of national IDs, directories and lookup services abroad. Addressing may also lead to technical incompatibilities. Consider for instance an Italian public administration trying to address an Austrian recipient with given name, family name and date of birth. The Italian PEC sender using a standard e-mail client will thus be faced with protocol and software limitations when trying to enter the address of an Austrian recipient into the "To:" field. Questions arise how to solve this issue reasonably. Define the e-mail address format as the standard format? Most existing systems already use e-mail addresses no matter whether they have Web services or e-mail architectures. Member States not supporting this kind of addressing scheme would have to introduce and integrate it into their domestic system. In this way recipients would have the opportunity to use their "qualified e-mail" no matter in which Member State they are making an application. Rather than achieving interoperability by standardizing addressing, another approach could make use of national solutions dealing with addressing issues in order to overcome technical and organizational barriers. Addressing can surely be considered as one of the major challenges. Even if this challenge is mainly a domestic issue, it has to be taken into account by an interoperability framework to ensure transparency and thus to hide the complexity of each system.

After having identified and discussed the main requirements a CMS interoperability framework has to meet and what challenges it has to tackle, the next chapter continues to introduce the concept of the CMS interoperability framework proposed in this thesis.

Chapter 7

CMS Interoperability Concept

"An idea whose time has come was waiting there all along."

[Carrie Latet, Poet.]

The aim of this thesis is to provide a concept for an interoperability framework being able to couple arbitrary CMS. The main focus is on achieving Level 2 interoperability and the framework should be able to couple different CMS in a way that the requirements stated in Chapter 6 are met. This means the framework should be scalable, transparent, secure, multilingual, use open standards, reuse existing components, preserve systems' autonomy and privacy, audit trails and allow the dynamic reconfiguration by an appropriate interoperability agreement.

Therefore, this chapter introduces and discusses the interoperability framework, which has been developed by the author as part of WP 6.4 - the e-Delivery Pilot[1] - of the European LSP STORK. Even if the focus of STORK is on identification and authentication, the objectives of the e-Delivery pilot had a much broader scope from its beginnings. The STORK description of work states [STORK Consortium, 2010, page 10]

> "*The objective of this pilot is to demonstrate cross-border electronic delivery based on the existing domestic infrastructure. It is essential for e-Government to conclude transactional processes electronically and inter alia also requested by the Service Directive to be able to transact administrative procedures fully electronically.*"

Besides demonstrating Level 1 interoperability, this means, the integration of the STORK authentication framework into operational CMS, the pilot also developed an interoperability framework for the secure, reliable and evidential document exchange between different CMS (Level 2 interoperability). Even if the pilot objective was to demonstrate Level 2 interoperability just between the Austrian DDS (cf. Section 4.2.1) and the Slovenian Moja.posta.si (cf. Section 4.2.4), a generic framework was developed to serve all business scenarios and different kinds of CMS by meeting the stated requirements at the same time. The remainder of this chapter introduces in detail the core elements of this framework, which have been discussed by the author of this thesis in several publications [Tauber and Rossler, 2010; Tauber et al., 2011c; Rössler and Tauber, 2009]. The Level 1 interoperability concept of the STORK e-Delivery pilot is introduced in detail in Chapter 11.

The concept presented in this chapter has been taken up by the European LSP SPOCS where several architectural and communicational aspects have been improved with respect to addressing, efficiency, design reuse, open standards and interoperability agreement. The author of this thesis was heavily involved in this process. Even if the SPOCS framework demonstrates the interoperability between six

[1] The author of this thesis was leading the pilot from July 2010 to June 2011.

systems[2] only, the interoperability framework is designed in a generic way to serve all kinds of CMS. The outcome of these improvements are reviewed in detail in Chapter 9.

The remainder of this chapter presents the scalable CMS interoperability framework. First, the conceptual model is introduced and discussed. This model adopted the concepts of the EIF to serve the needs for CMS interoperability. The second part of this chapter discusses how the single conceptual elements have been realized by using open standards and by reusing existing components and concepts to meet all stated requirements.

7.1 Conceptual Model

Interoperability between systems can basically be achieved in two different ways. Either through bilateral or multilateral solutions. Bilateral means that each couple of systems has its own way of achieving interoperability, for example by defining a mutual way of exchanging data on a technical level, finding common meanings for uniform semantics and aligning business processes. Obviously this kind of solution has one major drawback. It is not really scalable, because if each couple has an individual way of achieving interoperability, the resulting framework leads to an N-to-N interconnection architecture. The number of links is heavily increasing with the number N of systems ($\tilde{} N^2$). Instead of establishing direct links between the single systems, a central hub could manage interoperability. However, this does not mean that the number of transformations is reduced in any way, the full load has just to be carried out by the hub. By contrast, a multilateral solution uses a kind of mapping between single systems and an agreed understanding to achieve interoperability. This solution has the major benefit over bilateral ones in terms of being more scalable, since the total number of link-ups equals N. Like in the case of bilateral solutions, a multilateral one could also use a central hub or a decentralized way to establish the link-up between systems. A major drawback of a uniform mapping is of course a certain degree of information loss, since not all aspects of all systems can be mapped. Nevertheless, (administrative) scalability is an essential requirement and the presented concept thus uses a multilateral approach.

Before discussing the details and core elements, the conceptual model is sketched from an abstract point of view. For this purpose the conceptual model of the EIF [European Commission, 2010b, page 13] has been chosen, because it is an abstract model to sketch multilateral solutions and is further able to meet the requirements stated in Chapter 6. The EIF model is a result from a survey evaluation of the implementation of (European) public services. However, the model is not only applicable to public services. It can actually be applied to any kind of service. Furthermore, it reflects best-practice and is thus based on successfully tested systems and also incorporates lessons learned from failed designs and implementations. Since the model does not commit itself to particular design paradigms and underlying architectures, it is a generic and promising approach to show how interoperability can be achieved by defining building blocks on an abstract level to ensure interconnection and reusability. The model has two main objectives. First, access to various information sources (central registries, databases, etc.) should be eased. Second, existing public services should be combined so that users can access them in a uniform way. The conceptual model of CMS interoperability refers to the latter objective to combine different CMS such that the Level 2 interoperability of real cross-border document exchange is achieved by allowing senders to transparently and seamlessly address recipients of a foreign CMS.

Figure 7.1 illustrates a slightly adapted version of the EIF conceptual model [European Commission, 2010b, page 13] to serve the needs for CMS interoperability. The basic rationale behind the model is to connect loosely coupled modular service components in a harmonized way. The loose coupling facilitates scalability and guarantees autonomy so that if new components get connected or disconnected, all other components are not affected. The EIF defines three basic components. Base registries (residents registers, driver's license database, criminal records register, etc.), external services (payment services,

[2] Among those are the Austrian DDS, the Italian PEC and the German EGVP

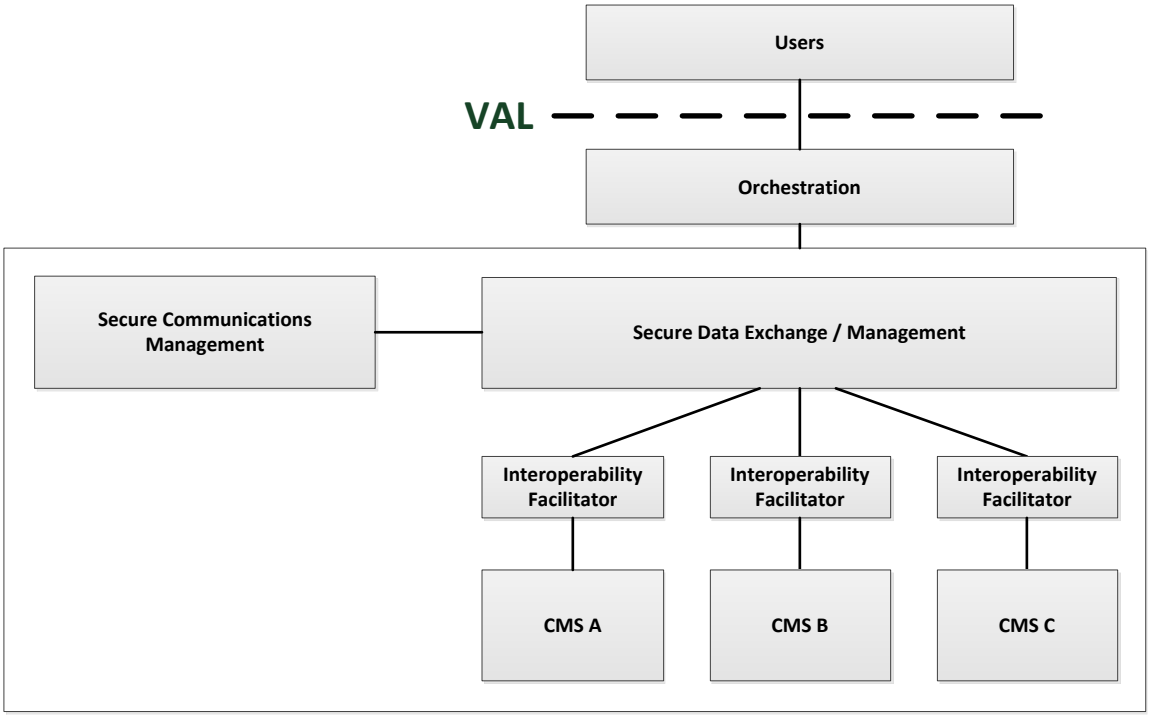

Figure 7.1: Conceptual model of the CMS interoperability framework according to the EIF [European Commission, 2010b, page 14].

telecommunication services, etc.) or *Interoperability Facilitators*. A facilitator is basically an intermediary component, which carries out conversions and translations on different interoperability levels and thus acts as information or transaction broker. As illustrated in Figure 7.1, the CMS interoperability conceptual model makes use of these facilitators to hide the complexity of single CMS. This ensures the requirements for transparency and scalability.

A so-called *Secure Data Exchange Layer* is the core of the model to ensure a multilateral solution whereby all exchanged data between the single interoperability facilitators has to pass through this layer. It can be seen as a harmonized layer with a common approach to ensure security. Such an approach is considered as necessary driver for interoperability. According to the EIF, the secure data exchange layer ensures that communications between interoperability facilitators are:

- ***Signed and certified***. Security provisions ensure that the communicating entities (interoperability facilitators) are authenticated and identified. Authenticity and integrity of exchanged data must be secured through basic mechanisms like digital signatures, electronic certificates, timestamps, etc.
- ***Encrypted***. Communications through this layer must be protected from disclosure by employing strong cryptography to ensure confidentiality.
- ***Logged***. An audit trail of certain parts of the communication provides evidence if a dispute arises. Therefore, these data should be appropriately logged and archived for later retrieval by an inspector. The audit trail ensures the requirement for preservation of information.

All the mentioned properties of the secure data exchange layer ensure security, privacy and preservation of information. The communication of the layer is monitored and controlled by a *Secure Communications Management* component. The main tasks of this component are:

- ***Service management***. Monitor the adherence of security functions like identification, authentication, authorization, data transport, etc.
- ***Service registration***. Checks whether connected interoperability facilitators are trustworthy and thus authorized to take part in the communication.
- ***Service logging***. Observe the generation and digital archiving of audit trail data.

All components, this means the interoperability facilitators, the secure data exchange layer and the service communications management component must be build upon open standards and wherever possible reuse established designs, technologies and components to meet the requirements stated in Chapter 6.

There is a slight difference between the CMS and the EIF conceptual model regarding user management. The EIF model enables the aggregation of services through orchestration so that multiple basic services appear as one single system. Popular examples are so-called *One-Stop-Shops*, where citizens or businesses can conduct all administrative tasks at one single point, for example a central portal. The PSC principle of the EU Services Directive can also be considered as a one-stop-shop for companies for the establishment of a new business abroad. The concept of aggregation is slightly modified for the CMS model. Interoperability facilitators and thus implicitly all connected CMS are aggregated by the secure data exchange layer through orchestration. The orchestration is steered by an interoperability agreement. Users, however, do not access foreign CMS through this aggregation interface. They still reside in their own system. So in Figure 7.1 the user, which is drawn on top, actually resides on the bottom as part of a CMS. It is nevertheless drawn on top to illustrate that foreign CMS services can be accessed through a so-called Virtual Access Layer (VAL), which symbolizes a transparent interoperability model through "virtual" aggregation of CMS.

The considerations made so far give a very abstract perspective to illustrate the basic working principle and rationale behind the CMS conceptual model for achieving interoperability. The next section discusses the CMS interoperability concept in detail by introducing and discussing its core elements.

7.2 Core Elements

This section introduces and discusses the core element of the CMS interoperability framework, this means those elements, which map single parts of the discussed conceptual model into concrete designs. The framework as a whole must thereby meet all requirements and tackle the issues discussed in Chapter 6. This is achieved with an approach, which is aligned to the interoperability provisions of the IDA eLink concept (cf. Section 5.2.1.1) and the PEPPOL BusDox network (cf. Section 4.3.4.2) to enable multilateral communications.

The eLink specification [European Dynamics SA, 2004] introduces an interoperable and scalable communicational model by defining a central network for the exchange of so-called *eLink messages*. The communication in this network is based on a profile of the SwA protocol by adopting mechanisms of the German OSCI and Swedish Government eLink (SHS) standard. Users are either called *Service Consumers* when initiating a request or *Service Providers* when providing a service. Users can be looked up in a central eLink directory. The eLink specification part, which is of interest for the CMS interoperability framework is the so-called *Gateway* component. An eLink gateway seamlessly integrates other networks into the eLink system by converting eLink messages to the ones of foreign systems and vice versa. According to the specification, a gateway acts as proxy and must know and understand both message formats: the eLink message format and the format of the connected network. Clients sitting in the foreign network can thus access eLink services in the same way as they would directly be connected to the eLink network.

With BusDox, PEPPOL has followed a similar approach as IDA eLink. As briefly discussed, BusDox relies on a four-corner communication model (cf. Section 4.3.4.2). National e-Procurement systems communicate with each other through so-called BusDox *Access Points* and the START protocol. Entities can be looked up in dedicated BusDox directories. A basic communication scenario could be as follows. A sender from system A submits a message to access point A, which packs the message into a transport envelope and forwards it to access point B using the START protocol. Access point B extracts the message from the START envelope and forwards the message to the designated recipient residing in system B. By comparing eLink with BusDox one can see that, from a conceptual view, BusDox is the eLink special case where two entities communicate over two eLink gateways. The BusDox access points have the tasks of the eLink gateways and START can be seen as the eLink message protocol.

The CMS interoperability concept uses the two core elements of an Electronic Delivery Gateway (EDG) and the Delivery Gateway Protocol (DGP). From a conceptual view, the EDG can be compared to the eLink gateway or BusDox access point and the DGP to START or the eLink message protocol. BusDox and eLink were designed to provide secure messaging infrastructures. Both BusDox and eLink have provisions for a reliable transport, for example WS-ReliableMessaging in case of BusDox and a dedicated *Acknowledgment* message in the case of eLink. However, certified mailing is not just messaging with basic receipting mechanisms. It concerns far more aspects on different interoperability levels like addressing, evidence types, authentication levels, digital signatures etc. All CMS-related aspects are taken into account by the concepts of EDG and DGP. Referring to the CMS conceptual interoperability model discussed above, the DGP represents the messaging format of the secure data exchange layer. By applying a decentralized multilateral approach, an EDG mainly implements the concept of the interoperability facilitator being in charge of the secure communications management. By combining both core elements with an interoperability orchestration, a consistent CMS interoperability framework is created. The two core elements of EDG and DGP and their interrelation are subsequently discussed in the following sections.

7.2.1 Electronic Delivery Gateway

The main task of the EDG as interoperability facilitator is to hide the complexity of single CMS to ensure transparency. This means that the EDG must convert the individual characteristics of each system for all kinds of interoperability aspects, be it either of technical, semantic or procedural nature. To illustrate how this is achieved in a multilateral environment, first the bilateral case of achieving interoperability with an EDG is discussed. Even if this case is more theoretical in nature and not applied for the CMS interoperability framework, it helps to better understand the basic working principle behind the EDG concept. Based on this consideration, the multilateral EDG concept with it's interrelation to the DGP is discussed. Finally, the link-up of all EDGs in a federated interoperability network is discussed.

7.2.1.1 Bilateral Case

The bilateral case illustrates the fictive link-up of two CMS A and B (cf. Figure 7.2). Even if the bilateral scenario is not part of the CMS interoperability concept, it facilitates the better understanding of the EDG concept since the multilateral scenario is quite similar and just an extension of the bilateral one. In Chapter 6, a number of challenges have been discussed, which have to be tackled to achieve the different levels of technical, semantic and procedural interoperability. Legal aspects are not directly covered by the CMS interoperability concept. Nevertheless, they are quite important and should have effect on the interoperability agreement to achieve full interoperability. This issue is discussed in Chapter 12.

To achieve interoperability between two different CMS, the interoperability concept makes use of the architectural concept of PEGS [Capgemini, 2004]. PEGS was developed under the EC's IDA programme and is compliant with the EIF (cf. Section 5.2.1.1). The PEGS approach introduces a logical model of four gateways to describe an abstract way of how to achieve interoperability on the trivial, tech-

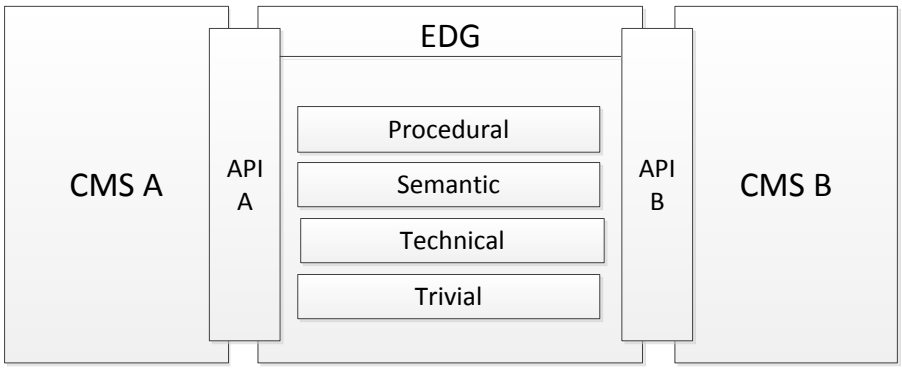

Figure 7.2: Bilateral Electronic Delivery Gateway.

nical, semantic and procedural layer. PEGS makes no assumptions on how these gateways are internally designed and how they implement interoperability. The procedural gateway aligns business processes of different systems and assumes the presence of a harmonized legal context. Equally a semantic gateway aligns different meanings and assumes that systems have similar business processes. The same holds for the technical and trivial layer. The trivial layer is also called the exchange layer and denotes the communicational part to ensure that information shared between two systems is correctly transmitted. Related to the Internet, the trivial layer would be TCP/IP. Since this work only focuses on solutions provided on the Internet, this means all open or closed CMS operate on TCP/IP, no link-up on the trivial layer is required.

The EDG is now defined as a logical unit of three virtual gateways establishing interoperability between two different CMS. The EDG structure is illustrated in Figure 7.3. Trivial interoperability is assumed to be already given. Such a gateway is thus not integral part of the EDG. A technical gateway represents the lowest layer and establishes interoperability on the technical level. A semantic gateway is a superset of the technical gateway and establishes interoperability on the semantic level. This means the technical gateway can automatically assume that different meanings are already aligned. Equally the procedural gateway is a superset of the semantic gateway and aligns different business processes. In this case the semantic gateway can assume that procedural interoperability is already given.

The EDG has explicitly been defined as a logical unit in order to clearly delimit the basic functionalities of each layer. Single functionalities and tasks are actually determined by the concrete design of the EDG. For the CMS interoperability concept the following tasks have been defined:

- ***Technical gateway***
  - Protocol conversions for both dispatch and evidence messages
  - Addressing
- ***Semantic gateway***
  - Alignment of dispatch metadata
  - Alignment of authentication qualities
  - Alignment of evidence meanings
- ***Procedural gateway***
  - Maintaining fairness
  - Maintaining timeliness

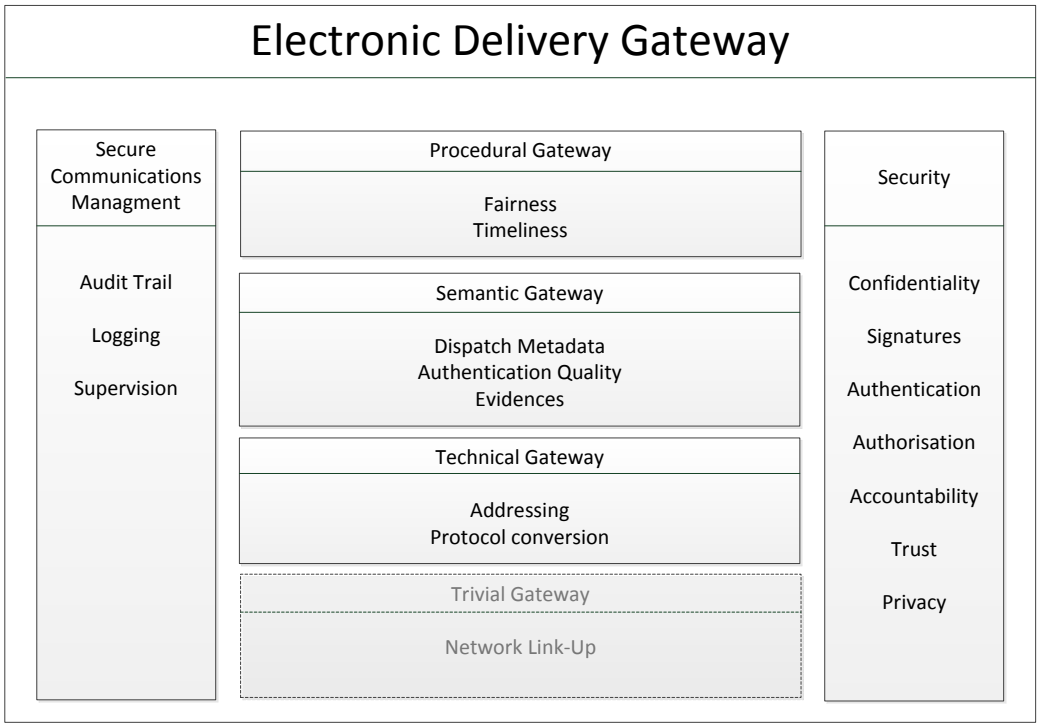

Figure 7.3: The layers of an Electronic Delivery Gateway and its main interoperability tasks.

Further tasks and duties are:

- ***Security***
  - Confidentiality
  - Signatures
  - Authentication
  - Authorization
  - Accountability
  - Trust
  - Privacy
- ***Secure communications management***
  - Audit trail
  - Logging
  - Supervision

The latter tasks are "vertical" and embrace all interoperability levels (cf. Figure 7.3). The following sections discuss in detail each level by referring to vertical duties at the same time. Some vertical duties are introduced later in this section as they become only relevant in the multilateral scenario.

Technical Gateway

A desired situation of seamless technical interworking with aligned semantics and business objects cannot be realized in practice. As seen in Chapter 4, system are too different in their technical nature. The technical gateway must thus convert different character sets (UTF-8, ASCII) and protocols (SOAP, SMTP, HTTP, X.400, etc.) between CMS A and B. By having a look at systems provided on the Internet (cf. Section 4.4.3), a roughly comparable number of representatives of each category - SMTP and Web services - can be observed.

By taking into account all possible combinations, the gateway must be able to convert form SOAP to SOAP, SOAP to e-mail, e-mail to SOAP and e-mail to e-mail. In a first step, different character encodings must translated. SOAP is usually encoded in some UTF-* or ISO-* character format. Pure e-mail without any attachments is usually encoded in ASCII format. However, with MIME parts any other character encoding may be used as well. Character set translations are quite simple operations. They are an integral part of most programming languages and numerous libraries out there can master this task. In a second step, protocol formats must be converted to each other. This means converting HTTP to SMTP and vice versa. This is also a rather straightforward operation. Finally, data formats must be converted to each other. XML must be converted to ASCII text or MIME parts (and vice versa), SOAP headers into SMTP headers, binary MTOM attachments into MIME-based SwA attachments.

In contrast to character set and protocol conversions, data format conversions require a certain knowledge about the used CMS protocols. The technical gateway must know the details of the protocol of CMS A in order to be able to convert it to the protocol of CMS B. For example, the conversion from an e-mail-based CMS to a Web services CMS would require the technical gateway to know, which protocol part contains the message subject. For example, the e-mail protocol has a particular `Subject:` header, whereas SOAP-based protocols may have foreseen a certain XML field. The same applies to the unique message or evidence ID. SMTP has a unique `Message-ID` header, SOAP may use the Web Services Addressing (WS-Addressing) `<wsa:MessageID>` element in the SOAP header or any other XML element.

Ideally, translations should be bidirectional and reversible. If a technical gateway converts a message of CMS A to CMS B, the reconversion from the message of CMS B should result in the original CMS A message. From a practical viewpoint this does not make much sense. The technical gateway must just convert the parts that are supported by the destination CMS and eventually those parts that are necessary for the reconversion of any messages. For example, assumed that a messaging functionality in CMS A requires two properties, whereas in CMS B it only requires one property, the first property of CMS A. If the second property is just optional and not needed, for example in the case of evidence reconversions from CMS B to CMS A, then it should be discarded rather than producing unnecessary load in CMS B. In any other case, the gateway must convert the property also to CMS B.

The gateway must be able to deal with digital signatures. As already briefly discussed (cf. Section 6.2.1), each single modification invalidates a digital signature. The conversion of an SMTP message sealed with a digital signature to a SOAP message would thus not be possible. However, transparency is an essential requirement and implies that each CMS must only understand its own signature types and trust relationships. In order to achieve this, the technical gateway must act as digital signature broker between CMS A and CMS B. Assumed that a signed message is converted from CMS A to CMS B, the gateway first has to check whether the signature is valid and trusted according to the policies of CMS A. The converted message is then signed by the gateway according to the policies of CMS B. Since signature B requires a valid signature A, signature B implicitly asserts the validity of signature A. The gateway therefore acts as *Assertion Authority*. The assertion process should be documented appropriately by the gateway in an audit trail. The log entry may contain the complete original signature or at least a reference uniquely identifying the signature. The format conversion is one aspect of digital signatures. Trust is another one. This aspect is more a semantic issue and is discussed in the next section covering

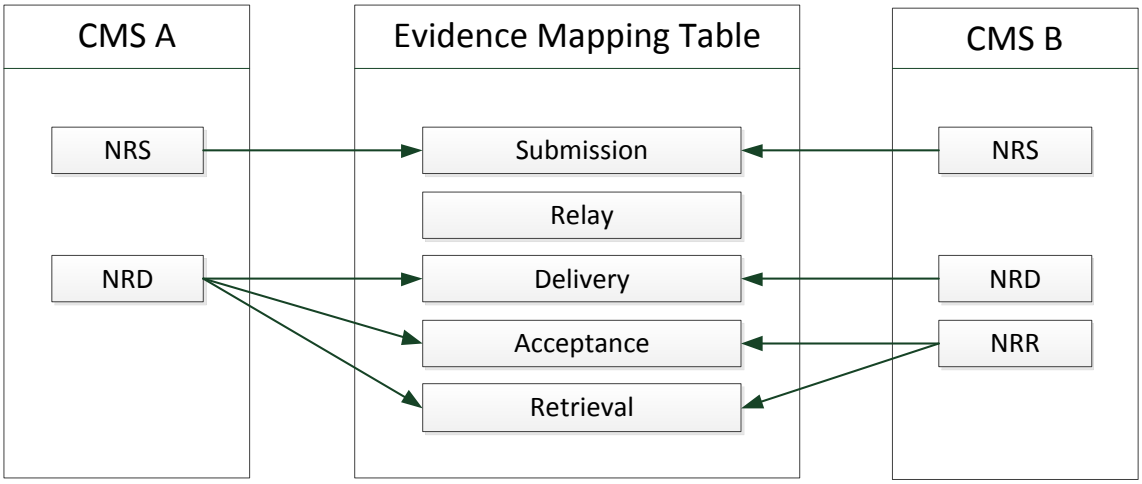

Figure 7.4: Example of two CMS mapping their evidences to a common set of evidences.

the concept of the semantic gateway part of the EDG.

Confidentiality is an essential requirement. Each CMS has a point-to-point encryption between each communication link on the route from the sender to the recipient. A technical gateway as additional node on the communication route must also meet this requirement. The communication from the last node in a CMS to the gateway must be confidential and encrypted with strong state-of-the-art cryptographic means. TLS with state-of-the-art cipher suites is a good choice on the transport layer. However, the communication between the last CMS node and the gateway may also be encrypted on the message layer using PGP or S/MIME for e-mail messages and XML encryption [Imamura et al., 2002] for SOAP messages. As discussed in the preceding chapter (cf. Section 6.2.1), E2EE from the sender to the recipient across system boundaries is not possible, at least not if any conversion is necessary. If technical interoperability is already given by nature, an encrypted message could be simply forwarded as it is. However, intervention on the semantic and procedural layer may be handicapped without proper knowledge of the message metadata. Forwarding of encrypted messages usually only works if both systems use a common standard like ETSI REM.

Semantic Gateway

Existing CMS have many aspects and properties (cf. Section 6.2), which have different meanings and cannot be directly mapped and converted by a technical gateway. This is where the semantic gateway comes into play. The semantic gateway is a superset of the technical gateway, this means it is cascaded with the technical gateway and is responsible for creating a common understanding of different meanings.

First of all, this concerns evidences. In order to get a common understanding, it is important to identify the basic commonalities of evidences in different CMS. All evidences are generated upon some event. This may be the submission of a message, the forwarding between MTAs or TTPs, the storage into a mailbox, the acceptance or rejection, the retrieval, download, etc. The semantic gateway uses a set of evidences related to basic messaging events to enable a mapping between different systems.

Figure 7.4 illustrates this concept. Assumed that the semantic gateway has defined a common set of five basic evidences (submission, forwarding, delivery, acceptance and retrieval), in a first step each CMS maps its own evidences to the harmonized ones. In this example CMS A has only two evidences, an NRS and an NRD evidence. The policy of CMS A may rule that the delivery into the recipient's mailbox is the final step and the recipient has no choice of accepting or rejecting a delivery. In this case

the CMS may decide to map the NRD to the delivery, acceptance and retrieval evidence. CMS B has three evidences, an NRS, NRD and NRR evidence. In contrast to CMS A, it maps the NRR evidence to the acceptance and retrieval evidences. With this mapping table, systems are able to determine whether they are compatible to each other in terms of supporting certain evidences. If compatibility is given, they are further able to implicitly map evidences between different systems. In the above example, CMS B can interpret the NRD of CMS A implicitly as NRR evidence and the correct operation of CMS B is guaranteed.

The EDG relies on the ETSI REM evidence content and semantics definition [ETSI, 2010c]. Chapter 5 of the REM part 2 defines the basic evidences, which have been adopted for the semantic gateway. The following REM evidences represent the EDG evidence mapping table:

- ***SubmissionAcceptanceRejection***. Indicates whether a message has or has not been successfully accepted by the sender's MTA. This evidence is generated by the sender's MTA and addressed to the sender or recipient.
- ***RelayToREMMDAcceptanceRejection***. Indicates whether a message has or has not been successfully accepted by the recipient's MS. This evidence is generated by the sender's MTA and addressed to the sender.
- ***RelayToREMMDFailure***. Indicates that a message could not successfully be delivered to the recipient's MS. This could have several reasons. The recipient's MS may not be trusted, not exist or not be reachable. This evidence is generated by the sender's MTA and addressed to the sender.
- ***DeliveryNonDeliveryToRecipient***. Indicates whether a message has or has not been successfully delivered into the recipient's MS (or a delegate's MS). This evidence is generated by the recipient's MS and addressed to the sender.
- ***DownloadNonDownloadByRecipient***. Indicates whether a message has or has not been successfully downloaded by the recipient or an authorized delegate. This evidence is generated by the recipient's MS and addressed to the sender.
- ***RetrievalNonRetrievalByRecipient***. Indicates whether a message has or has not been successfully retrieved by the recipient or an authorized delegate. This evidence is generated by the recipient's MS and addressed to the sender.
- ***AcceptanceRejectionByRecipient***. Indicates whether a message has or has not been successfully accepted by the recipient or an authorized delegate. This evidence is generated by the recipient's MS and addressed to the sender.

The two REM evidences *RelayToNonREMSystem* and *ReceivedFromNonREMSystem* are not part of the list since the presented interoperability framework only couples CMS and no standard communication systems.

Authentication and identification faces a similar semantic problem as evidence handling. Chapter 4 clearly points out the heterogeneity and diversity of authentication mechanisms in each CMS. Entities may want to know the sender's or recipient's authentication (or even registration) quality to render certain services (cf. Section 6.2.2). Like for evidences, a common understanding of authentication qualities is necessary.

Figure 7.5 illustrates an exemplary mapping of authentication qualities between two systems. It is assumed that the authentication mapping table of the semantic gateway has four well-defined levels. Users of CMS A can authenticate at their MS either with username/password combination, a software token (for example PKCS#12 key) or a conventional smartcard token. The assigned qualities are 1,2 and 3, respectively. CMS B offers two authentication levels for its users. Either a two-factor mechanism

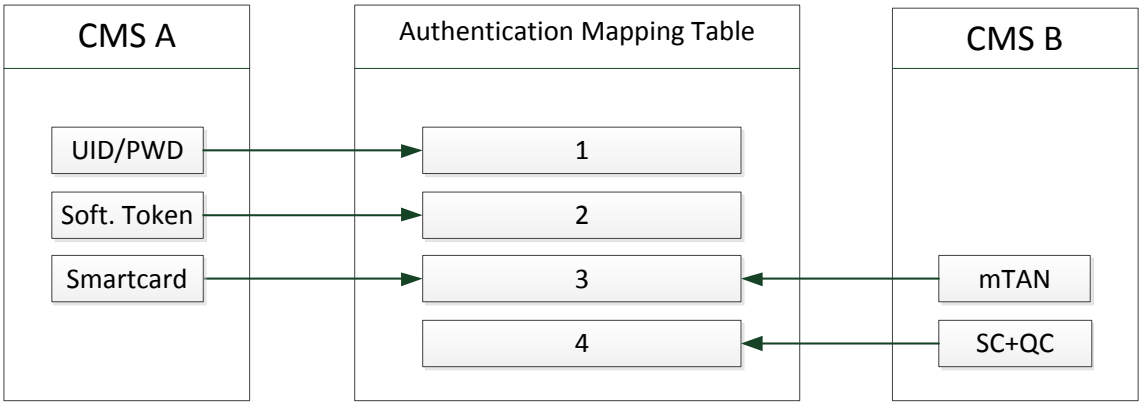

Figure 7.5: Example of two CMS mapping their authentication levels to a common set of evidences.

with mTAN or an SSCD with a QC. The assigned qualities are 3 and 4, respectively. Both systems are now able to determine whether they are compatible with each other regarding authentication qualities. Assumed that CMS B requires at least level 3 for a particular service, only smartcard users of CMS A can consume the service.

The EDG relies on the STORK quality authentication assurance framework [Hulsebosch et al., 2009]. STORK provides an eID interoperability framework for the mutual recognition of eIDs. The QAA framework facilitates the assurance of a user's identity with different well-defined levels. The higher the level, the higher the assurance of the identity. The STORK framework itself follows the IDABC approach, which has proposed in a report [European Commission, 2007] an authentication assurance framework with four levels. Each level is associated with well-defined organizational and technical factors [Hulsebosch et al., 2009, page 11]. Organizational factors comprise the quality of the identification process, the quality of the credential issuing process or the quality of the entity issuing the credential. Technical factors may be the type and robustness of a credential or the security features of the authentication mechanism. In this way both the registration and authentication aspects are covered by one single definition. STORK defines the following four QAA levels:

1. ***STORK QAA level 1***. *No or minimal assurance*. This level assures minimal or no confidence in the user's identity. The user's credentials have not been verified and just basis checks, for example the correctness of an e-mail address, may have been conducted.

2. ***STORK QAA level 2***. *Low assurance*. Even if no physical presence is required for registration, the user's electronic identity is somehow associated to the real-world identity.

3. ***STORK QAA level 3***. *Substantial assurance*. The user's identity is verified on a high level to assure that the subject is the one who claims to be. At least software or hardware certificates are used on this level.

4. ***STORK QAA level 4***. *High assurance*. This level is applied when the use of wrong identities has a heavy (legal) impact. Qualified identification is required for registration and authentication tokens are comparable to qualified certificates as defined in Annex I of the EU Signature Directive.

So how is this authentication assurance framework applied in practice? Consider the scenario where a German De-Mail sender wants to deliver a message to an Italian PEC recipient. The message should be a restricted delivery, thus tightly bound the recipient's identity. Assumed that De-Mail requires for this option at least QAA level 3, the PEC recipient must authenticate at the provider with at least this level

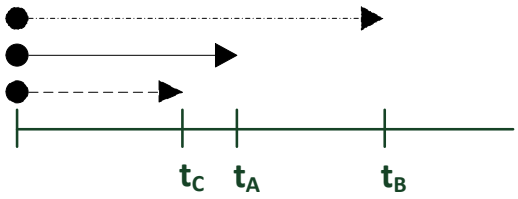

Figure 7.6: Example of three CMS having different deadlines of message expiration.

in order to retrieve the message. Even if PEC provides lower levels like username/password (QAA level 1), this kind of authentication is not admissible in this case.

Procedural Gateway

Usually different CMS do not share the same business objects and processes. A procedural gateway is needed in those cases where a process change in CMS A cannot be handled by CMS B. It is a superset of the semantic gateway, this means it is cascaded with the semantic gateway and aligns different business objects and processes.

First of all, this concerns the security management. In a coupled state, both CMS A and B must have a shared security context with the EDG. This is necessary, because due to its gateway functionality, the EDG must act as inline TTP between CMS A and CMS B. Even if signature formats can be converted and transformed by a technical gateway, the matter of trust remains open. Signatures are issued by local CMS entities and thus unknown to foreign CMS. In the case where a sender of CMS A delivers a message to a recipient of CMS B, the following requirements must be met to ensure transparency. CMS A must trust the EDG and recognize it as trusted part of the CMS. Since all CMS today use inline TTPs, the EDG could for example simply impersonate a TTP of the system. The EDG must verify whether the signature issuer is trusted. Equally, CMS B must trust the EDG, since a transformed signature appears as a local signature implicitly asserting the validity of the original one. The preceding chapter discussed the requirement for a common understanding of different signatures (cf. Section 6.2.2). A CMS may want to know whether a foreign signature was an AdES or a QES or had some other properties. The EDG tackles this issue in two ways: first, signatures generated by end entities like recipients signing an NRR evidence are often bound to the authentication quality. For example QAA level 4 implicitly asserts a signature creation device for QES. Second, the EDG may provide the original signature to the destination system upon request. At the bottom line, a shared security context is necessary wherever security elements are applied. This not only applies to signatures for dispatch or evidence messages, but also to authentication qualities as well.

A second procedural aspect is the preservation of fairness. If for example CMS B does not provide the same evidences as CMS A, fairness is threatened. Evidence types are already harmonized by the semantic gateway and thus systems can align their evidence sets. Missing evidences are mimicked by the EDG. Consider again the evidence alignment use case discussed above (cf. Figure 7.4) where CMS A provides just an NRD evidence and CMS B provides both NRD and NRR evidences. A sender of CMS B delivering a message to a recipient of CMS A expects two evidences, however, CMS B can only provide one. In this case the EDG knows that the CMS A NRD evidence replaces a NRR evidence and as a consequence the EDG generates the missing NRR evidence on its own. Since the EDG is an assertion authority, entities of CMS B cannot distinguish whether the evidences have been provided by CMS A or have been generated by the EDG on behalf.

Besides fairness, timeliness is another essential CEM property, which must be preserved. Consider

the case of message retrieval expiration as illustrated in Figure 7.6. CMS A has a deadline t_A where recipients can retrieve a message from the their MS. If recipients fetch a message before the deadline, a positive NRR evidence is returned to the sender, otherwise a negative NRR is generated and returned at t_A. This deadline may be regulated by laws or certain policies and heavily influences process flows of dependent applications, which expect either a positive or negative NRR evidence at the latest at t_A. If CMS B has a longer deadline t_B (or even no deadline), and a sender of CMS A sends a message to a recipient of CMS B, t_A may not be satisfied anymore. Like in the case of fairness, the procedural gateway ensures the preservation of timeliness by mimicking foreign evidences. In the above example the procedural gateway generates a negative NRR evidence as soon as t_A expires. The evidence is then immediately returned to the sender of CMS A. A similar situation arises for a CMS C with a shorter message retrieval expiration deadline t_C. In this case the gateway has to preserve a negative NRR evidence until t_A and then return the evidence to the sender of CMS A.

The mimicry and preservation of evidences by the procedural gateway may also be necessary in other situations where deadlines are involved. Examples are:

- Deadline for MTAs to forward messages to other MTAs.
- Message delivery deadline.
- Message acceptance/rejection deadline.
- Message download deadline.

The alignment of processes usually requires a procedural gateway to be weak stateless. In order to ensure fairness and timeliness or to just simply map returning evidences back to the domestic format, certain information of the original message may be required. This information must be preserved by the procedural gateway until the end of the protocol run. A good example in this context is addressing. Consider two CMS A and B where CMS A addresses recipients with demographics (name, date of birth) plus e-mail address and CMS B addresses recipients just with their e-mail address. If all addressing information is used both in dispatch and evidence messages, and if returning evidences from CMS B only contain the e-mail address, the missing information must be reconstructed from the preserved information of the original dispatch message. The preservation of information, however, not only concerns the exchange of messages, but also the audit trail. The procedural gateway must log exactly those data for long-term archival, which are required to be logged by the policies of both CMS A and CMS B.

The considerations made so far for the bilateral EDG include all essential and vital aspects of cross-border CEM. The behavior of the EDG has been described from a rather generic point of view, because in the end the concrete implementation depends on the CMS, which should be made interoperable. The number and types of evidences to be preserved or mimicked, deadlines or particular information to be preserved are all CMS-specific. The next section continues to discuss the multilateral EDG, which extends the bilateral approach discussed in this section with a generic model to serve a scalable CMS interoperability framework.

7.2.1.2 Generic Multilateral Gateway Approach

Extending the concept of the bilateral EDG to N systems would lead to an N-to-N interconnection architecture and each EDG would have to implement N different conversion procedures. Such an approach would not scale.

To achieve a simple multilateral solution, an additional virtual CMS layer is introduced. This approach is illustrated in Figure 7.7. The virtual CMS is denoted as CMS V. Sending a message from CMS A to CMS B via the virtual CMS V would be as follows: EDG_{AV} is a gateway making CMS A and CMS V interoperable. Thus the functionality of this gateway is the same as discussed above for the

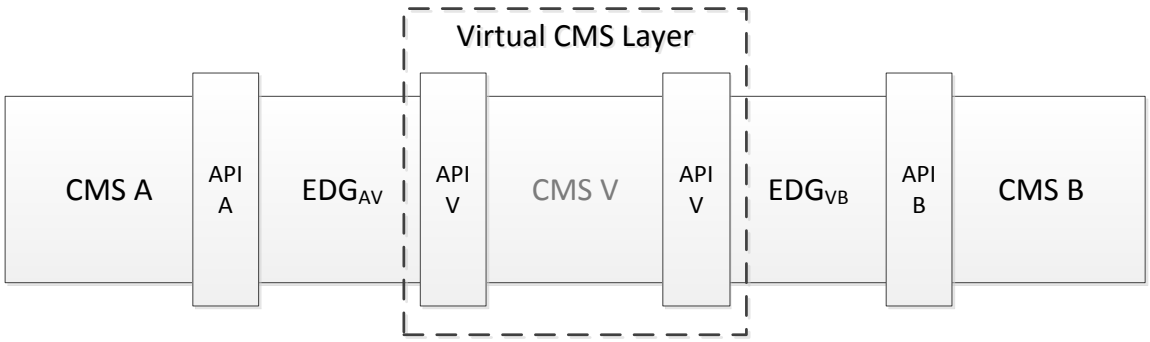

Figure 7.7: Virtual intermediary Electronic Delivery Gateway model.

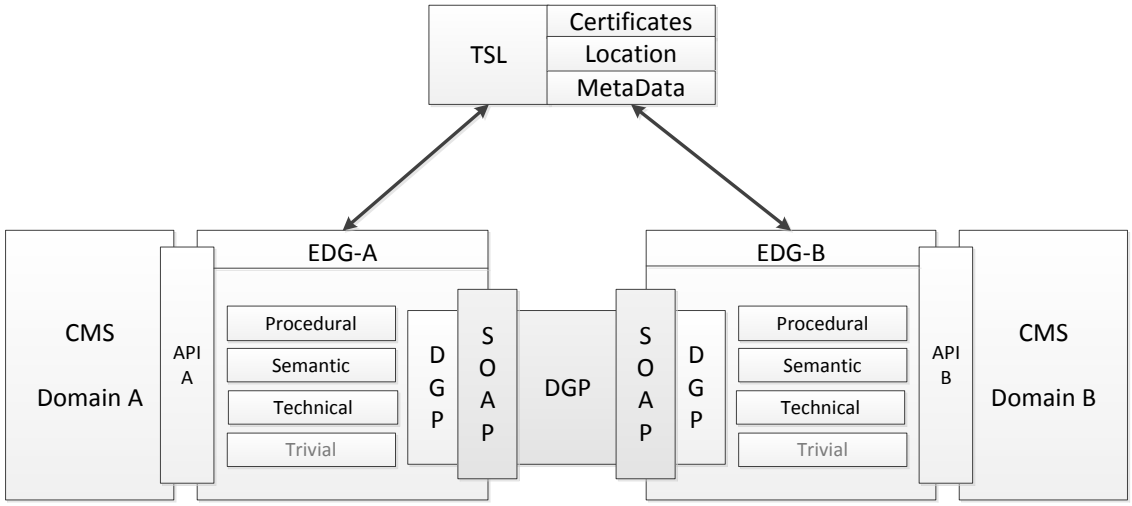

Figure 7.8: Generic Electronic Delivery Gateway Model.

bilateral approach. In the same way EDG_{VB} is a gateway making CMS V and CMS B interoperable. CMS V uses the so-called Delivery Gateway Protocol (DGP) as communication means to carry dispatch and evidence messages. It is a generic CMS protocol being able to map all relevant CMS messaging and security aspects on the technical and semantic (and some aspects of the procedural) layer. The protocol is based on an intensive survey of CMS provided on the Internet [Tauber, 2011], a requirements analysis for CMS [Tauber, 2009, 2010], a work identifying requirements and challenges for cross-border CMS interoperability [Tauber and Rössler, 2010c][3] and a report on existing CMS conducted by ETSI in 2007 [ETSI, 2007]. The DGP is discussed in more detail in the next section.

Using an additional CMS would require a centrally operated instance. To achieve a decentralized multilateral solution, only the virtual CMS V is employed. EDG A and EDG B are directly communicating with each other just as if both gateway instances would be part of a single CMS, this means CMS V. As illustrated in Figure 7.8, interoperability between two CMS with the multilateral model now requires two gateways, EDG A and EDG B, both communicating with each other over the generic DGP. In case an envelope is delivered from CMS A to CMS B, the following two basic preconditions are defined to facilitate transparency:

[3] All the mentioned research has been conducted by the author of this thesis.

1. EDG A acts as legitimate receiving unit from the viewpoint of CMS A. There are no constraints on where the gateway is located. It might be realized as MS or additional part of an MTA (acting as TTP), shared between MTAs or even be realized as standalone instance within the CMS. It must, however, be ensured that a message addressed to an external recipient is correctly routed to EDG A.

2. EDG B acts as legitimate sending unit from the viewpoint of CMS B. Like for EDG A, there are no restrictions on where EDG B is located. It might be realized as a regular UA or either as integral part of a delivery agent, for example as MTA.

For the reverse case, this means an envelope is delivered from CMS B to CMS A, the roles of both gateways are interchanged. The implementation of this precondition is completely CMS-specific.

To deliver now a message from CMS A to CMS B, EDG A converts the message from the local format to the DGP, forwards the DGP envelope to EDG B, which down-converts it to the local format of CMS B. This simplified model of cross-CMS delivery shows that CMS A and B can be substituted by any other CMS X or Y. Single CMS are decoupled from each other by the DGP mimicking a central virtual CMS. In this way a scalable interoperability framework can easily be realized while hiding system complexities and maintaining autonomy of single CMS at the same time. However, to enjoy the mentioned benefits, loss of system-specific information to a certain degree is the consequence. Even if the DGP is dimensioned to be generic enough to cover most important aspects and elements of CMS, it cannot hold all system-specific information. It is important to find the right balance between simplicity of use and the amount of information the DGP can hold.

7.2.1.3 Federated Trust Network

Based on the considerations of the generic EDG model, any two CMS can be made interoperable with this concept. To connect more than two CMS with each other, an inter-autonomous network of EDGs is defined for the CMS interoperability framework. Inter-autonomous conversions, this means conversions across different autonomous systems, can be found in many disciplines. The Border Gateway Protocol (BGP) is an example of an inter-autonomous system routing protocol backing the core routing on the Internet. That idea is transfered to the CMS interoperability problem to define a network of EDGs bridging single autonomous systems through a core EDG network. In this way, CMS envelopes can be seamlessly transferred from each system to other systems in the network. However, transparency not only requires the smooth translation of protocols and semantics using the unified DGP. A shared security context is also needed to establish implicit trust relationships between different CMS.

Figure 7.9 illustrates the federated trust network of EDGs, which is based on segmented trust relationships. The figure shows one gateway per CMS. However, depending on the policy, a CMS may have more than one gateway. Equally, several CMS may also share one single gateway. Each CMS has its own trust relationships between entities (senders, recipients, TTPs) based on internal system policies. The CMS interoperability framework defines each CMS thus as an own circle of trust. A further circle of trust is defined as the union of all EDGs where all entities trust each other on the basis of a certain shared security context. The shared security context within this federated network is managed by a central trust-sharing model implemented by using a so-called Trust-service Status List (TSL) [ETSI, 2009]. The choice of using TSL and its underlying technology is discussed in more detail in the next section. Using this federated network, trust relationships between entities of different CMS can be implicitly established. For example, TTPs of CMS A can automatically trust the evidence signature of a TTP of CMS B. This is enabled by segmented trust relationships where on the one hand EDG B asserts the validity and trust of evidence signatures originating from CMS B. On the other hand EDG A trusts and asserts the validity of envelopes coming from EDG B. Since EDG A must be a legitimate and trusted instance of CMS A, evidence signatures of CMS B are implicitly trusted by instances of CMS A.

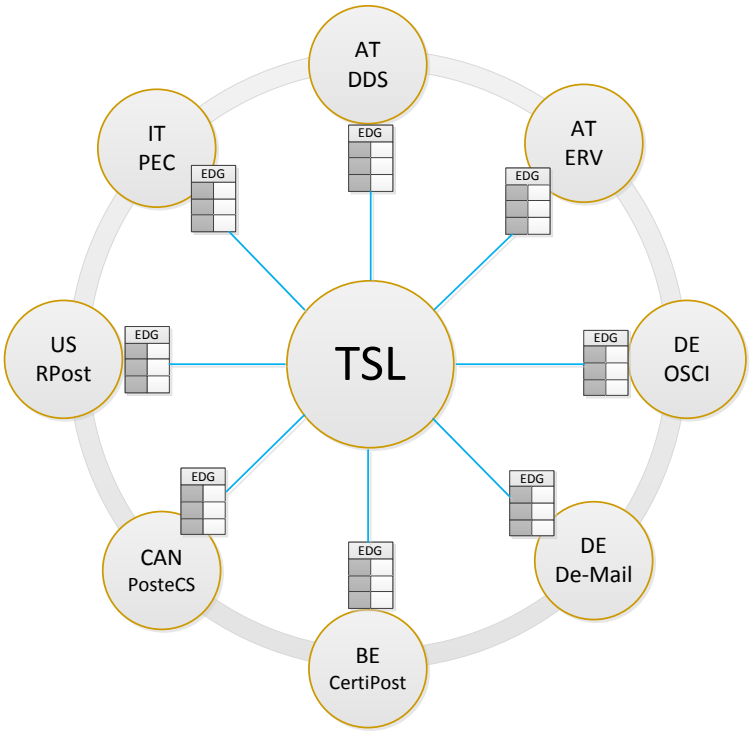

Figure 7.9: Federated trust network of Electronic Delivery Gateways.

By using a federated approach, this model is also cascadable. Not only national CMS or systems of postal operators could be made interoperable through a global network. Also local or regional systems could be connected to the national CMS and thus implicitly to the global network, for example custom delivery solutions of public agencies. This approach, however, requires an appropriate governance structure, which is discussed in more detail in Chapter 12.

7.2.2 Delivery Gateway Protocol

As the DGP is one of the major technical means to achieve interoperability between different systems, it is vital that the protocol is able to map all relevant and essential generic aspects of CMS. It is nonetheless crucial to choose the right granularity of information it has to carry. The protocol should be both simple to use and not overloaded.

The DGP can mainly map technical and semantic interoperability aspects. Some procedural aspects like fairness, timeliness, preservation of information and trust must be managed by the process logic of each EDG. The process handling is discussed in more detail in the next chapter. This section discusses the EDG, the rationale behind choosing certain technologies, the approach of cross-CMS addressing, the translation of dispatch and evidence messages, security provisions and trust management.

7.2.2.1 Communication Protocol

When designing the DGP, at the beginning questions came up of which technology to use. Should an established and wide-spread technology like SMTP or a fast messaging technology like the Common Object Request Broker Architecture (CORBA) [Object Management Group, 2008] be used, a specification designed for distributed applications in heterogeneous environments? In the end, Web services tech-

nologies based on SOAP and the HTTPs 1.1 binding have been chosen for the following reasons: Web services are internationally standardized and well-established in SOAs. Even if widely used as the "de facto" communication standard for asynchronous messaging, SMTP is a rather outdated technology. It was primarily introduced with the aim to transport text-based information. In contrast to SMTP, SOAP is better suited for carrying structured information like XML. This is a major requirement, since the whole DGP holds structured information and metadata of CMS mappings on the technical and semantic level. Even if CORBA is much faster than SOAP, only some parts of the CORBA architecture are available as open-source implementations. By contrast, many open-source frameworks for Web service technologies are freely available. A popular example is the Java Metro[4] implementation. Furthermore, the WS-family is usable in a modular way. Additional protocols for addressing, security, trust and reliable-messaging can be integrated on demand. Last not least, several initiatives like the Web Services Interoperability organization (WS-I) , which is now part of the standardization organization OASIS, are supporting interoperability by publishing best practices, creating interoperability profiles and providing test tools.

The DGP is based on SOAP version 1.1 [Box et al., 2000]. Attachments are carried using MTOM [Gudgin et al., 2005] for the efficient binary transmission of payload data. Binary data can be transported in several ways. By default, the whole data is directly embedded as Base64-encoded content of an XML element. Particularly in case of large data this is a bottleneck for Document Object Model (DOM)-based parsers. SwA tackles this issue by transferring larger data into attachments represented as single MIME parts. Attachments can be referenced from within the XML document using the Content-ID Uniform Resource Identifier (URI) scheme as described in RFC 2111 [Levinson, 1997]. The SwA mechanism, however, has the drawback that referenced data does not directly appear as embedded data in the XML content and is thus not covered by digital signatures. All attachments must be additionally signed. MTOM enjoys the benefits of both models. First, like SwA, MTOM also carries the actual data as MIME parts of the SOAP message. The data may be stored as binary content, which saves 33% of storage space compared to a Base64 encoding scheme. Second, MTOM attachments are referenced with the XML-binary Optimized Packaging (XOP) mechanism from within the XML document. With this referencing mechanism the binary data appears logically as inline and parsers see the Base64-encoded data instead of the reference.

Only attachments are carried using MTOM. Addressing information and DGP metadata for both dispatch and evidence messages are carried in the SOAP body. The concrete definition is discussed in the next sections. Security provisions are also discussed below.

7.2.2.2 Addressing and Routing

Existing CMS use two different basic kinds of addressing schemes. Recipients can either be addressed using single address values, for example an e-mail address or another unique identifier like a tax number. In some systems recipients can also be addressed using demographics (name, date of birth) and the postal address. The DGP provides an XML structure being able to map both mechanisms.

Figure 7.10 illustrates the XML schema fragment for addressing the end-entities sender and recipient. First of all, the `ID` element allows entities to be addressed by their unique ID. The scheme makes no restrictions on the number of unique IDs. One could use no unique ID, for example if it is not at hand or not used in the particular system. For example, in Austria business senders may address recipients just by demographic data like given name, family name and date of birth. In this case a unique ID is not at hand. But one could also use more unique IDs, for example a unique e-mail address plus the tax number. This may be the case in the Slovenian moja.posta.si CMS. The `ID` addressing scheme is generic and allows the definition of any type of unique ID through the provision of the `Type` / `Value` tuple. The following types have been defined for the DGP:

- `urn:delivery-eu-id:address:email`. Denotes a qualified CEM address having a for-

[4] `http://metro.java.net/`

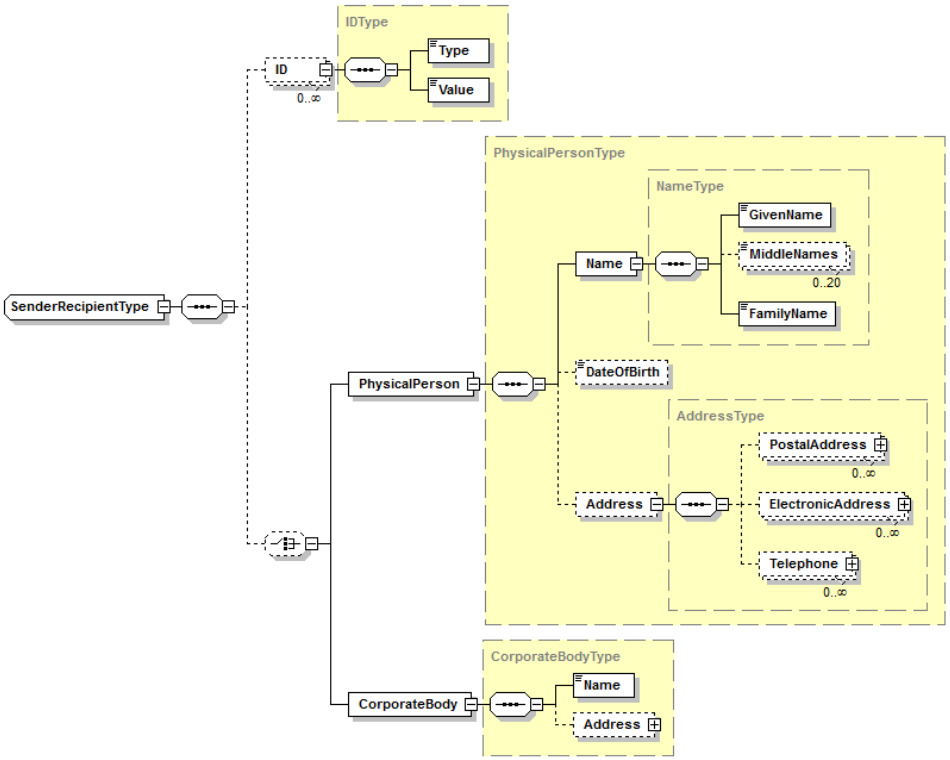

Figure 7.10: EDG addressing scheme for senders and recipients. Optional elements are marked by dotted lines.

mat as defined in RFC 5322 [Resnick, 2008]. It is the typical e-mail address format and is used in several SMTP-based systems (De-Mail, PEC) as well as SOAP-based systems like moja.posta.si. Typical examples are mario.conti@pec.it or max.mustermann@de-mail.de.

- `urn:delivery-eu-id:address:fiscal`. Denotes a person's fiscal (or tax) number. This kind of addressing scheme is used in the Slovenian moja.posta.si CMS.

- `urn:delivery-eu-id:address:ssn`. Denotes a person's social security or insurance number. This kind of addressing scheme may be of interest for the qualified document exchange in the e-Health sector.

- `urn:delivery-eu-id:address:company.number`. Denotes the unique number of a company. For example, company mailboxes in the Austrian DDS can be addressed by their company number.

- `urn:delivery-eu-id:address:unique.identifier`. Denotes a person's unique (national) identification number. An e-mail address, the tax number or social security number are just examples of unique identifiers. Particularly CMS operated by governments may choose to use other identifiers like personal identification numbers. Further numbers could address associations and other types of organizations.

- `urn:delivery-eu-id:address:sspin`. Denotes a person's sector specific identification number. In this case the unique identifier is derived from another unique identifier. For example, in the Austrian DDS recipients can be addressed by their ssPIN (ZU), the recipient's unique id number in the context of certified electronic mail. The ssPIN is thereby derived from the recipient's sourcePIN, the unique national identification number used in governmental proceedings.

- `urn:delivery-eu-id:address:web`. Instead of an e-mail address, recipients may also be addressed by their Web address. The SOAP-based German OSCI standard uses standard HTTP Web service endpoint addresses.

The mentioned types are just a predefined set of addressing schemes. Due to the generic type/value approach, further schemes can be defined and added on demand.

In addition to the ID-based addressing scheme, senders and recipients can also be addressed by demographic data. The DGP schema distinguishes between natural persons (`PhysicalPerson` element) and legal persons (`CorporateBody` element). The data for natural persons comprises the name (`GivenName`, `MiddleNames` and `FamilyName` elements), the date of birth (`DateOfBirth` element) and a set of addresses. The data for legal persons comprises the full name (`Name` element) and a set of addresses.

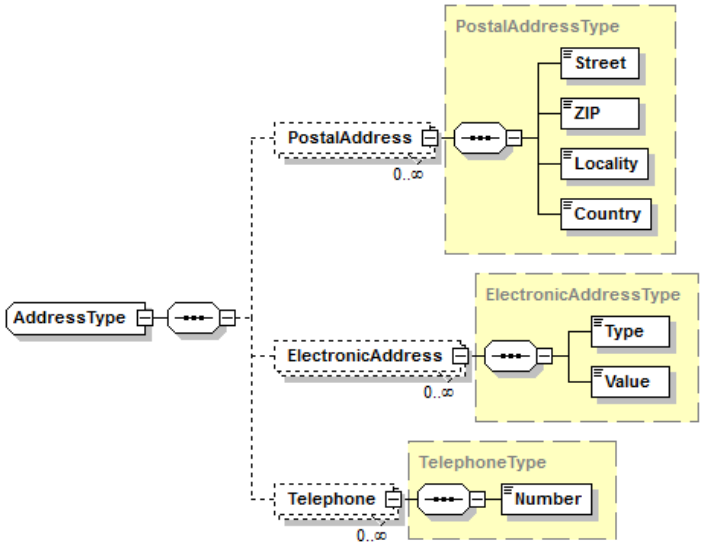

Figure 7.11: EDG address types. Optional elements are marked by dotted lines.

As illustrated in Figure 7.11 the following address types are defined for both natural and legal persons:

- `PostalAddress`. Denotes a person's postal address, identified by street name (`Street` element), zip code (`ZIP` element), place of residence (`Locality` element) and country of residence (`Country` element) in ISO-3166 format [ISO, 2006].

- `ElectronicAddress`. Denotes a person's electronic address. At the moment, only the e-mail address format is specified for the DGP. Due to the type/value tuple, basically any kind of electronic address can be defined. The e-mail address type is the same as describe above and has the value `urn:delivery-eu-id:address:email`.

- `Telephone`. Denotes a person's telephone number according to ITU-T E.123 [ITU-T, 2001].

All the mentioned address types are optional and can be used multiple times, because a person may have multiple e-mail addresses or telephone numbers. One might wonder why not established standards like the OASIS Customer Information Quality (CIQ) specification [OASIS Customer Information Quality TC, 2008] or the ebXML ISO-15000-5 [ISO/TS, 2005] have been used for naming and addressing. Existing standards out there are quite comprehensive and try to cover all addressing elements. Even if

this might be useful in certain circumstances, the DGP aims to be concise and not too overloaded to allow for an easier handling. Moreover, addressing focuses on unique identifiers and not on naming and postal addressing elements.

The challenge is, however, to route an envelope message to the correct destination gateway just on the basis of the available address information. This must be managed by the processing part of the gateway and is discussed in more detail in the next chapter.

7.2.2.3 Dispatch Messages

Independent from the underlying technology, CMS dispatch messages usually consist of several parts: a set of metadata used for transport and routing or to describe the message, some optional payload data (attachments), etc. The same structure is applied for converted messages, which are carried in the XML body part of the SOAP DGP dispatch message. The common set of metadata has been identified by assessing existing CMS (cf. Chapter 4). The following metadata are found in each CMS and are thus defined compulsory: sender name and address, recipient name and address, a unique message ID and a submission timestamp. Additional data, which can be found in most but not all CMS are for example: message expiration date or subject. Nevertheless, the DGP specification is extensible in case a CMS wants to add custom properties, for example based on bilateral agreements.

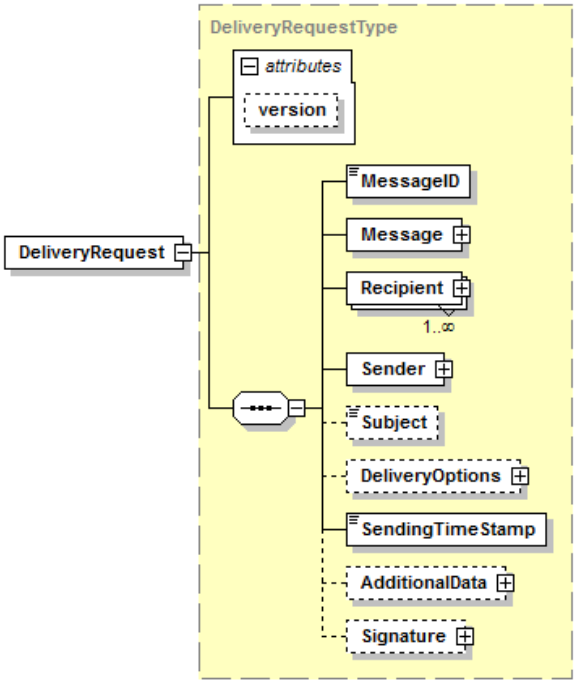

Figure 7.12: EDG delivery request for dispatch messages. Optional elements are marked by dotted lines.

Figure 7.12 illustrates the XML schema of the DGP delivery request for dispatch messages. The following core elements and attributes are defined:

- `version`. Denotes the version of the request format to enable the support of multiple versions for backwards compatibility.
- `MessageID`. Denotes the unique ID of the dispatch message. It may, but must not necessarily be the same as the original dispatch message. In case a new message ID is used, the procedural gateway must preserve the necessary information to map between both dispatch messages.

- `Message`. Denotes the details of the message content. This element is described in more detail below in this section.
- `Recipient`. Denotes the recipient's address data according to the format described above (cf. Section 7.2.2.2).
- `Sender`. Denotes the senders's address data according to the format described above (cf. Section 7.2.2.2).
- `Subject`. Denotes the message subject. This element is optional since not all CMS implementations support a message subject.
- `DeliveryOptions`. Denotes several options for the dispatch message delivery. The details of this element are discussed below in this section.
- `SendingTimeStamp`. Denotes the date and time the original message has been submitted. This value may be of interest for the recipient or for TTPs when calculating deadlines.
- `AdditionalData`. Denotes arbitrary additional data, which can be bilaterally exchanged between different CMS. Basically all necessary information should be covered by the introduced elements. Therefore, the use of this element is only intended for exceptional cases.
- `Signature`. Denotes the digital signature element to ensure authenticity and integrity. The details of this element are discussed below (cf. Section 7.2.2.6).

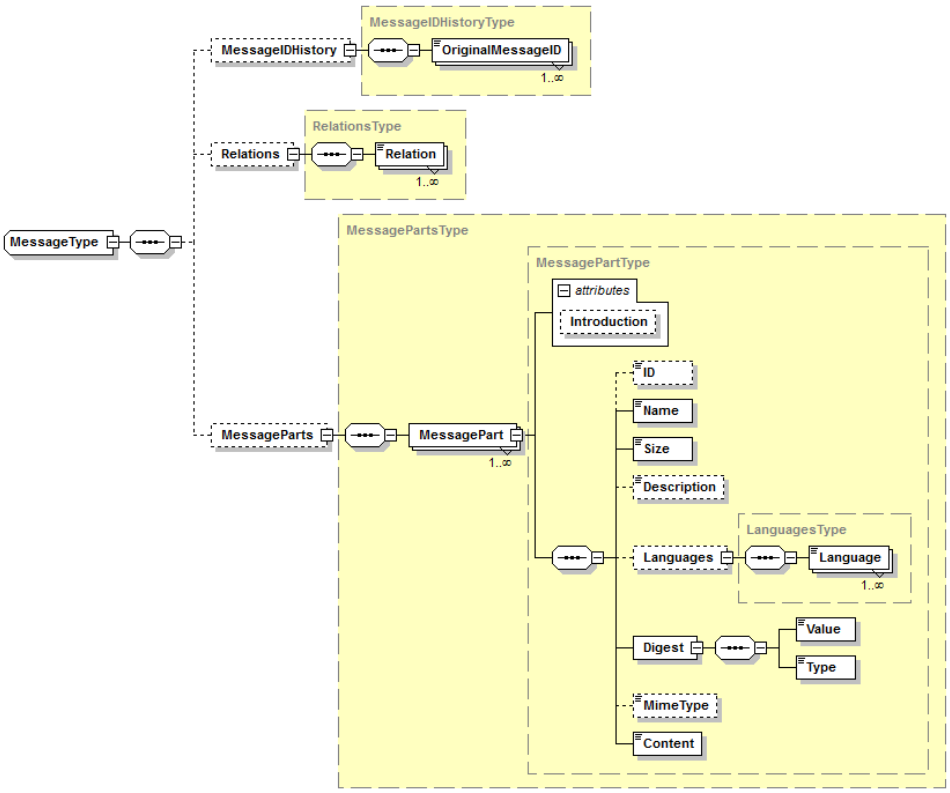

Figure 7.13: EDG delivery request message details fragment. Optional elements are marked by dotted lines.

Figure 7.13 illustrates the XML schema fragment of the dispatch message details having the following elements:

- `MessageIDHistory`. Denotes the list of message IDs of the original dispatch message. If the EDG does not alter or wants to hide the original ID, this element can be ignored.
- `Relations`. Denotes message IDs of related messages, for example of replies or forwarded messages.
- `MessageParts`. Denotes attachments of the original dispatch message. They are carried without modification as MTOM binary data of the SOAP message. This also includes informational text like the message body of an e-mail. The following subelements and attributes are defined.
  - `Introduction`. Defines whether this part is just informational like the body of an e-mail message.
  - `ID`. Denotes the unique ID of this attachment part.
  - `Name`. Denotes the file name of this attachment part.
  - `Size`. Denotes the file size (in bytes) of this attachment part.
  - `Description`. Denotes a brief description outlining this attachment part.
  - `Languages`. Denotes the languages in ISO-3166 format [ISO, 2006] in which this attachment part has been composed.
  - `Digest`. Denotes the message digest of this attachment part. With the type/value tuple, digest algorithms can be dynamically added in future. The standard value is SHA-256 (`digest:SHA256`) as defined in [National Institute of Standards and Technology (NIST), 2002].
  - `MimeType`. Denotes the MIME or file type of this attachment part. For example, in case of PDF documents the MIME type would be `application/pdf`.
  - `Content`. Denotes the actual content of this attachment part.

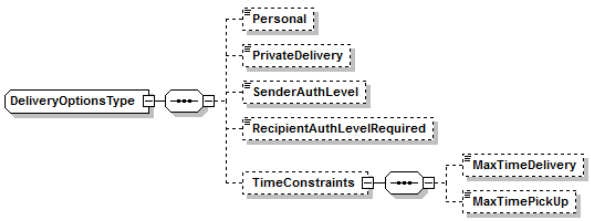

Figure 7.14: EDG delivery request options schema fragment. Optional elements are marked by dotted lines.

Figure 7.14 illustrates the XML schema fragment of the `DeliveryOptions` element with the following defined delivery options:

- `Personal`. Denotes a restricted delivery. If set to `true`, only the designated recipient and no delegate is authorized to accept, retrieve or download the dispatch message.
- `PrivateDelivery`. Denotes if a dispatch message is sent as official delivery of a public body or as private delivery. Some systems like the Austrian DDS distinguish between these types since the former type is bound to the "Law on the Delivery of Official Documents".
- `SenderAuthLevel`. Denotes the sender's QAA level. Allowed values range from 1 to 4 (cf. Section 7.2.1.1).

- `RecipientAuthLevelRequired`. Denotes the required QAA level for the recipient. If the recipient's system cannot fulfill this requirement, the dispatch message must be rejected by the recipient's EDG. Allowed values range from 1 to 4 as (cf. Section 7.2.1.1).

- `MaxTimeDelivery`. Denotes the expiration time (in seconds) for the delivery of a dispatch message. This means if a dispatch message does not arrive at the recipient's MS within this timeframe, a negative NRD evidence should be returned. If the recipient's system does not have an implementation for such a deadline, it must either ignore this element or the procedural gateway must implement it. Alternatively the procedural part of the sender's EDG must implement this feature if not anyhow foreseen by the recipient's system.

- `MaxTimePickup`. Denotes the expiration time (in seconds) for the retrieval of a dispatch message. This means if a dispatch message is not retrieved by the recipient MS within this timeframe, a negative NRR evidence should be returned. If the recipient's system does not have an implementation for such a deadline, it must either ignore this element or the procedural gateway must implement it. Alternatively the procedural part of the sender's EDG must implement this feature if not anyhow foreseen by the recipient's system.

7.2.2.4 Evidence Messages

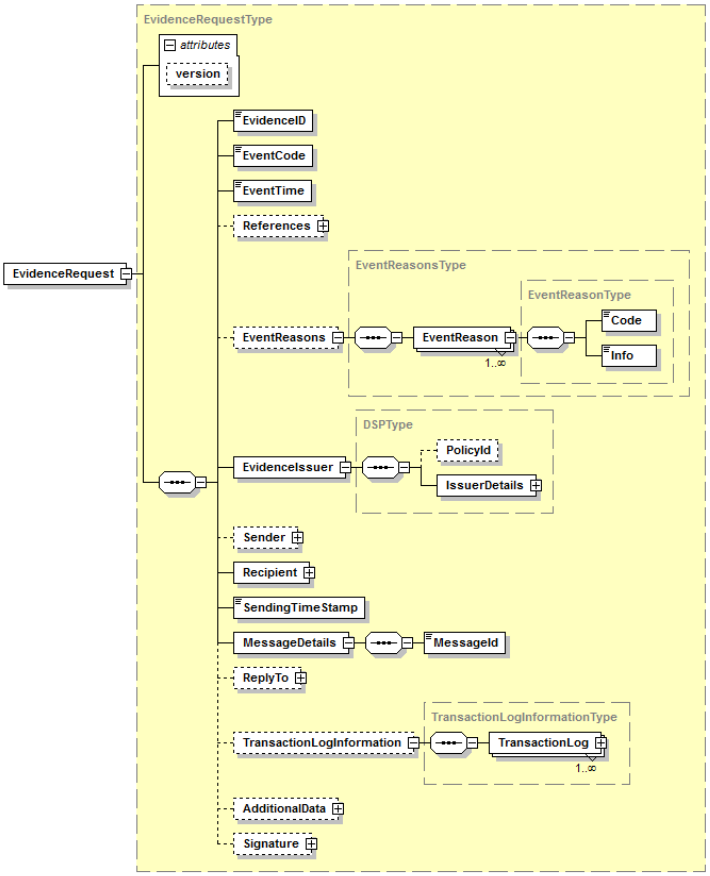

Figure 7.15: EDG evidence request schema fragment. Optional elements are marked by dotted lines.

Like dispatch messages, converted evidence messages are also carried within the SOAP body of the DGP. To map CMS evidences to the common intermediate DGP format, the ETSI REM standard for

XML evidences has been adopted and extended. Figure 7.15 illustrates the XML schema fragment of an evidence message request having the following elements:

- `version`. Denotes the version of the request format to enable the support of multiple versions for backwards compatibility.
- `EvidenceID`. Denotes the unique ID of this evidence message. It has the same meaning as the REM `EvidenceIdentifier` element.
- `EventCode`. Denotes the event code for this evidence. According to the defined evidences (cf. Section 7.2.1.1), the following REM event codes are defined for the DGP.
  - `http:uri.etsi.org/02640/Event#Acceptance`
  - `http:uri.etsi.org/02640/Event#Rejection`
  - `http:uri.etsi.org/REM/Event#Delivery`
  - `http:uri.etsi.org/REM/Event#DeliveryExpiration`
  - `http:uri.etsi.org/REM/Event#Download`
  - `http:uri.etsi.org/REM/Event#DownloadExpiration`
  - `http:uri.etsi.org/REM/Event#Retrieval`
  - `http:uri.etsi.org/REM/Event#NonRetrievalExpiration`
  - `http:uri.etsi.org/REM/Event#Rejection`

  The complete list of event codes and their detailed meanings can be found in [ETSI, 2010c, Appendix B.1.2, page 58].
- `EventTime`. Denotes the date and time of the evidence event. It has the same meaning as the REM `EventTime` element.
- `References`. Has the same functionality as the `Message` element for dispatch messages. This allows the definition of IDs of original evidence messages to create relations to other messages.
- `EventReasons`. Denotes the reasons for an error event with a Code/Info tuple. It has the same meaning as the REM `EventReasons` element. The complete list of event reason identifiers and codes can be found in the ETSI REM specification [ETSI, 2010c, Appendix D, page 77].
- `EvidenceIssuer`. Denotes the entity having issued the original evidence. It covers both the REM `EvidenceIssuerPolicyID` and REM `EvidenceIssuerDetails` element. Issuer details (element `IssuerDetails`) are defined according to the DGP addressing format (cf. Section 7.2.2.2).
- `Sender`. Denotes the sender's name, address and authentication detail. This element is described in more detail below in this section.
- `Recipients`. Denotes the sender's name, address and authentication detail. This element is described in more detail below in this section.
- `SendingTimeStamp`. Denotes the date and time the original evidence has been submitted. This value may be of interest for the recipient of this evidence.
- `MessageDetails`. Denotes the dispatch message ID this evidence refers to.
- `ReplyTo`. Denotes the entity to which a reply to this evidence is sent. This element is defined according to the DGP addressing format (cf. Section 7.2.2.2).

- `TransactionLogInformation`. Denotes arbitrary audit trail data, which may be relevant for the recipient of this evidence.
- `AdditionalData`. This element has the same meaning as for the dispatch message request.
- `Signature`. Denotes the digital signature element to ensure authenticity and integrity (cf. Section 7.2.2.6).

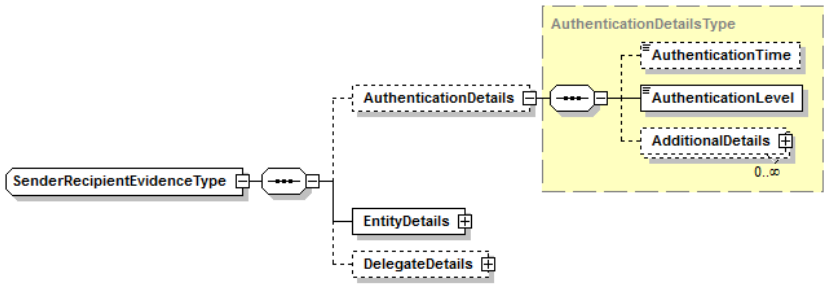

Figure 7.16: EDG evidence request schema fragment for sender and recipients. Optional elements are marked by dotted lines.

Figure 7.16 illustrates the XML schema fragment for the sender and recipients. This element allows the definition of authentication details of the entity, which might be of interest for the receiving entity. Besides the date and time of authentication, the QAA level can also be defined. Along with the entity's details (element `EntityDetails`), which must have the DGP addressing format (cf. Section 7.2.2.2), details of a delegate who acted on behalf of the entity, might be provided as well.

7.2.2.5 Trust Model

The federated EDG network relies on a single trust management model, which is technically expressed by means of a TSL according to the ETSI TS 102 231 standard [ETSI, 2009]. TSL has been defined as a standard for publishing information about trusted services and their providers. From a technical point of view, a TSL is an XML structure, which is electronically signed by the maintainer. TSLs can be maintained in a centralized or decentralized way. A centrally maintained TSL holds all trusted service providers directly within the TSL. In the case of decentralized maintenance, a central TSL holds a list of pointers to other TSLs, which are maintained independently by for example national supervisory boards.

TSL has many similarities and shares the benefits of CRLs used by PKIs to determine the revocation status. Both are hosted as a single file signed by the maintainer, which can also be used offline. In this way, there is no point of single failure, at least not for a short period of time. Like CRLs, TSLs have also a "next-update" entry indicating the time when the TSL will be updated. TSLs may also contain a history of their content so that past transactions can still be verified.

Currently the TSL standard is mainly used to provide information about trusted national Certification Service Providers (CSPs) in the EU issuing qualified electronic certificates. The EC is promoting the TSL standard as default model for national trust lists and explicitly allows the inclusion of other trusted providers in its decision 2009/767/EC [European Commission, 2009a, page 20].

> "*Additional information on other supervised/accredited CSPs not issuing QCs but providing services related to electronic signatures (for example CSP providing Time Stamping Services and issuing Time Stamp Tokens, CSP issuing non-Qualified certificates, etc.) may be included in the Trusted List at a national level on a voluntary basis.*"

For the CMS interoperability framework an own TSL holding entries for trusted EDGs is defined. For each EDG entry, the name, DGP Web service URL and used signature certificate are listed.

The list of supported REM evidences and authentication levels are also part of each TSL gateway entry. On the basis of the list of supported evidences, which must be a subset of the seven discussed REM evidences, gateways know whether a remote CMS can provide certain evidences so that fairness in the domestic system is still preserved. The list of supported QAA levels indicates whether a remote CMS supports authentication and identification of senders or recipients with a certain quality. In this way, the sending gateway can prevent the delivery of personal documents if the remote CMS does not support a high authentication quality.

Listing 7.1: Exemplary EDG TSL entry

```
<tsl:TSPService>
  <tsl:ServiceInformation>
    <tsl:ServiceTypeIdentifier>http://uri.etsi.org/TrstSvc/Svctype/REM</
       tsl:ServiceTypeIdentifier>
    <tsl:ServiceName>
      <tsl:Name xml:lang="en">Austrian DDS Gateway</tsl:Name>
    </tsl:ServiceName>
    <tsl:ServiceDigitalIdentity>
      <tsl:DigitalId>
        <tsl:X509Certificate>Y2VydGlmaWNhdGU=</tsl:X509Certificate>
      </tsl:DigitalId>
    </tsl:ServiceDigitalIdentity>
    <tsl:ServiceStatus>http://uri.etsi.org/TrstSvc/Svcstatus/inaccord</tsl:ServiceStatus>
    <tsl:StatusStartingTime>2010-05-30T09:00:00</tsl:StatusStartingTime>
    <tsl:ServiceSupplyPoints>
      <tsl:ServiceSupplyPoint>https://gateway.dds.at/webservice</tsl:ServiceSupplyPoint>
    </tsl:ServiceSupplyPoints>
    <tsl:ServiceInformationExtensions>
      <tsl:Extension Critical="true">
        <SupportedEvidences>
          <Evidence>RetrievalNonRetrievalByRecipient</Evidence>
        </SupportedEvidences>
        <SupportedQAALevels>
          <Level>4</Level>
        </SupportedQAALevels>
      </tsl:Extension>
    </tsl:ServiceInformationExtensions>
  </tsl:ServiceInformation>
</tsl:TSPService>
```

Listing 7.1 shows an example of an exemplary Austrian DDS EDG entry as “TSPService” in the TSL. The entry contains the service type identifier (standard TSL value for CEM services), the name, the signature certificate (for both dispatch and evidence DGP messages), the current status, the DGP Web service URL (as service supply point) and the list of supported evidences and authentication levels as critical service extensions.

Like for CRLs, a TSL must be signed and maintained by some trusted authority, because the whole trust of the interoperability framework relies on the TSL. Since this is a critical issue, it must be part of an interoperability agreement and governance strategy. Therefore, this aspect is discussed in more detail in Chapter 12.

7.2.2.6 Further Security Provisions

Besides the TSL trust mechanism, the federated gateway network has several security provisions. To ensure confidentiality, the whole inter-gateway communication is secured through TLS. Strong state-of-the-art cipher suites must be used. Integrity and authenticity outside the TLS context is ensured by signing all DGP messages using XML signatures. This concerns both dispatch and evidence messages. Both message types have a `Signature` child element, which holds an enveloped XML signature. The signature covers the whole SOAP body, thus including not only the metadata in the DGP messages,

but all message attachments as well. By doing so, a gateway asserts the validity of own CMS requests including all metadata and attachments. Receiving gateways can verify the authenticity of a message by looking up the signature certificate of the sending gateway in the TSL. This signature transformation and assertion process is described in more detail in the next chapter. Having discussed the core elements of the CMS interoperability concept, the next chapter continues to discuss its process model.

Chapter 8

Process Model

"Giving is better than receiving because giving starts the receiving process."

[Jim Rohn, American Speaker, 1930–2009.]

This chapter defines the single process steps of the CMS interoperability concept discussed in the preceding chapter in more detail. It puts together the single pieces and discusses the cross-border process flow from the sender to the recipient.

This chapter illustrates the cross-border delivery process by means of two CMS A and CMS B where CMS A is the sender's CMS and CMS B the recipient's CMS. Each of the two systems is associated with a gateway, labeled EDG A and EDG B, respectively.

8.1 Basic Process Model

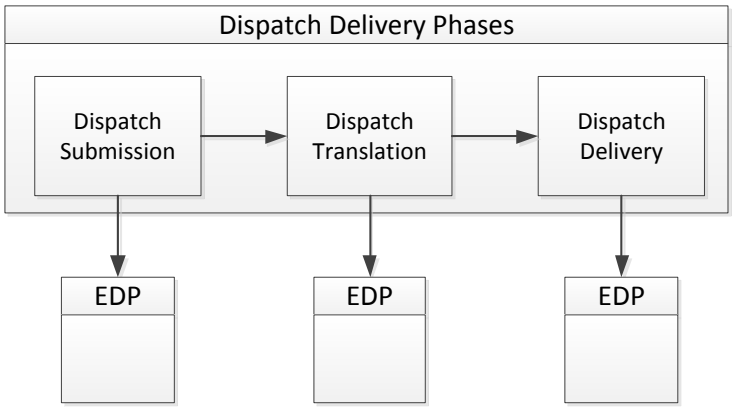

Figure 8.1: The three basic CMS interoperability phases from an abstract viewpoint. This example shows the cross-border delivery of a dispatch message. EDP denotes the evidence delivery phases, which are the same as for the dispatch message delivery and are thus not explicitly drawn.

This section outlines the main phases of the cross-border CMS delivery from an abstract viewpoint. A message delivery process from a sender to a recipient across CMS boundaries can be separated into the following three main phases:

1. ***Message submission***. This phase takes place between the sender, the sender's CMS and the related EDG. The sender's UA generates, prepares and submits the message to the MTS of the sender's CMS. The MTS subsequently tries to route the message to the corresponding EDG.

2. ***Message translation***. This phase mainly takes place between the sender's EDG and the recipient's EDG. The sender's EDG translates the domestic CMS message to the DGP message format and forwards it to the recipient's EDG.

3. ***Message delivery***. This phase takes place between the recipient's EDG, the recipient's CMS and the final recipient. The recipient's EDG translates the received DGP message into the domestic format of the recipient's CMS and submits it to the MTS of the associated CMS. Subsequently, the recipient's CMS delivers the message to the recipient's MS.

Figure 8.1 illustrates the three phases for delivering a cross-border dispatch message from the sender to the recipient. Basically each phase may produce a set of evidence messages, which are generated by some involved entity. These evidence messages have to undergo the same three delivery phases as the dispatch message. The figure intentionally does not outline the CMS the sender and the recipient belong to. It just illustrates the main phases. The rationale behind this is that in case of evidence messages the roles of the sender's and recipient's systems are interchanged in comparison to dispatch messages. The conceptual and technical process for delivering a dispatch message, however, is almost the same as for evidence messages.

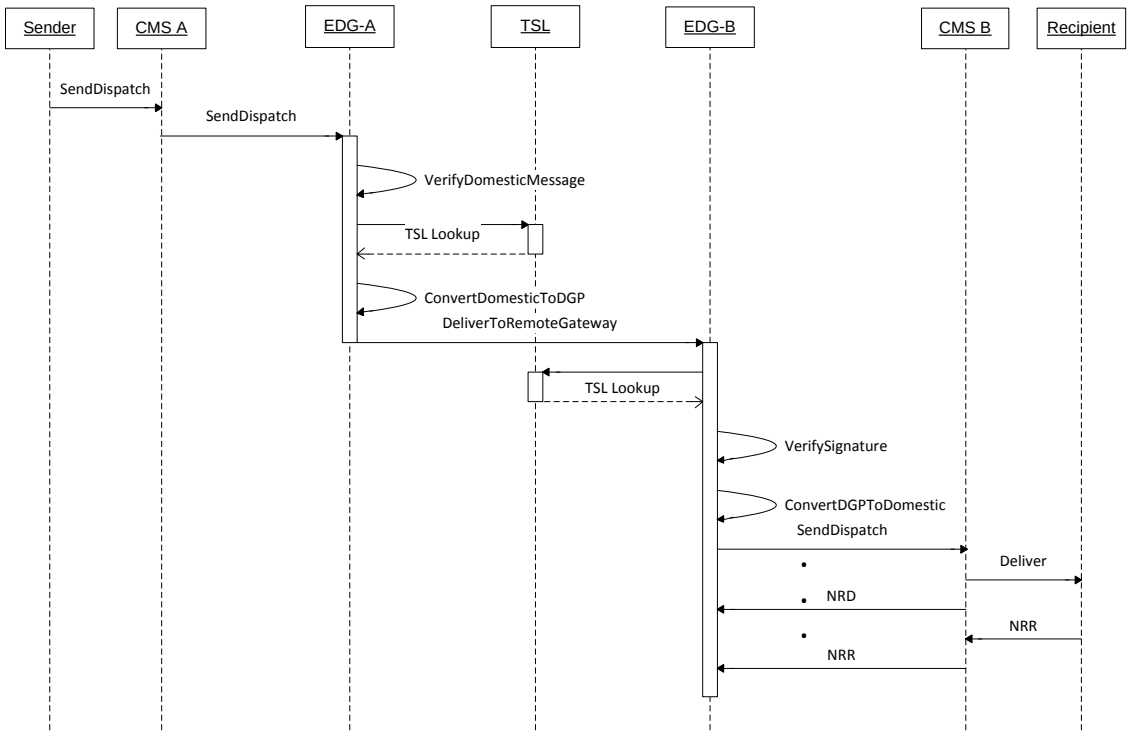

Figure 8.2: Sequence diagram of the basic dispatch process flow.

Figure 8.2 shows a more fine-grained illustration of the cross-border CMS dispatch message process flow. The next sections discuss in detail the main phases of message submission, translation and deliv-

ery and explicitly outline in which parts they differ for dispatch and evidence messages. The process descriptions refer to the delivery scenario where a sender of CMS A delivers a message to a recipient of CMS B. The related gateways, which handle the message exchange between the two systems are called EDG A and B, respectively.

Particularly for the message submission and delivery phase many actions are CMS-specific. These actions are described from a rather abstract and generic point of view. A concrete implementation for the Austrian DDS is described exemplarily in Chapter 10.

8.2 Message Submission Phase

In the CMS interoperability model, the message submission phase covers the transmission of a message from the sender to the sender's EDG. The CMS interoperability framework mainly deals with the communication between EDGs. In order to foster transparency and autonomy, domestic processes behind gateways are out of scope of the framework. Nevertheless, this section briefly describes common process steps, requirements and constraints that should be taken into account by a CMS implementing an EDG.

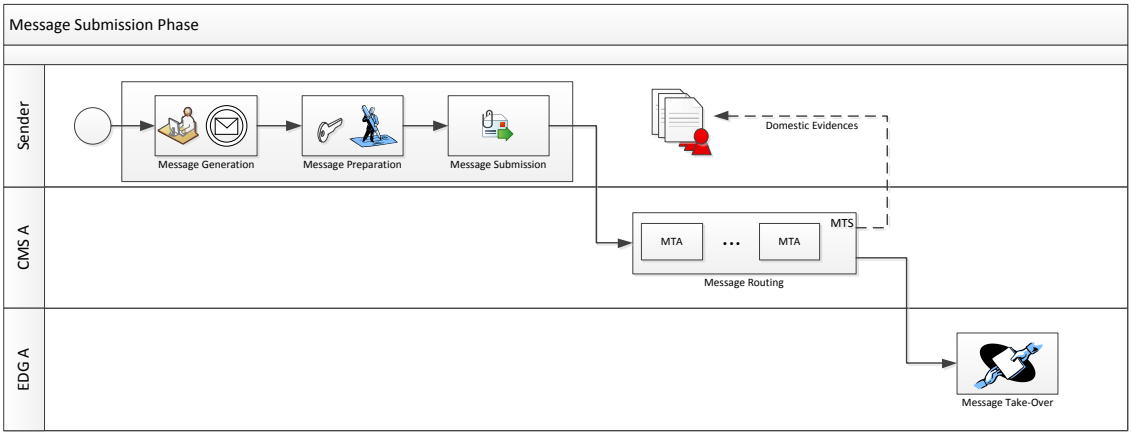

Figure 8.3: Process details of the message submission phase.

8.2.1 Actors

The following actors are involved in the message submission phase:

- Sender
- CMS A
- EDG A

Sender

The sender is the originator of a message. The sender is often associated with a natural person sending a dispatch message using a standard e-mail client as UA. However, the sender may also be a UA triggered by an automated application in business environments. In case of evidence messages, the

sender may also be a core CMS component like an MTA or a TTP generating evidences. As illustrated in Figure 8.3, depending on the concrete scenario and the CMS, the basic functions of a sender are:

1. Message generation
2. Message preparation
3. Message submission

A version of Figure 8.3 with more details can be found in Appendix A.

CMS A

The sender is part of CMS A and uses this system to deliver a message to the foreign recipient. As illustrated in Figure 8.3, the basic functions of CMS A are

1. Authenticate the sender to ensure that only authorized entities can initiate a cross-border message exchange.
2. Accept the sender's message.
3. Route the sender's message correctly to EDG A.

EDG A

EDG A is the gateway being in charge of handling cross-border messages of CMS A. As illustrated in Figure 8.3, the only function of EDG A in this phase is to accept domestic messages coming from CMS A.

8.2.2 Prerequisites

Even if this phase is completely CMS-specific and not covered by the EDG network, some prerequisites must nonetheless be fulfilled for a shared cross-border security context. A major prerequisite is trust, which must be regulated by an appropriate interoperability agreement. Only CMS complying with this agreement and fulfilling its requirements are allowed to join the interoperability network. Several aspects of the interoperability agreement and a governance structure are discussed in more detail in Chapter 12.

Prerequisites for the sender

The sender has to fulfill the following requirements:

1. The sender must be a registered user of CMS A.
2. The sender must be authorized by CMS A and have the means (for example UA) to submit messages to the MTS of CMS A.

The requirement of a registered sender has been applied to not compromise the security of single CMS. Most CMS expect that senders are registered users and are authenticated in some way. Systems allowing incoming messages from untrusted sources would thus bypass the basic security requirements of other CMS. For example, the Italian PEC allows incoming messages from regular e-mail users. Even if these messages are clearly tagged as "Non-CEM", the PEC system would have to ensure that only registered PEC users can submit cross-border messages.

Prerequisites for CMS A

CMS A has to fulfill the following requirements:

1. Have provisions to authenticate the sender.
2. Have a trust relationship with EDG A.
3. Be technically coupled with EDG A so that domestic CMS messages can be delivered to the gateway.

Prerequisites for EDG A

EDG A has to fulfill the following requirements:

1. Have a trust relationship with CMS A.
2. Provide an interface for CMS A to accept domestic CMS messages.

8.2.3 Stepwise Process Description

The cross-border CMS delivery is initiated by the sender. Subsequently the single activities of this process step are defined in detail. Each activity is numbered accordingly. For example, P1-A1 denotes the first Activity of Process 1 (message submission phase).

P1-A1: Sender Message Submission

Responsibility: Sender
Input/Prerequisites: None
Output/Results: Non-E2EE message submitted to the MTS of CMS A

First of all, the sender has to generate the message. This is done either manually or automatically by some application. This step is usually carried out within the sender's UA. The challenging part of message generation is addressing. As already discussed (cf. Section 6.2.3), it may be a difficult task for e-mail based CMS users to address recipients having different addressing schemes like unique identifiers. Addressing definitely threatens the desired property of transparency. Therefore, the sender's CMS must provide workarounds to tackle this issue. For example, the CMS can assign an own domain to the EDG. Slovenian recipients can then be addressed by their tax number using a virtual e-mail domain like `<taxnumber>.si@gateway-domain.com`. The addressing problem can also be solved by providing custom plugins for UAs offering a generic GUI for entering foreign address data. The address data can then be wrapped into a domestic address format or be wrapped as additional message metadata, for example as e-mail header, XML fragment in SOAP messages or even as message attachment if the use of metadata is restricted. These are just a few possible approaches of how to solve the addressing problem. All of them potentially threaten transparency, but in general, this requirement can only be met partially due to the heterogeneity of addressing schemes and the fact that addressing is a core CMS aspect on the transport and message layer.

After having generated the message, the sender may decide to prepare it for submission by additionally signing or encrypting the message. The signature provides NRO evidence for each entity on the message route. As discussed in the preceding chapter, the sender must not encrypt the message for E2EE on the message layer. Nevertheless, single parts like attachments may be encrypted without any problems as long as the routing information of the message envelope is preserved.

Finally, the sender submits the message to the MTS of CMS A. This step heavily depends on the actual CMS type. For example, in e-mail-based CMS, the sender's UA submits the message to the sender's MTA. In SOAP-based system like the Austrian DDS, the message may be directly submitted to the recipient's MS. This is EDG A. Independent from the actual submission process, the MTS must authenticate the sender and confidentiality should be ensured by a point-to-point encryption like TLS between the sender's UA and the CMS. Both aspects should be defined as a requirement by an interoperability agreement.

P1-A2: Message Routing

Responsibility:	CMS A
Input/Prerequisites:	Message of an authenticated sender
Output/Results:	Message routed and transmitted to EDG A

CMS A has the duty to correctly route the sender's message to EDG A. In order for this to work, the CMS must recognize that the message is addressed to an external recipient not belonging to the own system. This step heavily depends on the CMS type and on how cross-border addressing is solved by the system. For example, if as described above, the gateway has an own domain, routing is quite straightforward and easy. No matter what mechanism is applied, both the CMS and the sender must have a common understanding of how external recipients are addressed. In lookup-based system like the Austrian DDS, the lookup service could directly redirect the sender to the EDG in case of foreign addresses. By all means, the addressing information entered by the sender must be preserved by CMS A for further routing by the EDG. Depending on the CMS, several evidences could be generated on the message route to EDG A.

The actual location of EDG A is not significant as long as CMS A has a trust relationship with EDG A. EDG A could be:

- A standalone instance mimicking a standard CMS provider.
- An integral part of an existing CMS provider.
- A TTP service having a custom interface.

In the latter case, transparency would not be preserved anymore. However, systems like moja.posta.si having just one single provider could settle for implementing one additional interface. At the bottom line, the actual implementation of EDG A depends on the decision of the CMS on how to best integrate the gateway functionality into the existing system.

8.3 Message Translation Phase

The message translation phase comprises the needed steps to process an incoming domestic message of CMS A. The incoming message must be validated, translated to the DGP format and routed correctly to the recipient's gateway, which in this case is EDG B.

8.3.1 Actors

The following actors are involved in the message translation phase:

- CMS A
- EDG A

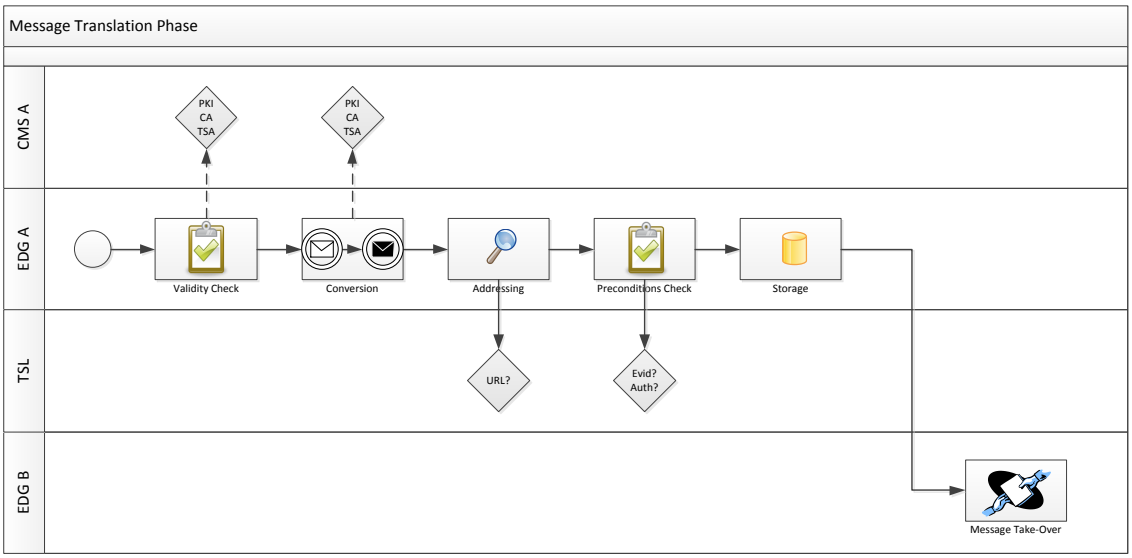

Figure 8.4: Process details of the message translation phase.

- Central TSL instance
- EDG B

CMS A

In this phase, CMS A has just an auxiliary function and helps EDG A to verify domestic messages. As illustrated in Figure 8.4, the basic functions of CMS A in this phase are:

1. Provide necessary means to check the validity of domestic CMS messages.
2. Provide necessary means to translate the domestic message into the DGP format.

A version of Figure 8.4 with more details can be found in Appendix A.

EDG A

EDG A has the duty to translate domestic CMS messages into the DGP format and to forward them to the gateway of the designated recipient. As illustrated in Figure 8.4, the basic functions of EDG A in this phase are:

1. Check the validity of incoming domestic messages of CMS A.
2. Convert the CMS A message format into the DGP format.
3. Resolve the Web service location of the recipient's EDG.
4. Check if the remote gateway fulfills all requirements and preconditions.
5. Storage of any necessary message-related state information in order to be able to correctly terminate the delivery process.
6. Forward the DGP message to the recipient's EDG.

Central TSL instance

The central TSL instance provides the means to operate a trusted network of EDGs and to check if a remote system fulfills certain requirements and preconditions in terms of evidences and authentication levels.

As illustrated in Figure 8.4, the basic functions of the TSL instance in this phase are:

1. Resolve the Web service location of EDG B, the recipient's gateway.
2. Provide the necessary metadata to check if a remote gateway fulfills certain requirements and preconditions in terms of evidences and authentication levels.

EDG B

EDG B is the recipient's gateway and has the duty to handle incoming cross-border messages of other gateways, in this case EDG A. As illustrated in Figure 8.4, the only function of EDG B in this phase is to accept incoming messages of EDG A.

8.3.2 Prerequisites

EDG A, the central TSL instance and EDG B must fulfill certain prerequisites to ensure a smooth message translation from the domestic CMS A format to the DGP protocol and the subsequent transmission to EDG B.

Prerequisites for EDG A

EDG A has to fulfill the following requirements:

1. Have a trust relationship with CMS A to verify incoming domestic CMS messages.
2. Be part of the EDG trust network and have a custom TSL service entry.

Prerequisites for the central TSL instance

The central TSL instance has to fulfill the following requirement: be signed and centrally hosted by the governance body of the interoperability network.

Prerequisites for EDG B

EDG B has to fulfill the following requirement: be part of the EDG trust network and have a custom TSL service entry.

8.3.3 Stepwise Process Description

This section defines in detail the single process steps for translating local CMS A messages to the DGP format and delivering them to the recipient's gateway (EDG B). The process for both dispatch and evidence messages is quite similar. Therefore, these steps are just described once. Those parts that differ for each message type are explicitly highlighted.

P2-A1: Domestic Message Validity Check

Responsibility:	EDG A, CMS A
Input/Prerequisites:	Domestic CMS A message
Output/Results:	Validated CMS domestic message

The main aim of this step is to ensure the validity and genuineness of incoming domestic messages. This step is completely domain-specific and typically comprises technical checks concerning formats and policies as well as security-related checks like signature verification, trust validation, etc. Particularly the latter check may require the gateway to access certain trust information within CMS A, for example a PKI.

If the message is not valid, it must be rejected. Depending on the sender's CMS and the role of the EDG within the CMS, an evidence indicating the rejection status may be generated by the gateway or the submitting entity.

P2-A2: Domestic Message Translation

Responsibility:	EDG A, CMS A
Input/Prerequisites:	Validated CMS A message
Output/Results:	Translated DGP message

Successfully validated CMS messages must be translated to the DGP format. In case of dispatch messages, the gateway has no previously stored information on this message. This may not be the case for evidence messages. A gateway may be forced to store certain information of the original dispatch message or even previous evidences. In this case the gateway can now access this information for the translation process.

CMS dispatch messages are converted to the DGP dispatch message format (cf. Section 7.2.2.3) and CMS evidence messages are converted to the DGP evidence message format (cf. Section 7.2.2.4). Most of this translation is quite straightforward and is conducted by the technical gateway part. The gateway creates an empty SOAP DGP message and fills in all available parts from the domestic CMS message. Information, which is mandatory for the DGP message but not available from the domestic message is artificially generated by the gateway. For example, if the domestic format does not have file names for message attachments, the gateway can generate new ones.

Semantic information like the sender's or recipient's authentication level are processed by the semantic gateway part. Each gateway has to provide a mapping table between domestic authentication levels and the four QAA levels when joining the interoperability framework. This mapping table must be continuously maintained and also updated accordingly in the TSL. The conversion of authentication levels is thus just a simple table lookup operation.

The DGP only supports the sending of messages to single recipients. If the domestic CMS message is addressed to multiple recipients, EDG A has to split up the message and create an own DGP message for each recipient.

Finally, the gateway signs the final DGP message using an enveloped XML signature. The format and quality of this signature is given by the interoperability agreement. This agreement could force the gateway to sign the message for example with a XAdES signature. The gateway must use the signature certificate, which is defined as digital identity in its TSL entry. The signature process is the same for dispatch and evidence messages.

P2-A3: Address Resolution

Responsibility: EDG A, TSL
Input/Prerequisites: CMS A message, DGP message
Output/Results: Web service URL of the recipient's DGP

Addressing is the most difficult part and requires some gateway logic. First of all, the destination system has to be determined. This can only be done on the basis of the available addressing information from the domestic CMS message or in case of evidence messages from previously stored information. For example, an e-mail address ending with "@moja.posta.si" unequivocally identifies an address of the Slovenian moja.posta.si CMS. The tuple (john.doe@pec-system.com, IT) would for example unequivocally identify a PEC e-mail address. If the address cannot be unequivocally matched with another CMS, the message must be rejected. Depending on the sender's CMS and the role of the EDG within the CMS, an evidence indicating the rejection status may be generated by the gateway or the submitting entity.

If the addressing information is valid, the EDG looks up the Web service URL of the matching gateway EDG B in the TSL. This described addressing approach is rather complex and requires a lot of processing and alignment with other CMS. If the change management process of addressing is not correctly conducted throughout the whole interoperability framework, this part is at risk of becoming error-prone. A better approach to addressing is discussed in the next chapter.

P2-A4: Delivery Preconditions Check

Responsibility: EDG A, TSL
Input/Prerequisites: CMS A message, DGP message
Output/Results: Validated preconditions

This step only concerns dispatch messages and is carried out when the address resolution check is performed. Having found the EDG B entry in the TSL, the procedural gateway part checks whether CMS B fulfills the necessary requirements and preconditions. First, it may check whether CMS B supports a minimum authentication level for the recipient. If this requirement is not fulfilled, the request must be rejected. Depending on the sender's CMS and the role of the EDG within the CMS, an evidence indicating the rejection status may be generated by the gateway or the submitting entity. Second, the procedural gateway part checks whether CMS B supports all required evidences. If some domestic evidences are not supported, the procedural gateway must initiate the process of mimicking evidences. This means, the gateway exactly knows, which evidences it must mimic and at what point in time this has to generate them. Depending on the CMS and the implemented logic, the gateway may have to store some information related to this dispatch message. This is done in the next process step.

P2-A5: Information Storage

Responsibility: EDG A
Input/Prerequisites: CMS A message, DGP message
Output/Results: Storage of necessary message-related information

This step is completely CMS-specific. The storage of message-related information may be necessary to avoid complex gateway logics. Storing metadata of dispatch messages allows the gateway to easily associate incoming evidence messages to their related dispatch message or to easily reconstruct or mimic evidences.

Depending on CMS policies, the gateway may also be forced to create an audit trail and store evidential information for a certain amount of time.

After having made the precondition fulfillment check and eventually stored any message-related information, the translated DGP message is sent to the Web service of EDG B. This is where the message delivery phase starts.

8.4 Message Delivery Phase

The message delivery phase deals with the delivery of a message within the recipient's CMS. The process steps in this phase cover the reception of the DGP message by EDG B, the translation to the domestic format of CMS B, validity and precondition checks and the delivery to the final recipient by the MTS of CMS B.

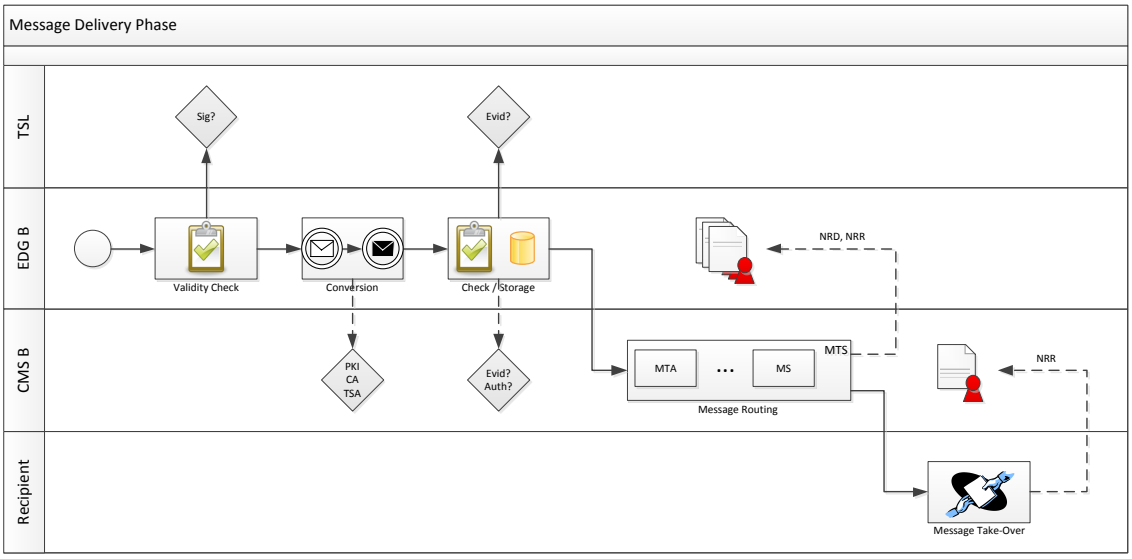

Figure 8.5: Process details of the message delivery phase.

8.4.1 Actors

In the message delivery phase the following actors are involved:

- Central TSL instance
- EDG B
- CMS B
- Recipient (being part of CMS B)

Central TSL instance

As illustrated in Figure 8.5, the basic functions of the TSL instance in this phase are:

1. Resolve the signature certificate of EDG A.
2. Determine evidences required by EDG A.

A version of Figure 8.5 with more details can be found in Appendix A.

EDG B

EDG B translates DGP messages into the domestic CMS B format and forwards them to CMS B for final delivery to the designated recipient. As illustrated in Figure 8.5, the basic functions of EDG B in this phase are:

1. Check the validity of incoming DGP messages.
2. Convert the DGP message format into the domestic format of CMS B.
3. Check the preconditions for the final delivery.
4. Forward the domestic message to the MTS of CMS B.

CMS B

CMS B delivers the message to the final recipient. As illustrated in Figure 8.5, the basic functions of CMS B in this phase are:

1. Provide necessary means to translate the DGP message to the domestic CMS B format.
2. Deliver the message to the final recipient.
3. Provide resulting evidences to EDG B to be returned to the sender.

Recipient

The recipient is the last entity in the delivery process and receives the message. As illustrated in Figure 8.5, the basic functions of the recipient in this phase are:

1. Eventually accept/reject the message.
2. Eventually sign a corresponding NRR evidence to be returned to the sender.
3. Retrieve/Download the message.

8.4.2 Prerequisites

All actors including the central TSL instance, EDG B, CMS B and the recipient must fulfill certain prerequisites to ensure a smooth message delivery.

Prerequisites for the central TSL instance

The central TSL instance has to fulfill the following requirement: be signed and centrally hosted by the governance body of the interoperability framework.

Prerequisites for EDG B

EDG B has to fulfill the following requirements:

1. Be part of the EDG trust network and have an own TSL service entry.
2. Have a trust relationship with CMS B.
3. Be allowed to deliver domestic CMS B messages.

Prerequisites for CMS B

CMS B has to fulfill the following requirements:

1. Be able to correctly address the recipient by means of the data provided by EDG B.
2. Support the required authentication level.

Prerequisites for the Recipient

The recipient has to fulfill the following requirements:

1. Be a registered user of CMS B.
2. Support the required authentication level.

8.4.3 Stepwise Process Description

This section defines in detail the single process steps for translating DGP messages to the local CMS B message format and delivering them to the final recipient. The process for both dispatch and evidence messages is quite similar. Therefore, these steps are just described once. Those parts that differ for each message type are explicitly discussed.

P3-A1: Message Validity Check

Responsibility:	EDG B
Input/Prerequisites:	Incoming DGP message from EDG A.
Output/Results:	Validated DGP message.

Incoming DGP messages first have to be checked for validity. This check includes the format correctness of the SOAP message, the XML schema check of the DGP message, a digest value validation of message attachments as well as an XML digital signature validation of the DGP message. EDG B looks up in the TSL the signature certificate of EDG A to check whether the signature is trusted. If the message validation fails, the message must be rejected and an appropriate SOAP error indicating this circumstance must be returned to EDG A. Depending on the sender's CMS and the role of EDG A within the CMS, an evidence indicating the rejection status may be generated by EDG A or the submitting entity.

P3-A2: Message Conversion to Domestic Format

Responsibility: EDG B, TSL
Input/Prerequisites: Validated DGP message
Output/Results: Converted CMS B message

The message conversion from the DGP format to the domestic format of CMS B is carried out by the different gateway parts in a similar manner as for the conversion from the domestic CMS A format to the DGP format by EDG A. Based on the available data (metadata, attachments) from the DGP message, the domestic CMS B message is constructed. In case of evidence messages this conversion may require access to previously stored information, for example to reconstruct entity information or original message IDs. This step is quite straightforward and basically includes conversions on the technical level and several mappings on the semantic level. Depending on the architecture of CMS B, EDG B may need to access some of its security services (PKI, TSA, etc.) to generate the domestic CMS B message.

P3-A3: Preconditions Check and State Storage

Responsibility: EDG B, TSL, CMS B
Input/Prerequisites: Validated DGP message, Converted CMS B message
Output/Results: Determined preconditions for CMS B message delivery

Prior to submitting the converted message to the MTS of CMS B, EDG B checks two necessary preconditions: first, the gateway checks whether the recipient can actually fulfill the required minimum authentication level. Even when the supported authentication levels of CMS B are listed in the TSL, EDG A actually does not know which of these levels the recipient supports. This requires knowledge of CMS B where EDG B is the first instance in the delivery process having potential knowledge of this. Second, like EDGA, EDG B may also mimic evidences even if they are not supported by CMS B. For example, if the message delivery in CMS B is only acknowledged by a SOAP success message, EDG B may create an appropriate NRD evidence for CMS A. If EDG B supports such mimicked evidences, they must be listed in its TSL entry.

Depending on the actual conversion and delivery procedure, EDG B may need to store certain state information in order to finish the delivery process. Usually several evidences like NRD or NRR are produced on the delivery route in CMS B. These evidences have to be routed back to the sender. However, sometimes the sender of CMS A may not be visible from the point of view of CMS B. For example, due to addressing problems. In this case EDG B may be the "official" sender and insert its address data in the sender field of the CMS B message. Nevertheless, if such a replacement takes place, the original sender should be somewhere evident, for example by adding a cover sheet.

P3-A4: Message Routing and Delivery

Responsibility: EDG B, CMS B
Input/Prerequisites: Converted CMS B message
Output/Results: Message delivered to final recipient

Finally, EDG B submits the domestic message to the MTS of CMS B for the final delivery to the recipient. This step is completely CMS-specific. If EDG B is a core part of CMS B, for example having an own MTA, the step is quite straightforward. On the message delivery route several domestic CMS B evidences may be generated, which are addressed to the sender and routed back to EDG B.

Chapter 9

Improvements

"The biggest room in the world, is the room for improvement."

[Unknown source.]

The CMS interoperability concept and its process models presented in Chapter 7 and Chapter 8 have been elaborated by the author of this thesis as part of the e-Delivery pilot (WP 6.4) of the EU LSP STORK. Even if the concept has laid down a solid groundwork for CMS interoperability, there was still some room for improvement. Particularly the routing between EDGs of the presented concept requires a rather complex processing logic in each EDG and is a major barrier for autonomy, since addressing mechanisms of systems joining the interoperability network have to be integrated into each gateway. Static metadata like supported evidences and authentication levels is currently provided in the TSL. However, the main purpose of a TSL is to provide trust information and not arbitrary metadata. This information should be better located at each gateway. Last not least, some security aspects like replay attacks or man-in-the-middle attacks are also not fully covered.

WP3 of SPOCS is dealing with interoperable transport infrastructures. In its description of work [SPOCS Consortium, 2010], WP3 stated its e-Delivery-related objective already from the beginning.

> "*The overall objective of WP3 is to enable understanding and recognition of eDelivery systems in different member states. This leads to the following specific objectives:*
>
> - *Establish a common view on existing approaches regarding eDelivery in member states, identify areas for harmonization and describe possible solutions towards interoperability*
> - *Identify and deliver the required specifications to provide for interoperability of national approaches*
> - *Implement required modules and/or gateway functionality*
> - *Evaluate take-up and usage of the concepts and common specifications in the pilots"*

Due to their similar objectives, SPOCS WP3 has taken up the STORK concept presented in the preceding chapters and further extended and improved it in several aspects like addressing, efficiency, design reuse, open standards and interoperability agreement. The author of this thesis was heavily involved and actively participated in this improvement process. In contrast to the STORK e-Delivery pilot, which is demonstrating the CMS Level 2 interoperability framework between two CMS, SPOCS WP3 has a larger number of project partners and is thus implementing and testing the framework in a much broader scope. The improvements made in the course of the LSP SPOCS are discussed in the remainder of this chapter. The basic conceptual model of CMS interoperability has been taken from STORK and the next sections

discuss the improvements, which have been made to the STORK approach with the general SPOCS WP3 specifications [Apitzsch et al., 2010b] and the specifications of the Interconnect Protocol (ICP) [Apitzsch et al., 2010a], the improved version of the DGP. Implementation and testing aspects of the STORK and SPOCS approaches are discussed in Chapter 10 and Chapter 12, respectively.

9.1 Addressing and Routing

The STORK concept provides a rather generic and flexible addressing mechanism by supporting both unique identifiers and demographic data like name, date of birth, postal addresses, etc. This is quite useful in various scenarios and thus SPOCS follows a similar approach with some adjustments.

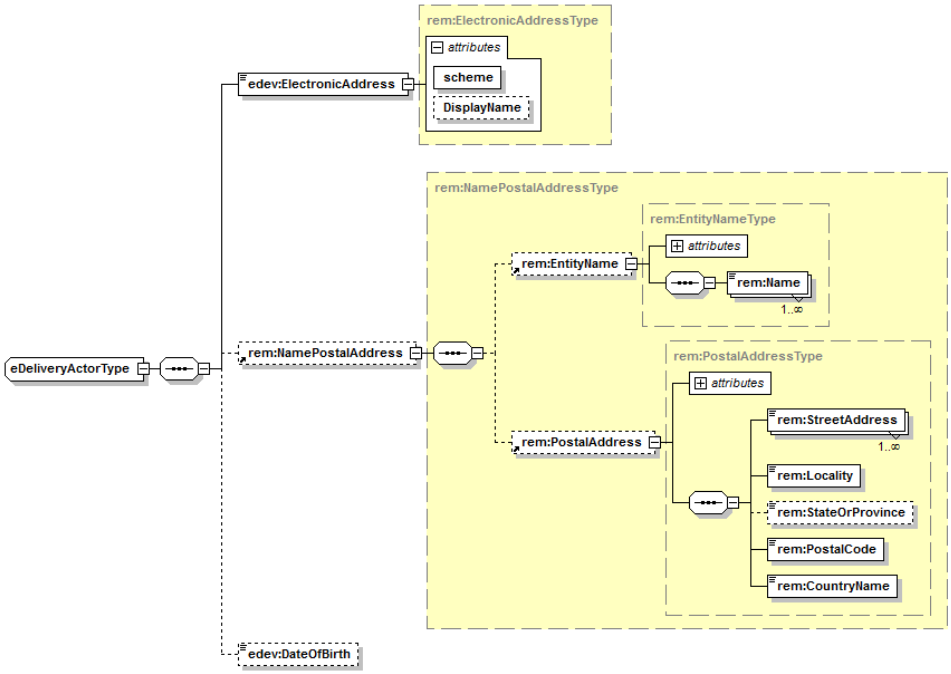

Figure 9.1: The eDeliveryActorType XML schema fragment is used by the ICP to uniquely address end-entities like senders and recipients.

Minor adjustments concern the ICP XML schema definition for addressing. The ICP *eDeliveryActorType* schema fragment (counterpart to STORK *SenderRecipientType*) is illustrated in Figure 9.1, which contains the following elements:

- `ElectronicAddress`. The definition of generic unique identifiers was replaced with the `ElectronicAddressType` element, which is an extension of the ETSI REM *ElectronicAddress* schema definition allowing a similar generic definition of unique addresses as has done STORK. The `scheme` attribute replaces the `Type` element of unique IDs in the STORK scheme and allows the definition of any kind of identifier. Even non-electronic IDs like tax numbers or social security numbers could be used. The `DisplayName` attribute has the same functionality as the display name in angled brackets used for Internet e-mail.

- `NamePostalAddress`. An entity's names and postal address can be defined with the REM `EntityName` and `PostalAddress` elements. When specifying the eDeliveryActorType, focus was on design reuse and the ETSI REM definition for entities provides a not-overloaded but yet fine-grained addressing mechanism well suitable for the ICP.

A major adjustment concerns the routing process. Whereas STORK requires all gateways to implement the routing on their own, SPOCS has chosen a smarter approach by relying on a Domain Name System (DNS)-based address routing model. Therefore, SPOCS has defined the Internet e-mail address format as the default scheme for electronic addresses, which must be supported by all EDGs. E-mail addresses are intuitive and familiar to most people. A CEM address in terms of an Internet e-mail address can also be easily printed on business cards. About half of today's CMS already use e-mail addresses. Therefore, for SMTP-based systems nothing changes. Other systems have to provide a virtual address by encoding the domestic format into an e-mail address format. The following list shows examples of potential virtual addresses:

- A Slovenian citizen being addressed by the tax number "1234567890" in the domestic CMS, would have the virtual address "1234567890@cem.si" in the cross-CMS context.
- An Austrian citizen addressed by name and date of birth may have the following virtual address in the cross-CMS context: "name.dateofbirth@cem.at".
- A EGVP entity being addressed by an URL like "http://egvp-provider.de/recipient-id", may have the virtual address "recipient-id@egvp-provider.de".

Besides user-friendliness, e-mail addresses ease the routing process, since the destination gateway can be determined on the basis of the domain part of the virtual or real e-mail address. The SPOCS approach works as follows: each domain of a CMS address is associated with a particular gateway instance. However, the gateway must not necessarily be part of the related domain infrastructure. This would be a problem in systems like PEC, where users can choose arbitrary domains as PEC addresses. SPOCS just requires that the address of the associated gateway can be looked up through the corresponding DNS entry <gateway-prefix>.<domain-name>, where <gateway-prefix >must be a fixed value defined by an interoperability agreement. For instance, if <gateway-prefix>would be "cmsgw", in case of the above example address 1234567890@cem.si, the corresponding gateway address could be looked up by resolving the DNS name "cmsgw.cem.si". The DNS-lookup will provide the IP-address of the gateway related to recipient's domain.

As the ICP is based on SOAP, a common value for the local part of the SOAP entry point of all gateways must be agreed upon, for example "cms-gw", which then would lead to a gateway Web service URL like "https://<gateway-prefix>.<domain-name>/cms-gw".

9.2 Evidences

The ICP improves the STORK DGP evidence format in several aspects. The DGP has adopted single elements and their meanings from the REM schema. The ICP fully integrates the REM schema. This fosters interoperability by relying on existing open standards. The REM XML schema is rather generic so that a restricted REM profile has been defined for the ICP. For example, the REM `AuthenticationMethod` element must match one of the following six authentication qualities:

1. `http:uri.etsi.org/REM/AuthMethod#Basic`
2. `http:uri.etsi.org/REM/AuthMethod#Enhanced`
3. `http:uri.etsi.org/REM/AuthMethod#Strong`
4. `http:uri.etsi.org/REM/AuthMethod#AdES`
5. `http:uri.etsi.org/REM/AuthMethod#AdES-Plus`

6. `http:uri.etsi.org/REM/AuthMethod#QES`

The exact meaning of the single authentication qualities is described in detail in part 2 of the ETSI REM standard [ETSI, 2010c, B1.6, page 61]. The use of the STORK QAA levels and authentication tokens for senders and recipients is described in more detail below in the security part (cf. Section 9.6).

In contrast to the DGP, the ICP defines the following (REM) evidences:

1. SubmissionAcceptanceRejection
2. RelayToREMMDAcceptanceRejection[1] (denotes the acceptance or rejection of the ICP message by the recipient's gateway)
3. DeliveryNonDeliveryToRecipient
4. RetrievalNonRetrievalByRecipient
5. AcceptanceRejectionByRecipient
6. ReceivedByNonREMSystem

Compared to the DGP evidence set, it can be seen that the *DownloadNonDownloadByRecipient* evidence has been replaced with the *ReceivedByNonREMSystem*. In the end there is a thin line between downloading or retrieving a message. A download can be seen as a kind of retrieval. Therefore, SPOCS has decided to simplify evidence handling by removing the DownloadNonDownloadByRecipient evidence. The RetrievalNonRetrievalByRecipient evidence should cover both events. The ReceivedByNonREMSystem evidence has been added in turn. As discussed for the semantic gateway part (cf. Section 7.2.1.1), forwarding non-CEM messages may threaten the security requirements of single systems expecting only CMS messages. However, some systems like PEC allow the reception of non-CMS messages. The next section discusses in detail how both aspects have nevertheless been reconciled.

9.3 Messaging

The ICP message format extends the DGP in several aspects. First of all, SOAP 1.2 [Gudgin et al., 2007] is supported in addition to SOAP 1.1. SOAP 1.2 has several advantages over its predecessor. It supports XML information sets [John and Tobin, 2004], other transport protocols than HTTP and allows to customize the SOAP processing model.

To ease inter-gateway communications, the ICP makes use of the WS-Addressing [Gudgin et al., 2006] standard. SPOCS uses WS-Addressing to define the EDG addresses within the SOAP header. Receiving gateways can extract this address and more easily search in the TSL for the entry of the sending gateway. WS-Addressing is also used to define a unique message ID (not to be confused with the dispatch message ID) to prevent replay attacks. This aspect is discussed later in this chapter in the security part (cf. Section 9.6). The WS-Addressing `Action` element makes it easier for applications implementing the gateway functionality to determine the message type. In the case of STORK, the message type (dispatch or evidence) can only be differentiated when parsing the SOAP body. SPOCS facilitates this by providing the necessary data already in the SOAP header. The following message types are defined:

- REMDispatch (dispatch message)
- REMMDMessage (evidence message)

[1] REM-MD is the abbreviation for REM-Management Domain

- WS-Addressing fault message
- SOAP fault message

Besides the two fault types, an ICP message may hold either a so-called *REMDispatch* or a *REMMDMessage* message. Their structure, content and meaning is discussed below.

SOAP per se does not guarantee that messages actually arrive at their destination. In most cases, resilient communication channels are used and messages may get lost. This is usually no big deal. If the sender of a SOAP message does not receive an answer, it can simply resend the message. However, if acknowledge messages get lost on the way back to the sender, the recipient may be flooded with always the same message. This is not a desired situation. Therefore, SPOCS uses the WS-ReliableMessaging standard to ensure that messages are delivered exactly once. WS-ReliableMessaging uses additional message brokers, one for the sender and one for the recipient. Both brokers transparently communicate with each other and by using sequence numbers they assure that the message is delivered exactly once. A similar mechanism is used by TCP/IP to ensure that each packet arrives at its destination.

The STORK DGP stores static metadata like supported authentication levels and evidences within the EDG entry of the TSL. Since the TSL should just contain trust-related information, the SPOCS approach outsources this information into a parallel file of the WSDL file each gateway has to provide for its Web services interface. Prior to sending a message to the recipient's gateway, the sender's gateway has to fetch the this metadata file and to check the necessary preconditions. The metadata content may be cached for a short period of time, for example if multiple messages have to be sent to the same gateway in a row.

Another difference between the DGP and ICP is evidence metadata. In case of the DGP, the TSL holds a list of evidences supported by the CMS. The static EDG metadata in the case of the ICP differentiates between supported and requested evidences. Both sets must not necessarily be congruent. For example, a CMS may decide to support more evidences than offered by the system itself. This can be achieved by mimicking additional evidences.

The structure of ICP dispatch and evidence messages is slightly different compared to the STORK DGP format. First of all, the *DeliveryRequest* and *EvidenceRequest* elements are named *REMDispatch* and *REMMDEvidence*, respectively. Their details are discussed in the following sections.

9.4 Dispatch Messages

Figure 9.2 illustrates the XML schema fragment of an ICP dispatch message. Compared to the DGP format, the information is structured more compact and contains the following elements:

- `MetaData`. Holds the sender's and recipient's address information as well as any delivery constraints (similar to the DGP's delivery options). The details of this element are discussed below.
- `NormalizedMessage`. Denotes the translated message body (for example e-mail body) as well as any attachments. The details of this element are discussed below.
- `OriginalMessage`. The ICP allows to optionally carry the original CMS message. Even if this will be the rare case, it may be of interest for the recipient's CMS to have certain knowledge about the original message. This requires that the recipient's EDG establishes a bilateral context with the sender's EDG and has knowledge about the specific message format. Receiving gateways can declare their request for original messages in their metadata file (the one parallel to the WSDL file). The original message is embedded "as is" and can be referenced via the XOP mechanism as Base64-encoded data. The two attributes `size` and `ContentType` denote the size and MIME type of the original message, for example `message/rfc822` for Internet e-mail MIME messages.

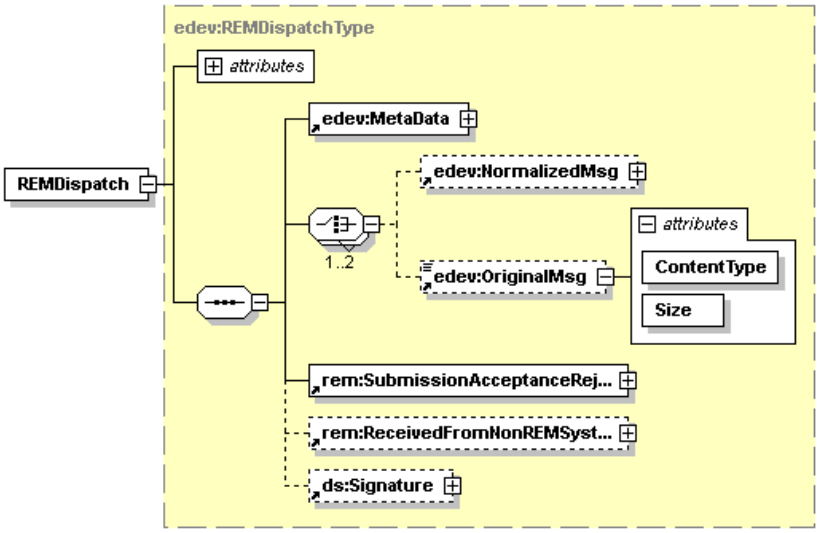

Figure 9.2: ICP REMDispatch XML schema fragment.

- `SubmissionAcceptanceRejection`. Denotes a REM XML SubmissionAcceptanceRejection evidence attesting that the sender's gateway has accepted the message from the domestic CMS. This evidence is mandatory and it is up to the recipient's gateway whether it is processed or not.
- `ReceivedByNonREMSystem`. Denotes a REM XML ReceivedByNonREMSystem evidence attesting that the sender's gateway has forwarded a message originating from a non-CMS. Some system like PEC accept that kind of messages. Most other systems will likely reject the ICP message if it contains such an evidence. It has to be regulated by the interoperability agreement that all systems are required to embed this evidence if they forward a message from a non-CMS.
- `Signature`. As will discussed below, the whole ICP including SOAP header and body is signed with a Web Services Security (WS-Security) [OASIS Web Service Security (WSS) TC, 2006] signature. This signature is contained in the header and processed automatically and thus not directly visible to the processing part of the EDG. However, the SOAP body may be additionally signed to provide a transferable evidence of the whole body using the `Signature` element.

Figure 9.3 illustrates the *MetaData* element. This element holds any non-content-related data like addressing information, delivery metadata (timestamps), deadlines, etc.

- `DeliveryConstraints`
  - `Origin`. Denotes the date and time the message was submitted by the sender.
  - `InitialSend`. Denotes the mandatory date and time the message was first delivered by the sender's CMS. This element corresponds to the DGP `SendingTimeStamp` element.
  - `ObsoleteAfter`. Denotes the message expiration deadline. This element corresponds to the DGP `MaxTimePickUp` element.
  - `Any`. Allows the definition of additional constraints, either negotiated bilaterally or defined by future extensions of the specification.
- `Originators`
  - `From`. Denotes the sender's address and identity.

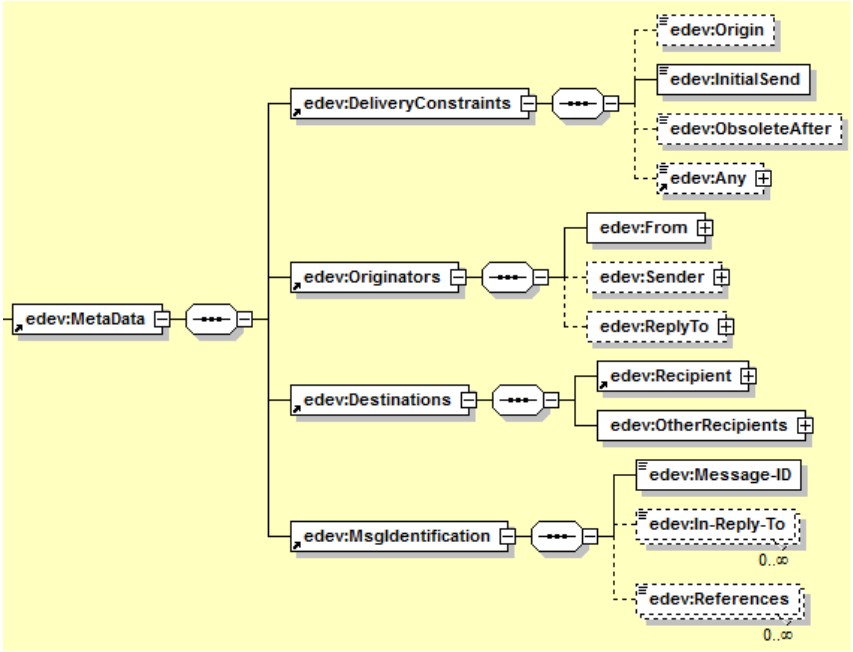

Figure 9.3: ICP MetaData XML schema fragment.

  - `Sender`. Denotes a delegate's address and identity acting on behalf of the actual sender.
  - `Reply-To`. Denotes the address where a reply to this message should be sent to. This messaging element has been adopted from Internet e-mail.

- `Destinations`
  - `Recipient`. Denotes the recipient's address and identity.
  - `OtherRecipients`. Denotes the address and identity of other recipients, for example the ones listed in the "CC:" or "BCC:" fields of an e-mail message. This element is just informal, because like in the STORK case, an ICP can only be sent to one single recipient. If the message is addressed to multiple recipients, the sending EDG must split up the original CMS message into multiple ICP messages.

- `MsgIdentification`
  - `Message-ID`. Denotes the unique ICP message ID of the dispatch message.
  - `In-Reply-To`. Denotes the ICP message ID this dispatch message is a reply to.
  - `References`. Denotes a series of ICP message IDs this message is related to, for example from a conversation or communication thread.

Figure 9.4 illustrates the XML schema fragment of a normalized message, which holds all content-related data. This includes all attachments as well as any informational data like an e-mail body or the message subject. The structure of the normalized message element is aligned to the e-mail message for an easier understanding and take-up by implementers, but basically covers most content-related aspects of other CMS types as well.

- `Informational`
  - `Subject`. Denotes the message subject.
  - `Comments`. Denotes informal comments to the message according to RFC 5322 [Resnick, 2008].

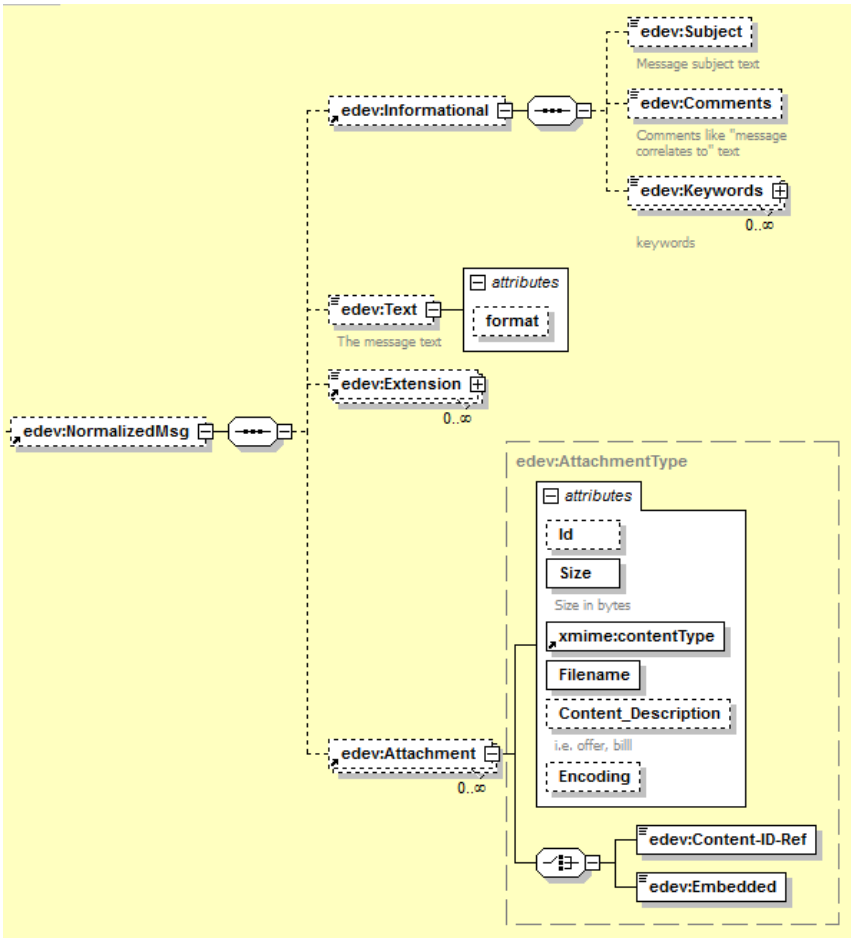

Figure 9.4: ICP NormalizedMessage XML schema fragment.

  - `Keywords`. Denotes additional keywords regarding the message according to RFC 5322 [Resnick, 2008].

- `Text`. Contains the textual part of message, for example the e-mail body or a cover sheet. The `Format` attribute indicates the text format. It may either have the value “text” or “html”.
- `Extension`. Allows the definition of additional content, either negotiated bilaterally or defined by future extensions of the specification.
- `Attachment`. Contains all attachments. The attribute `contentType` denotes the MIME type, `Filename` the file name, `Content_Description` a brief description of the attachment and `Encoding` the MIME “Content-Transfer-Encoding”, respectively. The actual content of the attachment is either referenced by the `Embedded` element through the MTOM XOP referencing mechanism or by the `Content-ID-Ref` element, which must be the content ID referencing a message part of the original message in the `OriginalMsg` element.

9.5 Evidence Messages

Figure 9.5 illustrates the XML schema fragment of an ICP evidence message. Compared to the DGP format, the information is structured more compact and contains the following elements:

- `REMMDSingleEvidence`. Holds the evidence in the ETSI REM XML format. The SubmissionAcceptanceRejection and ReceivedByNonREMSystem evidences can only be used in conjunction

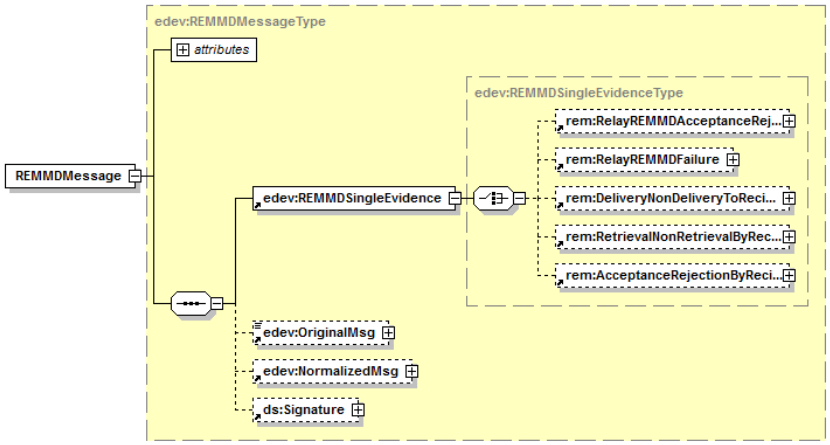

Figure 9.5: ICP REMMDMessage XML schema fragment.

with the dispatch message in the direction from the sender's to the recipient's CMS. The remaining five evidences are intended for the way back from the recipient's to the sender's CMS. Therefore, this elements provides a choice to select between one of these evidences.

- `OriginalMsg`. Has the same structure as for the dispatch message, but denotes the original message of an evidence message.
- `NormalizedMsg`. Has the same structure as for the dispatch message, but denotes the original content of an evidence message.
- `Signature`. Has the same meaning as for the dispatch message to generate a transferable ICP evidence message.

9.6 Security

Compared to the STORK approach, SPOCS has introduced several additional security measures to mitigate the risks of potential threats and attacks at a minimum. Each TSL entry not only contains the certificate for signing ICP messages, but additionally contains the SSL server certificate. Sending gateways can now directly check during the SSL handshake whether the server's certificate is trusted or not. This measure prevents man-in-the-middle attacks and avoids the implementation of SSL client authentication. An attacker intercepting the SSL connection establishment would be immediately detected due to a different SSL server certificate. One may argue that SSL client authentication would provide an additional security layer. However, receiving gateways have to check the ICP signature and would thereupon detect a non-authorized gateway. If an attacker really comes in the possession of the signature certificate, one can assume that the sender's gateway has been compromised and that the attacker may potentially be in the possession of the SSL client certificate as well. At the bottom line, its also a trade-off between usability and security. Web server solutions out there (Apache HTTP server[2], Microsoft IIS[3], etc.) have custom SSL handling mechanisms. So far, none of these solutions has a built-in TSL support. Mandatory SSL client authentication would thus be a barrier for an easy integration of the CMS interoperability framework into existing infrastructures.

SPOCS uses WS-Security as the core mechanism for the ICP message. WS-Security provides a security token by means of an XML signature in the SOAP header. This signature covers the following elements:

[2] `http://httpd.apache.org`
[3] `http://www.iis.net`

1. ***SOAP body***. By signing the SOAP body, the integrity and authenticity of the ICP message content is ensured. The signature is applied to both dispatch and evidence messages. Receiving gateways must validate this signature and check whether the signing certificate matches the certificate of the corresponding EDG entry in the TSL. If the signature value check or the certificate trust check fails, the ICP request must be rejected.

2. ***Timestamp***. A WS-Security timestamp ensures that the message is only valid for a short period of time (for example 5 minutes). This mitigates the risk that lost or unsent messages can be used for replay attacks.

3. ***WS-Addressing headers***. By signing the WS-Addressing headers, the sender's gateway source address is protected. Moreover, the WS-Addressing `MessageID` must be unique and thus prevents any replay attacks. This implies that the receiving gateway preserves the message ID for at least the validity period of the timestamp value described above.

Even when covered by the overall WS-Security signature, all REM evidences are additionally signed with an enveloped signature. This makes evidences transferable so that they can be extracted from the ICP by still having a valid signature. In this way they can independently be used by the receiving EDG or CMS for long-term archival.

Evidences may contain additional authentication or identification information by means of an OASIS Security Assertion Markup Language (SAML) assertion [OASIS Security Services TC, 2005] in the `AdditionalDetails` part of the entity's `AuthenticationDetailsType` element. The ICP has profiled the assertion defined and used by STORK. STORK has specified a protocol for carrying identity attributes of authenticated entities in a cross-border context. Examples of identity attributes are

- Unique electronic identifier (eIdentifier)
- Given name
- Surname
- Date of birth
- Gender
- Nationality code
- e-mail address
- Residence address
- Age
- Fiscal number
- QAA level

The use of the STORK protocol ensures better interoperability with other components processing foreign identities according to STORK. The STORK eID interoperability model uses the SAML *bearer* subject confirmation method, because the identity and authentication information is carried over HTTPs POST requests through the user's browser from the identity (and attribute) provider to the service provider. In the case of CMS interoperability, entities are just involved in the initial (sender) or final (recipient) delivery phase. The sender's or recipient's EDG vouches for the correct authentication procedure and supplied identity attributes of entities. SAML assertions in ICP evidences therefore use the *sender-vouches* subject confirmation method.

9.7 Process Flow

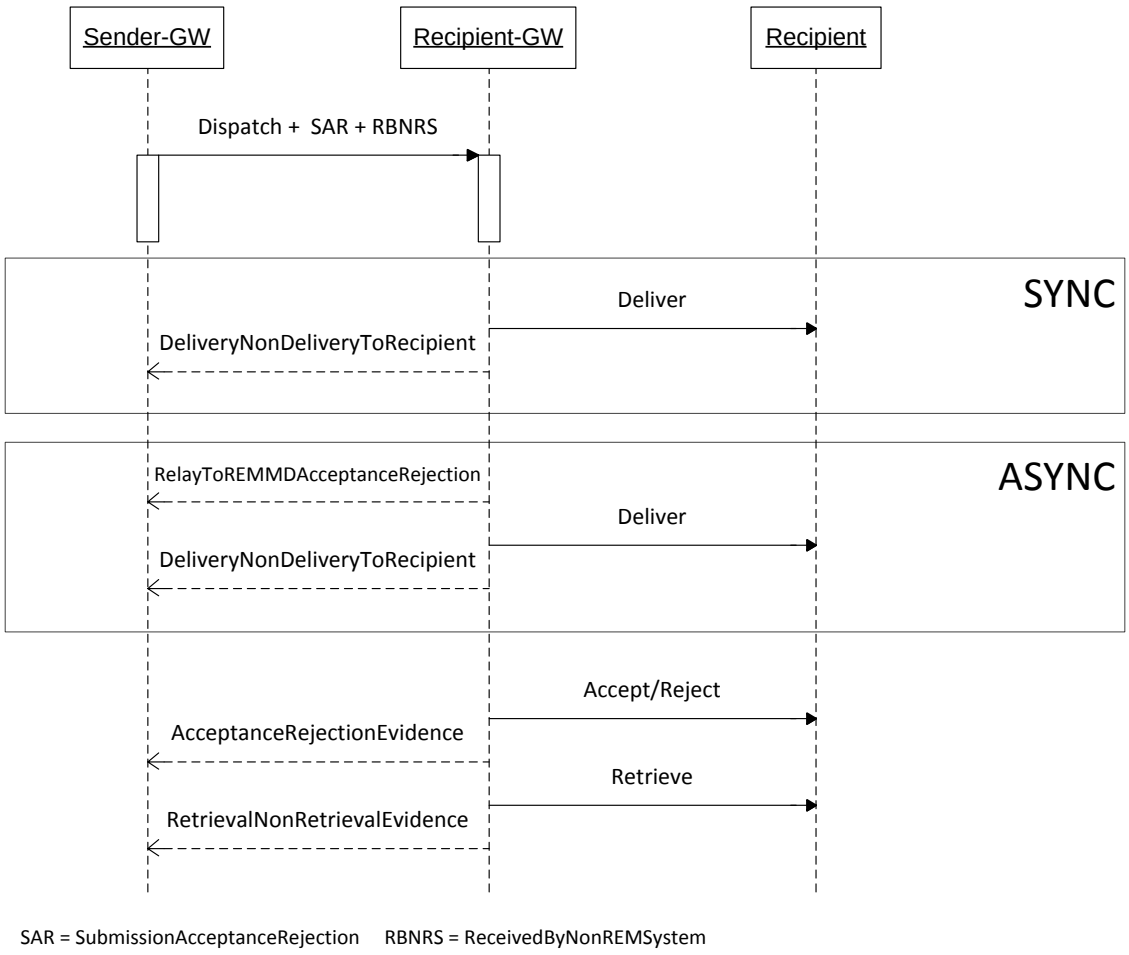

Figure 9.6: SPOCS evidence process flow.

The process flow of the SPOCS CMS interoperability concept (cf. Figure 9.6) is almost equal to the STORK process discussed in Chapter 8. Besides the mentioned different addressing and security mechanisms, the main difference of both process models is evidence handling. STORK has a rather simple evidence handling. Per request either exactly one dispatch or evidence message is supported. Moreover, all evidences can only be returned asynchronously. This means the sender's gateway is usually forced to preserve information about the dispatch message in order to match incoming evidences. In this regard, SPOCS applies a smarter approach. First, the SubmissionAcceptanceRejection and ReceivedByNonREMSystem evidences can be carried together with the dispatch message to the recipient's gateway. This saves extra inter-gateway evidence messages. Second, SPOCS supports two delivery modes: synchronous and asynchronous delivery. The asynchronous mode is the same as used by STORK. This means the ICP message is forwarded to the recipient's gateway, which checks it and immediately returns a RelayToREMMDAcceptanceRejection evidence back to the sender's gateway (STORK returns a SOAP acknowledgment). Further evidences like DeliveryNonDeliveryToRecipient, RetrievalNonRetrievalByRecipient or AcceptanceRejectionByRecipient are returned asynchronously at a later point in time. With the synchronous mode the recipient's gateway tries to deliver the message to the recipient's MS upon receiving an ICP dispatch request. If the status can immediately be determined, the recipient's

gateway returns a DeliveryNonDeliveryToRecipient evidence as response in the SOAP backchannel of the ICP dispatch request. This saves one more extra asynchronous evidence message. If the delivery status cannot immediately be determined, the RelayToREMMDAcceptanceRejection is returned and all further evidences are returned asynchronously.

Having discussed the improvements made by SPOCS with the ICP, the next chapter continues to present selected details of the SPOCS implementation, inter alia a concrete EDG implementation of the Austrian DDS provided by the author.

Chapter 10

Selected Details of the Implementation

" An idea not coupled with action will never get any bigger than the brain cell it occupied."

[Arnold H. Glasgow, U.S. Psychologist.]

In the course of the LSPs STORK and SPOCS, the presented concepts have been implemented to demonstrate their working principle and their applicability in real environments and under real conditions. STORK demonstrated Level 2 interoperability between the Austrian DDS and the Slovenian Moja.posta.si. The setup was considered as a first prototype to test the concept in a real and operational CMS environment. The main target was to show the basic document exchange of simple documents (for example PDF) for an NRR evidence.

SPOCS has taken up the proved STORK approach and aimed for demonstrating the concept in a larger context with five[1] CMS in an initial phase. In a second phase five[2] further CMS joined the interoperability system. In contrast to the STORK e-Delivery pilot, whose focus is on authentication and identification, CEM is a major pillar in the context of the implementation of the EU Services Directive. Therefore, SPOCS aims for a fully-fledged operational interoperability scenario with a much more sophisticated setup than STORK has realized in its demonstration phase. This includes all phases starting from the message submission to the message translation and delivery phase.

Since both concepts are quite similar (even so from a technical and implementation viewpoint), this chapter discusses only selected details of the SPOCS implementation. The focus of this chapter is first of all on the message translation phase, which represents the core concept of the CMS interoperability framework. Many parts of this phase are common to all gateways, for example, TSL lookups or inter-gateway communication. Therefore, SPOCS has developed a generic gateway integrating all common functionalities. The software architecture of this generic gateway is discussed in detail below in Section 10.1. Nevertheless, it is interesting to know how gateways deal with the message submission phase and message delivery phase. As an example, this thesis presents and discusses in detail the gateway of the Austrian DDS, which has been planned, tested and implemented by the author of this thesis. This chapter further outlines the technical details (programming languages, environments) of both the generic gateway and Austrian gateway.

Even if the theoretical groundwork has been discussed in Chapters 7 and 8, it is important to test its applicability in practice. Section 10.4 discusses the topic of interoperability testing, particularly the SPOCS testing methodology covering unit, integration, system and system integration tests.

Finally, this chapter illustrates how interoperability tests have been conducted and how the system operates in practice.

[1] The CMS are provided by Austria, Germany, Greece, Italy and Poland. More details to these systems are provided later in this chapter.

[2] The CMS from Lithuania, Luxembourg, Romania, Portugal and Slovenia

10.1 Generic Gateway

By having a look at the message translation phase (cf. Section 8.3), several functionalities can be identified, which are common to each EDG instance. These are as follows:

- Determination of routing information
- Messaging-related operations
  - WS-Addressing
  - SOAP communication
  - Metadata retrieval to check preconditions
- Security-related operations
  - TSL checks (SSL server certificate, signature certificate)
  - WS-Security functionality
  - Single evidence signatures
  - Explicit signature of SOAP body

Preliminarily, SPOCS has decided to implement two mechanisms in a different way than has been specified. These are routing and the metadata storage of supported evidences and authentication levels. Routing is based on resolving the recipient's gateway from a DNS subdomain of the CMS e-mail address. The setup of DNS subdomains in all supported address domains requires a certain effort and time. In a first step all routing information is stored within the TSL. For each EDG entry the TSL holds a list of supported CMS address domains. Storing routing information in the TSL is just preliminary, because it has several drawbacks. First, a TSL is just intended to hold trust-related information, not any routing information. Second, TSL is a structured XML container. Storing a couple of supported domains is not a big issue. However, the PEC or De-Mail systems support arbitrary domain names as valid CMS domains. XML parsers will struggle with an XML file containing millions of entries. Third, a central approach is not that scalable and manageable as a decentral one. The number of registered PEC and De-Mail domains is steadily increasing every day. Including all new domains would require a persistent TSL update.

A second mechanism, which is preliminarily implemented in a different way is the metadata storage of supported evidences and authentication levels. The SPOCS design specifies that these metadata is stored in a parallel file of the WSDL file of the concerned gateway. In a first step, SPOCS stores this information along with the list of supported CMS domains in the TSL. This is also the metadata storage approach of STORK.

To ease the take-up of the interoperability concept by single systems, SPOCS WP3 has decided to develop common modules implementing the mentioned common functionalities. The entirety of these common functionalities is called the *Generic Gateway*.

Figure 10.1 illustrates the software architecture of the generic gateway. Briefly outlined, the architecture consists of the following components, which are discussed in detail in the next sections:

- ***ICP handler***. Manages the whole SOAP-based communication based on the ICP protocol.
- ***Security management***. Handles all security-related functions like signatures or authentication tokens.
- ***TSL module***. Is a submodule of the security management part and handles the TSL part.

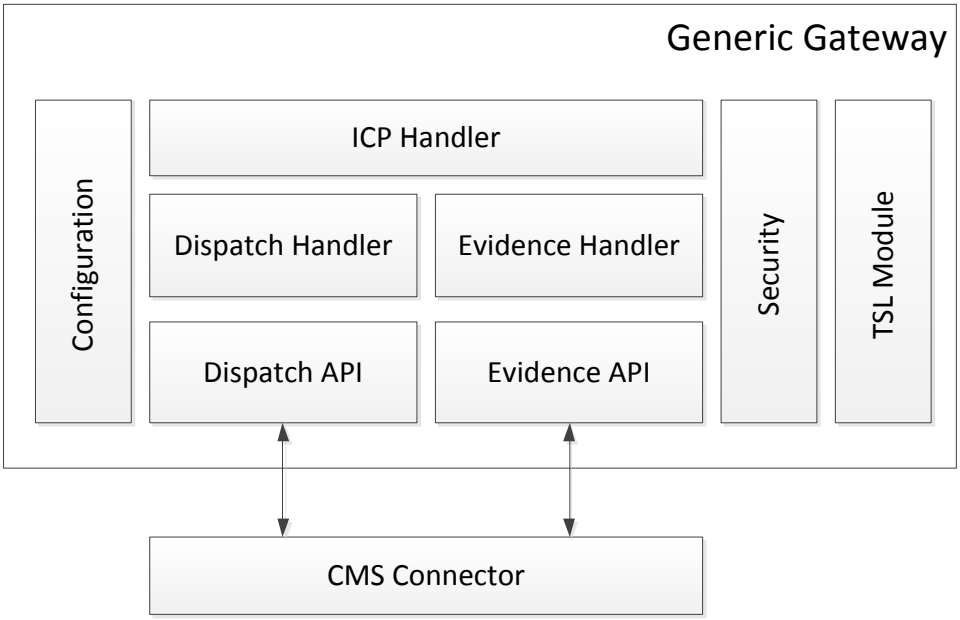

Figure 10.1: SPOCS generic gateway software architecture.

- ***Dispatch handler***. This module is in charge of passing to or receiving an ICP dispatch message from the ICP handler. The dispatch message is passed to or retrieved from the CMS connector through the *Dispatch API*.
- ***Evidence handler***. This module is in charge of passing to or receiving an ICP evidence message from the ICP handler. The evidence message is passed to or retrieved from the CMS connector through the *Evidence API*.
- ***CMS connector***. Represents the interface to the domestic, for example national, CMS.
- ***Configuration***. Provides a flexible way to configure the behavior of the generic gateway.

10.1.1 ICP Handler

The ICP handler is the main processing module to deal with ICP messages. So, first of all, this module provides the main Web services interface for inter-gateway communication. If ICP dispatch or evidence messages are not transmitted over the wire, they are kept within the generic gateway as data objects in order to easily access properties or to perform operations on these data objects. So one major task of the ICP handler is the marshalling (or serialization) of outgoing ICP messages and the unmarshalling (or deserialization) of incoming ICP messages. Incoming XML byte streams are parsed into DOM objects and subsequently unmarshalled into data objects of the used programming language. This enables greater possibilities to access messages in different ways. The same applies to outgoing ICP messages. The ICP handler marshalls the data object into an XML byte stream and transmits it over the wire to the designated EDG.

Another major task of the ICP handler is the message preparation of outgoing messages and the validation of incoming messages. Depending on the message type, outgoing ICP messages are passed in by the so-called *Dispatch Handler* or *Evidence Handler* components. Then the ICP handler resolves the remote gateway by querying the TSL module. If no associated gateway can be found, the message is rejected and returned to the corresponding handler. In a next step, missing parts are automat-

ically generated. This includes the mandatory SubmissionAcceptanceRejection evidence and required WS-Addressing and WS-Security headers. In a last step, the prepared message is passed to the security management part, which signs the single parts with the gateway's certificate. This includes the WS-Security signature over the whole SOAP message, eventually the signature over the whole body as well as the signatures for all single evidences. Finally, the SSL server certificate of the recipient's gateway is checked for genuineness and validity.

Incoming ICP messages are first checked for validity. Therefore, the ICP passes the message to the security management part, which validates all signatures and checks whether the used signature certificate matches the gateway's TSL entry. In a second step, the handler checks the structural correctness of the incoming messages and unmarshalls the message into a DOM and data object. Depending on the message type, this object is then passed either to the dispatch or evidence handler.

Finally, the ICP handler also controls the synchronous and asynchronous mode. In case of the synchronous mode and incoming dispatch messages, a DeliveryNonDeliveryToRecipient evidence is returned, otherwise a RelayToREMMDAcceptanceRejection evidence is returned.

10.1.2 TSL Module

The TSL module provides all means to access trust data within the TSL. It can be initialized with an XML file or XML stream representing the TSL data, for example from a remote URL. When being initialized, the module verifies the signature of the TSL issuer. The TSL XML structure is then unmarshalled into data objects of the used programming language in order to be able to easily access all properties. The module offers a search interface with several functions to search for trusted EDGs on the basis of a CMS address domain, the SSL server or signature certificate or even by country code. If the search was successful, it returns a data object of the trusted EDG service implementation. This object contains the following data:

- Service name of the EDG service.
- Signature certificate.
- SSL server certificate.
- Status of the EDG service.
- Date of registration of the EDG service.
- Web service URL.
- Friendly name of the CMS.
- Supported CMS address schemes.
- Supported CMS e-mail domains.
- Supported authentication levels.
- Supported evidences.
- Requested evidences.

10.1.3 Security Management

Besides the security functions provided through the TSL module implementation, the security management fully relies on integrated and proved functionalities of the used programming language Application Programming Interface (API) and run-time system. This applies to:

- The secure TLS communication management.
- The XML signature creation engine.
- The WS-Security component, which is configured through the WSDL file.

Implementational details are provided below in the technical outline section (cf. Section 10.3).

10.1.4 Dispatch Message Handler

The dispatch message handler represents the "bridge" between the ICP handler and the dispatch handler of a concrete CMS. The handler provides a so-called *Dispatch API*, which operates on data objects and allows a CMS connector to send and receive ICP dispatch messages. Furthermore, the API provides access to the generic gateway configuration as well as the security and TSL modules.

10.1.5 Evidence Message Handler

The evidence message handler represents the "bridge" between the ICP handler and the evidence handler of a concrete CMS. The handler provides a so-called *Evidence API*, which operates on data objects and allows a CMS connector to send and receive ICP evidence messages. The API features extra methods for receiving a DeliveryNonDeliveryToRecipient, RetrievalNonRetrievalByRecipient and AcceptanceRejectionByRecipient evidence. Furthermore, the API provides access to the generic gateway configuration as well as the security and TSL modules.

10.1.6 CMS Connector API

The CMS connector represents the part of a concrete EDG, which implements both the dispatch API and evidence API and thus communicates with the domestic CMS. The used connector can be configured in the configuration of the generic gateway. The generic gateway carries out many of the operations presented and discussed in Chapter 8. However, a large part of a gateway's work is also conducted by the CMS connector. Within the context of SPOCS, the author of this thesis has implemented a connector for the Austrian DDS, which is exemplarily presented in the next section.

10.1.7 Configuration

Since the functionalities of the generic gateway are quite common, only a few parameters have to be configured. The generic gateway configuration is based on XML and allows to define the location of the TSL, the EDG name, the EDG's Web service address (needed for WS-Addressing), the mode (synchronous/asynchronous) and the implementing class of the CMS connector.

10.2 Austrian CMS Connector

The presented generic gateway illustrates how many parts of the message translation phase have been implemented. In order to show how the message submission and message delivery phase as well as the

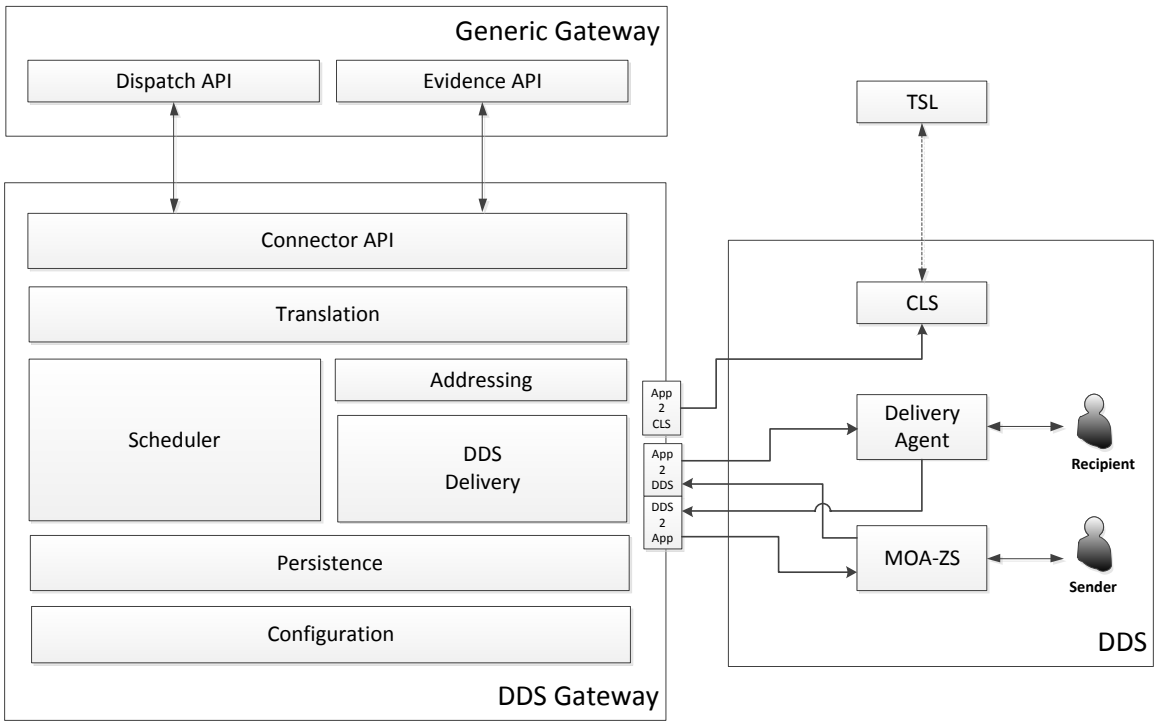

Figure 10.2: Austrian DDS gateway software architecture.

remaining parts of the message translation phase are realized by a concrete EDG implementation, this section exemplarily presents the software architecture and process flows of the Austrian DDS gateway, which has been implemented by the author of this thesis for the SPOCS piloting phase.

Figure 10.2 illustrates the software architecture of the Austrian DDS gateway and its interrelationship with the generic gateway part on the one hand and the Austrian DDS on the other hand. The gateway consists of the following components, which are discussed in more detail in the next sections:

- ***Conncector API***. Implements the dispatch and evidence API of the generic gateway.
- ***Translation module***. Translates the dispatch and evidence messages from the ICP format to the Austrian DDS format and vice versa.
- ***Address resolution module***. Resolves the local Austrian DDS address from the provided virtual CMS address and creates virtual addresses from the local Austrian format.
- ***DDS delivery module***. Handles the delivery and reception of Austrian DDS dispatch and evidence messages.
- ***Scheduler***. Ensures fairness and timeliness by ensuring the punctually evidence delivery according to Austrian laws.
- ***Persistence layer***. Ensures the necessary state storage for a successful delivery process termination.
- ***Configuration***. Allows the individual configuration of all mentioned components.

10.2.1 Connector API

The connector API is the "bridge" on the Austrian side to the generic gateway and implements both the dispatch API and evidence API provided by the generic gateway. This means it handles all necessary communication with the generic gateway part. It basically has only two functions. First, it passes incoming ICP data objects of dispatch and evidence messages to the Austrian translation module. Second, it passes translated outgoing DDS dispatch and evidence messages from the translation module as ICP messages to the generic gateway.

10.2.2 Translation Module

The translation module is the core part for translating ICP dispatch and evidence messages to the Austrian DDS format and vice versa. Depending on the use case, the translation module invokes one of the following four submodules:

- ***DispatchDDS2ICPTranslator***. Translates a DDS dispatch message to an ICP dispatch message.
- ***DispatchICP2DDSTranslator***. Translates an ICP dispatch message to a DDS dispatch message.
- ***EvidenceDDS2ICPTranslator***. Translates a DDS evidence message to an ICP evidence message.
- ***EvidenceICP2DDSTranslator***. Translates an ICP evidence message to a DDS evidence message.

The dispatch translation process is rather straightforward and comprises a set of mappings. First of all, the whole dispatch message is persistently stored by the persistence layer, which is discussed below (cf. Section 10.2.6). This allows to easily associate future occurring evidences with the dispatch message and to retrieve necessary data from the original dispatch message for future translations.

The first part of the translation concerns the identification data of senders and recipients. Demographic data like name, date of birth and postal address are directly mapped since both the ICP and the DDS protocol have a similar XML structure for this part. A more complex part is the mapping between Austrian virtual CMS addresses in the ICP format and the address data in the DDS format. This part of the translation is carried out by the addressing module, which is discussed in detail in the next section.

A second part of the translation concerns the mapping of metadata. To avoid the collisions of message IDs, a conversion between both formats is carried out. For each dispatch message, be it an ICP or DDS message, a new message ID is created in the translated format. ICP message IDs are generated with a secure random algorithm, have a long prefix and end with the Austrian CMS domain.

ICP message ID example: `RWAALS3RAM.5651899266@zustellung.gv.at`

Another metadata part is the informal text. Both the ICP and the DDS support the two informational text types "plain text" and "HTML". This text can be mapped directly. The conversion of message attachments is also a simple mapping between the ICP MTOM and the DDS SwA formats.

Regarding the semantic translation part, the Austrian gateway has a fixed mapping table for authentication levels and evidences. Austrian senders of dispatch messages always have to authenticate with SSL client authentication. This corresponds to the ICP authentication level "Strong". Austrian recipients either authenticate with their citizen card ("QES") or with a software certificate through their Web browser or e-mail client, which corresponds to the "Strong" level. The gateway supports all (foreign) sender authentication levels of incoming ICP dispatch messages.

The Austrian DDS supports only an NRR evidence. This evidence is generated as soon as the recipient authenticates at the MS of the delivery agent by signing the evidence with the citizen card. If the recipient logs in with an SSL certificate, the NRR evidence is generated by the delivery agent on behalf of the recipient. Therefore, the gateway classifies the NRR evidence as ICP AcceptanceRejectionByRecipient and RetrievalNonRetrievalByRecipient evidences. When a dispatch message is delivered to an

Austrian recipient, the DDS SOAP protocol provides only an XML acknowledgment message to the sender. This is a non-transferable evidence, but the gateway maps it to the ICP DeliveryNonDelivery-ToRecipient evidence.

Evidence messages are translated in a similar way than dispatch messages. Besides mapping the sender's and recipient's address and identification data, message IDs and evidence types, in case of negative evidences the corresponding error code and error info text are also mapped. The detailed handling of evidences is explained in more detail below when discussing the process flow of the Austrian gateway (cf. Section 10.2.8).

10.2.3 Address Resolution Module

The Austrian DDS has no addressing scheme based on unique e-mail addresses like PEC, De-Mail or Moja.posta.si. Since SPOCS uses by default the e-mail addressing scheme, the Austrian gateway has to provide a mapping between the ICP e-mail addressing scheme and the Austrian addressing schemes (cf. Section 9.1). Austrian senders and recipients can be addressed according to the following schemes:

- ***Demographic data - natural person***. This includes the recipient's given name, family name and notification e-mail address. The notification address is not a unique system address, but just serves to inform the recipient that a new message has been delivered and is ready for retrieval. Multiple persons may share the same notification address.
- ***Demographic data - legal person***. This includes the recipient's name, for example company number, and notification address.
- ***Recipient's ssPIN***. This is the ssPIN for CEM in case of natural persons and the register number in case of legal persons, for example the company number.

To achieve a virtual CMS address, a simple approach has been chosen to wrap the mentioned identification data into the e-mail address format. All used identification parameters are concatenated and form the local part of the virtual e-mail address. As domain "zustellung.gv.at" has been chosen. As delimiter for the identification parameters the "+" sign is used. Examples of virtual address mappings are:

- John;Doe;john@doe.com leads to
  - `John+Doe.john.at.doe.com@zustellung.gv.at`
- Company name;info@company.com leads to
  - `CompanyName.info.at.company.com@zustellung.gv.at`
- Company number leads to
  - `CompanyNumber+FN@zustellung.gv.at`

By using this mechanism, both the ICP and DDS addressing formats for Austrian users can be easily mapped to each other. In contrast to the publicly known company number, a recipient's ssPIN cannot be used abroad and thus not be directly embedded into a virtual CMS address. For this purpose another mechanism has been implemented, which provides a useful feature and better convenience for Austrian users. Users can register with their citizen card a virtual CMS consisting of their name, which is then mapped to their ssPIN. For example, the user John Doe can register the new address `John.Doe@zustellung.gv.at` at the gateway. This kind of address is way easier to remember for users than the "composed" one and they can even put this address easily on their business cards. This address is unique for each user and cannot be changed in order to avoid abuse in case a user deregisters

an address. To ensure uniqueness, an additional number is added to the local part of the address in case of users with the same name. For example, if a second user with the name John Doe registers, the address `John.Doe.1@zustellung.gv.at` is assigned to the user.

10.2.4 DDS Delivery Module

The DDS delivery module is the core gateway component handling all communications with the Austrian DDS. It implements the necessary functionality from the following two viewpoints:

1. ***Sending unit***. As a sending unit it delivers translated incoming ICP dispatch and evidence messages to Austrian recipients.
2. ***Receiving unit***. As a receiving unit it takes in charge outgoing DDS dispatch and evidence messages from Austrian senders and delivery agents.

As a sending unit the gateway handles translated incoming ICP dispatch and evidence messages. Dispatch messages have to be delivered to the designated Austrian recipient. Evidence messages have to be delivered to the original Austrian sender. For this purpose, the gateway mimics either an Austrian sender or a delivery agent. In case of an ICP dispatch message, which has been converted by the translation module into a DDS dispatch message, the gateway mimics an Austrian sender. This requires the gateway to have registered its SSL client certificate at the CLS. This has to be done only once. With the resolved Austrian address (from the address resolution module), the delivery module first queries the CLS to determine the delivery agent the recipient is registered with. Therefore, the gateway implements the App2CLS [Tauber and Rössler, 2010a] client API. If the recipient's Web service address could be successfully determined, the gateway delivers the dispatch message to the delivery agent with an integrated App2DDS [Rössler and Tauber, 2010a] client. The procedure for an incoming ICP evidence is pretty similar. Instead of querying the CLS for the recipient's delivery agent address, the gateway retrieves the persisted original DDS dispatch message, reads out the Austrian sender's notification address and forwards the translated DDS evidence to the sender. This notification address can either be a traditional e-mail address or a Web service for automated processing by applications. In the latter case the delivery module mimics the delivery agent of the foreign recipient and uses the integrated DDS2App [Rössler and Tauber, 2010a] server API to forward the evidence to the Austrian sender.

The use case of outgoing DDS messages to a different CMS was more difficult. In this case, the gateway represents the Austrian delivery agent serving all foreign recipients. The tricky part was to make all foreign recipients look like Austrian recipients. Austrian senders first query the CLS and deliver the message to the delivery agent returned in the CLS response. For transparency purposes, this behavior cannot be changed. Therefore, the idea was to make the gateway a standard delivery agent, which is registered together with all other delivery agents in the list of the CLS. The CLS itself has been enhanced to deal with foreign recipients. By integrating the TSL functionality to search by means of a foreign address, the CLS hosts a virtual directory of all foreign recipients. For example, if an Austrian sender queries the CLS with the search parameters givenName=John,surName=Doe,mail=john.doe@moja.posta.si, the CLS can check whether the given e-mail address is a foreign CMS by looking into the TSL. If a match is found in the TSL, the CLS returns the gateway as delivery agent in its answer. The Austrian sender can then deliver the dispatch message to the gateway in the usual manner. For this purpose, the gateway implements the App2DDS server API. If a an Austrian recipient retrieves a message, an NRR evidence is returned to the sender. If the dispatch has been sent by the gateway on behalf of a foreign sender, then the corresponding delivery agent sends the NRR evidence to the integrated DDS2App server API of the gateway.

Summarizing, the DDS delivery module implements the following interfaces:

- ***App2CLS client API*** to query the CLS when delivering a dispatch to an Austrian recipient.

- ***App2DDS client API*** to deliver a dispatch message to an Austrian recipient's delivery agent on behalf of a foreign sender.
- ***App2DDS server API*** to receive a DDS dispatch message from an Austrian sender for a foreign recipient.
- ***DDS2App client API*** to deliver an evidence message to an Austrian sender on behalf of the recipient's CMS.
- ***DDS2App server API*** to receive a DDS evidence message from an Austrian delivery agent for a foreign sender.

10.2.5 Scheduler

The scheduler has the primary tasks of ensuring timeliness and fairness. Timeliness must be ensured for both incoming ICP messages as well as outgoing DDS messages. Austrian law states that if a recipient does not retrieve a message within 7 days, a negative NRR must be returned by the concerned delivery agent to the sender. The same must hold in case of foreign recipients. Therefore, the Austrian gateway monitors whether an incoming ICP evidence message (equal to NRR evidence) has been received for a sent DDS dispatch message. If no evidence message has been received for 7 days, the gateway automatically generates a negative NRR evidence in the DDS format on behalf of the recipient's CMS and forwards it to the Austrian sender.

In case of incoming ICP dispatch messages foreign senders may define a message expiration date (cf. "ObsoleteAfter" element explained in Section 9.4). In this case the gateway monitors whether the Austrian recipient retrieves the message within this time interval. If the deadline expires the gateway automatically creates ICP AcceptanceRejectionByRecipient and RetrievalNonRetrievalByRecipient evidences on behalf of the Austrian recipient's delivery agent. In this way the gateway ensures timeliness for both incoming and outgoing dispatch messages.

The scheduler ensures fairness for the Austrian DDS by simple checking whether the foreign CMS supports an AcceptanceRejectionByRecipient or a RetrievalNonRetrievalByRecipient evidence. If this is the case, the gateway waits for one of these evidences, at least for the 7 days mentioned above (to ensure timeliness). If the foreign CMS does not support one of these evidences, the gateway interprets the DeliveryNonDeliveryToRecipient evidence, which is compulsory in each system, as NRR evidence.

10.2.6 Persistence Layer

The persistence layer is in charge of storing any required data of the other modules. This ranges from small data like message IDs to large data comprising whole dispatch messages. The persistence layer uses a object-relational mapping mechanism to store and access objects in the underlying database as data object model, for example to simply store and retrieve ICP and DDS messages as data objects. Implementational details are provided below in the technical outline section (cf. Section 10.3).

10.2.7 Configuration

The configuration module allows to configure all single parts of the Austrian gateway, except those parts concerning the generic gateway, which have to be configured in an extra file. Due to its abstract design, different configuration implementations can be used. The default configuration is provided through a text-based properties file, but each other format like XML can be integrated as well. Basically, the following properties can be configured:

- The addressing module, including:

  - The domain part of the Austrian virtual address (default = zustellung.gv.at).
  - A list of resolvers for Austrian virtual addresses, including by default:
    * *DynamicAddressResolver* resolving addresses of concatenated identification data.
    * *StaticAddressResolver* resolving fixed registered CMS addresses.

- The DDS delivery module, including:
  - The App2CLS client
  - The App2DDS client and server
  - The DDS2App client and server
- Time intervals for the monitoring part of the scheduler
- Access to the underlying database by the persistence layer

10.2.8 Process Flow

In the preceding sections the software architecture of the Austrian gateway implementation has been presented in detail. Even if some procedural parts have already been explained during the discussion of some of the modules, this section aims to provide a clearer overview of the gateway's process model. The process flows of outgoing DDS messages are the same as discussed when introducing the Austrian DDS (cf. Section 4.2.1). Therefore, this section focuses on incoming ICP messages and discusses the process models for both dispatch and evidence messages. The description does not cover any internal processes, for example the translation or addressing parts of the gateway, but just outlines the interrelationships between the different actors.

Incoming ICP Dispatch Message

Figure 10.3 illustrates the Unified Modeling Language (UML) sequence diagram of an incoming ICP dispatch message. The following actors are involved:

- The foreign sender's EDG
- The Austrian EDG
- The recipient's delivery agent
- The recipient

To simplify the illustration of the process, the CLS is not explicitly shown. The dispatch message process can be separated in a delivery phase and a retrieval phase.

- ***Delivery phase***. After having processed the incoming ICP dispatch message, the Austrian gateway queries the CLS and sends the translated DDS dispatch to the recipient's delivery agent. The delivery agent acknowledges the reception or rejection of the message with a corresponding SOAP message and notifies the recipient that a new message is ready to be retrieved. The gateway immediately translates the acknowledgement into a DeliveryNonDeliveryToRecipient evidence, which is returned to the sender's gateway. If the message delivery was successful, the Austrian gateway stores the ICP dispatch message using the persistence layer.

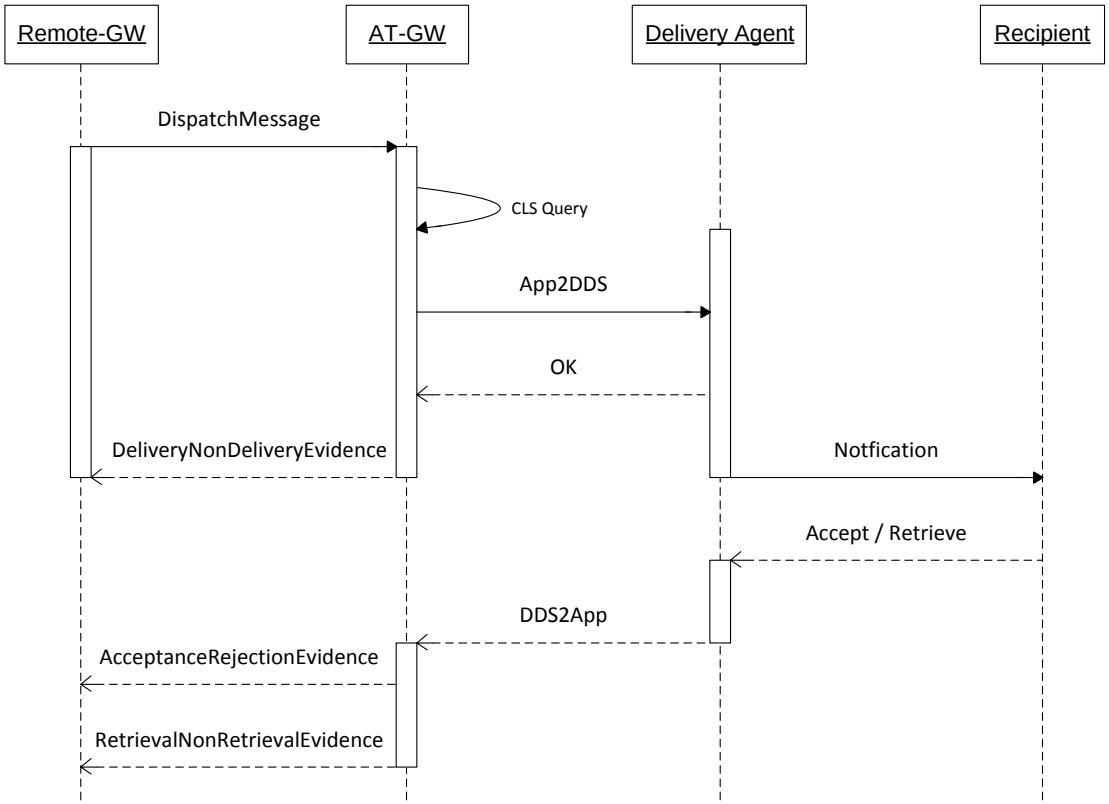

Figure 10.3: DDS gateway - incoming ICP dispatch message.

- ***Retrieval phase***. As soon as the recipient signs an NRR evidence upon retrieving the message, the delivery agent forwards the NRR evidence to the dispatch sender, in this case the Austrian gateway. The gateway retrieves the stored ICP dispatch message through the persistence layer and creates a RetrievalNonRetrievalByRecipient and AcceptanceRejectionByRecipient evidence based on the contents of the stored ICP dispatch message and the received DDS NRR evidence. If supported by the sender's CMS, both evidences are sent consecutively to the foreign sender's gateway.

Incoming ICP Evidence Message

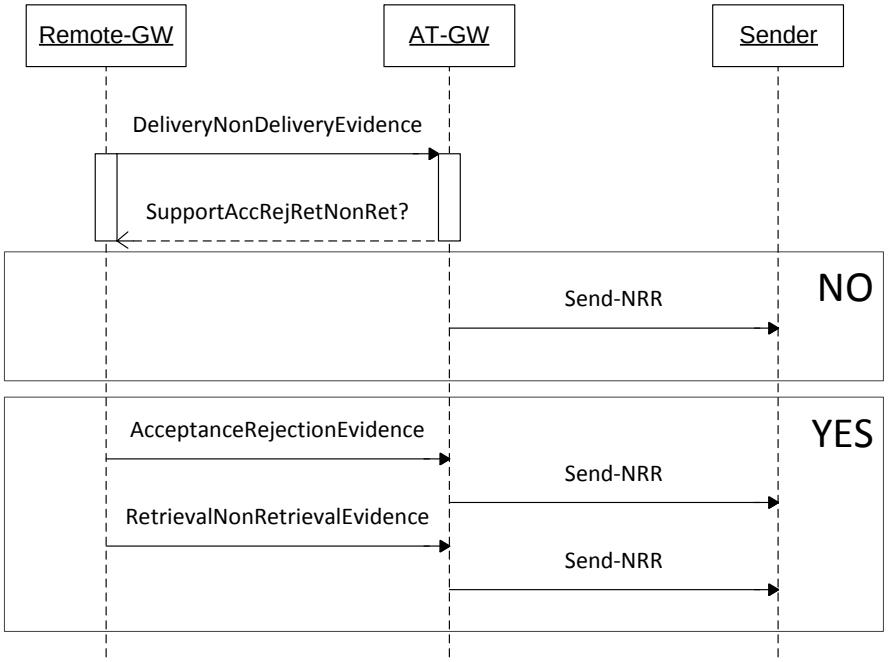

Figure 10.4: DDS gateway - incoming ICP evidence message.

Figure 10.4 illustrates the UML sequence diagram of an incoming ICP evidence message. The following actors are involved:

- The foreign sender's EDG
- The Austrian EDG
- The sender

The process of incoming ICP evidence messages has already been outlined when having introduced the scheduler module (cf. Section 10.2.5). Apart from the RelayToREMMDAcceptanceRejection evidence, which is the first evidence in asynchronous mode, the first evidence attesting the delivery status is an incoming DeliveryNonDeliveryToRecipient evidence. In this case the scheduler part checks whether the foreign recipient's CMS supports either a RetrievalNonRetrievalByRecipient or AcceptanceRejectionByRecipient evidence (both can be considered as NRR evidence). If none of these evidences can be

provided, the Austrian gateway treats the DeliveryNonDeliveryToRecipient evidence as NRR evidence, retrieves the original corresponding DDS dispatch through the persistence layer, creates and signs a DDS NRR evidence on behalf of the foreign recipient and forwards the evidence to the Austrian sender. If an AcceptanceRejectionByRecipient or RetrievalNonRetrievalByRecipient evidence is supported by the foreign CMS, the Austrian gateway waits for such an incoming evidence and creates a DDS NRR evidence in the same way as for an incoming DeliveryNonDeliveryToRecipient evidence. As already mentioned, the gateway waits at most for 7 days, then a negative NRR evidence is automatically generated and forwarded to the Austrian sender.

10.3 Technical Outline

It has already been stated in the requirements chapter that the use of open specifications and open source software is a major requirement to enable a widespread and large-scale take-up by implementers and to foster the sustainability of the whole framework. This section describes the chosen software technologies of both the SPOCS generic gateway and the Austrian DDS gateway developed in the course of the SPOCS project. The gateway component developed for the STORK project uses the same technologies. Therefore, this section focuses just on the SPOCS gateway.

The choice was made to use Java[3] as the main programming language, for both the generic gateway part as well as for all parts of the Austrian DDS gateway. Even if Java is somewhat slower than programs compiled to native machine language, Java byte code programs have several benefits. First, they run on multiple platforms. Java programs have to be compiled only once and run anywhere, at least on those platforms for which a Java Runtime environment is provided. Furthermore, Java runs in a secure environment (kind of sandbox) and, if configured correctly, Java programs cannot harm the host system with a virus, Trojan horse or similar malware. Finally, Java has a built-in support for a large number of additional functionalities including the Java Cryptography Architecture (JCA) and Java Cryptography Extension (JCE), the Java XML Digital Signature API, the Java API for XML Binding (JAX-B), the Java API for XML Web Services (JAX-WS) and many many more. Non-included functionalities are provided by thousands of Java open source libraries out there on the Web. Moreover, the Java Enterprise Edition (EE) provides a solid platform for the development and deployment of transaction-based Web services in a scalable and interoperable environment.

To summarize, these are the software characteristics of the generic gateway part:

- Java Software Development Kit (SDK) Version 1.6.0
- Java Servlet 2.5 Specification
- Java JCE
  - Bouncycastle[4] Version 1.4.0 provider overriding the SDK's internal JCE implementation
- Java XML Digital Signature API (included in SDK)
- Java JAX-B API
- Java JAX-WS API
  - Java Metro[5] overriding the SDK's internal JAX-WS implementation

[3] The Java programming language, an Oracle technology, see `http://java.oracle.com`
[4] The Legion of the Bouncycastle, see `http://www.bouncycastle.org`
[5] `http://metro.java.net`

The software of the generic gateway is licensed under the EUPL[6] and is going to be published on the Open Source Observatory and Repository (OSOR)[7] platform by the SPOCS consortium.

The software characteristics of the Austrian gateway part are as follows:

- Java SDK Version 1.6.0
- Java Servlet 2.5 Specification
- Java JCE
  - Bouncycastle Version 1.4.0 provider overriding the SDK's internal JCE implementation
- Java JAX-B API
- Java JAX-WS API
  - Java Metro overriding the SDK's internal JAX-WS implementation
- Austrian Java-based open source modules Modules for Online Applications - Signature Creation (MOA-SS) and Modules for Online Applications - Signature Verification (MOA-SP)[8] Version 1.5.0 to create and validate XAdES and XML QES in the context of the Austrian DDS.
- Apache HTTP Client Version 4.0.3 (CLS client communication)
- Apache Struts Version 1.3.5 for the GUI part where users can register a CMS address with their citizen card.
- Hibernate Version 3.2.5 as persistence layer
  - MySQL Version 5.0 as underlying database
- Apache Tomcat Version 6.0 as Servlet Container

10.4 Interoperability Tests

Testing is a continuous process in the Software Engineering (SE) life-cycle and is vital to verify that specifications are correctly delivered and that functional and implementation requirements are met. First of all, this concerns the generic gateway part, which is the core of each CMS connector and handles many parts of the translation phase. The correct functionality of the interoperability concept depends on this core component and is thus particularly crucial, since potential errors would occur in all CMS connectors relying on this basic implementation. Second, each CMS connector must be tested by each implementer for correct interoperation with the generic gateway. This part of testing can partly be generalized for all implementers, but CMS-specific testing parts have to be customized per system. Last not least, the interoperation of different CMS connector implementations has to be tested. Even if previous tests can be tested automatically to a great extent, these kind of interoperability tests also require at least some user interaction, for example the retrieval of messages to trigger the generation of a RetrievalNonRetrieval-ByRecipient or AcceptanceRejectionByRecipient evidence. The focus is clearly on functional testing, this means the SPOCS test framework aims to test specific functionalities whether based on user input or not. Nevertheless, non-functional testing like quality of code is particularly crucial for the generic gateway part.

In order to cover all mentioned testing aspects, SPOCS has defined a four-tier testing strategy for its SE life-cycle (cf. Figure 10.5), which are defined as follows:

[6] http://www.osor.eu/eupl
[7] http://www.osor.eu
[8] http://egovlabs.gv.at/projects/moa-idspss/

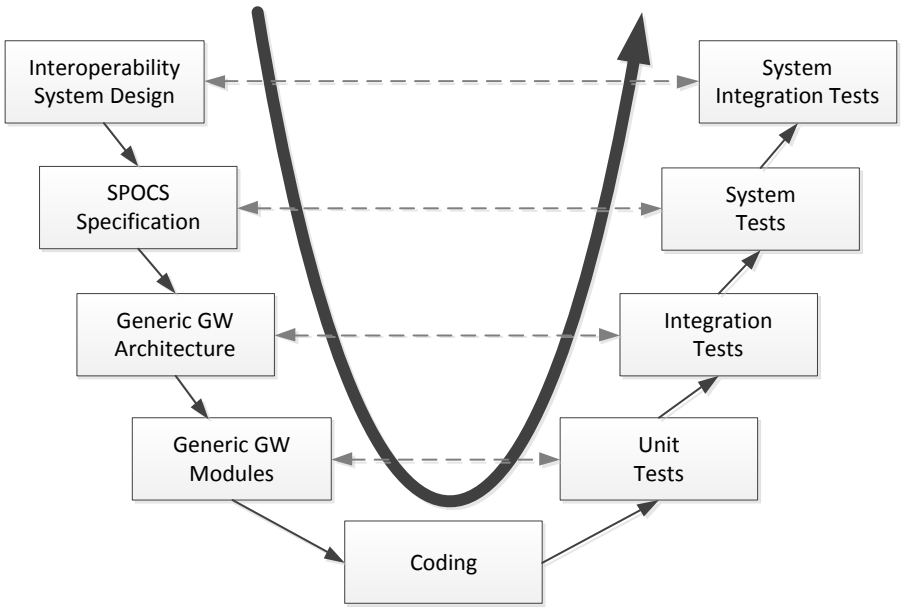

Figure 10.5: SPOCS software testing lifecycle.

1. On the lowest level unit tests for modules and software parts ensure the correct implementation and functionality of single parts of the generic gateway.

2. Integration tests validate the correct interaction of the modules and software parts of the generic gateway and test the correct functionality of the generic gateway architecture as a whole.

3. With system tests, implementers can validate and check the correct operation of a single CMS connector based on the generic gateway whether it fulfills the SPOCS specifications or not.

4. On the highest level, system integration tests validate the correct interoperation of single CMS connectors on a larger scale and in a more complex environment.

The four test tiers are subsequently discussed in the next sections.

10.4.1 Unit tests

The generic gateway is made up of a number of single software parts. This includes the ICP Handler, the TSL Module, the Security Management as well as the Dispatch and Evidence Handlers. All of these components of the generic gateway are verified through unit tests to verify the basic functionalities of ICP signature creation, signature verification, TSL handling, XML schema compliance, message integrity, etc. Unit tests are simple and basic functionality tests and do not cover any interactions between different units. In contrast to "black box" testing, which only tests the output on the basis of a certain input, this testing approach is called "white box" testing, because it targets on particular APIs or parts of the code. Unit tests of the generic gateway part are conducted before each release cycle on an integration server[9]. SPOCS only covers unit tests for the generic gateway. However, each one implementing a CMS connector is advised to follow the same testing methodology and to conduct unit tests for the concrete CMS connector implementation.

[9]The SPOCS team in charge of implementing the generic gateway uses the Hudson integration server for this purpose, see `http://java.net/projects/hudson/`

10.4.2 Integration tests

Unit tests only cover the functionality of single software components. This means, that, for example, the functionality of the TSL module and the security management part are tested independently. Integration tests aim to validate cross-unit functionalities, for example the signature verification process, which accesses the TSL module to validate the genuineness of the signature certificate. Another example is the validation of the correct communication between the ICP handler and the corresponding dispatch and evidence handlers. Due to the focus on testing particular interfaces between the single gateway components, integration tests can also be classified as "white box" tests. Testing whether a certain CMS connector implementation meets the specified requirements and complies with the interfaces given by the generic gateway, is also considered as integration testing.

10.4.3 System tests

System tests verify the integration of the generic gateway part into a particular CMS in its entirety; this means they help developers to verify the correct functionality and the correct behavior when implementing a particular CMS connector. For this purpose, SPOCS has set up a reference implementation of a CMS based on the generic gateway. This reference implementation operates a running CMS connector having a deterministic behavior. When conducting system tests for a CMS connector, the implemented gateway can send arbitrary ICP requests to the reference implementation and control the resulting ICP response messages. The behavior of the reference implementation can be controlled with particular keywords in the metadata of the ICP request. In this way, developers can test the handling of the following functions:

- ***Message mirroring***. By setting a particular flag, ICP dispatch or evidence messages sent by a CMS connector can be mirrored by the reference implementation. During the mirroring process, the sender and recipient of a message are interchanged. In this way, implementers can test whether their sent messages are correctly parsed and syntactically correct. Subsequently the CMS connector can be tested whether it can correctly parse and understand the mirrored message.
- ***Evidence sequences***. If dispatch and evidence messages can be correctly handled, in a second step, the correctness of a CMS connector's process flow must be tested. Adding particular keywords to the message forces the reference implementation to generate certain evidences as response to the request. For example, if a CMS expects first a mandatory DeliveryNonDeliveryToRecipient and thereafter an optional AcceptanceRejectionByRecipient or RetrievalNonRetrievalByRecipient evidence, this behavior can easily be mimicked by the reference implementation.

Like unit or integration tests, system tests can also be classified as "white box" tests, because the behavior of the reference implementation is deterministic and known and thus the difference to unit and integrations tests is quite small.

10.4.4 System integration tests

System integration tests are often called plug-tests and their aim is to test the cross-CMS interoperability. This task bears more challenges than unit, integration or system testing. By connecting different CMS, dynamic process flows arise by coupling processes of different CMS. For the reference implementation, evidences are created upon request of the tested CMS connector. With system integration tests, "real" systems are connected and processes depend on several factors, which also include actions and decisions made by people, for example recipients. Figure 10.6 illustrates this complexity with an UML activity diagram of a plug-test where a fictive CMS receives an ICP dispatch message. This diagram could also be replaced with a corresponding decision graph. Depending on the content of the incoming message or

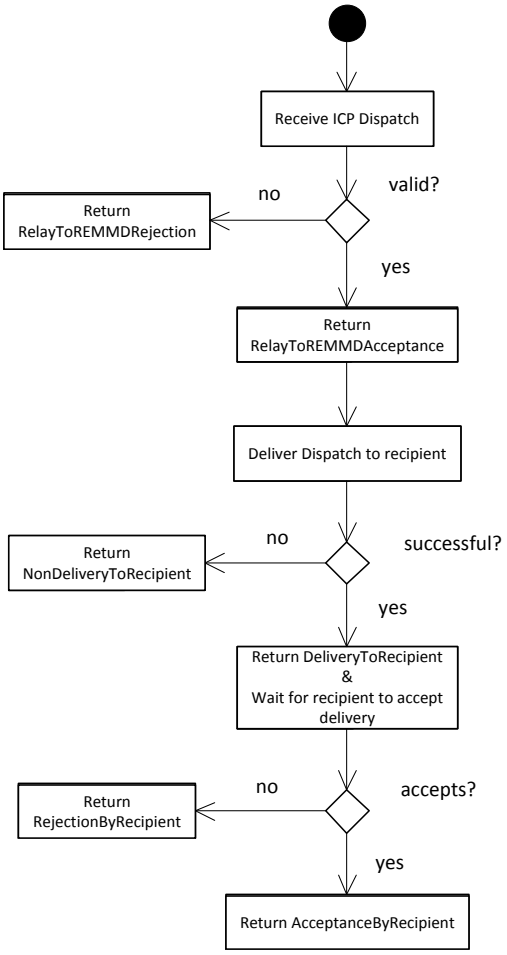

Figure 10.6: Process flow of a fictive CMS.

CMS policies and user interactions, particular evidences are produced and returned at different points in time.

For this purpose, SPOCS has decided to organize so-called plug-tests, where national development teams can test their CMS connectors for interoperability. Plug-tests are based on a test-bed with well-defined test cases, where different teams test their system in an iterative process (trial & error) for interoperability. The plug-tests should also help to identify errors and shortcomings of the SPOCS specifications, which were iteratively refined in this process. Test results have been captured in a final test report. Systems can only be put operational if all tests have been passed successfully.

All plug-tests between CMS participating in SPOCS have been completed successfully and the specification has iteratively been refined being now in its final shape.

10.5 Framework in Operation

Besides the Austrian DDS, the following CMS or messaging systems are participating in SPOCS:

- The German EGVP (cf. Section 4.2.6.4)
- The Italian PEC (cf. Section 4.2.2)

- The Slovenian Moja.posta.si (cf. Section 4.2.4)
- Polish ePUAP. The Austrian, German, Italian and Slovenian CMS are standalone systems with the sole purpose of providing certified mail services. Poland has no such dedicated infrastructure. However, it provides a citizen portal called ePUAP[10] with integrated messaging functionality providing a mailbox for registered citizens.
- The Greek pendant to the Polish citizen portal ePUAP is called ERMIS (Hermes)[11]. It also has an integrated messaging functionality providing a mailbox for registered citizens.
- Portugal provides a messaging platform called iAP[12] to communicate with the public sector.

Even if not all participating systems are real CMS providing transferable non-repudiation services, gateways can mask standard messaging systems and make them appear as CMS. For example, if the messaging systems operate on SOAP acknowledgments, the gateway can create evidences on the basis of these acknowledgments.

To illustrate the working SPOCS CMS interoperability framework in practice, the following screenshots show the submission of a message from the German EGVP to the Austrian DDS and vice versa. The screenshots clearly highlight and demonstrate the environments of end entities, this means sender and recipient. The remaining part is carried out on the transport layer and thus not directly visible.

[10] ePUAP = Electronic Platform of Public Administration Services, see http://epuap.gov.pl
[11] http://www.ermis.gov.gr
[12] http://www.iap.gov.pt

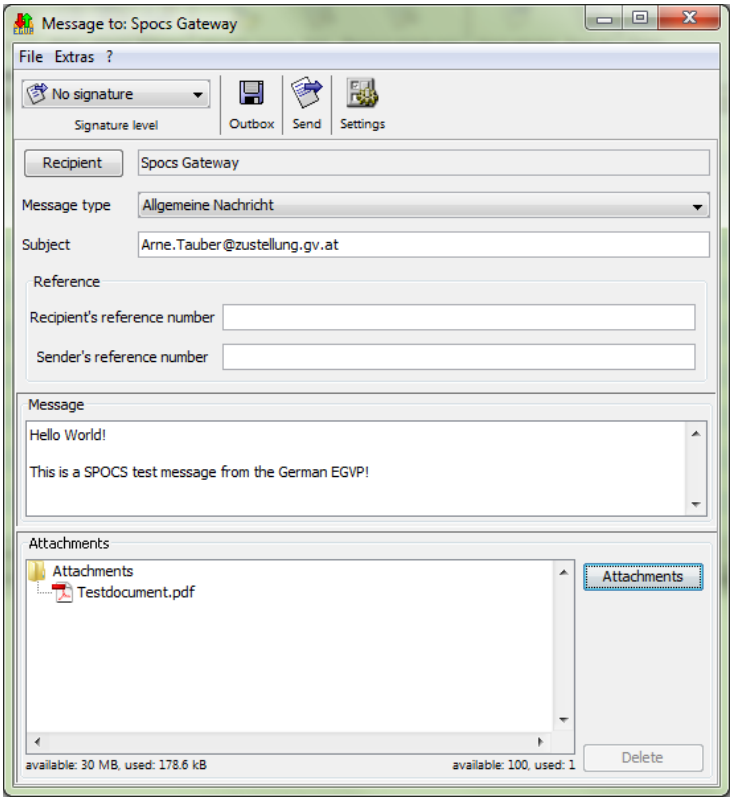

Figure 10.7: Message submission with a standard EGVP client to an Austrian recipient.

Figure 10.7 illustrates a sender's mask of the German EGVP. All messages sent to foreign recipients have to be addressed to the EGVP's "SPOCS Gateway". The actual recipient address, in this case `Arne.Tauber@zustellung.gv.at`, has to be entered in the "Subject" field. The sender can define an informational text ("Message" field) and attach an arbitrary number of files ("Attachments" part). By clicking on the "Send" button, the message is submitted to the EGVP's SPOCS gateway.

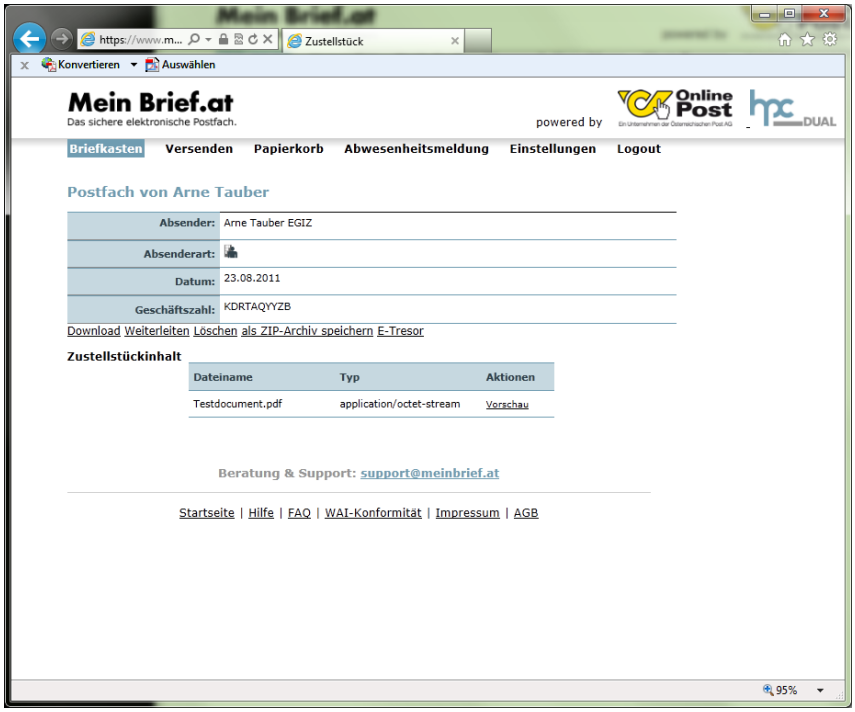

Figure 10.8: Received message from EGVP in the Austrian DDS Web client.

Figure 10.8 illustrates the details of the received message at the Web GUI of the Austrian delivery agent Meinbrief. Besides the sender's name ("Arne Tauber EGIZ"), the sending timestamp ("23.08.2011") and the message ID ("KDRTAQYYZB"), all message attachements are displayed. In this case a PDF test document ("Testdocument.pdf").

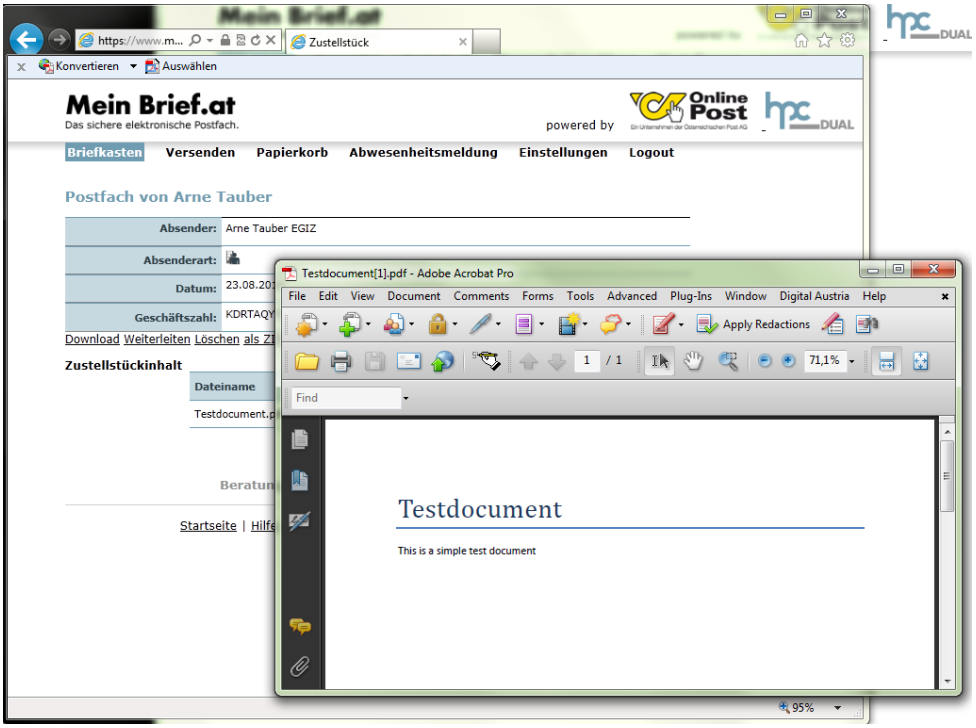

Figure 10.9: Details of a received message from EGVP in the Austrian DDS Web client.

Figure 10.9 shows the attached PDF document.

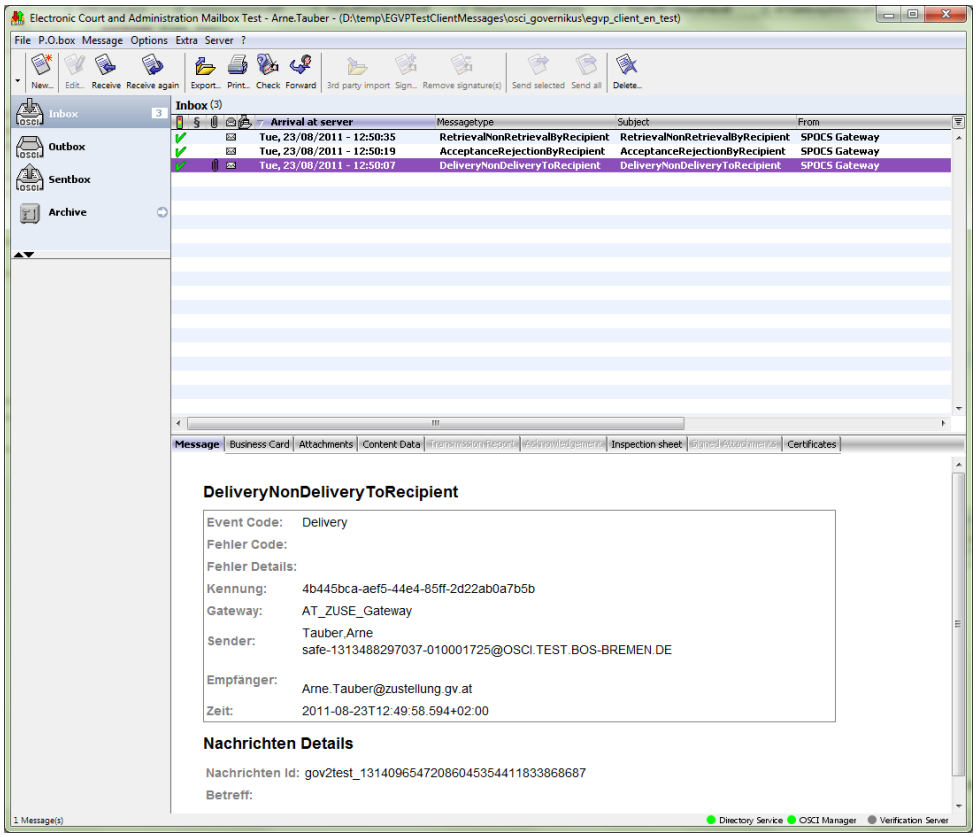

Figure 10.10: Evidences from the Austrian DDS shown in EGVP client.

After having read the message, the Austrian delivery provider returns a NRR evidence back to the Austrian gateway, which forwards a RetrievalNonRetrievalByRecipient and a AcceptanceRejectionByRecipient evidence to the EGVP's gateway. Figure 10.10 illustrates the sender's EGVP mailbox with the three related evidences. The first is a DeliveryNonDeliveryToRecipient evidence, sent back synchronously by the Austrian gateway when having delivered the dispatch message. The other two evidences have been received after the Austrian recipient has accepted and read the message.

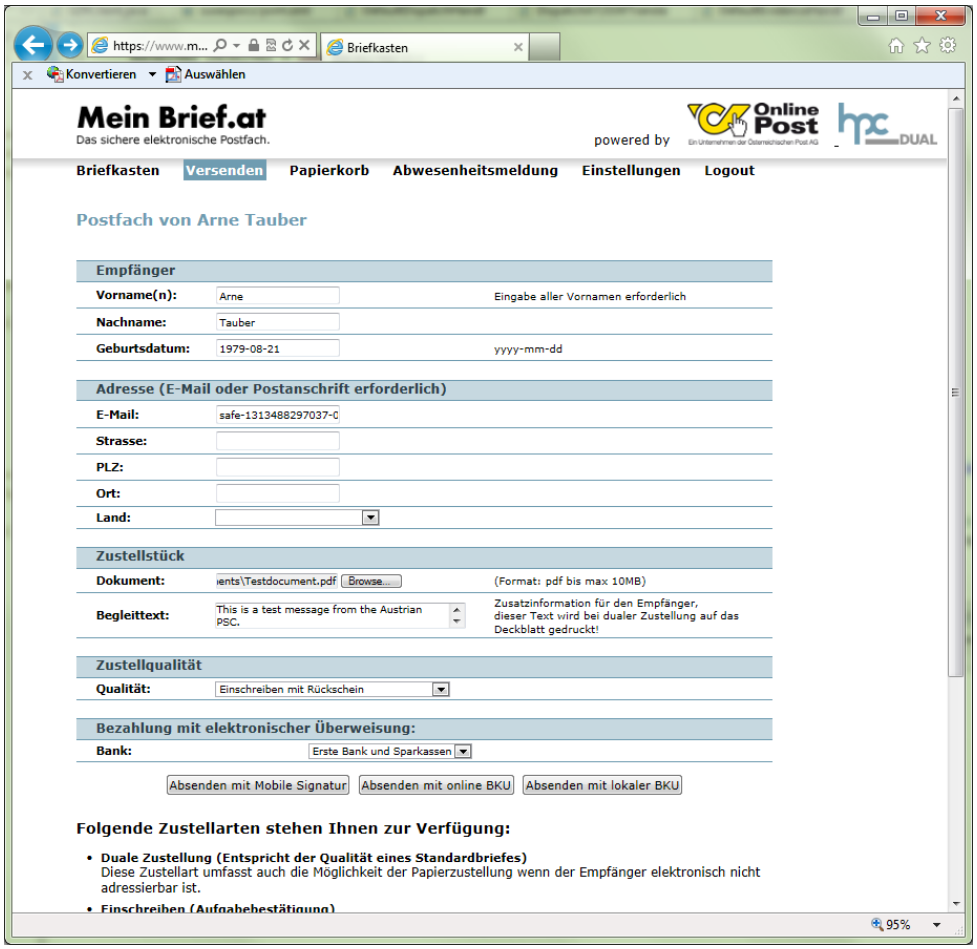

Figure 10.11: Message submission from the Austrian DDS Web client to an EGVP recipient.

Figure 10.11 illustrates the other way around. Austrian senders can use the Web GUI of the delivery agent Meinbrief.at to deliver messages to foreign recipients. Basically, only the e-mail address field is mandatory. Given name ("Vorname(n)"), family name ("Nachname") and date of birth ("Geburtsdatum") are optional elements. The GUI allows one attachment up to 10 MB ("Dokument") and to define an informational text ("Begleittext"). The are three send buttons to choose from. Each button denotes a different citizen card type to sign and initiate the message delivery to the German EGVP.

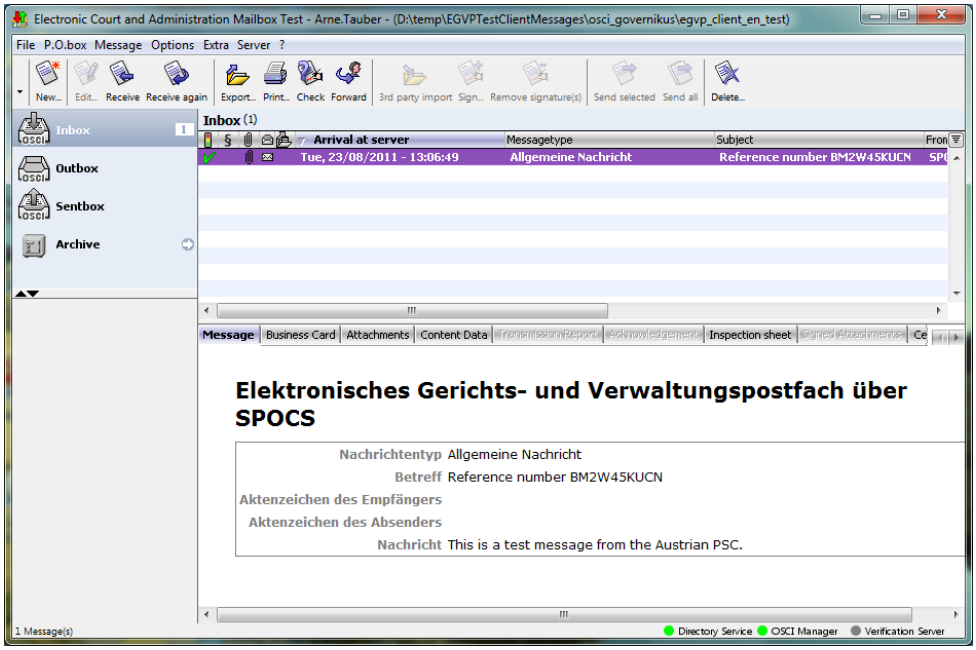

Figure 10.12: Received message from the Austrian DDS shown in the EGVP client.

Figure 10.12 illustrates the dispatch message as it has been received by the EGVP recipient. The informational text is shown as "Nachricht" at the bottom. By clicking on the "Attachments" tab, the sent PDF test document becomes available (not shown in figure).

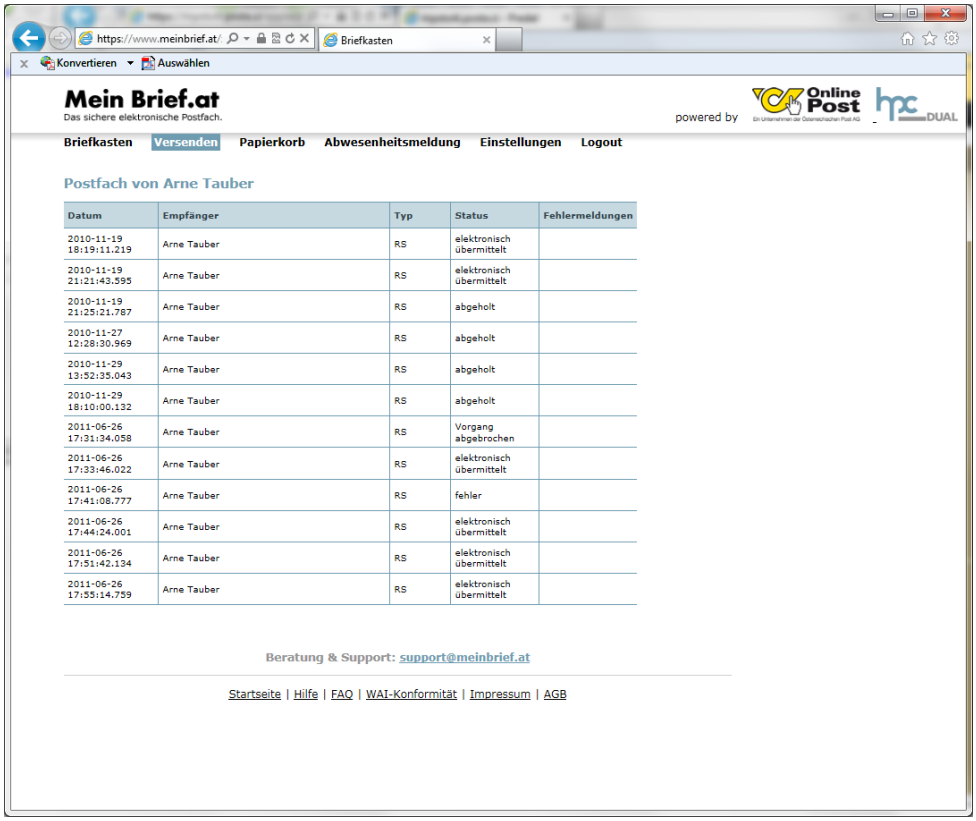

Figure 10.13: Status of sent messages shown in the Austrian DDS Web client.

After the recipient has read the message, an evidence is sent back to the Austrian sender. Figure 10.13 shows the delivery status of all messages. "abgeholt" denotes a successfully received NRR evidence.

Chapter 11

Interoperability Level 1

> *"This lets operators roll out national or international systems that use the same authentication they already have in place."*
>
> [Bert Williams, Entertainer, 1874–1922.]

This chapter discusses the concept of Level 1 interoperability, this means the authentication of foreign users at (national) CMS portals or infrastructures. The concept has been implemented by the STORK e-Delivery pilot (WP6.4) by settings its focus on the following three objectives [Rössler, 2010].

1. "*Verify whether the STORK authentication components developed by WP5 are scalable and usable for authenticating people at e-Delivery portals. e-Delivery portals require user authentication for several reasons: registration, login, and pick-up of deliveries. Therefore, WP6.4 will gather feedback from*
   - ***Service Providers/Owners:*** *... regarding take up of STORK and deployment/integrating of STORK components.*
   - ***End-Users:*** *... regarding usability and the subjective impression regarding transparency and security of a STORK enabled process.*"
2. "*e-Delivery systems often require the generation of evidences which prove that receivers have picked up their deliveries. Today, most of the e-Delivery systems make use of electronic signatures for creating these kinds of proofs. WP6.4 will try to adopt the STORK components so that proofs can be created (or signed) through STORK components. This should demonstrate the flexibility and extensibility of STORK components.*"
3. "*The STORK protocol and its particular element should be used as a basis for a cross-border e-Delivery concept. Especially protocol elements for identifying senders and receivers of deliveries should base on the common STORK protocol.*"

The first objective deals with the integration of the STORK authentication framework into existing CMS infrastructures. The pilot started with the integration at the beginning of 2010 and after a successful test phase started its 18-month piloting phase in June 2010. The pilot aims to demonstrate the applicability and scalability of the authentication components in a cross-border context and to evaluate this by inter alia gathering feedback from end-users and service providers.

The second objective deals with digital signatures. Several CMS and CEM protocols require recipients to create an NRR evidence by digitally signing a delivery confirmation. In system like the Austrian DDS, this can be done with the national eID. Particularly in Europe many countries have rolled out

eIDs featuring the creation of QES. It is thus advantageous if these eIDs tokens can be accessed through STORK components to create QES being legally equivalent to handwritten ones.

The third objective refers to Level 2 interoperability where the pilot has contributed to integrate STORK protocol elements like the QAA levels into cross-border CEM. Both the STORK and SPOCS CMS interoperability concepts have adopted some of the STORK authentication elements.

The following Member States have participated in the pilot:

- Austria
- Estonia
- Finland[1]
- Luxembourg
- Slovenia

The remainder of this chapter discusses both the STORK authentication components and their integration into three pilot partner CMS. Section 11.1 introduces in detail the STORK concept with its major interoperability models, the Middleware (MW) and Pan-European Proxy Service (PEPS) approach as well as the V-IDP concept bridging both models. The signature functionality, which has been integrated into the STORK protocol, is also discussed. The author of this thesis was not directly involved in the developement of the STORK framework and its specifications. This introduction is just made for a better understanding of the STORK framework and its working principle and underlying technology. Section 11.2 reflects the work that has been done in the e-Delivery pilot to integrate the STORK authentication components into existing CMS and shows the major results. The author of this thesis was the leader of the STORK e-Delivery pilot from July 2010 to June 2011[2].

11.1 Conceptual Model

STORK investigated two interoperability models [Leitold and Zwattendorfer, 2010; Leitold, 2011; Koulolias et al., 2011]. The first is the so-called Middleware (MW) model, which provides a user-centric approach of authentication. The second is the so-called Pan-European Proxy Service (PEPS) model, which uses a federated identity approach to delegate the authentication process to the national infrastructure.

11.1.1 MW Model

Figure 11.1 illustrates the so-called *Middleware* model. The identity data is usually stored on or accessed with tokens being in the possession of the user, for example a smartcard or a mobile phone. The communication with the token is usually provided by a client MW allowing the user to confirm the authentication process with a Personal Identification Number (PIN) or TAN code. In the MW model, service providers, which aim to integrate cross-border authentication support, must set up a server MW within their operational environment. This software is in charge of handling the authentication process with the user and the client MW. Therefore, the server-side MW must integrate the authentication mechanisms for all token types it supports.

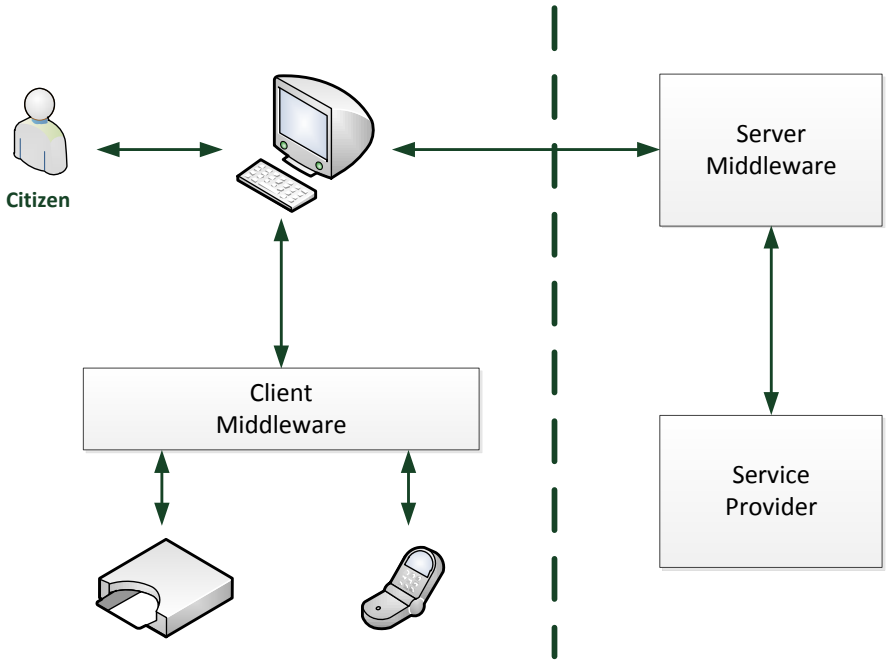

Figure 11.1: STORK MW authentication model.

11.1.2 PEPS Model

In contrast to the MW model, the PEPS interoperability model uses a federated approach between centralized national gateways. According to Majava and Graux [2007, page 25], any European interoperability framework has to perform a number of basic functions. These include the identification of a local identity provider, the retrieval of identity attributes and the transport of these attributes to a trusted service provider. A service implementing these functionalities is called *Pan-European Proxy Service (PEPS)*. A PEPS can be seen as a gateway, which hides national infrastructural complexities. Figure 11.2 illustrates the cross-border PEPS authentication process from a logical level. Consider the scenario where a user from Member State A wants to authenticate against a service provider residing in Member State B. Both Member States host an own PEPS instance. The PEPS instance of Member State A is called Citizen PEPS (C-PEPS) and the PEPS instance of Member State B is called Service Provider PEPS (S-PEPS). Both the C-PEPS and the S-PEPS have a trust relationship with each other. The same holds for the S-PEPS and the service provider. The authentication process is as follows: if a user wants to access a protected resource of the service provider **(1)**, the service provider delegates the authentication process to the S-PEPS **(2)**, which delegates the process to the C-PEPS of the user's home country **(2)**. The actual authentication is carried out at the C-PEPS or another national identity provider behind **(3)**. The C-PEPS may also retrieve additional identity information from an attribute provider **(4)**. The authentication information and additional identity attributes are transfered by the C-PEPS back to the S-PEPS **(5)**, which finally transfers it to the service provider **(5)**. The user is now authorized to access the requested resource **(6)**. According to Majava and Graux [2007, page 26], this decentralized model can be compared with a generalized MW approach where

> *[...] a fully decentralized PEPS model can essentially be implemented as a so-called middleware approach, where the PEPS basically functions as a middleware emulator that*

[1] Finland has joined STORK in the so-called enlargement phase in the second half of 2010.

[2] The STORK piloting phase was extended from 12 to 18 months to run until December 2011. The pilot lead has been handed over to Slovenia in May 2011.

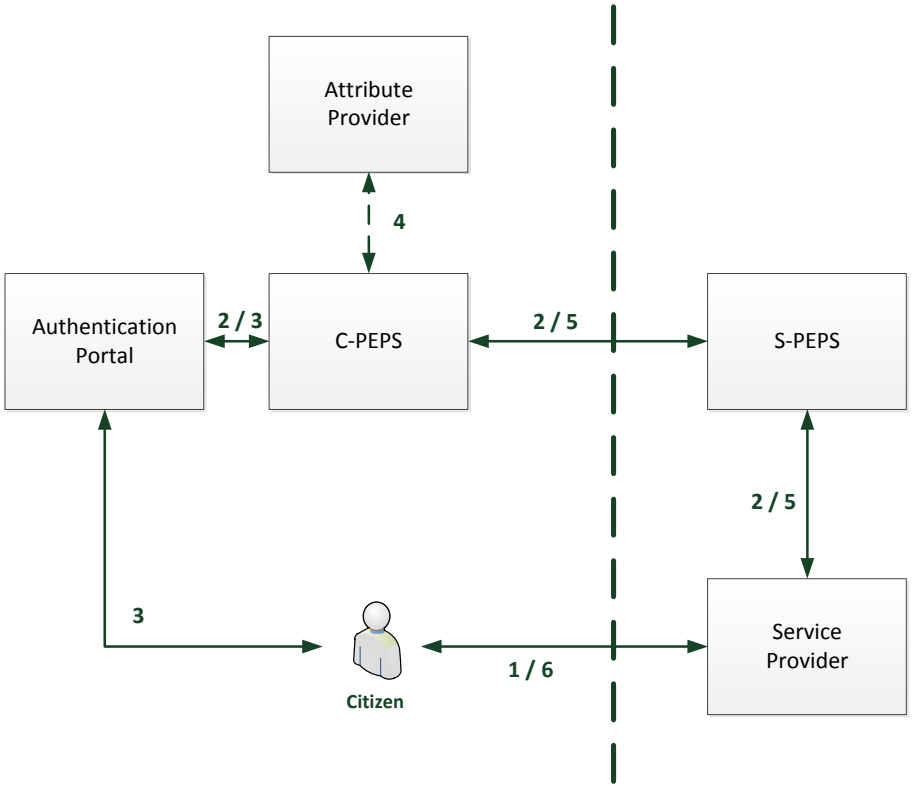

Figure 11.2: STORK logical PEPS model.

presents a commonly understood middleware to all SPs, regardless of the authentication method being used.

Figure 11.3 illustrates the PEPS approach as federated model with the concrete flow of identity information. The dotted curved lines visualize the identity data flow with the user as bearer. The STORK authentication protocol is designed in a way that identity data between different entities is exchanged and forwarded using HTTPs POST requests conducted by the user's browser.

11.1.3 Comparison of Both Models

When comparing the MW and the PEPS model, several differences become evident. In the MW model, authenticating foreign users directly communicate with the service provider. There are no intermediaries between the user and the service provider, which enables end-to-end security. Since the authentication data is retrieved from the user's eID, the user remains the data owner, the service provider is the data controller. Even if this model has a high degree of privacy and security, the major drawback is the dependency on eID token maintenance.

In contrast to the MW model, the PEPS model involves third parties. Since PEPS instances act as intermediary between the user's identity data source and the service provider, a PEPS becomes either an identity data processor or controller. By contrast with the MW, there is a liability shift from the service provider to the PEPS. Moreover, the MW end-to-end security is replaced with segmented trust relationships in the PEPS model. Even if this model provides a good way to hide complexities of the national authentication infrastructure, the degree of privacy and security is not the same as for the MW model.

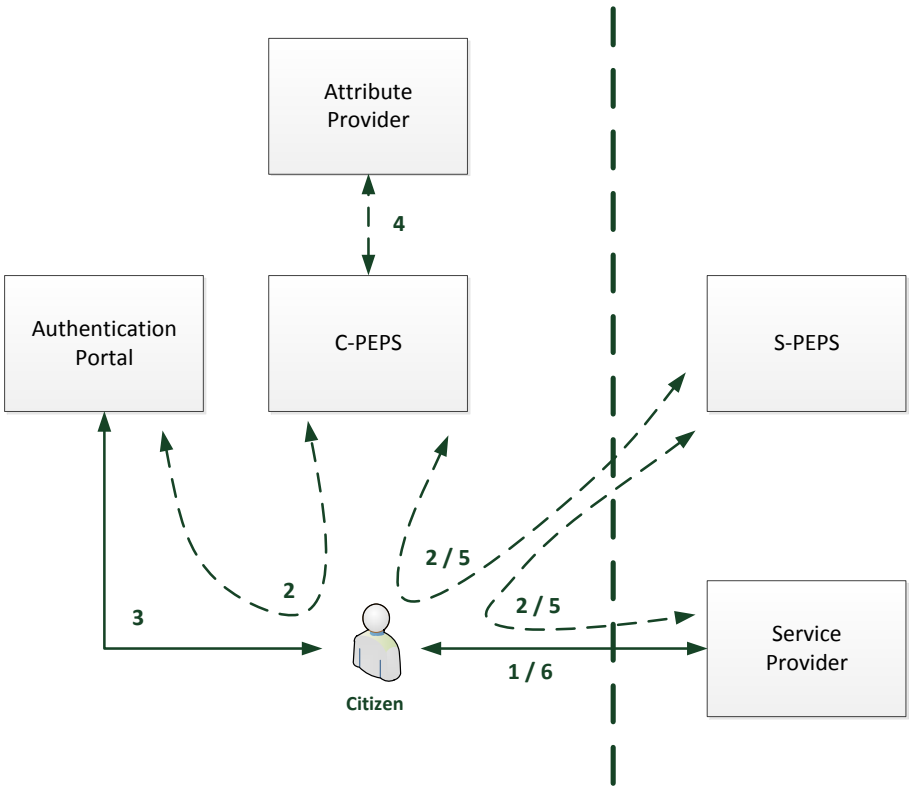

Figure 11.3: STORK federated PEPS model.

Nevertheless, in both models users must give their consent that their data is used abroad.

11.1.4 Combining both Models - the V-IDP

In the discussions above, only two scenarios have been sketched. The MW-MW and PEPS-PEPS scenario. This may lead to the view that a user from a MW country can only authenticate at a service provider having a server-side middleware installed and, in turn, a user coming from a PEPS country can only authenticate at a service provider of a PEPS country. Even if the two interoperability models are quite different, STORK aims for a common interoperability architecture, which combines both models in order to support all possible scenarios. This means:

- A user from a MW country authenticates at a service provider located in another MW country.
- A user from a MW country authenticates at a service provider located in a PEPS country.
- A user from a PEPS country authenticates at a service provider located in a MW country.
- A user from a PEPS country authenticates at a service provider located in another PEPS country.

Even though MW and PEPS have different operational models, they can be combined with the concept of a V-IDP, which is illustrated in Figure 11.4. A V-IDP is a MW with a PEPS interface so that both instances can communicate with each other. The STORK common specifications have been designed so that major components operate on the same protocols, irrespective of the model or its combinations.

According to Figure 11.4, a PEPS country may install the V-IDP in the S-PEPS environment so that users from PEPS countries are delegated to their national PEPS and users from middleware countries

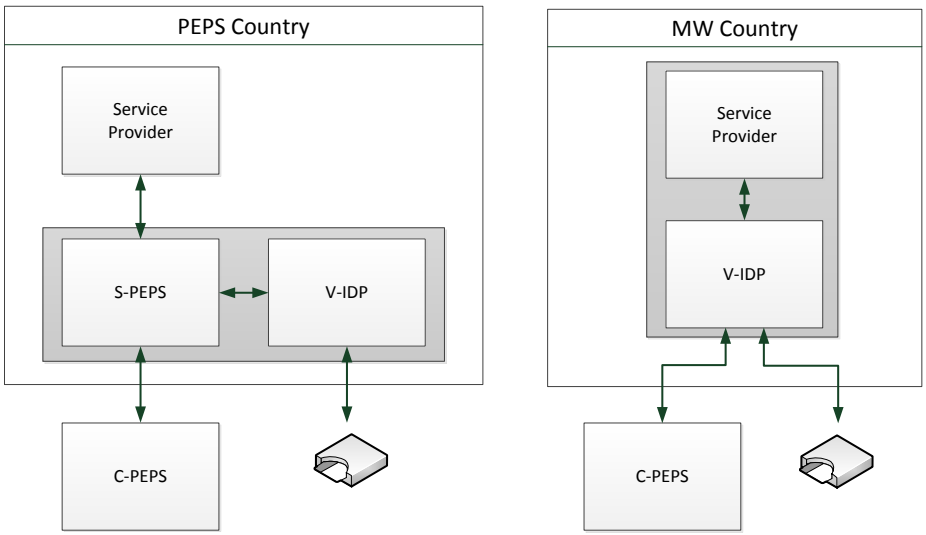

Figure 11.4: STORK Virtual Identity Provider (V-IDP).

can directly be authenticated at the V-IDP. The authentication data is then returned back to the service provider over the same interface. In a middleware country a service provider may install the V-IDP so that users from PEPS countries are delegated to their national PEPS and user from middleware countries can directly be authenticated at the V-IDP. In this way both the MW-PEPS and PEPS-MW scenarios can be realized.

11.1.5 STORK Common Specifications

Several work packages contributed to the production of the STORK common specifications and their deployment and demonstrations in the single pilots. WP2 investigated the legal situation in each partner Member State. A survey on state-of-the-art eID and IdM-related technologies was made by WP3. WP4 sketched the basic process flows of all interoperability model combinations for all supported scenarios: authentication, attribute transfer and certificate validation. The input of WP2 was particularly important to validate whether the process flows were compatible with data protection restrictions in each country. Based on the input of WP3 and WP4, WP5 was in charge of generating the STORK common specifications, main building blocks and architectural models. WP5 has produced the following relevant STORK specification documents as project deliverables:

1. ***D5.8.2 Technical Design for PEPS, MW models and interoperability*** [Heppe, 2010]. This is the parent document briefly describing the four single specification parts of the STORK technical design. Each part is specified in an own annex document. These annex documents are subsequently briefly introduced.

2. ***D5.8.2a Software Architecture Design*** [Berbecaru et al., 2010b]. This annex part specifies the main architectural model of the STORK framework. It describes the main use cases of authentication, attribute transfer and certificate validation in detail for each model: the PEPS model and the MW model, the latter including the V-IDP.

3. ***D5.8.2b Interface Specification*** [Alcalde-Moraño et al., 2010]. This document specifies the main interface, the protocol to exchange authentication data between different STORK components. The protocol is based on SAML 2.0 [OASIS Security Services TC, 2005]. The specification defines in detail request and response messages, bindings, profiles and authentication and identity attributes.

4. ***D5.8.2c Software Design*** [Berbecaru et al., 2010a]. This annex part specifies in detail the software architecture and process model for the PEPS component. Interfaces, classes, methods and their behavior is defined in detail.

5. ***D5.8.2d Security Principles and Best Practices*** [Stern, 2010]. STORK deals with the transfer of personal and thus privacy-sensitive data across national borders and thus deserves a high protection. This part of the specification identifies security threats, states security requirements in terms of confidentiality, integrity and availability and defines the necessary security functions for the STORK interoperability framework.

In some scenarios it may not be enough if the user just authenticates at the application. Particularly in CMS scenarios recipients authenticating at their MS have to additionally sign an NRR evidence. STORK has thus provided a functionality for creating digital signatures using STORK components. Users should be able to sign arbitrary data with their eID either at their C-PEPS or at the V-IDP if the user comes from a middleware country.

Besides authentication, STORK supports the attribute transfer of personal identification attributes. This includes unique identifiers, name, date of birth, gender, e-mail address, QAA level, age, etc. In the STORK authentication scenario, the service provider can request through the S-PEPS or V-IDP the attribute it requires. To avoid the introduction of a new process model and protocol for digital signatures, STORK has defined an additional attribute, which can be requested by service providers. During the authentication process at the C-PEPS or the V-IDP, the user creates a digital signature, which is completely eID-specific. Depending on the national eID solution, the signature could be created within the browser using Java or ActiveX technology or with local software like the Austrian citizen card environment. The actual signature creation process and its underlying technology is not part of the STORK specification, but depends on the eID solution.

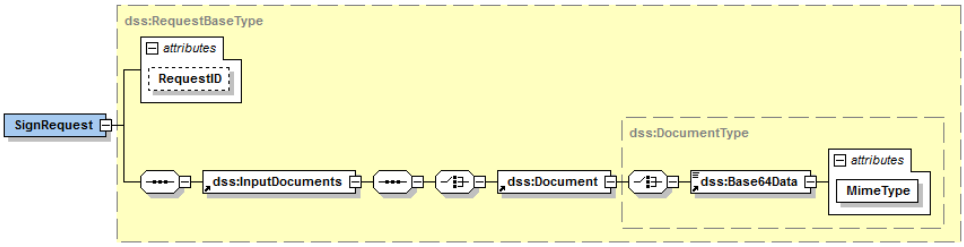

Figure 11.5: STORK SignedDoc attribute content as DSS XML schema fragment. Taken from the STORK interface specification [Alcalde-Moraño et al., 2010, Section 7.5].

From a technical viewpoint, the requested signature attribute ("signedDoc") consists of an OASIS DSS [OASIS Digital Signature Services TC, 2007] request, which contains only one element: the data to be signed encoded as Base64 (as illustrated in Figure 11.5). To avoid any complexities, no transformations like Extensible Stylesheet Language Transformations (XSLT) are allowed. The requesting entity is thus in charge of transforming the signature data in advance. The resulting signature should be an enveloping basic electronic signature XAdES-BES [ETSI, 2010a, page 14]. Currently, STORK supports the signature creation functionality only for eIDs supporting QES.

11.2 Integration

This section discussed the integration of STORK authentication components into national CMS infrastructures within the e-Delivery pilot[3]. To ease the integration of STORK into the national authentication

[3]The author of this thesis has mainly contributed to this and was the leader of the e-Delivery pilot from July 2010 to June 2011.

infrastructure, WP5 has developed a common code basis for a PEPS instance to be taken up by the Member States for national-specific implementations. The common code is based on a Java implementation and implements all required communications using the STORK protocol. Member States can simply extend this code by implementing the interface and connecting their national authentication solutions. This approach is similar to the SPOCS generic gateway discussed in Chapter 10.

Germany and Austria are the only MW countries in the STORK consortium and have implemented a code basis for a common V-IDP where Member States can integrate their national MW. In case of PEPS countries, the common V-IDP can be installed in the environment of the PEPS to support both authentication models. Since the common V-IDP was not available until the final phase of the STORK project, Austria has developed its so-called mini-V-IDP, which provides a PEPS interface for the Austrian national MW solution called Modules for Online Applications - Identification (MOA-ID)[4]. The basic working principle behind MOA-ID is discussed by the author of this thesis in [Zwattendorfer et al., 2011a].

The e-Delivery pilot integrated the STORK authentication functionality into existing CMS to demonstrate the applicability of the framework in real environments and under real conditions. Austria was the only MW pilot Member State. All other pilot Member States (Estonia, Finland, Luxembourg and Slovenia) are PEPS countries and have deployed a central national PEPS instance for all STORK pilots. The work of the e-Delivery pilot started with a functional design (cf. Deliverable D6.4.1 eDelivery - Functional Specification [Tauber et al., 2009]) sketching the basic use cases for cross-border authentication at national CMS. These are as follows:

1. ***Authentication***. This is the basic use case and describes how a sender or recipient authenticates at a foreign CMS provider using STORK authentication components.

2. ***Registration***. The use case of *Registration* requires a preceding valid authentication of the sender or recipient. Some identity attributes of the user are automatically provided through STORK authentication components to the registration procedure. Others must be entered manually by the user. Provided identity attributes by STORK components are given name, family name, date of birth and the unique electronic identifier. Since the registration in CMS is a crucial issue regarding the genuineness of the user's identity, the e-Delivery pilot supports in all use cases only QAA level 4. This level is supported by the eID tokens of all pilot Member States.

3. ***Message retrieval***. If the user has been successfully registered with a foreign CMS provider, the user is ready to send and receive CMS messages. In this use case a sender delivers a message to a foreign recipient registered with the same CMS provider.

With the pilot's planning documents [Rössler et al., 2009; Rössler, 2010], the project plan for integrating STORK authentication components into national CMS providers has been defined. The plan further defines the management tasks for testing (setup, test criteria, test cases, etc.) and demonstrating the authentication framework in a one-year piloting phase. The STORK authentication framework has been integrated in the following CMS providers:

- ***Meinbrief.at***. MeinBrief.at[5] is one of the three CMS providers of the Austrian DDS. The service has been approved by the Federal Chancellery in 2008. Besides administrative deliveries, MeinBrief.at can also serve deliveries of registered private senders with a CEM quality. Due to privacy protection legislations, in this case the recipient must explicitly give the consent to accept private sector deliveries; otherwise only administrative deliveries can be received.

[4] MOA-ID is an identity provider middleware implementing all necessary functions to authenticate and identify Austrian citizens with their eID.

[5] https://www.meinbrief.at

Meinbrief.at has deployed a mini V-IDP, which is able to authenticate both Austrian citizens with MOA-ID and foreign citizens by delegating the authentication process to their national C-PEPS. Besides supporting the pilot Member States Estonia, Finland and Slovenia, Meinbrief.at has extended the list of supported Member States to Island, Italy, Lithuania, Portugal and Spain. The Austrian DDS requires the recipient to sign an NRR evidence with a QES. The same must apply for recipients coming from other countries. The mini-V-IDP supports two ways of creating a signature using the STORK protocol. The signature creation process can either be delegated to the C-PEPS or the citizen can create the signature directly at the V-IDP, in case a C-PEPS has not implemented the signature functionality. The V-IDP thus provides a Java applet, which supports the creation of signatures with foreign eID tokens according to the approach discussed by the author of this thesis in [Tauber et al., 2010]. The underlying technology of this Applet, which is also used in Austrian e-Government, is discussed in detail by Orthacker and Centner [2011] and Centner et al. [2009]. Citizens from Estonia, Finland, Island and Lithuania can generate signatures with their eID directly at the V-IDP. Citizens from Italy, Portugal, Slovenia and Spain create signatures directly at their C-PEPS using national specific technologies to access their eIDs.

- ***DigiDoc***. The DigiDoc[6] platform is a full-scale architecture for digital signatures and documents. The platform is not a traditional CMS in terms of providing the non-repudiable fair exchange of documents. It is rather a secure environment for digitally signing documents and making them available for retrieval by other users. Access to the platform is enabled through an end-user portal (DigiDoc Portal), end-user client software (DigiDoc Client) as well as standardized Web services technologies. Estonian users can access the service with their national eID card. Registration with the system is not necessarily required, because user accounts are bound to the national identification number. If a user makes a document available for another user, this document is stored within a MS, which is solely accessible with the corresponding user's eID. The initiating user ("sender") must inform the receiving user ("recipient") that a document has been uploaded and is retrievable from the MS. Besides the authentication mechanism for Estonian citizens, the portal has been extended to support STORK authentication.

  DigiDoc delegates the authentication process to their national S-PEPS, which further delegates the authentication process to another C-PEPS or to its integrated common V-IDP in case of MW country citizens. Besides supporting the pilot Member States Austria, Finland, Luxembourg and Slovenia, DigiDoc has extended the list of supported Member States to Germany, Island, Italy, Lithuania, Portugal, Spain and Sweden. DigiDoc has no kind of transferable NRR evidences and citizens are thus not required to sign any confirmation or receipt during authentication.

- ***Moja.posta.si***. The CMS Moja.posta.si[7] has been reviewed in detail in Chapter 4. A brief summary is thus given here. The CMS of the Slovenian Post is a Web portal with the aim to provide a secure messaging infrastructure for both natural and legal persons. Access to the portal is provided to Slovenian citizens by means of SSL client authentication using their national eID. The service also offers a Web services infrastructure to send messages to registered recipients and for automated access to the MS. Besides the access with the Slovenian eID, the portal has integrated STORK authentication components to enable access by all citizens from other pilot Member States[8].

  Moja.posta.si delegates the authentication process to their national S-PEPS, which further delegates the authentication process to another C-PEPS or to its integrated common V-IDP in case of MW country citizens. Besides supporting the pilot Member States Austria, Estonia, Finland and Luxembourg, Moja.posta.si has extended the list of supported Member States to Island, Italy, Lithuania, Portugal and Spain. Moja.posta.si creates NRR evidences on behalf of recipients with

[6] https://digidoc.sk.ee
[7] http://moja.posta.si
[8] https://mpstork.posta.si/epprasp/

a server-side signature. Therefore, recipients are thus not required to sign any confirmation or receipt during authentication.

To illustrate the working STORK infrastructure in practice, the following screenshots show the step-wise authentication of a Slovenian citizen at the Austrian CMS provider Meinbrief.at. This use case has been intentionally be chosen as it demonstrates the interaction of all types of STORK components: the V-IDP, the PEPS and the signature creation functionality.

Figure 11.6: Meinbrief.at start page.

The start page of the Austrian DDS provider Meinbrief.at shows five different buttons symbolizing the different authentication methods. Four of them enable different authentication methods with the Austrian citizen card. Clicking on the STORK symbol redirects the user to the V-IDP.

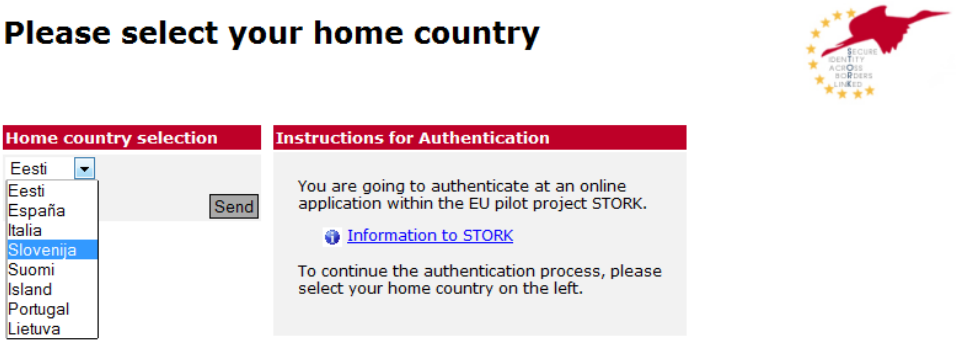

Figure 11.7: Meinbrief.at V-IDP country selection.

After being redirected to the V-IDP installed in the environment of Meinbrief.at, the user can choose the home country from the available list.

Figure 11.8: Confirmation of requested attributes.

After having chosen Slovenia as the home country, the user is redirected to the Slovenian C-PEPS to continue the authentication process. The C-PEPS shows the list of attributes the V-IDP has requested for the service provider Meinbrief.at.

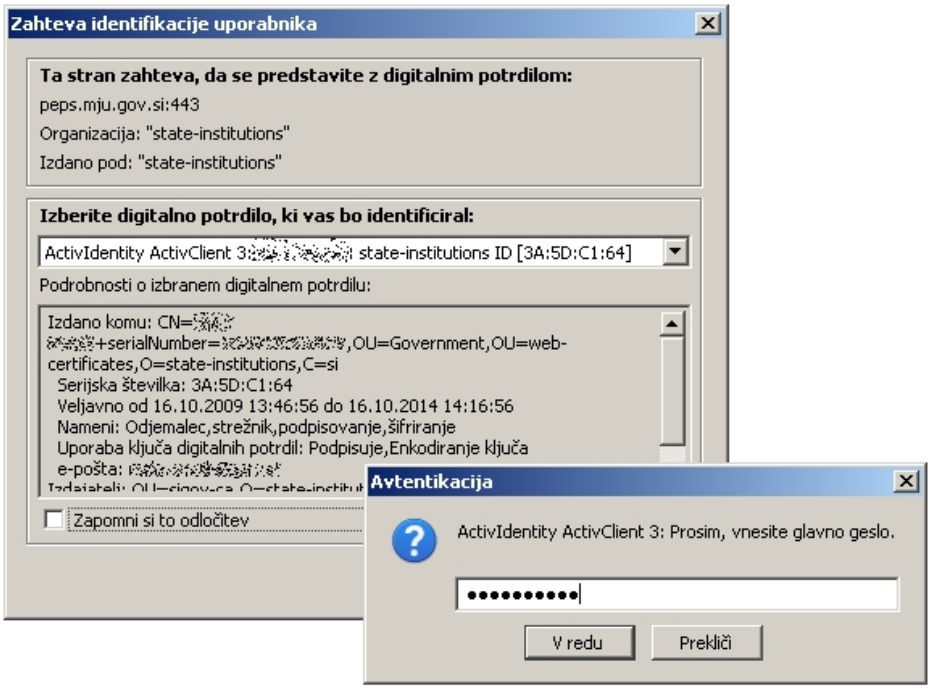

Figure 11.9: Access Slovenian eID card.

By confirming the requested attributes, the user's eID is accessed within the browser by selecting the certificate and entering the PIN code.

Figure 11.10: Start of signature process.

The user has the possibility to view the data, which has to be signed.

Figure 11.11: Display signature data.

Figure 11.12: Sign data confirmation.

After having checked the correctness of the signature data, the user actually starts the signature creation process.

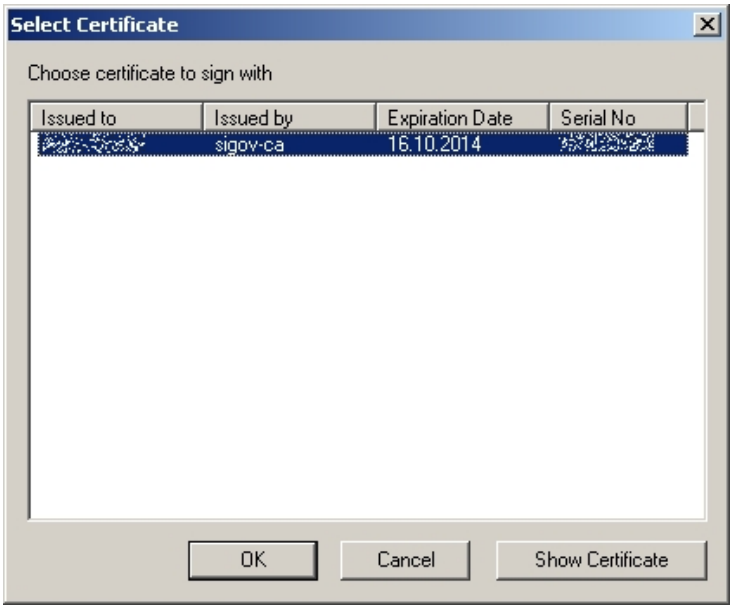

Figure 11.13: Select signature certificate.

The user selects the signature certificate from the ones available in the browser...

Figure 11.14: Prepare sending of attributes.

...and continues to finalize the authentication process.

Figure 11.15: Confirm authentication and identification attributes.

Before actually sending the authentication and identity attributes back to the V-IDP and Meinbrief.at, in a final step the C-PEPS asks the user to confirm the correctness of all attributes.

Figure 11.16: Successful login at Meinbrief.at.

After being redirected along with the attributes to the V-IDP and back to Meinbrief.at, the user sees the MS after successful authentication.This completes the process. It shows the successful implementation of Level 1 interoperability in a real production environment.

Chapter 12

Evaluation, Summary and Conclusions

"However beautiful the strategy, you should occasionally look at the results."

[Winston Churchill, British Prime Minister, 1874–1965.]

This chapter evaluates the CMS interoperability framework presented in this thesis. First, a requirements compliance analysis is made. Chapter 6 discussed a list of requirements and recommendations that a potential interoperability framework has to fulfill. Therefore, Section 12.1 makes a brief analysis for each requirement to determine to what extent it has been fulfilled. Besides the technical interoperability, an appropriate interoperability agreement and governance structure is a vital requirement for a working CMS interoperability network. Section 12.2 highlights this aspect in more detail. The CMS interoperability concept developed in STORK with the EDG and DGP has been improved in the course of SPOCS with the ICP. Since the topic of CMS interoperability is highly topical, particularly against the background of the Digital Single Market, SPOCS was searching for synergies with the public sector, industry, academia and standardization bodies to support the sustainability of the developed framework. The SPOCS ICP specification has been taken up by ETSI to extend REM towards a standard supporting all kinds of CMS protocols. This topic is discussed in Section 12.3. The work presented in this thesis focuses on technical aspects. So have also done STORK and SPOCS. However, there are also further organizational aspects, which have to be taken into account. One is accounting, because CEM services are usually not free of charge. This circumstance does not change in the cross-border case. Section 12.4 discusses this in more detail and proposes a potential accounting concept. Legal aspects have not been tackled by this thesis so far. However, they are a vital instrument towards a working interoperability network, particularly for the delivery of documents in administrative matters. Section 12.5 discusses this aspect in more detail. Finally, a brief summary of the work made in this thesis is given and conclusions are drawn.

12.1 Requirements Compliance Analysis

Chapter 6 analyzed and identified the requirements, which a CMS interoperability framework should have to fulfill. The requirements have been discussed on an abstract level and were mainly related to design principles rather than deciding on concrete technical details. This section reviews whether and to which extent the interoperability framework presented in this thesis complies with the stated requirements and recommendations. The compliance with each requirement or recommendation is subsequently discussed.

12.1.1 Scalability

A major requirement was the use of multilateral solutions as recommended by the EIF. This has been achieved by using a decentral communication architecture. Only a central TSL is required to distribute the necessary trust information. The ICP (or STORK DGP) and the EDG federated trust network guarantee a seamless communication between different CMS in a decentral way. This means that even though no central hub or proxy (except from the TSL information source) is used, the CMS interoperability infrastructure constitutes a multilateral solution paving the way for the compliance with other requirements.

The chosen multilateral solution eases both technical and administrative scalability. Regarding technical scalability, the ICP or DGP act as a "lingua franca"[1], because they are designed to be CMS independent. Since the protocol has only few mandatory elements, which are common to most messaging systems, virtually each messaging system can be seamlessly coupled with this framework. The concept allows even to couple CMS having non-transferable evidences. For example SOAP-based systems like PEPPOL's BusDox, the Danish RASP, the French PRESTO or the Estonian X-Road (cf. Section 4.3.4) may generate transferable evidences through their gateways on the basis of SOAP messaging events or status codes. This means that even elements or components, which are mandatory in the ICP, for example a DeliveryNonDeliveryToRecipient evidence, can be created by a gateway on behalf of a CMS.

Administrative scalability is achieved through the TSL approach. In both projects, STORK and SPOCS, a single root TSL approach has been chosen due to the low number of gateways. Assuming that more gateways are joining an interoperability network, a single TSL becomes unmanageable. However, the CMS interoperability framework can also be operated with a decentral TSL model like it is done in the European Union for CAs issuing QCs. With the decentral approach, countries or larger organizations could manage an own TSL for their domain. This enables administrative scalability, since decentral TSL maintainers know their systems better than a central body and can thus better decide on a system's trust status. Using a decentral TSL approach allows for a federated and thus scalable interoperability model on different levels. For example, a national regulatory body could manage a national TSL containing gateway entries of ministerial or regional CMS, for example e-Justice systems. This national TSL may contain pointers to regional TSLs, where a regional regulatory body could manage an own TSL containing gateway entries of local smaller CMS. By having a cascadable concept, administrative scalability is facilitated, but shifting the responsibility of trust to other bodies requires a sound governance structure and interoperability agreement. This aspects is discussed below.

12.1.2 Autonomy

The requirement of autonomy stated that a loose coupling of systems is necessary. This means that systems can easily join or leave an interoperability network without affecting other systems. Systems should not notice whether a system joined or leaved the interoperability network, unless messages actively sent do not reach their destination. The proposed concept in this thesis guarantees autonomy and a loose coupling through the use of a TSL. References to single CMS are completely managed in the TSL. If a new system joins the network, a new TSL gateway entry is created. If a system leaves the network, the corresponding entry is removed. There are no direct dependencies between single CMS, unless there is a bilateral agreement between two systems.

[1] A lingua franca denotes a language, which is used as a means between communication partners speaking different languages. For example, in traditional communications, Latin, French and now English have been used as a lingua franca in the European history to communicate between people speaking different languages.

12.1.3 Transparency

Even if the requirements of scalability and autonomy are entirely fulfilled, transparency was a hard challenge and could only be partially fulfilled. The framework was designed in a generic way to avoid changes of the domestic CMS infrastructure as far as possible. Even if the framework per se does not require any changes, necessary modifications fully depend on the CMS and its gateway implementation. Particularly addressing has been identified as a challenging part, because it is in an intrinsic messaging property determining the routing and addressing GUIs within a CMS. This is perfectly demonstrated by the Austrian DDS: the DDS message routing relies completely on the CLS. Without according modifications the CLS would not be able to recognize foreign CMS e-mail addresses and always return a "not found" error to the Austrian sender. Such a change is virtually inevitable in the Austrian system. Alternatively, senders could directly send a message, which is addressed to a foreign recipient, to the Austrian gateway. However, this requires some changes in the software of Austrian senders and would thus hinder scalability in the Austrian system. Virtual addresses tackle the general addressing problem to a great extent, but they cannot solve it completely. They ease the routing in the EDG network and leave e-mail-based systems untouched. However, SOAP-based CMS may still struggle with e-mail addresses.

Apart from addressing, the interoperability concept guarantees transparency for all other aspects on a technical, semantic and procedural level. Receiving systems must not take care of the underlying messaging technology of the sending system. Technical aspects are completely hidden through the ICP. This includes communication protocols, cryptographic functionalities as well as authentication levels and evidences. Moreover, the ICP is able to wrap any messaging system, not just those based on Internet e-mail or Web services technologies.

Even though technical and semantic aspects can be completely mapped by the ICP and thus be handled by the generic gateway, procedural aspects are custom to each system and have to be specifically implemented by each gateway. This mainly concerns trust establishment, fairness and timeliness. Trust between gateways is established through the generic gateway part. However, the segmented trust path between entities of different systems requires gateways to establish a trust relationship with the system they belong to. Evidence management to preserve fairness and timeliness completely depend on the CMS policies and processes and have to be implemented by each gateway in a custom way. However, for entities residing in the system itself, gateways and the interconnection network ensure a transparent message handling.

12.1.4 Security and Privacy

Security and privacy have a top priority when designing the interoperability framework. The design process was constantly accompanied by a risk management to identify potential security risks, threats and vulnerabilities. The following key security principles were taken into account:

- Confidentiality
- Integrity
- Authenticity
- Availability
- Accountability

Security is not only a matter of inter-gateway communication, but concerns the communication between single CMS and their related gateway(s) as well. Confidentiality, integrity and authenticity in the inter-gateway communication are ensured through an encrypted TLS layer and digital signatures. Their implementation in gateways towards the domestic CMS is completely system-specific and depends on

the CMS protocols and policies. Availability is another important aspect, particularly for the preservation of timeliness. The central TSL is less critical, since it can be used offline for a short period of time like a CRL. However, the availability of single gateways is more critical and should be ensured through appropriate means. For example, an interoperability agreement could define Service Level Agreements (SLAs) to be implemented by single gateways. The adherence to these SLAs would have to be controlled by the responsible governance body. The importance of an interoperability agreement and governance structure is discussed later in this chapter (cf. Section 12.2). Accountability is another important security aspect, which deals with the responsibilities and liability if something goes wrong. In the inter-gateway communication this concerns the central TSL. Since the whole trust management relies on the TSL, it is of paramount importance that new gateway entries are carefully added to the TSL, for example through some kind of accreditation procedure. This governance aspects is also discussed later in this chapter (cf. Section 12.2). Accountability also concerns single gateways. In fact, in the multilateral interoperability approach many security aspects are delegated to single gateways. For example, the mapping of authentication levels, evidences and connections to non-CMS systems like in the PEC case. Particularly the latter aspects poses a certain risk to compromise the whole interoperability network if not handled properly. PEC must thus mark each message coming from traditional Internet e-mail systems with a ReceivedByNonREMSystem evidence. Gateways also manage the trust to their domestic CMS. It is important to supervise these aspects with a governance body and to regulate them in an interoperability agreement to allot liabilities to each entity.

Privacy is a matter of subsidiarity and has to be preserved by each gateway. The interoperability concept presented in this thesis does not require the exposure of personal details or other privacy-sensitive information. All privacy-related information can be provided by CMS on a voluntary basis. Therefore, each CMS can maintain their own data privacy regulations by deciding which data are transmitted to other systems.

12.1.5 Preservation of Information

According to CMS-specific policies, systems may be required to store particular information for a certain amount of time. Therefore, the interoperability framework and particularly the generic gateway part provide the means to store all ICP-related information. This includes metadata, attachments, original messages, evidences with transferable signatures, STORK SAML authentication tokens, etc. Data storage across systems is a serious matter, because for example some systems may allow the data transmission across borders, but not their persistent storage due to national data protection legislations. In the current state, gateways may unconsciously store data by violating foreign data protection legislation. This is one reason why a unified legislation, either for certified mail or for the processing of private data is required for an operational interoperability network.

12.1.6 Open Standards

The whole interoperability framework is based on open standards. The inter-gateway communication uses the following open standards:

- MTOM
- WSDL
- WS-ReliableMessaging
- WS-Addressing
- WS-Security

- ETSI REM
- STORK SAML profile (not a standard, but a publicly available specification)

Even the implementation of the generic gateway is completely based on open and freely available programming languages and tools. This ranges from the open Java programming language to open source tools like Metro as Web services messaging framework or Bouncycastle as cryptography provider.

12.1.7 Design Reuse

Reuse of existing design principles and architectural models was a key priority from the very beginning. The interoperability framework is based on and reuses the following components:

- Design principles of the EIF as fundamental basis.
- PEGS gateway architecture as key model to achieve interoperability.
- ICP meta-layer aligned to best-practice approaches like eLink, the STORK protocol or the PEPPOL BusDox infrastructure.
- STORK protocol and ETSI REM specifications to map authentication, identification and evidence information.

12.1.8 Multilingualism

The interoperability framework can be seen as a "meta" messaging framework and does not deal with contents on the document level. Due to this nature, informational text is only used for status or event reporting. All ICP information text belongs to certain status or event codes. For example, the framework uses a well-defined list of error codes. In this way implementing gateways can either use the default English error code description or provide a custom translation for a particular error code.

12.1.9 Interoperability Agreement

An appropriate agreement is vital for a gateway interoperability network. For the SPOCS piloting phase a corresponding interoperability agreement has been defined and applied. Details of this agreement are discussed in the next section.

12.2 Governance Aspects

Besides a legal framework, an appropriate interoperability agreement and governance structure is also vital.

An interoperability agreement or governance policy is necessary and should have the following duties:

- Maintain the root TSL
- Regulate and supervise:
  - The accreditation of new CMS/gateways
    - Technical assessment
    - Security and privacy assessment

    - Certification
  - The ongoing operations of gateways
    - Availability (SLA)
    - Technical compliance
    - Security and privacy compliance
    - Data protection compliance
    - Compliance with other legal regulations
    - Information preservation
    - ...
  - Regulate accountability and liability matters.

All these tasks should be conducted under a harmonized legal framework.

During the piloting phase, SPOCS hosts a central TSL to manage trust. The SPOCS consortium acts as governance body and has published a document defining a TSL accreditation and operation policy [Seeger, 2010] regulating the mentioned duties. This document is aligned with part 3 of the ETSI REM specification "Information Security Policy Requirements for REM Management Domains" [ETSI, 2010d] and defines the following governance aspects for the SPOCS piloting phase:

- ***Accreditation process***. This part of the document describes the necessary requirements and steps for both public agencies and private business entities in order to be registered in the SPOCS TSL. Circumstances for revocation and suspension are described as well.
- ***Requirements for operation***. This part describes the operational compliance requirements of the SPOCS governance policy. First, organizations operating a gateway must continuously improve its ISMS in accordance with ISO/IEC 27001 [ISO/IEC, 2005a] (cf. [Seeger, 2010, page 10]). Second, security risks must be assessed and appropriately mitigated. For the SPOCS piloting phase, a security self-assessment has been deemed as sufficient.

A future interoperability network will require a governance structure operated on European level, for example by the EC itself. This structure will then be in charge of defining a suitable accreditation and operation policy for CMS systems on the basis of a harmonized legal framework, which is currently still missing, at least for documents in administrative matters (cf. Section 12.5). Besides accreditation, other cross-CMS aspects like signature recognition, data privacy, certification, liability and supervision will also have to be taken into account. The same would apply to a framework on the international level. In this case, not the EC, but the UPU could for example be the responsible regulatory body.

12.3 Standardization

In January 2010, ETSI has initiated the Specialist Task Force (STF) 402[2], a group of experts, with the aim to update the current REM specifications for the seamless exchange of messages between different CMS. The initial goal was to couple SMTP-based REM systems with CMS solutions based on other protocols (primarily Web services based on SOAP). Initially two targets had been identified: the UPU PReM standard (cf. Section 4.3.2) and PEPPOL's BusDox network (cf. Section 4.3.4.2).

Because of the similar goals of SPOCS and the ETSI STF 402, both initiatives have tightly collaborated to produce specifications for a CMS interoperability framework. ETSI STF 402 has mainly taken up the SPOCS ICP specifications with a few minor changes to define a REM SOAP message transport binding to couple different CMS. According to its description of scope the REM SOAP profile provides:

[2] http://portal.etsi.org/stfs/STF_HomePages/STF402/STF402.asp

- A model for decoupling REM semantic content and its binding to a predefined message structure and underlying transport technology.
- Definition of a generic electronic address scheme being able to carry arbitrary single electronic address values bound to a particular scheme, for example Internet e-mail.
- Rules for building a REM envelope as well-defined XML metadata. This includes both REM dispatches and REM evidences.
- Rules for the secure transport of the above REM XML metadata using SOAP, combined with appropriate parts of the Web services stack, this means a profiling of WS-Addressing and WS-Security.
- Specifications of the technical parameters a REM domain must publish in order to allow a different REM domain to interoperate with it.

The updated REM standard has been consolidated and published in September 2011 [ETSI, 2011].

In 2007, OASIS released version 3.0 of its ebMS specification [OASIS, 2007]. ebMS defines a communication-protocol independent method for exchanging electronic business messages within an XML framework that leverages common Internet standards. Specifications include messaging functions to operate over SOAP (SOAP 1.1 or SOAP 1.2, and SwA), intended for reliable and secure delivery of business information, without committing to specific format types for payload. While ebMS 3.0 does not define a specific schema for evidences (receipt signal, in ebMS terminology), this is part of AS4 [OASIS, 2011], a specific profile which reuses structures from the OASIS ebXML standard.

To some extent, this initiative overlaps with ETSI's ongoing effort for extending REM to support SOAP. Even if they differ in technical details and in the requirements they are designed to support, both OASIS and ETSI doubt whether there is a market for all these protocols. Hence a proposal for the convergence of the two standards is currently being made, with respect to the envelope format and the evidence production. The success of this convergence would result in a simplification and consolidation of the standard's landscape, to the advantage of all stakeholders.

12.4 Open Issues

The major goal of piloting in STORK and SPOCS was to demonstrate the technical feasibility in real environments and under real conditions. However, several other aspects like a governance structure have not been taken into account completely, reasoned by a missing legal framework. Another open issue is accounting, which is a key aspect in most CMS, particularly in those operated by private businesses or postal services. Depending on the CMS, different business models are used for accounting. Basically two different accounting models can be found in today's systems: system like the Austrian DDS or the German E-Postbrief have a per-message payment scheme. This means that certain costs are accounted for each (sent) message. This price may be fixed or depend on the message volume. Other systems like the Italian PEC have a "flatrate" accounting model, where sending and receiving of messages is for free. However, PEC providers charge a particular amount for each mailbox per month or year.

Accounting has not been designed as integral part of the interoperability framework, but should be considered as a future task when putting such an interoperability network into operation. A possible accounting scenario is illustrated in Figure 12.1. This scenario requires that gateways manage some kind of accounting information within their metadata file (denoted as MD), which lies parallel to the WSDL (cf. Section 9.3). This metadata could include prices for single messages, volume discounts or differences in prices for administrative and private business deliveries. In this way a sending gateway knows in advance the total amount for one or more deliveries. Moreover, it can also compare prices. Assumed that a recipient is registered in two or more systems or that more gateways are serving the same CMS, the sending gateway can compare the resulting price for each gateway and deliver the message to

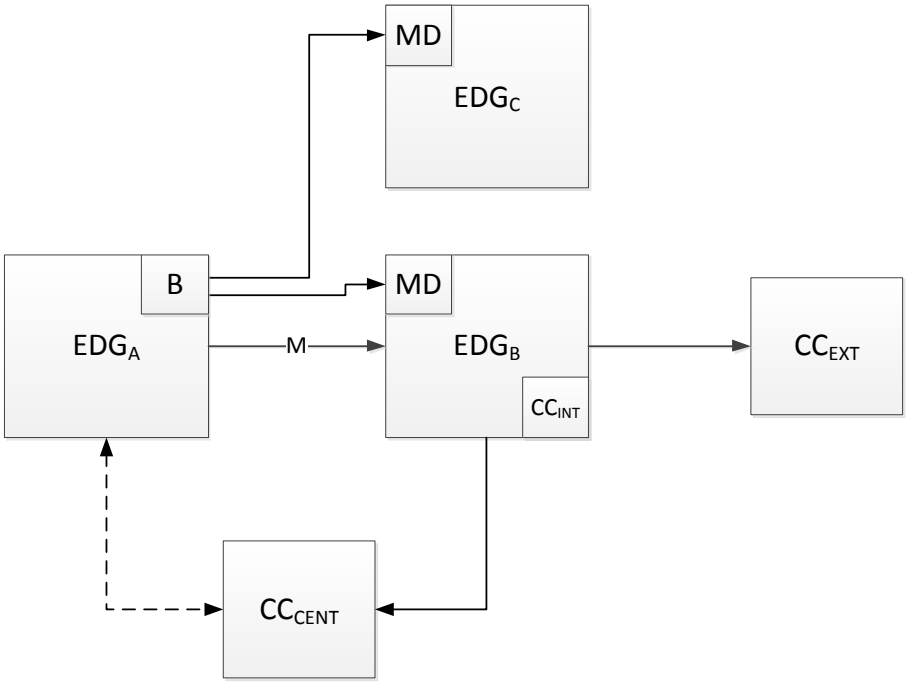

Figure 12.1: Possible accounting concept for cross-border CMS interoperability.

the cheapest gateway. The presented model uses a Clearing Center (CC) to manage accounting. This could be a central CC (CC_{CENT}) shared between all gateways, an internal CC (CC_{INT}) of the gateway or an external service provider (CC_{EXT}). In all cases these CCs manage the billing and charge sending gateways for delivered messages. The presented accounting solution is just a possible solution and needs further investigation, discussion and possible improvement by the concerned community.

Even if E2EE on the message level is a desired property, it became evident that it cannot be realized due to necessary translations. Exceptions are systems having the same or compatible CMS protocols. In many cases, however, E2EE is not just a desired, but actually a required property. Particularly the transmission of highly privacy-sensitive data like medical patient data is often subject to such a requirement. In this case a document-based E2EE should be used instead. E2EE requires knowledge of the recipient's encryption certificate. CMS or domestic PKIs often provide public directories to share these encryption certificates. Since such directories are not available, visible or known in the cross-CMS case, a global directory for all CMS in the interoperability framework could be of help towards document-based E2EE. This must not necessarily be a physical directory containing all encryption certificates. A possible solution could be a virtual directory in terms of a "certificate lookup broker" forwarding certificate search requests to foreign directories.

12.5 Legal Aspects

Traditional certified mail for the private sector, this means B2x and C2x communication scenarios, is not regulated by law in most countries. Usually postal services offer certified mail as a value-added service for its customers. The provision of this service is thereby regulated by a bilateral agreement between the customer and the postal service, for example by accepting the general terms and conditions of the postal service. This kind of contract defines the delivery policy and may include the definition of single services like the delivery confirmation service or the signature confirmation service, but may also comprise the assignment of responsibilities or even non-liability clauses. If anything goes wrong, the customer can

rely on this bilateral contract and in case of a non-resolvable dispute, the customer can take court action.

Certified mail delivery in administrative procedures works on the same principle. However, in the public sector, policies, agreements and general terms and conditions are regulated by law. Certified mail ensures the exact determination of periods for appeal, whereby the delivery instant is documented for example with a receipt signed by the recipient. In most countries the service of administrative documents is regulated by law. This applies at least for traditional postal mail delivery. Some countries like Austria, Germany and Italy have enacted dedicated laws for CEM delivery and built custom CMS on top of that legislation. However, for both traditional and certified electronic mail delivery the scope of these laws usually covers only the own country. But what happens in the cross-border scenario, where a delivery passes on its way from the sender to the recipient through different legislations? This circumstance could be resolved with a bilateral agreement between the sender's and the recipient's country. However, taking the number of (European) countries into consideration, this would lead to an unmanageable number of laws. Therefore, economic or political unions have tried to regulate the cross-border delivery within their territory with cross-national treaties. This section gives an overview of existing regulations for the cross-border delivery of both traditional and certified electronic mail within the European Union. The scope of application and limitations are discussed in detail. The section closes with a brief discussion of what is currently possible in the context of servicing general administrative documents to foreign citizens and what needs to be addressed in the near future to close remaining gaps.

12.5.1 Existing Regulations for Cross-border Mail Delivery

The following regulations exist for cross-border mail delivery:

1. European Treaty No. 94/1977
2. Directive 2008/6/EC
3. Regulation (EC) 1393/2007

European Treaty No. 94/1977

On 24 November 1977 a treaty of the Council of Europe "European Convention on the Service Abroad of Documents Relating to Administrative Matters" [Council of Europe, 1977] was officially opened for signature. The aim of this treaty is to achieve a greater unity between its members through the mutual assistance between authorities. The convention is about the delivery of administrative documents to foreign citizens in reasonable time. The essential provisions are as follows:

1. ***Scope of the convention***. All Contracting States commit themselves to a mutual assistance in the delivery of administrative documents. The scope of the convention basically covers all administrative areas except for financial and criminal matters. However, each Contracting State can declare anyway to serve the delivery of administrative documents for one of these two areas. Comparably, each Contracting State can define a list of administrative matters to which the convention will not apply. In this case, all other Contracting States may claim reciprocity.
2. ***Central authority***. Each Contracting State designates a central authority, which is in charge of accepting and handling incoming delivery requests of other Contracting States relating to administrative matters. Federal States are free to designate multiple central authorities. Name and address of this authority has to be communicated by each State to the Council of Europe. States may also set up other authorities implementing the functionality of the central authority. However, foreign States may always have the right to directly contact the central authority. Last not least, each Contracting State may designate a central sending authority being in charge of channeling all outgoing

administrative deliveries addressed to foreign citizens. This sending authority may then directly contact the central authority of the foreign State.

3. ***Request for service***. The convention defines a specific request form for the service of delivery. This form must be used by the sending authority and sent along with the actual document to the central authority of the foreign State. The main form data are the address of the sending (requesting) authority, a brief description of the contents of the document, the recipient's detailed address and the manner of service, which is described subsequently.

4. ***Manner of service***. The convention defines two basic manners how the delivery can be conducted. First, the default way is delivering the document according to the rules and regulations of the requested State, this means under the sovereignty of the recipient's State. Secondly, the sender's State may desire a custom delivery manner. However, in this case the procedure must not be incompatible with the law of the recipient's State. The latter manner may also include the definition of a delivery deadline, a specific point in time up to which the delivery must be handed over to the recipient. This deadline must be compatible with the law of the recipient's State.

5. ***Language***. Sending authorities are not required to translate the document to an official language of the recipient's State. However, in this case the recipient can refuse to accept the delivery and thereafter the central authority of the recipient's State or the sending authority have to translate the document.

6. ***Certificate***. The convention defines the cross-border delivery of administrative documents as certified mail and requires the recipient's State to issue a certificate of delivery. This certificate either attests the successful conclusion of the delivery or documents the failed delivery attempt. The form of the certificate is predefined by the convention. It mainly contains the address of the sending authority, date, time, delivery address, delivery manner and a signature or stamp of the central authority of the recipient's State. In case the certificate is not issued by the central authority, the sending authority may request the central authority to countersign the certificate. The standard terms of this certificate may be printed in one of the official languages of the Council of Europe or in one of the official languages of the sender's State. Values may be filled in this form in one of the official languages of the recipient's State.

7. ***Transmission channels***. Contracting States may basically effect the delivery in the foreign country directly with the help of consular officers or eventually if feasible by diplomatic agents. Each State may, however, refuse this kind of delivery in its territory. The same applies to postal services. Contracting States may directly use postal services to effect delivery in the foreign country and each State may decide whether it accepts this kind of delivery. The convention does not exclude bilateral agreements defining other transmission channels, for example the direct communication between authorities.

8. ***Costs, Refusal to comply and time limits***. If the delivery is carried out according to the regulations of the recipient's State, no costs can be charged for the activities of the recipient's State. Otherwise costs have to be paid that originate from the desired delivery procedure.

   The recipient's State can refuse the delivery if one of the following applies:

   - The document refers to an administrative matter, whose delivery is not covered by the recipient's State.
   - The delivery of the document could threaten the sovereignty, security, public policy or other essential interests of the State.
   - The recipient is not addressable or reachable.

Last not least, if the delivery is bound to any deadline, for example a period for appeal, the recipient must be granted a reasonable time limit to react on the delivery.

Directive 2008/6/EC

The postal sector is definitely one of the larger areas, which are subject to intensified regulations by the European Community. In 1997, the Community put the Directive 97/67/EC[3] [The Council of the European Union, 1997] into force. The main goal of this directive is to harmonize the conditions in the postal sector across Europe and to create a common legal framework for establishing an internal market in the postal sector. This should be achieved with a gradual and controlled liberalization of the market to ensure competitiveness throughout the EU. According to the directive, the establishment of the internal market in the postal sector is important for the economic and social cohesion of the Community and postal services are an essential instrument for communications and trade.

The directive also aims for improving the performance quality of postal services by defining minimum requirements for universal postal services, this means access to postal services by all natural and legal persons and delivery of items on all working days. However, besides economic growth, performance quality and availability, people should have the choice to select between different postal services and last not least these services should be offered at affordable prices.

The directive also regulates several aspects of cross-border postal services, which are as follows:

- **Performance quality**

  "*Whereas cross-border postal links do not always meet the expectations of users and European citizens, and performance, in terms of quality of service with regard to Community cross-border postal services, is at the moment unsatisfactory.*" (page 1 (07))

  "*[. . .] Quality standards shall focus, in particular, on routing times and on the regularity and reliability of services. These standards shall be set by: [. . .] the European Parliament and the Council in the case of intra-Community cross-border services [. . .]*" (Article 16)

  "*Whereas, in the case of intra-Community cross-border services requiring the combined efforts of at least two universal service providers from two different Member States, quality standards must be defined at Community level.*" (page 3 (32))

  "*Member States shall day down quality standards for national mail and shall ensure that they are compatible with those laid down for intra-Community cross-border services [. . .]*" (Article 17)

  "*[. . .] The Commission shall publish in the Official Journal of the European Communities any adjustments made to the quality standards for intra-Community cross-border services and shall take steps to ensure the regular independent monitoring and the publication of performance levels certifying compliance with these standards and the progress accomplished [. . .]*" (Article 18)

- **Interoperability**

[3] The directive was amended in 2002 with the directive 2002/39/EC [The Council of the European Union, 2002] with respect to the further liberalization of the market in the postal sector. A third amendment was made in 2008 with the directive 2008/6/EC [The Council of the European Union, 2008] with regard to the full accomplishment of the Internal Market of Community postal services.

> "*Whereas progress in the interconnection of postal networks and the interests of users require that technical standardisation be encouraged; whereas technical standardisation is indispensable for the promotion of interoperability between national networks and for an efficient Community universal service*" (page 4 (36), see also Article 20)

- **Implementation**

  > "*Whereas a committee should be established to assist the Commission with the implementation of this Directive, particularly in relation to the future work on the development of measures relating to the quality of Community cross-border service and technical standardisation*" (page 4 (38))

- **Certified mail**

  For security reasons the directive does not regulate the delivery of documents in judicial or administrative matters:

  > "*The provisions of Article 7 shall be without prejudice to Member States' right to organise the siting of letter boxes on the public highway, the issue of postage stamps and the registered mail service used in the course of judicial or administrative procedures in accordance with their national legislation.*" (Article 8)

Regulation 1393/2007/EC

Particularly in the justice sector documents need to be delivered[4] in a reliable and evidential way. This starts from summons, subpoenas and appeals to final court decisions. So far, all European Member States have provisions to ensure that documents are actually delivered to the intended recipient. However, these provisions greatly differ from Member State to Member State. The European Judicial Network (EJN)[5] in civil and commercial matters, a network of national contact points in judicial matters, has published a detailed survey[6] of judicial delivery in each Member State.

To support the proper functioning in the internal market, the Community has put in force the regulation 1393/2007/EC[7] [The Council of the European Union, 2007] to improve and speed up the smooth transmission of judicial and extrajudicial documents in civil or commercial matters. This goal has been expressed and manifested in Article 65 of the Treaty of Lisbon[8] [European Union, 2007], which states:

> "*The Union shall develop judicial cooperation in civil matters having cross-border implications, based on the principle of mutual recognition of judgments and of decisions in extrajudicial cases. Such cooperation may include the adoption of measures for the approximation of the laws and regulations of the Member States*"

and in particular ensuring:

[4] The legal term for delivering documents in the justice sector is "serving documents".

[5] The EJN was created in 1998 to support the cross-border judicial collaboration to fight organized crime.

[6] The list of country profiles is available online at `http://ec.europa.eu/civiljustice/serv_doc/serv_doc_gen_en.htm`. The site also contains information about the Community law and International law, for example the 1965 Hague Convention, which constitutes a network of central agencies designated by each country for the transmission of judicial documents. The Directive prevails over the provisions contained in the Hague Convention or given by bilateral agreements.

[7] The directive amends the council regulation (EC) 1348/2000 of 29 May 2000 on the service in the Member States of judicial and extrajudicial documents in civil or commercial matters [The Council of the European Union, 2000a].

[8] The treaty entered into force on 1 December 2009 with the aim to "to complete the process started by the Treaty of Amsterdam and by the Treaty of Nice with a view to enhancing the efficiency and democratic legitimacy of the Union and to improving the coherence of its action" [European Union, 2007, see preamble page 5]

"*. . . the cross-border service of judicial and extrajudicial documents. . .*"

Regulation (EC) 1393/2007 has many similarities with the Convention on serving administrative documents abroad (cf. Section 12.5.1). In contrast to the Treaty, whose focus is on general administrative documents, the scope of application of this directive is on judicial and extrajudicial documents in civil or commercial matters, which have to be transmitted from one Member State to another one. It explicitly excludes the service of documents in administrative matters.

Cross-border delivery is carried out through so-called transmitting and receiving agencies, this means a public officer, authority or other person designated by a Member State. The transmitting and receiving agency must not necessarily be the same entity. In case of federal states, multiple agencies may be designated. The concept of "agency" in this directive is comparable to the central authority term defined by the treaty of 1977. In addition to agencies, a Member State shall designate a so-called central body, which is in charge of supplying information to the transmitting agencies and of resolving any occurring problems during transmission. Federal states may designate multiple central bodies.

The delivery of judicial documents can be carried out by any means as long as the received document corresponds with the transmitted document in terms of content. The document must also be accompanied by a form sheet in one of the official languages of the recipient's Member State. Recipients may refuse to accept the document if it is not available in one of these official languages. Receiving agencies return as soon as possible, but at the latest within seven days, a receipt (comparable to an NRS evidence) back to the transmitting agency. If subsequently anything goes wrong during the delivery process, for example due to an inexistent address or form errors, the transmitting agency is immediately notified about that event.

By default, the delivery is carried out according to the regulations and laws of the recipient's Member State. However, if desired, the sender's Member State can request a particular method. This method must be compatible with the laws of the recipient's Member State. There is a time limit of one month for the receiving agency to deliver the document. Nevertheless, Member States must try to deliver the document as soon as possible. The receiving agency immediately returns a "certificate of service or non-service of documents" in one of the official languages of the sender's Member State back to the transmitting agency. This certificate can be compared to an NRD evidence. In case of refusal by the recipient or if the delivery failed for any reason, this circumstance must be documented on the certificate.

Basically no costs incur for the receiving Member State except that further public officers are involved or the transmitting agency desires a particular delivery method. Judicial documents may also be delivered by postal services or even by consular or diplomatic channels.

The European Judicial Atlas in Civil Matters[9] provides information about judicial cooperation in civil matters bundled in a central Web resource. One section covers the topic of "serving documents" and provides a lookup directory with information about (transmitting, receiving) agencies, central bodies, judicial officers and form sheets of each Member State.

12.5.2 Discussion

Three regulations for cross-border delivery of documents have been introduced in the preceding sections. All have as primary target traditional postal mail delivery. But are they also valid for cross-border electronic delivery of documents? This section discusses the scope of application of these regulations in the context of electronic delivery as well as what is currently possible with given regulations and what actions are required in the near future.

Treaty No. 94 entered into force in 1977 and enables the cross-border certified mailing in administrative matters. At that time, electronic communication was reserved to just a few people in the military and educational sectors. Therefore, the convention covers traditional mail delivery only. However, even

[9] http://ec.europa.eu/justice_home/judicialatlascivil/html/index_en.htm

if it would be applicable to electronic mail, the number of States having ratified the convention is quite low. The Council of Europe has 47 Member States and the convention has been ratified by the following eight Member States only[10]: Austria, Belgium, Estonia, France, Germany, Italy, Luxembourg, Spain. Greece, Malta, Portugal and Switzerland have signed, but not ratified it. The convention for these four States has thus not come into effect.

Whereas Treaty No. 94 primarily covers documents and cross-border mailing in administrative matters, the directive 2008/6/EC deals with the harmonization of postal services regarding private sector deliveries. Even if several articles refer to cross-border mailing, this only includes deliveries originating from natural or legal persons and does not explicitly mention registered or certified mail. For security reasons, the directive explicitly leaves certified mailing in judicial or administrative matters out of its scope. Furthermore, even if electronic means are explicitly mentioned as drivers for the postal sector to enhance its portfolio, improve the efficiency and enhance the availability (hybrid mail), the directive only covers traditional mail delivery. The same applies to the Regulation (EC) 1393/2007.

Currently, only a few regulations provide the basis for cross-border certified electronic mail. However, these regulations are tailored to specific use cases. One example is the Regulation (EC) No 1896/2006 [The Council of the European Union, 2006b] creating a European order for payment procedure. Art. 13 regulates the service with proof of receipt by the defendant explicitly covering certified electronic mail. Deliveries in the context of the Services Directive, which is an administrative matter, are thus not subject to any cross-border regulation or law. At the present moment, cross-border certified mailing in administrative matters is therefore, with the exception of a few countries, impossible. For example, Austria has provided in its Service of Documents Act a regulation [Republik Österreich, 2004, Article 11 and 12] for cross-border delivery. This regulation covers both traditional postal and certified electronic communications. According to this regulation Austrian public authorities can send electronic documents in administrative matters to foreign recipients, if, and only if the foreign CMS allows that. The reverse direction, this means electronic deliveries from foreign senders to Austrian DDS recipients are not covered by the law. However, with this regulation, Austrian public bodies could for example deliver documents in administrative matters to PEC recipients, since the Italian law [Repubblica Italiana, 2009, Article 35] enables the interoperability of PEC with "analogous international systems".

However, not all countries have legal provisions for (partial) cross-border certified mail delivery. Generally, from a legal perspective, if somebody wants to receive a certified mail in an administrative matter from a public authority residing in a different Member State, the only option is to register with the foreign CMS (Level 1 interoperability) or directly with the public authority. In this case the recipient's mailbox and associated actions are conducted on a server, which is in the sender's Member State sovereign capacity, and not on a server abroad where the sender has no authority. Since such a scenario is not the aim of user-friendly and convenient interoperability, there is an essential requirement for a Community regulation enabling the European certified electronic mailing in administrative matters.

12.6 Summary

This thesis treated CEM as an IT security and e-Government discipline. It tackled the question, whether existing CMS could be made interoperable through an appropriate framework, and if so, presented and discussed a technical concept meeting the requirements for such a framework. To be more precise, the main goal was to develop a scalable interoperability framework, which is able to make existing CMS interoperable by ensuring the requirements of transparency, autonomy, security, privacy and by using open standards and reusing best-practice tools and technologies.

First, the traditional registered and certified mail services have been reviewed and discussed. Traditional registered and certified mail have a long history and over time their security services portfolio has

[10]The chart of signatures and ratification is available at `http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=094&CM=1&DF=&CL=ENG`

been extended and single services have been improved. Basically, the mail security services of insurance, delivery confirmation, signature confirmation, collect on delivery, restricted delivery and return receipt could be identified. The discussion of these services helped to get a better understanding of the basic mail security services and to map their requirements also to the electronic world. A brief comparison of mail security services of different national universal postal services confirmed the use of these common basic security services, but in different configurations. Hybrid mail can be seen as the intermediate service between the physical and the electronic world. It has been discussed that with hybrid mail several security services like confirmations are provided electronically, however, the final mail delivery is still carried out physically.

The next step after hybrid mail is the full electronic provision of certified mail services. This thesis gave a detailed overview of CEM by discussing its evolution and security services and properties. This was done by referring to the general electronic mail handling architecture and model defined by X.400. The X.400 specifications provide a model, which is suitable to describe many of today's messaging systems, including Internet e-mail and most CMS. The thesis described in detail the approaches of the Internet community toward secure and reliable e-mail, for example MDN, DSN or signed S/MIME receipts, and discussed why these services provide no evidential value. The discussion continued with a detailed overview of CEM security properties found in the literature and introduced by the research community in the past two decades to propose protocols for the fair and non-repudiable message exchange. The properties of non-repudiation services, evidences, fairness, trusted third parties, communication channels, timeliness, state storage, confidentiality, integrity, authenticity, performance and policy have been discussed in detail, particularly by identifying different flavors and their practical relevance. The thesis also discussed the dependency between different properties and why some of them are mutually exclusive. This is also an important practical aspect.

By drawing on the basic groundwork elaborated in the first part, the thesis provided a detailed survey of existing CMS. The main goal was to assess and evaluate the identified security properties in systems actually provided on the Internet. Many properties found in the literature are only considered from a theoretical point of view. The design of an interoperability framework needs to take practical properties in account. The survey gave an overview about architectures and process flows of several CMS having publicly available specifications. Other systems of postal services, private businesses, the justice sector and notary systems have been discussed as well. Over the last decade, several standards for the fair and non-repudiable message exchange have evolved. To not only consider the view of implementers, but also of standard designers, this thesis discussed predominant standards like ETSI REM, UPU PReM or OSCI. Other standards having non-transferable evidences, nonetheless ensuring the reliable message transport have been introduced as well. The evaluation showed that standards and systems provided on the Internet mainly adopt the model of postal certified mail. In addition to strong fairness, all systems and standards make use of inline TTPs. Even if they have some drawbacks from an efficiency viewpoint, they facilitate the deployment in terms of infrastructural requirements. The last research decade was dominated by optimistic solutions. The thesis also showed that there is a consensus that an NRD evidence is a core property of practical systems, whereas NRO evidences are just considered as optional. This also matches the model of postal certified mail. At least within the European context, AdES and QES are widely used. This eases interoperability efforts, even if there is no common approach regarding the use of transport protocols.

Interoperability is a topic which becomes more and more important. This is particularly manifested by the interoperability initiatives of the EC. One hot topic is CMS interoperability. The work presented in this thesis has been elaborated and carried out in the course of two European LSPs: STORK and SPOCS. Therefore, this thesis gave and overview about the political and technical background of these initiatives. This includes the review of the IDA programme (during the eEurope initiative), the IDABC programme (during the i2010 initiative) and the recently started ISA programme of the Digital Agenda supported by the e-Government Action Plan 2011-2015. The thesis has also reviewed the work of the five Type-A LSPs STORK, SPOCS, PEPPOL, epSOS and e-CODEX to illustrate their approach of

achieving interoperability and the synergies between these projects. In a next step the thesis highlighted the importance and the need for CMS interoperability, particularly in the light of the Services Directive. It defined the basic interoperability Levels 1 and 2.

Before designing an interoperability framework, it is very important to clearly define the main requirements. These requirements heavily influence the resulting framework and its operation. This thesis has thus defined several requirements and recommendations for the presented interoperability framework. These requirements are aligned to the EIF to take into account aspects on the four levels of technical, semantic, procedural and legal interoperability. The following requirements and recommendations have been identified: scalability, autonomy, transparency, security and privacy, preservation of information, the use of open standards, reusing existing tools, components and technologies, multilingualism and an appropriate interoperability agreement. The design of an interoperability framework coupling heterogeneous systems naturally bears several challenges. This thesis discussed in detail potential challenges on the technical (protocol conversion, cryptography), semantic (evidences, signatures, authentication and identification) and the procedural level (addressing, fairness, timeliness).

In a next step, the thesis discussed in detail the proposed CMS interoperability concept. The conceptual model is aligned to the EIF resulting in a multilateral solution. The core of the framework is the EDG, which is based on the PEGS architectural model and aligned to the interoperability provisions of the IDA eLink concept and the PEPPOL BusDox network. For a better understanding, the thesis first discussed the bilateral case for the EDG, this means making two arbitrary systems interoperable. This included the detailed discussion of the technical, semantic and procedural gateway part and their duties. Then the thesis discussed the multilateral gateway approach by introducing the DGP as communication protocol of a virtual CMS and being able to carry common CEM and CMS aspects of today's systems and standards. To complete the discussion of the concept, the federated trust network using a TSL was introduced. This network connects EDGs of different CMS and automatically establishes implicit trust between entities of different systems.

Even if many procedural aspects of the concept have been introduced in the course of the conceptual discussion, the thesis has subsequently discussed in more detail the process flows of cross-border CMS message exchange. This includes both the discussion for dispatch and evidence messages. Three main phases of the cross-border delivery phase have been identified and discussed in detail: the message submission phase, the message translation phase and the message delivery phase. The message submission phase denotes the submission and delivery of a message from the sender to the sender's EDG. The message translation phase denotes the delivery phase between two EDGs including the translation and validation of domestic CMS message formats to the common DGP format. The message delivery phase denotes the phase of delivery from the recipient's EDG to the final recipient.

The presented concept and process model has been developed and elaborated by the author of this thesis in the course of the STORK LSP. SPOCS has taken up the concept and improved it in several aspects, including addressing, efficiency, design reuse, open standards and interoperability agreement. This thesis has discussed these improvements in detail (the author was heavily and actively involved in this improvement process). Even if some improvements concern procedural aspects like addressing, most of them are made on the technical and semantic layer refining the DGP. With the SPOCS ICP, a 2^{nd} generation interoperability protocol has been developed.

Both, STORK and SPOCS have deployed their interoperability framework to demonstrate its applicability in real environments and under real conditions. This thesis has discussed selected details of the implementation made in SPOCS. First, this concerns the development of the generic gateway, a component implementing generic aspects common to each gateway. This includes addressing, message- and security-related operations like the SOAP communication, signature handling or TSL operations. As part of the SPOCS project, the author has developed a gateway for the Austrian DDS. The thesis discussed in detail the concept, core components and process model of this gateway to illustrate the message submission and message delivery phase. The message translation phase is mainly carried out by the generic

gateway part. The SPOCS interoperability testing approach with unit, integration, system and system integration (plug) testing has also been discussed.

Even if this thesis mainly deals with interoperability Level 2, this means providing a cross-border CMS interoperability framework, Level 1 interoperability is reviewed as well. Therefore, this thesis also discussed how in the course of the STORK LSP the cross-border authentication framework has been integrated into several CMS to enable CEM for foreign citizens.

Finally, the work presented in this thesis has been evaluated in terms of requirements compliance. This means it has been discussed how the stated requirements and recommendations have been fulfilled and, if so, to what extend. Last not least, governance aspects, standardization of the ICP as ETSI REM standard, open issues like accounting and legal aspects have also been discussed.

12.7 Conclusions

The work presented in this thesis has developed a framework, which is able to make existing (and future) CMS interoperable. The focus was on a scalable architecture, which should be transparent so that existing systems remain untouched and autonomous. The framework is able to couple any kind of CMS on local, regional or national level and those provided by the industry.

The work started with a detailed overview and discussion of CEM security properties. In the past two decades, researchers have introduced and defined many security properties. Each of these properties has usually different flavors. Fairness may be strong, weak, true, light or probabilistic. TTPs may be inline, online or offline. The same applies to the properties of timeliness, communication channels or state storage. At the bottom line, as is also confirmed by other researchers, there is no common view in the research community on the essential security properties a CEM protocol has to provide. However, there can be observed a trend towards offline approaches having strong fairness. But are these kinds of protocols taken up by implementers and standard designers?

An answer to this question was found with a comprehensive survey of existing CMS and standards, which has assessed the CEM security properties actually applied in practice. The views of the research community and practitioners are not congruent and quite differ in some parts. Existing CMS are not aligned to newer optimistic (offline) design patterns applied by the research community. They rather follow the conceptual model of traditional postal security services. Inline TTPs and strong fairness are core properties in practice. Like within the research community, discordance about the provided non-repudiation services and evidences can also be found in practice. Most systems provide an NRD evidence, only in some systems, particularly in those with legal requirements, NRR evidences have to be signed by the recipient. There is also no agreement on the kind of transport protocol. Half of the assessed systems use e-mail architectures, whereas the other part relies on Web services technologies. At least for CMS established in Europe there is an agreement on the predominant use of cross-border capable signatures (AdES, QES) being compliant with the Signature Directive. An answer to this question was found with a comprehensive survey of existing CMS and standards, which has assessed the CEM security properties actually applied in practice. The views of the research community and practitioners are not congruent and quite differ in some parts. Existing CMS are not aligned to newer optimistic (offline) design patterns applied by the research community. They rather follow the conceptual model of traditional postal security services. Inline TTPs and strong fairness are core properties in practice. Like within the research community, discordance about the provided non-repudiation services and evidences can also be found in practice. Most systems provide an NRD evidence, only in some systems, particularly in those with legal requirements, NRR evidences have to be signed by the recipient. There is also no agreement on the kind of transport protocol. Half of the assessed systems use e-mail architectures, whereas the other part relies on Web services technologies. At least for CMS established in Europe there is an agreement on the predominant use of cross-border capable signatures (AdES, QES) being compliant with the Signature Directive.

Based on the assessment and evaluation of existing CMS and a deep requirements analysis, a concrete CMS interoperability concept has been developed. The proposed framework uses the core elements of a federated trust network of EDGs and the ICP (or DGP), which is a "lingua franca" for a common understanding of CEM protocol elements. The EDG concept as "entry" and "exit" point completely decouples each CMS from the interoperability network and thus provides a scalable and autonomous architecture. The ICP is generic enough to be able to couple arbitrary CMS and to provide a transparent coupling. Transparency is the only requirement, which cannot be fully fulfilled. This mainly results from the issue of addressing, a core and intrinsic messaging functionality. Addressing in today's CMS is quite different and SPOCS has tried to tackle this issue with a DNS-based approach using the accustomed e-mail addressing format. Even if half of existing systems are compatible with this format out of the box, others have to make adaptations. For example, this has become evident in the Austrian DDS where even with a virtual CMS address the main routing mechanism in the CLS had to be adapted. This has violated the transparency principle, but was needed for practical deployment.

Summarizing, the concept presented in this thesis has demonstrated the technical feasibility of a CMS interoperability framework meeting the stated requirements (transparency cannot be fulfilled to 100% in each case). The concept was also intensively tested within the LSP SPOCS. However, some aspects like accounting or a virtual directory for E2EE certificates remain open and should be tackled by some future work. Nevertheless, a future interoperability network, which is based on the work presented in this thesis, for example by relying on the recently published ETSI REM standard for SOAP-based systems, should employ an appropriate governance structure and interoperability agreement. In case of national CMS or e-Justice systems, this could be the EC. In case of CMS of postal services this could be the UPU. Nevertheless, a sound CMS interoperability framework, particularly in the European public sector, requires a legal framework backing the cross-border delivery of documents in administrative matters (which is currently still missing). This is where the European Community is in demand.

Appendix A

Process Model

This appendix illustrates all process models described in Chapter 8 in a higher resolution.

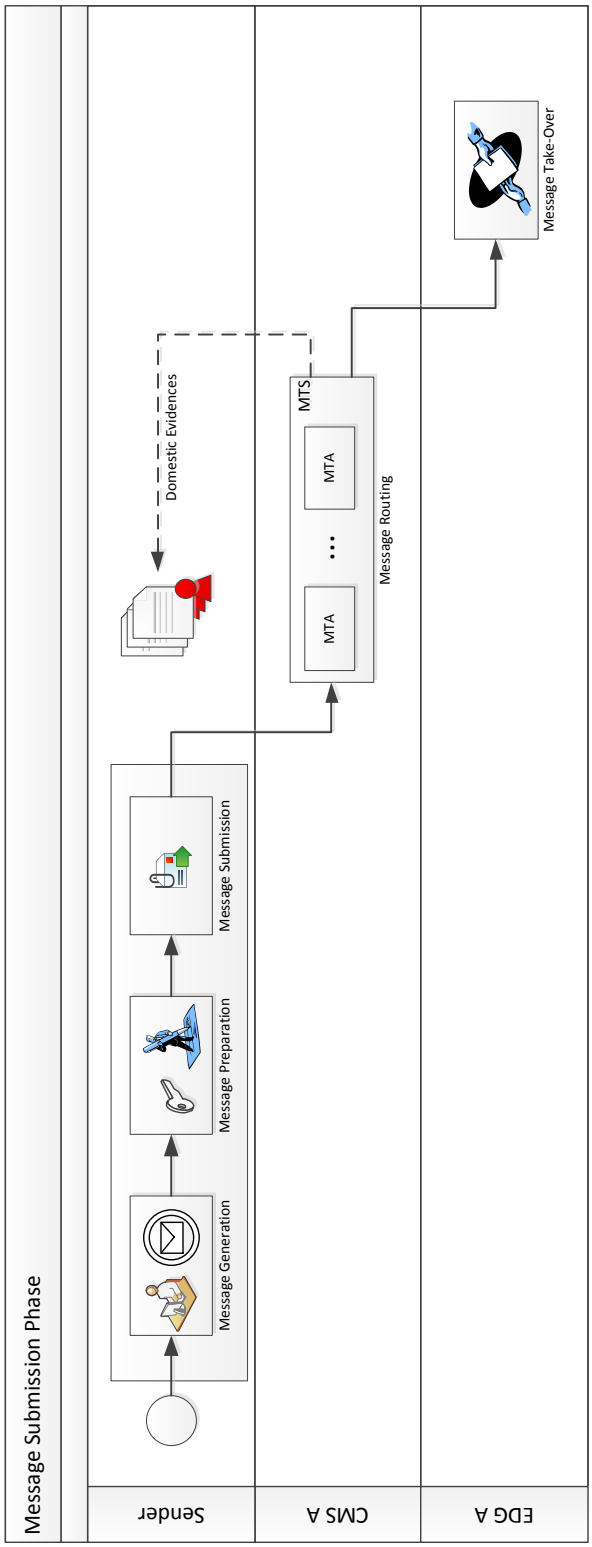

Figure A.1: Process details of the message submission phase.

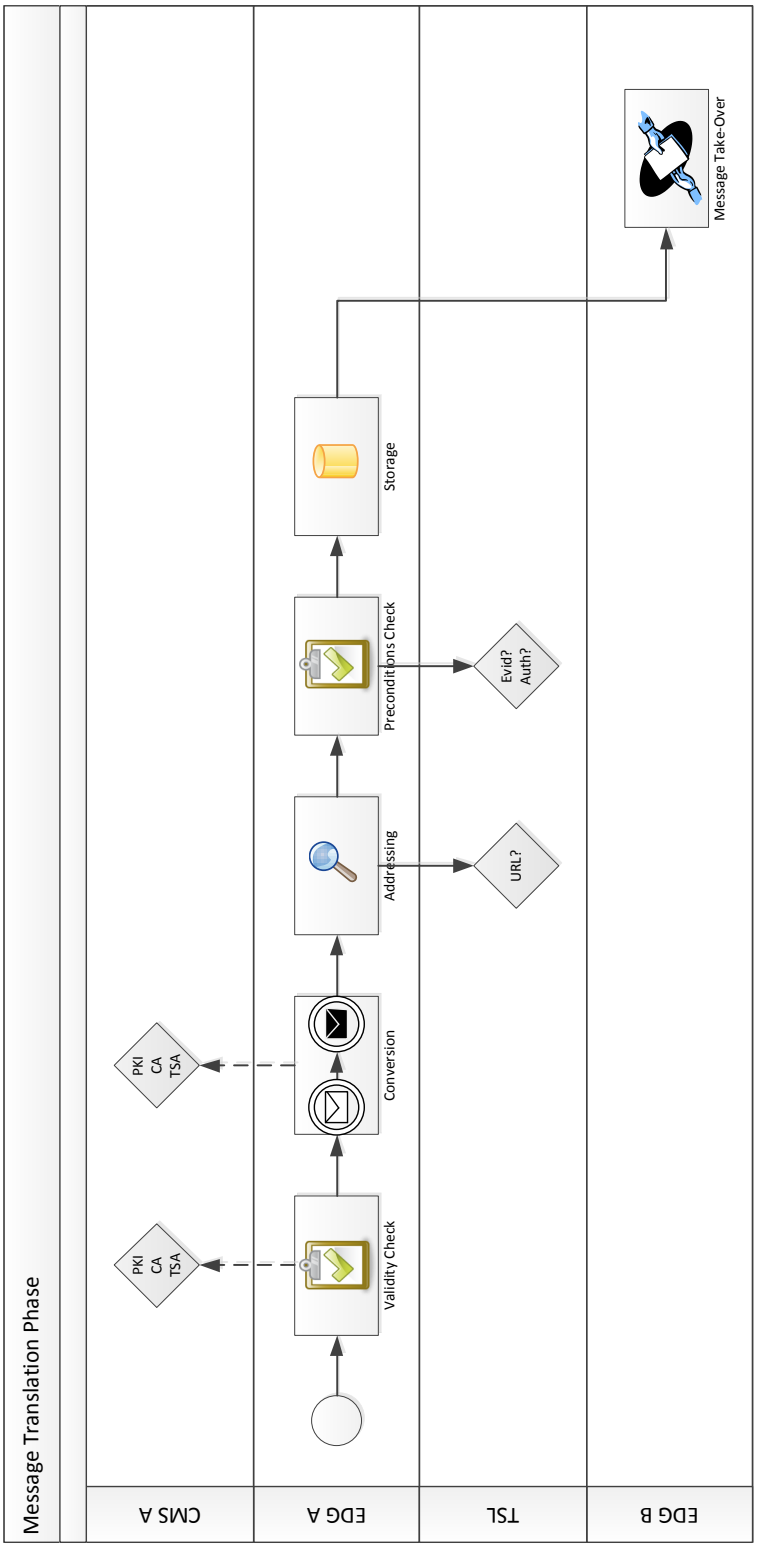

Figure A.2: Process details of the message translation phase.

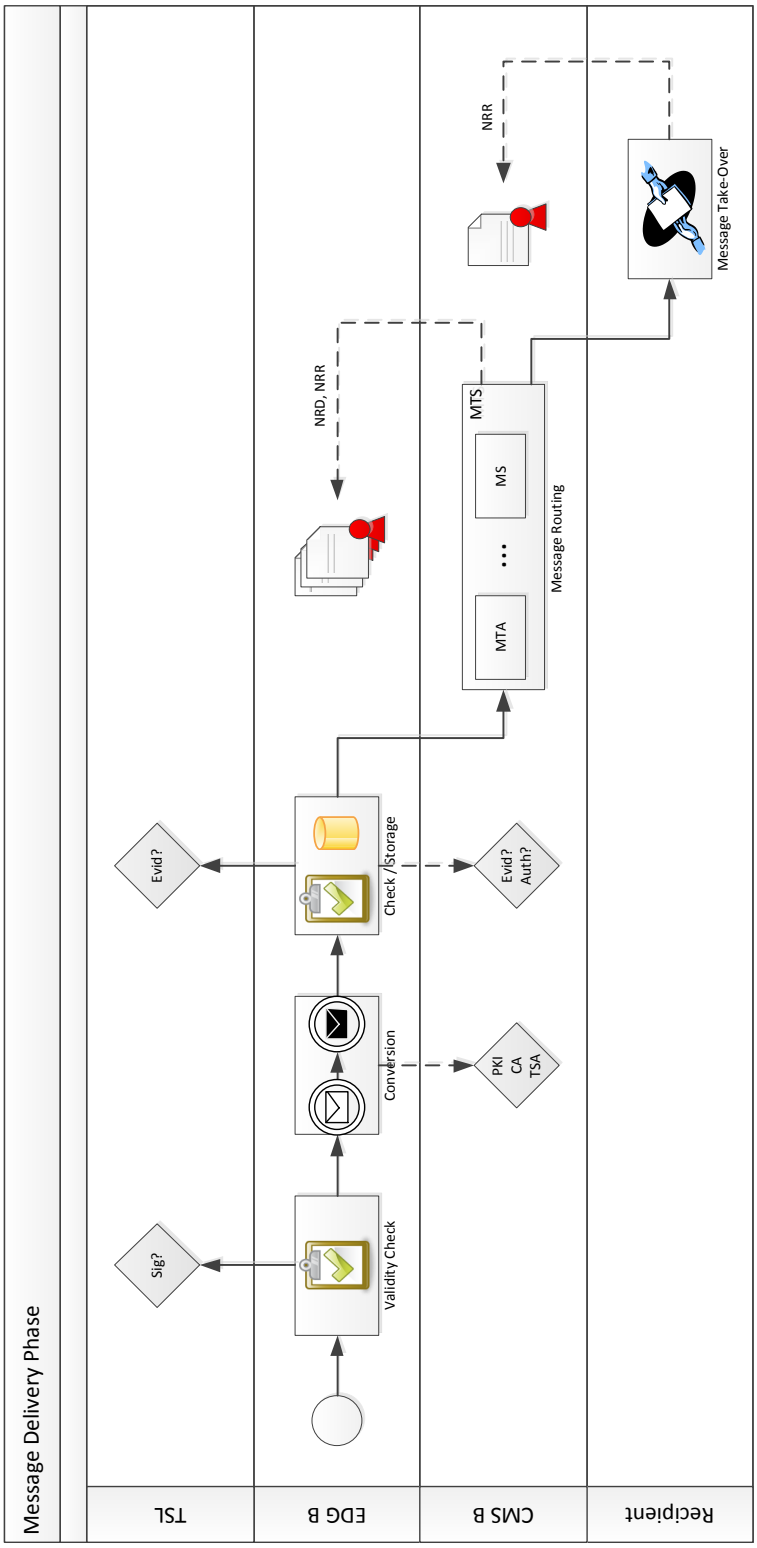

Figure A.3: Process details of the message delivery phase.

Appendix B

List of Definitions

Definition 1 *Non-Repudiation of Origin (NRO). A protocol provides non-repudiation of origin if and only if it gives evidence against the false denial of having originated the message.*

Definition 2 *Non-Repudiation of Receipt (NRR). A protocol provides non-repudiation of receipt if and only if it gives evidence against the false denial of having received the message.*

Definition 3 *Non-Repudiation of Submission (NRS). A protocol provides non-repudiation of submission if and only if it gives evidence against the false denial of having submitted the message.*

Definition 4 *Non-Repudiation of Delivery (NRD). A protocol provides non-repudiation of delivery if and only if it gives evidence against the false denial of having delivered the message.*

Definition 5 *Evidence transferability. Evidences are transferable if and only if they can be used independently by senders and recipients without the need to request input from other entities.*

Definition 6 *Strong fairness. A protocol fulfills strong fairness if and only if all entities get the expected items, or none of the entities gets what is expected.*

Definition 7 *Weak fairness. A protocol fulfills weak fairness if and only if just one entity gets the expected item, and the other party has proof of this situation.*

Definition 8 *True fairness. A protocol fulfills true fairness if and only if it fulfills fairness as defined in Definition 6, and in case of success, generated evidences are independent of how the protocol is executed.*

Definition 9 *Probabilistic fairness. A protocol is probably fair with a probability ϵ if and only if it fulfills fairness as defined in Definition 6 and the probability that a cheating party is in an advantageous position is $< \epsilon$.*

Definition 10 *Light fairness. A protocol fulfills light fairness if and only if sender and recipient get an NRR and an NRO evidence, respectively, or none of them gets an evidence.*

Definition 11 *Inline TTP. A TTP is said to be "inline" if it is involved in each protocol step.*

Definition 12 *Online TTP. A TTP is said to be "online" if it is involved in each protocol run but not in each protocol step.*

Definition 13 *Offline TTP. A TTP is said to be "offline" if it is only involved in a dispute resolution process.*

Definition 14 *Transparent TTP. A TTP is said to be "transparent" if it is not possible to decide whether an evidence was issued by the TTP itself or by some other involved entity.*

Definition 15 *Online Verifiability. A service is "on-line" verifiable when a user can immediately know whether the TTP misbehaved by checking the evidences received from the TTP. In case of problems the user can start a dispute to correct the situation.*

Definition 16 *Offline Verifiability. The verifiability of a security service is "off-line" when the evidences received from the TTP are not enough to know if it has been provided properly or not. But if a dispute arises between the parties involved in the protocol, then the evidences can be used to prove whether the TTP misbehaved.*

Definition 17 *Neutral TTP. A TTP is said to be "neutral" if its correct operation is not conditioned by its knowledge of the message content.*

Definition 18 *Operational channel. A communication channel is said to be "operational" if the transmitted data arrives after a finite and known amount of time.*

Definition 19 *Unreliable channel. A communication channel is said to be "unreliable" if transmitted data may get permanently lost.*

Definition 20 *Resilient channel. A communication channel is said to be "resilient" if the transmitted data arrives after a finite and unknown amount of time.*

Definition 21 *Timeliness. A protocol fulfills the timeliness property if and only if honest entities can stop the protocol execution in a finite amount of time while keeping fairness.*

Definition 22 *Synchronous timeliness. A CEM protocol is said to respect synchronous timeliness if all honest entities are able to terminate the protocol in a finite and known amount of time without loosing fairness.*

Definition 23 *Asynchronous timeliness. A CEM protocol is said to respect asynchronous timeliness if all honest entities are able to terminate the protocol at any time without loosing fairness.*

Definition 24 *Strong stateless. A TTP is said to be "strong stateless" if and only if it never needs to store any data to accomplish its tasks.*

Definition 25 *Weak stateless. A TTP is said to be "weak stateless" if and only if it needs to store data for a finite and known amount of time to accomplish its tasks.*

Definition 26 *Weak stateful. A TTP is said to be "weak stateful" if and only if it needs to store data for a finite and unknown amount of time to accomplish its tasks.*

Definition 27 *Strong stateful. A TTP is said to be "strong stateful" if and only if it needs to store data forever to accomplish its tasks.*

Definition 28 *Confidentiality. Property that information is not made available or disclosed to unauthorized individuals, entities, or processes*

Definition 29 *Integrity. Property of protecting the accuracy and completeness of assets*

Definition 30 *Authenticity. Property that an entity is what it claims to be.*

Definition 31 *Interoperability Level 0. A recipient of Member State A registers with a CMS of Member State A, for example by using an eID. As a result, the recipient is able to receive messages from senders of Member State A through the CMS of Member State A. The sender receives in exchange an NRD or NRR evidence from the CMS of Member State A.*

Definition 32 *Interoperability Level 1. A recipient of Member State B registers with a CMS of Member State A, for example by using an eID. As a result, the recipient is able to receive messages from senders of Member State A through the CMS portal of Member State A. The sender receives in exchange an NRD or NRR evidence from the CMS of Member State A.*

Definition 33 *Interoperability Level 2. A recipient of Member State C registers with a CMS of Member State B, for example by using an eID. As a result, the recipient is able to receive messages from senders of any participating Member State (for example A) through the CMS of Member State B. The sender receives in exchange an NRD or NRR evidence from the CMS of Member State B. The envelope content of messages, for example a document, must not be altered on its way from the sender to the recipient.*

Appendix C

List of Requirements and Recommendations

Requirement 1 *The CMS interoperability framework must use a multilateral solution and support administrative scalability.*

Requirement 2 *The CMS interoperability framework must support the loose coupling of autonomous systems.*

Requirement 3 *The CMS interoperability framework must be able to transparently couple different systems.*

Requirement 4 *The CMS interoperability framework must respect security and privacy provisions of single systems and provide an overarching framework with well-defined security policies.*

Requirement 5 *The CMS interoperability framework must support the generation of a customizable audit trail for cross-border transactions.*

Requirement 6 *The CMS interoperability framework must use open standards to facilitate autonomy and scalability.*

Requirement 7 *The CMS interoperability framework must support multilingualism for control information on the message level.*

Recommendation 1 *The CMS interoperability framework should reuse existing components to ensure a faster and cheaper development by relying on best-practice and components tested for reliability and robustness.*

Recommendation 2 *The CMS interoperability framework should have an interoperability agreement regulating all cross-border relevant aspects.*

Bibliography

Abadi, Martin, Neal Glew, Bill Horne, and Benny Pinkas [2002]. *Certified Email with a Light On-line Trusted Third Party : Design and Implementation*. In *Proceedings of the 11th International World Wide Web Conference*, pages 387–395. ACM Press. (Cited on page 35.)

Alcalde-Moraño, Joaquin, Jorge López Hernández-Ardieta, Adrian Johnston, Daniel Martinez, Bernd Zwattendorfer, Marc Stern, and John Heppe [2010]. *STORK Deliverable D5.8.2b Interface Specification*. (Cited on pages 194 and 195.)

Allman, E [2004]. *RFC 3886 - An Extensible Message Format for Message Tracking Responses*. (Cited on page 22.)

Allman, E and T Hansen [2004]. *RFC 3885 - SMTP Service Extension for Message Tracking*. (Cited on page 22.)

Apitzsch, Jörg [2007]. *Mechanismen zur Nachweisbarkeit der Kommunikation bei OSCI Transport*. *Datenschutz und Datensicherheit - DuD*, 31(10), pages 744–746. ISSN 1614-0702. (Cited on page 66.)

Apitzsch, Jörg, Luca Boldrin, and Arne Tauber [2010a]. *Specifications for interoperable access to eDelivery and eSafe systems - Appendix 3: eDelivery Interconnect Protocol and Gateway detailed Specification*. (Cited on page 154.)

Apitzsch, Jörg, Olaf Rohstock, Lars Thölken, Luca Boldrin, Bernd Martin, Stefanie Rieger, Michael Seeger, Arne Tauber, and Peter Worofka [2010b]. *Specifications for interoperable access to eDelivery and eSafe systems*. (Cited on page 154.)

Asokan, N, M Schunter, and M Waidner [1997]. *Optimistic protocols for fair exchange*. In *CCS '97 Proceedings of the 4th ACM conference on Computer and communications security*, pages 7–17. (Cited on page 36.)

Asokan, N., V. Shoup, and M. Waidner [1998a]. *Optimistic fair exchange of digital signatures*. In *Advances in Cryptology - Proceedings of Eurocrypt'981*, pages 591–606. ISSN 07338716. (Cited on page 36.)

Asokan, N, Victor Shoup, and Michael Waidner [1998b]. *Asynchronous protocols for optimistic fair exchange*. In *Proceedings 1998 IEEE Symposium on Security and Privacy*, pages 86–99. RZ 2976 (#93022), {IEEE} Computer Society, Technical Committee on Security and Privacy. ISBN 0818683864. ISSN 15407993. (Cited on pages 31 and 36.)

Ateniese, Giuseppe and Michael T Goodrich [2001]. *TRICERT : A Distributed Certified E-Mail Scheme*. In *Proceedings of Network and Distributed System Security Symposium*. (Cited on page 36.)

Bahreman, Alireza and J.D. Tygar [1994]. *Certified electronic mail*. In *Proceedings of the Internet Society Symposium on Network and Distributed System Security*, pages 3–19. ISSN 01674048. (Cited on page 34.)

Bao, F, Robert H. Deng, and W Mao [1998]. *Efficient and practical fair exchange protocols with off-line TTP*. In *IEEE Symposium on Security and Privacy*. (Cited on page 36.)

Bartel, Mark, John Boyer, Barb Fox, Brian LaMacchia, and Ed Simon [2008]. *XML Signature Syntax and Processing (Second Edition)*. http://www.w3.org/TR/xmldsig-core/. (Cited on page 67.)

Barton, John J., Satish Thatte, and Hendrik Frystyk Nielsen [2001]. *SOAP Messages with Attachments*. http://www.w3.org/TR/SOAP-attachments.html. (Cited on page 50.)

Ben-or, Michael, Oded Goldreich, Silvio Micali, and Ronald L. Rivest [1990]. *A fair protocol for signing contracts*. *IEEE Transaction on Information Theory*, 36(1), pages 40–46. (Cited on pages 32 and 33.)

Berbecaru, Diana, Joaquin Alcalde-Moraño, Jorge López Hernández-Ardieta, Renato Portela, and Ricardo Ferreira [2010a]. *STORK Deliverable D5.8.2c Software Design*. (Cited on page 195.)

Berbecaru, Diana, Eva Jorquera, Joaquin Alcalde-Moraño, Renato Portela, Wolfgang Bauer, Bernd Zwattendorfer, Jan Eichholz, and Tim Schneider [2010b]. *STORK Deliverable D5.8.2a Software Architecture Design*. (Cited on page 194.)

Blum, Manuel [1983]. *How to exchange (secret) keys*. *ACM Transactions on Computer Systems*, 1(2), pages 175–193. ISSN 07342071. (Cited on page 32.)

Bosak, Jon, Tim McGrath, and G. Ken Holman [2006]. *Universal Business Language v2.0*. (Cited on page 88.)

Box, Don, David Ehnebuske, Gopal Kakivaya, Andrew Layman, Noah Mendelsohn, Henrik Frystyk Nielsen, Satish Thatte, and Dave Winer [2000]. *Simple Object Access Protocol (SOAP) 1.1*. http://www.w3.org/TR/2000/NOTE-SOAP-20000508/. (Cited on page 127.)

BSI [2011]. *Technische Richtlinie De-Mail*. (Cited on page 54.)

Bundesrepublik Deutschland [2005]. *Zivilprozessordnung*. (Cited on page 9.)

Callas, J, L Donnerhacke, H Finney, D Shaw, and R Thayer [2007]. *RFC 4880 - OpenPGP Message Format*. (Cited on page 20.)

Capgemini [2004]. *Architecture for delivering pan-European e-Government services*. (Cited on pages 81 and 115.)

Centner, Martin, Clemens Orthacker, and Wolfgang Bauer [2009]. *Minimal-Footprint Middleware for the Creation of Qualified Signatures*. In *Proceedings of the 6th International Conference on Web Information Systems and Technologies*, pages 64–69. (Cited on page 197.)

CEN/TS [2010a]. *Postal Services - Hybrid Mail - Part 1: Secured electronic postal services (SePS) interface specification - Concepts, schemas and operations*. (Cited on page 65.)

CEN/TS [2010b]. *Postal Services - Hybrid Mail - Part 2: Secured electronic postal services (SePS) interface specification - ECPM Service*. (Cited on page 65.)

Chen, Liqun [1998]. *Efficient Fair Exchange with Verifiable Confirmation of Signatures*. In *Advances in Cryptology - ASIACRYPT 98*, pages 286–299. (Cited on page 36.)

Chinnici, Roberto, Jean-Jacques Moreau, Arthur Ryman, and Sanjiva Weerawarana [2007]. *Web Services Description Language (WSDL) Version 2.0 Part 1: Core Language*. http://www.w3.org/TR/wsdl20/. (Cited on page 66.)

Cimato, Stelvio, Clemente Galdi, Raffaella Giordano, Barbara Masucci, and Gildo Tomasco [2005]. *Design and Implementation of an Inline Certified E-mail Service*. In Desmedt, Yvo G., Huaxiong Wang, Yi Mu, and Yongqing Li (Editors), *Cryptology and Network Security, 4th International Conference, CANS 2005*, *Lecture Notes in Computer Science*, volume 3810, pages 186–199. Springer Berlin Heidelberg, Berlin, Heidelberg. ISBN 978-3-540-30849-2. (Cited on page 34.)

Coffey, Tom and Puneet Saidha [1996]. *Non-repudiation with mandatory proof of receipt*. *ACM SIGCOMM Computer Communication Review*, 26(1), pages 6–17. ISSN 01464833. (Cited on page 34.)

Cooper, D, S Santesson, S Farrell, S Boeyen, R Housley, and W Polk [2008]. *RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. (Cited on pages 20 and 27.)

Council of Europe [1977]. *European Convention on the Service abroad of Documents Relating to Administrative Matters*. (Cited on page 213.)

Council of the European Union and European Commission [2000]. *eEurope - An Information Society for All - Action Plan*. (Cited on page 77.)

Cox, Benjamin, J D Tygar, and Marvin Sirbu [1995]. *NetBill Security and Transaction Protocol*. In *Proceedings of the first USENIX Workshop of Electronic Commerce*, pages 77–88. July. (Cited on page 35.)

Davis, Doug, Anish Karmarkar, Gilbert Pilz, Steve Winkler, and Ümit Yalçinalp [2009]. *Web Services Reliable Messaging (WS-ReliableMessaging) Version 1.2*. (Cited on page 68.)

Davis, Doug, Ashok Malhotra, Katy Warr, and Wu Chou [2010]. *Web Services Transfer (WS-Transfer)*. `http://www.w3.org/TR/2010/WD-ws-transfer-20100330/`. (Cited on page 69.)

DeMillo, Richard A. and Michael Merritt [1983]. *Protocols for Data Security*. *Computer*, 16(2), pages 39–51. ISSN 0018-9162. (Cited on page 35.)

Deng, Robert H., Li Gong, Aurel a. Lazar, and Weiguo Wang [1996]. *Practical protocols for certified electronic mail*. *Journal of Network and Systems Management*, 4(3), pages 279–297. ISSN 1064-7570. (Cited on page 35.)

DGME [2006]. *A Technical Reference for the PRESTO protocol*. (Cited on page 69.)

Dietrich, Jens and Jutta Keller-Herder [2010]. *De-Mail - verschlüsselt, authentisch, nachweisbar*. *Datenschutz und Datensicherheit - DuD*, 34(5), pages 299–301. ISSN 1614-0702. (Cited on page 54.)

Engeljehringer, Wolfgang [2004]. *Das Projekt e-Recht in Österreich: eine Erfolgsstory*. Technical Report, Parlamentsdirektion Kompetenzzentrum. (Cited on page 44.)

ETSI [2007]. *ETSI TR 102 605 - Electronic Signatures and Infrastructures (ESI); Registered E-Mail*. (Cited on page 124.)

ETSI [2009]. *ETSI TS 102 231 - Electronic Signatures and Infrastructures (ESI); Provision of harmonized Trust-service status information*. (Cited on pages 63, 125 and 135.)

ETSI [2010a]. *Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signatures (XAdES)*. (Cited on page 195.)

ETSI [2010b]. *ETSI TS 102 640-1 - Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 1: Architecture*. (Cited on page 63.)

ETSI [2010c]. *ETSI TS 102 640-2 - Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 2: Data requirements, Formats and Signatures for REM*. (Cited on pages 63, 120, 134 and 156.)

ETSI [2010d]. *ETSI TS 102 640-3 - Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 3: Information Security Policy Requirements for REM Management Domains*. (Cited on pages 63 and 210.)

ETSI [2010e]. *ETSI TS 102 640-4 - Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) Part 4: REM-MD Conformance Profiles*. (Cited on page 63.)

ETSI [2010f]. *ETSI TS 102 640-5 - Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 5: REM-MD Interoperability Profiles*. (Cited on page 64.)

ETSI [2011]. *Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 6: Interoperability Profiles; Sub-part 3: REM-MD SOAP Binding Profile*. (Cited on page 211.)

European Commission [2000]. *eEurope - An Information Society for All - Communication on a Commission Initiative for the Special European Council of Lisbon, 23 and 24 March 2000*. (Cited on page 77.)

European Commission [2002]. *eEurope 2005: An information society for all - An Action Plan to be presented in view of the Sevilla European Council*. (Cited on page 77.)

European Commission [2003]. *Linking up Europe: the Importance of Interoperability for eGovernment Services*. (Cited on page 76.)

European Commission [2004a]. *Architecture Guidelines - For Trans-European Telematics Networks for Administrations*. (Cited on page 80.)

European Commission [2004b]. *European Interoperability Framework for pan-European e-Government Services*. (Cited on pages 81, 101, 106, 107 and 109.)

European Commission [2005a]. *i2010 - A European Information Society for growth and employment*. (Cited on page 77.)

European Commission [2005b]. *Information Society Benchmarking Report*. (Cited on page 77.)

European Commission [2006]. *i2010 eGovernment Action Plan: Accelerating eGovernment in Europe for the Benefit of All*. (Cited on pages 78 and 79.)

European Commission [2007]. *Proposal for a multi-level authentication mechanism and a mapping of existing authentication mechanisms*. (Cited on page 121.)

European Commission [2009a]. *Commission Decision of 16 October 2009 setting out measures facilitating the use of procedures by electronic means through the 'points of single contact' under Directive 2006/123/EC of the European Parliament and of the Council on services in the internal*. (Cited on page 135.)

European Commission [2009b]. *EIIS - European Interoperable Infrastructure Service - Study on Potential Reuse of System Components*. (Cited on page 82.)

European Commission [2009c]. *Smarter, Faster, Better eGovernment - 8th Benchmark Measurement*. (Cited on page 78.)

European Commission [2009d]. *Study on eID Interoperability for PEGS: Update of Country Profiles Analysis & assessment report*. (Cited on page 82.)

European Commission [2009e]. *Study on Mutual Recognition of eSignatures: update of Country Profiles Analysis & assessment report*. (Cited on page 83.)

European Commission [2009f]. *Supporting the European Interoperability Strategy Elaboration*. (Cited on page 81.)

European Commission [2010a]. *A Digital Agenda for Europe*. (Cited on pages 78 and 87.)

European Commission [2010b]. *European Interoperability Framework (EIF) for European public services*. (Cited on pages 75, 81, 99, 112 and 113.)

European Commission [2010c]. *Europe's Digital Competitiveness Report 2010*. (Cited on page 78.)

European Commission [2010d]. *The European eGovernment Action Plan 2011-2015 - Harnessing ICT to promote smart, sustainable & innovative Government*. (Cited on pages 79 and 95.)

European Dynamics SA [2004]. *IDA eLink Specification*. (Cited on pages 81 and 114.)

European Union [2007]. *Treaty of Lisbon - Amending the Treaty on European Union and the Treaty establishing the European Community (2007/C 306/01)*. (Cited on page 216.)

European Union [2008]. *Consolidated Version of the Treaty of the European Union*. (Cited on page 75.)

European Union [2009]. *Multi-annual European e-Justice Action Plan 2009-2013*. (Cited on page 92.)

Ferrer-Gomilla, Josep Lluis, Jose a. Onieva, Magdalena Payeras, and Javier Lopez [2010]. *Certified electronic mail: Properties revisited*. *Computers & Security*, 29(2), pages 167–179. ISSN 01674048. (Cited on pages 23, 24, 27, 31, 35, 36, 37, 38, 41 and 42.)

Franklin, Matthew K. and Michael K. Reiter [1997]. *Fair exchange with a semi-trusted third party (extended abstract)*. *Proceedings of the 4th ACM conference on Computer and communications security - CCS '97*, pages 1–5. (Cited on pages 35 and 36.)

Fremantle, Paul [2009a]. *Lightweight Message Exchange Profile (LIME)*. (Cited on page 69.)

Fremantle, Paul [2009b]. *Secure Trusted Asynchronous Reliable Transport (START)*. (Cited on page 69.)

Füll, Martin [2005]. *Potenzial elektronischer Zustellung in Österreich*. Technical Report, input marketing & consulting. (Cited on page 44.)

Gennai, Francesco, Loredana Martusciello, and Marina Buzzi [2005]. *A Certified Email System for the Public Administration in Italy*. In Nunes, Miguel Baptista and Pedro Isaía (Editors), *Proceedings of the IADIS International Conference on WWW/Internet*, pages 143–147. (Cited on page 52.)

González-Deleito, Nicolás [2005]. *No Author-Based Selective Receipt in Certified Email with Tight Trust Requirements*. In *Proceedings of the 2005 conference on Applied Public Key Infrastructure: 4th International Workshop: IWAP 2005*, pages 78–91. ISBN 1-58603-550-9. (Cited on page 28.)

Gudgin, Martin, Marc Hadley, Noah Mendelsohn, Jean-Jacques Moreau, Henrik Frystyk Nielsen, Anish Karmarkar, and Yves Lafon [2007]. *SOAP Version 1.2 Part 1: Messaging Framework (Second Edition)*. `http://www.w3.org/TR/soap12-part1/`. (Cited on page 156.)

Gudgin, Martin, Marc Hadley, and Tony Rogers [2006]. *Web Services Addressing 1.0 - Core*. `http://www.w3.org/TR/ws-addr-core/`. (Cited on page 156.)

Gudgin, Martin, Noah Mendelsohn, Mark Nottingham, and Hervé Ruellan [2005]. *SOAP Message Transmission Optimization Mechanism*. `http://www.w3.org/TR/soap12-mtom/`. (Cited on page 127.)

Gürgens, Sigrid, Carsten Rudolph, and Holger Vogt [2005]. *On the security of fair non-repudiation protocols*. *International Journal of Information Security*, 4(4), pages 253–262. ISSN 1615-5262. (Cited on page 36.)

Hallam-Baker, Philip and Shivaram H. Mysore [2001]. *XML Key Management Specification (XKMS 2.0)*. http://www.w3.org/TR/xkms2/. (Cited on page 89.)

Hansen, T [2004a]. *RFC 3887 - Message Tracking Query Protocol*. (Cited on page 22.)

Hansen, T [2004b]. *RFC 3888 - Message Tracking Model and Requirements*. (Cited on page 21.)

Hansen, T and G Vaudreuil [2004]. *RFC 3798 - Message Disposition Notification*. (Cited on page 21.)

Harding, T, R Drummond, and C Shih [2002]. *RFC 3335 - MIME-based Secure Peer-to-Peer Business Data Interchange over the Internet*. (Cited on page 21.)

Harding, T and R Scott [2007]. *RFC 4823 - FTP Transport for Secure Peer-to-Peer Business Data Interchange over the Internet*. (Cited on page 21.)

Heppe, John [2010]. *STORK Deliverable D5.8.2 Technical Design for PEPS, MW models and interoperability*. (Cited on page 194.)

Hoffman, P [1999]. *RFC 2634 - Enhanced Security Services for S/MIME*. (Cited on page 22.)

Housley, R [2009]. *RFC 5652 - Cryptographic Message Syntax (CMS)*. (Cited on pages 20 and 53.)

Hulsebosch, B, G Lenzini, and H Eertink [2009]. *STORK Deliverable D2.3 Quality authenticator scheme*. (Cited on pages 85 and 121.)

Il Presidente del Consiglio dei Ministeri [2009]. *Decreto del presidente del consiglio dei ministri 6 maggio 2009 - Disposizioni in materia di rilascio e di uso della casella di posta elettronica certificata assegnata ai cittadini*. (Cited on page 52.)

Il Presidente della Repubblica [2005a]. *Decreto del presidente della repubblica 11 febbraio 2005, n.68 - Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della legge 16 gennaio 2003, n. 3.* (Cited on page 52.)

Il Presidente della Repubblica [2005b]. *Decreto legislativo 7 marzo 2005, n. 82 pubblicato in G.U. del 16 maggio 2005, n. 112 - S.O. n. 93 "Codice dell'amministrazione digitale"*. (Cited on page 52.)

Imamura, Takeshi, Blair Dillaway, and Ed Simon [2002]. *XML Encryption Syntax and Processing*. http://www.w3.org/TR/xmlenc-core/. (Cited on page 119.)

ISO [1989]. *ISO 7498-2 - Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture*. (Cited on page 25.)

ISO [2006]. *International Standard ISO 3166-1, Codes for the representation of names of countries and their subdivisions*. (Cited on pages 6, 129 and 132.)

ISO/IEC [1997]. *ISO/IEC 10181-4 - Information technology - open systems interconnection - security frameworks for open systems: non-repudiation framework*. (Cited on page 25.)

ISO/IEC [2003a]. *ISO/IEC 10021-1 - Information technology – Message Handling Systems (MHS) – Part 1: System and service overview*. (Cited on page 16.)

ISO/IEC [2003b]. *ISO/IEC 10021-2 - Information technology – Message Handling Systems (MHS): Overall architecture*. (Cited on page 16.)

ISO/IEC [2005a]. *ISO/IEC 27001 - Information technology – Security techniques – Information security management systems – Requirements*. (Cited on pages 63, 72 and 210.)

ISO/IEC [2005b]. *ISO/IEC 27002 - Information technology – Security techniques – Code of practice for information security management*. (Cited on page 63.)

ISO/IEC [2008]. *ISO/IEC 9594-1 - Information technology – Open Systems Interconnection – The Directory: Overview of concepts, models and services*. (Cited on page 18.)

ISO/IEC [2009a]. *ISO/IEC 13888-1 - Information technology - Security techniques - Non-repudiation - Part 1: General*. (Cited on pages 25, 26 and 29.)

ISO/IEC [2009b]. *ISO/IEC 13888-3 - Information technology - Security techniques - Non-repudiation - Part 3: Mechanisms using asymmetric techniques*. (Cited on page 26.)

ISO/IEC [2009c]. *ISO/IEC 27000 - Information technology - Security techniques - Information security management systems - Overview and vocabulary*. (Cited on pages 39 and 40.)

ISO/IEC [2010]. *ISO/IEC 13888-2 - Information technology - Security techniques - Non-repudiation - Part 2: Mechanisms using symmetric techniques*. (Cited on pages 26 and 27.)

ISO/TS [2005]. *Electronic Business Extensible Markup Language (ebXML) - Part 5: ebXML Core Components Technical Specification, Version 2.01(ebCCTS)*. (Cited on page 129.)

ITU-T [1988]. *X.400 - Message handling system and service overview*. (Cited on pages 15, 16, 18 and 26.)

ITU-T [1996]. *X.813 - Information Technology - Open Systems Interconnection - Security Frameworks in Open Systems: Non-repudiation Framework*. (Cited on page 25.)

ITU-T [1999a]. *X.402 - Message Handling Systems: Overall Architecture*. (Cited on pages 16 and 18.)

ITU-T [1999b]. *X.411 - Message Handling Systems: Message Transfer System: Abstract Service Definition und Procedures*. (Cited on page 17.)

ITU-T [1999c]. *X.413 - Message Handling Systems: Message Store: Abstract Service definition*. (Cited on page 17.)

ITU-T [2001]. *E.123 - Series E: Overall Network Operation, Telephone Service, Service Operation and Human Factors*. (Cited on page 129.)

John, Cowan and Richard Tobin [2004]. *XML Information Set (Second Edition)*. `http://www.w3.org/TR/xml-infoset/`. (Cited on page 156.)

John, Richard R. [1998]. *Spreading the News - the American Postal System from Franklin to Morse*. Harvard University Press. (Cited on page 9.)

Joyce, Herbert [1893]. *The History of the Post Office from Its Establishment Down to 1836*. Richard Bentley & Son, 460 pages. (Cited on page 8.)

Klensin, J [2001]. *RFC 2821 - Simple Mail Transfer Protocol*. (Cited on page 53.)

Knall, Thomas, Arne Tauber, Thomas Zefferer, Bernd Zwattendorfer, Arnaldur Axfjord, and Haraldur Bjarnson [2011]. *Secure and Privacy-preserving Cross-border Authentication: the STORK Pilot "SaferChat"*. In *Proceedings of the Conference on Electronic Government and the Information Systems Perspective (EGOVIS 2011)*, pages 94–106. (Cited on page 87.)

Koulolias, Vasilis, Athanasios Kountzeris, Alberto Crespo, Herbert Leitold, Bernd Zwattendorfer, and Marc Stern [2011]. *STORK e-Privacy and Security*. In *Proceedings of 5th International Conference on Network and System Security (NSS 2011)*, pages 234–238. (Cited on page 190.)

Kremer, Steve and Olivier Markowitch [2000]. *Optimistic non-repudiable information exchange*. In *21st Symposium on Information Theory in Benelux*, pages 139–146. (Cited on page 36.)

Kremer, Steve and Olivier Markowitch [2001]. *Selective Receipt in Certified E-mail*. In *INDOCRYPT '01 Proceedings of the Second International Conference on Cryptology in India: Progress in Cryptology*, pages 136–148. ISBN 3-540-43010-5. (Cited on page 28.)

Kremer, Steve, Olivier Markowitch, and Jianying Zhou [2002]. *An intensive survey of fair non-repudiation protocols*. *Computer Communications*, 25(17), pages 1606–1621. ISSN 01403664. (Cited on pages 24, 31 and 36.)

Lapp, Thomas [2009]. *Brauchen wir De-Mail und Bürgerportale? Datenschutz und Datensicherheit - DuD*, 33(11), pages 651–655. ISSN 1614-0702. (Cited on page 55.)

Lechtenbörger, Jens [2010]. *Zur Sicherheit von De-Mail. Datenschutz und Datensicherheit - DuD,*, 35(4), pages 268–269. (Cited on page 55.)

Leitold, Herbert [2011]. *Challenges of eID Interoperability: The STORK Project*. In Fischer-Hübner, Simone, Penny Duquenoy, Marit Hansen, Ronald Leenes, and Ge Zhang (Editors), *Privacy and Identity Management for Life - IFIP Advances in Information and Communication Technology*, *IFIP Advances in Information and Communication Technology*, volume 352, pages 144–150. Springer Berlin Heidelberg, Berlin, Heidelberg. ISBN 978-3-642-20768-6. (Cited on pages 86 and 190.)

Leitold, Herbert, Arno Hollosi, and Reinhard Posch [2002]. *Security Architecture of the Austrian Citizen Card Concept*. In *18th Annual Computer Security Applications Conference (ACSAC 2002)*, pages 391–402. (Cited on page 49.)

Leitold, Herbert and Bernd Zwattendorfer [2010]. *STORK: Architecture, Implementation and Pilots*. In *ISSE 2010 Securing Electronic Business Processes: Highlights of the Information Security Solutions Europe 2010 Conference*, pages 131–142. (Cited on pages 86 and 190.)

Levinson, E [1997]. *RFC 2111 - Content-ID and Message-ID Uniform Resource Locators*. (Cited on page 127.)

Lockhart, Hal, Steve Andersen, Jeff Bohren, Yakov Sverdlov, Maryann Hondo, Hiroshi Maruyama, Anthony Nadalin, Nataraj Nagaratnam, Toufic Boubez, K Scott Morrison, Chris Kaler, Arun Nanda, Don Schmidt, Doug Walters, Hervey Wilson, Lloyd Burch, Doug Earl, Siddharth Baja, and Hemma Prafullchandra [2006]. *Web Services Federation Language (WS-Federation)*. (Cited on page 66.)

MAAWG [2011]. *Messaging Anti-Abuse Working Group (MAAWG) - Email Metrics Program: The Network Operator's Perspective - Report #14 - Third and Fourth Quarter 2010*. Technical Report, Messaging Anti-Abuse Working Group (MAAWG). `http://www.maawg.org/sites/maawg/files/news/MAAWG_2010_Q3Q4_Metrics_Report_14.pdf`. (Cited on page 45.)

Majava, Jarkko and Hans Graux [2007]. *Common specifications for eID interoperability in the eGovernment context*. (Cited on page 191.)

Markowitch, Olivier and Steve Kremer [2001]. *An Optimistic Non-repudiation Protocol with Transparent Trusted Third Party*. *Proceedings of the 4th International Conference ISC 2001*, 2200, pages 363–378. (Cited on page 36.)

Markowitch, Olivier and Yves Roggeman [1999]. *Probabilistic Non-Repudiation without Trusted Third Party*. In *Proceedings of 1999 Conference on Security in Communication Networks*. (Cited on pages 32 and 33.)

Markowitch, Olivier and Shahrokh Saeednia [2002]. *Optimistic Fair Exchange with Transparent Signature Recovery*. In *Proceedings of the 5th International Conference on Financial Cryptography*, pages 339–350. ISBN 3-540-44079-8. (Cited on page 36.)

Maseberg, Sönke, Matthias Intemann, and Ingo Schumann [2008]. *Die Virtuelle Poststelle des Bundes*. *Datenschutz und Datensicherheit - DuD*, 32(2), pages 117–122. ISSN 1614-0702. (Cited on page 66.)

McMillan, P [2001]. *Hybrid mail - from a print service to e-messaging*. In *Proceedings of the International Conference on Mail Technology: evolution to e-revolution*, pages 121–131. (Cited on pages 11 and 12.)

Melnikov, A [2003]. *RFC 5303 - Message Disposition Notification (MDN) profile for Internet Message Access Protocol (IMAP)*. (Cited on page 21.)

Micali, Silvio [1996]. *Simultaneous Electronic Transactions with Visible Trusted Third Parties*. (Cited on page 34.)

Micali, Silvio [1997a]. *Certified E-mail with Invisible Post Offices*. In *Proceedings RSA97*. (Cited on pages 35 and 36.)

Micali, Silvio [1997b]. *Simultaneous Electronic Transactions*. (Cited on page 35.)

Micali, Silvio [1997c]. *Simultaneous Electronic Transactions with Visible Trusted Third Parties*. (Cited on page 34.)

Miranda, José Pina and Joao Melo [2004]. *EPM: Tech, Biz and Postal Services Meeting Point*. In *Proceedings of Securing Electronic Business Processes ISSE 2004*, pages 259–267. (Cited on page 65.)

Mitsianis, John [2001]. *A new approach to enforcing non-repudiation of receipt*. (Cited on page 33.)

Moberg, D and R Drummond [2005]. *RFC 4130 - MIME-Based Secure Peer-to-Peer Business Data Interchange Using HTTP, Applicability Statement 2 (AS2)*. (Cited on page 21.)

Moore, K [2003]. *RFC 3461 - Simple Mail Transfer Protocol (SMTP) Service Extension for Delivery Status Notifications (DSNs)*. (Cited on page 21.)

Moore, K and G Vaudreuil [2003]. *RFC 3464 - An Extensible Message Format for Delivery Status Notifications*. (Cited on page 21.)

Mueller-Schloer, C [1984]. *Method and Apparatus Providing Registered Mail Features in an Electronic Communication System*. (Cited on page 35.)

Nadalin, Anthony, Marc Goodner, Martin Gudgin, Abbie Barbir, and Hans Granqvist [2007]. *WS-Trust 1.3*. (Cited on page 66.)

National Institute of Standards and Technology (NIST) [2002]. *Federal Information Processing Standards Publication 180-2*. (Cited on page 132.)

National IT and Telecom Agency [2007]. *OIO Reliable Asynchronous Profile version 1.1*. (Cited on page 68.)

Nenadić, Aleksandra, Ning Zhang, and Stephen Barton [2004]. *Fair Certified E-mail Delivery*. *Proceedings of the 2004 ACM symposium on Applied computing - SAC '04*, page 391. (Cited on page 36.)

Newman, C and A Melnikov [2008]. *RFC 5337 - Internationalized Delivery Status and Disposition Notifications*. (Cited on page 21.)

OASIS [2007]. *OASIS ebXML Messaging Services Version 3.0: Part 1, Core Features*. (Cited on page 211.)

OASIS [2011]. *AS4 Profile of ebMS 3.0 Version 1.0*. (Cited on page 211.)

OASIS Customer Information Quality TC [2008]. *Customer Information Quality Specifications Version 3.0*. (Cited on page 129.)

OASIS Digital Signature Services TC [2007]. *Digital Signature Service Core Protocols, Elements, and Bindings Version 1.0*. (Cited on pages 89 and 195.)

OASIS Security Services TC [2005]. *Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0*. (Cited on pages 162 and 194.)

OASIS Web Service Security (WSS) TC [2006]. *Web Services Security: SOAP Message Security 1.1 (WS Security 2004)*. (Cited on page 158.)

Object Management Group [2008]. *Common Object Request Broker Architecture 3.1*. http://www.omg.org/technology/documents/corba_spec_catalog.htm. (Cited on page 126.)

Olnes, Jon, Leif Buene, Anette Andresen, Havard Grindheim, Jörg Apitzsch, and Adriano Rossi [2010]. *A General Quality Classification System for eIDs and e-Signatures*. Vieweg+Teubner, Wiesbaden. ISBN 978-3-8348-0958-2, 72–86 pages. (Cited on page 89.)

Onieva, Jose a., Javier Lopez, and Jianying Zhou [2009]. *Secure Multi-Party Non-Repudiation Protocols and Applications*. Advances i Edition. Springer. ISBN 978-0387756295. (Cited on page 32.)

Onieva, Jose a., Jianying Zhou, and Javier Lopez [2008]. *Multiparty Nonrepudiation: A Survey*. *ACM Computing Surveys*, 41(1), pages 1–43. ISSN 03600300. (Cited on pages 24, 28, 29 and 32.)

Oppliger, Rolf [2004]. *Certified Mail: The Next Challenge for Secure Messaging*. *Communications of the ACM*, 47(8), pages 75–79. ISSN 0736-4679. (Cited on page 24.)

Oppliger, Rolf [2007]. *Providing Certified Mail Services on the Internet*. *IEEE Security and Privacy Magazine*, 5(1), pages 16–22. ISSN 1540-7993. (Cited on pages 22, 24, 33 and 35.)

Oppliger, Rolf and Peter Stadlin [2004]. *A certified mail system (CMS) for the Internet*. *Computer Communications*, 27(13), pages 1229–1235. ISSN 01403664. (Cited on page 35.)

Ornetsmüller, Gerhard and Andreas Dreer [2011]. *webERV ERVServices - Beschreibung der Webservice Schnittstelle Teilnehmer Übermittlungsstelle*. (Cited on page 57.)

Orthacker, Clemens and Martin Centner [2011]. *Minimal-Footprint Middleware to Leverage Qualified Electronic Signatures*. In Filipe, Joaquim and José Cordeiro (Editors), *Lecture Notes in Business Information Processing*, *Lecture Notes in Business Information Processing*, volume 75, pages 60–68. Springer Berlin Heidelberg, Berlin, Heidelberg. ISBN 978-3-642-22809-4. (Cited on page 197.)

Orthacker, Clemens, Martin Centner, and Christian Kittl [2010]. *Qualified Mobile Server Signature*. In *Proceedings of the 25th TC 11 International Information Security Conference, SEC 2010*. (Cited on page 49.)

OSCI Steering Office [2009]. *OSCI-Transport, Version 2.0 - Web Services Profiling and Extensions Specification*. (Cited on page 66.)

Parlamento Italiano [2009]. *Legge 28 gennaio 2009, n.2. Conversione in legge, con modificazioni, del decreto-legge 29 novembre 2008, n. 185, recante misure urgenti per il sostegno a famiglie, lavoro, occupazione e impresa e per ridisegnare in funzione anti-crisi il quadro strategico*. (Cited on page 52.)

Payeras-Capella, M.M., M. Mut-Puigserver, J.L. Ferrer-Gomila, and L. Huguet-Rotger [2009]. *No Author Based Selective Receipt in an Efficient Certified E-mail Protocol*. IEEE. ISBN 978-0-7695-3544-9, 387–392 pages. (Cited on page 28.)

Pfitzmann, Birgit, Matthias Schunter, and Michael Waidner [1998]. *Optimal efficiency of optimistic contract signing*. *Proceedings of the seventeenth annual ACM symposium on Principles of distributed computing - PODC '98*, pages 113–122. (Cited on page 36.)

Planitzer, F and W Weisweber [2007]. *Virtual Post Office in Practice*. In *Proceedings of Securing Electronic Business Processes ISSE 2007*, pages 427–437. (Cited on page 66.)

Posch, Karl-Christian, Reinhard Posch, Arne Tauber, Thomas Zefferer, and Bernd Zwattendorfer [2011]. *Secure and Privacy-preserving eGovernment - Best Practice Austria*. In *Rainbow of Computer Science*, pages 259–269. Springer. (Cited on page 48.)

Posch, Reinhard, Clemens Orthacker, Klaus Stranacher, Arne Tauber, Thomas Zefferer, and Bernd Zwattendorfer [2012]. *Open Source Bausteine als Kooperationsgrundlage*. In Eixelsberger, Wolfgang and Jürgen Stember (Editors), *E-Government - Zwischen Partizipation und Kooperation*, pages 185–209. Springer Vienna. ISBN 978-3-7091-0916-8. (Cited on page 48.)

Postel, Jonathan B. [1982]. *RFC 821 - Simple Mail Transfer Protocol*. (Cited on page 20.)

Puigserver, MM, JLF Gomila, and L Rotger [2005]. *Certified e-mail protocol with verifiable third party*. *2005 IEEE International Conference on e-Technology, e-Commerce and e-Service (EEE'05)*, pages 548–551. (Cited on page 36.)

Radicati, Sara [2010]. *Email Statistics Report, 2010*. Technical Report, The Radicati Group, Inc. (Cited on page 43.)

Ramsdell, B and S Turner [2010]. *RFC 5751 - Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification*. (Cited on page 20.)

Reichstädter, Peter [2003]. *e-Signatures for Delivery in e-Government*. In *EGOV 2003 - Electronic Government Lecture Notes in Computer Science*, pages 260–265. (Cited on page 48.)

Reichstädter, Peter and Arne Tauber [2008]. *Modell und Prozesse der Elektronischen Zustellung*. (Cited on page 47.)

Repubblica Italiana [2005a]. *Decreto 2 novembre 2005 - Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata*. (Cited on page 52.)

Repubblica Italiana [2005b]. *Regole tecniche del servizio di trasmissione di documenti informatici mediante posta elettronica certificata*. (Cited on pages 52 and 103.)

Repubblica Italiana [2009]. *Legge 18 giugno 2009, n. 69 - Disposizioni per lo sviluppo economico, la semplificazione, la competitività nonché in materia di processo civile*. (Cited on page 218.)

Republik Österreich [1982]. *Bundesgesetz vom 1. April 1982 über die Zustellung behördlicher Schriftstücke (Zustellgesetz)*. `http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10005522`. (Cited on pages 11 and 47.)

Republik Österreich [2004]. *Erlassung eines E-Government-Gesetzes sowie Änderung des Allgemeinen Verwaltungsverfahrensgesetzes 1991, des Zustellgesetzes, des Gebührengesetzes 1957, des Meldegesetzes 1991 und des Vereinsgesetzes 2002*. (Cited on pages 47, 49 and 218.)

Republik Österreich [2005]. *Elektronischer Rechtsverkehr - ERV (2006)*. (Cited on page 57.)

Republik Österreich [2008]. *Erlassung eines E-Government-Gesetzes sowie Änderung des Allgemeinen Verwaltungsverfahrensgesetzes 1991, des Zustellgesetzes, des Gebührengesetzes 1957, des Meldegesetzes 1991 und des Vereinsgesetzes 2002*. (Cited on page 47.)

Republik Österreich [2009]. *Änderung der Verordnung über den elektronischen Rechtsverkehr (ERV 2006)*. (Cited on page 57.)

Resnick, P [2001]. *RFC 2822 - Internet Message Format*. (Cited on page 52.)

Resnick, P [2008]. *RFC 5322 - Internet Message Format*. (Cited on pages 18, 128, 159 and 160.)

Rivest, R. L., A. Shamir, and L. Adleman [1978]. *A method for obtaining digital signatures and public-key cryptosystems*. *Communications of the ACM*, 21(2), pages 120–126. ISSN 00010782. (Cited on page 50.)

Rössler, Thomas [2008]. *Giving an interoperable e-ID solution: Using foreign e-IDs in Austrian e-Government*. *Computer Law & Security Report*, 24(5), pages 447–453. (Cited on page 87.)

Rössler, Thomas [2009a]. *Empowerment through Electronic Mandates - Best Practice Austria*. In *Software Services for e-Business and e-Society, IFIP Advances in Information and Communication Technology*, pages 148–160. (Cited on page 49.)

Rössler, Thomas [2009b]. *Object Identifier der öffentlichen Verwaltung (Teil 2 - Taxative Definition)*. (Cited on page 49.)

Rössler, Thomas [2010]. *STORK Deliverable D6.4.3 eDelivery - Detailed Planning*. (Cited on pages 189 and 196.)

Rössler, Thomas and Arne Tauber [2009]. *Interoperability: Coupling of e-Delivery Domains*. In *Proceedings of the 8th International Conference on Ongoing Research, General Development Issues and Projects of Electronic Government (EGOV 09)*, pages 247–254. (Cited on page 111.)

Rössler, Thomas and Arne Tauber [2010a]. *Elektronische Zustellung - Message Spezifikation (1.3.2)*. (Cited on page 173.)

Rössler, Thomas and Arne Tauber [2010b]. *The SPOCS Interoperability Framework: Interoperability of eDocuments and eDelivery Systems taken as Example*. In *Proceedings of ISSE 2010 Securing Electronic Business Processes*, pages 122–130. (Cited on page 89.)

Rössler, Thomas, Arne Tauber, Alenka Zuzek, Pierre Clausse, and Tarvi Martens [2009]. *STORK Deliverable D6.4.2 eDelivery - Draft Planning*. (Cited on page 196.)

Rossnagel, Alexander, Gerrit Hornung, Michael Knopp, and Daniel Wilke [2009]. *De-Mail und Bürgerportale*. *Datenschutz und Datensicherheit - DuD*, 33(12), pages 728–734. ISSN 1614-0702. (Cited on page 54.)

Ruggieri, Franco [2010]. *Registered e-mail (REM) - Reliable e-mail for everybody*. *Datenschutz und Datensicherheit - DuD*, 34(5), pages 314–317. ISSN 1614-0702. (Cited on page 63.)

Schulz, Sönke E [2010]. *Datenschutz beim E-Postbrief*. *Datenschutz und Datensicherheit - DuD2*, 35(4), pages 263–267. (Cited on page 59.)

Seeger, Michael [2010]. *Specifications for interoperable access to eDelivery and eSafe systems - Appendix 5: SPOCS TSL Accreditation and Operation Policy*. (Cited on page 210.)

Shirey, R [2000]. *RFC 2828 - Internet Security Glossary*. (Cited on pages 26 and 29.)

Siemens and Timelex [2008]. *Study on electronic procedures as foreseen under Art. 8 of the Services Directive*. (Cited on page 83.)

Siemens and Timelex [2009]. *Study on electronic documents and electronic delivery for the purpose of the implementation of Art. 8 of the Services Directive*. (Cited on page 83.)

SPOCS Consortium [2010]. *Proposal Part B - Simple Procedures Online for Cross-border Services (SPOCS)*. (Cited on page 153.)

Statskontoret [2003]. *SHS Version 1.2 Architecture*. (Cited on page 81.)

Stern, Marc [2010]. *STORK Deliverable D5.8.2d Security Principles and Best Practices*. (Cited on page 195.)

STORK Consortium [2010]. *Annex I - "Description of Work"*. (Cited on page 111.)

Stranacher, Klaus and Bernd Zwattendorfer [2009]. *Web-Service based Transformation of Digital Signature Formats*. In *Taking the eGovernment Agenda Forward: Meeting the Challenges of Digital Governance, Justice and Public Sector Information*, pages 523–532. (Cited on page 107.)

Tauber, Arne [2009]. *Requirements for Electronic Delivery Systems in eGovernment - An Austrian Experience*. In *Software Services for e-Business and e-Society, IFIP Advances in Information and Communication Technology*, pages 123–133. Springer. (Cited on pages 48 and 124.)

Tauber, Arne [2010]. *Requirements and Properties of Qualified Electronic Delivery Systems in eGovernment: An Austrian Experience*. *International Journal of E-Adoption*, 2(1), pages 45–58. (Cited on pages 48 and 124.)

Tauber, Arne [2011]. *A survey of certified mail systems provided on the Internet*. *Computers & Security*, 30(6-7), pages 464–485. ISSN 01674048. (Cited on pages 45 and 124.)

Tauber, Arne and Herbert Leitold [2011]. *A Systematic Approach to Legal Identity Management - Best Practice Austria*. In *Proceedings of the Information Security Solutions Europe 2011 Conference*. (Cited on page 49.)

Tauber, Arne and Peter Reichstädter [2010]. *Privatzustellung - Der elektronisch eingeschriebene Brief*. *eGovernment review*, 5, pages 18–19. (Cited on page 52.)

Tauber, Arne and Thomas Rössler [2009a]. *Elektronische Vollmachten im österreichischen E-Government*. *eGovernment review*, 4, pages 22–23. (Cited on page 49.)

Tauber, Arne and Thomas Rössler [2009b]. *Professional Representation in Austrian E-Government*. In *Proceedings of the 8th International Conference on Ongoing Research, General Development Issues and Projects of Electronic Government (EGOV 09)*, volume 5693, pages 388–398. Springer Verlag. ISBN 9783642035159. (Cited on page 49.)

Tauber, Arne and Thomas Rossler [2010]. *A Scalable Interoperability Architecture for Certified Mail Systems*. In *2010 IEEE 12th Conference on Commerce and Enterprise Computing*, pages 9–16. IEEE. ISBN 978-1-4244-8433-1. (Cited on pages 100, 106 and 111.)

Tauber, Arne and Thomas Rössler [2010a]. *Elektronische Zustellung - Zustellkopf - Schnittstellenspezifikation (1.3.2)*. (Cited on page 173.)

Tauber, Arne and Thomas Rössler [2010b]. *Enhancing security and privacy in certified mail systems using trust domain separation*. In *ISC'10 Proceedings of the 13th international conference on Information security*, pages 152–158. ISBN 978-3-642-18177-1. (Cited on page 52.)

Tauber, Arne and Thomas Rössler [2010c]. *Interoperability Challenges for Pan-European Qualified Exchange of Electronic Documents*. In *The Proceedings of the 10th European Conference on eGovernment (ECEG 2010)*, pages 382–390. (Cited on pages 106 and 124.)

Tauber, Arne, Thomas Rössler, Alenka Zuzek, Pierre Clausse, and Tarvi Martens [2009]. *STORK Deliverable D6.4.1 eDelivery - Functional Specification*. (Cited on page 196.)

Tauber, Arne, Thomas Zefferer, and Bernd Zwattendorfer [2011a]. *Elektronisches Einschreiben im D-A-CH Raum*. In *DACH Security 2011*, pages 510–521. (Cited on page 45.)

Tauber, Arne, Bernd Zwattendorfer, and Thomas Zefferer [2011b]. *A Shared Certified Mail System for the Austrian Public and Private Sectors*. In *Proceedings of the International Conference on Electronic Government and the Information Systems Perspective (EGOVIS 2011)*. (Cited on page 52.)

Tauber, Arne, Bernd Zwattendorfer, and Thomas Zefferer [2011c]. *STORK: Pilot 4 Towards Cross-border Electronic Delivery*. In *Electronic Government and Electronic Participation - Joint Proceedings of Ongoing Research and Projects of IFIP EGOV and ePart 2011*, pages 295–301. (Cited on pages 87 and 111.)

Tauber, Arne, Bernd Zwattendorfer, Thomas Zefferer, Yasmin Mazhari, and Eleftherios Chamakiotis [2010]. *Towards Interoperability: An Architecture for Pan-European eID-based Authentication Services*. In *Proceedings of the International Conference on Electronic Government and the Information Systems Perspective (EGOVIS)*, pages 120–133. (Cited on page 197.)

Tauber, Arne, Bernd Zwattendorfer, Thomas Zefferer, and Klaus Stranacher [2011d]. *Grenzüberschreitendes E-Government in Europa*. *eGovernment review*, 8, pages 8–9. (Cited on page 84.)

Tedrick, Tom [1983]. *How to exchange half a bit*. In *Advances in Cryptology - Proceedings of Crypto 83*, pages 147–151. (Cited on page 32.)

Tedrick, Tom [1985]. *Fair exchange of secrets*. In *Advances in Cryptology - Proceedings of Crypto 84*, pages 434–438. (Cited on page 32.)

The Council of the European Union [1997]. *Directive 97/67/EC the European Parliament and of the Council of 15 December 1997 on common rules for the development of the internal market of Community postal services and the improvement of quality of service*. (Cited on page 215.)

The Council of the European Union [2000a]. *Council Regulation (EC) No 1348/2000 of 29 May 2000 on the service in the Member States of judicial and extrajudicial documents in civil or commercial matters*. (Cited on page 216.)

The Council of the European Union [2000b]. *Directive 1999/93/EC the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures*. (Cited on pages 48, 70 and 83.)

The Council of the European Union [2002]. *Directive 2002/39/EC of the European Parliament and of the Council, of 10 June 2002 amending Directive 97/67/EC with regard to the further opening to competition of Community postal services*. (Cited on page 215.)

The Council of the European Union [2006a]. *Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market*. (Cited on pages 2, 79, 89 and 90.)

The Council of the European Union [2006b]. *Regulation (EC) No 1896/2006 of the European Parliament and of the Council of 12 December 2006 creating a European order for payment procedure*. (Cited on page 218.)

The Council of the European Union [2007]. *Regulation (EC) No 1393/2007 of the European Parliament and of the Council of 13 November 2007 on the service in the Member States of judicial and extrajudicial documents in civil or commercial matters (service of documents), and repealing Council Regulat*. (Cited on page 216.)

The Council of the European Union [2008]. *Directive 2008/6/EC of the European Parliament and of the Council of 20 February 2008 amending Directive 97/67/EC with regard to the full accomplishment of the internal market of Community postal services*. (Cited on page 215.)

UPU [1996]. *S10c-5 Identification of postal items - Part C : 13 character identifier for special letter products*. (Cited on page 6.)

UPU [2003]. *Secured electronic postal services (SePS) interface specification - Part A: Concepts, schemas and operations*. (Cited on page 65.)

UPU [2008]. *Postal Registered eMail (PReM) Functional Specification*. (Cited on page 65.)

USPS [2006]. *The United States Postal Service - An American History 1775 - 2006*. (Cited on page 9.)

Vaudreuil, G [2003a]. *RFC 3462 - The Multipart/Report Content Type for the Reporting of Mail System Administrative Messages*. (Cited on page 21.)

Vaudreuil, G [2003b]. *RFC 3463 - Enhanced Mail System Status Codes*. (Cited on page 21.)

Wikipedia [2011a]. *Mail*. `https://secure.wikimedia.org/wikipedia/en/wiki/Mail`. (Cited on page 1.)

Wikipedia [2011b]. *Zustellungsurkunde*. `http://de.wikipedia.org/wiki/Zustellungsurkunde`. (Cited on page 8.)

X-Tee [2005]. *Protocol: Data exchange protocol between database and information system - Requirements on information systems and adapter servers*. (Cited on page 69.)

Zefferer, Thomas, Arne Tauber, and Bernd Zwattendorfer [2011]. *Secure and Reliable Online-Verification of Electronic Signatures in the Digital Age*. In *Proceedings of IADIS International Conference WWW/Internet 2011*, page in press. (Cited on page 109.)

Zhang, N and Q Shi [1996]. *Achieving non-repudiation of receipt*. *The Computer Journal*, 39(10), page 844. ISSN 00104620. (Cited on page 35.)

Zhou, Jianying, Robert Deng, and Feng Bao [1999]. *Evolution of Fair Non-repudiation with TTP*. In *ACISP '99 Proceedings of the 4th Australasian Conference on Information Security and Privacy*, pages 258–269. (Cited on pages 24 and 36.)

Zhou, Jianying and Dieter Gollmann [1996a]. *A fair non-repudiation protocol*. In *Proceedings of the 1996 IEEE Symposium on Security and Privacy SP96 (1996)*, pages 55–61. ISBN 0-8186-7417-2. (Cited on pages 35 and 36.)

Zhou, Jianying and Dieter Gollmann [1996b]. *Certified Electronic Mail*. In *Proc European Symp on Research in Computer Security ESORICS*, pages 3–19. February, Internet Society, Citeseer. (Cited on pages 23, 28 and 34.)

Zhou, Jianying and Dieter Gollmann [1997]. *An Efficient Non-repudiation Protocol*. *Proceedings 10th Computer Security Foundations Workshop*, pages 126–132. (Cited on page 36.)

Zwattendorfer, Bernd, Thomas Zefferer, and Arne Tauber [2011a]. *A Privacy-Preserving eID based Single Sign-On Solution*. In *Proceedings of 5th International Conference on Network and System Security (NSS 2011)*, pages 295–299. (Cited on page 196.)

Zwattendorfer, Bernd, Thomas Zefferer, and Arne Tauber [2011b]. *E-ID Meets E-Health on a Pan-European Level*. In *Proceedings of the IADIS International Conference e-Health 2011*, pages 97–104. (Cited on page 92.)