Draft ETSI EN 319 522-2 V0.0.4 (2017-10)

Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services Part 2: Semantic Contents

STABLE DRAFT FOR PUBLIC REVIEW UNTIL 29 DECEMBER 2017

Download the template for comments:

https://docbox.etsi.org/ESI/Open/Latest_Drafts/Template-for-comments.doc

Send comments ONLY 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://www.etsi.org/standards-search

Reference

DEN/ESI-0019522-2

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

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
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

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

Essential patents

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 (https://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.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

This draft European Standard (EN) has been produced by ETSI Technical Committee| ESI and is now submitted for public review before approval by TC ESI and submission for the combined Public Enquiry and Vote phase of the ETSI standards EN Approval Procedure.

The present document is part 2 of a multi-part deliverable. Full details of the entire series can be found in [1].

Proposed national transposition dates	
Date of latest announcement of this EN (doa):	3 months after ETSI publication
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	6 months after doa
Date of withdrawal of any conflicting National Standard (dow):	6 months after doa

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.

1 Scope

The present document specifies the semantic content that flows across the interfaces of ERD systems which are specified in [1] clause 5.

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 https://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.

[1] ETSI EN 319 522-1: " Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 1: Framework and Architecture".

[3] ETSI EN 319 522-3: " Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 3: Formats".

[4] ETSI EN 319 522-4-1: " Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 4-1: Message delivery binding".

[5] ETSI EN 319 522-4-2: " Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 2: Evidence and identification binding".

[9] IETF RFC 3061: "A URN Namespace of Object Identifiers".

[10] CEF eIDAS Technical Sub-group: "eIDAS SAML Attribute profile". Version 1.1.2. October 2016.

[17] Core Person Vocabulary. https://joinup.ec.europa.eu/asset/core_vocabularies/description.

[18] Registered Organizations Vocabulary. https://joinup.ec.europa.eu/asset/core_vocabularies/description.

[19] IETF RFC 4122: A Universally Unique IDentifier (UUID) URN Namespace

[20] IETF RFC 5332: Internet Message Format

[21] ETSI TS 119 312 Electronic Signatures and Infrastructures (ESI); Cryptographic Suites

[22] ETSI TS 119 612 Electronic Signatures and Infrastructures (ESI); Trusted Lists

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.

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]	Regulation (EU) No 910/2014

3 Definitions and abbreviations

For the purposes of the present document, the definitions and abbreviations given in [above1] apply.

4 Overview

The present document specifies the semantic content that flows across the interfaces which have been identified in ETSI EN 319 522-1 [1]. No requirements are introduced on the specific formats for the content; formats are specified in ETSI EN 319 522-3 [3].

The figure 1 below outlines how data flows through the interfaces in the four corner model. As detailed below, not all objects are always required.

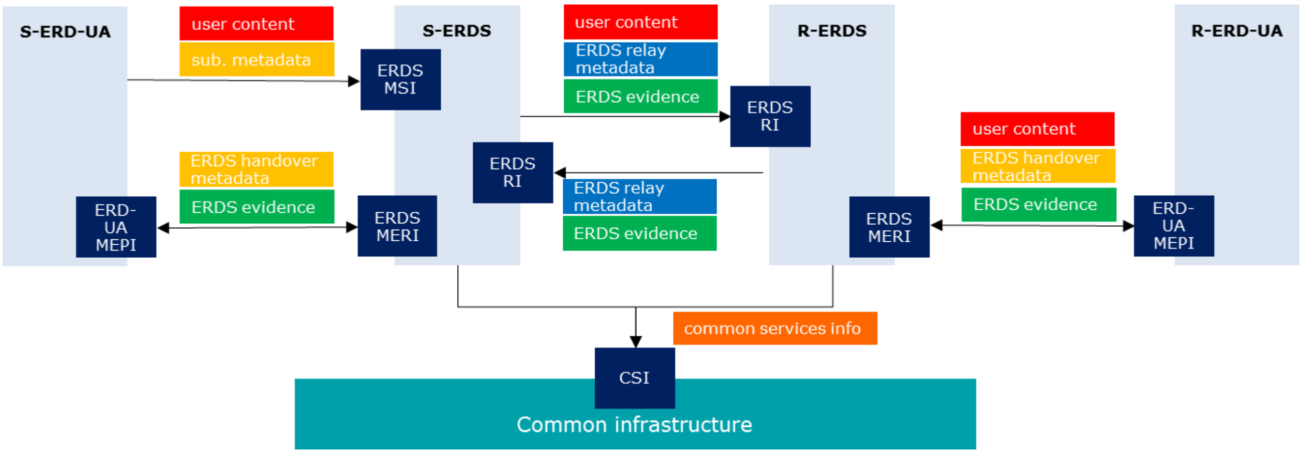

Figure 1: data flowing through interfaces

For convenience, we define some aggregate constructs (ERD dispatch, ERDS receipt, ERDS notification, ERD payload, original message) which package the basic objects (user content, ERDS relay metadata, ERDS evidence, submission metadata) in different modes. The naming convention used in this document is that constructs whose content is completely generated by the ERDS are prefixed with “ERDS”, while constructs whose content includes user generated data is prefixed with “ERD”. The table below specifies the composition of constructs:

Table 1. composition of constructs

construct		user content	ERDS relay metadata	ERDS evidence	submission metadata
ERD message	ERD dispatch	1	1	1-n	
	ERDS receipt		1	1-n	
	ERDS serviceInfo		1		
	ERD payload	1	1		
	original message	1			0-1

The table below provides an abstraction of the APIs, which reflect the arrows in the sequence diagram of [1]:

Table 2. abstract interfaces

Interface	Pseudo code API	Description	Arguments and output
ERDS MSI	out := SubmitMessage(uc, a)	The method is used for posting an original message to the S-ERDS. In order to use the SubmitMessage API, the UA/Application has to prove that the ERD Sender is the owner of the ERD Sender's identifier (via an authentication token, a challenge response, etc.).	uc: user content a: submission metadata out: this is the outcome of the request, which normally includes a message identifier. There is no specification on the outcome, which may be a simple success/error indication, or may include a larger set of information.
ERDS MERI	out := AccessToMessage(mi)	The method is used for retrieving a user content from the R-ERDS. Alternatively, a push of the user content to the recipient UA/application can be used through the ERD-UA MEPI interface In order to use the AccessToMessage API, the UA/Application has to prove that the ERD Recipient is the owner of the ERD Recipient's identifier (via an authentication token, a challenge response, etc.).	mi: this is a set of parameters which is used for the identification and retrieval of the requested user content out: this is the outcome of the request, which, in case of success, includes the user content and possibly some handover metadata, ERDS relay metadata and evidence. In case of failure the outcome will include error information.
	e := GetEvidence(ei)	The method is used for retrieving one or more evidences associated to a user content which has previously been managed by the ERDS. Note that this is not the only way to obtain evidence, since an evidence can be transmitted in different ways (e.g. as an output of the SubmitMessage or the AccessToMessage)	ei: this is a set of parameters which is used for the identification and retrieval of the requested evidence. e: the requested evidences
ERDS RI	out := Relay(uc, m, e)	The method is used for relaying an ERD message to a different ERDS. Relying of the payload is used when S-ERDS has not the capability to deliver to the recipient itself. Metadata and evidences may be transmitted with the payload through this method.	uc: user content m: (optional) ERDS relay metadata e: (optional) evidences out: this is the outcome of the relay request, which is a success/failure indication plus error information in case of failure. It may also include an evidence and ERDS relay metadata.
CSI	re:= identify_ERDS(ri)	This method is used to identify the ERDS which has competence for delivering to a defined recipient. The method may return more ERDSs.	ri: unique identification of the recipient, which may be one identifier or a set of attributes that together provides unique identification (e.g. id, domain, application protocol, …) re: one or more endpoints of the ERDS(s) which has(have) competence for delivering to the recipient identified by ri.

	out := validate_ERDS(ei, p)	This method is used to validate the inclusion of an ERDS intro a trust circle. The method may receive some parameters for the validation (e.g., date and time of validity, specific trust circle, …)	ei: a unique identifier for the ERDS p: a set of parameters for the validation out: the outcome of the check, which may include a set of information about the ERDS from a trust perspective.
	em := get_ERDS_Metadata (ei)	This method is used to retrieve operational metadata about a specific ERDS.	ei: a unique identifier for the ERDS em: a set of information about the ERDS from an operational perspective (capabilities, requirements, endpoints….).

The following clauses specify the semantics of the data which are transported through the interfaces; in particular:

- Clause 5 specifies the semantics of the components required for identifying the sender and the recipient..
- Clause 6 specifies the semantics of ERDS relay metadata.
- Clause 8 specifies the semantics of ERDS Evidence.
- Clause 9 specifies the semantics of Common Service Information.

5 Identification of actors

5.1 Introduction

An ERDS needs to generate, exchange and validate attributes to support the identification and authentication of end entities like sender, recipient or a delegate.

5.2 Identifiers

An identifier shall have two components: an identifying scheme name and the identifier value, which shall be coherent with the identifying scheme name.

5.3 Identity attributes

All attributes in this document related to identification and authentication are derived from the EU Vocabulary. For natural persons, the definitions of the Core Person Vocabulary [17] apply, for legal persons, the definitions of the Registered Organization Vocabulary [18]. The Registered Organization Vocabulary defines the core vocabulary for legal persons registered through a formal process, typically in a national or regional register.

For the sake of simplicity, this document limits the supported attributes to the ones defined in the eIDAS attribute profile specification [10], which are also attributes derived from the ISA vocabulary.

5.3.1 Identity attributes of natural persons

For natural persons, the following identity attributes are defined.

Table 3. natural person identity attributes

Attribute (Friendly) Name as defined by [10]	eIDAS minimum data set attribute	Core Vocabulary Equivalent
FamilyName	Current Family Name	cbc:FamilyName
FirstName	Current First Names	cvb:GivenName
DateOfBirth	Date of Birth	cvb:BirthDate
PersonIdentifier	Uniqueness Identifier	cva:Cvidentifier
BirthName	First Names at Birth	cvb:BirthName
BirthName	Family Name at Birth	cvb:BirthName
PlaceOfBirth	Place of Birth	cva:BirthPlaceCvlocation
CurrentAddress	Current Address	cva:Cvaddress
Gender	Gender	cvb:GenderCode

5.3.2 Identity attributes of legal person

For legal persons, the following identity attributes are defined.

Table 4. legal person identity attributes

Attribute (Friendly) Name as defined by [10]	eIDAS MDS Attribute	Core Vocabulary Equivalent
LegalName	Current Legal Name	cvb:LegalName
LegalPersonIdentifier	Uniquenes Identifier	cva:Cvidentifier
LegalAddress	Current Address	cva:Cvaddress
VATRegistration	VAT Registration Number	cva:CvbusinessCode
TaxReference	Tax Reference Number	cva:CvbusinessCode
BusinessCodes	Directive 2012/17/EU Identifier	cva:CvbusinessCode
LEI	Legal Entity Identifier (LEI)	cva:CvbusinessCode
EORI	Economic Operator Registration and Identification (EORI)	cva:CvbusinessCode
SEED	System for Exchange of Excise Data (SEED)	cva:CvbusinessCode
SIC	Standard Industrial Classification (SIC)	cva:CvbusinessCode

5.3.4 Identity attributes of other entities

Identity attributes may also be provided for entities which do not correspond to natural or legal persons (e.g., applications, things). They are not specified in the current version of this document.

5.5 Identity assurance information

This clause defines the information which is necessary to establish the level of assurance for the entities which take part in the electronic delivery process. The following attributes are required:

- An attribute containing details of the registration and identity proofing and verification assurance level. This attribute:
    - shall contain one identifier of the assurance level itself. This identifier shall have a URI as value.
    - may also contain an identifier of the identification policy. This identifier shall have a URI as value.
    - may also contain details on the identification policy.
    - may also contain one or more URIs pointing to resources that contain details of the aforementioned policy provided in different languages.

- An attribute containing details of the authentication means and mechanisms assurance level. This attribute:
    - shall contain one identifier of the assurance level itself. This identifier shall have a URI as value.
    - may also contain an identifier of the authentication policy. This identifier shall have a URI as value.
    - may also contain details on the authentication policy.
    - may also contain one or more URIs pointing to resources that contain details of the aforementioned policy provided in different languages.

- An attribute containing details of the performed authentication, either an assertion generated by an assertion provider or as a sequence of components. This attribute includes:
    - the date and time when the authentication process was conducted.
    - the identification of the authentication method used.

6 ERDS relay metadata

6.1 Introduction

ERDS relay metadata is produced by an ERDS and is provided to a peer ERDS or to a UA/Application. It includes a set of information for the correct processing of the user content between different actors in the delivery process. The ERDS relay metadata may be transmitted together with the user content, with some evidence, or alone as described in [4, 5].

Part of ERDS relay metadata may be replicated in evidences. This is allowed, since metadata may be used for the delivery process; it is also relevant when the user content flows detached from the evidence.

Table 5. metadata components

	Component code	**Component name**	Cardinality	Ref.
	MD01	Metadata version	1	6.2.1
Delivery constraints	MD02	Relay date and time	0-1	6.2.2
	MD03	Expiry date and time	0-1	6.2.3
	MD04	Recipient required auth. level	0-1	6.2.4
	MD05	Applicable policy	0-1	6.2.5
	MD06	Mode of consignment	0-1	6.2.6
	MD07	Scheduled delivery	0-1	6.2.7
Sender/ Recipient	MD08	Sender's identifier	1	6.2.8
	MD09	Reply-to	1	6.2.9
	MD10	Recipient's identifier	1	6.2.10
ERD Message information	MD11	Message identifier	0-1	6.2.11
	MD12	In reply to	0-1	6.2.12
	MD13	ERD Message type	1	6.2.13
	MD14	user content information	1	6.2.14
	MD15	Extensions	0-1	6.2.15
		Signature	0-1	7

The following metadata components are defined:

6.2 Metadata components

6.2.1 MD01 - Metadata version

Description	Metadata version
Format	EN319522.y.z.t
Meaning	The version of the metadata, corresponding to the version of the binding document where it is defined
Requirements	None

6.2.2 MD02- Relay date and time

Description	Relay date and time
Format	Date and time
Meaning	The date and time when an ERDS relays the ERD message to the next ERDS in the delivery chain.
Requirements	An ERDS which forwards the ERD message to a different ERDS **may** use this component to indicate the time when the relay takes place.

6.2.3 MD03 - Expiry date and time

Description	Expiry date and time
Format	Date and time
Meaning	The date-time by which the consignment or handover to recipient is required to be completed.
Requirements	R-ERDS **should not** consign or hand over the user content if the date-time is after the one indicated by this component. The content of this component is provided by the S-ERDS on the base of its policies or of specific requests from the sender. R-ERDS and intermediate ERDS (in the extended model) **shall** propagate this component as received from the previous ERDS in the delivery chain.

6.2.4 MD04 - Recipient required level of assurance

Description	Recipient required level of assurance
Format	LoA enumeration
Meaning	The level of assurance of the identity of the recipient that the sender requires
Requirements	The content of this component is provided by the S-ERDS on the base of its policies or of specific requests from the sender. An ERDS **should not** relay the ERD message if R-ERDS capabilities (retrieved through CSI) do not include the capability to identify the recipient at or above the required level R-ERDS **should not** deliver the user content if it cannot meet the required identification LOA specified by this component. R-ERDS and intermediate ERDS (in the extended model) **shall** propagate this component as received from the previous ERDS in the delivery chain.

6.2.5 MD05 - Applicable policy

Description	Applicable policy
Format	Policy enumeration
Meaning	The policy that the S-ERDS requires to be applied to the management of the ERD message by the subsequent ERDSs in the delivery chain.
Requirements	The content of this component is provided by the S-ERDS on the base of its policies or of specific requests from the sender. Any ERDS **should not** relay the user content if the next ERDS capabilities (retrieved through CSI) do not include the capability to support the mentioned policy. Any ERDS in the chain **should** refuse the ERD message if it can not support the policy specified by this component. R-ERDS and intermediate ERDS (in the extended model) **shall** propagate this component as received from the previous ERDS in the delivery chain.

6.2.6 MD06 - Mode of consignment

Description	Mode of consignment
Format	Binding specific, so that to express one of the options below.
Meaning	The requested mode of consignment of the user content to the recipient chosen among the following options: • **Basic**: the user content has to be made available to the recipient without the possibility for the recipient to accept/deny before delivery. • **Consented**: a notification shall be sent to the recipient before actual consignment/handover. The recipient shall be required to perform an explicit action to accept or reject the uer content; the user content shall only be accessible to the recipient upon acceptance. • **Consented signed**: as for Consented, with the addition that the recipient shall be required to digitally sign an acknowledgment of receipt. • **Other**: other modes of consignment can be agreed and specified in specific domains
Requirements	• . If this component is not present, R-ERDS shall consign the user content according to its policy and to the recipient’s setting. Any ERDS **should not** relay the ERD message if the R-ERDS capabilities (retrieved through CSI) do not include the capability to support the consignment mode. R- ERDS **shall** refuse the relay of the user content if it cannot support the requested consignment mode or if the recipient’s settings do not allow that consignment mode. Otherwise, it **shall** consign the user content according to the requested consignment mode. R-ERDS and intermediate ERDS (in the extended model) **shall** propagate this component as received from the previous ERDS in the delivery chain.

6.2.7 MD07 - Scheduled delivery

Description	Scheduled delivery
Format	Date and time
Meaning	The time instant after which the user content can be consigned/handed over.
Requirements	The user content shall not be handed over to the recipient before this time. If this component is present, its content **shall** be provided by the S-ERDS on the base of its policies or of specific requests from the sender. Any ERDS in the chain **should** refuse the ERD message if it cannot support delaying the delivery of the user content until the time indicated in this component. R-ERDS and intermediate ERDS (in the extended model) **shall** propagate this component as received from the previous ERDS in the delivery chain.

6.2.8 MD08 - Sender's identifier

Description	Senrer’s identifier
Format	
Meaning	Identifier of the sender of the user content..
Requirements	As defined in clause 5.2.

6.2.9 MD09 - Reply-to

Description	A unique reply-to identifier
Format	Binding specific
Meaning	The identifier, as specified in 5.2, to which any reply from the recipient or delegate of the recipient should be sent to, as a result of the reception of the sender’s user content
Requirements	The content of this component is provided by the S-ERDS on the base of its policies or of specific requests from the sender. R-ERDS and intermediate ERDS (in the extended model) **shall** propagate this component as received from the previous ERDS in the delivery chain.

6.2.10 MD10 - Recipient's identifier

Description	Recipient’s identifier
Format	
Meaning	Identifier of the recipient of the user content, as defined in clause 5.2.
Requirements	None

6.2.11 MD11 - Message identifier

Description	Message identifier
Format	Binding specific
Meaning	Unique identifier of the original message as generated by S-ERDS (e.g. a UUID according to RFC 4122 [19], or an UID as defined in RFC 5322 [20])
Requirements	. The content of this component is provided by the S-ERDS. R-ERDS and intermediate ERDS (in the extended model) **shall** propagate this component as received from the previous ERDS in the delivery chain.

6.2.12 MD12 - In reply to

Description	In reply to
Format	Binding specific
Meaning	Association to a previous original message. I.e. the message identifier of the original message to which the new original message is a reply
Requirements	S-ERDS **should** produce this component if in-reply-to information is present in submission metadata . R-ERDS and intermediate ERDS (in the extended model) **shall** propagate this component as received from the previous ERDS in the delivery chain.

6.2.13 MD13 - Message type

Description	Message type
Format	Binding specific
Meaning	Type of the ERD message
Requirements	ERDSs **may** use this component to specify the type of the ERD message (ERD payload, ERD dispatch, ERDS notification, ERDS receipt).

6.2.14 MD14 - User content information

Description	User content information
Format	Binding specific
Meaning	Information on the structure of the user content
Requirements	ERDSs **should** use this component to specify relevant information about the user content, in a binding specific way. In case the payload is accompanied with an application layer identifier, this information should be captured in this component. In case the payload is accompanied with an application layer subject, this information should be captured in this component. Information for this component should be provided by S-ERDS R-ERDS and intermediate ERDS (in the extended model) **shall** propagate this component as received from the previous ERDS in the delivery chain. Information **may** include: • Application layer protocol identifier • Number of parts composing user content • Identifier for each part • Content type for each part • digest for each part ERDS may add further information on the internal structure of the user content, including information on attachments and their digest

6.2.15 MD15 - Other metadata

Further components may be specified in addition to those mentioned above.

7 Digital signatures in ERDS provisioning

7.1 Objects and actors for digital signatures

The following objects may or shall be digitally signed during regular operation of an ERDS:

1) User content may consist of one or more digitally signed documents. Such signatures belong to the application protocol and are out of scope of the present document. An ERDS shall not change user content as this will invalidate digital signatures for the application protocol.

NOTE 1: Signatures on user content will often not be available to the ERDS since the user content can be encrypted end-to-end between sender and receiver.

2) An ERDS shall digitally sign all ERD messages. Such signatures will usually be internal to the ERDS and shall be verified when the ERD message is conveyed to an ERDS-RI interface.. Signature on ERD messages are used for ERDS-to-ERDS non repudiation and integrity and do not need to be validated by end users. The subject generating the digital signature on the ERD message (i.e. the entity named in the corresponding certificate) may be a legal or natural person or some other entity, e.g. a device or logical component.

3) Each evidence shall be digitally signed as an individual document by the ERDS issuing the evidence, even when the evidence is embedded in a signed ERD message. This ensures that an evidence can be extracted from an ERD message if necessary and delivered to sender, receiver or other parties, or be archived, as an individual, protected document. A digital signature on an evidence shall be verifiable by any party; this means that the entire certificate chain supporting the signature shall be available and that certificate status information for these certificates shall be openly available.

4) Messages exchanged with the Common Service Infrastructure may be digitally signed; this may apply to both requests and responses. Requirements may exist for digitally signing metadata stored in a CSI metadata repository and for conveying these metadata in their signed form.

7.2 Common requirements for digital signatures

The following requirements shall apply to all digital signatures applied by ERDSs to ERD messages and ERDS evidence.:

NOTE: Digital signatures exchanged with the Common Services Infrastructure are not affected by these requirements.

5) The digital signature should be a CAdES, XAdES or PAdES baseline signature as specified in ETSI EN 319 122-1, ETSI EN 319 132-1, ETSI EN 319 142-1.

NOTE 1: A XAdES signature can be regarded as the best option for SOAP-based ERD services, while CAdES signatures can be a better alternative in Registered Electronic Mail environments.

NOTE 2: As no part of this specification specifies use of PDF documents, no further requirements are posed for use of PAdES. An example of use is an ERDS that issues PDF-formatted evidences to its subscribers and signs these evidences using PAdES.

6) The digital signature shall use cryptographic algorithms of sufficient strength, e.g. as recommended by ETSI TS 119 312 [21].

7) The digital signature may include a signed property containing the explicit identifier of the signature policy governing the signing and/or validating processes.

8) A signature time-stamp should be added to the digital signature; when a CAdES or XAdES signature is used, the B-T signature level should be used.

NOTE 3: When the digital signature individually signs an ERDS evidence, the incorporation of the signature time-stamp is an indirect time-stamp on the ERDS evidence itself. This time-stamp token supports requirements related to the time-stamping of ERDS evidences that can be defined by different regulatory or legal frameworks; in particular, this can support the requirements on time-stamping defined by the Regulation (EU) No 910/2014 [i.1], Article 44.

8 ERDS evidence set and components

8.1 Introduction

This clause specifies evidence content. Evidences are composed by a set of basic components, which are listed in the table 6 and semantically specified in clause 8.2. When components take values from predefined lists, these values provided in clause 8.3. Clause 8.4 eventually specifies which components are used for different evidences.

Table 6. evidence components

	Component code	**Component name**	Clause
Core components	G01	Evidence identifier	8.2.1
	G02	Evidence version	8.2.2
	G03	Event Identifier	8.2.3
	G04	Reason identifier	8.2.4
	G05	Event Time	8.2.5
	G06	Transaction log information	8.2.6
ERDS provider components	R01	Evidence issuer policy identifier	8.2.7
	R02	Evidence issuer details	8.2.8
	R03	Signature by issuing REM-MD	8.2.9
Identity components	I01	Sender' s identity attributes	8.2.10
	I 02	Sender's identifier	8.2.11
	I03	Recipient's identity attributes	8.2.12
	I04	Recipient's identifier	8.2.13
	I05	Recipient's delegate identity attributes	8.2.14
	I06	Recipient's delegate identifier	8.2.15
	I07	Recipient referred to by the Evidence	8.2.16
	I08	Sender assurance details	8.2.17
	I09	Recipient assurance details	8.2.18
	I10	Recipient’s delegate assurance details	8.2.19
Messaging components	M01	message identifier	8.2.20
	M02	user content information	8.2.21
	M03	Submission date and time	8.2.22
	M04	Forwarded to external system	8.2.23
	M05	Received from external system	8.2.24
	E01	Extensions	8.2.25

8.2 Evidence components

8.2.1 G01 – Evidence identifier

Description	Evidence identifier
Format	text
Meaning	Unique identifier for the evidence, used to keep track of issued REM-MD Evidence, for possible later retrieval
Requirements	

8.2.2 G02 – Evidence version

Description	Evidence version
Format	EN319522.x.y.z.t
Meaning	The version of the evidence, corresponding to the version of the document where it is defined
Requirements	

8.2.3 G03 – Event identifier

Description	Event identifier
Format	URI. A different URI shall be assigned to each event that can trigger the issuance of an evidence.
Meaning	Identifier of the event that has triggered the issuance of the evidence.
Requirements	Events belong to the list of events in [1] clause 6

8.2.4 G04 – Reason identifier

Description	Reason identifier
Format	URI.
Meaning	One identifier identifying one specific reason for the occurrence of the event that triggered the issuance of the evidence.
Requirements	This component shall contain one identifier of reason. This component may also contain additional textual details linked to the reason identifier. Only the identifiers defined in clause 8.3.3 shall be used. This component shall appear within the evidence when this evidence is triggered by a “negative” event (failure to deliver, rejection, etc.). Positive events may include a reason component.

8.2.5 G05 – Event time

Description	Event time
Format	UTC date and time.
Meaning	Date and time when the ERDS provider has generated the evidence.
Requirements	

8.2.6 G06 – Transaction log information

Description	Transaction log information
Format	Dependent of the underlying transport protocol.
Meaning	A log of the transaction, specific to the underlying transport protocol, and related to the event that has triggered the generation of the evidence.
Requirements	This element shall contain one log related to the evidence’s triggering event. The log record and its contents shall be specified by the applicable policy. The inner structure of this log record shall depend on the specific underlying transport protocol.

8.2.7 R01 – Evidence issuer policy identifier

Description	Evidence issuer policy identifier
Format	Each identifier this component shall be either an URI or an OID. If the identifier is an OID, it shall be represented as URN built as specified in RFC 3061 [9]
Meaning	The identifier of one or more policies under which operates the ERDS provider that has issued the evidence this component is member of.
Requirements	This component shall contain one or more identifiers that unambiguously identify the policies under which the ERDS provider that has issued the evidence this component is member of, operates.

8.2.8 R02 – Evidence issuer details

Description	Evidence issuer details
Format	
Meaning	Details of the ERDS provider that has issued the evidence.
Requirements	This component shall meet the semantic requirements defined in clause 5.3 with the details of the ERDS provider that has issued the evidence this component is a member of.

372 8.2.9 R03 – Signature by issuing ERDSP

Description	Signature by issuing ERDSP
Format	
Meaning	The signature generated by the ERDS provider on the evidence.

Requirements

This component shall meet the requirements defined in clause 7 Digital signatures in ERDS provisioning

7.1 Objects and actors for digital signatures

The following objects may or shall be digitally signed during regular operation of an ERDS:

9) User content may consist of one or more digitally signed documents. Such signatures belong to the application protocol and are out of scope of the present document. An ERDS shall not change user content as this will invalidate digital signatures for the application protocol.

NOTE 1: Signatures on user content will often not be available to the ERDS since the user content can be encrypted end-to-end between sender and receiver.

10) An ERDS shall digitally sign all ERD messages. Such signatures will usually be internal to the ERDS and shall be verified when the ERD message is conveyed to an ERDS-RI interface.. Signature on ERD messages are used for ERDS-to-ERDS non repudiation and integrity and do not need to be validated by end users. The subject generating the digital signature on the ERD message (i.e. the entity named in the corresponding certificate) may be a legal or natural person or some other entity, e.g. a device or logical component.

11) Each evidence shall be digitally signed as an individual document by the ERDS issuing the evidence, even when the evidence is embedded in a signed ERD message. This ensures that an evidence can be extracted from an ERD message if necessary and delivered to sender, receiver or other parties, or be archived, as an individual, protected document. A digital signature on an evidence shall be verifiable by any party; this means that the entire certificate chain supporting the signature shall be available and that certificate status information for these certificates shall be openly available.

12) Messages exchanged with the Common Service Infrastructure may be digitally signed; this may apply to both requests and responses. Requirements may exist for digitally signing metadata stored in a CSI metadata repository and for conveying these metadata in their signed form.

7.2 Common requirements for digital signatures

The following requirements shall apply to all digital signatures applied by ERDSs to ERD messages and ERDS evidence.:

NOTE: Digital signatures exchanged with the Common Services Infrastructure are not affected by these requirements.

13) The digital signature should be a CAdES, XAdES or PAdES baseline signature as specified in ETSI EN 319 122-1, ETSI EN 319 132-1, ETSI EN 319 142-1.

NOTE 1: A XAdES signature can be regarded as the best option for SOAP-based ERD services, while CAdES signatures can be a better alternative in Registered Electronic Mail environments.

NOTE 2: As no part of this specification specifies use of PDF documents, no further requirements are posed for use of PAdES. An example of use is an ERDS that issues PDF-formatted evidences to its subscribers and signs these evidences using PAdES.

14) The digital signature shall use cryptographic algorithms of sufficient strength, e.g. as recommended by ETSI TS 119 312 [21].

	15) The digital signature may include a signed property containing the explicit identifier of the signature policy governing the signing and/or validating processes. 16) A signature time-stamp should be added to the digital signature; when a CAdES or XAdES signature is used, the B-T signature level should be used. NOTE 3: When the digital signature individually signs an ERDS evidence, the incorporation of the signature time-stamp is an indirect time-stamp on the ERDS evidence itself. This time-stamp token supports requirements related to the time-stamping of ERDS evidences that can be defined by different regulatory or legal frameworks; in particular, this can support the requirements on time-stamping defined by the Regulation (EU) No 910/2014 [i.1], Article 44. for digital signatures that individually sign an ERDS evidence.

8.2.10 I01 – Sender's identity attributes

Description	Sender's identity attributes.
Format	
Meaning	This component specifies the Sender's identity attributes as defined in the applicable S-ERDS Policy.
Requirements	This is a subset of the identity attributes defined in clause 5.3. No attribute is mandatory.

8.2.11 I02 – Sender's identifier

Description	Sender’s identifier
Format	
Meaning	Identifier of the sender of the user content.
Requirements	This component shall include an identifier of the sender as defined in clause 5.2. Same as MD08 even if the format may differ due to a different binding

8.2.12 I03 – Recipient’s identity attributes

Description	Recipient’s identity attributes.
Format	
Meaning	This component specifies the recipient's identity attributes as defined in the applicable R-ERDS Policy.
Requirements	This is a subset of the identity attributes defined in clause 5.3. No attribute is mandatory.

8.2.13 I04 – Recipient's identifier

Description	Recipient’s identifier.
Format	
Meaning	This component shall include an identifier of the recipient.
Requirements	As defined in clause 5.2. Same as MD10 even if the format may differ due to a different binding

8.2.14 I05 – Recipient’s delegate identity attributes

Description	This component specifies the Recipient’s identity attributes.
Format	
Meaning	In case the R-ERDS provider allows for delegation, this component will be used to provide recipient's delegate identity attributes as defined in the applicable R-ERDS Policy.
Requirements	This is a subset of the identity attributes defined in clause 5. No attribute is mandatory.

8.2.15 I06 – Recipient's delegate identifier

Description	Recipient’s delegate identifier
Format	
Meaning	In case the R-ERDS provider allows for delegation, this component will be used to provide an identifier of the recipient’s delegate.
Requirements	As defined in clause 5.2.

8.2.16 I07 – Recipient referred to by the evidence

Description	Recipient referred to by the evidence
Format	Identifier
Meaning	Identifies the recipient of the user content submitted by the sender the evidence refers to in case there are several intended recipients (each indicated via component I04 specified in clause 8.2.13).
Requirements	When several recipients are defined in the Evidence (several I04 components will be present), this component is used to indicate which of them is the one the Evidence refers to.

8.2.17 I08 – Sender’s identity assurance details

Description	Sender’s identity assurance details
Format	
Meaning	Details of the authentication process conducted by the sender of the payload.
Requirements	This component shall meet the semantic requirements defined in clause 5.5 with the details of the authentication process conducted by the sender of the payload whose processing has resulted in the issuance of the evidence this component is a member of

8.2.18 I09 – Recipient’s identity assurance details

Description	Recipient’s identity assurance details
Format	
Meaning	Details of the authentication process conducted by the intended recipient of the payload.
Requirements	This component shall meet the semantic requirements defined in clause 5.5.

8.2.19 I10 – Recipient’s delegate identity assurance details

Description	Recipient’s delegate identity assurance details
Format	
Meaning	Details of the authentication process conducted by the delegate of the intended recipient of the payload.
Requirements	This component shall meet the semantic requirements defined in clause 5.5

8.2.20 M01 – Message identifier

Description	Message identifier
Format	Binding specific
Meaning	Unique identifier for the ERD message
Requirements	Same as MD11 even if the format may differ due to a different binding.

8.2.21 M02 – User content information

Description	User content information
Format	Binding specific
Meaning	Information on the structure of the original message
Requirements	Same as MD14 even if the format may differ due to a different binding

8.2.22 M03 – Submission date and time

Description	Submission date and time
Format	Date and time
Meaning	The date and time when the sender initiated the delivery process (i.e., time of invocation of SubmitMessage() by UA/Application). It may differ from the time of acceptance/rejection of the user content by the ERDS.
Requirements	The source of the information for this component is the S-ERDS. R-ERDS and intermediate ERDS (in the extended model) **shall** use submit date and time as provided by S-ERDS.

8.2.23 M04 – Forwarded to external system

Description	Forwarded to external system
Format	
Meaning	Indicates that the the user message has been forwarded to a non-ERD service
Requirements	This component shall provide a description, in plain text, of the external system (non ERDS) where the user message, has been forwarded to.

8.2.24 M05 – Received from external system

Description	Received from external system
Format	
Meaning	Indicates that the user message has been received from a non-ERD service.
Requirements	This component shall provide a description, in plain text, of the external system (non ERDS) from which the user content has been received

8.2.25 E01 – Extensions

Description	Extensions
Format	
Meaning	A placeholder for additional components not specified in the present document
Requirements	This component shall be a placeholder for components that are not specified in the present document, but that may be specified elsewhere, including future versions of the present document or specifications produced at national, sectorial, or private-basis.

8.3 Evidence components values

Evidence Data Elements are elementary pieces of information used to make up the Evidence Components.

8.3.1 Free text

Information in free text **shall** be written in UK English. Text in other languages **may** be added.

8.3.2 Events

The G02 – Event identifier field should contain the one of the values from [1], clause 6.1, Table 1, column “Event”.

8.3.3 Reasons

8.3.3.1 Reasons related to Events A.1, A.2 (Sender's submission)

Table 7. reasons for events A.1, A.2

Reason
Message accepted
Invalid message format
Malware found in ERD original message
Sender's signing certificate expired or revoked
Sender's ERDS provider’s policy violation, e.g.: max message size exceeded, invalid attachment formats, etc.
Other

8.3.3.2 Reasons related to the Events B.1, B.2, B3 (Relay between ERDSs)

Table 8. reasons for events B.1, B.2. B.3

Reason
ERD message successfully relayed to the Recipient's ERDSP
ERD message successfully relayed to, but rejected by, the Recipient's ERDSP for: Invalid message format
ERD message successfully relayed to, but rejected by, the Recipient's ERDSP for: Malware found in ERD message
ERD message successfully relayed to, but rejected by, the Recipient's ERDSP for: Invalid ERDS signature format or signature policy violation
ERD message successfully relayed to, but rejected by, the Recipient's ERDSP for: ERDS signing certificate in the signature of ERD message or ERD evidence expired or revoked
ERD message successfully relayed to, but rejected by, the Recipient's ERDSP for: Recipient's ERDSP policy or ERDSP policy violation, e.g.: max message size exceeded, invalid attachment formats, relaying ERDSP not accepted
ERD message not relayed to the Recipient's ERDSP for: Recipient's ERDSP malfunction
ERD message not relayed to the Recipient's ERDSP for: Recipient's ERDSP not identified in the Internet
ERD message not relayed to the Recipient's ERDSP for: Recipient's ERDSP unreachable
ERD message not relayed to the Recipient's ERDSP for: Unknown Recipient
Other

8.3.3.3 Reasons related to events C.1, C.2, C.3, C.4, C.5 (acceptance/rejection by the recipient)

Table 9. reasons for events C.1, C.2, C.3, C.4, C.5

Reason
Notification for acceptance sent to recipient
Subsequent notification for acceptance sent to recipient after no response to previous notificatoins
Error in delivering notification for acceptance to recipient
Error in delivering subsequent notification for acceptance to recipient
Error in delivering notification for acceptance to recipient after multiple attempts
Error in delivering subsequent notification for acceptance to recipient after multiple attempts
Message accepted by the recipient
Message explicitly rejected by the recipient
Message not accepted by the recipient after a defined time period from firsts successful notification
Other

8.3.3.4 Reasons related to events D.1, D.2, D.3, D.4 (consignment to the recipient)

Table 10. reasons for events D.1, D.2, D.3, D.4

Reason
message successfully consignedto the recipient
message successfully consigned to a recipient's delegate
The sender's ERDSP received within a given period no information on consignment from the recipient's ERDSP
Not consigned for excessing recipient quota
Not consigned for technical malfunction
Not consigned for message type not accepted by recipient
Other

8.3.3.5 Reasons related to events E.1, E.2 (Handover to the recipient)

Table 11. reasons for events E.1, E.2

Reason
message successfully handed over to the recipient
message successfully handed over to a recipient's delegate
Not handed over for message type not accepted by recipient
Message handover failed after specific time period
Other

8.3.3.6 Reasons related to events F1, F2 (connection to non ERDS)

Table 12. reasons for events F.1, F.2

Reason
Successful relay to non ERDS
external system unreachable
external system rejected submission (see note)
Received from non ERDS
Other

8.4 Requirements for components of evidence

Table 133, within this clause show the presence, cardinality and additional requirements and notes that apply to the different components in all the evidence set specified in [1] clause 6. Below follows a detailed explanation of their meanings and contents:

1) the first row contains the set of events on which an evidence may me issued [1]

2) The first column contains the set of evidence components listed in clause 8.2

3) Each cell within the table contains the cardinality requirements that apply to the component identified by the row, for the evidence associated to the event identified by the column.

4) The cardinality requirements are expressed in the following form:

    - **0:** The evidence associated to the event identified by the column shall not incorporate any the component identified by the row.

    - **1:** The evidence associated to the event identified by the column shall incorporate exactly one instance of the component identified by the row.

    - **0..1:** The evidence associated to the event identified by the column shall incorporate zero or one instance of the component identified by the row.

    - ***:** The evidence associated to the event identified by the column shall incorporate zero or more instances of the component identified by the row”.

- **1..*:** The evidence associated to the event identified by the column shall incorporate one or more instances of the component identified by the row.

Table 13. Requirements on presence and cardinality of components in different evidence.

event component	Submission Acceptance	Submission Rejecttion	RelayAcceptance	RelayRejection	RelayFailure	NotificationForAcceptanc	NotificationForAcceptanc	Consignment Acceptance	Consignment Rejection	AcceptanceRejectionExpir	ContentConsignment	ContentConsignmentFailu	Consignment Notification	Consignment NotificationF	ContentHandover	ContentHandoverFailure	RelayToNonERDS	RelayToNonERDSFailure	ReceivedFromNonERDS
G01 Evidence version	1	1	1	1	1	1	1	1	1	1	1	1	**1**	**1**	1	1	1	1	1
G02 Event identifier	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
G03 Reason identifiers	0..1	*	0..1	*	*	0..1	*	0..1	*	*	0..1	*	0..1	*	0..1	*	0..1	*	0..1
G04 Event time	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
G05 Transaction information log	* (b)	* (b)	* (b)	* (b)	* (b)	* (b)	* (b)	* (b)	* (b)	* (b)	* (b)	* (b)	* (b)	* (b)	* (b)	* (b)	* (b)	* (b)	* (b)
R01 Evidence issuer policy Identifier	1..*	1..*	1..*	1..*	1..*	1..*	1..*	1..*	1..*	1..*	1..*	1..*	1..*	1..*	1..*	1..*	1..*	1..*	1..*
R02 Evidence issuer details	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
R03 Signature	0..1	0..1	0..1	0..1	0..1	0..1	0..1	0..1	0..1	0..1	0..1	0..1	0..1	0..1	0..1	0..1	0..1	0..1	0..1
I01 Sender’s identity attributes	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0..1
I02 Sender’s identifier	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0..1
I03 Recipient’s identity attributes	1..*	1..*	1..*	1..*	1..*	1..*	1..*	1..*	1..*	1..*	1..*	1..*	1..*	1..*	1..*	1..*	1..*	1..*	1..*
I04 Recipient’s identifier	1..*	1..*	1..*	1..*	1..*	1..*	1..*	1..*	1..*	1..*	1..*	1..*	1..*	1..*	1..*	1..*	1..*	1..*	1..*
I05 Recipient’s del. identity attributes	0	0	0	0	0	0..1	0..1	0..1	0..1	0..1	0..1	0..1	0..1	0..1	0..1	0..1	0	0	0
I06 Recipient’s delegate identifier	0	0	0	0	0	0..1	0..1	0..1	0..1	0..1	0..1	0..1	0..1	0..1	0..1	0..1	0	0	0
I07 Recipient ref. to by the evidence	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0
I08 Sender’s identity assurance details	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
I09 Recipient’s identity ass. details	0	0	0	0	0	0	0	0..1	0..1	0	0	0	0..1	0	0..1	0..1	0	0	0
I10 Recipient’s del. identity ass. details	0	0	0	0	0	0	0	0..1	0..1	0	0	0	0..1	0	0..1	0..1	0	0	0
M01 Message identifier	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
M02 User content information	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
M03 Submission date and time	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
M04 Forwarded to external system	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0..1	0..1	0
M05 Received from external system	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0..1
E01 Extensions	0..1	0..1	0..1	0..1	0..1	0..1	0..1	0..1	0..1	0..1	0..1	0..1	0..1	0..1	0..1	0..1	0..1	0..1	0..1

NOTE (b): If more Policies are to be complied with, each requiring a specific log content and format, multiple instances of component G06 Transaction log information are possible

9 Common Services Interface content

9.1 Introduction

The CSI component is needed when sender and recipient(s) are served by different ERDSs. As identified by part 1 of this specification, this component for the 4-corner model and the extended model may have four purposes:

1. Message routing,
2. Trust establishment,
3. Capability management,
4. Governance support.

These purposes are described below, with trust establishment and governance in the same clause.

9.2 ERD message routing

By use of the CSI component, an S-ERDS shall be able to identify the R-ERDS of which the recipient is a subscriber, see clause 9.4.2. When the S-ERDS and the R-ERDS are directly connected, e.g. in the 4-corner model, the ERDS RI interface between the two ERDSs shall be identified, in order for the S-ERDS to route ERD messages to the R-ERDS; correspondingly for evidences between the two ERDSs. The format of the ERDS RI identification depends on technology; as one example, a URI format may be used.

Multi-hop routing of an ERD message or evidence via a path consisting of one or more I-ERDSs is out of scope of this specification.

NOTE 1: One possibility is to configure multi-hop routing locally at the S-ERDS based on knowledge of the topography of the interconnection of ERDSs.

NOTE 2: An example of a topography is the situation where all ERDSs are connected to one I-ERDS that provides an interconnecting infrastructure. The S-ERDS will forward to the ERDS RI interface to the interconnecting I-ERDS, which in turn will forward to the ERDS RI interface to the R-ERDS.

Before forwarding the ERD message, the S-ERDS shall establish trust in the ERDS it is forwarding to (see clause 9.3), should obtain the full path to that ERDS, and shall assess that the ERDS has the capabilities necessary (see clause 9.4) to fulfil the S-ERDS' policy for the ERD message.

9.3 ERDS trust establishment and governance

When an ERD message needs forwarding to another ERDS, trust in the other ERDS shall be evaluated. An ERDS shall not relay an ERD message to another ERDS, unless it can identify and authenticate the other ERDS and can confirm that the identified ERDS is trusted.

Trust is defined as the existence of a trust domain within which co-operation between participating ERDSs is regulated. The specific conditions (policies) for a trust domain may vary; this specification has no requirements on how a trust domain is established or governed. Typically, parameters such as responsibilities, possibilities for claiming recourse in case of breaches, and payment are defined for a trust domain.

A trust domain shall have governance, at least for the policy regarding conditions for an ERDS to join.

A trust domain may be established bilaterally between two or more ERDSs; in this case the governance should be through explicit or implicit agreements.

A trust domain may require specific policy, security, and technical conditions to be met by all participating ERDSs. If this is the case, the capabilities of the participating ERDSs may be implicit from the participation in the trust domain. In other cases, both trust in and capabilities (metadata) of the other ERDS shall be assessed.

Trust may be established unilaterally, meaning an ERDS trust another ERDS but not the other way around, or an ERDS trust participants of a trust domain of which the ERDS itself is not a participant. This implies that ERD messages can be sent in one direction (if the ERDS and/or trust domain policy accepts receiving from outside), but not in the opposite direction. If such one-way sending of ERD messages is used, the R-ERDS shall provide evidences to the S-ERDS.

Participation in a trust domain should be assessed by an X.509 certificate representing an ERDS in the trust domain. By use of this certificate, or certificates derived from it, ERDSs can be authenticated towards one another, and ERD messages and evidences can be signed and encrypted between ERDSs.

Information about ERDSs participating in specific trust domains may be found by the following means:

- Locally configured by exchange of information, including certificates, between the involved ERDSs.
- Maintaining a trust domain Trust Status List (TSL), typically a responsibility of an actor co-ordinating the trust domain, termed the “scheme operator” by ETSI TS 119 612 [22]. An X.509 certificate represents the “service digital identity” of the ERDS in the TSL
- As a special case of TSL, the EUMS TL system will list qualified ERDSs; and the trust domain may be defined as "all qualified ERDSs".
- The trust domain may be defined by a domain PKI issuing X.509 certificates to all participating ERDSs.
- Metadata on capabilities of an ERDS may be extended to contain trust domain information; this is out of scope of this specification.

9.4 Capability management

9.4.1 Introduction

Capability management shall provide the functionality to resolve the unique identification of a recipient into:

1. Identification of the R-ERDS of which the recipient is a subscriber,
2. Metadata for the capabilities of this ERDS,
3. Metadata for the capabilities of the recipient in this ERDS.

A recipient may be a subscriber of several ERDSs, in which case the unique identification of the recipient shall either include identification of the ERDS (see clause 9.4.2 item 1) or further information such as application protocol or message type identification that through lookup in recipient metadata will identify the ERDS that serves the recipient for this ERD message.

NOTE: An example is a business actor (typically a legal person) that uses the services of one ERDS for procurement orders and another ERDS for invoices.

9.4.2 Resolving recipient identification to ERDS identification

The R-ERDS may be explicitly identified by the identifier of the recipient, e.g. when this is on an email format recieverID@ERDS.domain. When the identification of the recipient is by other means than an identifier, identification of the ERDS may be explicit by a separate parameter (in sender metadata).

However, a recipient may also be uniquely identified by an identifier (scheme name and value, see clause 5.2) that is not bound to identification of the R-ERDS, or by a set of identity attributes that together provide unique identification, see clause 5.3, and without identification of R-ERDS as separate parameter; e.g. the sender may not know which ERDS that serves the recipient. In this case, either:

1. The S-ERDS may be able to locally decide the identity of the R-ERDS, e.g. based on identifier scheme name or specific identity attributes like country, or
2. The R-ERDS may be identified through lookup in recipient metadata; as stated above, further parameters in sender metadata may be used in the identification of the R-ERDS.

9.4.3 Recipient metadata

The capabilities of a recipient may be implicit from the ERDS metadata; the conditions for becoming a subscriber of an ERDS may require all subscribers to fulfil certain requirements.

In other cases, recipient metadata shall be available for the S-ERDS to determine if an ERD message can be forwarded to this recipient or not. This specification does not assume that metadata for all recipients is in the same place. When recipient metadata is used, the CSI shall provide functionality to derive a unique address for the recipient's metadata, e.g. a URI, from the recipient identification.

Recipient metadata repositories may be organised in different manners:

1. One metadata repository may be provided for an ERDS; when the ERDS is identified, all metadata for its subscribers will be in one place.
2. Several metadata repositories may be provided for one ERDS, e.g. when the ERDS is provided by several ERDSPs.
3. One metadata repository may span several ERDSs.
4. Recipients may be allowed to manage their own metadata repositories, mostly relevant for legal persons.

When recipient metadata is used in the ERDS provisioning, an ERDSP shall ensure that sufficient metadata about all subscribers is stored, maintained, and made available.

Depending on the identification of the recipient and the technology used for the ERDS, different organisations of metadata repositories can be used, as well as different mechanisms to locate and access the recipient metadata. No requirements are posed here but specifications for specific ERDS technologies may pose requirements.

The content of recipient metadata depends on the specific ERDS technologies used. No requirements are posed here but specifications for specific ERDS technologies may pose requirements.

9.4.4 ERDS capability metadata

An ERDS shall not relay an ERD message to another ERDS unless it can assess that the other ERDS can provide a service respecting the constraints and options defined in the applicable ERD policy.

The assessment may be based on both ERDSs participating in the same trust domain (see clause 9.3) if the trust domain policy ensures that all participating ERDSs have the same capabilities.

In other cases, a decision on forwarding of an ERD message depends on evaluation of capabilities (metadata) about the other ERDS. If ERDS metadata is needed, an ERDSP shall ensure that capability metadata for the ERDS is stored, maintained, and made available. Two alternatives exist:

1. The CSI shall provide functionality to derive a unique address for the ERDS metadata repository, e.g. a URI, from the ERDS identification, or
2. ERDS metadata shall be stored as part of recipient metadata, meaning a lookup on recipient metadata returns information also on the ERDS.

This specification defines metadata on capabilities of an ERDS according to the table below:

Table 14. capability metadata

ERDS identification	Scheme and identifier, see clause 5.2
ERDS domain name	Domain name of ERDS for DNS lookup etc.
ERDS governing body	Identification of the ERDSP providing the ERDS, or – if the ERDS is provided by several co-operating ERDSPs – of the governing organisation. Legal person identity as per clause 5.3.2, alternatively natural person identity as per clause 5.3.1.
Protocol/profile/binding	Alternatives as per ETSI EN 319 522-4 and indication of REM/not REM. List of metadata types supported as per clause 6.2.
[optional] Metadata repository	URL of repository for recipient metadata.
[optional] Trust domains	Information on the trust domains (see 9.4) where the ERDS is a member: a) EU Qualified indicator (EU TL system referenced) b) URL for location of domain TSL

	c) Root-certificate for domain PKI
ERDS capabilities	Shall include the following: a) Support for the “expiry date and time” feature: Yes/no flag, see clause 6.2.3. b) Authentication LoAs supported: List of LoA levels by scheme and level identifier, see clause 6.2.4. c) [Optional] ERD policy support: List of identifiers (OID or URI) of supported ERD policies, see clause 6.2.5. d) Supported mode of consignment: See clause 6.2.6. e) Support of scheduled delivery: Yes/no flag, see clause 6.2.7.

History

Document history		
0.0.1	03/2017	V0.0.1 for ESI comments
0.0.2	06/2017	V0.0.2 for ESI comments
0.0.3	09/2017	V0.0.3 stable draft for ESI
0.0.4	10/2017	V0.0.4 for public comment