# SLOVENSKI STANDARD
# SIST SR 019 050 V1.1.1:2015

**01-oktober-2015**

**Elektronski podpisi in infrastruktura (ESI) - Racionalizirani okvir standardov za priporočeno elektronsko dostavo z uporabo elektronskih podpisov**

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

**Ta slovenski standard je istoveten z: SR 019 050 V1.1.1**

**ICS:**

| | | |
|---|---|---|
| 35.040 | Nabori znakov in kodiranje informacij | Character sets and information coding |

**SIST SR 019 050 V1.1.1:2015 en,fr,de**

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

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

Reference

DSR/ESI-0019530

Keywords

electronic signature, electronic registered delivery, security

*ETSI*

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

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

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

### *Important notice*

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (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:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

### *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 Electronic Signatures and Infrastructures (ESI).

# Modal verbs terminology

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

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

# Introduction

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

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

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

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

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

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

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

# 1 Scope

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

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

# 2 References

## 2.1 Normative references

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

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

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

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

Not applicable.

## 2.2 Informative references

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

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

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

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

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

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

[i.2] Commission Decision 2009/767/EC of 16 October 2009 setting out measures facilitating the use of procedures by electronic means through the 'points of single contact' under Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[i.20] OASIS WS-Trust 1.4.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[i.34] PEPPOL Infrastructure specifications.

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

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

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

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

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

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

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

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

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

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

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

# 3 Definitions and abbreviations

## 3.1 Definitions

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

## 3.2 Abbreviations

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

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

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

# 4 Methodology

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

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

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

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

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

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

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

# 5 Features

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

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

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

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

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