SR 019 530 V 0.0.2 (2013-09)

SPECIAL REPORT

Rationalised framework of Standards for Electronic Delivery Applying Electronic Signatures

STABLE DRAFT FOR PUBLIC REVIEW UNTIL 15 NOVEMBER 2013

Download the template for comments:

http://docbox.etsi.org/ESI/Open/Latest Drafts/Template-for-comments.doc

Send comments to E-SIGNATURES COMMENTS@LIST.ETSI.ORG

CAUTION: This DRAFT document is provided for information and is for future development work within the ETSI Technical Committee ESI only. ETSI and its Members accept no liability for any further use/implementation of this Specification.

Approved and published specifications and reports shall be obtained exclusively via the ETSI Documentation Service at

http://pda.etsi.org/pda/queryform.asp

Reference
<Workitem>

Keywords
<keywords>

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

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

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 ESI.

Introduction

Electronic delivery in the broad sense, i.e the transmission of data by electronic means, is ubiquitous in most human activities. This is potentially true also when restricting to e-Delivery in the stricter sense provided by the definition in clause 3, since the requirements of integrity, confidentiality, non-repudiation, provability of a message easily apply to a wide range of contexts: when comparing e-Delivery with “registered paper mail”, it appears that it can be considered as a general purpose commodity.

The necessity of a governance on this field has been clearly recognized by the proposed EC regulation on guidelines for trans-European telecommunications networks [i.32] and by the proposed EC regulation on electronic identification and trust services for electronic transactions in the internal market (eIDAS) [i.5]. 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 explicitely identifies electronic delivery amont the “building blocks” for the digital service infrastructure. Reference to European Interoperability Framework (EIF) [i.31] suggests that a layered approach to interoperability has to be adopted, distinguishing legal, organizational, semantic and technical (syntax, transmission) aspects. It may be reasonable to assume that eIDAS proposed Regulation [i.5] aims at covering the “legal” layer, while the other layers have to be covered by specific standards.

The impact assessment accompaining [i.32] recognizes that:

> *“large number of cross-border digital services, implementing exchanges between European public administrations in support of EU 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, such as for instance the ISA programme, the Fiscalis programme and Horizon 2020.”*

As a matter of fact, we are presently witnessing the emergence of several e-Delivery services, most of them restricted either to a member state or to a community, a business, etc. These services are normally not homogeneous and not interoperable, mainly because of the lack of a normative and standardization base, hence hindering the emergence of e-Delivery as a global (or, at least, pan-european) commodity service.

A first attempt was already provided by Registered E-Mail (REM) specifications ([i.8], [i.9], [i.10], [i.11], [i.12], [i.13], [i.14], [i.15], [i.16]) and the related UPU specifications ([i.6]) which, however, were focussed on a subset of features and technologies.

This document aims at identifying a framework of standards for e-Delivery services in order to fill the standardization gap, fully in line with the Rationalised Framework of Standards for Electronic Signatures, in the context of [i.1].

1 Scope

The present document provides a proposal for a rationalised framework of standards for Electronic Delivery Services, fully aligned with the principles, criteria and structure of the European Rationalised Framework of Electronic Signatures. The framework of standards proposed provides full technical support to the requirements established in the COM(2012) 238/2 Regulation [i.5] “on electronic identification and trust services for electronic transactions in the internal market”.

The present document also includes a set of recommendations for future standardization activities that target at implementing the framework of standards for e-Delivery.

Clause 4 provides details on the methodology followed for producing the framework of standards for e-Delivery.

Clause 5 lists a number of relevant features identified among a number of real e-Delivery solutions.

Clause 6 presents a reference model for Electronic Delivery Services. This model identifies participating entities, exchanges among them, relevant roles, etc., and drives to the identification of the set of required standards

Clause 7 explores currently existing related standards and specifications, in order to identify the gaps.

Clause 8 includes the proposed rationalized framework of standards for Electronic Delivery Services.

Clause 9 contains a set of recommendations for standardization activities targeting at implementing the aforementioned framework.

Annex A provides details of a set of pan-european solutions analized, which have been of great importance for identifying the features listed in clause 5, as well as to define the reference model for e-Delivery in clause 6.

Annex B comes as a separate excel sheet which includes the list of standards and specifications related to e-Delivery.

Annex C provides a larger bibliography on electronic delivery.

2 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.

2.1 Normative references

Not applicable.

2.2 Informative references

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] 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".

[i.2] Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market.

[i.3] 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.

[i.4] 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.

[i.5] COM(2012) 238/2: Proposal for a Regulation of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market –

Note: Available from: http://extranet.cor.europa.eu/subsidiarity/Lists/SmnItemsList/Attachments/3056/com_2012_2038_en.pdf

[i.6] CEN/TS 16326:2013: “Postal Services - Hybrid Mail - Functional Specification for postal registered electronic mail”

[i.7] ETSI TS 102 231 V3.1.2 (2009-12) “Electronic Signatures and Infrastructures (ESI);Provision of harmonized Trust-service status information”

[i.8] ETSI TS 102 640-1: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 1: Architecture”.

[i.9] ETSI TS 102 640-2: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 2: Data requirements, Formats and Signatures for REM”.

[i.10] 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.11] ETSI TS 102 640-4: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 4: REM-MD Conformance Profiles".

[i.12] ETSI TS 102 640-5: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 5: REM-MD Interoperability Profiles".

[i.13] ETSI TS 102 640-6.1: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 6.1: REM-MD UPU PReM nteroperability Profile ".

[i.14] ETSI TS 102 640-6.2.: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 6.2: REM-MD BUSDOX Interoperability Profile ".

[i.15] ETSI TS 102 640-6.3: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 6.3: REM-MD SOAP Binding Profile ".

[i.16] ETSI SR 001 604 V1.1.1 (2012-07): “Rationalised Framework for Electronic Signature Standardisation”

[i.17] IETF RFC 5751, January 2010, Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification

[1.18] IETF RFC 2459, January 1999, Internet X.509 Public Key Infrastructure Certificate and CRL Profile

[i.19] ISO 32000-1: "Document management -- Portable document format -- Part 1: PDF 1.7".

[i.20] ITU-T Recommendation X.1254/ISO/IEC DIS 29115: "Information technology – Security techniques - Entity authentication assurance framework".

[i.21] OASIS WS-Trust 1.4

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

[i.22] OASIS Web Services Security: SOAP Message Security 1.1 (WS-Security 2004) OASIS Standard Specification, 1 February 2006

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

[i.23] OASIS Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0, OASIS Standard, 15 March 2005

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

[i.24] W3C Recommendation: "XML Signature Syntax and Processing (Second Edition)", 10 June 2008.

[i.25] OASIS ebXML Messaging Services Version 3.0: Part 1, Core Features (1 October 2007)

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

[i.26] IETF RFC 5321 Simple Mail Transfer Protocols

[i.27] IETF RFC 5322 Internet Message Format

[i.28] OASIS, Web Services Reliable Messaging 1.2, OASIS Standard, 2009.

[i.29] W3C, SOAP Version 1.2 Part 1: Messaging Framework (Second Edition), 2007.

[i.30] OASIS, Web Service Federation Language, 1.2, 2009.

[i.31] European Commission, European Interoperability Framework for European Public Services (EIF) version 2.0, 2010.

[i.32] 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

[i.33] 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.34] ETSI TR 102 605: Electronic Signatures and Infrastructures (ESI); Registered E-Mail

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

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in [i.5], [i.8], [i.9], [i.10], [i.16] 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 elsewere in the mentioned sources
- they are present elsewere 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

trust service means any electronic service consisting in the creation, verification, validation, handling and preservation of electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic delivery services, website authentication, and electronic certificates, including certificates for electronic signature and for electronic seals;

qualified trust service means a trust service that meets the applicable requirements provided for in [i.5];

trust service provider means a natural or a legal person who provides one or more trust services;

qualified trust service provider means a trust service provider who meets the requirements laid down in [i.5]

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 e-delivery services, as well as long term storage services related to signed data and Electronic Signatures.

electronic delivery (e-Delivery): the 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 delivery service (eDS): a service that makes it possible to transmit data by electronic means and 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;

qualified electronic delivery service (QeDS): an electronic delivery service which meets the requirements laid down in Article 36 of [i.5]

(qualified) electronic delivery management domain ((Q)eDMD): set of technical and physical components, personnel, policies and processes that provide (qualified) electronic delivery serviceswithin a network (see electronic delivery network)

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

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

(qualified) electronic delivery service provider –((Q)eDSP): trust application service provider which provides (qualified) electronic delivery services

end entity: message senders and recipients; users (using user agents) or systems using e-Delivery services for data exchange

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

registered e-mail service provider: trust application service provider which provides registered e-mail services.

3.2 Abbreviations

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

AdES	Advanced Electronic Signature
AdES$_{QC}$	Advanced Electronic Signature supported by a Qualified Certificate
AP	Access Point
AS	Attribute Service
ASiC	Associated Signature Container
BES	Basic Electronic Signature
BusDox	Business Document Exchange Network
CA	Certification Authority
CAdES	CMS Advanced Electronic Signature
CEC-PAC	Comunicazione Elettronica Certificata tra Pubblica Amministrazione e Cittadino
CEN	Comité Européen de Normalisation
CMS	Cryptographic Message Syntax
CP	Certificate Policy
CPS	Certificate Practices Statement
CRL	Certificate Revocation List
CSP	Certification Service Provider
CWA	CEN Workshop Agreement
DN	Distinguished Name

DSS	Digital Signature Standard (as published by OASIS)
E-CODEX	e-Justice Communication via Online Data Exchange
(Q)eDMD	(Qualified) Electronic Delivery Management Domain
(Q)eDS	(Q)ualified Electronic Delivery Service
(Q)eDSP	(Qualified) Electronic Delivery Service Provider
EEA	European Economic Area
EESSI	European Electronic Signature Standardization Initiative
EN	European Norm
EGVP	Elektronischen Gerichts- und Verwaltungspostfach
EPES	Explicit Policy-based Electronic Signature
ETSI	European Telecommunications Standards Institute
EU	European Union
EUMS	European Member States
FTP	File Transfer Protocol
GW	Gateway
HTTP	Hypertext Transfer Protocol
IAS	Identification, Authentication and Digital Signature
IGPEC	Indice Gestori Posta Elettronica Certificata
ISO	International Organization for Standardization
LDAP	Lightweight Directory Access Protocol
LoA	Level of Assurance
LTV	Long term Validation (used with PAdES)
MS	Member State
OASIS	Organization for the Advancement of Structured Information Standards
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OSCI	Online Service Computer Interface
PAdES	PDF Advanced Electronic Signature
PEC	Posta Elettronica Certificata
PEC-ID	Posta Elettronica Certificata con Identificazione
PEPPOL	Pan-European Public eProcurement On-Line
PKC	Public Key Certificate
PKI	Public Key Infrastructure
QC	Qualified Certificate
QES	Qualified Electronic Signature
RA	Registration Authority
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
SOAP	Simple Object Access Protocol
SP	Signature Policy
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
SVA	Signature Validation Application
SVSP	Signature Validation Service Provider
S&N	Store And Notify
TASP	Trust Application Service Provider
TC	Technical Committee
TL	Trusted List
TLS	Transport Layer Security
TR	Technical Report
TrST	Trust Service Token
TS	Technical Specification
TSL	Trust-service Status List
TSP	Trust Service Provider

TSSLP	Trust Service Status List Provider
TSSP	Time-Stamping Service Provider
TST	Time Stamp Token
UPU	Universal Postal Union
URI	Uniform Resource Identifier
URN	Uniform Resource Name
UTC	Coordinated Universal Time
WS	Web Service
WWW	World Wide Web
XAdES	XML Advanced Electronic Signature
XML	eXtensible Markup Language
XMLDSig	XML Digital Signature

4 Methodology

In order to identify a framework of standards for e-Delivery services, which fills the current standardization gap and is fully in line with the Rationalised Framework of Standards for Electronic Signatures, a well-conceived methodology has been applied, which is also reflected in the structure of this document as follows.

Clause 5 identifies the main e-Delivery features to provide a basic understanding of requirements for creating the different e-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 e-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, organisational and trust ones.

Based on the identified features, clause 6 sketches the different e-Delivery service models and thereof tries to identify the implications on standardization activities. The service model description uses a top-down approach by starting with a simple and basic model (e-Delivery as a black-box), continuing with the distributed model (different e-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 e-Delivery features, main roles and functionalities of an e-Delivery management domain are categorized into core, optional and ancilliary ones. Based on the features, service models and role definitions, the implications to standardization activities have been identified. To be in line with the EU proposed regulation COM(2012) 238/2 [i.5], implications cover both the conformance with requirements for qualified and non-qualified 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) e-Delivery service providers with respect to service discovery, message delivery and registered delivery.

Clause 7 provides input to the rationalised 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 rationalised framework can fill these gaps. Due to their diversity, the inventory does not include national (or private business) e-Delivery solutions. It rather focusses on existing national and international standards in the field of e-Delivery and also covers European efforts in the area of cross-border e-Delivery, which pave(d) the technical way towards the new EU regulation.

Clause 8 introduces the rationalised structure for Electronic Delivery Standards, which is based on the e-Delivery service model and provides standards to fill the identified gaps. The rational structure of the framework follows a classification scheme based on the document types identified within the European Rationalized Framework of Standards for Electronic Signatures (guidance, technical, conformance, etc.).

Finally, clause 9 completes the rationalised 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.

5 Features

The table below 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 e-Delivery services, are affected or may benefit from the feature. For the purpose of this table, the following entities have been identified:

- user: human or application using the e-Delivery service
- service access point: point of entrance to the service
- service node: any intermediate note involved in the service
- external provider of ancillary services

Column “Scope” identifies the specific point-to-point exchanges within the e-Delivery transaction which are affected or may benefit from the feature (that is why, for instance, authentication scope may be user-to-service access point, service node-to-service node, and service access point-to-user). Finally, the last column may contain 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.

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 e-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 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 a end-to-end basis.
Integrity	Signature	- user - service AP - service node	1. User-to--User 3. S.node-to-S.node	Feature that can be used on a 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 a 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 hat 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 allow to synchronize the clocks of all the server nodes to a trusted reference. This Is relevant for the creation of coherent log. Also the client may 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 electonic 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 releated to how trust is built between different Service provider. It may be implemented by a trusted list [i.5] (as recommended in REM [i.9]), via a shared directory (as in Italian PEC), via Security token Service as defined by WS Trust [i.21]/ WS Federation [i.30], etc.
Service Discovery	Provider index, Directory	- Service node	1. S.node-to-S.node	This feature is related to how the details of an e-Delivery Service Provider may be discovered and retrieved. It May be implemented by a specific protocol (like DNS-based SML-SMP in PEPPOL), via a shared directory (as in 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 a end user (or participant) may be discovered/retrieved and used to send some message. It may 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. EGVP), etc.
Address manage-ment		- user - service AP - service node	1. User-to-ServiceAP 2. ServiceAP-to-User 3. S.node-to-S.node	Each e-Delivery Service manages addresses of its subscribers. For example some of these often use the standard "rfc 5321" to implement this feature but also other means/schemes are used.
Translation		- service node	1. S.node-to-S.node	Some e-Delivery solutions implement a feature for the normalization of content.
Semantic check		- service node	1. S.node-to-S.node	Some e-Delivery solutions implement a feature for the semantic check of content.

Structured/ non-structured contents		- service node	1. S.node-to-S.node	Some e-Delivery solutions (but not all) manage structured contents.
Service Level/ Provision Negotiation		- user - service AP - service node	1. User-to-ServiceAP 2. ServiceAP-to-User 3. S.node-to-S.node	Some e-Delivery solutions may offer different delivery options, e.g: • Generation ofsome 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	Regulates the functionality and behavior of all other features. May be defined by (national/European/international) law or rules.

Table 1: e-Delivery features

6 e-Delivery service model

Starting from the feature analysis if clause 5, this clause presents a high level model of an electronic delivery service as a basis for further elaboration, not intended to impose specific requirement for the successive standardization activity.

The model aims at describing the entities and the events which constitute the essence of an “e-Delivery act” in most known systems.

6.1 Basic service model

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

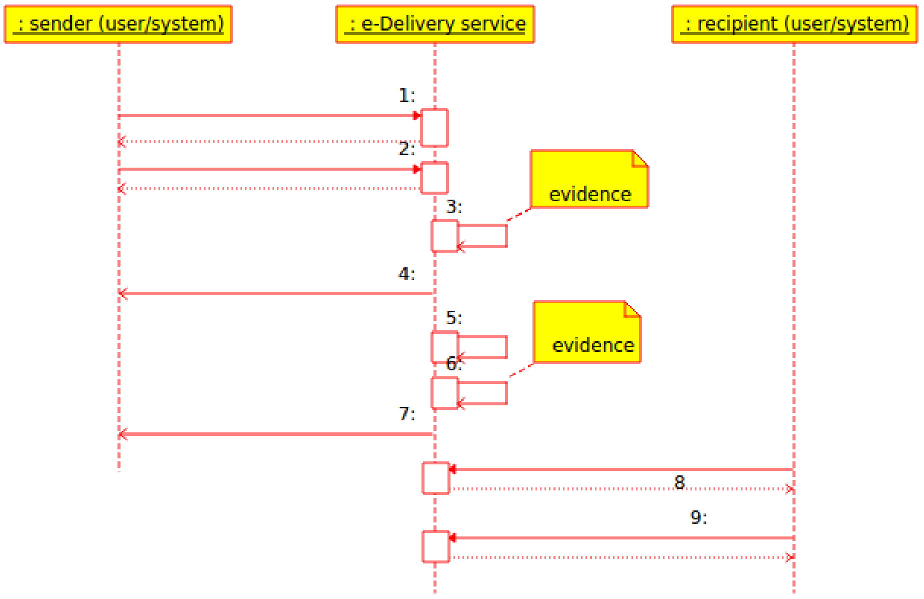


Figure 1: basic e-Delivery service model

1. the sender (either a user or a system) authenticates to the e-Delivery service
2. the sender (either a user or a system) prepares a message, specifies one or more addressees, indicates some options on the delivery service required (e.g., “confidential”, “mark it as Urgent”, etc.), and sumbits it to the e-Delivery service
3. at this point the e-Delivery service tracks the event that the message has been submitted (some systems may 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 e-Delivery service acts as a trusted third party.
4. Sometimes the evidence is sent back to the sender. This behaviour may be fixed for the system, or may depend on a delivery option indicated by the sender. Independently from sending to the sender, the attestation is always stored for a certain amount of time by the system.
5. The “delivery” to the recipient(s) happens, meaning that the data submitted by the sender is made available to the recipient(s), in a way that depend on the specific service implementation.
6. the e-Delivery service tracks the event that the message has been made available to the recipient. Again, this is often done producing an “attestation of delivery” (delivery evidence), i.e. a (signed) file containing the basic information of the event. In case of multiple delivery, one or more attestations may be produced.

7. As in point 4, the evidence might be sent back to the sender. This behaviour may be fixed for the system, or may depend 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.

8. the recipient (either a user or a system) authenticates to the e-Delivery service

9. 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.). The flow does not deal also with different modes for consigning the message to the recipient (push/pull, etc.).

6.2 Distributed service model

While the user experience is that of an opaque black-box, the reality behind an e-Delivery service is often made of several interacting domains, operated by different providers. In this case the relevant sequence diagram appears as follows:

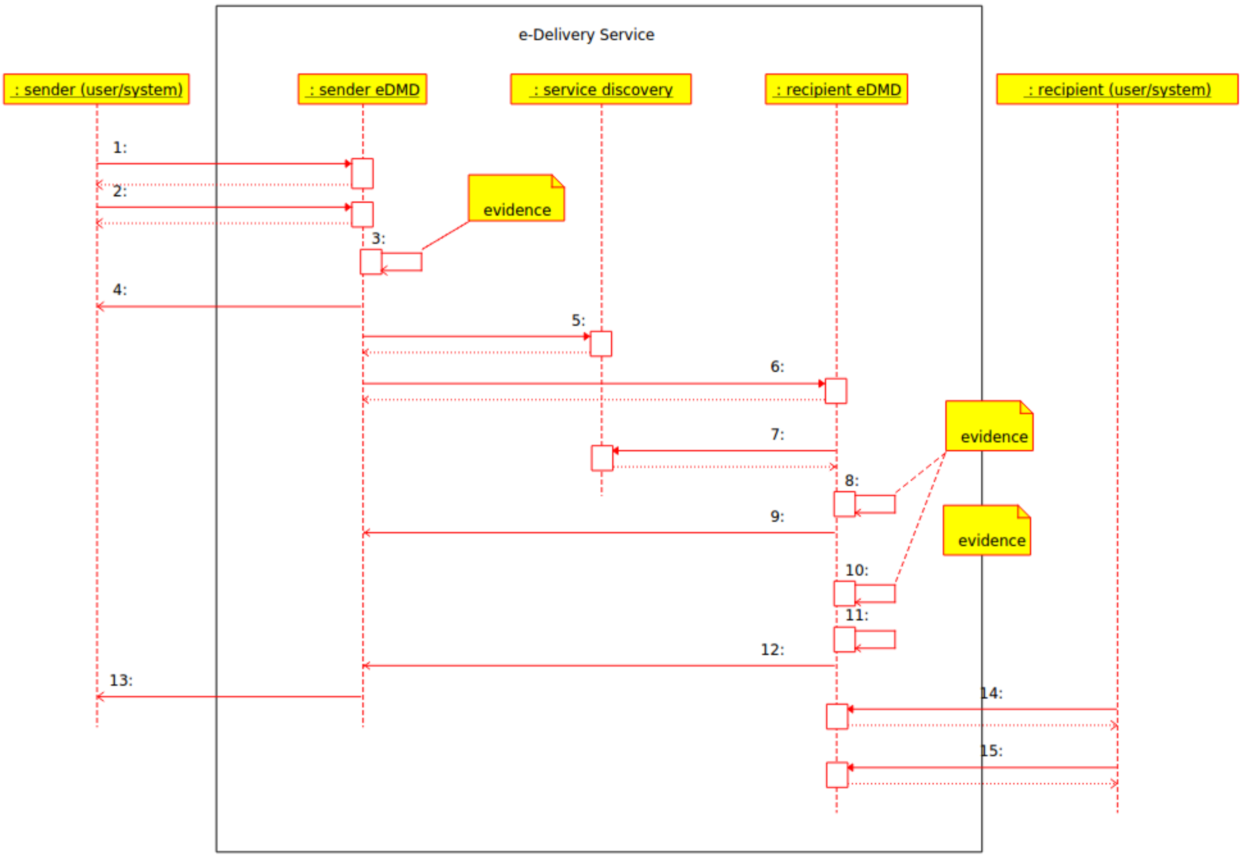


Figure 2: distributed e-Delivery service model

1. the sender (either a user or a system) authenticates to her eDMD.
2. the sender (either a user or a system) prepares a message, specifies one or more recipients, indicates some options on the delivery service required, and submits it to her eDMD.
3. at this point the eDMD tracks the event that the message has been submitted (submission evidence)
4. Sometimes the evidence is sent back to the sender.

5. The sender’s eDMD retrieves the necessary information on the recipient’s eDMD form 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 info: Depending on the underlying transport, this may be standard DNS lookup or lookup to a specific registry.

    - Retrieve remote eDMD capabilities info and conduct an handshake in order to negotiate on different aspects (security management, payload and related meta data, provision of evidences, strength of authentication of end entities, …)

    - Establish trust on remote eDMD, possibly checking against a trust info provider (in a restricted network, peer-to-peer agreements may be established with no central trust info provider). Since trust networks are normally slowly changing, the process is not necessarily synchronous.

6. The message is dispatched to the recipient’s eDMD (in case of more recipients, the message is dispatched to the respective eDMDs). The original payload is normally integrated with meta-informations, which is sometimes packaged with the payload 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.

7. The recipient’s eDMD may check, on its turn, that the sender’s eDMD is trustable.

8. The recipient’s eDMD tracks the fact that a message has been relayed o itself (relay evidence).

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

10. The message is delivered to the recipient.

11. the recipient’s eDMD tracks the event that the message has been made available to the recipient (delivery evidence).

12. The delivery evidence is normally sent back to the sender’s eDMD.

13. The sender’s eDMD might hand the evidence back to the sender (or might store the evidence for a later request).

14. the recipient (either a user or a system) authenticates to its eDMD.

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

6.3 Extended e-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, this document will only focus 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 e-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.

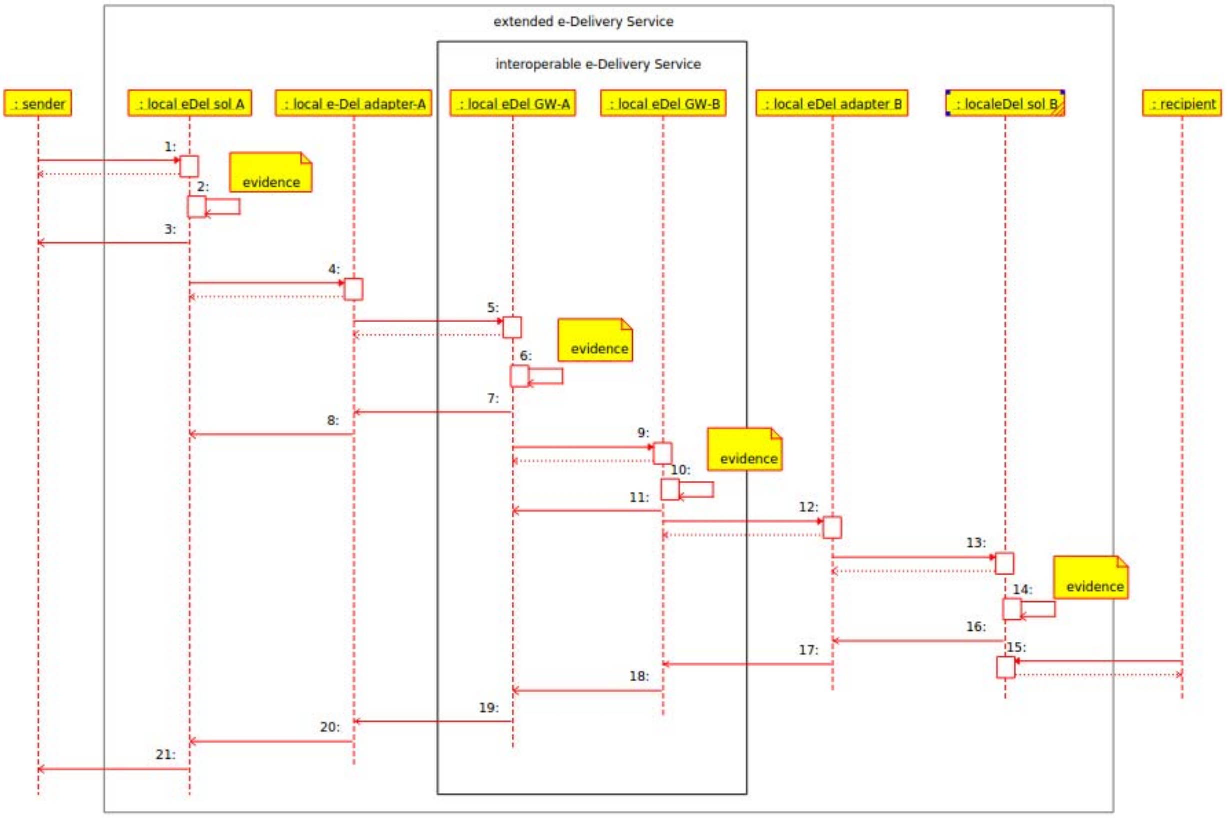


Figure 3: extended e-Delivery service model

It appears that, while the users still percieve the service as a black-box (the larger box, named “extended e-Delivery Service), several interactions take place in the between, which we may roughly classify as:

- sender side: includes the (non-interoperable) sender’s e-Delivery solution and a translation to/from the interoperable e-Delivery network (the network of gateways)
- interoperable e-Delivery network: the core network connecting local gateways which implements, at all effects, a distributed e-Delivery service (see clause 6.2), 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 e-Delivery solution and a translation from/to the interoperable e-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.

6.4 Roles in e-Delivery management domains

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

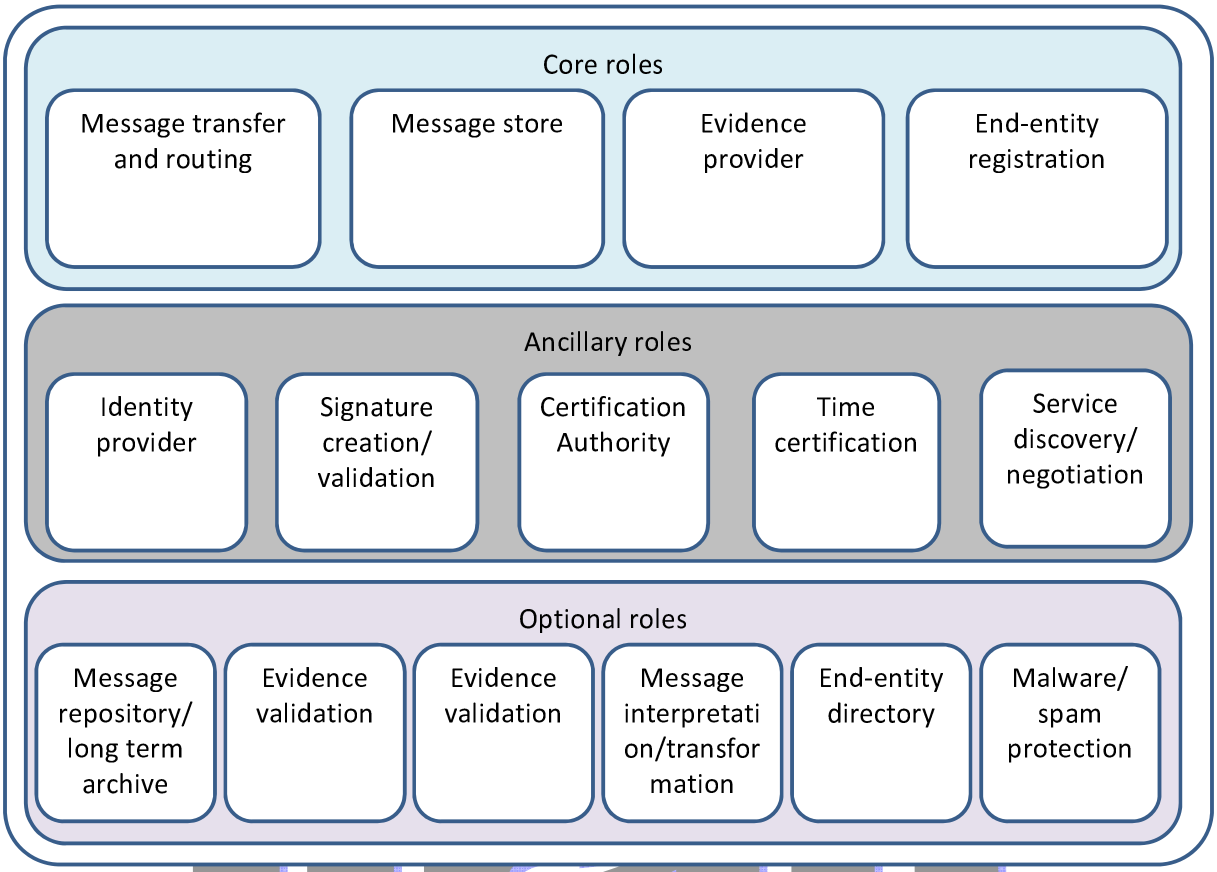


Figure 4: roles in e-Delivery management domain

As illustrated in Figure 4, an e-Delivery management domain necessarily includes the following core roles:

- **message transfer and routing**: this role is requested for the (secure and reliable) transfer of the message from the sender to the recipient;
- **message store**: this role is requested since asynchronous transmission is normally supported by e-Delivery services;
- **evidence provider**: this role plays a fundamental role in the production of evidences attesting the different events in the e-Delivery process;
- **end-entity registration** this role provides for the registration of end-entities to the service, associating them with an address for e-Delivery. This role is not required if the end-entities are addressed by some direct identifier (e.g., the fiscal code).

An e-Delivery management domain necessarily incude the following ancillary roles. Ancillary roles differ from core roles since they are not specific to e-Delivery and may be delegated to third parties:

- **identity provider**: this role is requested for the proper identification of end-users. It may include a Registration Authority role;
- **signature creation/validation**: this role is requested for the creation/validation of signatures on evidencesas well as for signing/validating payload.
- **malware/ spam protection**: this role is requested for the protection of user and systems against malware and spam.
- **certification authority**: this role is necessary for providing the actors with the necessary keys and certificates (for securing the transport, for the creation/validation of signatures on evidences, etc.);

- **time certification**: this role is requested for ensuring a reliable time reference on the evidences/signatures. It might be implemented by a Time Stamping Authority or by different means, provided that the provider has gone through an appropriate assessment process;

- **Service discovery/negotiation**: this role is requested for the proper management of the service discovery, for the exposure of additional characteristics of e-Delivery management domains (requirements and/or capabilities) and for the negotiation process against peer domains.

To provide further features, an e-Delivery management domain may incude optional roles, like:

- **message repository /long term storage**: this role provides archiving services for the messages;

- **evidence validation**: this role provides a validation service for the eveidences generated in the process;

- **message gateway**: this role supports the transfer of e-Delivery messages to and from external electronic/traditional delivery services

- **message interpretation/transformation**: this role provides advanced services for the semantical interpretation, translation, transformation of message’s format;

- **end-entity directory**: this role provides services for the discovery of end users of the system

The table below summarizes the allocation of e-Delivery service features identified in clause 5 to the appropriate role:

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	Maleware/spam protection
Antispam	Maleware/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	---

Table 2: Features and Roles

6.5 Implications to standardization activities

From a standardization perspective, the basic service model (clause 6.1) raises some relevant issues related to conformance: in order to qualify as an e-Delivery service (according to the Draft regulation) some basic features have to be provided. Some more advanced features are required for qualified electronic delivery service[1].

The distributed service model adds some more issues, related to the information flow between eDMDs (the "internal interface"). According to the distributed sequence diagram, three different interactions should be supported:

- service discovery/negotiation. This interaction may be further split into "getting routing info", "trust establishment", "capability negotiation", as discussed in clause 6.2.
- payload delivery. It includes payload security and additional meta-data
- evidence and identification information. It includes the exchange of evidences and identity information in order to promote the message exchange to a "registered" status.

In order for two providers to interact, the "internal interface" must be fully speficified according to the layers introduced in EIF [i.31], in terms of content semantics (the information which should be transported, 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 natural candidate for "routing info" semantics, syntax and protocol, S/MIME may play a role as "payload delivery" syntax, TSL may be used for trust content and syntax, while ebMS [i.25] and SMTP [i.26] are two likely alternatives for the protocol of "payload delivery".

The table below summarizes the necessary specifications for interoperable e-Delivery and whether they are currently available or need to be provided by future standardization activities.

Files within this table 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 wich are not already prodived (or, at least, not fully provided) by existing known standards are marked as "In scope" of a standardization activity for e-Delivery, which may result either in the production of the specific targeted specification or in the profiling of existing standards.

[1] The basic model also raises a standardization issue on external interfaces: 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 analysis.

		Content Semantics	Content syntax	Messaging protocol
Message delivery	Payload delivery	Out of scope	Out of scope	Out of scope
	Meta-info 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 n scope (extension)	Partially in scope (binding)
	Trust establishment	In scope	Partially in scope (extension)	Partially in scope (binding)

Table 3: classification fo e-Delviery specifications

Routing

eDMD 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 conection with the transport protocol, so it is largely out of scope.

Capabilities/requirements

eDMD need to identify the cababilities 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 may apply to this interaction, there are some points of interest to e-Delivery standardization:

- the contents of the e-Delivery specific negotiation parameters need to be standardized
- an appropriate extension to the syntax for e-Delivery negotiation may be required.

Trust establishment

eDMD need to trust the remote counterpart, otherwise they wouldn't forward the message. The natural candidate to this purpose is the Trust Service List [i.XXX] as required by Commission Decision 2010/425/EU ([i.3], [i.4]). The specific content for e-Delivery needs to be standardized (possibly, leveraging on the TSL [i.7] extension mechanism). The binding to a protocol may be required, depending on the specific technology (under the TL model [i.4] 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).

Payload delivery

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

Meta-info exchange

Payload delivery is normally associated to the transfer of meta-information which is relevant to the e-Delivery process. This falls in scope of the standardization activity for these aspects:

- Semantics/syntax: several e-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.17] or XML [i.24]).
- 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 bingings.

User identity exchange

In order to set up a registered delivery process, eDMDs must interact for the exchange of end-user identity information and related Level of Assurance (as defined, for instance, in [i.20] or in the STORK project). This implies that:

- a profile of standards identity information tokens (e.g. X.509 [i.18], SAML [i.23], etc.) have to be in place.
- A precise way to exchange the above information over a transport protocol (binding) have to be established.

Evidence exchange

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

- a common semantics and syntax for evidences must be in place (e.g, PDF [i.19] or XML [i.24]).
- evidences may be exchanged 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, one or more specific bindings are required.

7. Inventory of existing specifications

As a major input to the development of the rationalised framework an inventory has been collected of existing standardisation and publicly available specifications. This ensures that the rationalised 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 focussed on the standards and specifications related to “core” e-Delivery services, as identified in the model [clause 6]. Specifications related to ancillary services, which are nevertheless necessary to the implementation of a complete e-Delviery solution, are out of scope form the present inventory.

The inventory does not takes 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 introperabilily.

The information has been collected from information known to the specialist task force developing this framework and provided by stakeholders.

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

8 Rationalised Structure for Electronic Delivery Standardisation Documents

8.1 e-Delivery Standardisation Classification Scheme

In order to meet its objectives and in particular simplification requirements for the standardisation landscape and its structuring, as well as requirements on the accessibility to the relevant standards and their presentation, the rationalised structure has been organised in the eSignature Rationalised Frameworks around 6 (functional) areas and 5 types of documentation, corresponding Area 5 to Trust Application Service Providers. This contains two sub-areas, respectively the one dedicated to Registered Electronic Mail (REM) services provisioning, and the one dedicated to Data Preservation Service Providers (DPSP).

The documents required for standardisation of e-Delivery have been organised around the following five types of documents:

1) **Guidance:** This type of documents does not include any normative requirements but provides business driven guidance on addressing the eSignature (functional) area, on the selection of applicable standards and their options for a particular business implementation context and associated business requirements, on the implementation of a standard (or a series of standards), on the assessment of a business implementation against a standard (or a series of standards), etc.

2) **Policy & Security Requirements:** This type of document specifies policy and security requirements for services and systems, including protection profiles. This brings together use of other technical standards and the security, physical, procedural and personnel requirements for systems implementing those technical standards.

3) **Technical Specifications:** This type of document specifies technical requirements on systems. This includes but is not restricted to technical architectures (describing standardised elements for a system and their interrelationships), formats, protocols, algorithms, APIs, profiles of specific standards, etc.

4) **Conformity Assessment:** This type of document addresses requirements for assessing the conformity of a system claiming conformity to a specific set of technical specifications, policy or security requirements (including protection profiles when applicable). This primarily includes conformity assessment rules (e.g. common criteria evaluation of products or assessment of systems and services).

5) **Testing Compliance & Interoperability:** This type of document addresses requirements and specifications for setting-up interoperability tests or testing systems or for setting-up tests or testing systems that will provide automated checks of compliance of products, services or systems with specific set(s) of technical specifications.

			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 e-Delivery services applying e-Signatures
					Policy & Security Requirements	
EN	3	19	5	1	1	Policy & Security Requirements for Registered Electronic Mail (REM) Service Providers
EN	3	19	5	2	1	Policy & Security Requirements for Data Preservation Service Providers (DPSPs)
EN	***3***	***19***	***5***	***3***	*1*	***Policy & Security Requirements for e-Delivery Service Providers***
					Technical Specifications	
EN	3	19	5	1	2	Registered Electronic Mail (REM) Services
EN	3	19	5	2	2	Data Preservation Services through signing
EN	***3***	***19***	***5***	***3***	*2*	***E-Delivery Services*** ***Part 1: Framework and Architecture*** ***Part 2: Semantic Contents*** ***Part 3: Formats*** ***Part 4: Bindings***
					Conformity Assessment	
EN	3	19	5	1	3	Conformity Assessment for REM Service Providers
EN	3	19	5	2	3	Conformity Assessment of Data Preservation Service Providers
EN	3	19	5	3	3	***Requirements for conformity assessment bodies assessing Electronic Delivery Services Providers***
					Testing Compliance & Interoperability	
TS	1	19	5	0	4	General requirements for Testing Compliance & Interoperability of TASPs
TS	1	19	5	1	4	Testing Compliance & Interoperability of REM Service Providers
TS	***1***	***19***	***5***	***2***	***4***	***Testing Compliance & Interoperability of e-Delviery Service Providers***

Table 4: Standards for Trust Appliactioin Service Providers

8.2. e-Delivery Standardisation proposal aligned with the Rationalized Framework and based on the model

Guidance

TR 119 500 Guidance for Trust Application Service Provider

This document should provide guidance for the selection of standards for Trust Application Service Providers for given business requirements. It should include guidance for e-Delivery service providers

Policy and Security Requirements

EN 319 531 Policy & Security Requirements for e-Delivery Service Providers

This document specifies policy and security requirements for TASPs providing electronic delivery services and for TASPs providing qualified electronic delivery services considering, when necessary, different conformity levels and styles of operation. This is a multi-part document structured as follows:

Part 1: Policy and Security Requirements for TASPs providing Electronic Delivery Services. This part might define general and common requirements for all conformity levels. It also addresses requirements on Information Security Management. Informative annexes will provide check lists for conformity assessment.

Part 2: Policy and Security Requirements for TASPs providing Qualified Electronic Delivery Services. This part might define specific requirements for all for TASPs providing Qualified Electronic Delivery Services aligned with the general requirement's document, including requirements on Information Security Management. Management. Informative annexes will provide check lists for conformity assessment.

New Policy and Security Requirements parts could appear in the future if new categories of TASPs providing Electronic Delivery Services with additional requirements will be defined.

Technical Specifications

EN 319 532 e-Delivery Services

This document provides technical specifications for the provision of e-Delivery. 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 this document, are proposed and accepted. Should this happen, part 1 (Framework, Architecture and Evidence) should be properly updated and extended to be aligned with the new part.

EN 319 532-1: 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 e-Delviery transactions;
- Interfaces between the different roles and providers;
- Relevant events in the data objects flows and the corresponding evidence;
- Trust building among providers pertaining to the same or to different administrative domains.

EN 319 532-2: Semantic Contents. This is a multi-part document which provides a specification of the semantic contents to be produced and managed in e-Delivery transactions, according to table 2 in clause 6.5. It includes:

- **Message delivery content.** This document specifies the semantic of the meta-information which will possibly be associated to the transmission of the payload;
- **Evidence and identification content**. This document fully specifies 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. This document also specifies the content related to end user identity to be managed in the transactions.
- **Service discovery content.** This document specifies the information related to the identification of the remote eDMD, 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 e-Delivery services);

EN 319 532-3: Formats. This is a multi-part document which provides a specification of the formats for the different contents to be produced and managed in e-Delivery transactions, according to table 2 in clause 6.5. It includes:

- **Message delivery formats.** This document specifies the specific format/formats for the meta-information specified in EN 119 532 Part 2 sub-part 2. Meta-information may come either in attached (as an envelope including the payload) or detached format.
- **Evidence and identification formats**. This document fully specifies the specifies syntax for the set of evidence and user identity information specified in EN 119 532 Part 2 sub-part 3
- **Service discovery formats.** This document specifies the specific format/formats for capabilities, requirements and trust information specified in EN 119 532 Part 2 sub-part 1;

EN 319 532-4: Bindings. This is a multi-part document. Each part will fully specify the binding to a messaging protocol that is supporting Electronic Delivery Services provision. This will include, among other things: specification on how to transport evidence within the protocols messages, how to include signature’s provider within the protocol’s message, etc. Each part will specify 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:

- **Message delivery binding(s):** this (these) document(s) will specify binding(s) for a number of identified relevant messaging protocols (such as e-bMS 3.0 [i.25], SOAP [i.29], or any other that is considered worth to include).
- **Evidence and identification binding(s):** this (these) document(s) will specify binding(s) for a number of identified relevant messaging protocols (such as e-bMS 3.0 [i.25], SOAP [i.29], or any other that is considered worth to include) or trust token exchange protocols (which may be completely unrelated to the messaging protocols).

- **Capability/requirements binding(s):** this (these) document(s) will specify 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.

Conformity Assessment

EN 319 533. Requirements for conformity assessment bodies assessing Electronic Delivery Services Providers

This document contains requirements for the competence, consistent operation and impartiality specific to conformity assessment bodies assessing conformity of TASPs providing Electronic Delivery Services to standardized criteria for the provision of this kind of services

Testing Conformance and Interoperability

TS 119 504 General requirements for Technical Conformance & Interoperability Testing for Trust Application Service Providers

This document specifies general requirements for specifying technical conformance and interoperability testing for TASPs. This document should be updated for taking into consideration the Electronic Delivery subarea.

TS 119 524 Testing Conformance & Interoperability of e-Delivery Service Providers

This document defines test suites that support interoperability tests among entities that plan to provide Electronic Delivery services. It also specifies tests to be performed for checking conformance against relevant specifications of EN 319 532. This is a multi-part document, whose structure is detailed below:

- **Test suites for interoperability testing of Electronic 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.

- **Testing conformance**: This document specifies the tests to be performed for checking conformance against relevant specifications of EN 319 532. This provides the basis for a tool that automatically checks conformance against the aforementioned relevant specifications.

Annex A: Pan-European Solutions

Far from pretending to be exhaustive, in the following some pan-European e-Delivery solutions will be presented. An inventory of national eDelivery solutions in Europe is provided in [i.33] and to some extent in [i.34].

A.1 SPOCS LSP

Description	The SPOCS European Large Scale Pilot (LSP) aimed at contributing to the next generation of online portals (Point of Single Contact or PSC) for enterprises, which every European country now has in place in abidance to Directive 2006/123/EC [i.2], through making cross-border electronic procedures available in these portals. One of his building blocks deals with interoperable, secure and trustworthy interconnection of the EUMS e-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 e-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.29] , WS-Addressing, WS-Security [i.22], WS-ReliableMessaging [i.28]
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 (RFC 5322 [i.26], Address Specification). Gateway address dispatches have to be targeted to beeing derived from addressee’s domain, resolution of delivery endpoint left to domestic capabilites of target domain.
Addressing	Open for different models, a concrete communication partner identifier always has to be marked by its type. Actually, only RFC 5322 (e-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 informations given by (propriatary) 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 support by domestic source/target solution, the gateway a solution is related to has to convert from/to domestic message formats (valid as well for evidences and authentication token).
Trust establishment	Trust Lists according ETSI TS 102 231, covering all e-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 must fulfil functionalities as defined by the TS 102 640 basic conformance profile.
Delivery traceability and provability	Gateway to gateway route: ETSI REM Evidences, according TS 102 640 Part 2. 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.2 e-SENS LSP

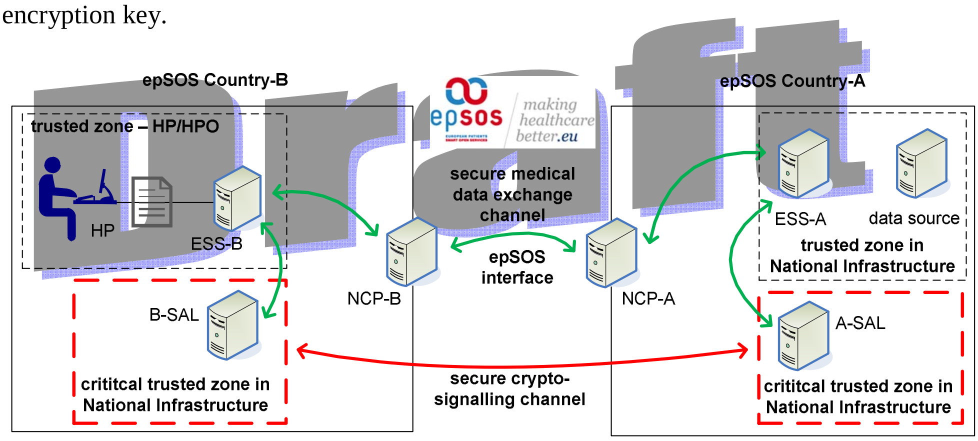
Note: e-SENS has recently started, so the information given below is not yet consolidated and may be subject to change.

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 WP 6 Sub Group Competence Cluster 6.1 (SGCC 6.1) deals with the building block e-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 e-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.

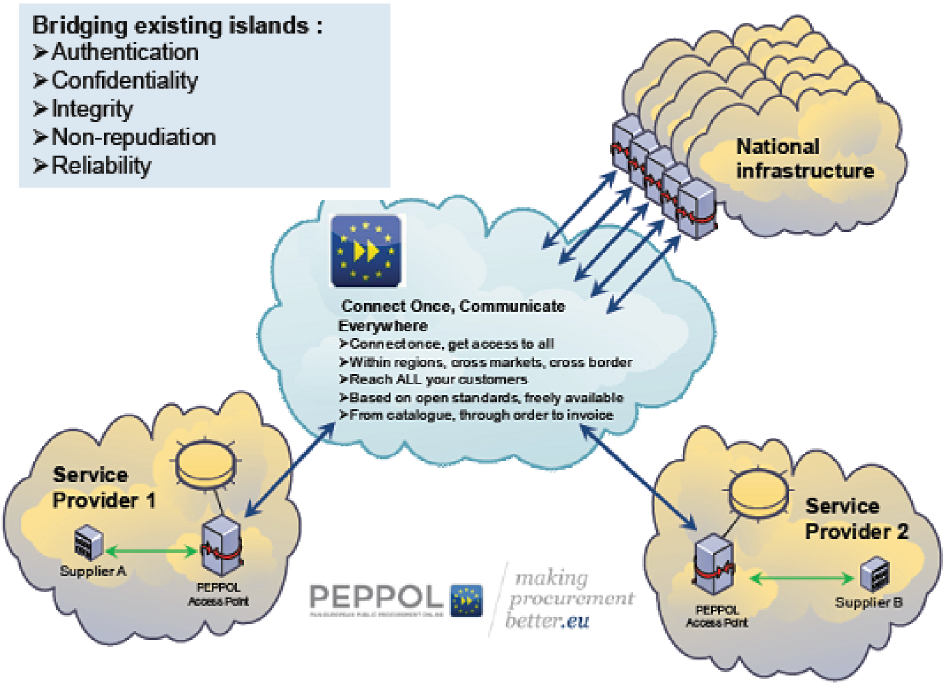
	Web Services
Service/Endpoint discovery	Open issue in e-SENS. Starting point (additional adoption of other concepts in discussion): Discovery of communication partners and service capabilities using the PEPPOL Service Metadata Locators (SML) and Service Metadata Publishers (SMP) technology.
Addressing	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-Deferation.
Non-repudiation services (Evidences)	ETSI REM standard (a profile of selected evidences is not yet available)

A.3 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-Citiziens
Architectural model	From an IT 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 thei 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 rfc5424-based protocol (for audit trails)
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 XCPD 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 adopter 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_j., 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-ESS is separating the encryption grade form the length of the secret (TAN) the patient has to provide to the HP. In contrast to Symmetrical Direct Encryption Mode, the TAN is not used directly as the encryption key anymore but merely as foundation for deriving a longer and more secure encryption key.  epSOS Country-B trusted zone – HP/HPO HP ESS-B B-SAL crititcal trusted zone in National Infrastructure epsos making healthcare better.eu secure medical data exchange channel NCP-B epSOS interface NCP-A secure crypto-signalling channel epSOS Country-A ESS-A data source trusted zone in National Infrastructure A-SAL crititcal trusted zone in National Infrastructure **Figure 6: 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 XCF (based on OASIS RegRep) - HL7v3 / IHE XCPD - Syslog (rfc5424)
Trust establishment	Mutual gateway authentication via TLSv1
Delivery traceability and provability	Based on Audit Trail and Node Authentication (IHE ATNA).

A.4 PEPPOL

NOTE: this text is derived from the PEPPOL web site at http://www.peppol.eu/peppol-projectDescription	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. The PEPPOL electronic delivery infrastructure is based on a four corner model of interchange: trading partners (or service provider on their behalf) are connected to PEPPOL using Access Points (AP)- The infrastructure provides services for eProcurement with standardised electronic document formats.
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 are connected to PEPPOL using Access Points (AP) and is described in a set of documents known as Business Document Exchange Network (BUSDOX) that includes: • CommonDefinitions: 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 REST (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. • Secure Trusted Asynchronous Reliable Transport (START): 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. • Lightweight Message Exchange Profile (LIME): providing a simple low-cost approach for Small and Medium Enterprises (SMEs) to access Business Document Exchange Network (BUSDOX) infrastructure. • PEPPOL Identifier Schemes: defining a set of identifier schemes that will be used in the context of the PEPPOL infrastructure.  Bridging existing islands : ➢Authentication ➢Confidentiality ➢Integrity ➢Non-repudiation ➢Reliability National infrastructure Connect Once, Communicate Everywhere ➢Connect once, get access to all ➢Within regions, cross markets, cross border ➢Reach ALL your customers ➢Based on open standards, freely available ➢From catalogue, through order to invoice Service Provider 1 Supplier A PEPPOL Access Point PEPPOL making procurement better.eu Service Provider 2 PEPPOL Access Point Supplier B
Transport layer	Web Services (WS-*) stack.
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 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 support mutual authentication of the nodes via SSL/TLS and issuance of signed SAML assertions to support the required authorizations.
Delivery traceability and provability	Based on Audit Trail and Node Authentication

A.5 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”[2]. 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 shall be used by all actors, connected by an interoperable, trustworthy and secure e-Delivery network for cross-border data exchange. In addition, the European e-Justice portal shall be 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 e-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 (MSH), 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. In

[2] e-CODEX Deliverable 5.1 Requirements

	evaluation, how dynamic discovery via SML/SMP can be made to work together with ebMS CPP/CPA mechanisms and Processing-Modes (“P-Mode”)[3]. Actually 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 e-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 SBDH 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. May 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 TS 102 640 Part 2. Evidences seen as related to “Business Level”, thus allocated to the message payload. Left to adapters to national solutions, how to deal with Evidences.

A.6 e-Trustex

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 e-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

[3] A proof of concept has been created, to be published.

	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: e-PRIOR (Procurement), e-GREFFE (Legislative support), e-COMP (Competition cases) and e-Cohesion (Support to cohesion policy). With so-called CIPA gateways, which serve as access points to other e-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 ID 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 must authenticate to the e-TrustEx platform with their credentials (UID/PWD).
Non-repudiation services (Evidences)	The following non-repudiation services are supported: • NRO (non-repudiation of origin) • NRS (non-repudiation of submission) • NRD (non-repudiation of delivery) • NRR (non-repudiation of receipt)

Annex B: Review of the Inventory

The annex is provided as a separate excel sheet.

Annex C: Bibliography

1. "ISA multimedia assets library". 2011.
2. "ISA Strategy - Commission's Communication on Interoperability". 2010.
3. Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures
4. 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
5. "Study on the standardisation aspects of e-signatures", SEALED, DLA Piper et al, 2007.
6. "CROBIES: Study onCross-Border Interoperability of eSignatures", Siemens, SEALED and TimeLex, 2010.
7. ISO/IEC 27000: "Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary".
8. IETF RFC 3647: "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework".
9. W3C Recommendation: "XML Signature Syntax and Processing (Second Edition)", 10 June 2008,
10. ISO 32000-1: "Document management -- Portable document format -- Part 1: PDF 1.7".
11. 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.
12. IETF RFC 3161 (August 2001): "Internet X.509 Public Key Infrastructure Time-Stamp Protocol".
13. CCMB-2006-09-001: "Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 3.1, Revision 3", July 2009
14. ITU-T Recommendation X.509/ISO/IEC 9594-8: "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks".
15. Apitzsch J. Mechanismen zur Nachweisbarkeit der Kommunikation bei OSCI Transport. Datenschutz und Datensicherheit – DuD 2007;31(10):744-46
16. Apitzsch J, Liehmann M, Martin B, Rieger S, Seeger M. Assessment of existing eDelivery systems and specifications required for interoperability, 2010.
17. Capgemini, Architecture for delivering pan-European e-Government services (PEGS Infrastructure) version 1.0, 2004.
18. Council of Europe. European convention on the service abroad of documents relating to administrative matters. European Treaty Series – No. 94. 1977.
19. Dietrich J, Keller-Herder J. De-Mail — verschlüsselt, authentisch, nachweisbar. Datenschutz und Datensicherheit – DuD 2010;34(5):299-301
20. European Commission, Architecture Guidelines For Trans-European Telematics Networks for Administrations version 7.1, 2004.
21. European Commission, Study on electronic documents and electronic delivery for the purpose of the implementation of Art. 8 of the Services Directive, 2009.
22. European Commission, European Interoperable Infrastructure Services – Study on potential reuse of system component version 1.1, 2010.

23. European Union. 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.

24. Ferrer-Gomilla F, Onieva J, Payeras M, Lopez J. Certified electronic mail: Properties revisited. Computers & Security 2010;29(2):167-79

25. Freemantle M, Lightweight Message Exchange Profile (LIME), Version 1.0.0, December 2009.

26. Freemantle M, Secure Trusted Asynchronous Reliable Transport (START), Version 1.0.0, December 2009.

27. Gennai F, Martusciello L, Buzzi M, A certified email system for the public administration in Italy. IADIS International Conference WWW/Internet, 2005, vol. 2, pp. 143—147

28. Hoffman P, Enhanced Security Services for S/MIME, Internet Engineering Task Force (IETF), RFC 2634, June 1999.

29. Hulsebosch B, Lenzini G, Eertink H. STORK D3.2 – Quality authenticator scheme, 2009.

30. ITU-T (International Telecommunication Union). Recommendation X.402 – Data Communication Networks – Message Handling Systems – Overall Architecture. 1992.

31. ITU-T (International Telecommunication Union). Recommendation F.400/X.400 - Series X: Data Networks and Open System Communications. Message handling system and service overview. 1999.

32. Kremer S, Markowitch O, Zhou J. An intensive survey of fair non-repudiation protocols. Computer Communications 2000;25:1606-21

33. Leitold H, Zwattendorfer B. STORK: Architecture, Implementation and Pilots. ISSE 2010 Securing Electronic Business Processes, 2010, pp. 131—142

34. Miranda J.P, Melo J. EPM: Tech, Biz and Postal Services Meeting Point, ISSE 2004 - Securing Electronic Business Processes; 259-267. 2004

35. Olnes J, Buene L, Andresen A, Grindheim H, Apitzsch J, 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

36. Onieva J, Zhou J, Lopez J. Multiparty Nonrepudiation: A survey. ACM Computing Surveys 2008;41(1)

37. Oppliger R. Providing certified mail services on the internet. IEEE Security and Privacy 2007;5(1)

38. Ornetsmüller G. webERV – ERVServices – Beschreibung der Webservice-Schnittstelle Teilnehmer <-> Übermittlungsstelle. 2007.

39. Planitzer F, Weisweber W. Virtual Post Office in Practice. ISSE/SECURE 2007 Securing Electronic Business Processes. 2007. p. 427-37

40. Rössler T, 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

41. 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

42. Tauber A. Requirements and Properties of Qualfied Electronic Delivery Systems in eGovernment – an Austrian Experience. International Journal of E-Adoption, vol 2., no. 1, 2010, pp. 45-58.

43. Tauber A. A survey of certified mail systems provided on the Internet. Computers & Security 2011 (in press)

44. UPU (Universal Postal Union). S43: Secured electronic postal services (SePS) interface specification - Part B: EPCM Service. 2003.

45. W3C, SOAP Message Transmission Optimization Mechanism, 2005.

46. Apitzch J., Boldrin L., Caccia A., Foti S., Cruellas J. C., Llaneza P, 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 Highligths of the Information Security Solutions Europe Conference 2011

47. Tauber A., Apitzsch J., Boldrin L. (2012). An interoperability standard for certified mail systems, Computer Standards & Interfaces, http://dx.doi.org/10.1016/j.csi.2012.03.002

48. IETF RFC 6109. La Posta Elettronica Certificata - Italian Certified Electronic Mail.

History

<table>
<tr><th colspan="3">Document history</th></tr>
<tr><td><Version></td><td><Date></td><td><Milestone></td></tr>
<tr><td>V0.0.1</td><td>June 2013</td><td>Early draft</td></tr>
<tr><td>V0.0.2</td><td>September 2013</td><td>Full draft for public review</td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
</table>