ETSI SR 019 050 V1.1.1 (2015-06)

Electronic Signatures and Infrastructures (ESI);
Rationalized framework of Standards for Electronic Registered Delivery Services Applying Electronic Signatures

Reference
DSR/ESI-0019530

Keywords
electronic signature, electronic registered delivery, security

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://ipr.etsi.org).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Special Report (SR) has been produced by ETSI Technical Committee Electronic Signatures and Infrastructures (ESI).

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Introduction

Electronic delivery services in the broad sense, i.e. services that make it possible to transmit data between third parties by electronic means, are ubiquitous in most human activities. This is potentially true also when focusing on electronic registered delivery services in the stricter sense provided by the European regulation No 910/2014 [i.4], which adds requirements on the integrity, confidentiality, non-repudiation and indisputability of transmitted data. Obviously, these requirements apply to a wide range of contexts. The necessity of a governance on this field has been clearly recognized by the Regulation (EU) No 283/2014 [i.31] (hereafter referred to as eTelNet) and by the Regulation (EE) No 910/2014 [i.4] (hereafter referred to as eIDAS or eIDAS Regulation). The first document states that:

> *"Member States should encourage local and regional authorities to be fully and effectively involved in the governance of digital service infrastructures, and ensure that projects of common interest relating to cross-border delivery of eGovernment services take into account the EIF recommendations."*

while, in the Annex, it explicitly identifies electronic delivery among the "building blocks" for the digital service infrastructure. Annex 2 to the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions Towards interoperability for European public services: "European Interoperability Framework" (hereafter referred to as EIF) [i.30] suggests that a layered approach to interoperability has to be adopted, distinguishing legal, organizational, semantic and technical (syntax, transmission) aspects. It is assumed that eIDAS Regulation [i.4] aims at covering the "legal" layer, while the other layers are covered by specific standards.

The impact assessment accompanying eTelNet Regulation [i.31] recognizes that:

> *"A large number of cross-border digital services implementing exchanges between European public administrations in support of Union policies are a reality. When providing new solutions, it is important to capitalise on existing solutions implemented in the context of other European initiatives, avoid duplication of work, and ensure coordination and alignment of approaches and solutions across initiatives and policies […]"*

As a matter of fact, several electronic (either registered or not) delivery services are emerging, most of them restricted either to a member state or to a community, a business, etc. Some of these services are not homogeneous and not interoperable, mainly because of the lack of a normative and standardization base, hence hindering the emergence of electronic registered delivery as a global (or, at least, pan-European) commodity service.

A first attempt was already provided by Registered Electronic Mail (hereafter referred to as REM) specifications (multi-part deliverable ETSI TS 102 640 [i.7] to [i.15]) and the related UPU specifications (CEN/TS 16326 [i.5]) which, however, were focused on a subset of features and technologies.

1 Scope

The present document provides a proposal for a rationalized framework of standards for electronic registered delivery services, as defined by the eIDAS Regulation [i.5], and fully aligned with the principles, criteria and structure of the ETSI TR 119 000 [i.15]: "Rationalized structure for Electronic Signature Standardization" which describes the rationalized structure for the current and future European eSignatures standardization documents.

The present document also includes a set of recommendations for future standardization activities that target at implementing the framework of standards for electronic registered delivery.

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are necessary for the application of the present document.

Not applicable.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market.

NOTE: Available from: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32006L0123.

[i.2] Commission Decision 2009/767/EC 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 market.

NOTE: Available from: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:299:0018:0054:EN:PDF.

[i.3] Commission Decision 2010/425/EU of 28 July 2010 amending Decision 2009/767/EC as regards the establishment, maintenance and publication of trusted lists of certification service providers supervised/accredited by Member States.

NOTE: Available from: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:199:0030:0035:EN:PDF.

[i.4] Regulation (EE) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

NOTE: Available from: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=EN.

[i.5] CEN/TS 16326:2013: "Postal Services - Hybrid Mail - Functional Specification for Postal Registered Electronic Mail".

[i.6] ETSI TS 119 612: "Electronic Signatures and Infrastructures (ESI); Trusted Lists".

[i.7] ETSI TS 102 640-1: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 1: Architecture".

[i.8] ETSI TS 102 640-2: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 2: Data requirements, Formats and Signatures for REM".

[i.9] ETSI TS 102 640-3: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 3: Information Security Policy Requirements for REM Management Domains".

[i.10] ETSI TS 102 640-4: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 4: REM-MD Conformance Profiles".

[i.11] ETSI TS 102 640-5: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 5: REM-MD Interoperability Profiles".

[i.12] ETSI TS 102 640-6-1: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 6: Interoperability Profiles; Sub-part 1: REM-MD UPU PReM Interoperability Profile".

[i.13] ETSI TS 102 640-6-2: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 6: Interoperability Profiles; Sub-part 2: REM-MD BUSDOX Interoperability Profile".

[i.14] ETSI TS 102 640-6-3: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 6: Interoperability Profiles; Sub-part 3: REM-MD SOAP Binding Profile".

[i.15] ETSI TR 119 000: "Electronic Signatures and Infrastructures (ESI); Rationalized structure for Electronic Signature Standardization".

[i.16] IETF RFC 5751, January 2010: " Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification".

[i.17] IETF RFC 2459, January 1999: "Internet X.509 Public Key Infrastructure Certificate and CRL Profile".

[i.18] ISO 32000-1: "Document management -- Portable document format -- Part 1: PDF 1.7".

[i.19] Recommendation ITU-T X.1254/ISO/IEC DIS 29115: "Information technology - Security techniques - Entity authentication assurance framework".

[i.20] OASIS WS-Trust 1.4.

NOTE: Available from: http://docs.oasis-open.org/ws-sx/ws-trust/v1.4/ws-trust.html.

[i.21] OASIS Standard Specification (1 February 2006): "Web Services Security: SOAP Message Security 1.1 (WS-Security 2004)".

NOTE: Available from: https://www.oasis-open.org/committees/download.php/16790/wss-v1.1-spec-os-SOAPMessageSecurity.pdf.

[i.22] OASIS Standard (15 March 2005): "Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0".

NOTE: Available from: http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf.

[i.23] W3C Recommendation, 11 April 2013: "XML Signature Syntax and Processing Version 1.1".

NOTE: Available from: http://www.w3.org/TR/2013/REC-xmldsig-core1-20130411/.

[i.24] OASIS Standard (1 October 2007): "OASIS ebXML Messaging Services Version 3.0: Part 1, Core Features".

NOTE: Available from: http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/core/os/ebms_core-3.0-spec-os.odt.

[i.25] IETF RFC 5321: "Simple Mail Transfer Protocols".

[i.26] IETF RFC 5322: "Internet Message Format".

[i.27] OASIS Standard, 2009: "Web Services Reliable Messaging 1.2".

[i.28] W3C: "SOAP Version 1.2 Part 1 Messaging Framework (Second Edition)", 2007".

[i.29] OASIS 2009: "Web Service Federation Language, 1.2".

[i.30] European Commission, European Interoperability Framework for European Public Services (EIF) version 2.0, 2010.

[i.31] Regulation (EU) No 283/2014 of the European Parliament and of the Council of 11 March 2014 on guidelines for trans-European networks in the area of telecommunications infrastructure and repealing Decision No 1336/97/EC (Text with EEA relevance).

NOTE: Available from: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.086.01.0014.01.ENG.

[i.32] DG-MARKT: "Study on electronic documents and electronic delivery for the purpose of the implementation of Art. 8 of the Services Directive. D1.2: National profiles deliverable (WP1)".

[i.33] ETSI TR 102 605: "Electronic Signatures and Infrastructures (ESI); Registered E-Mail".

[i.34] PEPPOL Infrastructure specifications.

NOTE: Available from http://www.peppol.eu/ressource-library/technical-specifications/infrastructure-resources.

[i.35] COM 2013/662/EU Commission implementing Decision amending Decision 2009/767/EC as regards the establishment, maintenance and publication of trusted lists of certification service providers supervised/accredited by Member States. 14 October 2013.

[i.36] ISO/IEC 13888-3:2009: "Information technology -- Security techniques -- Non-repudiation -- Part 3: Mechanisms using asymmetric techniques".

[i.37] STORK Large Scale Pilot project specifications.

NOTE 1: Available from https://www.eid-stork.eu/index.php?option=com_processes&act=list_documents&s=1&Itemid=60&id=312

NOTE 2: A further inventory of documents relating to electronic delivery is given in annex B and annex C (Bibliography).

[i.38] ETSI EN 319 401: "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers".

[i.39] ETSI TR 103 071: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Test suite for future REM interoperability test events".

[i.40] ETSI TS 102 231: "Electronic Signatures and Infrastructures (ESI); Provision of harmonized Trust-service status information".

[i.41] ISO 15459: "Information technology -- Unique identifiers".

[i.42] IETF RFC 5424: "The Syslog Protocol".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in eIDAS Regulation [i.4], ETSI TS 102 640 on REM [i.7], [i.8], [i.9], ETSI TR 119 000 [i.15] and the following apply.

The definitions below, which take precedence over the other definitions, have been provided according to one of the following criteria:

- They are not provided elsewhere in the mentioned sources.
- They are present elsewhere in the mentioned sources, but they are central to the present document.
- They are present in one or more of the mentioned sources, but there is no coincidence among those definitions or a variation in the definition is introduced.

electronic registered delivery: transmission of data by electronic means which provides evidence relating to the handling of the transmitted data, including proof of sending or receiving the data, and which protects transmitted data against the risk of loss, theft, damage or any unauthorised alterations

electronic registered delivery service (eRDS): service providing electronic registered delivery

end entity: message sender and recipient; user (using user agents) or system using electronic registered delivery services for data exchange

(qualified) electronic registered delivery management domain ((Q)eRDMD): set of technical and physical components, personnel, policies and processes that provide (qualified) electronic registered delivery services within a network

(qualified) electronic registered delivery network: network of interconnected (qualified) electronic registered delivery management domains federated in a trust circle in order to provide (qualified) electronic registered delivery services

qualified electronic registered delivery service (QeRDS): electronic registered delivery service which meets the requirements laid down in Article 42 of eIDAS Regulation [i.4]

(qualified) electronic registered delivery service provider ((Q)eRDSP): (qualified) trust application service provider which provides (qualified) electronic registered delivery services

(qualified) electronic registered delivery solution: set of technical and physical components, personnel, policies and processes that provide (qualified) electronic registered delivery services in autonomy

qualified registered electronic mail service: registered electronic mail service which meets the requirements laid down in Article 42 of eIDAS Regulation [i.4]

(qualified) registered electronic mail service provider: (qualified) electronic registered delivery service provider which provides (qualified) registered electronic mail services

qualified trust service: trust service that meets the applicable requirements laid down in eIDAS Regulation [i.4]

qualified trust service provider: a trust service provider that meets the requirements laid down in the applicable regulation

registered electronic mail service: electronic registered delivery service based on electronic mail as the underlying technology

trust application service provider: trust service provider operating a value added trust service based on electronic signatures that satisfies a business requirement that relies on the generation/verification of electronic signatures in its daily routine

NOTE: This covers namely services like registered electronic mail and other type of electronic registered delivery services, as well as preservation services related to signed data and electronic signatures.

trust service: electronic service which enhances trust and confidence in electronic transactions

trust service provider: natural or legal person who provides one or more trust services either as a qualified or as a non-qualified trust service provider

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AP	Access Point
AS	Attribute Service
ATNA	Audit Trail and Node Authentication
BDXR	Business Document Exchange
BusDox	Business Document Exchange Network
CEC-PAC	Comunicazione Elettronica Certificata tra Pubblica Amministrazione e Cittadino
CEN	Comité Européen de Normalisation
CIPA	Common Infrastructure for Public Administrations
CMS	Cryptographic Message Syntax
CRL	Certificate Revocation List
DNS	Domain Name System
E-CODEX	e-Justice Communication via Online Data Exchange
(Q)eRDMD	(Qualified) electronic Registered Delivery Management Domain
ebMS	ebXML Messaging Services
ebXML	eXtensible Markup Language
EC	European Commission
EEA	European Economic Area
EIF	European Interoperability Framework
EN	European Standard
EPCM	Electronic Postal Certification Mark
EPM	Electronic Post Mark
eRDMD	Electronic Registered Delivery Management Domain
ETSI	European Telecommunications Standards Institute
EU	European Union
EUMS	European Member States
HTTP	Hypertext Transfer Protocol
ICT	Information and Communication Technologies
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IFIP	International Federation for Information Processing
IHE	Integrating the Healthcare Enterprise
ISA	Interoperability Solutions for European Public Administrations
ISSE	Integration of Safety and Security Engineering
ISO	International Organization for Standardization
ITU-T	International Telecommunication Union - Telecommunication Standardization Bureau
LSP	Large Scale Pilot
NCP	National Contact Point
OASIS	Organization for the Advancement of Structured Information Standards
OSCI	Online Service Computer Interface
PACE	Password Authenticated Connection Establishment
PDF	Portable Document Format
PEC	Posta Elettronica Certificata
PEC-ID	Posta Elettronica Certificata con Identificazione
PEGS	Pan-European Government Services
PEPPOL	Pan-European Public eProcurement On-Line
PKI	Public Key Infrastructure
PReM	Postal Registered e-Mail
RED	Registered Electronic Delivery
REM	Registered Electronic Mail
REM-MD	Registered Electronic Mail - Management Domain
SAML	Security Assertion Markup Language
SMIME	Secure Multi-Purpose Internet Mail Extensions
SML	Service Metadata Locator

SMP	Service Metadata Publisher
SMTP	Simple Mail Transfer Protocol
SOA	Service Oriented Architecture
SOAP	Simple Object Access Protocol
SPOCS	Simple Procedures Online for Cross-border Services
SR	Special Report
SSL	Secure Socket Layer
STORK	Secure identity across borders linked) being the most relevant
S&N	Store And Notify
TC	Technical Committee
TL	Trusted List
TLS	Transport Layer Security
TR	Technical Report
TS	Technical Specification
TSL	Trust-service Status List
UPU	Universal Postal Union
URI	Uniform Resource Identifier
WS	Web Service
WWW	World Wide Web
XML	eXtensible Markup Language
XMLDSig	XML Digital Signature

4 Methodology

In order to identify a framework of standards for electronic registered delivery services, which fills the current standardization gap and is fully in line with the Rationalized Framework of Standards for electronic signatures, a well-conceived methodology has been applied, which is also reflected in the structure of the present document as follows.

Clause 5 identifies the main electronic registered delivery features to provide a basic understanding of requirements for creating the different electronic registered delivery service models. Features have been collected from different sources. Main sources were the literature as well as existing systems in place, i.e. existing specifications on international, European, national and local level, articles and contributions provided by the scientific community and implementations of electronic delivery solutions, mainly on a national level or private business services. Identified features range from core security aspects on communication and application layer to architectural, organizational and trust ones.

Based on the identified features, clause 6 sketches the different electronic registered delivery service models and thereof identifies the implications on standardization activities. The service model description uses a top-down approach by starting with a simple and basic model (electronic registered delivery as a black-box), continuing with the distributed model (different electronic registered delivery management domains for sender and recipient) and concluding with an extended one, which uses an interoperability layer to couple different systems. By referring to the electronic registered delivery features, main roles and functionalities of an electronic registered delivery management domain are categorized into core, optional and ancillary ones. Based on the features, service models and role definitions, the implications to standardization activities have been identified. To be in line with the eIDAS Regulation [i.4], implications cover both the conformance with requirements for qualified and non-qualified electronic registered delivery services as well as processes for sending and receiving data, when data is transferred between two or more qualified trust service providers. The latter mainly concerns the interoperability layer between different (qualified) electronic registered delivery service providers with respect to service discovery, message delivery and registered delivery.

Clause 7 provides input to the rationalized framework with a collection of existing standards and publicly available specifications. This complements the implications to standardization activities of clause 6 to identify gaps and highlight where the rationalized framework can fill these gaps. Due to their diversity, the inventory does not include national (or private business) electronic (either registered or not) delivery solutions. It rather focuses on existing national and international standards in this field and also covers European efforts in the area of cross-border electronic (either registered or not) delivery, which paves the technical way towards the eIDAS Regulation [i.4].

Clause 8 introduces the rationalized structure for electronic registered delivery standards, which is based on the electronic registered delivery service model and provides standards to fill the identified gaps. The rationalized structure of the framework follows a classification scheme based on the document types identified within ETSI TR 119 000 [i.15] (guidance, technical, conformance, etc.).

Finally, clause 9 completes the rationalized framework by placing the gap analysis and work plan together on a per document basis in table, recommending a direction toward the production of the identified specifications.

The present document includes three annexes, respectively containing: the set of pan-European solutions analyzed, the list of known standards and specifications related to electronic (either registered or not) delivery, a bibliography on the subject.

5 Features

Table 1 shows a number of features identified in the solutions listed in Annex A. The first column shows the term selected for identifying the feature henceforth in the present document. Column "Alternative terms" lists a number of terms that have been found in existing solutions or in the literature for identifying the same feature. Column "Entities Involved" lists the entities that in the context of the provision of electronic registered delivery services are affected or can benefit from the feature. For the purpose of this table, the following entities have been identified:

- User: human or application using the electronic registered delivery service.
- Service access point: point of entrance to the service.
- Service node: any intermediate value adding service node.
- External provider of ancillary services.

Column "Scope" identifies the specific point-to-point exchanges within the electronic registered delivery transaction which are affected or can benefit from the feature (e.g. authentication scope can be user-to-service access point, service node-to-service node, and service access point-to-user). Finally, the last column contains a short description of the feature when required, or/and comments on the specific feature in the light of its provision in the scenarios presented and analyzed.

Table 1: Electronic (either registered or not) delivery features

Feature name	Alternative terms	Entities involved	Scope	Comment related to features in the scenarios
End entity authentication	Identity validation	- user - service AP	1. User-to-ServiceAP 2. ServiceAP-to-User	This feature is used for authentication purposes of 'who' is using the service. Some electronic (either registered or not) delivery solutions provide for a token for authentication (e.g. STORK, PEC with PEC-ID, etc.).
Node authentication	mutual server authentication	- service node	3. S.node-to-S.node	(Mutual) authentication of services involved in the electronic (either registered or not) delivery process.
Non-repudiation	content commitment	- user - service AP - service node	1. User-to-ServiceAP 2. ServiceAP-to-User 3. S.node-to-S.node	This feature is implemented in many ways each covering different issues of repudiation during a communication flow by the generation of an evidence. For example: - Submission of a message by a sender, - Acceptance of a sender's message by own Service Provider, - Delivery of a message by a Service Provider (to another Service Provider or to the Recipient).
Confidentiality	Encryption	- user - service AP - service node	1. User-to-ServiceAP 2. ServiceAP-to-User 3. S.node-to-S.node 4. User-to-User	Feature that can be used in partial paths of the communications but also on an end-to-end basis.

Feature name	Alternative terms	Entities involved	Scope	Comment related to features in the scenarios
Integrity	Signature	- user - service AP - service node	1. User-to-User 3. S.node-to-S.node	Feature that can be used on an end-to-end basis as well as in partial paths of the transport route.
Reliable delivery		- user - service AP - service node	1. User-to-User 3. S.node-to-S.node	Feature that can be used on an end-to-end basis as well as in partial paths of the transport route
Antivirus		- service node - External antiabuse provider	1. User-to-ServiceAP 2. ServiceAP-to-User 3. S.node-to-S.node	Feature that can be offered to the final user to detect and to do specific actions on presence of malware on the communication content
Antispam		- service node - External antiabuse provider	1. User-to-ServiceAP 2. ServiceAP-to-User 3. S.node-to-S.node	Feature that can be offered to the final user to detect and to do specific actions when the received information is detected as spam
Time reference		- service node - External Time Server provider	1. Internal to the service 2. Client time sync	This feature allows synchronizing the clocks of all the server nodes to a trusted reference. This is relevant for the creation of coherent log. Also the client can be synchronized with a valid time reference.
Electronic Signature provision		- user - service AP - service node	1. User-to-ServiceAP 2. ServiceAP-to-User 4. User-to-User	Feature allowing the electronic signature of messages and/or evidence exchanged.
Service Trust	TSL, Provider Index, Directory, Security Token Service	- service node	1. S.node-to-S.node	This feature is related to how trust is built between different service providers. It can be implemented by a trusted circle as recommended in REM [i.8], via a shared directory (e.g. Italian PEC), via Security token Service as defined by WS Trust [i.20], WS Federation [i.29], etc.
Service Discovery	Provider index, Directory	- Service node	1. S.node-to-S.node	This feature is related to how the details of an electronic (either registered or not) delivery service provider can be discovered and retrieved. It can be implemented by a specific protocol (e.g. DNS-based SML-SMP in PEPPOL), via a shared directory (e.g. Italian PEC), etc.
End entity Discovery		- user - service AP	1. User-to-ServiceAP 2. ServiceAP-to-User	This feature is related to how the details of an end user (or participant) can be discovered/retrieved and used to send some message. It can be implemented by a browsable directory (e.g., Italian CEC-PAC), via the Attribute Service (AS) of an Identity Provider (IdP) as participant directory (e.g. Secure Access For E-government), etc.
Address management		- user - service AP - service node	1. User-to-ServiceAP 2. ServiceAP-to-User 3. S.node-to-S.node	Each electronic (either registered or not) delivery service manages addresses of its subscribers. For example some of these often use IETF RFC 5321 [i.25] to implement this feature but also other means/schemes are used.
Translation		- service node	1. S.node-to-S.node	Some electronic (either registered or not) delivery solutions implement a feature for the normalization of content.
Semantic check		- service node	1. S.node-to-S.node	Some electronic (either registered or not) delivery solutions implement a feature for the semantic check of content.
Structured/ non-structured contents		- service node	1. S.node-to-S.node	Some electronic (either registered or not) delivery solutions (but not all) manage structured contents.

Feature name	Alternative terms	Entities involved	Scope	Comment related to features in the scenarios
Service Level/ Provision Negotiation		- user - service AP - service node	1. User-to-ServiceAP 2. ServiceAP-to-User 3. S.node-to-S.node	Some electronic (either registered or not) delivery solutions can offer different delivery options, e.g.: • Generation of some optional evidence other than the mandatory one. • Request that a specific delivery mode is operated (e.g. S&N)
Evidence validation		- service node	1. User-to-ServiceAP 3. S.node-to-S.node	Some systems offer an evidence validation service, which grants proof of integrity/authenticity of the data, proof of delivery, etc.
Electronic Signature validation		- service node	1. User-to-ServiceAP 2. ServiceAP-to-User 3. S.node-to-S.node	Some systems offer a signature verification service (e.g. e-CODEX delivers a "Trust-Ok Token" to the recipient)
Deadlines	Timeliness	- service node	1. User-to-ServiceAP 2. ServiceAP-to-User 3. S.node-to-S.node	Processes (e.g. automatic send-out of non-delivery evidence) are triggered by deadlines. Some solutions allow for setting deadlines sender-side.
Governance	Service Policy	- user - service AP - service node	1. User-to-ServiceAP 2. ServiceAP-to-User 3. S.node-to-S.node	It regulates the functionality and behaviour of all other features. It can be defined by (national/European/international) law or rules.

6 Electronic registered delivery service model

6.1 Introduction

Starting from the feature analysis in clause 5, this clause presents a preliminary high-level model of an electronic registered delivery service as a basis for further elaboration, not intended to impose specific requirement for the successive standardization activity. It is intended that a more complete model will emerge from the dialogue with interested stakeholders and will serve as a basis for future standardization activities in the field.

The model aims at describing the entities and the events which constitute the essence of an "electronic registered delivery act" in most known systems, in line with the non-repudiation model described in [i.36].

6.2 Basic service model

From a user perspective, an electronic registered delivery service implements (in its simplest flavour) the sequence diagram represented in Figure 1. The electronic registered delivery service is seen as a single object (a black-box), even if it might consist of several geographically distributed interconnected components.

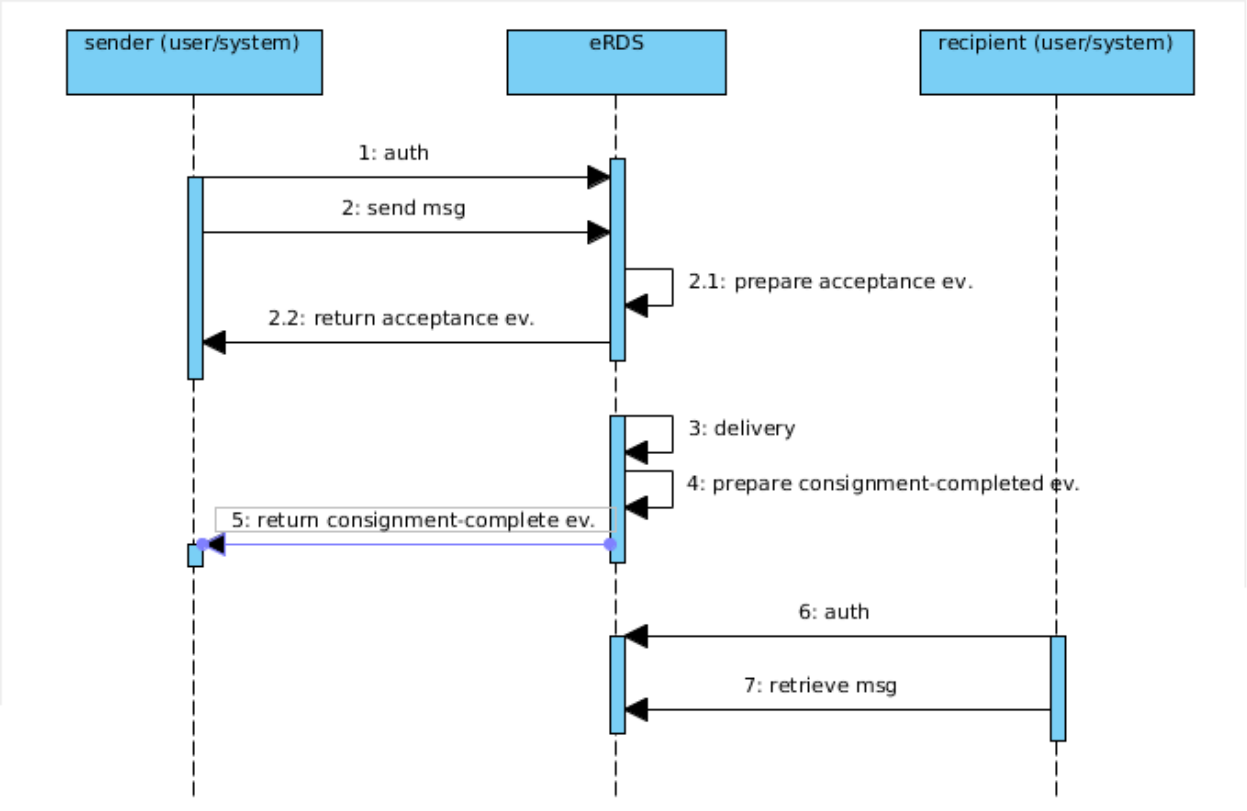


Figure 1: Basic electronic registered delivery service model

1. The sender (either a user or a system) authenticates to the electronic registered delivery service.

2. The sender (either a user or a system) prepares a message, specifies one or more addressees, indicates some options on the registered delivery service required (e.g., confidential, urgent, etc.), and submits it to the electronic registered delivery service.

2.1. At this point the electronic registered delivery service tracks the event that the message has been submitted (some systems can omit this step). This is often done producing an "attestation of submission" (submission evidence), i.e. a signed file containing the basic information of the event. In this respect, the electronic registered delivery service acts as a trusted third party.

2.2. Sometimes the evidence is sent back to the sender. This behaviour can be fixed for the system, or depends on a delivery option indicated by the sender. Independently from sending to the sender, the evidence is always stored for a certain amount of time by the system.

3. The consignment to the recipient(s) happens, meaning that the message submitted by the sender is made available to the recipient(s), in a way that depends on the specific service implementation.

4. The electronic registered delivery service tracks the event that the message has been made available to the recipient. Again, this is often done producing an attestation (consignment completed evidence), i.e. a (signed) file containing the basic information of the event. In case of multiple deliveries, one or more evidence can be produced.

5. As in point 4, the evidence can be sent back to the sender. This behaviour can be fixed for the system, or depends on a delivery option indicated by the sender. Independently from sending to the sender, the evidence is always stored for a certain amount of time by the system.

6. The recipient (either a user or a system) authenticates to the electronic registered delivery service.

7. The recipient (either a user or a system) gets the message.

For the sake of simplicity, the flow ignores all the negative cases (failure in delivery, refusal, etc.) and with different modes for consigning the message to the recipient (push/pull, etc.) The core model does not deal with other relevant evidence which may be available in some cases, most notably the evidence that the recipient actually retrieved the message from the system (retrieval evidence).

6.3 Distributed service model

While the user experience is that of an opaque black-box, the reality behind an electronic registered delivery service is often made of several interacting domains, operated by different providers. In this case the relevant sequence diagram appears as follows in Figure 2.

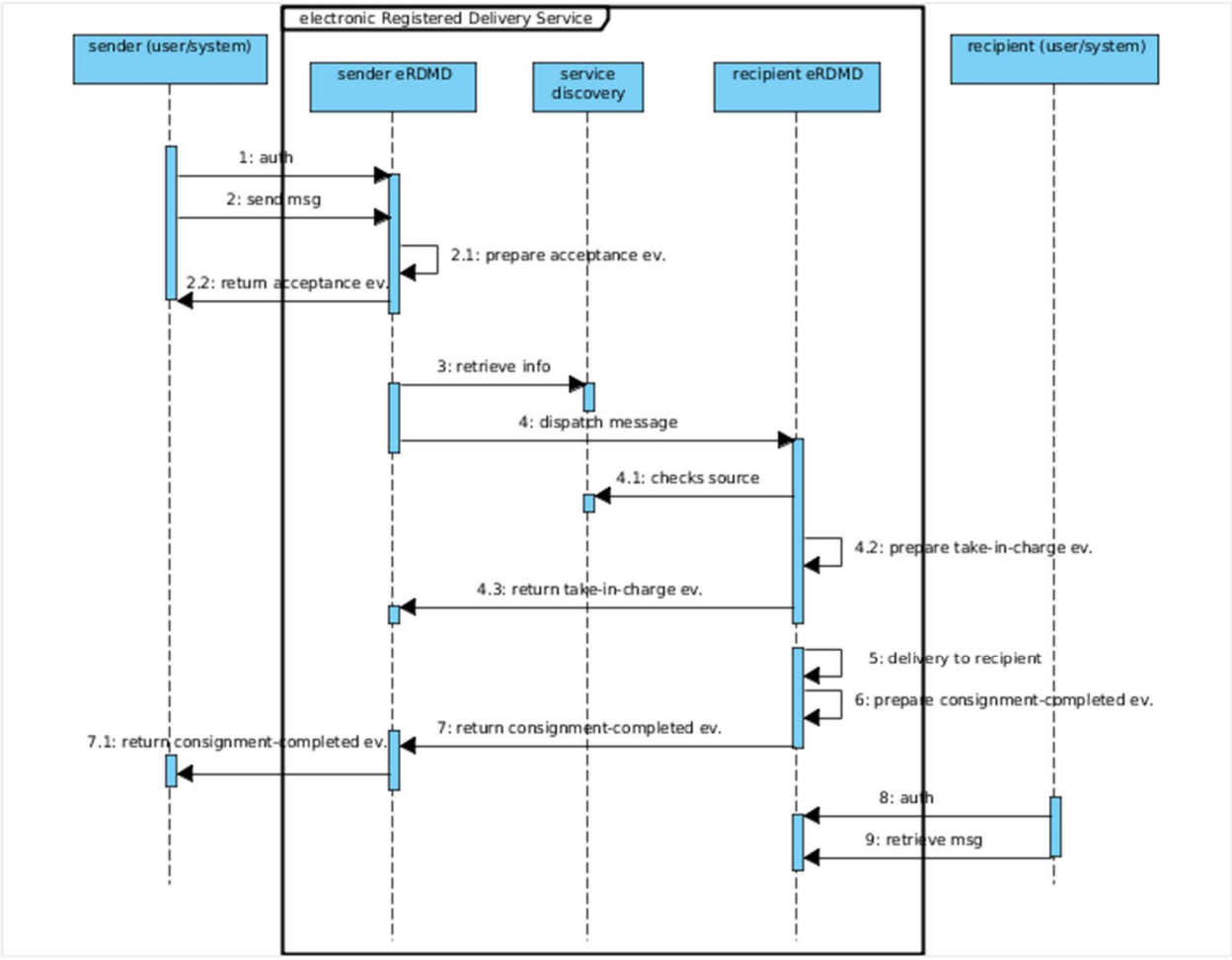


Figure 2: Distributed electronic registered delivery service model

1. The sender (either a user or a system) authenticates the eRDMD.

2. The sender (either a user or a system) prepares a message, specifies one or more recipients, indicates some options on the registered delivery service required, and submits it to the eRDMD.

2.1. At this point the eRDMD tracks the event that the message has been submitted (submission evidence).

2.2. Sometimes the evidence is sent back to the sender.

3. The sender's eRDMD retrieves the necessary information on the recipient's eRDMD from a service discovery service. This is an abstract entity, which may correspond to several distinct actors, in order to perform different tasks like:

   - Get routing information: Depending on the underlying transport, this may be standard DNS lookup or lookup to a specific registry.

- Retrieve remote eRDMD capabilities information and conduct a handshake in order to negotiate on different aspects (security management, payload and related meta data, provision of evidence, strength of authentication of end entities, etc.).

- Establish trust on remote eRDMD, possibly checking against a trust information provider (in a restricted network, peer-to-peer agreements may be established with no central trust information provider). Since trust networks are normally stable over long time periods and not changing frequently, the process does not necessarily need an on-line transaction.

4. The message is dispatched to the recipient's eRDMD (in case of more recipients, the message is dispatched to the respective eRDMDs). Before doing this, the eRDMD usually adds some meta-information using an envelope. The meta-information includes information which is relevant to the recipient, e.g. to establish the identity of the sender, the time of sending, etc.

4.1. The recipient's eRDMD may check, on its turn, that the sender's eRDMD is trustable.

4.2. The recipient's eRDMD tracks the fact that a message has been relayed to itself (relay evidence).

4.3. The evidence that the message has been taken in charge is optionally handed back to the sender's eRDMD (so that it can substantiate that it accomplished its task).

5. The message is delivered to the recipient.

6. The recipient's eRDMD tracks the event that the message has been made available to the recipient (consignment-completed evidence).

7. The consignment-completed evidence is normally sent back to the sender's eRDMD.

7.1. The sender's eRDMD can hand the evidence back to the sender (or can store the evidence for a later request).

8. The recipient (either a user or a system) authenticates to its eRDMD.

9. The recipient (either a user or a system) gets the message.

The model does not deal with other relevant evidence which may be available in some cases, most notably the evidence that the recipient actually retrieved the message from the system (retrieval evidence).

6.4 Extended electronic registered delivery service model

Several extensions are possible to the core models presented above, including additional features like message normalization, translation, storage, bridging to a different (electronic or traditional) messaging system, automatic signature verification, tracking of more specific events (like the forwarding of the message to a delegate, the opening of the message by the recipient, etc.).

While recognizing that all these extensions are relevant, the present document only focuses on those which have been considered by European Large Scale Pilots (LSP). Large scale pilots took place in a setting where there were already different, closed, non interoperable electronic (either registered or not) delivery solutions in place across Europe. To cope with this situation, a more complex service model was devised, called the 4-corner model, which is basically similar across the different LSPs. The model implies the implementation of an interoperability layer by means of a network of gateways and adapters interfacing to the different systems. This extended model is illustrated in Figure 3.

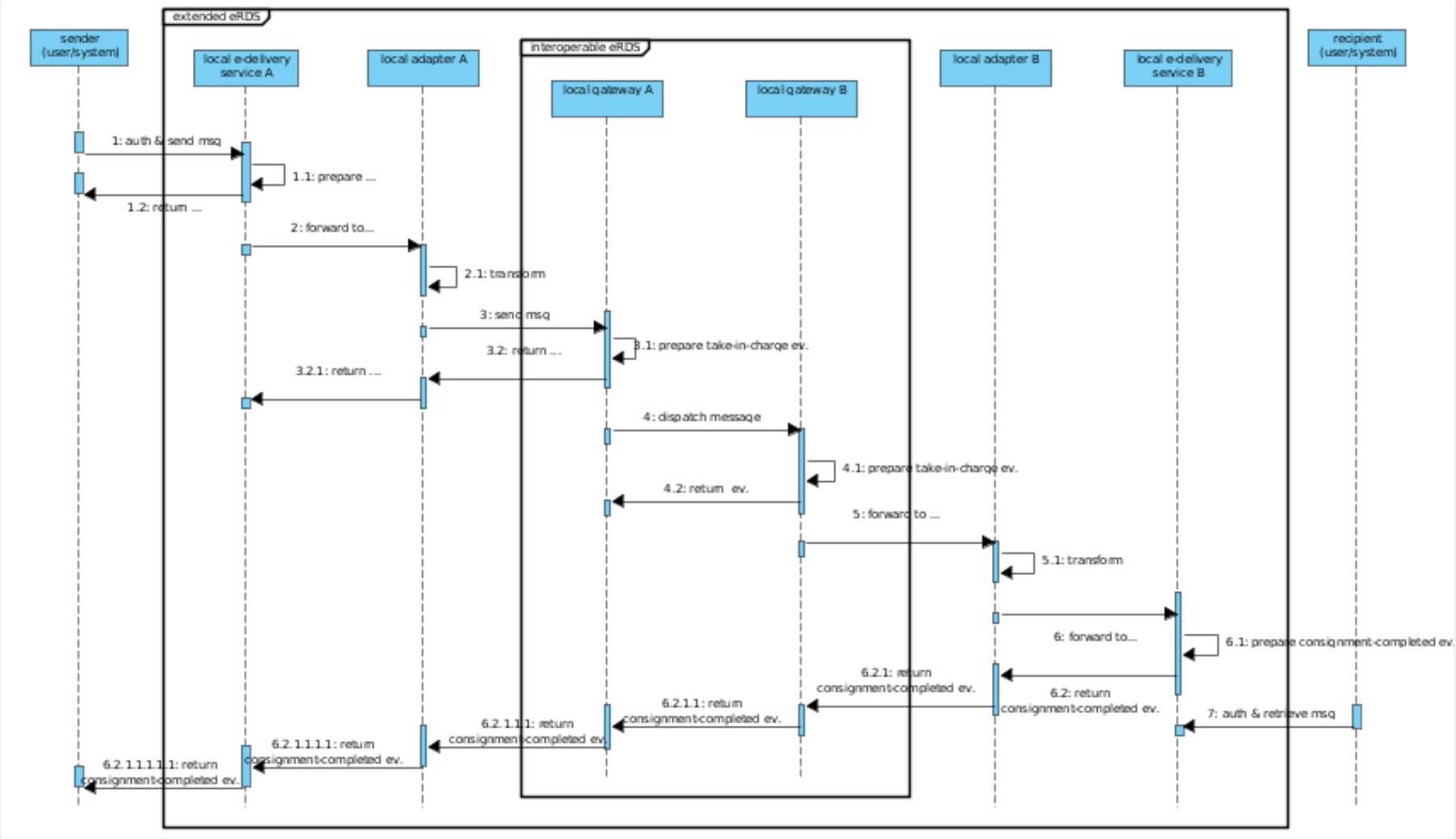


Figure 3: Extended electronic registered delivery service model

It appears that, while the users still perceive the service as a black-box (the larger box, named "extended electronic registered delivery service"), several interactions take place in between, which can be classified as:

- Sender side: includes the (non-interoperable) sender's electronic registered delivery solution and a translation to/from the interoperable electronic registered delivery network (the network of gateways).
- Interoperable electronic registered delivery network: the core network connecting local gateways which implements, to all effects, a distributed electronic registered delivery service (see clause 6.3), even if, for the sake of simplicity, the diagram does not show the service discovery agent inside it.
- Recipient side: includes the (non-interoperable) recipient's electronic registered delivery solution and a translation from/to the interoperable electronic registered delivery network (the network of gateways).

The schema is not exhaustive, since several other nodes may be included in the flow; they may be either transparent nodes (acting as message relay) or non-transparent nodes, providing extra services like semantic conversion, signature validation, business workflow, etc.

The local components of this extended model fall outside of the standardization domain, since they are largely constrained by legacy national/sector implementations.

6.5 Roles in electronic registered delivery management domains

The electronic registered delivery features, along with the service model described in previous clauses, drive to the identification of specific roles within an electronic registered delivery management domain. A role represents a high-level logical grouping of the features provided by an electronic registered delivery management domain. Roles do not necessarily map one-to-one on implementation components.

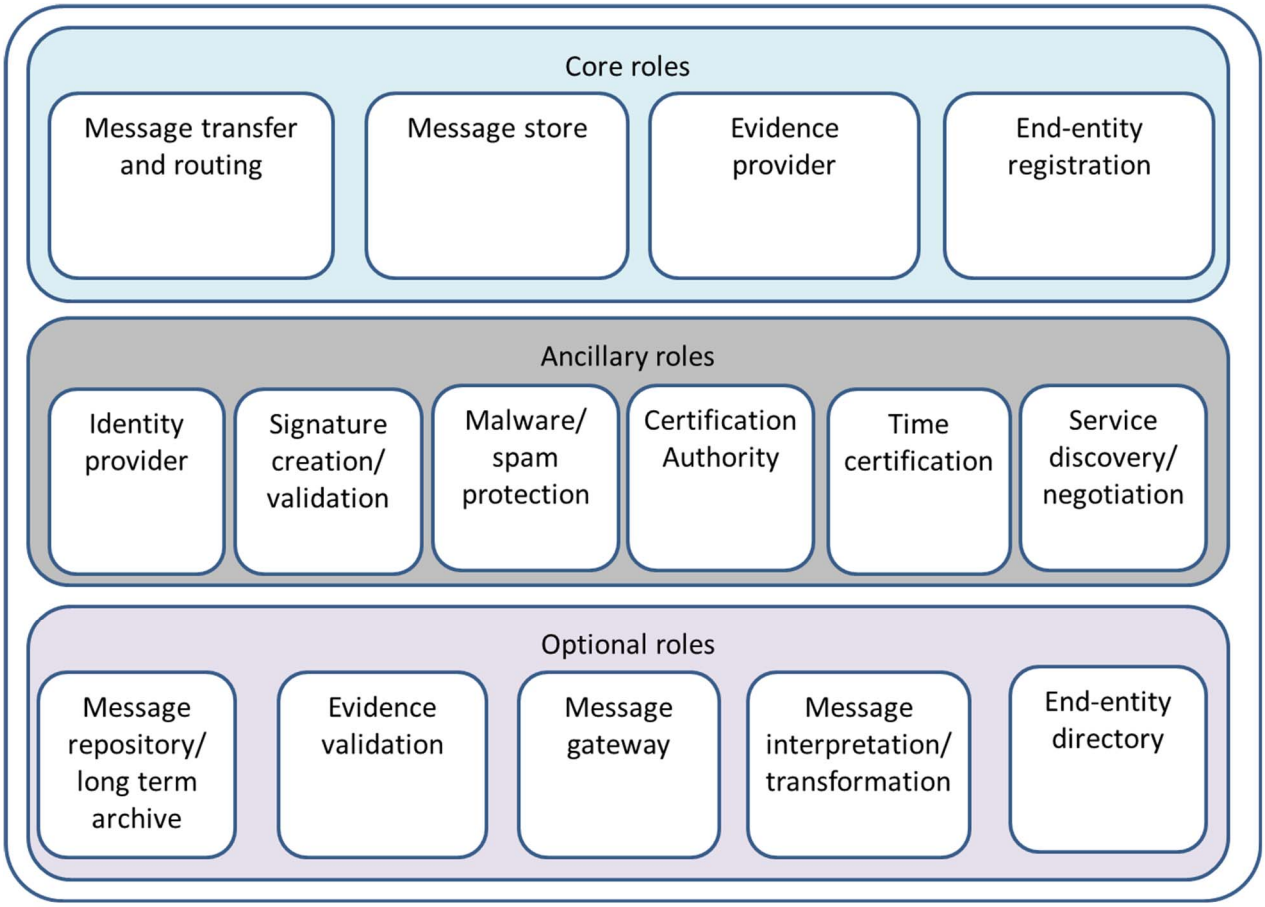


Figure 4: Roles in electronic registered delivery management domain

As illustrated in Figure 4, an electronic registered delivery management domain necessarily includes the following core roles:

- **Message transfer and routing:** for the (secure and reliable) transfer of the message from the sender to the recipient.
- **Message store:** to support asynchronous transmission.
- **Evidence provider:** for the production of evidence attesting the different events in the electronic registered delivery process.

And

- **End-entity registration:** for the registration of end-entities to the service, associating them with an address for electronic registered delivery. This role is not required if the end-entities are addressed by some direct identifier (e.g. the fiscal code).

An electronic registered delivery management domain necessarily includes the following ancillary roles. Ancillary roles differ from core roles since they are not specific to electronic registered delivery and can be delegated to third parties:

- **Identity provider:** for the provisioning of an electronic identity to end users (hence including a registration authority role) and for the subsequent authentication of end-users to the service.
- **Signature creation/validation:** for the creation/validation of signatures on evidence as well as for signing/validating payload.
- **Malware/ spam protection:** for the protection of user and systems against malware and spam.
- **Certification authority:** for providing the actors with the necessary keys and certificates (for securing the transport, for the creation/validation of signatures on evidence, etc.).
- **Time certification:** for ensuring a reliable time reference on the evidence/signatures. It can be implemented by a time stamping authority or by different means, provided that the provider has gone through an appropriate assessment process.

And

- **Service discovery/negotiation:** for the proper management of the service discovery, for the exposure of additional characteristics of electronic registered delivery management domains (requirements and/or capabilities) and for the negotiation process against peer domains.

To provide further features, an electronic registered delivery management domain can include optional roles, like:

- **Message repository/long term storage:** for archiving services for the messages.
- **Evidence validation:** for a validation service for the evidence generated in the process.
- **Message gateway:** for the transfer of electronic registered delivery messages to and from external electronic/traditional delivery services.
- **Message interpretation/transformation:** for the semantic interpretation, translation, transformation of message's format.

Or

- **End-entity directory**: for the discovery of end users of the system.

Table 2 summarizes the allocation of electronic registered delivery service features identified in clause 5 to the appropriate role.

Table 2: Features and Roles

Feature name	Role implementing the feature
User authentication	End-entity registration Identity provider
Node authentication	Message transfer and routing
Non-repudiation	Evidence provider Signature creation/validation
Confidentiality	Message transfer and routing
Integrity	Message transfer Evidence provider Signature creation/validation
Reliable delivery	Message transfer and routing Evidence provider
Antivirus	Malware/spam protection
Antispam	Malware/spam protection
Time reference	Time certification
Electronic Signature provision	Signature creation/validation
Service Trust	Service discovery/negotiation
Service Discovery	Service discovery/negotiation
User Discovery	End-entity directory Registration
Address management	Message transfer and routing Service discovery/negotiation
Translation	Message interpretation/transformation
Semantic check	Message interpretation/transformation
Structured/Non-Structured contents	Message interpretation/transformation
Service Level/ Provision Negotiation	Service discovery/ negotiation
Evidence validation	Evidence validation
Electronic Signature validation	Signature creation/validation
Deadlines	Message transfer Evidence provider Service discovery/negotiation
Governance	---

6.6 Implications to standardization activities

6.6.1 Introduction

From a standardization perspective, the basic service model (clause 6.2) raises some relevant issues related to conformance: in order to qualify as an electronic registered delivery service according to the eIDAS Regulation [i.4], some basic features have to be provided. Some more advanced features are required for qualified electronic delivery service.

NOTE: The basic model also raises a standardization issue on external interfaces, since the definition of a standard interface to sender/recipient (especially if they are systems) would allow for seamless switch from a provider to another. However this is not a core interoperability requirement, so it is not dealt with in the present document.

The distributed service model adds some more issues, related to the information flow between eRDMDs. According to the distributed sequence diagram, three different interactions should be supported:

- Service discovery/negotiation. This interaction can be further split into "getting routing information", "trust establishment", "capability negotiation", as detailed in clause 6.3.
- Payload delivery. It includes payload security and additional meta-data.

And

- Evidence and identification information. It includes the exchange of evidence and identity information in order to promote the message exchange to a registered status.

In order for two providers to interact, the information flow between eRDMDs need to be fully specified according to the layers introduced in EIF [i.30], in terms of content semantics (the transported information, at a semantic level), content syntax (the format for the above content), messaging protocol (the protocol used for the transmission of the information).

Many standards are already in place which can be used for the specification of these aspects on the three interactions: for instance, DNS is a candidate for routing information semantics, syntax and protocol, S/MIME can play a role as payload delivery syntax, TSL can be used for trust content and syntax, while ebMS [i.24] and SMTP [i.25] are two likely alternatives for the protocol of payload delivery.

Table 3 summarizes the necessary specifications for interoperable electronic registered delivery and whether they are currently available or need to be provided by future standardization activities.

Rows within table 3 identify the aforementioned components. Columns within this table identify the three main aspects that need to be covered in each component, unless stated otherwise, namely: their content and semantics, their syntax, and the messaging protocol supporting them. Components which are not already provided (or, at least, not fully provided) by existing known standards are marked as "In scope" of a standardization activity for electronic registered delivery, which may result either in the production of the specific targeted specification or in the profiling of existing standards. Cells are coloured in red when the implementation of a full specification is foreseen, in yellow when an extension/profiling to an existing specification is envisaged.

Table 3: Classification for e-Delivery specifications

		Content Semantics	Content syntax	Messaging protocol
Message delivery	Payload delivery	Out of scope	Out of scope	Out of scope
	Meta-information exchange	In scope	In scope	Partially in scope (binding)
Evidence and Identification	User identity exchange	Partially in scope (profiling)	Partially in scope (profiling)	Partially in scope (binding)
	Evidence exchange	In scope	In scope	Partially in scope (binding)
Service discovery	Routing	Out of scope	Out of scope	Out of scope
	Capabilities/requirements	In scope	Partially in scope (extension)	Partially in scope (binding)
	Trust establishment	In scope	Partially in scope (extension)	Partially in scope (binding)

6.6.2 Routing

eRDMD locate the remote counterpart based on the addressee (routing), however this is often provided by standard lookup facilities (e.g. DNS) or other facilities in connection with the transport protocol, so it is largely out of scope.

6.6.3 Capabilities/Requirements

eRDMD need to identify the capabilities and compliance to requirements of the remote counterpart in order to negotiate the appropriate parameters and perform the delivery according to the instruction of the sender. While there are several existing standards which can apply to this interaction, there are some points of interest to electronic registered delivery standardization:

- The contents of the electronic registered delivery specific negotiation parameters need to be standardized.

And

- An appropriate extension to the syntax for electronic registered delivery negotiation may be required.

6.6.4 Trust Establishment

eRDMD need to trust the remote counterpart, otherwise they would not forward the message. The candidate to this purpose is the trusted lists ETSI TS 119 612 [i.6] as required by Commission Decision CD 2009/767/EC as amended ([i.2], [i.3], [i.35]). The specific content for electronic registered delivery needs to be standardized (possibly, leveraging on the trusted lists ETSI TS 119 612 [i.6] extension mechanism). The binding to a protocol may be required, depending on the specific technology (under the trusted lists model implemented according to Commission Decision 2010/425/EU [i.3] this is a minor issue, since the list is published in some central site in order to be made available to all the participants to the process).

6.6.5 Payload Delivery

eRDMD need to interact for payload delivery. A number of well-established messaging protocols exist able to perform this task. The rationalized framework of standards for electronic registered delivery, however, neither does make a choice among them, nor defines a new one. What is actually relevant is that eRDMDs share a way to declare - either in-band or out-of-band - what the supported protocols are (through service discovery features).

6.6.6 Meta-information Exchange

Payload delivery is associated to the transfer of meta-information which is relevant to the electronic registered delivery process. This falls in scope of the standardization activity for two aspects:

- Semantics/syntax: several electronic delivery solutions rely on specific metadata associated to the payload, or on some enveloping mechanism for packaging together the payload and the evidence (e.g. SMIME [i.16] or XML [i.23]).

And

- Protocol: the transport of the meta-information associated to the payload over a specific protocol may be regulated by specific binding procedures. More protocols may be supported through different bindings.

6.6.7 User Identity Exchange

In order to set up a registered delivery process, eRDMDs interact for the exchange of end-user identity information and related Level of Assurance (as defined, for instance, in Recommendation ITU-T X.1254 [i.19] or in the STORK project [i.37]). This implies:

- a profile of standard identity information tokens (e.g. X.509 [i.17], SAML [i.22], etc.); and

- a precise way to exchange the above information over a transport protocol (binding).

6.6.8 Evidence Exchange

In order to set up a registered delivery process, eRDMDs interact for evidence exchange. This implies:

- a common semantics and syntax for evidence (e.g., PDF [i.18] or XML [i.23]); and
- methods for the exchange of evidence, the exchange being either in push or pull mode:
  - Push mode: evidence is sent from the sender's eRDMD to the recipient's eRDMD; evidence is either attached to the payload (within an envelope packaging together payload and evidence) or detached (as a separate flow). In the first case, the transport protocol and the binding rules are shared with the payload delivery. In the second case evidence can flow on different transport layers, so one or more specific bindings are required.

  Or

  - Pull mode: nodes generating evidence provide stores for evidence and mechanisms for their delivery on request. In this case, one or more specific bindings for evidence pulling are required.

7 Inventory of existing specifications

As a major input to the development of the rationalized framework an inventory has been collected of existing standardization and publicly available specifications. This ensures that the rationalized framework has a sound basis of all the known specifications and provides a reference point for the gap analysis.

This inventory includes standards, publicly available and regulatory specifications from the international, pan European and sector domains. The inventory is focused on the standards and specifications related to core electronic registered delivery services, as identified in the model [clause 6]. Specifications related to ancillary services, which are nevertheless necessary to the implementation of a complete electronic registered delivery solution, are out of scope from the present inventory.

The inventory does not take into account national solutions or commercial offerings because of their great diversity. Many of such solutions are not even based on open specifications, since they are implemented in centralized systems which are not conceived for interoperability.

The detailed data collected in the inventory is provided as Annex B of the present document.

8 Rationalized structure for electronic registered delivery standardization documents

8.1 Electronic registered delivery standardization classification scheme

The rationalized structure for electronic signature standardization document (ETSI TR 119 000 [i.15]) provides the framework for the x19 000 series of documents on electronic signature standards and specifies the schema for electronic signature standardization. It is organized around:

- 6 areas of standardization: signature creation & validation, signature creation and other related devices, cryptographic suites, trust service providers supporting e-signatures, trust application service providers and trust service status lists providers. An additional area is gathering ETSI TR 119 000 [i.15] as well as studies and other introductory deliverables related to the rationalized structure of electronic signature standards; and
- 5 types of documents: guidance, policy & security requirements, technical specifications, conformity assessment, and testing conformance & interoperability.

ETSI TR 119 000 [i.15] provides more details.

The proposed rationalized structure for standards related to electronic registered delivery will fit in area 5 of the rationalized structure for electronic signature standardization [i.15], namely in the trust application service providers area. It is proposed to (re)organize area 5 into the following sub-areas:

- Data preservation (through signing) services;
- Electronic registered delivery services; and
- Registered electronic mail (REM) services.

8.2 Electronic registered delivery standardization proposal aligned with the rationalized framework and based on the model

The documents for electronic signature standardization for trust application service providers are summarized in table 4 with further details provided below. Documents unrelated to electronic registered delivery, while being included in the table for completeness, are not detailed in the text.

Table 4: Standards for Trust Application Service Providers

Trust Application Service Providers						
				Sub-areas		
					Guidance	
TR	1	19	5	0	0	Business Driven Guidance for Trust Application Service Providers
SR	0	19	5	3	0	Study on Standardisation Requirements for Electronic Registered Delivery Services applying e-Signatures
					Policy & Security Requirements	
EN	3	19	5	1	1	Policy & Security Requirements for Data Preservation Service Providers (DPSPs)
EN	3	19	5	2	1	Policy & Security Requirements for Electronic Registered Delivery Service Providers
						Part 1: Policy and Security Requirements for TASPs providing Electronic Registered Delivery Services
						Part 2: Policy and Security Requirements for TASPs providing Qualified Electronic Registered Delivery Services
EN	3	19	5	3	1	Policy & Security Requirements for Registered Electronic Mail (REM) Service Providers
						Part 1: Policy and Security Requirements for TASPs providing REM Services
						Part 2: Policy and Security Requirements for TASPs providing Qualified REM Services
					Technical Specifications	
EN	3	19	5	1	2	Data Preservation Services through signing
EN	3	19	5	2	2	Electronic Registered Delivery Services
						Part 1: Framework and Architecture
						Part 2: Semantic Contents
						Part 3: Formats
						Part 4: Bindings
						Part 5: Tehcnical Specifications for Qualified Electronic Registered Delivery Services
EN	3	19	5	3	2	Registered Electronic Mail (REM) Services
						Part 1: Framework and Architecture
						Part 2: Semantic Contents
						Part 3: Formats
						Part 4: Interoperability Profiles
					Testing Conformance & Interoperability	
TS	1	19	5	0	4	General Requirements for Testing Conformance & Interoperabiltity of Trust Application Services
TS	1	19	5	1	4	Testing Conformance & Interoperability of Data Preservation Services
TS	1	19	5	2	4	Testing Conformance & Interoperability of Electronic Registered Delivery Services
						Part 1: Test suites for Interoperability Testing of Electronic Registered Delivery Services
						Part 2: Testing Conformance of Electronic Registered Delivery Services
TS	1	19	5	3	4	Testing Conformance & Interoperability of Registered Electronic Mail Services
						Part 1: Test suites for Interoperability Testing of Services using same Format and Transport Protocols
						Part 2: Test suites for Interoperability Testing of Services using different Format and Transport Protocols
						Part 3: Testing Conformance of Registered Electronic Mail Services

Guidance

ETSI TR 119 500: Business Driven Guidance for Trust Application Service Provider
This document provides guidance for the selection of standards for Trust Application Service Providers for given business requirements. It includes guidance for electronic registered delivery service providers.

Policy and Security Requirements

ETSI EN 319 521: Policy & Security Requirements for Electronic Registered Delivery Service Providers
This document specifies policy and security requirements for TASPs providing electronic registered delivery services and for TASPs providing qualified electronic registered delivery services considering, when necessary, different styles of operation. This is a multi-part document structured as follows:

- **ETSI EN 319 521-1: Policy and Security Requirements for TASPs providing Electronic Registered Delivery Services**
  This part defines policy and security requirements specific to TASPs providing electronic registered delivery services. It also addresses specific requirements on information security management for this type of TASPs. Informative annexes provide check lists for conformity assessment.

- **ETSI EN 319 521-2: Policy and Security Requirements for TASPs providing Qualified Electronic Registered Delivery Services**
  This part defines policy and security requirements that are specific to the TASPs providing qualified electronic registered delivery services. It also addresses specific requirements on information security management for this type of TASPs. Informative annexes provide check lists for conformity assessment.

ETSI EN 319 531: Policy & Security Requirements for Registered Electronic Mail (REM) Service Providers
This document specifies policy and security requirements which are particular to TASPs providing registered electronic mail services and for TASPs providing qualified registered electronic mail services considering, when necessary, different styles of operation.

The production of this document is conditioned to the identification of requirements which are specific to REM and do not apply to general electronic registered delivery services.

This is a multi-part document structured as follows:

- **ETSI EN 319 531-1: Policy and Security Requirements for TASPs providing Registered Electronic Mail Services**
  This part defines policy and security requirements specific to TASPs providing registered electronic mail services. It also addresses specific requirements on information security management for this type of TASPs. Informative annexes provide check lists for conformity assessment.

- **ETSI EN 319 531-2: Policy and Security Requirements for TASPs providing Qualified Registered Electronic Mail Services**
  This part defines policy and security requirements that are specific to the TASPs providing qualified registered electronic mail services. It also addresses specific requirements on information security management for this type of TASPs. Informative annexes provide check lists for conformity assessment.

Technical Specifications

ETSI EN 319 522: Electronic Registered Delivery Services
This document provides technical specifications for the provision of electronic registered delivery services in line with article 41 of eIDAS Regulation [i.4]. This is a multi-part document, initially structured in three parts as detailed below. Nevertheless, new parts could appear in the future if new architectural elements not identified at the time of writing the present document, are proposed and accepted. Should this happen, part 1 (Framework and Architecture) should be updated and extended to be aligned with the new part.

- **ETSI EN 319 522-1: Framework and Architecture**
  This is a document providing an overview of the whole set of specifications included in the technical specification. It also includes an overall view of the standardized service, addressing at least the following aspects:

  - Logical model, including an overview of the different entities, components and events involved in an electronic registered delivery transaction.

  - Interfaces between the different roles and providers.

- Relevant events in the data object flows and the corresponding evidence. And
- Trust building among providers pertaining to the same or to different administrative domains.

- **ETSI EN 319 522-2: Semantic Contents**
  This document provides a specification of the semantic contents to be produced and managed in electronic registered delivery transactions, according to table 2 in clause 6.6. It deals with:
  - **Message delivery content.** Specifications of the semantic of the meta-information which will possibly be associated to the transmission of the payload.
  - **Evidence and identification content.** Specifications of the set of evidence managed in the context of the service provision. The document fully specifies the semantics, the components, and the components' semantics for all the evidence. The document also specifies the content related to end user identity to be managed in the transactions. And
  - **Service discovery content.** Specifications of the information related to the identification of the remote eRDMD, the negotiation of capabilities and requirements that a service supports and the information related to the establishment of trust of a service (e.g. the content that will appear in an appropriate TSL extension for electronic registered delivery services).

- **ETSI EN 319 522-3: Formats**
  This document provides a specification of the formats for the different contents to be produced and managed in electronic registered delivery transactions, according to table 2 in clause 6.6. This is an open part where additional sub-parts could be added in the future if required. At this point in time it is proposed that this document deals with:
  - **Message delivery formats.** Specifications of the format/formats for the meta-information specified in EN 119 522-2. Meta-information may come either in attached (as an envelope including the payload) or detached format.
  - **Evidence and identification formats.** Specifications of the syntax for the set of evidence and user identity information specified in ETSI EN 319 522-2.
  - **Service discovery formats.** Specifications of the format/formats for capabilities, requirements and trust information specified in ETSI EN 319 522-2.

- **ETSI EN 319 522-4: Bindings**
  This is a multi-part document. Each part fully specifies the binding to a messaging protocol that is supporting electronic registered delivery services provision. This includes specification on how to transport evidence within the protocols messages, how to include signature's provider within the protocol's message, etc. Each part specifies anything that is required to ensure interoperability among providers of the service being compliant with that part. This is an open part where additional sub-parts could be added in the future if required. At this point in time it is proposed that this document has the following parts:
  - **One or more parts on message delivery binding(s):** this (these) document(s) specify(es) binding(s) for a number of identified relevant messaging protocols (such as SOAP [i.28] or any of its profiles like ebMS 3.0 [i.24], Busdox [i.34], PReM [i.5], or any other that is considered worth to include).
  - **One or more parts on evidence and identification binding(s):** this (these) document(s) specify(es) binding(s) for a number of identified relevant messaging protocols (such as SOAP [i.28] or any of its profiles like e-bMS 3.0 [i.24], Busdox [i.34], PReM [i.5], or any other that is considered worth to include) or trust token exchange protocols (which may be completely unrelated to the messaging protocols).

  And

  - **One or more parts on capability/requirements binding(s):** this (these) document(s) specify(es) binding(s) for the exchange of capability information on a number of identified relevant metadata-exchange protocols, which may be neutral with respect to the messaging protocol and unrelated to it.

- **ETSI EN 319 522-5: Technical Specifications for Qualified Electronic Registered Delivery Services**
  This document provides technical specifications that are particular to the provisioning of qualified electronic delivery services, in line with the requirements provided by article 42 of eIDAS Regulation [i.4].

ETSI EN 319 532: Registered Electronic Mail (REM) Services
This document provides technical specifications for the provision of registered electronic mail. This is a multi-part document whose structure is detailed below. This list could change if some of the parts are considered not needed after the production of ETSI EN 319 522, in which case the numbering of parts will change accordingly:

- **ETSI EN 319 532-1: Framework and Architecture**
  This document provides an overview of the whole set of specifications included in the technical specification. It also includes aspects of the provision of registered electronic mail (REM) standardized services, that are not common to the provision of other types of electronic registered delivery provision, but specific to REM. The production of this part is conditioned to the identification of requirements which are specific to REM and do not apply to general electronic registered delivery services and to the identification of mandatory requirements.

- **ETSI EN 319 532-2: Semantic Contents**
  If needed this document specifies semantic contents to be produced and managed in REM transactions, which are not common to the provision of other types of electronic delivery services, but specific to the provision of REM services. The production of this part is conditioned to the identification of semantic contents which are specific to REM and do not apply to general electronic registered delivery service.

- **ETSI EN 319 532-3: Formats**
  This document specifies the formats for the different messages to be produced and managed in REM transactions using SMIME on SMTP. The production of this part is conditioned to the identification of issues which are specific to REM and cannot be naturally dealt within a sub-part on message delivery binding of ETSI EN 319 522-4.

- **ETSI EN 319 532-4: Interoperability profiles**
  This part contains several sub-parts. Each sub-part specifies profile(s) for seamless exchange of data objects across providers that use the same or different formats and/or transport protocols. Below follows the list of the identified sub-parts:

  - Sub-Part 1: SMTP Interoperability profile. This document specifies a profile ensuring interoperability between REM services providers using SMIME on SMTP.

  - Sub-Part 2: REM-MD UPU Interoperability profile. This document specifies a profile ensuring interoperability between REM services providers and providers based on PReM [i.5].

Testing Conformance and Interoperability

ETSI TS 119 504: General requirements for Testing Conformance & Interoperability of Trust Application Services
This document specifies general requirements for specifying technical conformance and interoperability testing for TASPs. This document will consider the electronic registered delivery subarea.

ETSI TS 119 524: Testing Conformance & Interoperability of Electronic Registered Delivery Services
This document defines test suites that support interoperability tests among entities providing electronic registered delivery services. It also specifies tests to be performed for checking conformance against relevant specifications of ETSI EN 319 522. This is a multi-part document, whose structure is detailed below:

- **Part 1: Test Suites for Interoperability Testing of Electronic Registered Delivery Services**. This document specifies tests suites for supporting interoperability tests between providers that are using the same syntax for the evidence and/or the same binding to messaging protocols.

- **Part 2: Testing Conformance of Electronic Registered Delivery Services**: This document specifies the tests to be performed for checking conformance against relevant specifications of ETSI EN 319 522. This provides the basis for a tool that automatically checks conformance against the aforementioned relevant specifications.

ETSI TS 119 534: Testing Conformance & Interoperability of Registered Electronic Mail Services
This document defines test suites that support interoperability tests among entities providing this type of services. This is a multi-part document, whose structure is detailed below:

- **Test Suites for Interoperability Testing of Services using same Format and Transport Protocols**. This document applies to those providers that implement the service provision using the same combination of format and transport protocols.

- **Test Suites for Interoperability Testing of Services using different Format and Transport Protocols**. This document applies to those providers that implement the service provision using different combinations of format and transport protocols. This document defines test-suites for the interoperability profiles for REM.

- **Testing Conformance of Registered Electronic Mail Services**: This document specifies test assertions for checking conformance against ETSI EN 319 532. This could be the basis for developing a tool that could automatically check that the messages and evidence set generated by a certain provider are fully compliant with the relevant aforementioned specifications.

9 Analysis and work plan

9.1 Methodology

The analysis and resulting work plan are placed in a set of tables on a per document basis in tables showing:

a) The analysis of the required scope of each document identified in the rationalized structure against the currently available specifications identifying those whose scope most closely matches that of the required scope.

b) The work plan required to produce the required document from the currently available specifications.

The analysis identifies the existing documents from the inventory whose scope is near that of the required document in the rationalized framework and indicates the degree to which the requirements are met as follows:

1) Scope fully met: A document already exists at the level of standardization needed and with the required scope.

2) Scope nearly met: A document already exists but requires some minor enhancements to fulfil the required scope and / or completion of progression to the required level of standardization (e.g. finalizing EN).

3) Requirement partially met: A document already exists but some enhancements are needed to meet the required scope and/or the standardization level is not sufficient.

4) Inputs exist: Documents exist in the inventory which could be used as the basis of the required standard but significant work is required to bring the document to the required level of standardization addressing the identified scope.

5) Little basis: There is little basis for this document required.

The work plan identifies the tasks to be carried out to produce a document of the required scope and an indication or the expected time-scale.

9.2 Analysis and work plan for trust application service providers area

Tables 5 to 8 below present an analysis and work plan for the deliverables identified in clause 8.2 and other deliverables identified in ETSI TR 119 000 [i.15] which should be modified in coherence with the present proposal.

Table 5: Analysis and work plan for guidance documents

Deliverable id	Type	Title and Contents
GUIDANCE DOCUMENTS		
119 500	**TR**	**Title: Business Driven Guidance for Trust Application Service Providers**
		Description: This document provides guidance for the selection of standards for trusted application service providers for given business requirements. The document identifies a number of relevant trusted application services using electronic signatures in different business areas, and whose provision has already been standardized. Additionally, for each of the services, it provides guidance for the selection of the suitable standards, ensuring in this way their correct provision and interoperability across the European Union.
		ANALYSIS: **Relevant inputs as a result from analysis:** • Starting points: first published version of the deliverable. • Degree to which scope is met considering starting points: – Partially met, as a result of work performed to produce first publication.
		WORK PLAN **Task to be carried out:** • Production of a new version of this TR that will include guidance for trust applications services providers providing electronic delivery services. **Timescale** (planning)**:** • Start: T0 • Complete: T0+8

Table 6: Analysis and work plan for policy and security requirements documents

Deliverable id	Type	Title and Contents
POLICY AND SECURITY REQUIREMENTS DOCUMENTS		
319 521	**EN**	**Title: Policy & Security Requirements for Electronic Registered Delivery Service Providers**
		Description: This document defines the policy requirements that are specific for electronic delivery service providers required to be recognized as a provider of this type of services. It might define different conformance levels for each style of operation and the corresponding set of requirements to be satisfied in each level. It references ETSI EN 319 501 for generic requirements.
		ANALYSIS: **Relevant inputs from inventory (starting points) as a result from analysis:** • Starting points: ETSI TS 102 640-3 [i.9] V2.1.2 (2011-09) Registered Electronic Mail (REM); Architecture, Formats and Policies- Part 3: Information Security Policy Requirements for REM Management Domains; • Reasons why selecting starting points: These documents include security requirements of REM services. They will be reviewed in order to identify which ones are specific to REM service providers (and consequently be moved to ETSI EN 319 521) and which ones are common to any type of electronic delivery service providers. • Degree to which scope is met considering starting points: – Input exists
		WORK PLAN **Task to be carried out:** • Production of a EN based on a number of existing documents (including stakeholder consultation) **Timescale** (planning)**:** • Start: T0 • Complete: T0+10+8

319 531	**EN**	**Title: Policy & Security Requirements for Registered Electronic Mail (REM) Service Providers**
		Description: This document defines policy requirements that are specific for REM service providers required to be recognized as a provider of this type of services. It might define different conformance levels for each style of operation and the corresponding set of requirements to be satisfied in each level. It references ETSI EN 319 401 [i.38] for generic requirements and ETSI EN 319 521 for common requirements of electronic delivery service providers, of which REM service providers are a specific type. The production of this document is conditioned to the identification of requirements which are specific to REM and do not apply to general electronic registered delivery services.
		ANALYSIS: **Relevant inputs from inventory (starting points) as a result from analysis:** • Starting points: ETSI TS 102 640-3 [i.9] V2.1.2 (2011-09) Registered Electronic Mail (REM); Architecture, Formats and Policies- Part 3: Information Security Policy Requirements for REM Management Domains; ETSI TS 102 640-4 [i.10] Registered Electronic Mail (REM): Architecture, Formats and Policies - Part 4: REM-MD Conformance Profiles • Reasons why selecting starting points: These documents include security requirements of REM services • Degree to which scope is met considering starting points: – Input exists
		WORK PLAN **Task to be carried out:** Production of a new EN (e.g. EN, TS) based on a number of existing documents (including stakeholder consultation). The production of this document is conditioned to the identification of requirements which are specific to REM and do not apply to general electronic registered delivery services **Timescale (planning):** • Start: T0 • Complete: T0+10+8

Table 7: Analysis and work plan for technical specifications documents

Deliverable id	Type	Title and Contents
		TECHNICAL SPECIFICATION DOCUMENTS
319 522	**EN**	**Title: Electronic Registered Delivery Services**
		Description: This document provides technical specifications for the provision of registered electronic mail. This is a multi-part document whose structure is detailed below: **ETSI EN 319 522-1: Framework and Architecture**. This document provides an overview of the whole set of specifications included in the technical specification. It also includes an overall view of the standardized service, addressing at least the following aspects: • Logical model, including an overview of the different entities, components and events involved in an e-Delivery transaction. • Interfaces between the different roles and providers. • Relevant events in the data object flows and the corresponding evidence. • Trust building among providers pertaining to the same or to different administrative domains.

		ETSI EN 319 522-2: Semantic Contents. This document provides a specification of the semantic contents to be produced and managed in electronic registered delivery transactions, according to table 2 in clause 6.6. It deals with: • **Message delivery content.** Specifications of the semantic of the meta-information which will possibly be associated to the transmission of the payload. • **Evidence and identification content**. Specifications of the set of evidence managed in the context of the service provision. The document fully specifies the semantics, the components, and the components' semantics for all the evidence. The document also specifies the content related to end user identity to be managed in the transactions. • **Service discovery content.** Specifications of the information related to the identification of the remote eRDMD, the negotiation of capabilities and requirements that a service supports and the information related to the establishment of trust of a service (e.g. the content that will appear in an appropriate TSL extension for electronic registered delivery services). **ETSI EN 319 522-3: Formats**. This document provides a specification of the formats for the different contents to be produced and managed in electronic registered delivery transactions, according to table 2 in clause 6.6. This is an open part where additional sub-parts could be added in the future if required. At this point in time it is proposed that this document deals with: • **Message delivery formats.** Specifications of the format/formats for the meta-information specified in EN 319 522-2. Meta-information may come either in attached (as an envelope including the payload) or detached format. • **Evidence and identification formats**. Specifications of the syntax for the set of evidence and user identity information specified in EN 319 522-2. • **Service discovery formats.** Specifications of the format/formats for capabilities, requirements and trust information specified in EN 319 522-2. **ETSI EN 319 522-4: Bindings**. This is a multi-part document. Each part fully specifies the binding to a messaging protocol that is supporting electronic delivery services provision. This includes specification on how to transport evidence within the protocols messages, how to include signature's provider within the protocol's message, etc. Each part specifies anything that is required to ensure interoperability among providers of the service being compliant with that part. This is an open part where additional sub-parts could be added in the future if required. At this point in time it is proposed that this document has the following parts: • **One or more parts on message delivery binding(s):** this (these) document(s) specify(es) binding(s) for a number of identified relevant messaging protocols (such as SOAP [i.28] or any of its profiles like ebMS 3.0 [i.24], Busdox [i.34], PReM [i.5], or any other that is considered worth to include). • **One or more parts on evidence and identification binding(s):** this (these) document(s) specify(es) binding(s) for a number of identified relevant messaging protocols (such as SOAP [i.28] or any of its profiles like ebMS 3.0 [i.24], Busdox [i.34], PReM [i.5], or any other that is considered worth to include) or trust token exchange protocols (which may be completely unrelated to the messaging protocols). • **One or more parts on capability/requirements binding(s):** this (these) document(s) specify(es) binding(s) for the exchange of capability information on a number of identified relevant metadata-exchange protocols, which may be neutral with respect to the messaging protocol and unrelated to it. **ETSI EN 319 522-5: Technical Specifications for Qualified Electronic Registered Delivery Services.** This document provides the full technical specifications which characterize a qualified electronic registered delivery service with respect to an electronic delivery service, in line with the requirements provided by article 42 of eIDAS Regulation [i.4].

		ANALYSIS: **Relevant inputs from inventory (starting points) as a result from analysis:** • Starting points: ETSI TS 102 640-1 [i.7] Registered Electronic Mail (REM); Architecture, Formats and Policies- Part 1: Architecture; ETSI TS 102 640-2 [i.8] Registered Electronic Mail (REM); Architecture, Formats and Policies- Part 2: Data requirements, Formats and Signatures for REM. • ETSI TS 102 640-6 [i.12] to [i.14] Registered Electronic Mail (REM); Architecture, Formats and Policies- Part 6: "Interoperability Profiles" - Sub-part 3: "REM-MD SOAP Binding Profile". • Reasons why selecting starting points: ETSI TS 102 640-1 [i.7] covers general principles of REM services provision, including architecture and roles. Being REM services a specific type of Electronic Delivery Services, part of the material in this document would also apply in ETSI EN 319 532-1. ETSI TS 102 640-6-2 [i.13] specifies a binding for SOAP on HTTP, and will be the starting point for producing ETSI EN 319 532-4-1. • Degree to which scope is met considering starting points: – Little basis except for ETSI EN 319 532-4-1
		WORK PLAN **Task to be carried out:** • Production of an EN. **Timescale** (planning): • Start: T0 • Complete: T0+12+12
319 532	**EN**	**Title: Registered Electronic Mail (REM) Services** **Description:** This document provides technical specifications for the provision of registered electronic mail. This is a multi-part document whose structure is detailed below. This list could change if some of the parts are considered not needed after the production of ETSI EN 319 522, in which case the numbering of parts will change accordingly: **ETSI EN 319 532-1: Framework, Architecture.** This document provides an overview of the whole set of specifications included in the technical specification. It also includes aspects of the provision of registered electronic mail (REM) standardized services, that are not common to the provision of other types of electronic delivery provision, but specific to REM. The production of this part is conditioned to the identification of requirements which are specific to REM and do not apply to general electronic registered delivery services and to the identification of mandatory requirements. **ETSI EN 319 532-2: Semantic Contents**. If needed this document specifies semantic contents to be produced and managed in REM transactions, which are not common to the provision of other types of electronic delivery services, but specific to the provision of REM services. The production of this part is conditioned to the identification of semantic contents which are specific to REM and do not apply to general electronic registered delivery service. **ETSI EN 319 532-3: Formats**. This document specifies the formats for the different messages to be produced and managed in REM transactions using SMIME on SMTP. The production of this part is conditioned to the identification of issues which are specific to REM and cannot be naturally dealt with in a sub-part on message delivery binding of ETSI EN 319 522-4. **ETSI EN 319 532-4: Interoperability profiles**. This part contains several sub-parts. Each sub-part specifies profile(s) for seamless exchange of data objects across providers that use the same or different formats and/or transport protocols. Below follows the list of the identified sub-parts: • Sub-Part 1: SMTP Interoperability profile. This document specifies a profile ensuring interoperability between REM services providers using SMIME on SMTP. • Sub-Part 2: REM-MD UPU Interoperability profile. This document specifies a profile ensuring interoperability between REM services providers and providers based on PReM [i.5].

		ANALYSIS: **Relevant inputs from inventory (starting points) as a result from analysis:** • Starting points: – ETSI TS 102 640-1 [i.7] Registered Electronic Mail (REM); Architecture, Formats and Policies- Part 1: Architecture; – ETSI TS 102 640-2 [i.8] Registered Electronic Mail (REM); Architecture, Formats and Policies- Part 2: Data requirements, Formats and Signatures for REM. – ETSI TS 102 640-5 [i.11] Registered Electronic Mail (REM); Architecture, Formats and Policies- Part 5: REM-MD Interoperability Profiles. – ETSI TS 102 640-6 [i.12] to [i.14] Registered Electronic Mail (REM); Architecture, Formats and Policies- Part 6: "Interoperability Profiles". • Reasons why selecting starting points: These documents initially cover the scope. A review will be necessary for suitable update of their contents and for selection of the material to be incorporated in the new EN. • Degree to which scope is met considering starting points: – Scope almost fully met
		WORK PLAN **Task to be carried out:** • Production of an EN from an existing document with minor updates **Timescale** (planning): • Start: T0 • Complete: T0+12

Table 8: Analysis and work plan for testing compliance and interoperability documents

Deliverable id	Type	Title and Contents
		TESTING COMPLIANCE & INTEROPERABILITY
119 504	**TS**	**Title: General requirements for Technical Conformance & Interoperability Testing for Trust Application Service Providers and the Services they Provide**
		Description: This document specifies general requirements for specifying technical conformance and interoperability testing for TASPs. This document will consider the electronic delivery subarea
		ANALYSIS: **Relevant inputs from inventory (starting points) as a result from analysis:** • Starting points: ETSI TS specifying interoperability test suites and conformance testing assertions for signature formats, and the already existing ETSI TR 103 071 [i.39] Test suite for future REM interoperability test events; ETSI TS 102 640-6 [i.12] to [i.14] Registered Electronic Mail (REM); Architecture, Formats and Policies- Part 6: "Interoperability Profiles", which includes test suites for testing interoperability among REM providers. Also any existing document dealing with interoperability and conformance issues for the protocols targeted by the selected bindings. • Degree to which scope is met considering starting points: – Some inputs exist
		WORK PLAN **Task to be carried out:** • Production of a new TS document based on a number of existing documents (including stakeholder consultation) **Timescale** (planning)**:** • Start: T0 • Complete: T0+12+12

<table>
<tr><td rowspan="3">119 514</td><td rowspan="3">TS</td><td>Title: Testing Compliance & Interoperability of Electronic Registered Delivery Services Providers</td></tr>
<tr><td>Description:
This document defines test suites that support interoperability tests among entities providing electronic delivery services. It also specifies tests to be performed for checking conformance against relevant specifications of ETSI EN 319 522. This is a multi-part document, whose structure is detailed below:
• Part 1: Test suites for interoperability testing of Electronic Registered Delivery Service Providers .This document specifies tests suites for supporting interoperability tests between providers that are using the same syntax for the evidence and/or the same binding to messaging protocols.
• Part 2: Testing conformance: This document specifies the tests to be performed for checking conformance against relevant specifications of ETSI EN 319 522. This provides the basis for a tool that automatically checks conformance against the aforementioned relevant specifications.</td></tr>
<tr><td>ANALYSIS:
Relevant inputs from inventory (starting points) as a result from analysis:
• Starting points: ETSI TS specifying interoperability test suites and conformance testing assertions for signature formats, and the already existing ETSI TR 103 071 [i.39] Test suite for future REM interoperability test events; ETSI TS 102 640-6 [i.12] to [i.14] Registered Electronic Mail (REM); Architecture, Formats and Policies- Part 6: "Interoperability Profiles", which includes test suites for testing interoperability among REM providers. Also any existing document dealing with interoperability and conformance issues for the protocols targeted by the selected bindings.
• Degree to which scope is met considering starting points:
o Some inputs exist</td></tr>
<tr><td></td><td></td><td>WORK PLAN
Task to be carried out:
• Production of a new TS document based on a number of existing documents (including stakeholder consultation)
Timescale (planning):
• Start: T0
• Complete: T0+12+12</td></tr>
<tr><td rowspan="2">19 524</td><td rowspan="2">TS</td><td>Title: Testing Compliance & Interoperability of Registered Electronic Mail Service Providers</td></tr>
<tr><td>Description:
This document defines test suites that support interoperability tests among entities that plan to provide this type of services. This is a multi-part document, whose structure is detailed below:
• Test suites for interoperability testing of providers using same format and transport protocols. This document applies to those providers that implement the service provision using the same combination of format and transport protocols.
• Test suites for interoperability testing of providers using different format and transport protocols. This document applies to those providers that implement the service provision using different combinations of format and transport protocols. This document defines test-suites for the interoperability profiles for REM.
• Testing conformance: This document specifies the tests to be performed for checking conformance against ETSI EN 319 532. This could be the basis for a tool that could automatically check that the messages and evidence set generated by a certain provider are fully compliant with the relevant aforementioned specifications.</td></tr>
</table>

		ANALYSIS: **Relevant inputs from inventory (starting points) as a result from analysis:** • Starting points: ETSI TR 103 071 [i.39] Test suite for future REM interoperability test events; ETSI TS 102 640-6 [i.12] to [i.14] Registered Electronic Mail (REM); Architecture, Formats and Policies- Part 6: "Interoperability Profiles". • Degree to which scope is met considering starting points: o Input exists, that covers test suites for interoperability. Not material for testing conformance. It will be reviewed and updated
		WORK PLAN **Task to be carried out:** • Production of a new TS document based on a number of existing documents (including stakeholder consultation) **Timescale (planning):** • Start: T0 • Complete: T0+12+12

Annex A:
Pan-European solutions

A.1 Introduction

This annex presents some pan-European electronic registered delivery solutions. This is not exhaustive. An inventory of national electronic delivery solutions in Europe is provided in [i.32] and to some extent in [i.33].

A.2 SPOCS LSP

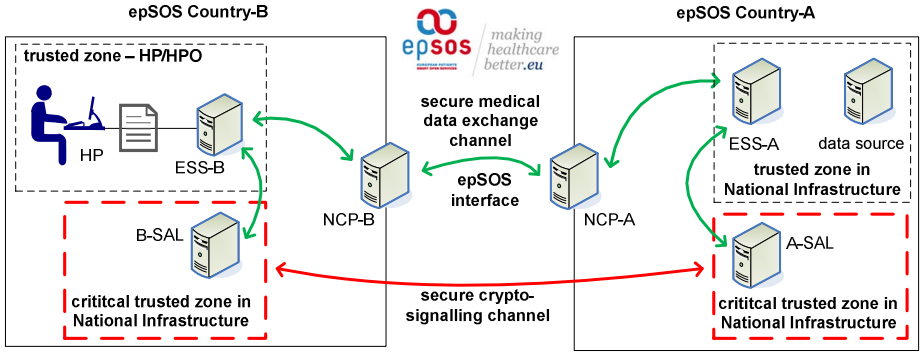
Description	The SPOCS European Large Scale Pilot (LSP) aimed at contributing to the next generation of online portals (Point of Single Contact) for enterprises, which every European country now has in place in abidance to Directive 2006/123/EC [i.1], through making cross-border electronic procedures available in these portals. One of its building blocks deals with interoperable, secure and trustworthy interconnection of the EUMS electronic delivery solutions established for trusted information exchange, most of them designated for general purpose in the area of e-government and not bound to dedicated application/business scenarios.
X2X communication scenarios	C2X B2X G2X
Architectural model	SPOCS eDelivery makes use of a "four-corner-model" based on (national) gateways in a trusted environment/network to connect national electronic delivery infrastructures.
Transport layer	Inside existing (national) domains according their established technology (profilings of SMTP/MIME, Web Services (WS-*) stack, or even proprietary). Between Gateways Web Services (WS-*) stack, in particular SOAP [i.28], WS-Addressing, WS-Security [i.21], WS-ReliableMessaging [i.27].
Mode of operation	Asynchronous - Store and Forward (S&F) only.
Endpoint discovery	Not covered, as foreign access to registries for most national solutions not possible, and re-registration in a central directory not feasible (both mostly restricted by national regulations, data protection considerations). Addressing logically based on domain-model (IETF RFC 5322 [i.26], Address Specification). Gateway address dispatches are targeted to being derived from addressee's domain, resolution of delivery endpoint left to domestic capabilities of target domain.
Addressing	Open for different models, a concrete communication partner identifier always is marked by its type. Actually, only IETF RFC 5322 [i.26] (electronic mail) type of logical addresses implemented.
End-to-end security	For E2E authentication a SAML token based on the STORK protocol foreseen. As SAML token not yet supported by all solutions interconnected and STORK not in place in all EUMS, SPOCS gateways issue SAML (sender vouches) token, based on information given by (proprietary) authentication token or mechanisms of national solutions. Integrity, authentication, confidentiality and non-repudiation services are guaranteed between the gateway-to-gateway communication and if applicable, i.e. depending on the national infrastructure, also between end users/services.
Message protocol	For the gateway-to-gateway route the ETSI REM-MD SOAP Binding Profile is used, providing an interoperability layer for the different message (packing) formats of national solutions. If not directly supported by domestic source/target solution, the gateway a solution is related to converts from/to domestic message formats (valid as well for evidence and authentication token).
Trust establishment	Trust Lists according ETSI TS 102 231 [i.40], covering all electronic delivery gateways in the network - gateways are seen as trust service instances. Mutual gateway authentication via X509 token used for TLS network level security as well for application level WS-Security message signature; X509 token verifiable in the TL as gateway digital identity. Trust establishment inside domains connected to the network left to domestic regulations and means. Solutions interconnected by gateways fulfil functionalities as defined by the ETSI TS 102 640 basic conformance profile.
Delivery traceability and provability	Gateway to gateway route: ETSI REM Evidences, according ETSI TS 102 640-2 [i.8]. If not directly supported by domestic source/target solution, to be converted from/to domestic format by the SPOCS Gateway a solution is connected to.

A.3 e-SENS LSP

NOTE: e-SENS has recently started, so the information given below is not yet consolidated and may be subject to change.

Description	e-SENS is a European Large Scale Pilot (LSP) with the aim of consolidating the results of the previous LSPs STORK, SPOCS, e-CODEX PEPPOL and epSOS. The e-SENS Work Package (WP) 6 Sub Group Competence Cluster 6.1 deals with the building block electronic delivery and will create a reusable set of generic tools (*Reference Implementation*) and specifications (*Common Framework for e-Delivery*) for a common e-SENS transport infrastructure covering the scenarios of all LSPs, i.e. the different domains of administration, e-Justice or e-Health.
X2X communication scenarios	C2X B2X G2X Besides asynchronous communications, e.g. H2H communication between natural persons as recipients, e-SENS also deals with synchronous M2M communications, which are e.g. used in e-Justice application scenarios between Web services.
Architectural model	Likewise all involved LSPs, e-SENS will make use of a "four-corner-model" based on (national) gateways in a trusted environment/network to connect national electronic delivery infrastructures.
Transport layer	Web Services (WS-*) stack, in particular the OASIS ebMS3 standard, which is a specific extension and profile of the WS-* stack.
Mode of operation	Asynchronous - Store and Forward (S&F) only Synchronous - direct communication between online services, e.g. Web Services
Service/Endpoint discovery	Open issue in e-SENS. Starting point (additional adoption of other concepts in discussion): Discovery of communication partners and service capabilities using the PEPPOL Service Metadata Locators (SML) and Service Metadata Publishers (SMP) technology.
Addressing	This is an open issue in e-SENS.
End-to-end security	For E2E authentication a SAML token based on the STORK protocol - as it is used in SPOCS - is planned. Integrity, authentication, confidentiality and non-repudiation services are guaranteed between the gateway-to-gateway communication and if applicable, i.e. depending on the national infrastructure, also between end users/services.
Message protocol	For the gateway-to-gateway communication the outcome of SPOCS, respectively the ETSI REM-MD SOAP Binding Profile is planned to be used.
Trust establishment	This is an open issue in e-SENS. Options on the table are ETSI Trust-service Status Lists (TSL), common PKI as used in PEPPOL or WS-Trust/WS-Federation.
Non-repudiation services (Evidences)	ETSI REM standard (a profile of selected evidence is not yet available)

A.4 ePSOS

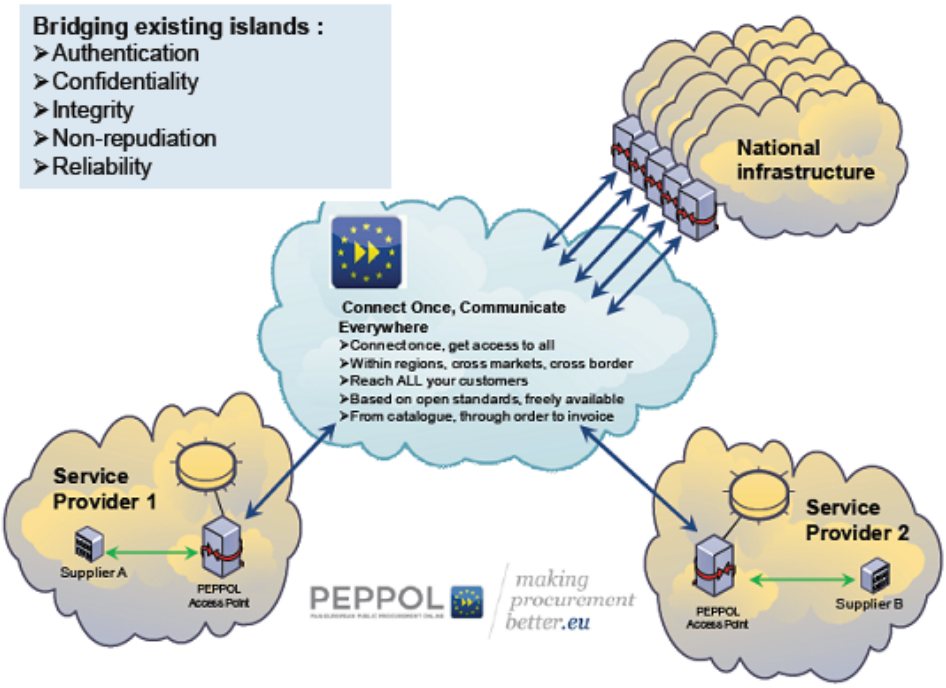
Description	The epSOS European Large Scale Pilot (LSP) "attempts to offer seamless healthcare to European citizens. Key goals are to improve the quality and safety of healthcare for citizens when travelling to another European country". Its transport infrastructure "concentrates on developing a practical eHealth framework that enables secure access to patient health information among different European healthcare systems".
X2X communication scenarios	Healthcare-to-Citizens
Architectural model	From an ICT architects viewpoint epSOS is a document sharing platform that provides means for sending and fetching medical data across borders. The epSOS architecture is based on a service-oriented paradigm. The epSOS services are passive and implemented as Web services whose interfaces are specified by the Web Service Description Language. Communication between service consumer and service provider is always initiated by the service consumer. Each participating nation provides these services through the National Contact Point (NCP) that acts as a service provider to other PN's and as a gateway for service consumers. The NCP is made up of a set of common components. The epSOS common components provide the following end-user services when connected to the national infrastructure of the patient's home country ("Country A"): • Identification Service • Patient Service • Order Service • eDispensation Service • Consent Service The NCP encompasses the following internal services for achieving semantic interoperability: • Taxonomy manager • Terminology Service Access Manager In addition, the NCP provides auditing and authentication services.
Transport layer	Inside existing national infrastructures, according to their established technology. The epSOS connector is responsible to produce epSOS-valid content from national infrastructures. Amongst the NCPs the transport is based on Web services. Inside the NCP, there exist also an IETF RFC 5424-based protocol (for audit trails) [i.42]
Mode of operation	Synchronous
Endpoint discovery	Endpoints do not change frequently. Given the fact that some countries are not allowed by their national law to publish such services, endpoints are listed in a TSL-based national service status list
Addressing	Based on patient identification, HL7v3 messages containing the remote country. This value is then used to retrieve the NCP's endpoints.
End-to-end security	Based on CMS-structured messages. Two main techniques have been adopted for granting end-to-end security: **Symmetrical Direct Encryption Mode:** the patient uses a portal in country A to manage the set of credentials, which are later on used in country B to access some protected epSOS document D_i., which has been encrypted on demand with a transaction specific key K_i. **PACE (Password Authenticated Connection Establishment)-based Key Exchange with Out-of-Band Signalling:** Adapting the PACE approach for epSOS is separating the encryption grade form the length of the secret the patient provides to the Health Practitioner. In contrast to Symmetrical Direct Encryption Mode, the secret is not used directly as the encryption key anymore but merely as foundation for deriving a longer and more secure encryption key.  **Figure 5: PACE-based Key Exchange with Out-of-Band Signalling in the epSOS context**

	Description of Use Cases There are different kinds of scenarios and Use Cases, which need to be distinguished in the following: • Creation and Provision of epSOS Documents • Management of Access Credentials • Accessing epSOS Documents
Message protocol	WS-based message exchange based on the following standards: • SOAP 1.2 • WS-Security 1.1 (SAML2.0 assertions) • IHE XCA/IHE Cross-Community Fetch profile(based on OASIS RegRep) • HL7v3 / IHE Cross-Community Patient Discovery (XCPD) • Syslog (rfc5424)
Trust establishment	Mutual gateway authentication via TLSv1
Delivery traceability and provability	Based on Audit Trail and Node Authentication (IHE ATNA)

A.5 PEPPOL

NOTE: This text is derived from the PEPPOL web site at http://www.peppol.eu/peppol-project

Description	Initiated in 2008, the Pan-European Public Procurement Online (PEPPOL) project has been developing and implementing the technology standards to align business processes for electronic procurement across all governments within Europe, aiming to expand market connectivity and interoperability between eProcurement communities. After completion of the PEPPOL project in 2012, OpenPEPPOL has taken over the continued maintenance and governance of the PEPPOL components. The PEPPOL electronic delivery infrastructure is based on a four corner model of interchange: trading partners (or service provider on their behalf) connected to PEPPOL using Access Points (AP). The infrastructure provides services for eProcurement with standardized electronic document formats [i.34]. See note.
X2X communication scenarios	G2B B2B
Architectural model	The PEPPOL infrastructure is based on a four corner model of interchange, trading partners or service provider on their behalf connected to PEPPOL using Access Points (AP) and is described in a set of documents known as Business Document Exchange Network (BUSDOX) that includes: • Common Definitions: containing the definitions and terms that are common between the Business Document Exchange Network (BUSDOX) service metadata and transport specifications. • Service Metadata Publishing: describing the Representational State Transfer interface for Service Metadata Publication within BUSDOX. • Service Metadata Locator Profile: defining the profiles for the discovery and management interfaces for the BUSDOX Service Metadata Locator service. • Profiles of secure messagetransfer protocols: – PEPPOL AS2 Service specification profiling the use of HTTP/AS2 and the PEPPOL PKI trust model for signing messages in the communication (mandatory). – Secure Trusted Asynchronous Reliable Transport: describing the SOAP-based profile that is used by BUSDOX Access Points to communicate and the SAML 2.0 assertions that are used in that communication (optional). • Lightweight Message Exchange Profile: providing a simple low-cost approach for Small and Medium Enterprises (SMEs) to access Business Document Exchange Network (BUSDOX) infrastructure (optional). • PEPPOL Identifier Schemes: defining a set of identifier schemes that will be used in the context of the PEPPOL infrastructure.

	
Transport layer	HTTP (AS2 mandatory) Web Services (WS-*) stack (optional)
Mode of operation	Synchronous (LIME provides a simplified asynchronous interface)
Endpoint discovery	Any trading partner/service provider registers its capabilities in the Service Metadata Publisher (SMP) that acts as the endpoint discovery service of PEPPOL. By registering capabilities in Service Metadata Publisher (SMP) any company within the network can send the registered party the corresponding document type without any further technical setup or agreements, thereby lowering the cost of entering into electronic trade with the party.
Addressing	Each endpoint has an address in the form of an URI. Each party is identified following the ISO 15459 [i.41] format scheme and the endpoint address is obtained using SMP/SML discovery service.
End-to-end security	Integrity, authentication and confidentiality services are guaranteed with mutual authentication of the nodes via SSL/TLS and, if applicable also between end users/services.
Message protocol	START and LIME (a simplified protocol for SMEs, see the Architectural model section in this table)
Trust establishment	Trust is established with a common certification authority that supports mutual authentication of the nodes via signed data, message transfer base on TLS/SSL and issuance of signed SAML assertions to support the required authorizations.
Delivery traceability and provability	Based on Audit Trail and Node Authentication
NOTE: PEPPOL promoted a standardization initiative in cooperation with OASIS BDXR TC (https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=bdxr). At the time of writing of the present document, some documents are under public review.	

A.6 eCODEX

Description	The e-CODEX European Large Scale Pilot (LSP) "aims to provide to citizens, enterprises and legal professionals an easier access to justice in cross border procedures and to make cross border collaboration of courts and authorities easier and more efficient by creating interoperability of the existing national ICT solutions" (see note 1). The e-CODEX transport infrastructure focuses on "the capability to bind together documents and data that need to be routed or exchanged to enable European cross-border processes in e-Justice" (ibid). Similar to e.g. SPOCS eDelivery, existing national infrastructure are used by all actors, connected by an interoperable, trustworthy and secure electronic delivery network for cross-border data exchange. In addition, the European e-Justice portal is connected, which provides functionality for editing and submitting e-proceeding forms.
X2X communication scenarios	C2X (Citizen-to Court) B2X (Business interact with Justice in e-Codex very much like citizens) G2X (Court-to-Citizen, Court-to-Court)
Architectural model	e-CODEX eDelivery makes use of a "four-corner-model" based on (national) gateways in a trusted environment/network to connect to the European e-Justice portal and national electronic delivery infrastructures used for e-Justice communication.
Transport layer	Inside existing (national) domains according to their established technology (profilings of SMTP/MIME, Web Services (WS-*) stack, or even proprietary). Between gateways a profiling of OASIS ebMS V3.0, itself an extension of the Web Services (WS-*) stack.
Mode of operation	Asynchronous - Store and Forward (S&F) only. Gateways are based on a kind of message relay, the ebMS Message Handler, which provides a message pull-mechanism, too. (The actual WS-calls between gateways are synchronous.)
Endpoint discovery	Intended to adopt the SML/SMP approach of PEPPOL's BusDox. Under evaluation, how dynamic discovery via SML/SMP can be made to work together with ebMS CPP/CPA mechanisms and Processing-Modes ("P-Mode") (see note 2). For the piloting phase, all configuration information for gateways is maintained and held in local configuration files. End entity addresses of courts are held in static lists in applications, and since there is only one gateway per country it is usually clear which gateways to use for a given end entity. End entity addresses of citizens are provided to courts as return addresses when citizens initiate a communication process.
Addressing	At receiving gateway / national adapter side: In order to enable routing of documents received from the sender to the correct recipient the messages are routed using the already existing electronic delivery solutions of the Member States End entity addresses are carried inside special properties in the ebMS transport header, and additionally at payload level in headers (which go end-to-end). For party identifiers the national (proprietary) format is used unaltered.
End-to-end security	As the ebMS communication is between gateways only, a complete end-to-end encryption is not foreseen and will not be provided by e-CODEX. Can be done on document (message item) level by end entities - out of scope of e-CODEX. For E2E authentication a SAML token based on the STORK profiling is foreseen. Communication partners can agree on a dedicated ebMS P-Mode, outlining whether they require delivery of SAML token or not. The Token can be provided as distinct payload. As SAML tokens are not yet supported by all solutions interconnected and STORK is not in place in all EUMS, currently SAML tokens are not yet used.
Message protocol	For the gateway-to-gateway route a profiling of ebMS concerning message meta data is used. The message payload is transported unchanged to the target gateway, as provided by source national gateway adapter.
Trust establishment	Mutual gateway authentication via SSL/TLS.
Delivery traceability and provability	Gateway to gateway route: ETSI REM Evidences, according ETSI TS 102 640-2 [i.8]. Evidences seen as related to "Business Level", thus allocated to the message payload. Left to adapters to national solutions, how to deal with Evidences.
NOTE 1: e-CODEX Deliverable 5.1 Requirements. NOTE 2: A proof of concept has been created, to be published.	

A.7 e-Trustex

The text below comes from the Open e-TrustEx platform hosted on the EC Joinup platform (https://joinup.ec.europa.eu/software/openetrustex/description).

Description	e-TrustEx is a platform offered (by the EC) to public administrations at European, national or local level to securely exchange documents. This is achieved by using standardized interfaces for machine-to-machine communication (e.g. backend services of public administrations) or a Web platform for access by citizens and businesses. Through dedicated CIPA (Common Infrastructure for Public Administrations) gateways, e-TrustEx can virtually be coupled with other electronic delivery architectural models like the ones from the EU LSPs STORK, SPOCS, epSOS, PEPPOL and e-CODEX.
X2X communication scenarios	G2X Besides asynchronous communications, e.g. H2H communication between natural persons as recipients, e-TrustEx also deals with synchronous M2M communications, which are e.g. used by backend applications of public administrations.
Architectural model	e-TrustEx uses a Service Oriented Architecture (SOA) with a central data exchange platform. The platform for cross-sector services supports the submission, retrieval and viewing of documents and its status. Due to its modular architecture, e-TrustEx can serve different use cases. As sector specific services are currently defined: Procurement, Legislative support, Competition cases and Support to cohesion policy. With so-called CIPA gateways, which serve as access points to other electronic delivery networks, architectures of LSPs like PEPPOL etc. can easily be connected to the e-TrustEx platform.
Transport layer	e-TrustEx uses the Simple Object Access Protocol (SOAP) for the connection of back-end services of public administrations. Furthermore, WS-ReliableMessaging is used for better reliability.
Mode of operation	Asynchronous - Store and Forward (S&F) in case of a CIPA gateway connection, otherwise documents are stored on the e-TrustEx platform.
Service/Endpoint discovery	e-TrustEx has address directories for routing messages. These directories contain the addresses of potential recipients. In the CIPA case document routing is realized with SML/SMP components by using as address the Identifier of the party and the specific type of business document (as it is realized in PEPPOL).
Addressing	See point service/endpoint discovery.
End-to-end security	E2E encrypted between sender and recipient is supported.
Message protocol	e-TrustEx uses XML messages based on SOAP.
Trust establishment	Users authenticate to the e-TrustEx platform with their credentials (UID/PWD).
Non-repudiation services (Evidences)	The following non-repudiation services are supported: • non-repudiation of origin • non-repudiation of submission • non-repudiation of delivery • non-repudiation of receipt

Annex B: Inventory

Annex B is contained in archive sr_019050v010101p0.zip which accompanies the present document.

Annex C: Bibliography

- "ISA multimedia assets library". 2011.
- "ISA Strategy - Commission's Communication on Interoperability". 2010.
- Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.
- Commission Decision 2003/511/EC of 14.7.2003 on the publication of reference numbers of generally recognised standards for electronic signature products in accordance with Directive 1999/93/EC of the European Parliament and of the Council.
- Directive 1998/34/EC of the European Parliament and the Council of 22.6.1998 laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on Information Society services.
- "Study on the standardisation aspects of e-signatures", SEALED, DLA Piper et al, 2007.
- "CROBIES: Study on Cross-Border Interoperability of eSignatures", Siemens, SEALED and TimeLex, 2010.
- ISO/IEC 27000: "Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary".
- IETF RFC 3647: "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework".
- W3C Recommendation: "XML Signature Syntax and Processing (Second Edition)", 10 June 2008.
- Commission Decision 2011/130/EU of 25 February 2011 establishing minimum requirements for the cross-border processing of documents signed electronically by competent authorities under Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market.
- IETF RFC 3161 (August 2001): "Internet X.509 Public Key Infrastructure Time-Stamp Protocol".
- CCMB-2006-09-001: "Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 3.1, Revision 3", July 2009
- Recommendation ITU-T X.509/ISO/IEC 9594-8: "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks".
- Apitzsch J.: "Mechanismen zur Nachweisbarkeit der Kommunikation bei OSCI Transport". Datenschutz und Datensicherheit - DuD 2007;31(10):744-46
- Apitzsch J., Liehmann M., Martin B., Rieger S. and Seeger M.: "Assessment of existing eDelivery systems and specifications required for interoperability, 2010.
- Capgemini: "Architecture for delivering pan-European e-Government services (PEGS Infrastructure)" version 1.0, 2004.
- Council of Europe: "European convention on the service abroad of documents relating to administrative matters". European Treaty Series - No. 94. 1977.
- Dietrich J, Keller-Herder J.: "De-Mail-verschlüsselt, authentisch, nachweisbar". Datenschutz und Datensicherheit - DuD 2010;34(5):299-301
- European Commission, Architecture Guidelines For Trans-European Telematics Networks for Administrations version 7.1, 2004.
- European Commission, Study on electronic documents and electronic delivery for the purpose of the implementation of Art. 8 of the Services Directive, 2009.

- European Commission, European Interoperable Infrastructure Services - Study on potential reuse of system component version 1.1, 2010.
- Directive 2008/6/EC of the European Parliament and of the Council of February 2008 amending Directive 97/67/EC with regard to the full accomplishment of the internal market of Community postal services. 2008.
- Ferrer-Gomilla F., Onieva J., Payeras M. and Lopez J.: "Certified electronic mail: Properties revisited". Computers & Security 2010;29(2):167-79
- Freemantle M.: "Lightweight Message Exchange Profile (LIME)", Version 1.0.0, December 2009.
- Freemantle M.: "Secure Trusted Asynchronous Reliable Transport (START)", Version 1.0.0, December 2009.
- Gennai F., Martusciello L. and Buzzi M.: "A certified email system for the public administration in Italy". IADIS International Conference WWW/Internet, 2005, vol. 2, pp. 143-147
- IETF RFC 2634, Hoffman P.: "Enhanced Security Services for S/MIME" June 1999.
- Hulsebosch B., Lenzini G. and Eertink H.: "STORK D3.2 - Quality authenticator scheme, 2009".
- Recommendation ITU-T X.402: "Data Communication Networks - Message Handling Systems - Overall Architecture". 1992.
- Recommendation ITU-T F.400/X.400 - Series X: "Data Networks and Open System Communications. Message handling system and service overview". 1999.
- Kremer S., Markowitch O. and Zhou J.: "An intensive survey of fair non-repudiation protocols". Computer Communications 2000;25:1606-21
- Leitold H. and Zwattendorfer B.: "STORK: Architecture, Implementation and Pilots", ISSE 2010 Securing Electronic Business Processes, 2010, pp. 131-142
- Miranda J.P. and Melo J.: "EPM: Tech, Biz and Postal Services Meeting Point", ISSE 2004 - Securing Electronic Business Processes; 259-267. 2004
- Olnes J., Buene L., Andresen A., Grindheim H., Apitzsch J. and Rossi A.: "A General Quality Classification System for eIDs and e-Signatures". Highlights of the Information Security Solutions Europe (ISSE) Conference, 2009, pp. 72-86
- Onieva J., Zhou J. and Lopez J.: "Multiparty Nonrepudiation: A survey". ACM Computing Surveys 2008;41(1)
- Oppliger R.: "Providing certified mail services on the internet". IEEE Security and Privacy 2007;5(1)
- Ornetsmüller G.: "webERV - ERVServices - Beschreibung der Webservice-Schnittstelle Teilnehmer <-> Übermittlungsstelle". 2007.
- Planitzer F. and Weisweber W.: "Virtual Post Office in Practice. ISSE/SECURE 2007 Securing Electronic Business Processes". 2007. p. 427-37
- Rössler T. and Tauber A.: "The SPOCS interoperability framework: interoperability of eDocuments and eDelivery systems taken as example". ISSE 2010 Securing Electronic Business Processes, 2010, pp. 122-130
- Tauber A.: "Requirements for Electronic Delivery Systems in eGovernment - An Austrian Experience. Software Services for e-Business and e-Society" - IFIP Advances in Information and Communication Technology 2009; 305; 123-33.
- Tauber A.: "Requirements and Properties of Qualified Electronic Delivery Systems in eGovernment - an Austrian Experience. International Journal of E-Adoption, vol 2., no. 1, 2010, pp. 45-58.
- Tauber A.: "A survey of certified mail systems provided on the Internet". Computers & Security 2011 (in press).
- UPU (Universal Postal Union): "S43: Secured electronic postal services (SePS) interface specification - Part B: EPCM Service". 2003.

- W3C: "SOAP Message Transmission Optimization Mechanism", 2005.
- Apitzch J., Boldrin L., Caccia A., Foti S., Cruellas J. C., Llaneza P. and Sun G. (2011): "ETSI STF 402 - Standardizing the pan-European infrastructure for Registered Electronic Mail and e-Delivery". In ISSE 2011 Securing Electronic Business Processes Highlights of the Information Security Solutions Europe Conference 2011.
- Tauber A., Apitzsch J. and Boldrin L. (2012): "An interoperability standard for certified mail systems", Computer Standards & Interfaces, http://dx.doi.org/10.1016/j.csi.2012.03.002.
- IETF RFC 6109: "La Posta Elettronica Certificata - Italian Certified Electronic Mail".
- Mandate M460: "Standardisation Mandate to the European Standardisation Organisations CEN, CENELEC and ETSI in the Field of Information and Communication Technologies Applied to Electronic Signatures".

NOTE: Available from: www.etsi.org/images/files/ECMandates/m460.pdf

- COM(2013) 329: "Proposal for a Regulation of the European Parliament and of the Council on guidelines for trans-European telecommunications networks and repealing Decision No. 1336/97/EC".

NOTE: Available from: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2013:0329:FIN:EN:PDF

History

Document history		
V1.1.1	June 2015	Publication