

Draft **ETSI EN 319 522-2** V1.2.0 (2023-10)



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

Reference

REN/ESI-0019522-2v121

Keywordse-delivery services, registered e-delivery services,
registered electronic mail**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 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Important notice

The present document can be downloaded from:

<https://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 prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

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/CommitteeSupportStaff.aspx>

If you find a security vulnerability in the present document, please report it through our
Coordinated Vulnerability Disclosure Program:

<https://www.etsi.org/standards/coordinated-vulnerability-disclosure>

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.

No recommendation as to products and services or vendors is made or should be implied.

In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.

The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2023.
All rights reserved.

Contents

Intellectual Property Rights	5
Foreword.....	5
Modal verbs terminology.....	5
1 Scope	6
2 References	6
2.1 Normative references	6
2.2 Informative references.....	6
3 Definition of terms, symbols and abbreviations.....	7
3.1 Terms.....	7
3.2 Symbols.....	7
3.3 Abbreviations	7
4 Overview	7
5 Identification of actors.....	10
5.1 Introduction	10
5.2 Identifiers	10
5.3 Identity attributes.....	10
5.3.1 Introduction.....	10
5.3.2 Identity attributes of natural persons.....	10
5.3.3 Identity attributes of legal person	10
5.3.4 Identity attributes of other entities	10
5.4 Identity verification and authentication assurance levels information	11
6 ERDS relay metadata	11
6.1 Introduction	11
6.2 Metadata components.....	12
6.2.1 MD01 - Metadata version	12
6.2.2 MD02 - Relay date and time	12
6.2.3 MD03 - Expiry date and time	12
6.2.4 MD04 - Recipient required level of assurance.....	12
6.2.5 MD05 - Applicable policy	13
6.2.6 MD06 - Mode of consignment.....	13
6.2.7 MD07 - Scheduled delivery	13
6.2.8 MD08 - Sender's identifier.....	14
6.2.9 MD09 - Reply-to.....	14
6.2.10 MD10 - Recipient's identifier	14
6.2.11 MD11 - Message identifier	14
6.2.12 MD12 - In reply to.....	14
6.2.13 MD13 - Message type.....	14
6.2.14 MD14 - User content information.....	15
6.2.15 MD15 - Other metadata	15
7 Digital signatures in ERDS provisioning	15
7.1 Objects and actors for digital signatures.....	15
7.2 Common requirements for digital signatures	15
8 ERDS evidence set and components	16
8.1 Introduction	16
8.2 Evidence components.....	17
8.2.1 G01 - Evidence identifier.....	17
8.2.2 G02 - Evidence version.....	17
8.2.3 G03 - Event identifier	17
8.2.4 G04 - Reason identifier.....	18
8.2.5 G05 - Event time.....	18
8.2.6 G06 - Transaction log information	18
8.2.7 R01 - Evidence issuer policy identifier.....	18

8.2.8	R02 - Evidence issuer details.....	18
8.2.9	R03 - Signature by issuing ERDS.....	19
8.2.10	I01 - Sender's identity attributes	19
8.2.11	I02 - Sender's identifier.....	19
8.2.12	I03 - Sender's delegate identity attributes	19
8.2.13	I04 - Sender's delegate identifier.....	20
8.2.14	I05 - Recipient's identity attributes	20
8.2.15	I06 - Recipient's identifier.....	20
8.2.16	I07 - Recipient's delegate identity attributes	20
8.2.17	I08 - Recipient's delegate identifier	21
8.2.18	I09 - Recipient referred to by the Evidence	21
8.2.19	I10 - Sender's identity assurance level details.....	21
8.2.20	I11 - Sender's delegate identity assurance level details	21
8.2.21	I12 - Recipient's identity assurance level details	22
8.2.22	I13 - Recipient's delegate identity assurance level details	22
8.2.23	M01 - Message identifier.....	22
8.2.24	M02 - User content information	22
8.2.25	M03 - Submission date and time	22
8.2.26	M04 - External system.....	23
8.2.27	M05 - External ERDS.....	23
8.2.28	E01 - Extensions	23
8.3	Evidence components values.....	23
8.3.1	Free text	23
8.3.2	Events	23
8.3.3	Reasons	24
8.3.3.1	Reasons related to Events A.x (Sender's submission).....	24
8.3.3.2	Reasons related to the Events B.x (Relay between ERDSs)	25
8.3.3.3	Reasons related to events C.x (Acceptance/rejection by the recipient).....	25
8.3.3.4	Reasons related to events D.x (Consignment to the recipient).....	27
8.3.3.5	Reasons related to events E.x (Handover to the recipient).....	27
8.3.3.6	Reasons related to events F.x (Connection to non ERDS).....	28
8.4	Additional requirements for components of evidence.....	29
9	Common Services Interface content.....	31
9.1	Introduction	31
9.2	ERD message routing.....	31
9.3	ERDS trust establishment and governance.....	31
9.4	Capability management.....	32
9.4.1	Introduction.....	32
9.4.2	Resolving recipient identification to ERDS identification.....	32
9.4.3	Recipient metadata.....	33
9.4.4	ERDS capability metadata.....	33
Annex A (informative): Change History		35
History		36

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are 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 Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, 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.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM®** and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This draft European Standard (EN) has been produced by ETSI Technical Committee Electronic Signatures and Infrastructures (ESI), and is now submitted 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 part 1 [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 services which are specified in ETSI EN 319 522-1 [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".
- [2] [IETF RFC 3061](#): "A URN Namespace of Object Identifiers".
- [3] [Core Person Vocabulary v2.0](#).
- [4] [Registered Organizations Vocabulary v2.0](#).
- [5] [CEF eIDAS Technical Sub-group](#): "eIDAS SAML Attribute profile", Version 1.2. August 2019.

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](#) 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.
- [i.2] Void.
- [i.3] IETF RFC 4122: "A Universally Unique IDentifier (UUID) URN Namespace".
- [i.4] IETF RFC 5322: "Internet Message Format".
- [i.5] ETSI TS 119 312: "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites".
- [i.6] ETSI TS 119 612: "Electronic Signatures and Infrastructures (ESI); Trusted Lists".
- [i.7] ETSI EN 319 522-3: "Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 3: Formats".

- [i.8] ETSI EN 319 522-4-1: "Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 4: Bindings; Sub-part 1: Message delivery bindings".
- [i.9] ETSI EN 319 522-4-2: "Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 4: Bindings; Sub-part 2: evidence and identification bindings".
- [i.10] Void.
- [i.11] ETSI EN 319 122-1: "Electronic Signatures and Infrastructures (ESI); CAAdES digital signatures; Part 1: Building blocks and CAAdES baseline signatures".
- [i.12] ETSI EN 319 132-1: "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures".
- [i.13] ETSI EN 319 142-1: "Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in ETSI EN 319 522-1 [1] and the following apply:

ERD dispatch: ERD message which contains the user content, some ERDS relay metadata and ERDS evidence

ERD payload: ERD message which contains the user content and some ERDS relay metadata

ERDS receipt: ERD message which contains ERDS evidence and some ERDS relay metadata

ERDS serviceinfo: ERD message which contains some ERDS relay metadata

3.2 Symbols

Void.

3.3 Abbreviations

Void.

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 [i.7].

Figure 1 outlines how data flows through the interfaces in the 4-corner model. User content shall not be changed by ERDSs. Data flowing between systems is always encrypted, as specified by the applicable binding. As detailed below, not all objects are always required.

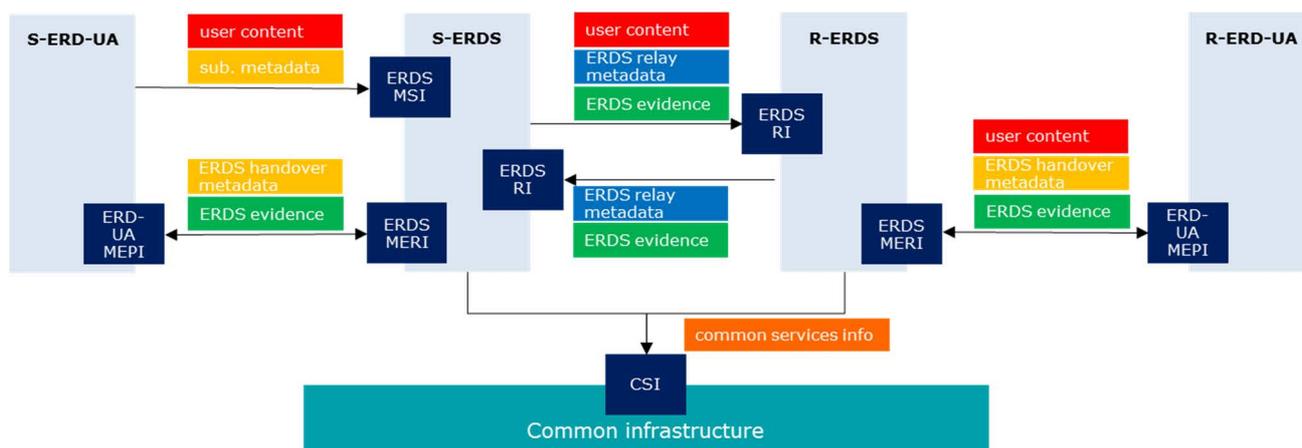


Figure 1: Data flowing through interfaces

For convenience, the present document defines (table 1) some aggregate constructs (ERD dispatch, ERDS receipt, ERDS serviceInfo, ERD payload, original message) which package the basic objects (user content, ERDS relay metadata, ERDS evidence, submission metadata) in different modes. Constructs define the semantic information flowing between parties, so they ease the definition of bindings [3] and [4], even if, specific bindings may split the construct in its basic objects for transport.

The naming convention used in the present 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". Table 1 specifies the composition of constructs as a collection of basic objects.

Table 1: Composition of constructs

Construct		Basic object	user content	ERDS relay metadata	ERDS evidence	submission metadata
ERD message	ERD dispatch		1	1	1..n	0
	ERDS receipt		0	1	1..n	0
	ERDS serviceInfo		0	1	0	0
	ERD payload		1	1	0	0
	original message		1	0	0	0..1

NOTE: ERDS receipt (which contains ERDS relay metadata and also ERDS evidence) and ERDS serviceInfo (which only contains ERDS relay metadata) may play the role of notifications in those cases where this feature is required, and in such cases the recipient can be informed of this role by some metadata or other element.

Table 2 provides an abstract specification of the functions provided by the ERDS APIs as defined in ETSI EN 319 522-1 [1].

Table 2: Abstract interfaces

Interface	Provided function	Description	Arguments and output
ERDS MSI	out := SubmitMessage(og)	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 sender is the owner of the sender's identifier (via an authentication token, a challenge response, etc.).	og: original message, composed of user content and (optional) submission metadata. out: the outcome of the method. There is no specification on the outcome, which may be a simple success/error indication, or may include a message identifier or a larger set of information.
ERDS MERI	out :=RetrieveMessage (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 RetrieveMessageAPI, the UA/Application has to prove that the recipient is the owner of the 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 method, which, in case of success, includes the user content and possibly handover metadata and ERDS evidence. In case of failure the outcome will include error information.
	e := GetEvidences(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 RetrieveMessage).	ei: this is a set of parameters which is used for the identification and retrieval of the requested evidence. e: the requested evidences.
ERD-UA MEPI	out := HandoverObjects(o)	The method is used for handing over user content, ERDS evidence, handover metadata to the ERD-UA.	o: a combination of user content [0..1], ERDS evidence [0..n], handover metadata [0..1], excluding void. out: this is the outcome of the method, which is a success/failure indication plus error information in case of failure.
ERDS RI	out := Relay(em)	The method is used for relaying an ERD message to a different ERDS. Relaying is used when S-ERDS has not the capability to deliver to the recipient itself. Metadata and evidences may be transmitted with the user content or independently from the user content through this method.	em: ERD message. out: this is the outcome of the method, 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:= LookupERDS(ri)	This method is used to identify the ERDS which has the capability to deliver to a defined recipient. The method may return more than one ERDS.	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, etc.). re: one or more endpoints of the ERDS(s) which has(have) the capability to deliver to the recipient identified by ri.
	out := ValidateERDS(ei, p)	This method may be used to validate the inclusion of an ERDS into a trust circle. The method may receive some parameters for the validation (e.g. date and time of validity, specific trust circle, etc.).	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 := GetERDSMetadata (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 information for Common Service Interface.

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. The identifier shall be unique within the network of interoperating ERDSs.

5.3 Identity attributes

5.3.1 Introduction

All attributes in the present document related to identification and authentication are derived from the EU Vocabulary. For natural persons, the attributes defined by the Core Person Vocabulary [3] shall be used, for legal persons, the attributes defined by the Registered Organization Vocabulary [4] shall be used. 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, the present document limits the supported attributes to the ones defined in the eIDAS attribute profile specification [5], which are also attributes derived from the ISA vocabulary.

5.3.2 Identity attributes of natural persons

For legal persons, a non empty subset of the identity attributes identified in [5], clause 2.3.1 shall be used.

Table 3: Void.

5.3.3 Identity attributes of legal person

For natural persons, a non empty subset of the identity attributes identified in [5], clause 2.2.1 shall be used.

Table 4: Void.

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 the present document.

5.4 Identity verification and authentication assurance levels 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. This information shall include:

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

Furthermore, the identity assurance information may include an attribute containing details of the performed authentication, either an assertion generated by an assertion provider or as a sequence of components, consisting of:

- 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. 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 ETSI EN 319 522-4-1 [i.8] and ETSI EN 319 522-4-2 [i.9].

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. ERDS relay metadata shall include metadata components as indicated in the Cardinality column of table 5.

Table 5: Relay metadata components

	Component code	Component name	Cardinality	Ref.
Delivery constraints	MD01	Metadata version	1	6.2.1
	MD02	Relay date and time	0-1	6.2.2
	MD03	Expiry date and time	0-1	6.2.3
	MD04	Recipient required level of assurance	0-1	6.2.4
	MD05	Applicable policy	0-n	6.2.5
	MD06	Mode of consignment	0-1	6.2.6
	MD07	Scheduled delivery	0-1	6.2.7
Sender/	MD08	Sender's identifier	1	6.2.8

Recipient	MD09	Reply-to	0-1	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

6.2 Metadata components

6.2.1 MD01 - Metadata version

Description	Metadata version
Format	Binding specific
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 in UTC values
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 in UTC values
Meaning	The date-time by which the consignment or handover to recipient is required to be completed.
Requirements	R-ERDS shall 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. 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 shall 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 shall not deliver the user content if it cannot meet the required identification LoA specified by this component. 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	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 IETF RFC 3061 [2].
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. As an example, the policy may require the evidence of relay to be returned to the sending ERDS, or that the message is not delivered to a delegate.
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 shall 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 shall refuse the ERD message if it cannot support the policy specified by this component. 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: <ul style="list-style-type: none"> • 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 user 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 shall 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 consignment 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. 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 in UTC values
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. 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	Sender'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 clause 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. 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 IETF RFC 4122 [i.3], or an UID as defined in IETF RFC 5322 [i.4]).
Requirements	The content of this component is provided by the S-ERDS. 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. 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 shall use this component to specify the type of the ERD message (ERD payload, ERD dispatch, ERDS serviceInfo, 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	<p>ERDSs should use this component to specify relevant information about the user content, in a binding specific way.</p> <p>In case the payload is accompanied with an application layer identifier, this information should be captured in this component.</p> <p>In case the payload is accompanied with an application layer subject, this information should be captured in this component.</p> <p>Information for this component should be provided by S-ERDS.</p> <p>Intermediate ERDS (in the extended model) shall propagate this component as received from the previous ERDS in the delivery chain.</p> <p>Information may include:</p> <ul style="list-style-type: none"> • Application layer protocol identifier • Number of parts composing user content • Identifier for each part • Content type for each part • Digest for each part <p>ERDS may add further information on the internal structure of the user content, including information on attachments and their digest.</p>

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

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.

NOTE: 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.

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.

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.

Messages exchanged with the Common Service Interface 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

For all digital signatures applied by ERDSs to ERD messages and ERDS evidence:

NOTE 1: Digital signatures exchanged with the Common Services Infrastructure are not affected by these requirements.

- 1) The digital signature should be a CAAdES, XAdES or PAdES baseline signature as specified in ETSI EN 319 122-1 [i.11], ETSI EN 319 132-1 [i.12], ETSI EN 319 142-1 [i.13].

NOTE 2: A XAdES signature can be regarded as the best option for SOAP-based ERD services, while CAAdES signatures can be a better alternative in Registered Electronic Mail environments.

NOTE 3: As no part of this multi-part deliverable 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.

- 2) The digital signature shall use cryptographic algorithms of sufficient strength, e.g. as recommended by ETSI TS 119 312 [i.5].
- 3) The digital signature may include a signed property containing the explicit identifier of the signature policy governing the signing and/or validating processes.
- 4) A signature time-stamp should be added to the digital signature of evidence; when a CAAdES or XAdES signature is used, the B-T signature level should be used.

NOTE 4: 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 table 6 and semantically specified in clause 8.2. When components take values from predefined lists, these values are 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 ERDS	8.2.9
Identity components	I01	Sender's identity attributes	8.2.10
	I02	Sender's identifier	8.2.11
	I03	Sender's delegate identity attributes	8.2.12
	I04	Sender's delegate identifier	8.2.13
	I05	Recipient's identity attributes	8.2.14
	I06	Recipient's identifier	8.2.15
	I07	Recipient's delegate identity attributes	8.2.16
	I08	Recipient's delegate identifier	8.2.17
	I09	Recipient referred to by the evidence	8.2.18
	I10	Sender assurance level details	8.2.19
	I11	Sender's delegate assurance level details	8.2.20
	I12	Recipient assurance level details	8.2.21
	I13	Recipient's delegate assurance level details	8.2.22
Messaging components	M01	Message identifier	8.2.23
	M02	User content information	8.2.24
	M03	Submission date and time	8.2.25
	M04	External system	8.2.26
	M05	External ERDS	8.2.27
	E01	Extensions	8.2.28

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 ERDS Evidence, for possible later retrieval.
Requirements	

8.2.2 G02 - Evidence version

Description	Evidence version
Format	Binding specific
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 shall belong to the list of events in ETSI EN 319 522-1 [1], clause 6.

8.2.4 G04 - Reason identifier

Description	Reason identifier
Format	Enumeration
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.). This component may appear within the evidence when this evidence is triggered by a "positive" event.

8.2.5 G05 - Event time

Description	Event time
Format	date and time in UTC values
Meaning	Date and time of the event (or its best possible approximation according to the information available to the ERDS).
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 included in this component shall be either a URI or an OID. If the identifier is an OID, it shall be represented as URN built as specified in IETF RFC 3061 [2].
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.

8.2.9 R03 - Signature by issuing ERDS

Description	Signature by issuing ERDSP
Format	
Meaning	The signature generated by the ERDS on the evidence.
Requirements	This component shall meet the requirements defined in clause 7.2 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 shall be a set of one or more of the identity attributes defined in clause 5.3. The source of the information for this component is the S-ERDS. R-ERDS and intermediate ERDS (in the extended model) shall use sender's identity attributes as provided in an available ERDS evidence or ERDS relay metadata generated by S-ERDS if they want to include this component in the ERDS evidence they produce. If such information is not available to the R-ERDS or intermediate ERDS, this component shall not be present in the evidence they produce.

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. The source of the information for this component is the S-ERDS. R-ERDS and intermediate ERDS (in the extended model) shall use sender's identifier as provided in an available ERDS evidence or ERDS relay metadata generated by S-ERDS if they want to include this component in the ERDS evidence they produce.

8.2.12 I03 - Sender's delegate identity attributes

Description	This component specifies the sender's delegate identity attributes
Format	
Meaning	In case the S-ERDS provider allows for delegation, this component will be used to provide sender's delegate identity attributes as defined in the applicable S-ERDS Policy.
Requirements	This shall be a set of one or more of the identity attributes defined in clause 5.3. The source of the information for this component is the S-ERDS. R-ERDS and intermediate ERDS (in the extended model) shall use sender's delegate identity attributes as provided in an available ERDS evidence generated by S-ERDS if they want to include this component in the ERDS evidence they produce. If such information is not available to the R-ERDS or intermediate ERDS, this component shall not be present in the ERDS evidence they produce.

8.2.13 I04 - Sender's delegate identifier

Description	Sender's delegate identifier
Format	
Meaning	In case the S-ERDS provider allows for delegation, this component will be used to provide an identifier of the sender's delegate.
Requirements	As defined in clause 5.2. The source of the information for this component is the S-ERDS. R-ERDS and intermediate ERDS (in the extended model) shall use sender's delegate identifier as provided in an available ERDS evidence generated by S-ERDS if they want to include this component in the ERDS evidence they produce. If such information is not available to the R-ERDS or intermediate ERDS, this component shall not be present in the ERDS evidence they produce.

8.2.14 I05 - 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 shall be a set of one or more of the identity attributes defined in clause 5.3. The source of the information for this component is the R-ERDS. S-ERDS and intermediate ERDS (in the extended model) shall use recipient's identity attributes as provided in an available ERDS evidence generated by R-ERDS if they want to include this component in the ERDS evidence they produce. If such an evidence is not available to the R-ERDS or intermediate ERDS, this component shall not be present in the ERDS evidence they produce.

8.2.15 I06 - 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. The source of the information for this component is the S-ERDS. R-ERDS and intermediate ERDS (in the extended model) shall use recipient's identifier as provided in an available ERDS evidence or ERDS relay metadata generated by S-ERDS if they want to include this component in the ERDS evidence they produce.

8.2.16 I07 - Recipient's delegate identity attributes

Description	This component specifies the Recipient's delegate identity attributes
Format	
Meaning	In case the R-ERDS provider allows for delegation, this component will be used to provide identity attributes for the recipient's delegate identified by I08 (in clause 8.2.17).
Requirements	This shall be a set of one or more of the identity attributes defined in clause 5.3. The source of the information for this component is the R-ERDS. S-ERDS and intermediate ERDS (in the extended model) shall use recipient's delegate identity attributes as provided in an available ERDS evidence generated by R-ERDS if they want to include this component in the ERDS evidence they produce. If such an evidence is not available to the S-ERDS or intermediate ERDS, this component shall not be present in the ERDS evidence they produce.

8.2.17 I08 - 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, together with a pointer to the delegating recipients the evidence refers to.
Requirements	The identifier shall be as defined in clause 5.2. The source of the information for this component is the R-ERDS. S-ERDS and intermediate ERDS (in the extended model) shall use recipient's delegate identifier as provided in an available ERDS evidence generated by R-ERDS if they want to include this component in the ERDS evidence they produce. If such an evidence is not available to the S-ERDS or intermediate ERDS, this component shall not be present in the ERDS evidence they produce.

8.2.18 I09 - Recipient referred to by the Evidence

Description	Identifier of the recipient to which the evidence refers to
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 I06 specified in clause 8.2.15).
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.

8.2.19 I10 - Sender's identity assurance level details

Description	Details of the assurance levels for the sender's identity verification and for the sender's authentication processes
Format	
Meaning	Details of the processes conducted for verifying the identity of the sender and for authenticating the sender.
Requirements	This component shall meet the semantic requirements defined in clause 5.4 with the details of the assurance levels of the processes conducted for identifying and authenticating the sender of the payload whose processing has resulted in the issuance of the evidence this component is a member of.

8.2.20 I11 - Sender's delegate identity assurance level details

Description	Details of the assurance levels for the sender's delegate identity verification and for the sender's delegate authentication processes
Format	
Meaning	Details of the processes conducted for verifying the identity of the sender's delegate and for authenticating the sender's delegate.
Requirements	This component shall meet the semantic requirements defined in clause 5.4 with the details of the assurance levels of the processes conducted for identifying and authenticating the delegate of the sender of the payload whose processing has resulted in the issuance of the evidence this component is a member of.

8.2.21 I12 - Recipient's identity assurance level details

Description	Details of the assurance levels for the recipient's identity verification and for the recipient's authentication processes
Format	
Meaning	Details of the processes conducted for verifying the identity of the recipient the evidence refers to, indicated by I09 (clause 8.2.18) and for authenticating the recipient.
Requirements	This component shall meet the semantic requirements defined in clause 5.4 with the details of the assurance levels of the processes conducted for identifying and authenticating the recipient of the payload whose processing has resulted in the issuance of the evidence this component is a member of.

8.2.22 I13 - Recipient's delegate identity assurance level details

Description	Details of the assurance levels for the recipient's delegate identity verification and for the recipient's delegate authentication processes
Format	
Meaning	Details of the processes conducted for verifying the identity of the delegate of the recipient referred to by the evidence and for authenticating the recipient's delegate.
Requirements	This component shall meet the semantic requirements defined in clause 5.4 with the details of the assurance levels of the processes conducted for identifying and authenticating the delegate of the recipient of the payload whose processing has resulted in the issuance of the evidence this component is a member of.

8.2.23 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.

8.2.24 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.

8.2.25 M03 - Submission date and time

Description	Submission date and time
Format	Date and time in UTC values
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 in an available evidence generated by S-ERDS if they want to include this component in the evidence they produce. If such an evidence is not available to the R-ERDS or intermediate ERDS, this component shall not be present in the evidence they produce.

8.2.26 M04 - External system

Description	Identification of an external system
Format	Plain text
Meaning	This component identifies a non-ERD service when "G03 Event identifier" assumes one of the values: <ul style="list-style-type: none"> • F.1 RelayToNonERDS • F.2 RelayToNonERDSFailure • F.3 ReceivedFromNonERDS • C.1 NotificationForAcceptance • C.2 NotificationForAcceptanceFailure
Requirements	This component shall provide a description, in plain text, of the external system (non ERDS) involved in the event. It may also identify an ancillary system used for delivering notifications.

8.2.27 M05 - External ERDS

Description	External ERDS
Format	
Meaning	Details of the ERDS provider the evidence refers to.
Requirements	When the evidence relates to an event which implies interaction between the ERDS emitting the evidence and another ERDS, this component shall meet the semantic requirements defined in clause 5.3 with the details of the second ERDS.

8.2.28 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

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 G03 - Event identifier field should contain a URI identifying one of the values from ETSI EN 319 522-1 [1], clause 6.1, table 1, column "Event".

8.3.3 Reasons

8.3.3.1 Reasons related to Events A.x (Sender's submission)

Table 7: Reasons for events A.x

Event	Code	Details and URI code identifying EventReason
(A.1) SubmissionAcceptance (A.2) SubmissionRejection	RA01	Message accepted http://uri.etsi.org/19522/EventReason/MessageAccepted
	RA02	Invalid message format http://uri.etsi.org/19522/EventReason/InvalidMessageFormat
	RA03	Malware found in ERD original message http://uri.etsi.org/19522/EventReason/MalwareFound
	RA04	Sender's signing certificate expired or revoked http://uri.etsi.org/19522/EventReason/S_ERDS_ExpiredSenderCertificate
	RA05	Sender's ERDS provider's policy violation, e.g.: max message size exceeded , invalid attachment formats , etc. http://uri.etsi.org/19522/EventReason/S_ERDS_PolicyViolation
	RA06	ERD message not accepted by the Sender's ERDSP for: Sender's ERDSP malfunction http://uri.etsi.org/19522/EventReason/S_ERDS_Malfunction
	RAXX	Extension

8.3.3.2 Reasons related to the Events B.x (Relay between ERDSs)

Table 8: Reasons for events B.x

Event	Code	Details and URI code identifying EventReason
		http://uri.etsi.org/19522/EventReason/S_ERDS_PolicyViolation
(B.1) RelayAcceptance (B.2) RelayRejection (B.3) RelayFailure	RB01	ERD message successfully relayed to the Recipient's ERDSP http://uri.etsi.org/19522/EventReason/S_ERDS_MessageSuccessfullyRelayed
	RB02	ERD message successfully relayed to, but rejected by, the Recipient's ERDSP for: Invalid message format http://uri.etsi.org/19522/EventReason/R_ERDS_MessageRejected
	RB03	ERD message successfully relayed to, but rejected by, the Recipient's ERDSP for: Malware found in ERD message http://uri.etsi.org/19522/EventReason/R_ERDS_MessageRejectedForMalware
	RB04	ERD message successfully relayed to, but rejected by, the Recipient's ERDSP for: Invalid ERDS signature format or signature policy violation http://uri.etsi.org/19522/EventReason/R_ERDS_MessageRejectedForInvalidSignature
	RB05	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 http://uri.etsi.org/19522/EventReason/R_ERDS_MessageRejectedForInvalidCertificate
	RB06	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 http://uri.etsi.org/19522/EventReason/R_ERDS_PolicyViolation
	RB07	ERD message not relayed to the Recipient's ERDSP for: Recipient's ERDSP malfunction http://uri.etsi.org/19522/EventReason/R_ERDS_Malfunction
	RB08	ERD message not relayed to the Recipient's ERDSP for: Recipient's ERDSP not identified in the Internet http://uri.etsi.org/19522/EventReason/R_ERDS_NotIdentified
	RB09	ERD message not relayed to the Recipient's ERDSP for: Recipient's ERDSP unreachable http://uri.etsi.org/19522/EventReason/R_ERDS_Unreachable
	RB10	ERD message not relayed to the Recipient's ERDSP for: Unknown Recipient http://uri.etsi.org/19522/EventReason/UnknownRecipient
	RB21	ERD message successfully relayed to, but rejected by, the Recipient's ERDSP for: Unregistered recipient to Recipient's ERDSP http://uri.etsi.org/19522/EventReason/MessageNotAcceptedForUnregisteredRecipient
	RB22	The sender's ERDSP received within a given period no information on relay acceptance from the recipient's ERDSP http://uri.etsi.org/19522/EventReason/S_ERDSP_ReceivedNoRelayAcceptanceInfoFromR_ERDSP
	RBXX	Other

8.3.3.3 Reasons related to events C.x (Acceptance/rejection by the recipient)

Table 9: Reasons for events C.x

Event	Code	Details and URI code identifying EventReason
(C.1) NotificationForAcceptance (C.2) NotificationForAcceptanceFailure (C.3) ConsignmentAcceptance (C.4) ConsignmentRejection (C.5) AcceptanceRejectionExpiry (C.6) NotificationDelivered	RC01	Notification for acceptance sent to recipient http://uri.etsi.org/19522/EventReason/R_ERDS_NotificationForAcceptanceSent
	RC02	Subsequent notification for acceptance sent to recipient after no response to previous notifications http://uri.etsi.org/19522/EventReason/R_ERDS_SubsequentNotificationForAcceptanceSent
	RC03	Error in delivering notification for acceptance to recipient http://uri.etsi.org/19522/EventReason/R_ERDS_NotificationForAcceptanceError
	RC04	Error in delivering subsequent notification for acceptance to recipient http://uri.etsi.org/19522/EventReason/R_ERDS_SubsequentNotificationForAcceptanceError
	RC05	Error in delivering notification for acceptance to recipient after multiple attempts http://uri.etsi.org/19522/EventReason/R_ERDS_NotificationForAcceptanceMultipleError
	RC06	Error in delivering subsequent notification for acceptance to recipient after multiple attempts http://uri.etsi.org/19522/EventReason/R_ERDS_SubsequentNotificationForAcceptanceMultipleError
	RC07	Message accepted by the recipient http://uri.etsi.org/19522/EventReason/R_ERDS_MessageAcceptedByRecipient
	RC08	Message explicitly rejected by the recipient http://uri.etsi.org/19522/EventReason/R_ERDS_MessageRejectedByRecipient
	RC09	Message not accepted by the recipient after a defined time period from first successful notification http://uri.etsi.org/19522/EventReason/R_ERDS_MessageNotAcceptedByRecipient
	RCXX	Other

8.3.3.4 Reasons related to events D.x (Consignment to the recipient)

Table 10: Reasons for events D.x

Event	Code	Details and URI code identifying EventReason
(D.1) ContentConsignment (D.2) ContentConsignmentFailure (D.3) ConsignmentNotification (D.4) ConsignmentNotificationFailure (D.5) NotificationAccessTracking (D.6) ContentAccessTracking	RD01	Message successfully consigned to the recipient http://uri.etsi.org/19522/EventReason/MessageConsignedToRecipient
	RD02	Message successfully consigned to a recipient's delegate http://uri.etsi.org/19522/EventReason/R_ERDS_MessageConsignedToDelegate
	RD03	The sender's ERDSP received within a given period no information on consignment from the recipient's ERDSP http://uri.etsi.org/19522/EventReason/S_ERDSP_ReceivedNoDeliveryInfoFromR_ERDSP
	RD04	Not consigned for exceeding recipient quota http://uri.etsi.org/19522/EventReason/MessageNotConsignedForQuota
	RD05	Not consigned for technical malfunction http://uri.etsi.org/19522/EventReason/MessageNotConsignedForMalfunction
	RD06	Not consigned for message type not accepted by recipient http://uri.etsi.org/19522/EventReason/MessageNotConsignedForUnallowedType
	RD21	ERD message not consigned for: Unregistered recipient to Recipient's ERDSP http://uri.etsi.org/19522/EventReason/MessageNotConsignedForUnregisteredRecipient
	RD31	Notification accessed by recipient http://uri.etsi.org/19522/EventReason/NotificationAccessed
	RD32	The sender's ERDS received within a given period of time no information about a notification having been accessed by the recipient. http://uri.etsi.org/19522/EventReason/S_ERDS_UnknownNotificationStatus
	RD33	Content accessed by recipient http://uri.etsi.org/19522/EventReason/R_ERDS_ContentAccessed
	RD34	The sender's ERDS received within a given period of time no information about a message content having been accessed by the recipient. http://uri.etsi.org/19522/EventReason/S_ERDS_UnknownContentAccessStatus
	RDXX	Other

8.3.3.5 Reasons related to events E.x (Handover to the recipient)

Table 11: Reasons for events E.x

Event	Code	Details and URI code identifying EventReason
(E.1) ContentHandover (E.2) ContentHandoverFailure	RE01	Message successfully handed over to the recipient http://uri.etsi.org/19522/EventReason/R_ERDS_MessageHandoverToRecipient
	RE02	Message successfully handed over to a recipient's delegate http://uri.etsi.org/19522/EventReason/R_ERDS_MessageHandoverToDelegate
	RE03	Not handed over for message type not accepted by recipient http://uri.etsi.org/19522/EventReason/R_ERDS_MessageTypeNotAcceptedByRecipient
	RE04	Message handover failed after specific time period http://uri.etsi.org/19522/EventReason/R_ERDS_MessageHandoverFailure
	REXX	Other

8.3.3.6 Reasons related to events F.x (Connection to non ERDS)

Table 12: Reasons for events F.x

Event	Code	Details and URI code identifying EventReason
(F.1) ContentConsignment (F.2) ContentConsignmentFailure (F.3) ReceivedFromNonERDS	RF01	Successful relay to non ERDS
		http://uri.etsi.org/19522/EventReason/RelayToNonERDS
	RF02	External system unreachable
		http://uri.etsi.org/19522/EventReason/ExternalSystemUnreacheanble
	RF03	External system rejected submission
		http://uri.etsi.org/19522/EventReason/RejectedRelayToNonERDS
RF04	Received from non ERDS	
	http://uri.etsi.org/19522/EventReason/ReceivedFromNonERDS	
RAXX	Other	

8.4 Additional requirements for components of evidence

Table 13 within this clause defines cardinality requirements and notes that apply to the different components in all the evidence set specified in ETSI EN 319 522-1 [1], clause 6. Below follows a detailed explanation of the content of the aforementioned table:

- 1) The first row contains the set of events on which an evidence may be 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.
- 5) In addition to the cardinality some cells identify an explanatory note on their contents using letters enclosed in round brackets. Notes appear after the table.

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

Component	Event																				
	Submission Acceptance	Submission Rejection	RelayAcceptance	RelayRejection	RelayFailure	NotificationForAcceptance	NotificationForAcceptanceFailure	ConsignmentAcceptance	ConsignmentRejection	AcceptanceRejectionExpiry	ContentConsignment	ContentConsignmentFailure	ConsignmentNotification	ConsignmentNotificationFailure	ContentHandover	ContentHandoverFailure	RelayToNonERDS	RelayToNonERDSFailure	ReceivedFromNonERDS	NotificationAccessTracking	ContentAccessTracking
G01 Evidence identifier	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
G02 Evidence version	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
G03 Event identifier	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
G04 Reason identifiers	0..1	*	0..1	*	*	0..1	*	0..1	*	*	0..1	*	0..1	*	0..1	*	0..1	*	0..1	*	*
G05 Event time	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
G06 Transaction information log	*(a)	*(a)	*(a)	*(a)	*(a)	*(a)	*(a)	*(a)	*(a)	*(a)	*(a)	*(a)	*(a)	*(a)	*(a)	*(a)	*(a)	*(a)	*(a)	*(a)	*(a)
R01 Evidence issuer policy Identifier	1..*	1..*	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	1	1
R03 Signature	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
I01 Sender's identity attributes	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	0..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	1	0..1	1
I03 Sender's delegate identity attributes	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	0	0..1
I04 Sender's delegate identifier	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	0	0..1
I05 Recipient's identity attributes	0..*	0..*	0..*	0..*	0..*	0..*	0..*	0..*	0..*	0..*	0..*	0..*	0..*	0..*	0..*	0..*	0..*	0..*	0..*	0..*	0..*
I06 Recipient's identifier	1..*	1..*	1..*	1..*	1..*	1..*	1..*	1..*	1..*	1..*	1..*	1..*	1..*	1..*	1..*	1..*	1..*	1..*	1..*	1..*	1..*
I07 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	0..1	0..1
I08 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	0..1	0..1
I09 Recipient ref. to by the evidence	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	0	0	0	1	1
I10 Sender's identity ass. level details	0..1(b)	0..1(b)	0..1(b)	0..1(b)	0..1(b)	0..1(b)	0..1(b)	0..1(b)	0..1(b)	0..1(b)	0..1(b)	0..1(b)	0..1(b)	0..1(b)	0..1(b)	0..1(b)	0..1(b)	0..1(b)	0	0..1(b)	0..1(b)
I11 Sender's del.id. ass. level details	0..1(b)	0..1(b)	0..1(b)	0..1(b)	0..1(b)	0..1(b)	0..1(b)	0..1(b)	0..1(b)	0..1(b)	0..1(b)	0..1(b)	0..1(b)	0..1(b)	0..1(b)	0..1(b)	0..1(b)	0..1(b)	0	0..1(b)	0..1(b)
I12 Recipient's id. ass. level details	0	0	0	0	0	0	0	0..1(c)	0..1(c)	0	0	0	0..1(c)	0	0..1(c)	0	0	0	0	0	0
I13 Recipient's del. id. ass. lev. details	0	0	0	0	0	0	0	0..1(c)	0..1(c)	0	0	0	0..1(c)	0	0..1(c)	0	0	0	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	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	1	1
M03 Submission date and time	1	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	0..1
M04 External system	0	0	0	0	0	0..1	0..1	0	0	0	0	0	0	0	0	0	1	1	1	0..1	0..1
M05 External ERDS	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
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	0..1	0..1

NOTE: (a) 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.
(b) either "I10 Sender's identity assurance level detail" component or I11 "Sender's delegate identity assurance level detail" component shall be present in these evidences.
(c) either "I12 Recipient's identity assurance level detail" component or I13 "Recipient's delegate identity assurance level detail" component shall be present in these evidences.

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 multi-part deliverable [1], 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 relay interfaces (ERDS RI) of 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 the present document.

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 topology 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; the present document 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 may trust another ERDS but not the other way around. It may also happen that an ERDS trusts all participants of a trust domain without being itself a member of that trust domain. This implies that ERD dispatches and ERD payload 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:

- 1) Locally configured by exchange of information, including certificates, between the involved ERDSs.
- 2) 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 [i.6]. An X.509 certificate represents the "service digital identity" of the ERDS in the TSL.
- 3) As a special case of TSL, the European Trust List system will list ERDSs which are qualified in the sense of eIDAS Regulation [i.1]; and the trust domain may be defined as "all qualified ERDSs".
- 4) The trust domain may be defined by a domain PKI issuing X.509 certificates to all participating ERDSs.
- 5) Metadata on capabilities of an ERDS may be extended to contain trust domain information; this is out of scope of the present document.

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 receiverID@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 submission 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 submission 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. The present document 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 organized 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) One metadata repository may span several ERDSs.
- 3) 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 ERDS 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 organizations of metadata repositories can be used, as well as different mechanisms to locate and access the recipient metadata. Similarly, 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.

Metadata on capabilities of an ERDS shall include the attributes listed in table 14.

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. Legal person identity as per clause 5.3.3, alternatively natural person identity as per clause 5.3.2.
Protocol/profile/binding	Alternatives as per ETSI EN 319 522-4-1 [i.8] 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 clause 9.4) where the ERDS is a member, which can be specifies as: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> a) Support for the "expiry date and time" feature: Yes/no flag, see clause 6.2.3. b) Authentication and identification level of assurance supported: List of assurance levels with the same semantic of clause 6.2.4. c) Supported mode of consignment: See clause 6.2.6. d) Support of scheduled delivery: Yes/no flag, see clause 6.2.7. May include the following: <ul style="list-style-type: none"> e) [Optional] ERD policy support: List of identifiers (OID or URI) of supported ERD policies, see clause 6.2.5.

Annex A (informative): Change History

Date	Version	Information about changes
June 2023	1.1.3	Revision of version 1.1.1. Specifically: <ul style="list-style-type: none">• Change to description and composition of some evidences(table 6, table 8)• Introduction of new evidences (impacts on table 13, table 10, M04)• Introduction of a new reason codes (table 8)• Fixed some URIs and descriptions (table 10)• Refactoring and improvement of tables 7, 8, 9, 10, 11 and 12

History

Document history		
V1.1.1	September 2018	Publication
V1.2.0	October 2023	EN Approval Procedure AP 20240103: 2023-10-05 to 2024-01-03