Draft ETSI EN 319 532-4 V1.3.0 (2023-10)

Electronic Signatures and Infrastructures (ESI);
Registered Electronic Mail (REM) Services;
Part 4: Interoperability profiles

Reference
REN/ESI-0019532-4v131

Keywords
e-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

Contents

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 4 of a multi-part deliverable. Full details of the entire series can be found in part 1 [4].

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.

Introduction

Registered Electronic Mail (REM) is a particular instance of an Electronic Registered Delivery Service (ERDS). Standard email, used as a backbone, makes interoperability smooth and increases usability. At the same time, the application of additional security mechanisms ensures integrity, confidentiality and non-repudiation (of submission, consignment, handover, etc.). It protects against the risk of loss, theft, damage and any illegitimate modification.
The present document covers the common and worldwide-recognized requirements to address electronic registered delivery securely and reliably. Particular attention is paid to the Regulation (EU) No 910/2014 [i.1]. However, the legal effects are outside the scope of the present document.

1 Scope

The present document specifies the interoperability profiles of the Registered Electronic Mail (REM) messages according to the formats defined in ETSI EN 319 532-3 [6] and the concepts and semantics defined in ETSI EN 319 532-1 [4] and ETSI EN 319 532-2 [5]. It deals with issues relating to authentication, authenticity and integrity of the information, with the purpose to address the achievement of interoperability across REM service providers, implemented according to the aforementioned specifications.

The present document covers all the options to profile REM services for both styles of operation: S&N and S&F.

More specifically, the present document:

a) Defines generalities on profiling.

b) Defines constraints for SMTP profile.

The present document also specifies a REM baseline supporting the technical interoperability amongst service providers in different regulatory frameworks.

NOTE: Specifically but not exclusively, REM baseline specified in the present document aims at supporting implementations of interoperable REM services by use of Trusted List Frameworks to constitute Trusted domains and qualified REM services (instances of electronic registered delivery services) by use of EU Trusted List system as per Regulation (EU) No 910/2014 [i.1].

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] ETSI EN 319 522-2: "Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 2: Semantic Contents".

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

[4] ETSI EN 319 532-1: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) Services; Part 1: Framework and Architecture".

[5] ETSI EN 319 532-2: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) Services; Part 2: Semantic Contents".

[6] ETSI EN 319 532-3: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) Services; Part 3: Formats".

[7] IETF RFC 5321: "Simple Mail Transfer Protocol".

[8] IETF RFC 5322: "Internet Message Format".

[9] IETF RFC 2045: "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies".

[10] IETF RFC 3207 (2002): "SMTP Service Extension for Secure SMTP over Transport Layer Security".

[11] ETSI EN 319 522-4-3: "Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 4: Bindings; Sub-part 3: Capability/requirements bindings".

[12] ETSI TS 119 612 (V2.2.1): "Electronic Signatures and Infrastructures (ESI); Trusted Lists".

[13] ETSI EN 319 122-1: "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures".

[14] ETSI EN 319 132-1: "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures".

[15] eIDAS Technical Specifications: "SAML Attribute Profile" - Version 1.2", 31 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] ISO/IEC TR 10000:1998: "Information technology - Framework and taxonomy of International Standardized Profiles".

[i.3] IETF RFC 6698: "The DNS-Based Authentication of Named Entities (DANE), Transport Layer Security (TLS) Protocol: TLSA".

[i.4] IETF RFC 7208: "Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1".

[i.5] IETF RFC 6376: "DomainKeys Identified Mail (DKIM) Signatures".

[i.6] NIST Special Publication 800-177: "Trustworthy Email".

[i.7] NIST Special Publication 800-45: "Guidelines on Electronic Mail Security, Version 2".

[i.8] IPJ - The Internet Protocol Journal - November 2016, Volume 19, Number 3: "Comprehensive Internet E-Mail Security: Review of email vulnerabilities and security threats".

[i.9] IETF RFC 4035: "Protocol Modifications for the DNS Security Extensions".

[i.10] IETF RFC 7489: "Domain-based Message Authentication, Reporting, and Conformance (DMARC)".

[i.11] IETF RFC 8551: "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 4.0 Message Specification".

[i.12] ETSI EN 319 521: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Electronic Registered Delivery Service Providers".

[i.13] IETF RFC 7817: "Updated Transport Layer Security (TLS) Server Identity Check Procedure for Email-Related Protocols".

[i.14] IETF RFC 2046: "Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types".

[i.15] ETSI TR 119 001 (V1.2.1): "Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures; Definitions and abbreviations".

[i.16] IETF RFC 8550: "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 4.0 Certificate Handling".

3 Definition of terms, symbols, abbreviations and terminology

3.1 Terms

For the purposes of the present document, the terms given in ETSI EN 319 532-1 [4] and the following apply:

REMID authority: entity entitled to govern the REMID

NOTE: A REMID authority governs the REMID by the management of the REMID policy and through processes of supervision and monitoring, ensuring the adherence to the REMID policy and the requirements specified in the present document.

REMID policy: set of organizational, security and technical requirements that each adherent REMSP is obliged to fulfil to achieve interoperability

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI EN 319 532-1 [4], ETSI TR 119 001 [i.15] and the following apply:

CC Country Code

NOTE: As defined in ETSI TS 119 612 [12], clause 3.2.

DNS Domain Name System
EML Electronic Mail Format

NOTE: As per Internet Message Format syntax defined in IETF RFC 5322 [8].

MS Member State

NOTE: As defined in ETSI TS 119 612 [12], clause 3.2.

QERDS Qualified Electronic Registered Delivery Service

NOTE: As per the definition in ETSI EN 319 522-4-3 [11], clause 7.2.

QREMS Qualified Registered Electronic Mail Service
SAN Subject Alternative Name (or SubjectAltName) X509v3 digital certificate extension

NOTE: As per extension defined in IETF RFC 8550 [i.16], clause 4.4.3.

TSL Trust Status List

NOTE: As per the definition in ETSI EN 319 522-2 [2], clause 9.3.

3.4 Terminology

Since Registered Electronic Email Services are specific types of Electronic Registered Delivery Services, the present document uses the terms and definitions from ETSI EN 319 521 [i.12] and ETSI EN 319 522 (Parts 1 to 3) [1], [2] and [3].

ETSI EN 319 532-2 [5], clause 4.1 specifies the usage of prefixes ERD versus REM or ERDS versus REMS for naming concepts and structures.

The naming convention used in the present document is that constructs whose content is completely generated by the REMS are prefixed with "ERDS" or "REMS". In contrast, constructs whose content includes user-generated data is prefixed with "ERD" or "REM".

4 General requirements

4.1 Introduction

The present document provides one profile as intended in ISO/IEC TR 10000 [i.2]: *"the identification of chosen classes, conforming subsets, options and parameters of base standards, or International Standardized Profiles necessary to accomplish a particular function"*. In the present document the concept of profile embraces references like architectural, protocol detail, semantic and implementation aspects, and technical standard and service interoperability aspects.

More specifically, the present document specifies a REM service profile that uses the same formats (S/MIME based) and the same transport protocols (SMTP). Annex B and Annex C specify the baseline set of requirements for the implementation and configuration of interoperable REM services.

The mandatory requirements defined in the aforementioned referenced REM services specifications are not normally repeated here, but, when necessary, the present document contains some references to them.

4.2 Compliance requirements

Requirements are grouped in three different categories, each with its corresponding identifier. Table 1 defines these categories and their identifiers.

Table 1: Requirements categories

Identifier	Requirement to implement
M	System **shall** implement the element
R	System **should** implement the element
O	System **may** implement the element

All the requirements shall be defined in tabular form.

Table 2: Requirements template

Nº	Service/Protocol element	EN reference	Requirement	Implementation guidance	Notes

Column **N**º shall identify a unique number for the requirements. This number shall start from 1 in each clause. The eventual references to it would also include the clause number to avoid any ambiguity.

Column **Service/Protocol element** shall identify the service element or protocol element the requirement applies to.

Column **EN Reference** shall reference the relevant clause of the standard where the element is defined. The reference is to ETSI EN 319 522-1 [1], ETSI EN 319 522-2 [2], ETSI EN 319 532-1 [4] or ETSI EN 319 532-3 [6] except where explicitly indicated otherwise.

Column **Requirement** shall contain an identifier, as defined in table 1.

Column **Implementation guidance** shall contain numbers referencing notes and letters referencing additional requirements. It is intended either to explain how the requirement is implemented or to include any other information not mandatory.

Column **Notes** shall contain additional notes to the requirement.

NOTE: Within a REMID, a provision different from the ones specified in the present document is viable if and only if such REMID does not envisage to interoperate with other REMIDs.

5 SMTP interoperability profile

5.1 General requirements

This clause defines a profile for interoperability among REMSPs based on SMTP relay protocol and the same formats. Under this basis, although many aspects described here are valid and reusable in other contexts, formats and protocols, all the sentences of the present part of the document mainly refer to interactions among REM services providers using - as a transfer protocol for REM messages - SMTP and its related updates, extensions and improvements (e.g. ESMTP or SMTP-AUTH, etc.).

In particular, the concepts defined in IETF RFC 5321 [7], clause 2.3.1 regarding envelope and content of the Mail Objects, and the concepts defined in IETF RFC 5322 [8], clause 2.2 and IETF RFC 2045 [9] regarding the collection of header fields, structure, formats and message representation shall apply.

5.2 Style of operation

From an interoperability standpoint, no impact is expected to occur because of the adopted style of operation by REMS (Store-And-Forward vs Store-And-Notify). Therefore, the present document shall deal with both on the same profile.

The reason for that is that any REM message exchanged between two REMSPs (even REM messages that contain a reference to the REM Object in a Store-And-Notify context) is conveyed using the Relay Interface that, within the present interoperability profile, is based on the SMTP protocol. Henceforth protocols, message formats and evidence formats are the same in the two cases.

Then, all the REMS operating under the Store-And-Notify style of operation also need a REMS operating under Store-And-Forward style of operation that represents a common layer between the two styles of operation.

Differences only arise in the set of mandatory evidence, which is specified within the two styles of operations, as described in clause 5.5.

5.3 REMS - interfaces constraints

5.3.1 Introduction

The next clauses profile the interfaces specified in ETSI EN 319 522-1 [1] and ETSI EN 319 532-1 [4], clause 5.

5.3.2 REM MSI: Message Submission Interface

Table 3: REM message submission interface

Nº	Service/Protocol element	ETSI EN 319 532-1 [4] reference	Requirement	Implementation guidance	Notes
1	Any protocol, provided that it is secured	Clause 5	M	a)	

Implementation guidance:

a) The Message Submission Interface shall be implemented with a protocol that shall secure the communication from the originating mail User Agent to the SMTP server. More specifically, this protocol shall ensure proper identification and authentication of the user, confidentiality of the communication, authenticity and integrity of the submitted data. For example, SMTP on TLS according to IETF RFC 7817 [i.13] or SSL plus a check of credential over SMTP-AUTH may be used.

5.3.3 REM MRI-ERI: Message and Evidence Retrieval Interface

Table 4: REM message and evidence retrieval interface

Nº	Service/Protocol element	ETSI EN 319 532-1 [4] reference	Requirement	Implementation guidance	Notes
1	Any protocol, provided that it is secured	Clause 5	M	a)	

Implementation guidance:

a) The Message and Evidence Retrieval Interface shall be implemented with a protocol that shall secure the communication from the sender/recipient mail User Agent to the REMSP server. More specifically, this protocol shall ensure proper identification and authentication of the user, confidentiality of the communication, authenticity and integrity of the retrieved data. For example, IMAP or POP or HTTP on TLS according to IETF RFC 7817 [i.13] or SSL may be used.

5.3.4 REM RI: Relay Interface

Table 5: REM relay interface

Nº	Service/Protocol element	ETSI EN 319 532-1 [4] reference	Requirement	Implementation guidance	Notes
1	SMTP on TLS	Clause 5	M	a)	see note
NOTE: This is a profile for SMTP relay protocol among REMSPs, and it is reflected in this requirement.					

Implementation guidance:

a) The Relay Interface shall be implemented using SMTP protocol securing the communication from the sender REMSP server to the recipient REMSP server using TLS according to IETF RFC 3207 [10].

NOTE: Particular attention has to be paid to preserving confidentiality, authenticity, integrity, identification and authentication. TLS and the best practices recommended in Annex A give the necessary provision to accomplish these requirements. Further IETF work about MTA-to-MTA (TLS everywhere) dialogue is actually under a draft status and not added as a reference in the present document. However, it is a desirable practice in addition to opportunistic STARTTLS/DANE (see NIST Special Publication 800-177 [i.6] for more details).

5.3.5 CSI: Common Service Interface

The services used throughout this interface are not necessarily provided by a REMS (see note 1) and, for the present profile, the following three main elements shall be considered:

1) Routing

2) Trusting

3) Capability discovery and management

NOTE 1: For this reason, the prefix REM is omitted before the definition of the interface.

ETSI EN 319 532-2 [5], clause 9 shall identify the semantic requirements that apply to CSI.

Table 6: Common service interface

Nº	Service/Protocol element	ETSI EN 319 532-3 [6] reference	Requirement	Implementation guidance	Notes
1	DNS	Clause 9.2	M	a)	Routing interface
2	TL	Clause 9.3	R	b)	Trusting interface
3	TL/SMP	Clause 9.4	O	c)	Discovery/management interface

Implementation guidance:

a) The Routing Interface, part of CSI, shall be implemented using DNS protocol properly secured.

NOTE 2: The best practices recommended in Annex A give further indications to accomplish security requirements about routing.

b) The Trusting Interface, part of CSI, should be implemented using TL protocol.

c) The Discovery/management Interface, part of CSI, may be implemented using both or either TL or SMP protocols.

5.4 REM message constraints

5.4.1 REMS relay metadata MIME Header Fields constraints

Table 7: REM message header fields constraints

Nº	Service/Protocol element	ETSI EN 319 532-3 [6] reference	Requirement	Implementation guidance	Notes
1	REM-MessageType	Clause 6.1	M	a)	
2	REM-EventIdentifier	Clause 6.1	M	b)	
3	REM-Evidence-ID	Clause 6.2.1	M	c)	
4	REM-ReasonIdentifier	Clause 6.2.1	R	d)	

Implementation guidance:

a) Its value shall be one of the 4 strings defined in table 2 of ETSI EN 319 532-3 [6], clause 6.1, related to the MD13 component.

b) Its value shall be the G03 component, as defined in table 2 of ETSI EN 319 532-3 [6], clause 6.1. It shall be composed by the URI in column 1, table 3 of ETSI EN 319 522-3 [3], clause 5.2.2.5.

c) Its value shall be the G01 component corresponding to the evidence specified inside the "EvidenceIdentifier" ERDS evidence element defined in ETSI EN 319 522-3 [3], clause 5.2.2.3.

d) Its value shall be the G04 component corresponding to a URI defined in table 4 of ETSI EN 319 522-3 [3], clause 5.2.2.7. EventReasons is a multivalue element. This property reflects a list of REM-*ReasonIdentifier* header fields in REM message, each with the corresponding URI value.

NOTE: Item Nº 4 in table 7 facilitates achieving interoperability that can also be reached without it.

5.4.2 signed data MIME Header Fields constraints

The header fields constraints, present in table 4 of ETSI EN 319 532-3 [6], clause 6.2.2 shall apply.

5.4.3 REMS introduction MIME Header Fields-Body constraints

5.4.3.1 General Requirements

Table 8: REMS introduction header fields constraints

Nº	Service/Protocol element	ETSI EN 319 532-3 [6] reference	Requirement	Implementation guidance	Notes
1	REM-Section-Type	Clause 6.2.3.1	M	a)	

Implementation guidance:

a) A REM-Section-Type header shall have the value "rem_message/introduction".

5.4.3.2 multipart/alternative: free text subsection Header Fields constraints

Table 9: REMS text introduction header fields constraints

Nº	Service/Protocol element	ETSI EN 319 532-3 [6] reference	Requirement	Implementation guidance	Notes
1	Content-Type	Clause 6.2.3.2	R	a)	

Implementation guidance:

a) The header field constraints in table 6 of ETSI EN 319 532-3 [6], clause 6.2.3.2 shall apply. An encoding according to charset="UTF-8" parameter should be used.

5.4.3.3 multipart/alternative: HTML subsection Header Fields constraints

Table 10: REMS HTML introduction header fields constraints

Nº	Service/Protocol element	ETSI EN 319 532-3 [6] reference	Requirement	Implementation guidance	Notes
1	Content-Type	Clause 6.2.3.3	R	a)	

Implementation guidance:

a) The header field constraints in table 6 of ETSI EN 319 532-3 [6], clause 6.2.3.3 shall apply. An encoding according to charset="UTF-8" parameter should be used.

5.4.4 original message MIME Header Fields constraints

Table 11: REMS user content header fields constraints

Nº	Service/Protocol element	ETSI EN 319 532-3 [6] reference	Requirement	Implementation guidance	Notes
1	REM-Section-Type	Clause 6.2.4.2	M	a)	

Implementation guidance:

a) A REM-Section-Type header shall have the value "rem_message/original".

5.4.5 REMS extensions MIME Header Fields constraints

Each extension section of the REM message shall contain an attachment. The following restrictions apply.

Table 12: REMS extensions header fields constraints

Nº	Service/Protocol element	ETSI EN 319 532-3 [6] reference	Requirement	Implementation guidance	Notes
1	REM-Section-Type	Clause 6.2.5	M	a)	

Implementation guidance:

a) The REM-Section-Type header shall have the value "rem_message/extension".

5.4.6 ERDS evidence MIME Header Fields constraints

Table 13: ERDS evidence MIME header fields constraints

Nº	Service/Protocol element	ETSI EN 319 532-3 [6] reference	Requirement	Implementation guidance	Notes
1	REM-Section-Type	Clause 6.2.6.2	M	a)	

Implementation guidance:

a) A REM-Section-Type header shall have the value "rem_message/xml_evidence".

Table 14: ERDS evidence MIME header fields constraints

Nº	Service/Protocol element	ETSI EN 319 532-3 [6] reference	Requirement	Implementation guidance	Notes
2	Content-Type	Clause 6.2.6.2	M	a)	

Implementation guidance:

a) The value for this field shall be: "application/xml;" and name/charset parameters shall have the values specified in ETSI EN 319 532-3 [6], clause 6.2.6.2.

For the ERDS evidence attachment, the present profile requires XML format (defined in clause 7.4 of ETSI EN 319 532-3 [6]).

Optionally, the PDF format may be also present as defined in clause 6.2.6.3 of ETSI EN 319 532-3 [6].

5.4.7 REMS signature MIME Header Fields-Body constraints

Table 15: REMS signature headers constraints

Nº	Service/Protocol element	ETSI EN 319 532-3 [6] reference	Requirement	Implementation guidance	Notes
1	Content-Type	Clause 6.2.7	M	a)	
2	Content-Disposition	Clause 6.2.7	M	b), c)	

Implementation guidance:

a) The value of the Content-Type header field shall be: "application/pkcs7-signature". An additional "name" parameter shall have the value "smime.p7s".

b) The value of the Content-Disposition header field shall be "attachment". An additional "filename" parameter shall have the value "smime.p7s".

c) Every REM message generated by a REMS shall include the field Content-Disposition and fill in the name/filename parameters. To maximize the level of interoperability, the REMSPs shall be able to correctly interpret incoming messages without the presence of either one or both of Content-Disposition and name/filename parameters.

5.5 REMS - evidence set constraints

5.5.1 ERDS evidence types constraints

5.5.1.1 Mandatory evidence - all styles of operation

Table 16 defines requirements for the evidence types specified in ETSI EN 319 522-1 [1] within the clauses identified below.

Table 16: Mandatory ERDS evidence set

Nº	Service/Protocol element	ETSI EN 319 522-1 [1] reference	Requirement	Implementation guidance	Notes
1	SubmissionAcceptance	Clause 6.2.1 A.1.	M	a)	see note 1
2	SubmissionRejection	Clause 6.2.1 A.2.	M	b)	see note 1
3	ContentConsignment	Clause 6.2.4 D.1.	M	c)	see note 2
4	ContentConsignmentFailure	Clause 6.2.4 D.2.	M	c)	see note 2
5	NotificationForAcceptance	Clause 6.2.3 C.1.	M	c)	see note 3
6	NotificationForAcceptanceFailure	Clause 6.2.3 C.2.	M	c)	see note 3
NOTE 1: Rationale: The sender is made aware of the successful/unsuccessful outcome of their message submission. NOTE 2: Rationale: The sender is made aware of whether the recipient was/was not made available (within the boundaries of the recipient's REMS) of the user content he/she sent (where the sender's REMS style of operation is "S&F"). NOTE 3: Rationale: The sender is made aware of whether the recipient was/was not made available (within the boundaries of the recipient's REMS) of the notification the sender's REMS generated with the original message (where the sender's REMS style of operation is "S&N").					

Implementation guidance:

a) The sender's REMS shall include the SubmissionAcceptance (obviously related to a successful submission) in the REM dispatch(es) to be forwarded to the final recipient(s).

b) The sender's REMS shall include the SubmissionRejection (obviously related to an unsuccessful submission) in the REMS receipt to be sent back to the sender.

c) The recipient's REMS shall send a REMS receipt to the sender, including the evidence relevant to the event of a consignment of the REM dispatch or REMS notification or REM payload.

5.5.1.2 Mandatory evidence - S&N style of operation

Table 17 defines requirements for the evidence types specified in ETSI EN 319 522-1 [1] within the clauses identified below.

Table 17: Mandatory ERDS evidence set for store-and-notify

Nº	Service/Protocol element	ETSI EN 319 522-1 [1] reference	Requirement	Implementation guidance	Notes
1	ContentHandover	Clause 6.2.5 E.1.	M	a)	see note
2	ContentHandoverFailure	Clause 6.2.5 E.2.	M	a)	see note
NOTE: Rationale: The sender needs to have evidence on whether the original message referenced in the notification was handed over to the recipient within a predefined time period.					

Implementation guidance:

a) The recipient's REMS shall send one REMS receipt to the sender, including the ContentHandover or the ContentHandoverFailure.

5.5.1.3 Conditional evidence - all styles of operation

Table 18 defines requirements for the evidence types specified in ETSI EN 319 522-1 [1] within the clauses identified below.

Table 18: Conditional ERDS evidence set

Nº	Service/Protocol element	ETSI EN 319 522-1 [1] reference	Requirement	Implementation guidance	Notes
1	RelayAcceptance	Clause 6.2.2 B.1.	Conditional	a), b)	see note 2
2	RelayRejection	Clause 6.2.2 B.2.	Conditional	a), b)	see note 2
3	RelayFailure	Clause 6.2.2 B.3.	Conditional	d), e)	see note 2
NOTE 1: The "Conditional" requirement category is used instead of that defined in table 1, with the meaning that the relevant requirement is subject to particular conditions made explicit in the implementation guidance. NOTE 2: Rationale: the sender needs to know if the sent message did not successfully reach or was rejected by the recipient's REMS to enact possible backup measures.					

Implementation guidance for 1 and 2:

a) RelayAcceptance and RelayRejection shall be generated if:

- no opposite provision is explicitly specified in the applicable REMID rules;
- no previous opposite agreement exists between the involved REMSPs.

Such agreement or interoperability provision should specify one of the following defaults, in case of timeout:

I) The sender's REMS will assume that the recipient's REMS has rejected a REM dispatch or payload if any other contrary indication (e.g. REMS receipt and/or SMTP DSN) is received within a predefined time period.

II) The sender's REMS will assume that the recipient's REMS has accepted a REM dispatch or payload if any other contrary indication (e.g. REMS receipt and/or SMTP DSN) is received within a predefined time period.

Alternative conditions to I) and II) may be specified in the aforementioned agreement provided that these conditions deal with the relay transaction closure with an exhaustive method.

b) If the evidence type is considered mandatory, the recipient's REMS shall send back to the sender's REMS a REMS receipt, including the RelayAcceptance or the RelayRejection evidence.

NOTE: These REMS receipts are sent to the S-REMS (as a "kind of answer" to a REM dispatch). One place where to get the email address where to send such receipts is represented by the mail/rfc822Name attribute of the X509v3 SAN extension of digital certificate used for the digital signature of the REM dispatch (see note at Clause D.2.2.1 and Clause D.2.2.2). Other places with the email addresses where to send such REMS receipts, other than the SAN and further detailed for instance in profiles or REMID policy, are possible and make sense when in coherence with REM specification.

c) Void.

Implementation guidance for 3:

d) RelayFailure shall be generated if there is no explicit requirement against its generation within REMID.

Such interoperability requirement should specify:

III) The sender's REMS will assume that is impossible to relay a REM dispatch or payload to the recipient's REMS, if any contrary indication (e.g. REMS receipt and/or SMTP DSN) is received within a predefined time period.

Alternative conditions to III) may be specified in the requirement above provided that these conditions deal with the relay transaction closure with an exhaustive method.

e) The sender's REMS shall build a REMS receipt, including the pertinent components of RelayFailure evidence (and any other contrary indication to the relay, like SMTP DSN) and shall send it back to the sender.

5.5.2 ERDS evidence components constraints

5.5.2.1 General requirements

Requirements for XML ERDS evidence defined in ETSI EN 319 522-3 [3], clause 5 shall apply.

In the following clauses, details on the Evidence components coming from ETSI EN 319 522-2 [2], clause 8 are listed (in the third columns of each table) for each mandatory evidence type indicated in clauses from 5.5.1.1 through 5.5.1.3. The modelling adopted in the tables defined in the following clauses from 5.5.2.2 to 5.5.2.6 differs from that used. More in detail, the following clauses list all Evidence components required to ensure interoperability, including those in table 13 in ETSI EN 319 522-2 [2], clause 8.4 are already indicated as mandatory or whose absence implies a default value.

NOTE 1: All the evidence components are listed regardless of the style of operation used. The evidence components relevant to the S&N style of operation have to be considered only when the S&N style of operation option is used.

Evidence components not listed in table 19, table 20, table 21, table 22 and table 23 from clause 5.5.2.2 to clause 5.5.2.6 may be absent within REMS based on the present interoperability profile.

NOTE 2: This different approach has been adopted to give a more complete and comfortable view to the reader.

5.5.2.2 SubmissionAcceptance - SubmissionRejection

Table 19: ERDS evidence components submission constraints

Nº	Evidence element	ETSI EN 319 522-2 [2] Clause 8 - reference	Requirement	Implementation guidance	Notes
1	Evidence identifier	G01	M		see note
2	Event identifier=SubmissionAcceptance or SubmissionRejection	G03	M		see note
3	Reason identifier	G04	M		
4	Reason code	G04	M (1..N)	a)	
5	Evidence version	G02	M		see note
6	Event time	G05	M		see note
7	Evidence issuer policy identifier	R01	M (1..N)		see note
8	Evidence issuer details	R02	M		see note
9	Sender's identifier	I02	M		see note
10	Recipient's identifier	I06	M (1..N)		see note
11	Sender's identity assurance details	I10	O	b)	
12	User content information	M02	M		see note
13	Submission date and time	M03	M		see note
14	Signature	R03	M		see note
15	Message Identifier	M01	M		see note
NOTE: This requirement is mandatory in table 13 in ETSI EN 319 522-2 [2], clause 8.4.					

Implementation guidance:

a) At least one Reason code shall be present, unless the applicable REMIDs explicitly require that no Reason code is necessary when submission is regularly accepted. Multiple Reason codes may be present depending on the reasons that caused the evidence's triggering event.

b) If this field is not present, the class of authentication is Basic. In the other cases, it specifies the class of Authentication according to the semantic of ETSI EN 319 522-2 [2], clause 5.4.

5.5.2.3 ContentConsignment - ContentConsignmentFailure

Table 20: ERDS evidence components consignment constraints

Nº	Evidence element	ETSI EN 319 522-2 [2] Clause 8 - reference	Requirement	Implementation guidance	Notes
1	Evidence identifier	G01	M		see note
2	Event identifier=ContentConsignment or ContentConsignmentFailure	G03	M		see note
3	Reason identifier	G04	M		
4	Reason code	G04	M (1..N)	a)	
5	Evidence version	G02	M		see note
6	Event time	G05	M		see note
7	Evidence issuer policy identifier	R01	M (1..N)		see note
8	Evidence issuer details	R02	M		see note
9	Sender's identifier	I02	M		see note
10	Recipient's identifier	I06	M (1..N)		see note
11	Recipient referred to by the evidence	I09	M		see note
12	User content information	M02	M		see note
13	Signature	R03	M		see note
14	Message Identifier	M01	M		see note
NOTE: This requirement is mandatory in table 13 in ETSI EN 319 522-2 [2], clause 8.4.					

Implementation guidance:

a) At least one Reason code shall be present, unless the applicable REMIDs explicitly require that no Reason code is necessary when consignment regularly occurred. Multiple Reason codes may be present depending on the reasons that caused the evidence's triggering event.

5.5.2.4 ContentHandover - ContentHandoverFailure

Table 21: ERDS evidence components handover constraints

Nº	Evidence element	ETSI EN 319 522-2 [2] Clause 8 - reference	Requirement	Implementation guidance	Notes
1	Evidence identifier	G01	M		see note
2	Event identifier=ContentHandover or ContentHandoverFailure	G03	M		see note
3	Reason identifier	G04	M		
4	Reason code	G04	M (1..N)	a)	
5	Evidence version	G02	M		see note
6	Event time	G05	M		see note
7	Evidence issuer policy identifier	R01	M (1..N)		see note
8	Evidence issuer details	R02	M		see note
9	Sender's identifier	I02	M		see note
10	Recipient's identifier	I06	M (1..N)		see note
11	Recipient referred to by the evidence	I09	M		see note
12	Recipient Authentication details	I05	O	b)	
13	User content information	M02	M		see note
14	Signature	R03	M		see note
15	Message Identifier	M01	M		see note
NOTE: This requirement is mandatory in table 13 in ETSI EN 319 522-2 [2], clause 8.4.					

Implementation guidance:

a) At least one Reason code shall be present, unless the applicable REMIDs explicitly require that no Reason code is necessary when download regularly occurred. Multiple Reason codes may be present depending on the reasons that caused the evidence's triggering event.

b) If this field is not present,the class of authentication is Basic. In the other cases, it specifies the class of Authentication.

5.5.2.5 RelayAcceptance - RelayRejection

Table 22: ERDS evidence components relay constraints

Nº	Evidence element	ETSI EN 319 522-2 [2] Clause 8 - reference	Requirement	Implementation guidance	Notes
1	Evidence identifier	G01	M		see note
2	Event identifier=RelayAcceptance or RelayRejection	G03	M		see note
3	Reason identifier	G04	M		
4	Reason code	G04	M (1..N)	a)	
5	Evidence version	G02	M		see note
6	Event time	G05	M		see note
7	Evidence issuer policy identifier	R01	M (1..N)		see note
8	Evidence issuer details	R02	M		see note
9	Sender's identifier	I02	M		see note
10	Recipient's identifier	I06	M (1..N)		see note
11	User content information	M02	M		see note
12	Signature	R03	M		see note
13	Message Identifier	M01	M		see note
14	External ERDS	M05	M		see note
NOTE: This requirement is mandatory in table 13 in ETSI EN 319 522-2 [2], clause 8.4.					

Implementation guidance:

a) At least one Reason code shall be present, unless the applicable REMIDs explicitly require that no Reason code is necessary when the relay to the recipient's REMS regularly occurred. Multiple Reason codes may be present depending on the reasons that caused the evidence's triggering event.

5.5.2.6 RelayFailure

Table 23: ERDS evidence components relay failure constraints

Nº	Evidence element	ETSI EN 319 522-2 [2] Clause 8 - reference	Requirement	Implementation guidance	Notes
1	Evidence identifier	G01	M		see note
2	Event identifier=RelayFailure	G03	M		see note
3	Reason identifier	G04	M		
4	Reason code	G04	M (1..N)	a)	
5	Evidence version	G02	M		see note
6	Event time	G05	M		see note
7	Evidence issuer policy identifier	R01	M (1..N)		see note
8	Evidence issuer details	R02	M		see note
9	Sender's identifier	I02	M		see note
10	Recipient's identifier	I06	M (1..N)		see note
11	User content information	M02	M		see note
12	Signature	R03	M		see note
13	Message Identifier	M01	M		see note
14	External ERDS	M05	M		see note
NOTE: This requirement is mandatory in table 13 in ETSI EN 319 522-2 [2], clause 8.4.					

Implementation guidance:

a) At least one Reason code shall be present, unless the applicable REMIDs explicitly require that no Reason code is necessary when relay to the recipient's REMS failed. Multiple Reason codes may be present depending on the reasons that caused the evidence's triggering event.

Annex A (informative): REM best practices

This annex provides a set of publications containing the best practices recommended for electronic email infrastructures that are also worthwhile for REM implementers.

NIST Special Publication 800-177 [i.6] - Trustworthy Email: Recommendations for deploying protocols and technologies that improve the trustworthiness of email, reduce the risk of spoofing email contents being disclosed to unauthorized parties.

NOTE 1: In particular, the following are of interest for REM: TLS and STARTTLS (IETF RFC 3207 [10]), DNS-based Authentication of Named Entities (DANE - IETF RFC 6698 [i.3]), Sender Policy Framework (SPF - IETF RFC 7208 [i.4]), Domain Keys Identified Mail (DKIM - IETF RFC 6376 [i.5]).

NIST Special Publication 800-45 [i.7] - Guidelines on Electronic Mail Security: Recommendations of security practices for designing, implementing, and operating email systems on public and private networks.

NOTE 2: In particular, the following are of interest for REM: Planning, managing and securing servers and operating systems; hardening servers, content and network; managing malware.

The Internet Protocol Journal November 2016, Volume 19, Number 3 [i.8] - Comprehensive Internet E-Mail Security: Review of email vulnerabilities and security threats.

NOTE 3: In particular, the following are of interest for REM: Domain Name System Security Extensions (DNSEC - IETF RFC 4035 [i.9]), Domain-Based Message Authentication, Reporting, and Conformance (DMARC - IETF RFC 7489 [i.10]), S/MIME (IETF RFC 8551 [i.11]).

Annex B (informative): REM baseline rationales

B.1 Introduction

The eIDAS Regulation (EU) No 910/2014 [i.1] defines a set of principles promoting the directions that emerged from the EU Digital Agenda and the subsequent conclusions of the European Council. The objectives of such principles are oriented to counteract <<*…the lack of interoperability and the rise in cybercrime…*>> through <<*...cross-border use of online services …by creating appropriate conditions for the mutual recognition of key enablers across borders, such as … electronic delivery services, …*>>.

The present informative annex provides a set of rationales used as context for the normative Annex C. The aim is to introduce the REM baseline, a "baseline" set of requirements leading the implementation and configuration of REM services facilitating the fulfilment of the principles as mentioned earlier.

REM baseline specifies a minimal set of requirements aiming to ensure maximal interoperability in the cross-REM interoperability domain and, specifically, in cross-border use of REM services. Compliance with REM baseline aims to simplify technical support of REM by Member States competent authorities supporting qualified registered electronic delivery services. Without common baseline requirements, the technical support of REM can be very costly and challenging.

The main characteristics of a system compliant with the requirements specified in the present document are:

- It is a "non-closed" system (see note 1).
- Easy verification methods are available.
- Clear access points and rules for interoperability are also available.

NOTE 1: The set of participants is not restricted nor predefined.

The present document deals in detail with trust, protocol handshake, digital signatures and time-stamp. This annex focuses attention on the boundary key elements to fulfil, as widely as possible, amongst others, the aim/requirement of eIDAS Regulation (EU) No 910/2014 [i.1] expressed in recital 66: "*facilitate cross-border recognition between existing national legal systems related to electronic registered delivery services*". In other words, digital signatures and time-stamps answer to the question "**what**" is cross/shared among system[s], and Common Service Interface (CSI) answers the question "**how**" to interoperate in such digital messaging ecosystem; finally, the eIDAS Regulation (EU) No 910/2014 [i.1] constitutes one of the "**why**". Answering both "what" and "how" questions, a great deal of care is placed aiming to satisfy this "why".

NOTE 2: The REM baseline aims to facilitate compliance with the eIDAS Regulation (EU) No 910/2014 [i.1], but the full legal value and the relevant legal effects are out of its scope.

B.2 Common Service Interface (CSI)

B.2.1 Overview

The present clause illustrates the approach adopted in identifying the solutions defined in Annex C to address the Common Service Interface (CSI) requirements in **REM messaging**.

NOTE: The definitions of CSI carry a strong characterization of the service in terms of interoperability, making it clear the appropriateness of CSI as the place where, among other things, to counteract <<*…the lack of interoperability and the rise in cybercrime…*>> as remembered in clause B.1 of the present document.

Table B.1 provides, for each concept of the second column, the suggested starting reference, in the third column, with the "first" prescription (e.g. text with some provision) in the full set of standards about the concept itself. The last column contains the other normative references linked from the main reference.

Table B.1: CSI - normative reference map

Nº	Concept	Main normative refence	Linked normative Reference(s)
1	Message Routing	ETSI EN 319 532-1 [4], clause 5	
		ETSI EN 319 532-2 [5], clause 9.2	ETSI EN 319 522-2 [2], clause 9.2
		ETSI EN 319 532-3 [6], clause 5	
		Clause C.2.3.2 of the present document	ETSI EN 319 532-3 [6], clause 9.2
2	Trust establishment	ETSI EN 319 532-1 [4], clause 5	
		ETSI EN 319 532-2 [5], clause 9.3	ETSI EN 319 522-2 [2], clause 9.3
		ETSI EN 319 532-3 [6], clause 9.3	ETSI EN 319 522-4-3 [11], clauses 7.2 and 7.3 ETSI TS 119 612 [12]
		Clause C.2.3.3 of the present document	ETSI EN 319 532-3 [6], clause 9.3 ETSI EN 319 522-4-3 [11], clauses 7.1 and 7.2 ETSI TS 119 612 [12], clauses 5.5.1, 5.5.3 and 5.5.7
3	Capability discovery and management	ETSI EN 319 532-1 [4], clause 5	
		ETSI EN 319 532-2 [5], clause 9.4	ETSI EN 319 522-2 [2], clauses 9.4.3 and 9.4.4
		ETSI EN 319 532-3 [6], clause 9.4	ETSI EN 319 522-3 [3], clause 6.3.2 ETSI EN 319 522-4-3 [11], clause 7.2 ETSI TS 119 612 [12], clause 5.5.9.4
		Clause C.2.3.4 of the present document	ETSI EN 319 532-3 [6], clause 9.4 ETSI EN 319 522-3 [3], clause 6.3.2 ETSI EN 319 522-4-3 [11], clause 7.2 ETSI TS 119 612 [12], clause 5.5.9.4
4	Governance support	ETSI EN 319 532-1 [4], clause 5	
		ETSI EN 319 532-2 [5], clause 9.3	ETSI EN 319 522-2 [2], clause 9.3
		Clause C.2.3.5 of the present document	ETSI EN 319 522-4-3 [11], clause 7.1 ETSI TS 119 612 [12], clause 5.3.9

Figure B.1 expresses in an explicit form the cross-border view (see also the Black-Box and 4-Corner models illustrated in clauses 4.2.1, 4.3.1 and 5 of ETSI EN 319 522 (Parts 1 to 2) [1], [2] and ETSI EN 319 532-1 [4]). Only the main details of the elements important for interfacing purposes are put in evidence in figure B.1. In particular, concepts coming from the Black-box model (high-level components) and 4-Corner model (functional infrastructures) are collapsed, outlining the "shared infrastructure" and its interface: namely a unique "Common Service Interface" (CSI) for cross-border interactions.

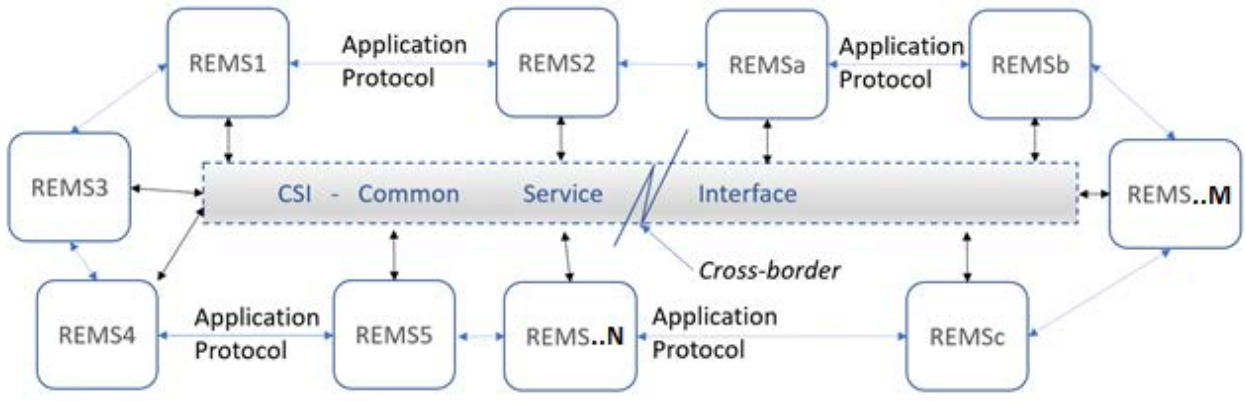

Figure B.1: Detailed view of a REMS (e-delivery) derived from the "Black-box" rationale

The exploded view above refers to a distributed model that addresses the interoperability requirements in a cross-border context.

B.2.2 Derived rationales

B.2.2.1 General

In a complete context like that introduced in clause B.2.1, where several REMSPs need to interoperate, the full set of elements of CSI to consider are:

1) Message Routing (detailed in clauses B.2.2.2 and C.2.3.2)

2) Trust establishment (detailed in clauses B.2.2.3 and C.2.3.3)

3) Capability discovery and management (detailed in clauses B.2.2.4 and C.2.3.4)

4) Governance support (detailed in clauses B.2.2.5 and C.2.3.5)

Message Routing and trust establishment lend itself to be addressed using widespread international and European standards. Instead, Capability and Governance are more strictly related to aspects of the particular e-delivery service type; they are instead covered through either one or both of ETSI standards and local authorities' activity and regulations (e.g. definition of applicable Policies and TL schemes according to the present REM baseline and as detailed in Governance support sections).

To provide a "context" to the dispositions of clause C.2, clause B.2 collects the main rationales starting from the referenced standards dealing with four points as mentioned earlier. Any rationale present in the last column from table B.2 to table B.11 is derived from and according to the entire set of statements (pure extracts of the standards) in the first column, taken together.

NOTE 1: Each table represents some concept outlined in the relevant title that is interesting for the present clause. The rationales (that are not connected one-to-one and row-by-row to each statement) are obtained considering the entire set of statements of the first column "as a whole".

NOTE 2: To have a consistent quoted text, in the first column of the tables mentioned above (where there are pure extracts of various standards), the original reference numbers of referenced documents are deleted, leaving the two square brackets emptied []. The original numbering cannot correspond with the actual numbering of the present document, resulting in misunderstandings. The complete original numbering reference is in the original source standard.

Since many elements about CSI (and, in particular, on trust establishment) are specified, at a more general ERDS level, in ETSI EN 319 522-2 [2] and ETSI EN 319 522-4-3 [11], these are captured and rationalized also at REM level with all due distinctions of case.

B.2.2.2 Message Routing

The usage of DNS international standards as a basic requirement for routing is considered fundamental for achieving interoperability. Some additional security measures to DNS operations are needed to reduce risks of cybercrime related to the use of DNS. For detailed requirements on message routing applied in REM, see clause C.2.3.2.

B.2.2.3 Trust establishment

The building of a mutually trusted set of REMS is a fundamental step for achieving interoperability. The present clause provides all the rationales to get this point. For detailed requirements on trust establishment applied in REM baseline, see clause C.2.3.3.

Table B.2: Trust domain and policy rationales

Nº	Statement	Reference	Derived rationales
1	*"Trust is defined as the existence of **a trust domain** within which **co-operation** between participating ERDSs is **regulated…., trust infrastructures may be used to establish trust**. In this case, the trust infrastructure, i.e. **the trust domain, shall have governance, at least for policy regarding conditions for an ERDS to join***	ETSI EN 319 522-4-3 [11], clause 7.1	The concept of **trust domain** (see figure B.2) is defined to substantiate a trust. In the REM context the **REM interoperability domain** (**REMID**) concept is used to identify a particular **subset** of a trust domain (possibly the whole) where all participants REMSs are interoperable (see figure B.3, figure B.4 and figure B.5). A **trust domain policy** (as per statements 2, 5 and 6 at side) can also include provisions for ensuring that all the participants have the same capabilities. In such a case, the trust domain would be a **REMID**. The REM baseline defined in the present document specifies the provisions for **technical interoperability** (see figure B.5). If the trust domain policy does not include provisions for **technical interoperability**, still one or more REMIDs can be defined within the trust domain, each one with its own set of provisions for technical interoperability, for the providers that meet such provisions. A **trust domain** is subjected to governance (which, among other provisions, defines rules for joining to the trust domain), carried by a so-called **scheme operator**. A **REM interoperability domain** (**REMID**) is subject to governance (which, among other provisions, defines rules for joining to the **REMID**, the definition of and operation to **REMID policy**), carried by a so-called **REMID authority**.
2	*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***	ETSI EN 319 522-2 [2], clause 9.3	
3	***REMID**: **REM Interoperability Domain*** ***REM interoperability domain**: homogeneous operational space consisting of a set of REMSPs able to properly interoperate among themselves* ***REM interoperability domain rules**: set of rules defining a REM interoperability domain*	ETSI EN 319 532-1 [4]. clause 3.1	
4	*Information about ERDSs participating in specific **trust domains** may be found by the following means:* *1) ...* *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 []. 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** []; and the **trust domain may be defined as "all qualified ERDSs"**.* *4)...* *5) Metadata on **capabilities** of an ERDS **may be extended to contain trust domain information** …*	ETSI EN 319 522-2 [2], clause 9.3	
5	*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***	ETSI EN 319 522-2 [2], clause 9.4.4	
6	*… a **trust domain policy** may specify **policy**, **security**, and **technical requirement** that each ERDS is **obliged** to fulfil; hence **technical interoperability** between the ERDSs **may be ensured**"*	ETSI EN 319 522-4-3 [11], clause 7.1	

The rationales of the table B.2 are illustrated from figure B.2 to figure B.6.

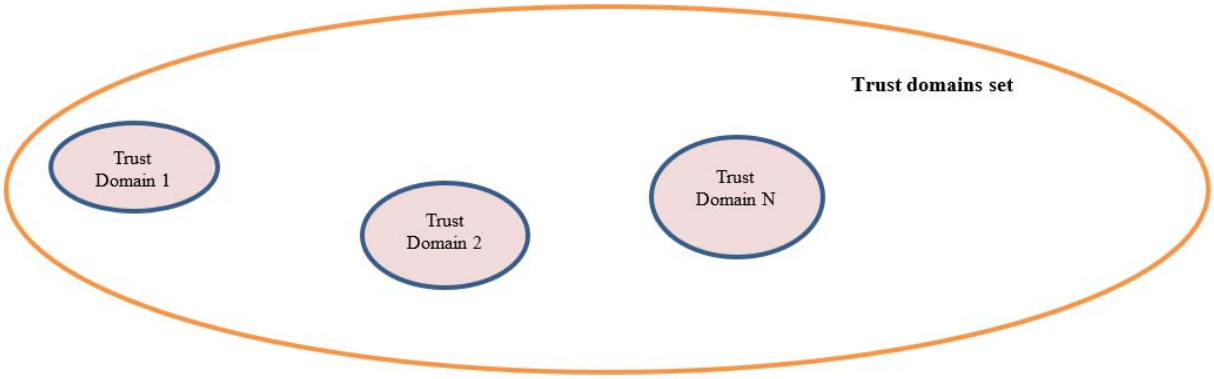

Figure B.2: Trust domains set

Figure B.2 shows a set of generic trust domains.

Each trust domain is composed of a list of REMS trusted by design.

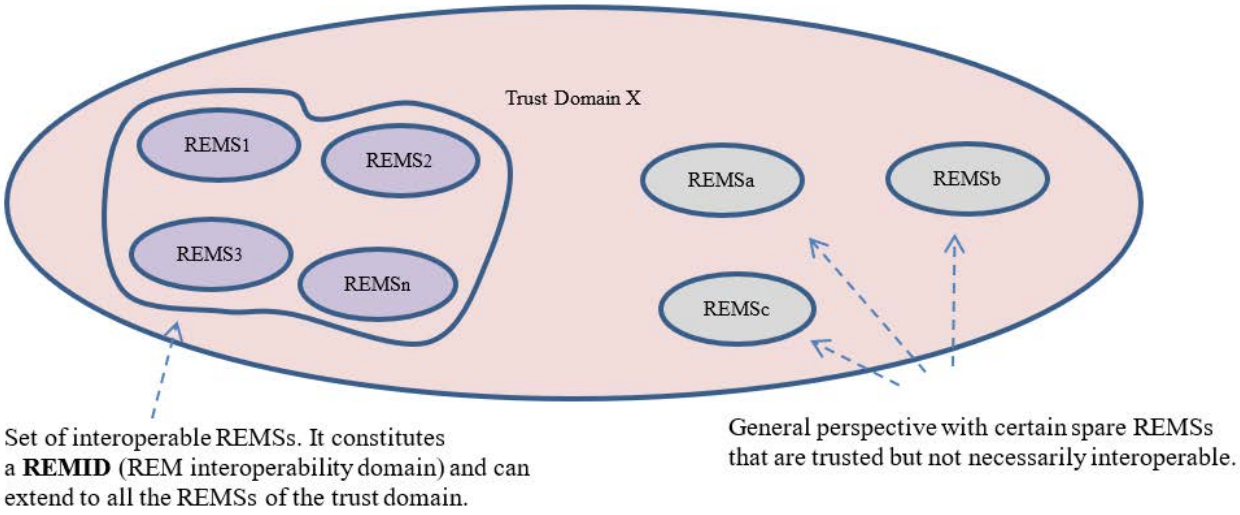

Figure B.3: Selection of interoperable REMS)

Figure B.4 actualizes the general view illustrated in figure B.3 in a trust domain where all REMS are interoperable.

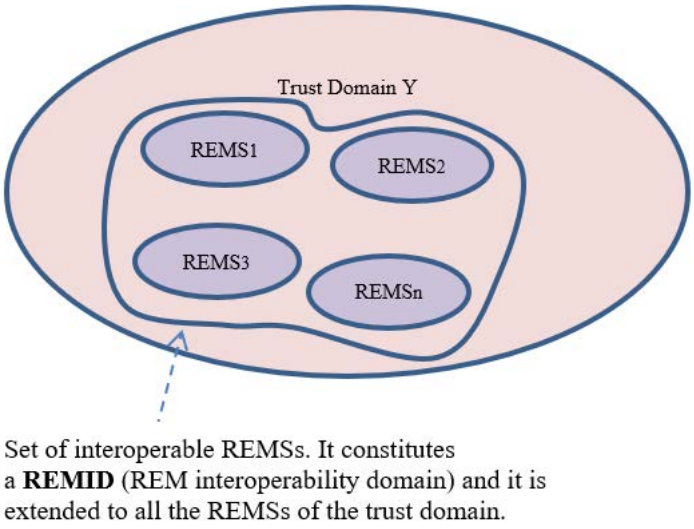

Figure B.4: REM interoperability domain (REMID)

A REM interoperability domain (REMID) is composed of a set of REMSs that enjoy the property to be interoperable. In particular, it can coincide with the entire trust domain when all participants REMSs are interoperable.

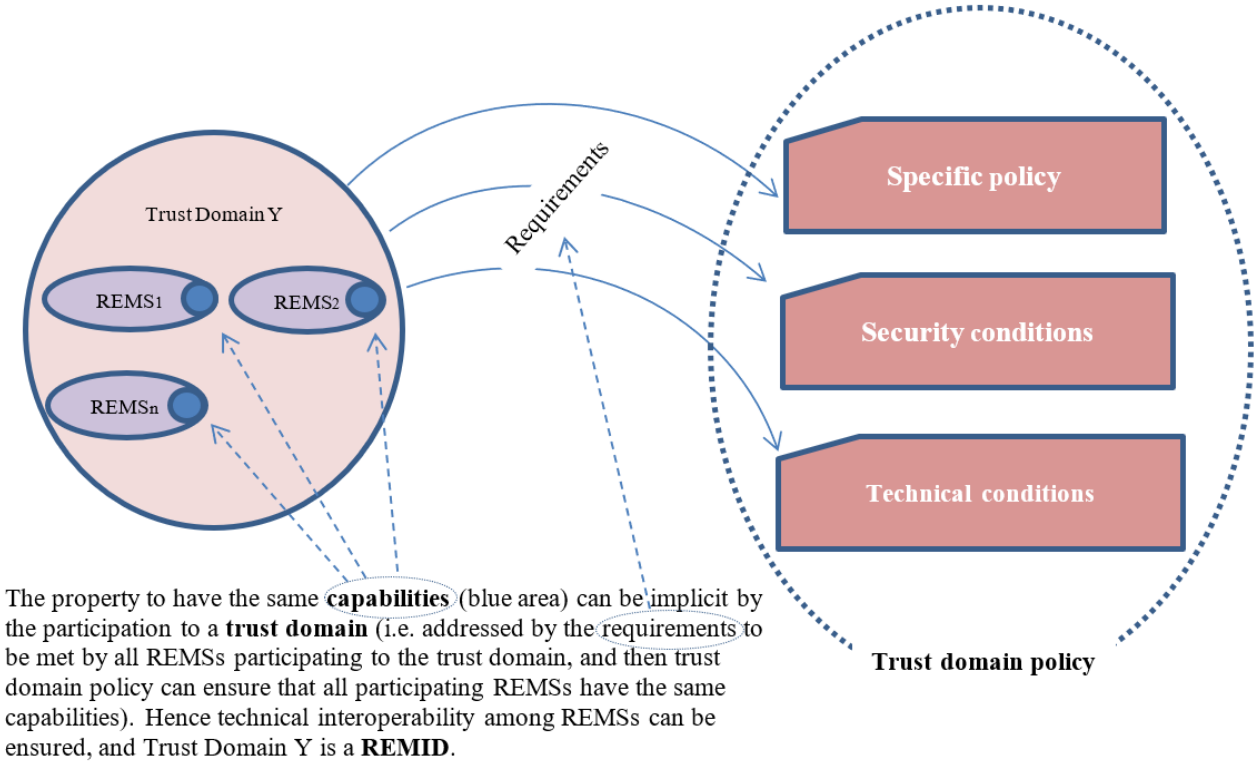

Figure B.5: Trust domain policy

The interoperability among a set of REMSs is practicable when all REMSs have the same capabilities. The trust domain policy can ensure that all participating REMSs to a trust domain have the same capabilities. In this case, such a trust domain is a REMID.

All the REMIDs that comply with the REM baseline are interoperable.

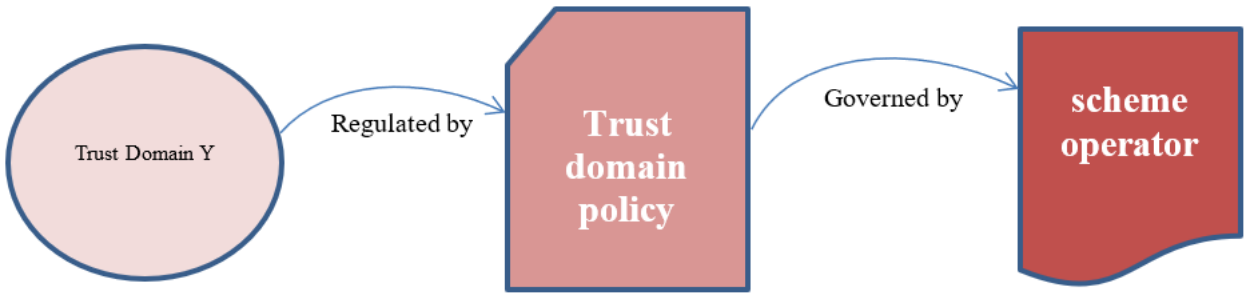

Figure B.6: Governance of trust domain policy

CONCLUSIONS: considering the rationales of table B.2 and summarizing:

As illustrated in figure B.6 a **trust domain** is **regulated** by a "**trust domain policy**".

For the purpose of REM baseline, the **governance** is operated by "**scheme operator**" regarding the **policy** and conditions for a REMS to join the **trust domain**. The **Scheme Operator** is the **entity** in charge of establishing, publishing, signing and maintaining the **Trusted Lists** (see table B.3 and table B.6 for the details). Whereas regarding the policy and conditions for a REMS to join the **REMID** (among others, the adherence to the **REMID policy**), the **REMID authority** operates the governance. The **REMID authority** is the entity in charge of signing and maintaining the **REMID policy**.

Table B.3: Trust domain and qualified services rationales

Nº	Statement	Reference	Derived rationales
1	*"The present document provides **requirements** for **establishment of trust domains** by use of the **EU Trusted List system**, by use of a **domain specific trusted list**, and by a domain specific PKI.*	ETSI EN 319 522-4-3 [11], clause 7.1	
2	***An ERDS that has been granted status as a qualified trust service** according to Regulation (EU) No 910/2014, i.e. the service is a QERDS, **shall be listed in the EU Trusted List system** established in accordance with article 22 of Regulation (EU) No 910/2014.*	ETSI EN 319 522-4-3 [11], clause 7.2	
3	***The Commission** implementing decision (EU) 2015/1505 **specifies the format of the national Trusted Lists based on ETSI TS 119 612.*** *The following service type identifiers (tsl:**ServiceTypeIdentifier**) URLs are supported for a (Q)ERDS according to ETSI TS 119 612 []:* • *http://uri.etsi.org/TrstSvc/Svctype/EDS/Q - A qualified electronic registered delivery service providing qualified registered electronic deliveries **in accordance with the applicable national legislation** in the territory identified by the TL Scheme territory or with Regulation (EU) No 910/2014 [] whichever is in force at the time of provision.* • ***http://uri.etsi.org/TrstSvc/Svctype/EDS/REM/Q -** A **qualified** electronic registered mail delivery service providing **qualified** electronic registered mail deliveries **in accordance with the applicable national legislation** in the territory identified by the TL Scheme territory **or with Regulation (EU) No 910/2014 []** whichever is in force at the time of provision.*	ETSI EN 319 522-4-3 [11], clause 7.2	

Nº	Statement	Reference	Derived rationales
	• *http://uri.etsi.org/TrstSvc/Svctype/EDS - An electronic registered delivery service, not qualified.* • ***http://uri.etsi.org/TrstSvc/Svctype/EDS/REM** - A Registered Electronic Mail delivery service, not qualified.*		Trust domains, established by use of the EU Member States Trusted List Framework (named also **EU Trusted List system** in the standard, see statement 1 at side) take the benefits of an infrastructure already deployed. This property, together the rationales of the present column contribute in the normative part of Annex C, for the definition of the REM baseline. Under this basis, and as per statement 2 in row 2, column 2, REMSs have the status of **qualified trust service** when listed as qualified within **EU Trusted List system**. A qualified REMSP is listed with the ServiceTypeIdentifier **Svctype/EDS/REM/Q - qualified electronic registered mail delivery services QREMSs**. The establishment of a trust domain is an abstraction aiming to capture, amongst others, the **intention** of the Regulation (EU) No 910/2014 [i.1] that **all qualified trust services are trusted**. In fact, a trust domain is not **directly** specified, with a tag or a specific element for example, in TL entries but, at the most, it is **indirectly** referenced in TL by the ServiceTypeIdentifier element. The most general **trust domain**, of the two first bullets of the statement 4 of the first column, including all qualified trusted services is "**All QERDSs**". This trust domain includes: • Svctype/EDS/Q - qualified electronic registered delivery services QERDSs; and • **Svctype/EDS/REM/Q - qualified electronic registered mail delivery services QREMSs** So, "**All QERDSs**" definition (that is a term used only in EU) includes also the services registered for the trust domain "All qualified REM services". As a consequence of the aforementioned rationales all the qualified REMSs registered according to the EU TL element with **ServiceTypeIdentifier** set to **http://uri.etsi.org/TrstSvc/Svctype/EDS/REM/Q** are trusted by definition and also belong to "**All QERDSs**" trust domain. NOTE: On the side, clarifies that the adhesion to the "**All QERDSs**" (that by design includes both EDS/Q and EDS/REM/Q) means having qualified services. Whereas interoperability is matter of technology and the capabilities choices.
4	*Where Regulation (EU) No 910/2014 [] is in force, the following **trust domains** may be established:* • ***All QERDSs** shall be trusted, meaning all services registered according to the two first bullet points above.* • *All non-REM QERDSs shall be trusted, meaning all services registered according to the first bullet point in the previous list.* • *All qualified REM services shall be trusted, meaning all services registered according to the second bullet point in the previous list.* • *To any of the trust domains in the previous bullet points, add non-qualified ERDSs and/or non-qualified REM services listed in the EU Trusted List system that shall be trusted.* *NOTE 1: The **intention** of Regulation (EU) No 910/2014 is that **all qualified trust services are trusted**. A different question is to what extent the Regulation requires QERDS providers to trust one another for ERD message relaying. It may be argued that a trust domain consisting of all QERDSs (the first bullet point above) is reasonable, and that the technology dependent trust domains of qualified non-REM or REM services (second and third bullet points) are not relevant since these are restrictions that are a matter of capabilities of the QERDSs rather than lack of trust."*	ETSI EN 319 522-4-3 [11], clause 7.2	

NOTE 1: The REM baseline can be established by a TL with different provisions outside the EU Member States Trusted List framework.

CONCLUSIONS: considering, together, the rationales of table B.2 and table B.3 and summarizing:

- A trust domain (and so also "**All QERDSs**" trust domain) is constituted by defining of the membership properties and conditions for a REMS to join.
- A **REM interoperability domain** (**REMID**) is a subset of the trust domain where the participants meet a set of provisions to have the same capability for achieving technical interoperability. A REMID can be the trust domain if the **trust domain policy** includes the provisions as mentioned earlier (see also figure B.5).
- The provisions specified in the REM baseline, allows to build a REMID.

NOTE 2: These conditions include the definition of a REMID within the "**All QERDSs**" trust domain. Therefore, this REMID would be formed by qualified and interoperable REMSP (see figure B.7).

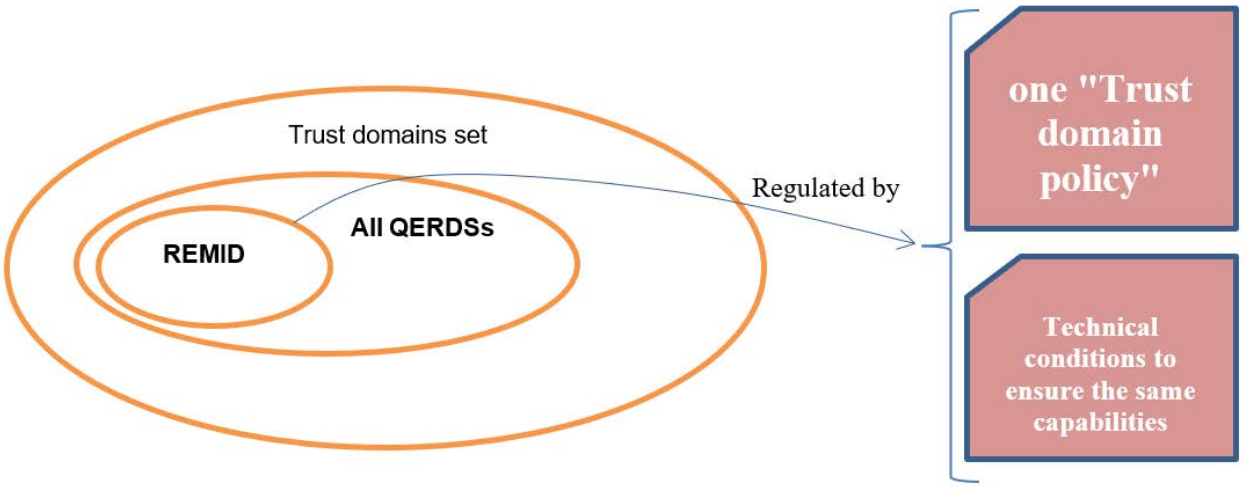

Figure B.7: REMID of qualified, trusted and interoperable REMSs

Further details on Trusted List structure are useful to introduce the rationales that connect REM concepts with TL usage possibilities.

As defined in ETSI TS 119 612 [12] the Trusted List have a set of components in a structured relationship. Essentially:

Schema (1..1)

TSPs (1..n)

SERVICEs (1..n)

A TSP is mainly structured as follows:

INFORMATION (4 elements)

TSP information extensions (1..n)

A SERVICE is mainly structured as follows:

INFORMATION (8 elements)

Service information extensions (1..n)

As further specified in ETSI TS 119 612 [12], clause 5.5.7 the Service Supply Point can be used to provide specific service-related information.

In particular, for REM baseline, the Service Supply Point is used to reference an XML document containing the technical information and conditions regarding the service capabilities (see table B.9 for details).

Table B.4: Trust establishment and digital identities rationales

Nº	Statement	Reference	Derived rationales
1	*"The service digital identity element (tsl:ServiceDigitalIdentity/tsl:DigitalId) of a (Q)ERDS in the EU Trusted List system shall be one of the following:* *1) A single certificate used by the ERDS for digital signing of all ERD messages and ERD evidences.* ***2) A single CA certificate that shall be used solely for the purpose of issuing certificates to components of the ERDS for digital signing of ERD messages and/or ERD evidences**.* *Use of a single signing certificate as service digital identity is only applicable where the ERDS is **a centralized service**, or where it is feasible to replicate the private key corresponding to the certificate to all components of the ERDS where digital signing will take place.*	ETSI EN 319 522-4-3 [11], clause 7.2	TL allows in its structure **only one** (or **more than one**, but with identical subject and representing the same public key) per service digital identity certificate. This implies that even if a **subordinate CA** certificate, having the **purpose** mentioned in statement 1, seems the suitable choice as service digital identity, in the case of ERDS, it is not always the best option. Firstly (due to its flexibility and cost efficiency) it is better to use, as service digital identity, the certificate used for ERD messages and ERDS evidence signatures. Furthermore, signatures with certificates issued in the path of a Root CA certificate (having a general scope) represent often the reality. But it is unlikely that these Root CA certificates have the required **purpose** mentioned in statement 1. It follows that it would be make sense that the service digital identity certificates are issued by a subordinate/intermediate CA certificate (issued and in the path of a general Root CA as per the previous indent), having the **purpose** mentioned in statement 1. So, in conclusion, the derived rationale is that, for the purposes of the REM baseline, the service digital identities are represented in TL only by single terminal leaves certificates. See also best practice in clause D.2.2 for other details on type of certificates and certification path that are out of scope with regards to the interoperability.
2	*When a **CA certificate** is used as **service digital identity**, this may be a root CA or **subordinate CA** certificate, and there may be a hierarchy of subordinate CAs underneath the CA. An ERD **message** or ERD **evidence** digitally **signed** using a subject certificate that has a **path to the CA certificate** used as **service digital identity shall be regarded as being digitally signed by the ERDS**. I.e. all subject certificates issued under this CA are authorized to sign ERD messages and ERD evidences on behalf of the ERDS.*	ETSI EN 319 522-4-3 [11], clause 7.2	
3	***Service digital identity*** *This field shall be present.* *It specifies **one and only one service digital identifier** uniquely and unambiguously identifying the service with the type it is associated to (as identified in 'Service type identifier', clause 5.5.1).* *When not using PKI […omissis…].* *When using PKI public-key technology, **a tuple giving**:* *- **one** or more **X509Certificate elements expressed in Base64 encoded format as specified in XML-Signature*** *- optionally, **one X509SubjectName element that contains a Distinguished Name encoded as established by XML-Signature*** *- optionally, a public key value expressed as a ds:KeyValue element* *- optionally, **a public key identifier expressed as an X.509 certificate Subject Key Identifier (X509SKI element) as specified in XML-Signature**.*	ETSI TS 119 612 [12], clause 5.5.3	
4	*The service digital identifier shall be specified by at least one representation of this digital identifier. To represent this public key, implementations:* ▪ *shall use at least one X509Certificate element [] representing the same public key. It should be represented by exactly one certificate. The TLSO may list **more than one** certificate to represent the public key, but only when all those certificates relate to the same public key and have identical subject names identifying the TSP identified in clause 5.4.1 as holder of the key. […omissis…]* *If public key representations are present more than once, all variants shall refer to the same public key.*	ETSI TS 119 612 [12], clause 5.5.3	

Nº	Statement	Reference	Derived rationales
5	*Service digital identity (as per clause 5.5.3 of ETSI TS 119 612 []); […omissis…] This element shall contain an X.509 certificate, which shall be one of the following:* • ***A single certificate** used by the REMS for digital signing of all REM messages and ERDS evidence.* • *A single CA certificate that is used solely for the purpose of issuing certificates to components of the REMS for digital signing of REM messages and/or ERDS evidence.* *This element may contain optionally the corresponding X509SKI element."*	ETSI EN 319 532-3 [6], clause 9.3	

Table B.5: Trust validation rationales

Nº	Statement	Reference	Derived rationales
1	*"For the trust information bindings specified in clauses 7.2 to 7.3, the **information retrieved from the ServiceEndpoint** shall be used by verifying that either:* • ***the certificate is the service digital identity of an ERDS included in a relevant TSL**; or* • ***the certificate has a path to a CA certificate that is the service digital identity of an ERDS in a relevant TSL**.*	ETSI EN 319 522-4-3 [11], clause 7.1	As per ETSI EN 319 522-4-3 [11], clause 7.1, the information retrieved from the **ServiceEndpoint** is used to **verify** the **service digital identity** certificate maintained in TL (**directly** or because it is within the **certificate path** up to the CA). For the purposes of the REM baseline, the first option mentioned in statement 1 at the side is used: **the certificate is the service digital identity** of a REMS directly included in TL. The **ServiceEndpoint** is represented in the Trusted List by the **Service supply point**/**ServiceSupplyPoint** element (see ETSI TS 119 612 [12], clause 5.5.7). See table C.5 of clause C.2.3.3.2 for the REM baseline implementation details.
2	***To establish trust** in an ERDS based on information in a **TL**, an actor, which may be another ERDS, **shall validate the ERDS's digital signature on an ERD message** or ERD **evidence**, **verify** that the signing certificate can be **linked** to the **service digital identity** in the **TL**, **verify** that the **service current status** is "**granted**", and **verify** that the **service type identifier** is set **according** to the **requirements** of the **applicable trust domain**. If this process is applied **to evaluate trust** at a time in the past, the process shall use the information (signature validity and service information in the TL) that was valid at that point in time.*	ETSI EN 319 522-4-3 [11], clause 7.2	
3	*In REM, the identifier of a recipient is an email address. The domain part of this email address shall identify the REMS responsible for that domain (of which the recipient is a subscriber): R-REMS. [..omissis..]* *The hostname provided **should be the same as the one included in a URI contained in the Service supply point** of the TL entry (see clause 9.3 of ETSI EN 319 532-3 []), if the REMS uses TL to publish trust information about itself and the Service supply point element is present."*	ETSI EN 319 532-2 [5], clause 9.4.2	

Table B.6: Trust and TL scheme rationales

Nº	Statement	Reference	Derived rationales
1	*"Trusted Lists may be used in other contexts than that **governed** by Regulation (EU) No 910/2014 []. A **domain TL** providing information on ERDSPs/ERDSs **shall** adhere to the specifications of clause 7.2 above except for the following amended requirements.* *The **TL shall be formatted** according to ETSI TS 119 612 [].* *A **Trusted List scheme shall define the conditions** that have to be met in order for a trust service provider and its services to be listed. The Trusted List scheme **shall be published** as required by ETSI TS 119 612 [], clause 5.3.* *A scheme **limiting** the TL to only contain ERDSPs/ERDSs may be used, or a scheme where ERDSPs/ERDSs are listed along with other types of services.* *A **Trusted List Scheme Operator** shall be **assigned and identified** as required by ETSI TS 119 612 [], clause 5.3.* ***Service type identifiers** shall be as **specified** in clause 7.2, but the **Trusted List scheme may restrict allowed service type identifiers to be a subset** of those defined. **If a service type identifier indicates a qualified ERDS or REM service, then the Trusted List scheme shall unambiguously identify the legislation that the qualified status refers to**.*	ETSI EN 319 522-4-3 [11], clause 7.3	In the contexts **governed** by Regulation (EU) No 910/2014 [i.1] the EU Member States Trusted List Framework is used (see note). It has already been defined and managed as follows (see note): • a specific **format** • a TL **scheme** • TL scheme **publication** • a TL **Scheme Operator** assignment & identification • the definition of possible **limitations** of the TL scheme • definition of possible restrictions to the ServiceTypeIdentifier (an admitted subset of values) • unambiguous identification of the legislation that the qualified status refers to. **Summarizing, the key concepts for the REM baseline, are:** • The **trust domains** within which the TL scheme will operate are defined in ETSI EN 319 522-4-3 [11], clause 7.2 (see rationales derived from requirement 4 of table B.3 for the baseline value and table C.2 for the implementation). • The **ServiceTypeIdentifier** (see rationales derived from requirement 3 of table B.3 for the baseline value and table C.3 for the implementation). • The **Trusted List scheme** defines all the requirements and measures usable for trust assertion (see table C.6). • The **Trusted List Scheme Operator** (e.g. for governmental administrative agencies) specifies the legal **entity** in charge of establishing, publishing, signing and maintaining the trusted list for each Member State (see clause C.2.3.5 for the implementation).
2	***Scheme operator name*** *Description: It specifies the **name of the entity** in charge of establishing, publishing, signing and maintaining the trusted list. …* *Value: The name of the scheme operator shall be the formal name under which the associated legal entity or mandated entity (e.g. for governmental administrative agencies) associated with the legal entity in charge of establishing, publishing and maintaining the trusted list operates. It shall be the name used in formal legal registration or authorization and to which any formal communication should be addressed."*	ETSI TS 119 612 [12], clause 5.3.5	
NOTE: The case illustrated in the present table is an element fully defined by a piece of regulation in the EU, and the present document focuses on it. In the case of contexts different from the EU TL framework, the list of elements already addressed, as initial work for EU framework, need to be duplicated; most of the ones it will be devoted to activities around TL scheme definition and management.			

B.2.2.4 Capability discovery and management

Table B.7: Capability and metadata rationales

<table>
<tr><th>Nº</th><th>Statement</th><th>Reference</th><th>Derived rationales</th></tr>
<tr><td>1</td><td>"Capability management provides the functionality to resolve the unique identifier of a recipient into:
1) Identification of the R-REMS of which the recipient is a subscriber
2) Metadata for the capabilities of the identified REMS
3) Metadata for the capabilities of the recipient in the R-REMS</td><td>ETSI EN 319 532-2 [5], clause 9.4.1</td><td rowspan="3">The concepts involved in these rationales are:
• REMS metadata and REMS capability
• Recipient's metadata and recipient's capability

The objective of the present rationales is to identify the "capabilities" that represents the basis for interoperability.

It is noted that:
• Only the capabilities at REMS level are interesting for interoperability (see note 1).
• The recipient's email address represents the link from S-REMS to R-REMS. And this element is part of the recipient's metadata.

According to statement 1 at the side, the unique identifier of a recipient (through Capability management) is mapped to:
• the identifier of R-REMS and
• the metadata of R-REMS (used to specify the R-REMS capabilities);

According to statement 3 at side, the relay of a REM message from S-REMS to R-REMS requires an assessment on constraints and options respected by both REMSs, and exhibited by their capabilities. This assessment is implicitly ensured if both S-REMS and R-REMS have the same capabilities; nevertheless, it needs to be in some way validated with a specific process (see note 2).

The CSI (through capability management) provides these mapping functionalities to individuate R-REMS capabilities.

As outlined in the CONCLUSIONS on pages 29 and 31: a particular trust domain policy with the additional provisions ensuring the same capabilities (for REMSs that will adopt it) can regulate a REM interoperability domain (REMID).

The capabilities, common to all REMSs of the abovementioned REMID, are collected and referenced from EU Trusted List without the need of extensions of the Trusted List scheme (see table C.6 of clause C.2.3.4.1 and table C.8 of clause C.2.3.4.2 for the implementation).</td></tr>
<tr><td>2</td><td>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. […omissis…] 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) […omissis…]
3) […omissis…]</td><td>ETSI EN 319 522-2 [2], clause 9.4.3</td></tr>
<tr><td>3</td><td>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."</td><td>ETSI EN 319 522-2 [2], clause 9.4.4</td></tr>
<tr><td colspan="4">NOTE 1: It is unnecessary to consider the user's capability for REM baseline interoperability purposes. It is noted that user's capability verification is simplified when the capabilities are grouped at the service level. According to statement 2 above, the capabilities of a recipient can be implicit from the R-REMS metadata; the conditions for becoming a subscriber of a REMS can require all subscribers to fulfil certain requirements. So, in this case, the service capabilities also represent the subscribers' capabilities. This property is important just in case any of these subscribers capabilities would affect the interoperability. At the level of REM baseline, there are not provisions to manage users capabilities.
NOTE 2: This is necessary during the "once only" registration phase at the REMID authority, but also, as a further consistency validation step, during the day-by-day run-time recognition phases of R-REMS from S-REMS.</td></tr>
</table>

Table B.8: Capability referencing in TL for publication rationales

Nº	Statement	Reference	Derived rationales
1	*"If the REMS uses TL to publish trust information about itself, the REMS capability metadata may also be published using the TL, as indicated for ERDS capability metadata in clause 7.2 of ETSI EN 319 522-4-3 []. In this case the options given in Table 14 may be used.* *[see next statement nr. 2]*	ETSI EN 319 532-3 [6], clause 9.4	For REM baseline, **REMS capability metadata** have to be referenced by TL and made accessible, in a downloadable form, by the **ServiceSupplyPoint** element of TL. See table B.9 for details on downloading rationales. Statement 1 at side specifies that a REMS, when using TL to publish trust information, can also use Trusted List to publish **REMS capability metadata**. To avoid any extension to the TL schema, the necessary information for the implementation of the REM baseline are published by reference, indirectly. The Transport Layer Security (TLS) mechanism (on the REMS **ServiceEndpoint** represented by the **ServiceSupplyPoint** element of TL, as seen in rationales of table B.5) is based on a set of security information (namely: security metadata or **REMS capability-based security**). So, with a similar mechanism like that used for **REMS capability metadata**, the Transport Layer Security (TLS) digital certificate of REMS, as part of **REMS capability-based security**, can be made accessible by reference, in a downloadable form, by the **ServiceSupplyPoint** element of TL, according to the statement 3 at side. Regarding the implementation, see table C.5 of clause C.2.3.3.2 for the requirements about the ServiceSupplyPoint, clause C.2.3.4.1 for the capabilities general requirements, clause C.2.3.4.2 for the specific part of REMS capability metadata and clause C.2.3.4.4 for the specific part of REMS capability-based security.
2	*[Options from table 14 of 532-3]* *If present, the additionalServiceInformation field, as per clause 5.5.9.4 of ETSI TS 119 612 [], may contain a URI, where the REMS capability metadata is downloadable, or alternatively, it may embed the REMS capability metadata structure itself (if it is in XML format)."*	ETSI EN 319 532-3 [6], clause 9.4	
3	*[Options from table 14 of 532-3]* *If present, ServiceSupplyPoint field may contain URIs, where the REMS capability and security metadata are downloadable.*	ETSI EN 319 532-3 [6], clause 9.4	

Table B.9: Capability downloadable from TL rationales

Nº	Statement	Reference	Derived rationales
1	*"ERDS metadata may be published as a service information extension in a TSL according to clause 5.5.9 of ETSI TS 119 612 []*	ETSI EN 319 522-3 [3], clause 6.3.2	For REM baseline **REMS capability metadata** have to be downloadable by the **ServiceSupplyPoint** field of TL Service information element (see figure B.8). Since the **ServiceSupplyPoint** TL element is per-service, the capabilities are closely bound to REMS (and not to the scheme level). To ensure the same capabilities on the trust domain relevant to the REM baseline, all the REMS capability metadata have to be the same for all the REMSs that meet the requirements of REM baseline. So, with regards to **REMS capability metadata** (clause C.2.3.4.2) and, similarly, as introduced in table B.8 rationales, for **REMS capability-based security** (clause C.2.3.4.4), the **ServiceSupplyPoint** TL element represents the URI where to download the whole XML structure, for **capability** and **security** metadata information (see figure B.8 and clause C.2.3.4.1). See table C.5 of clause C.2.3.3.2 for the implementation details regarding the ServiceSupplyPoint.
2	*5.6.6 Service information extensions* *Presence: This field is optional.* *Description: It may be used by TLSOs to provide specific service-related information, to be interpreted according to the specific scheme's rules, with the Format and Value used in clause 5.5.9."*	ETSI TS 119 612 [12], clause 5.5.6	

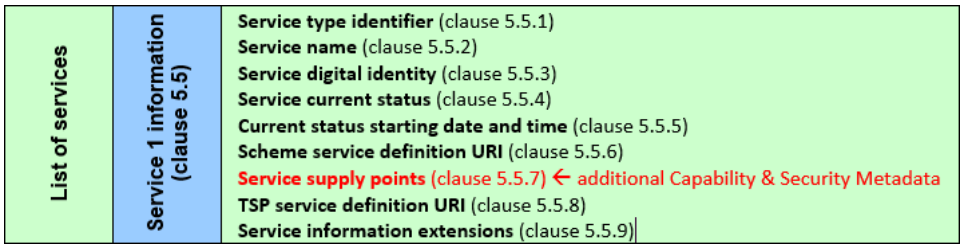

Figure B.8: Service supply points information of Trusted List for additional metadata

Table B.10: Capability discovery rationales

Nº	Statement	Reference	Derived rationales
1	*"Metadata related to the **user content**, […omissis…] are provided for purposes of handling and processing a message, […omissis…], or also for service **capabilities discovery**."*	ETSI EN 319 532-2 [5], clause 4.1	In REM, the metadata related to the user content is represented by the "header section" of the original message: the submission metadata (See ETSI EN 319 532-3 [6], figure A.1). Inside submission metadata, there is the recipient of the REM message. The domain part of the recipient's email address is used to individuate the R-REMS capabilities (see the derived rationales of table B.7).

Table B.11: Individuation of recipient's REM service rationales

Nº	Statement	Reference	Derived rationales
1	*"9.4.2 Resolving recipient identification to ERDS identification* *In REM, the identifier of a recipient is an email address. The domain part of this email address shall identify the REMS responsible for that domain (of which the recipient is a subscriber): R-REMS.* *If the REMS supports receiving relayed messages from other REMS (i.e. it can act as I-REMS or R-REMS in a chain of REMSs) using SMTP, then the REMS should ensure that the hostname of the server providing the REM RI is available in MX records of the DNS to all other REMSs, which need to relay messages to this REMS. The hostname provided* ***should be the same as the one included in a URI contained in the Service supply point*** *of the TL entry (see clause 9.3 of ETSI EN 319 532-3 []), if the REMS uses TL to publish trust information about itself and the Service supply point element is present.*	ETSI EN 319 532-2 [5], clause 9.4.2	The individuation of the recipient's REMS is implemented using the domain part of the recipient's email address of a REM message. The hostname configured in MX records of such domain is the same configured in the ServiceSupplyPoint element of the Trusted List for that REMS. See table C.5 of clause C.2.3.3.2 for the REM baseline implementation details.
2	*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."*	ETSI EN 319 522-2 [2], clause 9.4.2	

B.2.2.5 Governance support

The governance (supporting a REMID) addresses, typically, at least the following tasks:

- Publication of the REMID policy.
- Ensuring the publication of capabilities and security metadata by any REMS belonging to the REMID.
- Ensuring that the Trusted List section of any REMS references the capabilities as mentioned earlier characterizing the REMID.

This task is typically accomplished by the REMID authority. See clause C.2.3.5 for the requirements in the context of REM baseline.

B.3 Digital signatures and time-stamp

B.3.1 Overview

The present clause illustrates the approach adopted in identifying the solutions defined in clauses C.3 and C.4 to address the digital signatures and time-stamp application requirements in **REM messaging**. The definitions of digital signatures and time-stamp application connote a strong impact in terms of interoperability. For this reason, this subject is dealt with starting in a general way, covering the lack of common rules with other e-delivery services.

One of the key points to address interoperability is the format of the exchanged data and of the evidence (in essence: "what" it is exchanged, by whom and how to prove it).

The data format is addressed by definition in REM data structures since it uses a widespread email and standard format. The evidence, realized by means of the ERDS evidence structure, represents an auto-consistent and common foundational component between different e-delivery solutions.

Moreover, new ERDS elements are defined to cover certain peculiarities of REM baseline. These are adequate to hold information that makes it possible to discriminate and correctly manage the variability of determined situations over the course of execution of the flows in their completeness.

For such information that cannot be hosted in the canonical data structures, extension mechanisms (placeholders) are provided inside the basic ERDS evidence set of components. The necessary elements are added through these extensions (see the derived rationales from statement 8 of table B.13).

Table B.12 provides, for each concept of the second column, the suggested starting reference, in the third column, with the "first" prescription (e.g. text with some provision) in the full set of standards about the concept itself. The last column contains the other normative references linked from the main reference.

While table B.13 follows the same logical structure and meanings used from table B.2 to table B.11 in clause B.2.2 and illustrated in clause B.2.2.1.

Table B.12: Digital signatures and time-stamp - normative reference map

Nº	Concept	Starting refence	Linked normative Reference(s)
1	REM data structures	ETSI EN 319 532-2 [5], clause 4.1	ETSI EN 319 522-2 [2], clause 4
		ETSI EN 319 532-3 [6], clause 4	ETSI EN 319 522-3 [3], clause 4
2	ERDS evidence digital signature	ETSI EN 319 532-2 [5], clause 7	ETSI EN 319 522-2 [2], clause 7
		ETSI EN 319 532-3 [6], clause 8.2	ETSI EN 319 522-2 [2], clause 7.2 ETSI EN 319 522-3 [3], clause 5.2.2.28
		Clause C.4.3 of the present document	ETSI EN 319 522-2 [2], clause 7.2 ETSI EN 319 132-1 [14], clause 6
3	REM message digital signature	ETSI EN 319 532-2 [5], clause 7	ETSI EN 319 522-2 [2], clause 7
		ETSI EN 319 532-3 [6], clause 8.3	ETSI EN 319 522-2 [2], clause 7.2 ETSI EN 319 522-2 [2], clause 8.2.9 ETSI EN 319 522-2 [2], clause 9.3 ETSI EN 319 122-1 [13]
		Clause C.4.2 of the present document	ETSI EN 319 532-3 [6], clause 8.3 ETSI EN 319 522-2 [2], clause 8.2.9 ETSI EN 319 122-1 [13], clause 6
4	ERDS evidence time-stamp	Clause C.4.4 of the present document	ETSI EN 319 522-2 [2], clause 7.2 ETSI EN 319 132-1 [14], clause 6
5	ERDS evidence composition	Clause C.3 of the present document	ETSI EN 319 522-2 [2], clause 8 ETSI EN 319 522-3 [3], clause 5

Table B.13: Digital signatures and time-stamp rationales

Nº	Statement	Reference	Derived rationales
1	*"For signatures that sign all the components of REM messages ETSI EN 319 522-2 [], clause 7.2 shall apply. In addition:* *1) The signature shall be applied to the message using S/MIME multipart/signed as defined in IETF RFC 5751 [].* *This signature shall protect all the MIME parts that constitute a REM message.* *2) The digital signature should be a CAdES signature according to the semantics specified in ETSI EN 319 522-2 [], clause 8.2.9.* *NOTE 1: For the purposes to cover advanced digital signature on MIME, CAdES specification provides examples of structured contents, MIME and S/MIME digital signatures in Annex D of ETSI EN 319 122-1 [].* *3) This digital signature should be a CAdES baseline signature as specified in ETSI EN 319 122-1 []. This digital signature may include the signed attribute signature-policy-identifier, containing the explicit identifier of the signature policy governing the signing and validating processes.*	ETSI EN 319 532-3 [6], clause 8.3	All REM messages' components are digitally signed by using S/MIME with a CAdES signature. **ERDS evidence** XML structures are signed as an individual document with a **XAdES** signature. A signature **time-stamp** is added to the **XAdES** digital signature of the evidence; by the B-T signature level. For the REM baseline, the **digital signature** applies to the following subtypes of REM message: **REM dispatch** and **REMS receipt**. Each of these comprises the following **basic components**: **REMS introduction**, **user content**, **ERDS evidence** according to the cardinality as defined in ETSI EN 319 532-2 [5], table 1. The events considered for such REM messages are: • SubmissionAcceptance, SubmissionRejection • RelayAcceptance, RelayRejection, • RelayFailure • ContentConsignment, ContentConsignmentFailure E01 Extensions mechanism is an optional placeholder in the canonical structure. It represents the natural way of addressing new elements in ERDS evidence without changes in the consolidated standard. See table C.15 and table C.16 of clause C.3.2 for the REM baseline implementation details.
2	*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.*	ETSI EN 319 522-2 [2], clause 7.1	
3	*For all digital signatures applied by ERDSs to ERD messages and **ERDS evidence**:* *▪ […omissis…]* *1) The digital signature should be a CAdES, **XAdES** or PAdES baseline signature as specified in ETSI EN 319 122-1 [13], ETSI EN 319 132-1 [], ETSI EN 319 142-1 [].* *▪ […omissis…]* *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 CAdES 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 timestamp 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 [], Article 44.*	ETSI EN 319 522-2 [2], clause 7.1	
4	*The **digital signature** on the REM message shall cover all the **basic components**, as defined in clause 4.1, that are included in the REM message, except for the ERDS metadata (i.e. not only the mandatory components, but also the optional ones that are present, and all occurrences of a component that is included in multiple instances).*	ETSI EN 319 532-2 [5], clause 7	

Nº	Statement	Reference	Derived rationales
5	*The **basic components** (**REMS introduction**, **user content**, ERDS relay metadata, **ERDS evidence**, REMS extension) within each of the **subtypes** of REM message that are used in REM (**REM dispatch**, REM payload, REMS notification, **REMS receipt**) **shall** have the cardinality as defined in table 1.*	ETSI EN 319 532-2 [5], clause 4.1	
6	*In **S&F** style objects **relayed** between REMSs - through the REM RI: **Relay Interface** - shall always be in the form of **REM dispatch**, REM payload or **REMS receipt***	ETSI EN 319 532-2 [5], clause 4.1	
7	*Events related to the submission: SubmissionAcceptance, SubmissionRejection* *Events related to relay between REMSs: RelayAcceptance, RelayRejection, RelayFailure* *Events related to the consignment: ContentConsignment ContentConsignmentFailure*	ETSI EN 319 532-1 [4], clause 6.2.1	
8	***E01 - Extensions**.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."*	ETSI EN 319 522-2 [2], clause 8.2.28	

B.3.2 Submission event

Figure B.9 illustrates the steps immediately after a REMS has accepted the submitted original message. The REMSP takes responsibility for trying to deliver it to all specified recipients. These steps are relevant for digital signature and time-stamp application (see ETSI EN 319 532-1 [4], clause 6.2.1).

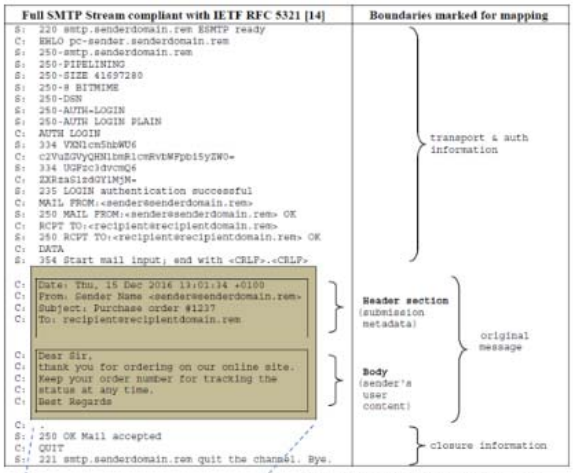

Figure A.1 ETSI EN 319 532 -3 [6]

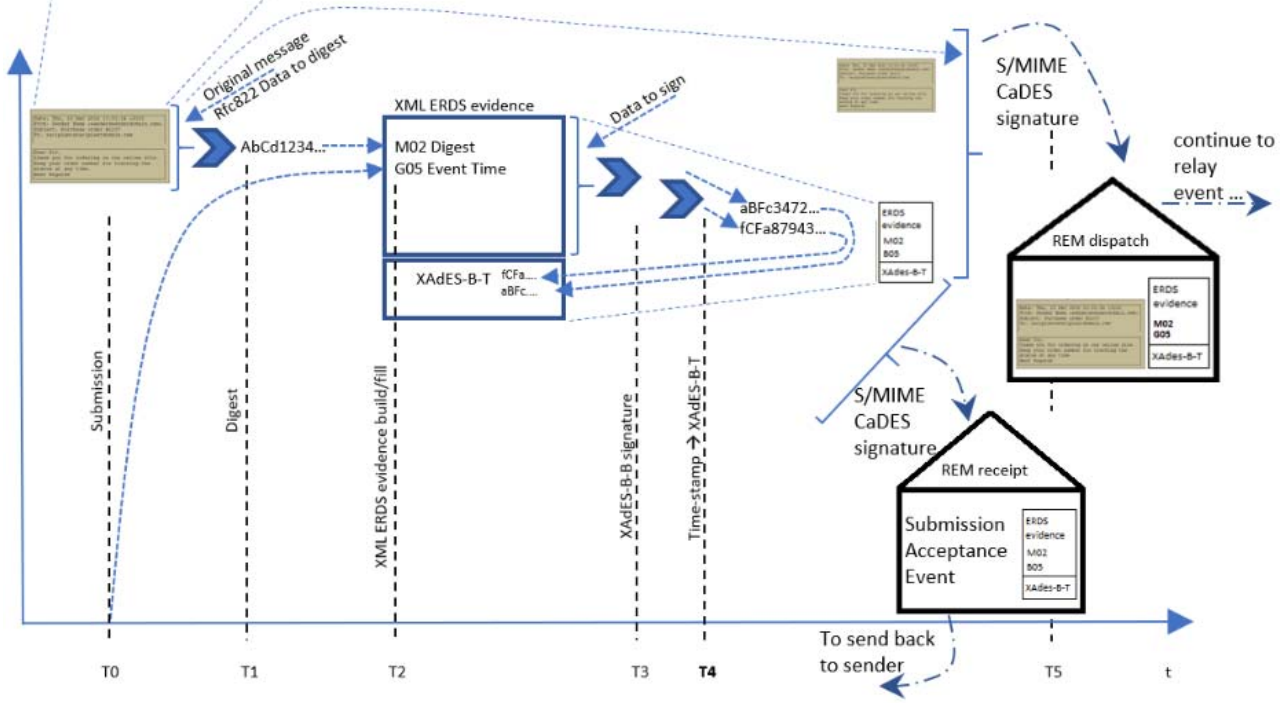

Figure B.9: Detailed submission event example

B.3.3 Relay event

Figure B.10 illustrates the steps of handing over a REM dispatch (containing the original message and the ERDS evidence) from S-REMS R-REMS through the REM relay interface using an SMTP transaction.

After a successful relay of such REM dispatch the R-REMS takes over the responsibility of handling that REM dispatch for consignment according to the steps of the consignment event (see ETSI EN 319 532-1 [4], clause 6.2.2).

R-REMS inspects the REM dispatch to decide its acceptance (verify trust in the sending REMS, check the compliance of the REM dispatch with **REMID policy** rules, security etc., as specified in clause C.2.3.3.3).

R-REMS issues ERDS evidence about acceptance/rejection of the REM dispatch, attaches the ERDS evidence to a REMS receipt and conveys this REMS receipt to the S-REMS.

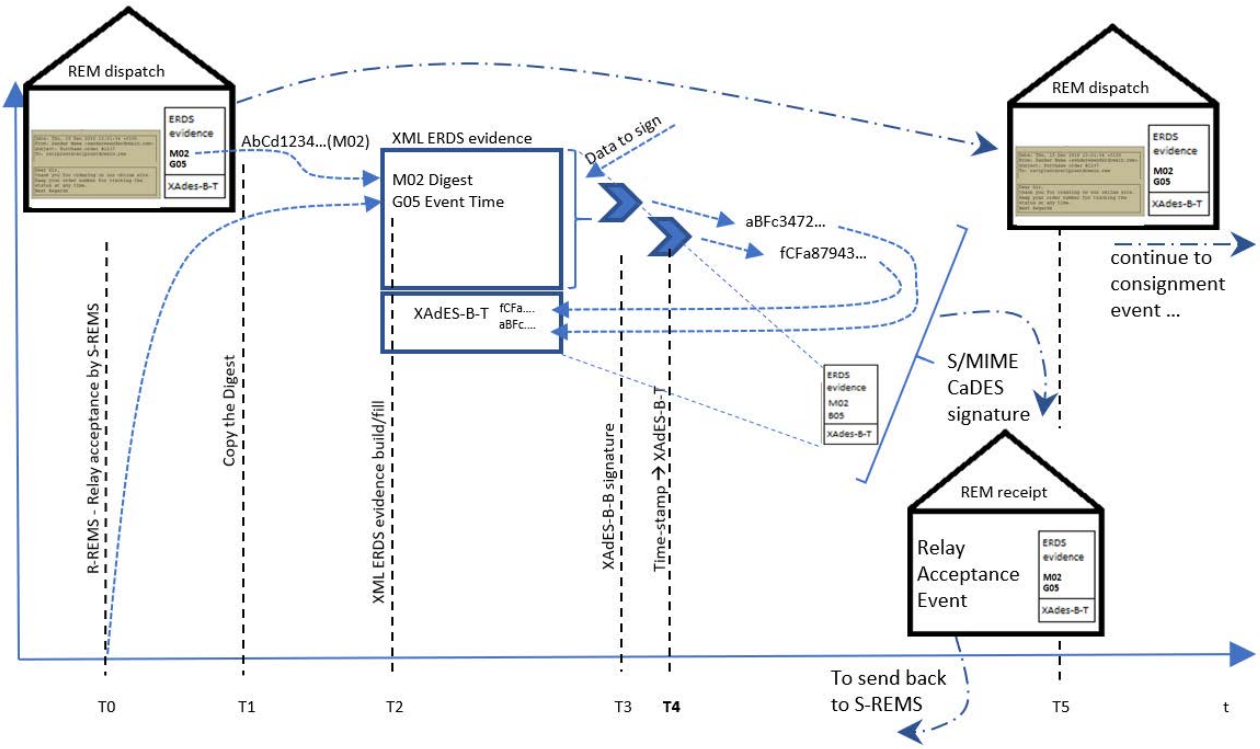

Figure B.10: Detailed relay acceptance event example (R-REMS side)

If the relay of a REM dispatch has failed then the S-REMS is responsible for issuing an ERDS evidence about the failure of the relay, attaching the ERDS evidence to a REMS receipt and convey this REMS receipt to the sender.

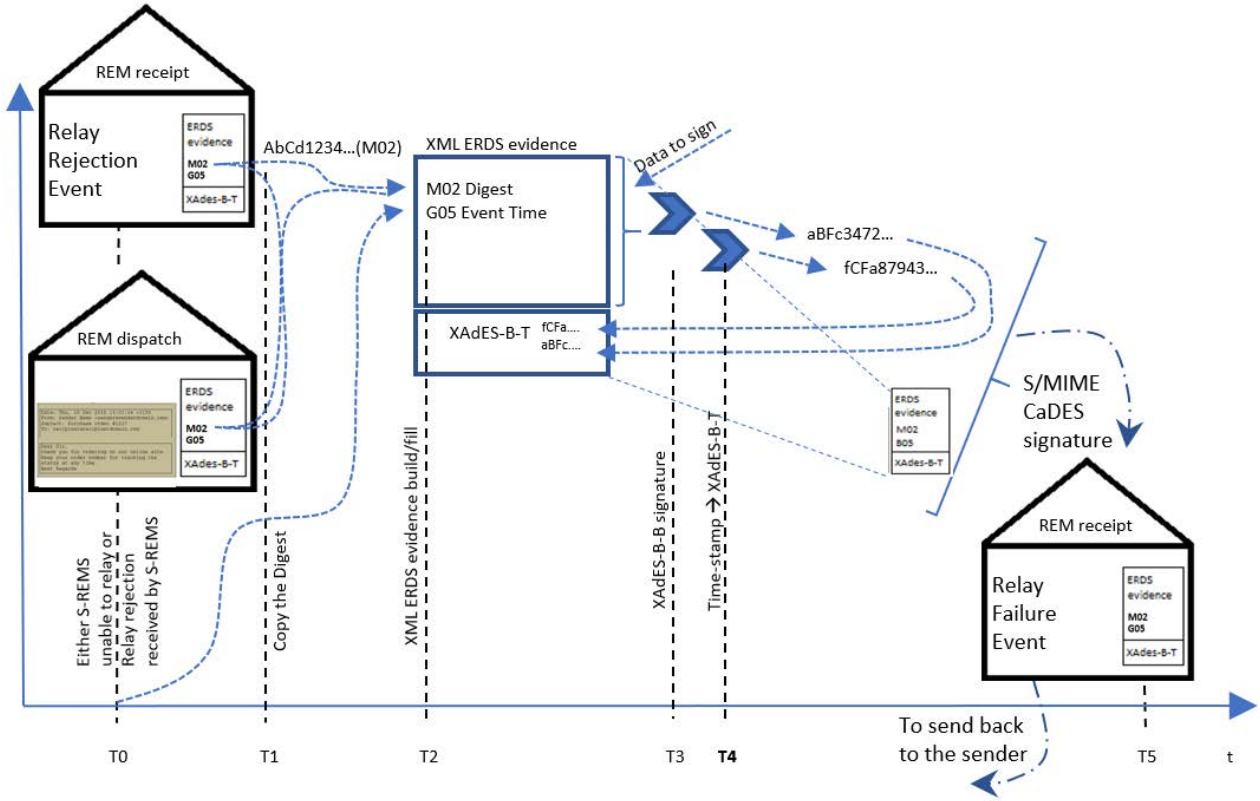

Figure B.11: Detailed relay rejection/failure events example (S-REMS side)

NOTE: The dotted lines without arrows between REM dispatch, Relay Rejection Event REMS receipt and ERDS evidence XML structures have the meaning that the M02 ERDS evidence element is the same in any place, and so it represents a correlator among these three elements.

B.3.4 Consignment event

Figure B.12 illustrates the steps immediately after a R-REMS has accepted the relayed REM dispatch from S-REMS, and the R-REMS provider takes responsibility for trying the consignment to all specified recipients. These steps are that relevant for digital signature and time-stamp application to the relevant ERDS evidence attached in REMS receipts to be sent back to the sender (see ETSI EN 319 532-1 [4], clause 6.2.4). Consignment is then performed by storing the message in a mailbox, which the recipient can access to get the REM dispatch.

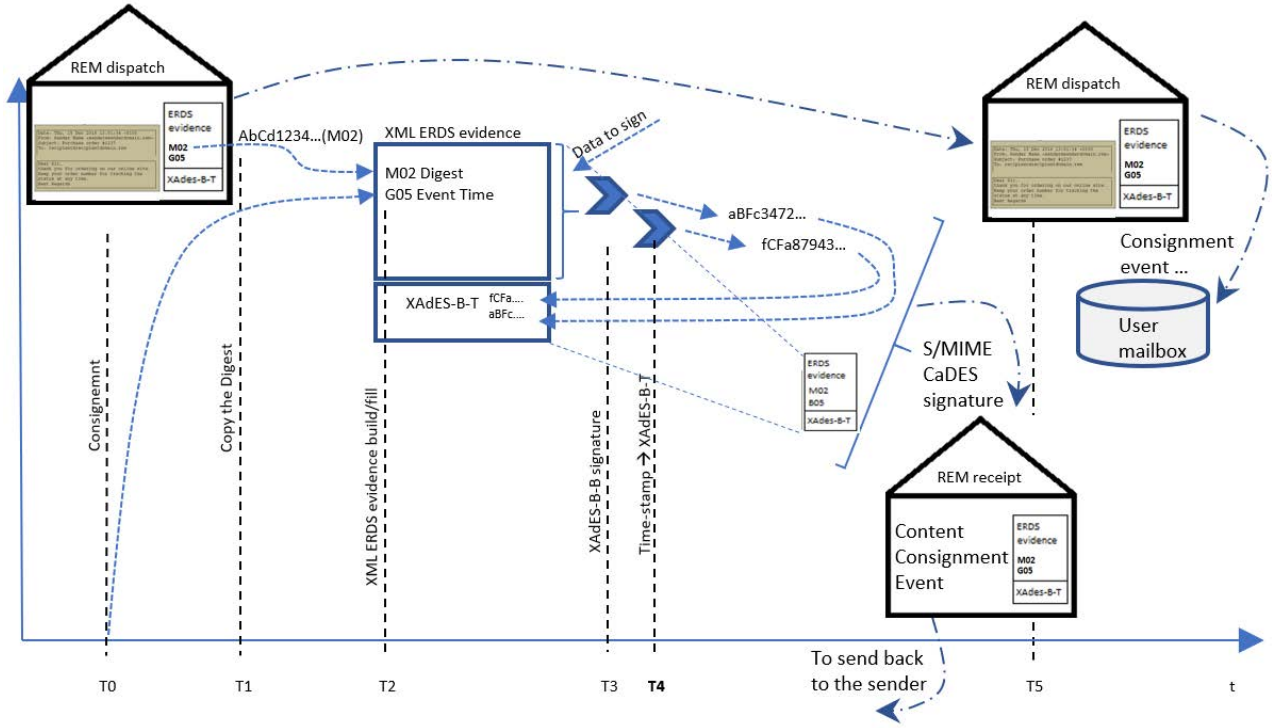

Figure B.12: Detailed consignment event example

Annex C (normative): REM baseline requirements

C.1 General requirements

The present annex defines the so-called REM baseline, which guarantees interoperability between REMS providers. It also provides the basic features needed for a wide range of business and government use cases for electronic procedures and communications to apply to a wide range of communities when there is a clear need for interoperability of registered electronic delivery services.

Unless otherwise specified in the present annex:

- Mandatory requirements in clause 5 (SMTP interoperability profile) of the present document and in the parts ETSI EN 319 532-1 [4], ETSI EN 319 532-2 [5], ETSI EN 319 532-3 [6] shall also be mandatory in REM baseline; and
- Optional requirements in clause 5 of the present document and in the parts ETSI EN 319 532-1 [4], ETSI EN 319 532-2 [5], ETSI EN 319 532-3 [6] shall not apply on REM baseline either.

Adoption of capabilities that are not part of REM baseline shall not introduce requirements that break the interoperability.

The following URI shall identify REM baseline: http://uri.etsi.org/19532/v1#/REMbaseline.

C.2 Common Service Interface (CSI)

C.2.1 Overview

Clause C.2 specifies the requirements of the Common Service Interface (CSI) in **REM messaging**.

C.2.2 General provisions

The shared technological infrastructure implementing the CSI, in a messaging context where several REMSPs need to interoperate, shall include the following functions:

1) Message Routing
2) Trust establishment
3) Capability discovery and management
4) Governance support

According to clause 5.3.4, the REM RI relay interface implements the interaction between REMS.

NOTE 1: The present version of REM baseline specifies a single type of interaction using DNS and TLS.

A REMS complying with REM baseline shall use CSI according to the basic handshake defined in clause C.2.3.

NOTE 2: The term "handshake" is used in a broad sense as "the process" that initiates the negotiations of the security details of the REM RI interface.

C.2.3 Basic handshake

C.2.3.1 Introduction

The present clause defines a basic solution to cover the CSI requirements maximizing interoperability avoiding the complexity of DNSSEC.

C.2.3.2 Message Routing

The Routing Interface implementation guidance a) of clause 5.3.5 is detailed in the present clause.

NOTE 1: This further detail is an answer to reducing the risks of cybercrime by properly securing the DNS protocol.

Table C.1: Common service interface - Routing

Nº	Service/Protocol element	ETSI EN 319 532-3 [6] main reference	Requirement	Implementation guidance	Notes
1	DNS	Clause 9.2	M	a.1), a.2), a.3)	Routing interface

Implementation guidance:

a.1) The Routing Interface, part of CSI, shall be implemented using DNS protocol.

a.2) The REMS shall ensure that the hostname of the server providing the REM RI is available in the MX records of the DNS to all other REMSs, *which need to relay messages to this REMS*; and that the hostname provided shall be the same as the one included in the URI contained in Service Supply Point, according to ETSI EN 319 532-2 [5], clause 9.4.2.

a.3) The definition of the REMID policy shall contain the measures that have to be adopted to secure the DNS.

NOTE 2: The measures to adopt include precautions, proactive prevention, and reporting techniques at the system and organizational level to protect from malicious attacks to DNS. The TLS handshake (see requirement 1 of clause 5.3.4) provides, at a different level, a further measure of protection (see also clause D.1.3).

C.2.3.3 Trust establishment

C.2.3.3.1 Trust - Trusted List general requirements

Table C.2: Common service interface - Trust

Nº	Service/Protocol element	ETSI EN 319 532-3 [6] main reference	Requirement	Implementation guidance	Notes
2.1	TL	Clause 9.3	M	b.2.1.1), b.2.1.2), b.2.1.3), b.2.1.4), b.2.1.5), b.2.1.6)	Trusting interface

Implementation guidance:

b.2.1.1) A **trust domain** within which a fully regulated ***co-operation*** among participating REMSs shall be defined for trust establishment according to ETSI EN 319 522-4-3 [11], clause 7.1 (see the derived rationales from statement 1 of table B.3 and statements 1 and 4 of table B.2).

EXAMPLE: The **trust domain** defined for the qualified electronic registered mail delivery services is established as "**All QERDSs**" trust domain, according to ETSI EN 319 522-4-3 [11], clause 7.1 (see the derived rationales from statements 3 and 4 of table B.3).

b.2.1.2) The information about participants to the **trust domain** defined for electronic registered mail delivery services shall be found by a **Trusted List**; and in the case of qualified REM services, by the use of **EU Trusted List system** that lists REMSs in the sense of eIDAS Regulation (EU) No 910/2014 [i.1] (see the derived rationales from statement 1 of table B.3 and statements 1 and 4 of table B.2).

b.2.1.3) The Trusting Interface, part of CSI **trust infrastructure**, allowing the **co-operation** among participants to the **trust domain** defined for electronic registered mail delivery services shall be implemented by use of a **Trusted List**; and in the case of qualified REM services, by the use of **EU Trusted List system** according to ETSI EN 319 522-4-3 [11], clause 7.1 (see the derived rationales from statement 1 of table B.3 and statements 1 and 4 of table B.2).

b.2.1.4) The **trust domain** of the electronic registered mail delivery services shall require **specific policy**, security and technical conditions to be met by all participating REMSs. The **capabilities** of the participating REMSs shall meet the requirements of ETSI EN 319 522-2 [2], clause 9.3 (see the derived rationales from statement 2 of table B.2 and clause D.1.3).

NOTE 1: The REMS are not obliged to be interoperable because they are qualified.

b.2.1.5) When **trust domain policy** does not include provisions for technical interoperability, its achievement shall require the specification of a **REMID policy** with security and the technical requirement that each REMS is obliged to fulfil **to ensure technical interoperability** among REMSs participating to the REMID, established according to the requirements b.2.1.1, b.2.1.2, b.2.1.3, b.2.1.4 and ETSI EN 319 522-4-3 [11], clause 7.1 (see the derived rationales from statements 1 and 6 of table B.2).

b.2.1.6) When **trust domain policy** does not include provisions for technical interoperability, the additional specifications defined according to the requirement b.2.1.5 shall **ensure** that all participating REMSs **have the same capabilities** according to ETSI EN 319 522-2 [2], clause 9.4.4 (see the derived rationales from statement 5 of table B.2).

NOTE 2: The list of REMSs joined to the trust domain defined according to the aforementioned **REMID policy** enjoys the technical interoperability of the participating REMSs. So such domain constitutes a **REM Interoperability Domain - REMID** (see the derived rationales from statement 3 of table B.2 and statement 4 of table B.3 and clause D.1.3).

C.2.3.3.2 Trust - Trusted List service element restrictions

Regarding the fields of TL covered in the present clause, their contents shall be expressed in conformance to ETSI TS 119 612 [12], with the restrictions and interpreted as defined in table C.3, table C.4 and table C.5.

Table C.3: Trusted List - ServiceTypeIdentifier constraints

Nº	Service/Protocol element	ETSI EN 319 532-3 [6] main reference	Requirement	Implementation guidance	Notes
2.2	TL / Service type identifier (as per clause 5.5.1 of ETSI TS 119 612 [12])	Clause 9.3	M	b.2.2.1)	Trusted List

Implementation guidance:

b.2.2.1) The **ServiceTypeIdentifier**, component of TL, shall be **http://uri.etsi.org/TrstSvc/Svctype/EDS/REM** for generic REM services, and http://uri.etsi.org/TrstSvc/Svctype/EDS/REM/Q for qualified services in the sense of eIDAS Regulation (EU) No 910/2014 [i.1] according to ETSI EN 319 532-3 [6], clause 9.3, ETSI EN 319 522-4-3 [11], clause 7.2 and ETSI TS 119 612 [12], clause 5.5.1 (see the derived rationales from statement 3 of table B.3).

Table C.4: Trusted List - ServiceDigitalIdentity constraints

Nº	Service/Protocol element	ETSI EN 319 532-3 [6] main reference	Requirement	Implementation guidance	Notes
2.3	TL / Service digital identity (as per clause 5.5.3 of ETSI TS 119 612 [12])	Clause 9.3	M	b.2.3.1), b.2.3.2), b.2.3.3)	Trusted List

Implementation guidance:

b.2.3.1) The **service digital identity** (ServiceDigitalIdentity element) of a REMS shall be represented by an X.509 certificate as a component of TL by the following **tuple** according to ETSI TS 119 612 [12], clause 5.5.3:

- One **X509Certificate elements expressed in Base64 encoded format as specified in XML-Signature**, used by the REMS for "**digital signing of REM messages and/or ERD evidence** XML structures" (see the derived rationales from statements 1 and 3 of table B.4)
- Optionally, one **X509SubjectName element that contains a Distinguished Name encoded as established by XML-Signature** (see the derived rationales from statement 3 of table B.4)
- Optionally, one **public key identifier expressed as an X.509 certificate Subject Key Identifier (X509SKI element) as specified in XML-Signature** (see the derived rationales from statement 3 of table B.4)

b.2.3.2) The single X509Certificate element, representing the REM service digital identity, shall be used to digitally sign all REM messages and ERDS evidence according to ETSI EN 319 532-3 [6], clause 9.3 and clauses C.4.2 and C.4.3 of the present document.

EXAMPLE 1:

```
<ServiceDigitalIdentity>
  <DigitalId>
    <X509Certificate>MII.....=</X509Certificate>
  </DigitalId>
  <DigitalId>
    <X509SubjectName>CN=REM Provider 1 CC, O=Org 1 CC, C=CC</X509SubjectName>
  </DigitalId>
  <DigitalId>
    <X509SKI>l8AB7g0AXEHD66Ya4rAzs52s8Xt=</X509SKI>
  </DigitalId>
</ServiceDigitalIdentity>
```

b.2.3.3) The X509Certificate of points b.2.3.2 and b.2.3.1 shall have the following properties:

i. It should be issued in the path of a general Root CA.

ii. It shall be issued by a subordinate/intermediate CA with the purposes and according to point 2) of ETSI EN 319 522-4-3 [11], clause 7.2 (namely: "*A single CA certificate that shall be used solely solely for the **purpose** of issuing certificates to components of the ERDS for **digital signing of ERD messages** and/or **ERD evidence***").

NOTE 1: There are no particular requirements on the general Root CA mentioned in i. regarding the interoperability. However, such general Root CA could have additional properties outside the scope of the REM baseline that makes sense, as an example, for a better user experience, and for simplicity of the overall configuration of the REM systems. Hence, as best practice, some further note is given in clause D.2.2.

Table C.5: Trusted List - ServiceSupplyPoints constraints

Nº	Service/Protocol element	ETSI EN 319 532-3 [6] main reference	Requirement	Implementation guidance	Notes
2.4	TL / Service supply point (as per clause 5.5.7 of ETSI TS 119 612 [12])	Clause 9.3	M	b.2.4.1), b.2.4.2), b.2.4.3)	Trusted List

Implementation guidance:

b.2.4.1) The ServiceEndpoint shall be represented, in the Trusted List, by the ServiceSupplyPoints element according to ETSI EN 319 522-4-3 [11], clause 7.2 and ETSI TS 119 612 [12], clause 5.5.7 (see the derived rationales from statements 1 and 2 of table B.5); and the ServiceSupplyPoints shall contain two entries, components of TL, with the following values.

b.2.4.2) One value of the **ServiceSupplyPoint** shall be the pointer to the SMTP server in the form of: "smtp://<DNS mx record of the REMS SMTP ServiceEndpoint>[:<optional port number>]" (e.g. with a value like `smtp://recipientdomain.rem` or as in the following more complete example 2).

b.2.4.3) Another value of the ServiceSupplyPoint shall be the pointer to the capability and security metadata XML structure in the form of: "https://<URI of the Capability and Security Information XML>" (e.g. as in the following more complete example 2).

EXAMPLE 2:

```
        <ServiceSupplyPoints>
             <ServiceSupplyPoint>smtp://rem-provider-1-MX-record.cc:25</ServiceSupplyPoint>
             <ServiceSupplyPoint>https://rem-provider-1-service.cc/CSI-REM-
PROVIDER1.xml</ServiceSupplyPoint>
        </ServiceSupplyPoints>
```

NOTE 2: For the addressing of the server the conventional URI generic syntax: <scheme>://<domain>[:<port>] is used. It is general for many types of protocols (e.g. http, https, etc. and for smtp servers, the scheme actually defined in "https://www.iana.org/assignments/uri-schemes/uri-schemes.xhtml" has been used).

C.2.3.3.3 Trust - Validation steps

To establish trust in a REMS based on information in a TL, an actor, which could be another REMS, shall validate:

Pre-relay R-REMS validations (at sender-side level) according to the specular steps defined in clause C.2.3.3.2:

1) verify the existence of a valid DNS MX record associated with the recipient's email domain;

2) verify that the aforementioned MX record is set as **ServiceSupplyPoint** TL element of a REMS;

3) verify the compliance of the **ServiceTypeIdentifier** TL element of such REMS to the expected type of service, according to the requirements of the applicable trust domain;

4) verify that the service current status TL element of such REMS is "granted"; and

5) verify the presence of a valid X.509 digital certificate on the **service digital identity** (ServiceDigitalIdentity).

Post-relay S-REMS validations (at recipient-side level) according to ETSI EN 319 522-4-3 [11], clause 7.2:

1) the REMS's digital signature on a REM message **or** ERD evidence;

2) verify that the signing certificate can be linked to the **service digital identity** (ServiceDigitalIdentity) in the TL;

3) verify that the service current status is "granted"; and

4) verify that the **ServiceTypeIdentifier** TL element is set according to the requirements of the applicable trust domain.

If this process is applied to evaluate trust in the past, the process shall use the information (signature validity and service information in the TL) that was valid then.

NOTE: Other run-time verifications further detailed for compliance in **REMID policy** are possible and make sense for coherence with REM specification (e.g. TLS certificate of R-REMS or signing certificate of S-REM expired). Hence some further note is given as best practice in clauses D.4.2, D.4.3 and D.4.4.

C.2.3.4 Capability discovery and management

C.2.3.4.1 Capabilities - Trusted List general requirements

Table C.6: Common service interface - Capabilities

Nº	Service/Protocol element	ETSI EN 319 532-3 [6] main reference	Requirement	Implementation guidance	Notes
3.1	TL, CapabilityAndSecurityInformation	Clause 9.4	M	c.3.1.1), c.3.1.2), c.3.1.3), c.3.1.4), c.3.1.5), c.3.1.6), c.3.1.7), c.3.1.8), c.3.1.9), c.3.1.10), c.3.1.11), c.3.1.12)	Capabilities general requirements

Implementation guidance:

c.3.1.1) Only the capabilities at REMS level (and not at user level) shall be used for technical interoperability purposes according to the points b.2.1.5) and b.2.1.6) of clause C.2.3.3.1 (see the derived rationales of table B.7).

c.3.1.2) The link from S-REMS to R-REMS, represented by the recipient's email address as part of the recipient's metadata, shall be used to identify the R-REMS and its capabilities (see the derived rationales from statement 1 of table B.7).

c.3.1.3) The respect of constraints and options required by S-REMS to R-REMS before the relay a REM message shall be verified by means of the capabilities exhibited by R-REMS according to ETSI EN 319 522-2 [2], clause 9.4.4 (see the derived rationales from statement 3 of table B.7 and also clauses C.2.3.3.3, C.2.3.4.3 and C.2.3.4.5 for the validation steps implementing such check); and such verification is facilitated by the additional provisions, of the particular REMID policy, that ensure interoperability through a set of common capabilities, according to the points b.2.1.5 and b.2.1.6 of clause C.2.3.3.1).

c.3.1.4) The common capabilities constituted according to the point c.3.1.3) shall be referenced in the **Trusted List** according to the format specified in ETSI EN 319 532-3 [6], clause 9.4 and downloadable by a URI specified in **ServiceSupplyPoint** TL element; and in the case of qualified REM services, by the use of **EU Trusted List system** (see the implementation guidance in table C.5 and the derived rationales in table B.8 and table B.9).

c.3.1.5) The collection of capabilities constituted according to the previous point c.3.1.4 shall be implemented through an XML structure composed of three sections:

i. a common **Scheme data** section (see point c.3.1.6 below for the implementation);

ii. the **REMS capability metadata** (see clause C.2.3.4.2 for the implementation);

NOTE 1: Once referenced from TL, such collection represents the metadata repository for the capabilities (see the derived rationales from statement 3 of table B.7).

iii. the **REMS capability-based security** (see clause C.2.3.4.4 for the implementation).

c.3.1.6) The whole XML structure container of capabilities, constituted according to the previous point c.3.1.5, shall be implemented through the REM baseline XML scheme definition for CapabilityAndSecurityInformation, defined in XML Schema file `1953204CSIxmlSchema.xsd`, whose location is detailed in clause E.1, and copied below for information. The XML Schema files shall take precedence in case of discrepancies between the XML schema excerpts provided in the present document and the XML Schema files.

NOTE 2: The XML Schema file stored at the location indicated above is contained in the attachment en_31953204v010300a0.zip accompanying the present document.

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- CapabilityAndSecurityInformation (REMS capabilities) -->

<!--                  ****** NOTICE ******
The present document is part of ETSI EN 319 532-4 and represents:
  1. the namespaces definitions and
  2. the required imports and
  3. the schema definitions for REM baseline Capability and Security Information (CSI) are composed
of:
     - Capability Information (CI)
        - CapabilityMetadata
           - ERDSMetadata
     - Security Information (SI)
        - SecurityMetadata
           - CapabilityBasedSecurity
-->

<xsd:schema targetNamespace="http://uri.etsi.org/19532/v1#"
                xmlns="http://uri.etsi.org/19532/v1#"
                xmlns:xsd="http://www.w3.org/2001/XMLSchema"
                xmlns:tl="http://uri.etsi.org/02231/v2#"
                xmlns:ci="http://uri.etsi.org/19522/v1#"
                xmlns:si="http://uri.etsi.org/19532/v1#"
                xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
                elementFormDefault="qualified" attributeFormDefault="unqualified">

        <!-- *** Imports facility section *** -->

        <!-- schemaLocation="http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/xmldsig-core-
schema.xsd"/> -->
        <xsd:import namespace="http://www.w3.org/2000/09/xmldsig#"
                 schemaLocation="xmldsig-core-schema.xsd"/>

        <!-- schemaLocation="http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/xenc-schema.xsd"/> -
->
        <xsd:import namespace="http://www.w3.org/2001/04/xmlenc#"
                schemaLocation="xenc-schema.xsd"/>

        <!-- schemaLocation="http://www.w3.org/2001/xml.xsd"/> -->
        <xsd:import namespace="http://www.w3.org/XML/1998/namespace"
                schemaLocation="xml.xsd"/>

       <!-- schemaLocation="http://docs.oasis-open.org/security/saml/v2.0/saml-schema-assertion-
2.0.xsd"/> -->
        <xsd:import namespace="urn:oasis:names:tc:SAML:2.0:assertion"
                schemaLocation="saml-schema-assertion-2.0.xsd"/>

        <xsd:import namespace="http://uri.etsi.org/19522/v1#"
                schemaLocation="1952203xmlSchema.xsd"/>

        <!-- schemaLocation="https://uri.etsi.org/19612/v2.2.1/ts_119612v020201_201601xsd.xsd"/> -->
        <xsd:import namespace="http://uri.etsi.org/02231/v2#"
                schemaLocation="ts_119612v020201_201601xsd.xsd"/>

        <!-- ROOT Element: CapabilityAndSecurityInformation (CSI) -->
        <xsd:element name="CapabilityAndSecurityInformation"
type="CapabilityAndSecurityInformationType"/>

        <xsd:complexType name="CapabilityAndSecurityInformationType">
                <xsd:sequence>
                        <xsd:element ref="SchemeData"/>
                        <xsd:element ref="CapabilityMetadata"/>
                        <xsd:element ref="SecurityMetadata"/>
                        <xsd:element ref="ds:Signature" minOccurs="0"/>
                </xsd:sequence>
                <xsd:attribute name="version" type="xsd:string" use="required"/>
                <xsd:attribute name="Id" type="xsd:ID" use="optional"/>
        </xsd:complexType>

        <!-- Capability and Security Information: Scheme data  -->
        <xsd:element name="SchemeData" type="SchemeDataType"/>
        <xsd:complexType name="SchemeDataType">
                <xsd:sequence>
                        <xsd:element name="CSIVersionIdentifier" type="xsd:integer"/>
                        <xsd:element name="CSISequenceNumber" type="xsd:positiveInteger"/>
```

```
                        <xsd:element name="CSISchemeOperatorName" type="tl:InternationalNamesType"/>
                        <xsd:element name="CSISchemeOperatorAddress" type="tl:AddressType"/>
                        <xsd:element name="CSISchemeInformationURI"
type="tl:NonEmptyMultiLangURIListType"/>
                        <xsd:element name="CSISchemePolicyCommunityRules"
type="tl:NonEmptyMultiLangURIListType"/>
                        <xsd:element name="CSIPointerToTL" type="tl:NonEmptyURIType"/>
                        <xsd:element name="CSIIssueDateTime" type="xsd:dateTime"/>
                        <xsd:element name="CSINextUpdate" type="tl:NextUpdateType"/>
                        <xsd:element name="CSIDistributionPoints" type="tl:NonEmptyURIListType"/>
                        <xsd:element name="CSIPointersToOtherMetadata" type="tl:NonEmptyURIListType"
minOccurs="0"/>
                        <xsd:element name="CSISchemeExtensions" type="tl:ExtensionsListType"
minOccurs="0"/>
                </xsd:sequence>
        </xsd:complexType>

        <!-- Capability Information (CI) -->
        <xsd:element name="CapabilityMetadata" type="CapabilityMetadataType"/>
        <xsd:complexType name="CapabilityMetadataType">
                <xsd:sequence>
                                <!-- The following is from ETSI EN 319 532-4, clause C.2.3.4.2 -->
                        <xsd:element ref="ci:ERDSMetadata"/>
                        <xsd:element name="CISchemeExtensions" type="tl:ExtensionsListType"
minOccurs="0"/>
                </xsd:sequence>
        </xsd:complexType>

        <!-- Security Information (SI) -->
        <xsd:element name="SecurityMetadata" type="SecurityMetadataType"/>
        <xsd:complexType name="SecurityMetadataType">
                <xsd:sequence>
                                <!-- The following is from ETSI EN 319 532-4, clause C.2.3.4.4 -->
                        <xsd:element ref="si:CapabilityBasedSecurity"/>
                        <xsd:element name="SISchemeExtensions" type="tl:ExtensionsListType"
minOccurs="0"/>
                </xsd:sequence>
        </xsd:complexType>

        <xsd:element name="CapabilityBasedSecurity" type="si:CapabilityBasedSecurityType"/>
        <xsd:complexType name="CapabilityBasedSecurityType">
                <xsd:sequence>
                        <!-- X509Certificate used for TLS specified in EN 319 532-4,
clause C.2.3.4.4 for Basic handshake -->
                        <xsd:element name="TLSCertificate" type="xsd:base64Binary"/>
                        <!-- X509Certificate used for Domain Signature specified in EN 319 532-4,
clause C.2.3.4.4 -->
                        <xsd:element name="DomainSignCertificate" type="xsd:base64Binary"
minOccurs="0"/>
                        <xsd:element name="CBSSchemeExtensions" type="tl:ExtensionsListType"
minOccurs="0"/>
                </xsd:sequence>
                <xsd:attribute name="version" use="required"/>
        </xsd:complexType>

</xsd:schema>
```

NOTE 3: The schema above uses the explicit method of local caching of any XSD namespace needed to be imported to avoid the impact of reloading the schema from the internet every time (consider that in production systems, the validation processes can require hundreds of checks per second, and the download is not practicable). Anyway, the original and canonical location is specified as XML comment just before the import for the once-only first download, or to set always, as location, just in case it is considered favourable.

c.3.1.7) The root element of XSD Capability and security information structure illustrated in point c.3.1.6 shall be `CapabilityAndSecurityInformation`.

i. CapabilityAndSecurityInformation shall have "EN319532v1" as value for version attribute.

ii. Attribute Id shall be used to reference the CapabilityAndSecurityInformation element.

c.3.1.8) The `SchemeData` element is composed as follows:

i. The content of `CSIVersionIdentifier` element shall have the semantic of TL element defined in ETSI TS 119 612 [12], clause 5.3.1 applied to `CapabilityAndSecurityInformation` instead of the TL scheme.

ii. The content of `CSISequenceNumber` element shall have the semantic of TL element defined in ETSI TS 119 612 [12], clause 5.3.2 applied to `CapabilityAndSecurityInformation` instead of the TL scheme.

iii. The `CSISchemeOperatorName` and the `CSISchemeOperatorAddress` elements shall specify the name and the address of the **REMID authority**, entity in charge of managing the `CapabilityAndSecurityInformation` scheme.

iv. The `CSISchemeInformationURI` element shall specify the URI(s) where relaying parties can obtain the master copy of the specific information regarding `CapabilityAndSecurityInformation` scheme; and `CSISchemePolicyCommunityRules` element shall specify the URI(s) where relaying parties can obtain the master copy of the scheme's policy (namely **REMID policy**) information with the security and technical requirements for the achievement of interoperability.

v. The content of the `CSIPointerToTL` element shall reference the location where the current and applicable TL is published, at the country level, by the TLSO.

vi. The content of `CSIIssueDateTime` element shall have the semantic of TL element defined in ETSI TS 119 612 [12], clause 5.3.14 applied to `CapabilityAndSecurityInformation` scheme instead of the TL one, transposing the role of TLSO to the **REMID authority** and according to the REM baseline **REMID policy** (see clause C.2.3.5 and clause D.1.3).

vii. The content of `CSINextUpdate` element shall have the semantic of TL element defined in ETSI TS 119 612 [12], clause 5.3.15 applied to `CapabilityAndSecurityInformation` scheme instead of the TL one, according to the REM baseline **REMID policy** (see clause C.2.3.5 and clause D.1.3).

NOTE 4: This element represents the date and time by which, at the latest, an update of the CapabilityAndSecurityInformation information structure occurs. The update can happen anytime when necessary (e.g. status changes, etc.) But if no changes occur, this structure is re-issued at the CSINextUpdate time to reduce the risks of substitution by an attacker with an old structure. Structures with CSINextUpdate occurring in the past are discarded.

viii. The content of `CSIDistributionPoints` element shall specify the location where the present capability and security information XML structure is published and where the relevant updates can be found. This element has a semantic like that of TL element defined in ETSI TS 119 612 [12], clause 5.3.16, but applied to `CapabilityAndSecurityInformation` scheme instead of the TL one.

ix. The content of `CSIPointersToOtherMetadata` element shall specify a list of references to the historical publications of the capability and security information XML structure. Once an XML file is obsoleted by a new one, it shall be published in the present historical list of the new one, through a URI composed of a fully qualified domain name in the host section and an absolute path without a query section. The name of the XML file shall be the SHA-256 hash value of the binary representation of the XML file itself, as it can be retrieved by resolving the aforementioned URI, adding the ".xml" file extension at the end of the absolute path.

EXAMPLE:

```
Content of CSIPointersToOtherMetadata element of the new file:

 <tns:CSIPointersToOtherMetadata>
     </tns:CSIPointersToOtherMetadata>
     <tl:URI>https://rem-provider-1-
service.cc/13bf128113ff2fb9d3607d897c6f403dc440278fcb914b8978c17bd812d03f49.xml</tl:URI>
     <tl:URI>https://rem-provider-1-
service.cc/378aa0e499cd37741f919226409b1d6efb67a6850d107ea77743ced7cdd0d9ed.xml</tl:URI>
 </tns:CSIPointersToOtherMetadata>


The published obsolete files (with content similar to that illustrated in figure C.2) are the
followings:
- "13bf128113ff2fb9d3607d897c6f403dc440278fcb914b8978c17bd812d03f49.xml" (already obsoleted)
```

```
- "378aa0e499cd37741f919226409b1d6efb67a6850d107ea77743ced7cdd0d9ed.xml" (new obsoleted)

and, the current new file, when and in case it is obsoleted by another one, it is published with the
same mechanism of the two above, and its SHA-256 digest value is added to the
CSIPointersToOtherMetadata of the new one.
At the first issue the CSIPointersToOtherMetadata element is empty.
```

NOTE 5: This historical list is necessary for security purposes (e.g. to support verifications after the change of digital certificates presents therein the present XML structure), and it not restricted to the last one. The number of saved historical elements is specified in the **REMID policy** (see clauses D.1.3 and D.3).

x. The `CSISchemeExtensions` (capability and security information) optional element shall have the semantic of TL element defined in ETSI TS 119 612 [12], clause 5.3.17 applied to `CapabilityAndSecurityInformation` scheme.

c.3.1.9) The `CapabilityMetadata` element is composed as follows:

i. The `ERDSMetadata` element shall be that defined in ETSI EN 319 522-3 [3], clause A.1 (see point c.3.2.31 of table C.7 for other requirements on this element).

ii. The `CISchemeExtensions` (capability information) optional element shall have the semantic of TL element defined in ETSI TS 119 612 [12], clause 5.3.17 applied to `CapabilityAndSecurityInformation` scheme.

c.3.1.10) The `SecurityMetadata` element is composed as follows:

i. The `CapabilityBasedSecurity` element shall be that defined in point c.3.4.3 of table C.10.

ii. The `SISchemeExtensions` (security information) optional element shall have the semantic of TL element defined in ETSI TS 119 612 [12], clause 5.3.17 applied to `CapabilityAndSecurityInformation` scheme.

c.3.1.11) The `Signature` element shall be a XAdES-B-B baseline digital signature as specified in ETSI EN 319 132-1 [14]. The **REMID policy** may specify, once the XAdES-B-B baseline signature has been generated if it should be also subject to time-stamp (e.g. through a XAdES-B-T baseline signature level, by incorporation into the digital signature of the unsigned attribute signature-timestamp, containing a time-stamp token computed as specified in ETSI EN 319 132-1 [14], clause 6). See clause D.1.3.

c.3.1.12) With regards to the point c.3.1.11, the certificate supporting the validation of the signature on the document shall either be one of the certificates used as digital identity of the REM service or be a certificate, issued to the REMSP, for which a valid certification path can be established to one of the certificates used as digital identity of the REM service, or a certificate issued to the REMID Authority.

NOTE 6: In all points above having options, from points c.3.1.7 to c.3.1.12, there can be additional rules, in local **REMID policy**, that dispose of particular usage of such options for specific functions or operation practices, as specified in the policy (see clauses C.2.3.5 and D.1.3). None of these "additional" functions or operation practices breaks the interoperability.

See figure C.1 for an example of TL referencing, by means of the ServiceSupplyPoint element, the whole `CapabilityAndSecurityInformation` structure defined as per the present clause, and fully exemplified in figure C.2.

C.2.3.4.2 Capability metadata - Trusted List referencing of REMS metadata

With regards to the fields of TL covered in the present clause, their contents shall be expressed in conformance to ETSI TS 119 612 [12], with the restrictions and interpreted as defined in table C.6 of clause C.2.3.4.1 and table C.7 of the present clause.

Table C.7: REMS capability metadata - ServiceSupplyPoint constraints

Nº	Service/Protocol element	ETSI EN 319 532-3 [6] main reference	Requirement	Implementation guidance	Notes
3.2	TL, CapabilityAndSecurity Information/Capability Metadata/ERDSMeta data	Clause 9.4	M	c.3.2.1), c.3.2.2), c.3.2.31), c.3.2.4)	Capability metadata

Implementation guidance:

c.3.2.1) The REMS capability metadata shall be made accessible, by reference, within one **ServiceSupplyPoint** element of TL according to ETSI TS 119 612 [12], clause 5.5.7 (see the derived rationales of table B.7, table B.8 and table B.9 of clause B.2.2.4, and the statement c.3.4.1 of table C.10 since it represents the same anchor point, in TL, for both forms of capabilities/metadata).

NOTE: The **ServiceSupplyPoint** element of TL is defined on a per-service basis. So, the capabilities referenced from such field are closely bound to REMS (and not to the scheme level).

c.3.2.2) The REMS capability metadata, referenced by **ServiceSupplyPoint** element, shall be the same, as specified in clause C.2.3.4.3, for all adherent REMSs, to ensure the same capabilities for the trust domain relevant to the REM baseline (see rationales of c.3.2.1).

c.3.2.31) ERDSMetadata XML structure shall be located at CapabilityAndSecurityInformation/CapabilityMetadata path, in order to reference the capability metadata, according to ETSI EN 319 532-3 [6], clause 9.4 (see the structure at c.3.1.6 of table C.6 and the rationales of c.3.2.1):

The ERDSMetadata element is defined in ETSI EN 319 522-3 [3], clause A.1 and copied below for information:

```
<!-- targetNamespace="http://uri.etsi.org/19522/v1#" -->
<xs:element name="ERDSMetadata" type="ERDSMetadataType"/>
<xs:complexType name="ERDSMetadataType">
<xs:sequence>
<xs:element name="ERDSId" type="EntityIdentifierType"/>
<xs:element name="ERDSDomain" type="xs:string"/>
<xs:element name="ERDSGoverningBody" type="xs:string"/>
<xs:element name="ERDSProfileSupported" type="xs:anyURI"/>
<xs:element name="ERDSMetadataRepository" type="xs:anyURI" minOccurs="0"/>
<xs:element name="ERDSEUQualifiedIndicator" type="xs:boolean" minOccurs="0"/>
<xs:element name="ERDSTLSLocation" type="xs:anyURI" minOccurs="0"/>
<xs:element name="ERDSRootCACertLocation" type="xs:anyURI" minOccurs="0"/>
<xs:element name="ERDSExpiryDateAndTimeSupport" type="xs:boolean"/>
<xs:element name="ERDSScheduledDeliverySupport" type="xs:boolean"/>
<xs:element name="ERDSAssuranceLevelsSupported" type="AssuranceLevelDetailsType"
minOccurs="0"/>
<xs:element name="ERDSPolicySupport" type="ERDSPolicyIDType" minOccurs="0"/>
<xs:element name="ERDSSupportedConsignmentModes" type="ConsigmentModeType" minOccurs="0"/>
</xs:sequence>
<xs:attribute name="version" use="required"/>
</xs:complexType>

<!-- targetNamespace="http://uri.etsi.org/19522/v1#" -->
<xs:complexType name="EntityIdentifierType">
  <xs:simpleContent>
    <xs:extension base="NonEmptyStringType">
      <xs:attribute name="IdentifierSchemeName" type="NonEmptyStringType" use="required"/>
    </xs:extension>
  </xs:simpleContent>
</xs:complexType>

<xs:simpleType name="NonEmptyStringType">
  <xs:restriction base="xs:string">
    <xs:minLength value="1"/>
  </xs:restriction>
</xs:simpleType>
```

c.3.2.4) ERDSMetadata element shall have "`EN319522v1.1.1`" as value for `version` attribute, and ERDSId element shall have "`http`" as value for `IdentifierSchemeName` attribute.

See figure C.1 for an example of TL referencing, by the ServiceSupplyPoint element, the ERDSMetadata structure defined as per the present clause and fully exemplified in figure C.2.

Table C.8: Capability metadata - ERDSMetadata constraints

Nº	Service/Protocol element	ETSI EN 319 532-3 [6] main reference	Requirement	Implementation guidance	Notes
3.3	CapabilityAndSecurityInformation/CapabilityMetadata/ERDSMetadata	Clause 9.4	M	c.3.3.1), c.3.3.3), c.3.3.4), c.3.3.5), c.3.3.6), c.3.3.7), c.3.3.2)	Capability metadata

Implementation guidance:

c.3.3.1) The ERDSDomain element of ERDSMetadata shall have the same value set to the "DNS mx record of the REMS SMTP ServiceEndpoint" (e.g. with a value like `recipientdomain.rem` or as in the following more complete example 1 below); and its content shall match the ServiceSupplyPoint with the exclusion of the "scheme" and the "service port number" if present (see b.2.4.2 of table C.5).

EXAMPLE 1:

```
<ServiceSupplyPoint>smtp://rem-provider-1-MX-record.cc:25</ServiceSupplyPoint>
and
<ERDSDomain>rem-provider-1-MX-record.cc</ERDSDomain>
```

c.3.3.2) The ERDSGoverningBody element of ERDSMetadata shall have the same value set to the "en" International/English language form of TL TSPName element according to table 14 of ETSI EN 319 522-2 [2], clause 9.4.4 (see the complete example 2 below).

c.3.3.3) The ERDSProfileSupported element of ERDSMetadata shall have the same the URI identifying the present REM baseline specification defined in clause C.1:

```
http://uri.etsi.org/19532/v1#/REMbaseline
```

c.3.3.4) The ERDSExpiryDateAndTimeSupport element of ERDSMetadata shall be set to `false`.

c.3.3.5) The ERDSScheduledDeliverySupport element of ERDSMetadata shall be set to `false`.

c.3.3.6) The ERDSAssuranceLevelsSupported element of ERDSMetadata, shall be set to the "substantial" level represented by the following URI:

```
http://eidas.europa.eu/LoA/substantial
```

c.3.3.7) The ERDSSupportedConsignmentModes element of ERDSMetadata shall be set to the "basic" consignment level, represented by the following URI:

```
http://uri.etsi.org/19522/v1#/consignment/basic
```

See below an excerpt of CapabilityAndSecurityInformation XML with an example of ERDSMetadata referenced from the **ServiceSupplyPoint** element of TL.

EXAMPLE 2:

```
       <ci:ERDSMetadata version="EN319522v1.1.1">
          <ERDSId IdentifierSchemeName="http">http://rem-provider-1-service.cc/rems-id.html</ERDSId>
          <ERDSDomain>rem-provider-1-same-as-MX-record.cc</ERDSDomain>
          <ERDSGoverningBody>Provider 1 CC</ERDSGoverningBody>
          <ERDSProfileSupported>http://uri.etsi.org/19532/v1#/REMbaseline</ERDSProfileSupported>
          <ERDSExpiryDateAndTimeSupport>false</ERDSExpiryDateAndTimeSupport>
          <ERDSScheduledDeliverySupport>false</ERDSScheduledDeliverySupport>
          <ERDSAssuranceLevelsSupported>
             <AssuranceLevel>http://eidas.europa.eu/LoA/substantial</AssuranceLevel>
          </ERDSAssuranceLevelsSupported>
<ERDSSupportedConsignmentModes>http://uri.etsi.org/19522/v1#/consignment/basic</ERDSSupportedConsign
mentModes>
        </ci:ERDSMetadata>
```

See figure C.1 for a complete example of TL referencing, by the ServiceSupplyPoint element, the ERDSMetadata sample defined as per the present clause and fully exemplified in figure C.2.

C.2.3.4.3 Capability metadata - Consistency and validation steps

The present clause addresses the implementation of the expression having the "same capabilities" used in the referenced standard (see ETSI EN 319 522-2 [2], clause 9.4.4).

The capabilities extensions are specified by a set of fields (elements and attributes), each one expressed by a list of tag/name and content/value assertions. The property of having the "same capabilities", between two such lists is implemented through a specific comparison of all those assertions.

NOTE: A special comparison process is necessary because some of the elements (e.g. ERDSDomain) has a specific value for any REMSP. So the ERDSDomain value of a certain REMSP is different from that of another one. But this does not mean that the capabilities of the first REMSP are different from the capabilities of the second one.

This specific comparison process is therefore named "equivalence"; and the equivalence between two generic capability structures shall be achieved by applying the requirements of table C.9 (a key point of the validation process necessary for the check/assessment mentioned in ETSI EN 319 522-2 [2], clause 9.4.4 as explained in the derived rationales of table B.7).

Below follows a detailed description of table C.9:

1) the first column contains a progressive identifier;

2) the second column contains capability elements and attributes coming from the formal definition of ERDSMetadata structure;

3) the third column contains the indication if the either the specified element tag (in case of XML elements) or the attribute name (in case of attributes of the elements) has to be considered in the equivalence process;

4) the fourth column contains the indication if either the specified element content (in case of XML elements) or the attribute value (in case of attributes of the elements) has to be considered in the equivalence process;

5) The fifth column informs where there is the implementation guidance with the fulfilment details of the referenced element or attribute.

The rationale of the equivalence criteria is to verify the capabilities according to the following matching requirements with either:

- the equivalence shall be verified when both tag/name is "present" and content/value is "equal" if the element/attribute has both third and fourth column selected; or

- the equivalence shall be verified when only of tag/name is "present" (without regards to the content/value) if the element/attribute has only the third column selected.

Table C.9: Capability metadata - ERDSMetadata elements equivalence

Nº	Capability metadata element/attribute	Element's/attribute tag/name	Element's/attribute content/value	Guidance reference
1	Version	✓	✓	c.3.2.4)
2	IdentifierSchemeName	✓	✓	c.3.2.4)
3	ERDSId	✓		see note
4	ERDSDomain	✓		c.3.3.1)
5	ERDSGoverningBody	✓		see note
6	ERDSProfileSupported	✓	✓	c.3.3.3)
7	ERDSExpiryDateAndTimeSupport	✓	✓	c.3.3.4)
8	ERDSScheduledDeliverySupport	✓	✓	c.3.3.5)
9	AssuranceLevel	✓	✓	c.3.3.6)
10	ERDSSupportedConsignmentModes	✓	✓	c.3.3.7)
NOTE:	Other verifications, outside the scope of the REM baseline and in addition to the ten above, are possible at registration time and run-time (for example, for Nº 3, Nº 4 and Nº 5), and they make sense for coherence with REM specification. Hence some further note is given as best practice in clause D.4.			

C.2.3.4.4 Capability-based security - Trusted List referencing of security tokens

With regards to the fields of TL covered in the present clause, their contents shall be expressed in conformance to ETSI TS 119 612 [12], with the restrictions and interpreted as defined in table C.6 of clause C.2.3.4.1 and table C.10 of the present clause.

Table C.10: Capability-based security - ServiceSupplyPoint constraints

Nº	Service/Protocol element	ETSI EN 319 532-3 [6] main reference	Requirement	Implementation guidance	Notes
3.4	TL, CapabilityAndSecurityInformation/SecurityMetadata/CapabilityBasedSecurity	Clause 9.4	M	c.3.4.1), c.3.4.2), c.3.4.3), c.3.4.4)	Capability-based security

Implementation guidance:

c.3.4.1) The REMS capability-based security information shall be made accessible, by reference, within one **ServiceSupplyPoint** element of TL according to ETSI TS 119 612 [12], clause 5.5.7.

NOTE 1: See the derived rationales of table B.7, table B.8 and table B.9 of clause B.2.2.4, and the statement c.3.2.1 of table C.7 since it represents the same anchor point, in TL, for both forms of capabilities/metadata.

c.3.4.2) The REMS capability-based security information, relevant to the "basic handshake", referenced by **ServiceSupplyPoint** element, shall be the same, as specified in clause C.2.3.4.5, for all adherent REMSs, to ensure the same capabilities for the trust domain relevant to the REM baseline (see note 1).

c.3.4.3) REMS CapabilityBasedSecurity XML structure shall be located at CapabilityAndSecurityInformation/SecurityMetadata path, to reference the security metadata (see the structure at c.3.1.6 of table C.6 and the rationales of note 1):

The CapabilityBasedSecurity element is defined in XML Schema file `1953204CSIxmlSchema.xsd`, whose location is detailed in clause E.1 (see point c.3.1.6 for a high-level illustration of the whole XML structure container of capabilities). The fragment relevant to the present definition is copied below for information. The XML Schema files shall take precedence in case of discrepancies between the XML schema excerpts provided in the present document and the XML Schema files.

```
<!-- Element CapabilityBasedSecurity (REMS capabilities) -->
        <!-- targetNamespace="http://uri.etsi.org/19532/v1#" -->
        <xsd:element name="CapabilityBasedSecurity" type="si:CapabilityBasedSecurityType"/>
        <xsd:complexType name="CapabilityBasedSecurityType">
                <xsd:sequence>
                        <!-- X509Certificate used for TLS specified in EN 319 532-4,
clause C.2.3.4.4 for Basic handshake -->
                        <xsd:element name="TLSCertificate" type="xsd:base64Binary"/>
                        <!-- X509Certificate used for Domain Signature specified in EN 319 532-4,
clause C.2.3.4.4 -->
                        <xsd:element name="DomainSignCertificate" type="xsd:base64Binary"
minOccurs="0"/>
                        <xsd:element name="CBSSchemeExtensions" type="tl:ExtensionsListType"
minOccurs="0"/>
                </xsd:sequence>
                <xsd:attribute name="version" use="required"/>
        </xsd:complexType>
```

c.3.4.4) CapabilityBasedSecurity element shall have "`EN319532v1`" as value for `version` attribute".

Table C.11: Capability-based security - CapabilityBasedSecurity constraints

Nº	Service/Protocol element	ETSI EN 319 532-3 [6] main reference	Requirement	Implementation guidance	Notes
3.5	CapabilityAndSecurityInformation/SecurityMetadata/CapabilityBasedSecurity/TLSCertificate	Clause 9.4	M	c.3.5.1)	Capability-based security

Implementation guidance:

c.3.5.1) The TLSCertificate element of CapabilityBasedSecurity shall contain the X509Certificate used for the Transport Layer Security (TLS) mechanism of REMS SMTP ServiceEndpoint, for the basic handshake.

NOTE 2: It is important to have the TLS certificate ensured by an anchor in the Trusted List. The sender's REMS needs to be sure that the contacted REMS, resolved by DNS lookup, is the intended server (thus guaranteeing that any REM message hands over only to Trusted REMS). The TLS handshake between Trusted REMS, that has to take place in its completeness, and the subsequent secure matching between the server's certificate and the TLS certificate anchored by the Trusted List concur for the accomplishment of this assurance task. The domain resolved by DNS is not always (indeed almost never) the same domain contained in the service's certificate. For example, in the case of a REMS managing thousands of email domains, these are resolved by the DNS to the MX records. Therefore, only the MX record hostnames are configured inside the certificate SAN, and not all the thousands of managed domains; and the TLS certificate certifies only the MX records hostnames. The coverage against security threats provided by this "basic handshake" mechanism is implemented by: DNS, TLS plus TLS certificate anchored in Trusted List through the CapabilityAndSecurityInformation XML structure. Possible MITM attacks are detected right through the TLS certificate ensured in TL and not solely by TLS standalone certificate checks; and the relevant session is intended in the "forced TLS" form (and not as an "opportunistic TLS").

NOTE 3: The present version of REM baseline does not specify the optional elements `DomainSignCertificate` and `CBSSchemeExtensions`.

See below an excerpt of CapabilityAndSecurityInformation XML with an example of CapabilityBasedSecurity referenced from **ServiceSupplyPoint** element of TL for the basic handshake.

EXAMPLE:

```
<si:CapabilityBasedSecurity version="EN319532v1">
   <si:TLSCertificate>MII.....=</si:TLSCertificate>
</si:CapabilityBasedSecurity>
```

See figure C.1 for a complete example of TL referencing, by the ServiceSupplyPoint element, the CapabilityBasedSecurity sample defined as per the present clause and fully exemplified in figure C.2.

C.2.3.4.5 Capability-based security - Consistency and validation steps

The requirements given and explained in clause C.2.3.4.3 for capability metadata shall apply to capability-based security implemented according to the basic handshake as well, with the following additional considerations:

1) the requirements of table C.12 are used instead of those of table C.9;

2) the second column contains capability elements and attributes coming from the formal definition of CapabilityBasedSecurity structure.

Table C.12: Capability-based security - CapabilitybasedSecurity elements equivalence

Nº	Capability-based security element/attribute	Element's/attribute tag/name	Element's/attribute content/value	Guidance reference
1	Version	✓	✓	c.3.4.4)
2	TLSCertificate	✓		c.3.5.1)
NOTE:	Other verifications, outside the scope of the REM baseline and in addition to the two above, are possible at registration time and run-time, and they make sense for coherence with REM specification. Hence some further note is given as best practice in clause D.4.			

C.2.3.4.6 Capability - Discovery interface

Table C.13: Capability - Discovery

Nº	Service/Protocol element	ETSI EN 319 532-3 [6] main reference	Requirement	Implementation guidance	Notes
3	TL	Clause 9.4	M	a), b)	Discovery interface

Implementation guidance:

a) The Discovery Interface shall be implemented using TL.

b) The domain part of the recipient's email address shall be used to individuate the R-REMS capabilities (see the derived rationales of table B.7 and table B.10).

C.2.3.5 Governance support

Table C.14: Common service interface - Governance

Nº	Service/Protocol element	ETSI EN 319 532-2 [5] main reference	Requirement	Implementation guidance	Notes
4	Policy	9.3	M	a), b), c), d)	Governance support

Implementation guidance:

a) The governance, operated by the REMID authority, should address at least the following tasks:

   I. Publication of the **REMID policy** denoting the adoption of the REM baseline and the required additional technical condition (e.g. regarding operation details like security, timeouts, historical retentions, certificate details or similar which do not break interoperability). See some other information in clauses D.1.3 and D.2.2.3.

   II. Ensuring the publication of the Capability and Security Information from any REMS adhering to the REMID.

   III. Ensuring the referencing of the Capability and Security Information required to implement the REMID, from the supporting Trusted List System through the ServiceSupplyPoint element (see clause C.2.3.4).

b) The URI used for the publication of the **REMID policy** and the additional information required by REM baseline shall be set to the `CSISchemePolicyCommunityRules` element of `CapabilityAndSecurityInformation` XML structure (see point iv./c.3.1.8 of table C.6, clause C.2.3.4.1 and clause D.1.3).

NOTE 1: The published information is a set of data for governance and consultation purposes that is typically defined initially and infrequently changed.

c) The data used for automatic run-time operations should always be a "cached" copy of the "master" ones maintained in TL and CapabilityAndSecurityInformation distribution points. That information is used by applications in machine-processable way to ensure trust and interoperability. In any case, any Service Provider should download the "master" copy from TL and CapabilityAndSecurityInformation, to align own "cached" copy, according to practices already recommended for TL operations (see also clauses D.3 and D.4).

d) The operations practices for TL illustrated in ETSI TS 119 612 [12], clause 6 shall apply to CapabilityAndSecurityInformation as well according to the **REMID policy** and with the roles properly transposed into the context of the REMID. In particular, REMSPs shall publish, at the same locations where they publish their CapabilityAndSecurityInformation XML file, a SHA-256 hash of such file - as it can be retrieved from CSIDistributionPoints URI. The hash shall be published with the same CSIDistributionPoints URI but replacing the ".xml" file extension, at the end of the absolute path, with ".sha2" (see also clauses D.3 and D.4).

NOTE 2: The mechanism, as mentioned earlier is used, by REMSPs, in combination with that defined in point ix./c.3.1.8 of table C.6, clause C.2.3.4.1. The file with extension ".sha2" contains a digest of the current version. Those illustrated in point ix., with the digest values in the filenames, refer to the historical capability information.

An example of Trusted List with some of the fields expressed as per the prescriptions of the present clause C.2 is illustrated in figure C.1.

```
<?xml version="1.0" encoding="UTF-8"?>
<!--
The present document is an example for ETSI EN 319 532-4 xsd definitions and represents:
  1. the namespaces definitions relevant to a TL exemplification for REM baseline
  2. a Trusted List (TL) XML structure composed by:
     - TrustServiceStatusList
-->

<TrustServiceStatusList
  xmlns="http://uri.etsi.org/02231/v2#"
  TSLTag="http://uri.etsi.org/19612/TSLTag"
  Id="TrustServiceStatusList-ERDS-Example">

  <SchemeInformation>
    <TSLVersionIdentifier>1</TSLVersionIdentifier>
    <TSLSequenceNumber>1</TSLSequenceNumber>
    <TSLType>http://uri.etsi.org/TrstSvc/TrustedList/TSLType/EUgeneric</TSLType>
    <SchemeOperatorName>
      <Name xml:lang="en">CC Supervision Agency</Name>
      <Name xml:lang="cc">TBD in CC language</Name>
    </SchemeOperatorName>
    <SchemeOperatorAddress>
      <PostalAddresses>
        <PostalAddress xml:lang="en">
          <StreetAddress>CC Supervision Agency address</StreetAddress>
          <Locality>CC locality</Locality>
          <PostalCode>CC postal code</PostalCode>
          <CountryName>CC</CountryName>
        </PostalAddress>
        <PostalAddress xml:lang="cc">
          <StreetAddress>TBD in CC language</StreetAddress>
          <Locality>TBD in CC language</Locality>
          <PostalCode>CC postal code</PostalCode>
          <CountryName>CC</CountryName>
        </PostalAddress>
      </PostalAddresses>
      <ElectronicAddress>
        <URI xml:lang="en">mailto:eIDAS@CC-supervision-agency.cc</URI>
        <URI xml:lang="en">https://www.CC-supervision-agency.cc</URI>
      </ElectronicAddress>
    </SchemeOperatorAddress>
    <SchemeName>
      <Name xml:lang="en">CC:Trusted list for ERDS services</Name>
      <Name xml:lang="cc">CC:TBD in CC language</Name>
    </SchemeName>
    <SchemeInformationURI>
      <URI xml:lang="en">https://CC-supervision-agency.cc/tl-en.html</URI>
      <URI xml:lang="cc">https://CC-supervision-agency.cc/tl-cc.html </URI>
    </SchemeInformationURI>
<StatusDeterminationApproach>http://uri.etsi.org/TrstSvc/TrustedList/StatusDetn/EUappropriate</Statu
sDeterminationApproach>
```

```
    <SchemeTypeCommunityRules>
      <URI xml:lang="en">http://uri.etsi.org/TrstSvc/TrustedList/schemerules/EUcommon</URI>
      <URI xml:lang="en">http://uri.etsi.org/TrstSvc/TrustedList/schemerules/CC</URI>
    </SchemeTypeCommunityRules>
    <SchemeTerritory>CC</SchemeTerritory>
    <PolicyOrLegalNotice>
      <TSLLegalNotice xml:lang="en">The applicable legal </TSLLegalNotice>
      <TSLLegalNotice xml:lang="cc">TBD in CC language </TSLLegalNotice>
    </PolicyOrLegalNotice>
    <HistoricalInformationPeriod>12345</HistoricalInformationPeriod>
    <PointersToOtherTSL>
      <OtherTSLPointer>
        <ServiceDigitalIdentities>
          <ServiceDigitalIdentity>
            <DigitalId>
              <X509Certificate>QUJDMTIzCg==</X509Certificate>
            </DigitalId>
          </ServiceDigitalIdentity>
        </ServiceDigitalIdentities>
        <TSLLocation>https://ec.europa.eu/tools/lotl/eu-lotl.xml</TSLLocation>
        <AdditionalInformation>
          <OtherInformation>
            <TSLType>http://uri.etsi.org/TrstSvc/TrustedList/TSLType/EUlistofthelists</TSLType>
          </OtherInformation>
          <!--[OMISSIS]-->
        </AdditionalInformation>
      </OtherTSLPointer>
    </PointersToOtherTSL>
    <ListIssueDateTime>2020-10-03T08:30:00Z</ListIssueDateTime>
    <NextUpdate>
      <dateTime>2021-10-03T08:29:59Z</dateTime>
    </NextUpdate>
    <DistributionPoints>
      <URI>https://CC-supervision-agency.cc/TL-CC.xml</URI>
    </DistributionPoints>
  </SchemeInformation>
  <TrustServiceProviderList>
    <TrustServiceProvider>
      <TSPInformation>
        <TSPName>
          <Name xml:lang="cc">Provider 1 CC</Name>
          <Name xml:lang="en">Provider 1 CC</Name>
        </TSPName>
        <TSPTradeName>
          <Name xml:lang="en">VATCC-12345678910</Name>
          <Name xml:lang="en">Provider 1 international trade name</Name>
        </TSPTradeName>
        <TSPAddress>
          <PostalAddresses>
            <PostalAddress xml:lang="en">
              <StreetAddress>Provider 1 CC street address</StreetAddress>
              <Locality>Provider 1 CC locality</Locality>
              <PostalCode>Provider 1 CC postal code</PostalCode>
              <CountryName>CC</CountryName>
            </PostalAddress>
          </PostalAddresses>
          <ElectronicAddress>
            <URI xml:lang="en">https://rem-provider-1.cc</URI>
            <URI xml:lang="en">mailto:rem-provider-1@rem-provider-1-domain.cc</URI>
          </ElectronicAddress>
        </TSPAddress>
        <TSPInformationURI>
            <URI xml:lang="en">https://rem-provider-1.cc/info.html</URI>
        </TSPInformationURI>
      </TSPInformation>
      <TSPServices>
        <TSPService>
          <ServiceInformation>
<ServiceTypeIdentifier>http://uri.etsi.org/TrstSvc/Svctype/EDS/REM/Q</ServiceTypeIdentifier>
            <ServiceName>
              <Name xml:lang="en">REM Provider 1 CC</Name>
              <Name xml:lang="cc">TBD in CC language</Name>
            </ServiceName>
            <ServiceDigitalIdentity>
              <DigitalId>
                <X509Certificate>QUJDMTIzCg==</X509Certificate>
              </DigitalId>
              <DigitalId>
```

```
              <X509SubjectName>CN=REM Provider 1 CC, O=Org 1 CC, C=CC</X509SubjectName>
            </DigitalId>
            <DigitalId>
              <X509SKI>bDdPQjdoMFVYREhGNDNZakFzbFhzPQo=</X509SKI>
            </DigitalId>
          </ServiceDigitalIdentity>
          <ServiceStatus>http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted</ServiceStatus>
          <StatusStartingTime>2021-12-30T22:00:00Z</StatusStartingTime>
          <SchemeServiceDefinitionURI>
            <URI
xml:lang="en">https://TBD/OptionalSchemeDefinitionByTLSOMakingReferenceToREMBaseline.html</URI>
          </SchemeServiceDefinitionURI>
          <ServiceSupplyPoints>
            <ServiceSupplyPoint>smtp://rem-provider-1-MX-record.cc:25</ServiceSupplyPoint>
            <ServiceSupplyPoint>https://rem-provider-1-
service.cc/CapabilityAndSecurityMetadata.xml</ServiceSupplyPoint>
          </ServiceSupplyPoints>
          <TSPServiceDefinitionURI>
            <URI xml:lang="en">https://rem-provider-1-service.cc/index-en.html</URI>
            <URI xml:lang="cc">https://rem-provider-1-service.cc/index-cc.html</URI>
          </TSPServiceDefinitionURI>
        </ServiceInformation>
        <ServiceHistory>
          <!--[OMISSIS]-->
        </ServiceHistory>
      </TSPService>
    </TSPServices>
  </TrustServiceProvider>
 </TrustServiceProviderList>
 <dsig:Signature
       xmlns:dsig="http://www.w3.org/2000/09/xmldsig#"
       xmlns:xades="http://uri.etsi.org/01903/v1.3.2#"
       xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" Id="tlsig-12345678910">
   <dsig:SignedInfo>
     <dsig:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
     <dsig:SignatureMethod Algorithm="http://www.w3.org/2007/05/xmldsig-more#sha256"/>
     <dsig:Reference Id="ref-id-12345678910" Type="" URI="">
       <dsig:Transforms>
         <dsig:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
         <dsig:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
       </dsig:Transforms>
       <dsig:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
       <dsig:DigestValue>
KHN0ZGluKT0gODM3MTYxMDdjYzgzZjc4MmE1ODMyYjFkYWYyYTk2NGNiMWMyNDljNGVkMWEzOGZmZTg2YzBkYWFiMDk3MzcxNwo=
       </dsig:DigestValue>
     </dsig:Reference>
     <dsig:Reference Id="ref-id-sp-1594988407883" Type="http://uri.etsi.org/01903#SignedProperties"
URI="#SignedProps-12345678910">
       <dsig:Transforms>
         <dsig:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
       </dsig:Transforms>
       <dsig:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
       <dsig:DigestValue>
KHN0ZGluKT0gODM3MTYxMDdjYzgzZjc4MmE1ODMyYjFkYWYyYTk2NGNiMWMyNDljNGVkMWEzOGZmZTg2YzBkYWFiMDk3MzcxNwo=
</dsig:DigestValue>
     </dsig:Reference>
   </dsig:SignedInfo>
   <dsig:SignatureValue>QUJDMTIzCg==</dsig:SignatureValue>
   <dsig:KeyInfo>
     <dsig:X509Data>
     <dsig:X509Certificate>QUJDMTIzCg==</dsig:X509Certificate>
     </dsig:X509Data>
   </dsig:KeyInfo>
   <dsig:Object>
     <xades:QualifyingProperties xmlns:dsig="http://www.w3.org/2000/09/xmldsig#"
xmlns:xades="http://uri.etsi.org/01903/v1.3.2#" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance" Target="#XmlDSig-12345678910">
       <xades:SignedProperties Id="SignedProps-12345678910">
         <xades:SignedSignatureProperties>
           <xades:SigningTime>2020-10-03T08:30:00Z</xades:SigningTime>
           <xades:SigningCertificate>
             <xades:Cert>
               <xades:CertDigest>
                 <dsig:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                 <dsig:DigestValue>QUJDMTIzCg==</dsig:DigestValue>
               </xades:CertDigest>
               <xades:IssuerSerial>
                 <dsig:X509IssuerName>CN=REM Provider 1 CC, O=Org 1 CC, C=CC</dsig:X509IssuerName>
```

```
                  <dsig:X509SerialNumber>1</dsig:X509SerialNumber>
                </xades:IssuerSerial>
              </xades:Cert>
            </xades:SigningCertificate>
          </xades:SignedSignatureProperties>
          <xades:SignedDataObjectProperties>
            <xades:DataObjectFormat ObjectReference="#ref-id-12345678910">
              <xades:MimeType>text/xml</xades:MimeType>
            </xades:DataObjectFormat>
          </xades:SignedDataObjectProperties>
        </xades:SignedProperties>
      </xades:QualifyingProperties>
    </dsig:Object>
  </dsig:Signature>
</TrustServiceStatusList>
```

Figure C.1: Detailed Trusted List example for REM baseline

An example of Capability and Security Information, anchored in TL (see *<ServiceSupplyPoint>https://rem-provider-1-service.cc/CapabilityAndSecurityMetadata.xml</ServiceSupplyPoint>* in TL example of figure C.1), with some of the field expressed as per the prescriptions of the present clause C.2 is illustrated in figure C.2.

```
<?xml version="1.0" encoding="UTF-8"?>
<!--
The present document is an XML example for ETSI EN 319 532-4 and represents:
  1. the namespaces definitions relevant to a Capability and Security Information exemplification
for REM baseline
  2. a scheme information header for the XML structure composed by:
     - Scheme Data
  3. a Capability and Security Information (CSI) XML structure composed by:
     - Capability Information (CI)
        - CapabilityMetadata
           - ERDSMetadata
     - Security Information (SI)
        - SecurityMetadata
           - CapabilityBasedSecurity
-->

<tns:CapabilityAndSecurityInformation
     xmlns:tns="http://uri.etsi.org/19532/v1#"
     xmlns:tl="http://uri.etsi.org/02231/v2#"
     xmlns:ci="http://uri.etsi.org/19522/v1#"
     xmlns:si="http://uri.etsi.org/19532/v1#"
     version="EN319532v1" Id="sec-cap-meta-id-0001">

    <tns:SchemeData>
       <tns:CSIVersionIdentifier>1</tns:CSIVersionIdentifier>
       <tns:CSISequenceNumber>3</tns:CSISequenceNumber>
       <tns:CSISchemeOperatorName>
          <tl:Name xml:lang="en">CC REMID authority</tl:Name>
          <tl:Name xml:lang="cc">TBD in CC language</tl:Name>
       </tns:CSISchemeOperatorName>
       <tns:CSISchemeOperatorAddress>
          <tl:PostalAddresses>
             <tl:PostalAddress xml:lang="en">
                <tl:StreetAddress>CC REMID authority address</tl:StreetAddress>
                <tl:Locality>CC locality</tl:Locality>
                <tl:PostalCode>CC postal code</tl:PostalCode>
                <tl:CountryName>CC</tl:CountryName>
             </tl:PostalAddress>
             <tl:PostalAddress xml:lang="cc">
                <tl:StreetAddress>CC REMID authority address (TBD in CC language)</tl:StreetAddress>
                <tl:Locality>CC locality</tl:Locality>
                <tl:PostalCode>CC postal code</tl:PostalCode>
                <tl:CountryName>CC</tl:CountryName>
             </tl:PostalAddress>
          </tl:PostalAddresses>
          <tl:ElectronicAddress>
             <tl:URI xml:lang="en">mailto:eIDAS@CC-remid-authority.cc</tl:URI>
             <tl:URI xml:lang="en">https://www.CC-remid-authority.cc</tl:URI>
          </tl:ElectronicAddress>
       </tns:CSISchemeOperatorAddress>
       <tns:CSISchemeInformationURI>
          <tl:URI xml:lang="en">https://www.CC-remid-authority.cc/remid-scheme-en.html</tl:URI>
          <tl:URI xml:lang="cc">https://www.CC-remid-authority.cc/remid-scheme-cc.html</tl:URI>
```

```
       </tns:CSISchemeInformationURI>
       <tns:CSISchemePolicyCommunityRules>
          <tl:URI xml:lang="en">https://CC-remid-authority.cc/remid-policy-en.html</tl:URI>
          <tl:URI xml:lang="cc">https://CC-remid-authority.cc/remid-policy-cc.html</tl:URI>
       </tns:CSISchemePolicyCommunityRules>
       <tns:CSIPointerToTL>https://CC-TL-scheme-operator.cc/TL-CC.xml</tns:CSIPointerToTL>
       <tns:CSIIssueDateTime>2021-01-16T07:30:00Z</tns:CSIIssueDateTime>
       <tns:CSINextUpdate>
          <tl:dateTime>2021-10-03T06:59:59Z</tl:dateTime>
       </tns:CSINextUpdate>
       <tns:CSIDistributionPoints>
          <tl:URI>https://rem-provider-1-service.cc/CSI-REM-PROVIDER1.xml</tl:URI>
       </tns:CSIDistributionPoints>
       <tns:CSIPointersToOtherMetadata>
          <tl:URI>https://rem-provider-1-
service.cc/13bf128113ff2fb9d3607d897c6f403dc440278fcb914b8978c17bd812d03f49.xml</tl:URI>
       </tns:CSIPointersToOtherMetadata>
    </tns:SchemeData>

    <tns:CapabilityMetadata>
       <ci:ERDSMetadata version="EN319522v1.1.1">
          <ERDSId IdentifierSchemeName="http">http://rem-provider-1-service.cc/rems-id.html</ERDSId>
          <ERDSDomain>rem-provider-1-same-as-MX-record.cc</ERDSDomain>
          <ERDSGoverningBody>Provider 1 CC</ERDSGoverningBody>
          <ERDSProfileSupported>http://uri.etsi.org/19532/v1#/REMbaseline</ERDSProfileSupported>
          <ERDSExpiryDateAndTimeSupport>false</ERDSExpiryDateAndTimeSupport>
          <ERDSScheduledDeliverySupport>false</ERDSScheduledDeliverySupport>
          <ERDSAssuranceLevelsSupported>
             <AssuranceLevel>http://eidas.europa.eu/LoA/substantial</AssuranceLevel>
          </ERDSAssuranceLevelsSupported>
<ERDSSupportedConsignmentModes>http://uri.etsi.org/19522/v1#/consignment/basic</ERDSSupportedConsign
mentModes>
       </ci:ERDSMetadata>
    </tns:CapabilityMetadata>

    <tns:SecurityMetadata>
       <si:CapabilityBasedSecurity version="EN319532v1">
         <si:TLSCertificate>QUJDMTIzCg==</si:TLSCertificate>
       </si:CapabilityBasedSecurity>
    </tns:SecurityMetadata>

</tns:CapabilityAndSecurityInformation>
```

Figure C.2: Detailed Capability and Security Information for REM baseline

NOTE 3: "CC" or "cc" are used in figure C.1 and figure C.2 as placeholders representing the Country or the language Code to outline all the country-specific details in the example. A particular case is the "cc" country code place holder put at the top-level domain part of URIs which is just one possibility. Other top-level domains are valid for any DNS name, without using exactly the country code.

C.3 ERDS evidence - composition

C.3.1 General requirements

With regards to the ERDS evidence XML structure composition, the requirements given and explained in ETSI EN 319 522-3 [3], clause 5 shall apply to REM baseline according to the provisions of the present clause and the clauses C.3.2, C.3.3 and C.3.4.

The requirements on ERDS evidence Extensions summarized in clause C.3.2, table C.15 and table C.16 shall apply.

NOTE: The placeholder extensions option is used to host, in a natural way, additional elements in the canonical and ERDS evidence data structure without introducing syntactical discontinuity (see component E01 as specified in ETSI EN 319 522-2 [2], clause 8.2.28 and the derived rationales from statement 8 of table B.13).

The ERDS evidence main structure requirements summarized in clause C.3.3, table C.17 shall apply.

The requirements on the presence and implementation guidance of the detailed ERDS evidence components summarized in clause C.3.4 table C.18 shall apply.

The requirements on cardinality declined to the full set of events provided for in REM baseline, summarized in table C.27, shall apply.

C.3.2 New ERDS evidence extensions

C.3.2.1 GeneralEvidenceInfo extension

The Extension (child of Extensions) root element for general additional ERDS information shall be `GeneralEvidenceInfo`, and it shall have "`false`" as value for `isCritical` attribute (see points a) and b) of table C.15 for the relevant implementation guidance).

NOTE 1: The child's elements defined in `GeneralEvidenceInfo` are used in a general way through all the events.

Table C.15: ERDS evidence - composition general extensions requirements

Nº	Service/Protocol element	ETSI EN 319 522-2 [2] main reference	Requirement	Implementation guidance	Notes
1	Extensions/ GeneralEvidenceInfo	Clause 8.2.28 E01	O	a)	see E01 table C.27
2	Extensions/ GeneralEvidenceInfo/ Subject UntrustedPathToRecipient	Clause 8.2.28 E01	O	b)	see E01 table C.27

Implementation guidance:

a) GeneralEvidenceInfo XML structure shall be located at the Extensions / GeneralEvidenceInfo path, as a specific instance of the ERDS evidence Extensions (see the rationales from statement 8 of table B.13). The GeneralEvidenceInfo element is defined in XML Schema file `1953204EvidencexmlSchema.xsd`, whose location is detailed in clause E.1 (see clause C.3.3 at point c) of table C.17 for a top-level illustration of the whole XML structure container of the extensions). The fragment relevant to the present definition is copied below for information. The XML Schema files shall take precedence in case of discrepancies between the XML schema excerpts provided in the present document and the XML Schema files.

```
        <!-- targetNamespace="http://uri.etsi.org/19532/v1#" -->

        <!-- *** (ERDS evidence) EXTENSIONS *** -->

        <!-- *** GeneralEvidenceInfo Element: General ERDS evidence extension elements *** -->

        <xs:element name="GeneralEvidenceInfo" type="GeneralEvidenceInfoType"/>

        <xs:complexType name="GeneralEvidenceInfoType">
                <xs:annotation>
                        <xs:documentation>The GeneralEvidenceInfo's Subject child element contains
the Subject of the original message. Each UntrustedPathToRecipient child element identifies, with a
integer reference, the recipient among all the recipients whose reachability by CSI is not verified.
                        </xs:documentation>
                </xs:annotation>
                <xs:sequence>
                        <xs:element name="Subject" type="xs:string" minOccurs="0"/>
                        <xs:element name="UntrustedPathToRecipient" type="xs:integer" minOccurs="0"
maxOccurs="unbounded"/>
                </xs:sequence>
        </xs:complexType>
...
```

b) The `GeneralEvidenceInfo` extension element shall contain the following elements:

   i. `Subject` element shall be used, when specified by the sender, to capture the subject of the original message as per the semantic defined in ETSI EN 319 522-2 [2], clauses 6.2.14 and 8.2.24, elements MD14/M02.

ii. `UntrustedPathToRecipient` element shall identify, when the present event occurs, the recipient(s), among all the intended recipients, whose reachability is not insurable through the CSI trust & security mechanisms (even if it results practicable with the canonical SMTP flow). For matching an integer value with one of the intended recipients, the first RecipientDetails child element in the list of recipients shall be assigned the number 1.

NOTE 2: This mark can be used as a valid advice for the sender (since the SubmissionAcceptance ERDS evidence) in overt cases of "not ensured recipients" to the REM baseline circuit (e.g. recipients of ordinary email whose domains are instantly recognized by CSI mechanisms as not ensured). But in some cases, the converse is not generally true. A REM message can be sent to an "unregistered" recipient but with an email domain/path perfectly ensured by CSI. In this case, the `UntrustedPathToRecipient` mark is not set in the SubmissionAcceptance ERDS evidence (and so the sender is initially led to believe that the recipient is "ensured" to the REM baseline circuit). Indeed the sender is informed later that the intended recipient is "unregistered" to Recipient's REMS. Sender's REMS receives a RelayReject for the "unregistered" recipient and, in turn, Sender's REMS issues a RelayFailure, with the same warning, for the sender. So to be sure that a recipient is "ensured/registered" to the REM baseline circuit, it is necessary to wait for the cycle completion with either the ContentConsignment or the RelayFailure evidence. Again, `UntrustedPathToRecipient` mark does not represent, in itself, an error condition, nor it is necessarily used together with negative reason codes.

An example of the extension, as mentioned earlier in an ERDS evidence, with some of the fields expressed as per the prescriptions of the present clause, is illustrated in figure C.3.

```
...
    <tns:Extensions>
       <tns:Extension isCritical="false">
          <ext:GeneralEvidenceInfo>
            <ext:Subject>this is the subject</ext:Subject>
            <ext:UntrustedPathToRecipient>2</ext:UntrustedPathToRecipient>
            <ext:UntrustedPathToRecipient>3</ext:UntrustedPathToRecipient>
          </ext:GeneralEvidenceInfo>
       </tns:Extension>
...
    </tns:Extensions>
...
```

Figure C.3: ERDS evidence general extension example

C.3.2.2 RelayEvidenceInfo extension

The Extension (child of Extensions) root element for general additional ERDS information shall be `RelayEvidenceInfo`, and it shall have "`false`" as value for `isCritical` attribute (see point a) of table C.16 for the relevant implementation guidance).

NOTE: The child elements defined in `RelayEvidenceInfo` are used in a peculiar way for relay events.

Table C.16: ERDS evidence - composition relay extensions requirements

Nº	Service/Protocol element	ETSI EN 319 522-2 [2] main reference	Requirement	Implementation guidance	Notes
1	Extensions/ RelayEvidenceInfo/	Clause 8.2.28 E01	O	a)	see E01 table C.27
2	Extensions/ RelayEvidenceInfo/ RelayEvidenceRefersTo	Clause 8.2.28 E01	O	b)	see E01 table C.27

Implementation guidance:

a) RelayEvidenceInfo XML structure shall be located at the Extensions / RelayEvidenceInfo path, as a specific instance of the ERDS evidence Extensions (see the rationales from statement 8 of table B.13). The RelayEvidenceInfo element is defined in XML Schema file `1953204EvidencexmlSchema.xsd`, whose location is detailed in clause E.1 (see clause C.3.3 at point c) of table C.17 for a top-level illustration of the whole XML structure container of the extensions). The fragment relevant to the present definition is copied below for information. The XML Schema files shall take precedence in case of discrepancies between the XML schema excerpts provided in the present document and the XML Schema files.

```
        <!-- targetNamespace="http://uri.etsi.org/19532/v1#" -->

        <!-- *** (ERDS evidence)EXTENSIONS *** -->
...
        <!-- *** RelayEvidenceInfo Element: Relay ERDS evidence extension elements *** -->

        <xs:element name="RelayEvidenceInfo" type="RelayEvidenceInfoType"/>

        <xs:complexType name="RelayEvidenceInfoType">
                <xs:annotation>
                        <xs:documentation>Each RelayEvidenceRefersTo child element identifies, with
a integer reference, one of the intended recipients whose the relay evidence refers to, among all
the RecipientDetails occurrences.
                        </xs:documentation>
                </xs:annotation>
                <xs:sequence>
                        <xs:element name="RelayEvidenceRefersTo" type="xs:integer" minOccurs="0"
maxOccurs="unbounded"/>
                </xs:sequence>
        </xs:complexType>
...
```

b) The `RelayEvidenceInfo` element, composed by a sequence of `RelayEvidenceRefersTo` child elements shall identify, with an integer reference, the recipient(s) whose the relay evidence refers to, among all the intended RecipientDetails occurrences (starting from the number 1 to match the first recipient of the succession, and so on).

An example of the extension, as mentioned earlier in an ERDS evidence, with the fields expressed as per the prescriptions of the present clause is illustrated in figure C.4.

```
...
    <tns:Extensions>
...
       <tns:Extension isCritical="false">
          <ext:RelayEvidenceInfo>
            <ext:RelayEvidenceRefersTo>2</ext:RelayEvidenceRefersTo>
            <ext:RelayEvidenceRefersTo>3</ext:RelayEvidenceRefersTo>
          </ext:RelayEvidenceInfo>
       </tns:Extension>
    </tns:Extensions>
...
```

Figure C.4: ERDS evidence relay extension example

C.3.3 Composition requirements

Table C.17: ERDS evidence - composition top-level requirements

Nº	Service/Protocol element	ETSI EN 319 522-2 [2] main reference	Requirement	Implementation guidance	Notes
1	ERDS evidence	Clause 8	M	a), b), c), d)	Top-level requirements

Implementation guidance:

a) The ERDS evidence instances incorporated as attachments in any REM message shall be composed by a selection of the necessary elements, from the full list in ETSI EN 319 522-2 [2], clause 8, according to the presence and cardinality requirements defined in table C.27 of the clause C.4.5.4 (see the derived rationales from statement 8 of table B.13).

b) The collection of elements constituted according to the previous point a) shall be implemented through an XML structure fully defined by the following three sections:

   i. an XSD wrapping skeleton composed of the namespace definitions and a suitable ordered list of imports, useful for any section in the XSD;

   ii. the main ERDS evidence XSD scheme section (see ETSI EN 319 522-2 [2], clause A.1);

iii. the ERDS Extensions XSD scheme section (see clause C.3.2 and next point c) for the implementation).

c) The whole XML structure container of ERDS evidence, constituted according to the previous points i., ii. and iii. shall be implemented through the REM baseline XML scheme definition for ERDS evidence, defined in XML Schema file `1953204EvidencexmlSchema.xsd`, whose location is detailed in clause E.1, of which a fragment significant in the present clause is copied below for information. The XML Schema files shall take precedence in case of discrepancies between the XML schema excerpts provided in the present document and the XML Schema files.

NOTE 1: The XML Schema file stored at the location indicated above is contained in the attachment en_31953204v010300a0.zip accompanying the present document.

```
<?xml version="1.0" encoding="UTF-8"?>

<!--                  ****** NOTICE ******
The present document is part of ETSI EN 319 532-4 and represents:
  1. the namespaces definitions and
  2. the required imports for REM baseline ERDS evidence schema (Evidence) are composed of:
     - ERDSEvidence
     - ERDSExtensions
     - eIDAS SAML Attribute Profile for Legal and Natural PersonIdentifier
-->

<xs:schema targetNamespace="http://uri.etsi.org/19532/v1#"
                xmlns="http://uri.etsi.org/19532/v1#"
                xmlns:xs="http://www.w3.org/2001/XMLSchema"
                elementFormDefault="qualified" attributeFormDefault="unqualified">

        <!-- *** Imports facility section *** -->

        <!-- schemaLocation="http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/xmldsig-core-
schema.xsd"/> -->
        <xs:import namespace="http://www.w3.org/2000/09/xmldsig#"
                schemaLocation="xmldsig-core-schema.xsd"/>

        <!-- schemaLocation="http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/xenc-schema.xsd"/> -
->
        <xs:import namespace="http://www.w3.org/2001/04/xmlenc#"
                schemaLocation="xenc-schema.xsd"/>

        <!-- schemaLocation="http://www.w3.org/2001/xml.xsd"/> -->
        <xs:import namespace="http://www.w3.org/XML/1998/namespace"
                schemaLocation="xml.xsd"/>

        <!-- schemaLocation="http://docs.oasis-open.org/security/saml/v2.0/saml-schema-assertion-
2.0.xsd"/> -->
        <xs:import namespace="urn:oasis:names:tc:SAML:2.0:assertion"
                schemaLocation="saml-schema-assertion-2.0.xsd"/>

        <!-- schemaLocation="http://uri.etsi.org/19612/v2.2.1/ts_119612v020201_201601xsd.xsd"/> -->
        <xs:import namespace="http://uri.etsi.org/02231/v2#"
                schemaLocation="ts_119612v020201_201601xsd.xsd"/>

        <!-- xsd from 'eIDAS SAML Attribute Profile v1.2.pdf' for Legal PersonIdentifier
definitions, section 2.3.2 - Figure 11 -->
        <xs:import namespace="http://eidas.europa.eu/attributes/legalperson"
                schemaLocation="eIDAS_SAML_Attribute_Profile-LegalPersonIdentifiers-v1.1.2.xsd"/>

        <!-- xsd from 'eIDAS SAML Attribute Profile v1.2.pdf' for Natural PersonIdentifier
definitions, section 2.2.2 - Figure 1 -->
        <xs:import namespace="http://eidas.europa.eu/attributes/naturalperson"
                schemaLocation="eIDAS_SAML_Attribute_Profile-NaturalPersonIdentifiers-v1.1.2.xsd"/>

        <!-- Note: the document 'eIDAS SAML Attribute Profile v1.2.pdf' containing the xsd for the
previous two imports is available at:
https://ec.europa.eu/cefdigital/wiki/download/attachments/82773108/eIDAS%20SAML%20Attribute%20Profil
e%20v1.2%20Final.pdf?version=2&modificationDate=1571068651772&api=v2 -->

        <!-- *** ROOT Element: Evidence *** -->
        <xs:import namespace="http://uri.etsi.org/19522/v1#"
                schemaLocation="1952203xmlSchema.xsd"/>
        <!-- Note: the xsd for the previous import is available at:
https://forge.etsi.org/rep/esi/x19_52203_ERDS/raw/v1.2.1/1952203xmlSchema.xsd -->

        <!-- *** EXTENSIONS *** -->
```

```
        <!-- see clauses C.3.2.1 and C.3.2.2 -->
</xs:schema>
```

NOTE 2: The schema fragment above uses the explicit method of local caching of any XSD namespace needed to be imported to avoid the impact of reloading the schema from the internet every time (consider that in production systems, the validation processes can require hundreds of checks per second, and the download is not practicable). Anyway, the original and canonical location is specified as XML comment just before the import for the once-only first download, or to set always, as location, just in case it is considered favourable.

d) The root element of XSD structure for ERDS evidence, constituted according to the previous points a), b) and c) shall be `Evidence`, and the value of `version` attribute shall be "`EN319522v1.1.1`".

C.3.4 Detail requirements

Table C.18: ERDS evidence - composition specific requirements

Nº	Service/Protocol element	ETSI EN 319 522-2 [2] main reference	Requirement	Implementation guidance	Notes
1	EvidenceIdentifier	Clause 8.2.1 G01	M	a)	see G01 table C.27
2	Version	Clause 8.2.2 G02	M	b)	see G02 table C.27
3	ERDSEventId	Clause 8.2.3 G03	M	c)	see G03 table C.27
4	EventReason	Clause 8.2.4 G04	M	d)	see G04 table C.27
5	EventTime	Clause 8.2.5 G05	M	e)	see G05 table C.27
6	EvidenceIssuerPolicyID	Clause 8.2.7 R01	M	f)	see R01 table C.27
7	EvidenceIssuerDetails	Clause 8.2.8 R02	M	g)	see R02 table C.27
8	SenderDetails/Identity	Clause 8.2.10 I01	O	h)	see I01 table C.27
9	SenderDetails/Identifier	Clause 8.2.11 I02	M	h)	see I02 table C.27
10	RecipientDetails/Identity	Clause 8.2.14 I05	O	i)	see I05 table C.27
11	RecipientDetails/Identifier	Clause 8.2.15 I06	M	i)	see I06 table C.27
12	SubmissionTime	Clause 8.2.25 M03	M/Conditional	j)	see M03 table C.27
13	MessageIdentifier	Clause 8.2.23 M01	M	k)	see M01 table C.27
14	UserContentInfo	Clause 8.2.24 M02	M	l)	see M02 table C.27
15	Signature	Clause 8.2.9 R03	M	m)	see R03 table C.27
16	Extensions	Clause 8.2.28 E01	M/Conditional	n)	see E01 table C.27
17	EvidenceRefersToRecipient	Clause 8.2.18 I09	M/Conditional	o)	see I09 table C.27
18	Sender/AssuranceLevelsDetails	Clause 8.2.19 I10	M/Conditional	p)	see I10 table C.27
19	ExternalERDSDetails	Clause 8.2.27 M05	M/Conditional	q)	see M05 table C.27
NOTE: The "Conditional" requirement category is used in addition to that defined in table 1, with the meaning that the relevant requirement is subject to particular conditions made explicit in the implementation guidance and related notes.					

Implementation guidance:

a) The EvidenceIdentifier element shall be a UID generated according to IETF RFC 5322 [8], clause 3.6.4.

NOTE 1: Void.

b) The `version` attribute shall be set to "EN319522v1.1.1".

c) The `ERDSEventId` element shall be one of the URI of table 2 of ETSI EN 319 522-3 [3], clause 5.2.2.5 according to one of the events foreseen for REM baseline and illustrated in clauses C.4.5.1, C.4.5.2 and C.4.5.3. (see the item G03 of table C.27 for the full list of admitted events, and the URI in column 1, table 3 of ETSI EN 319 522-3 [3], clause 5.2.2.5).

d) The `EventReason` element shall be set as follows:

I. `Code`: field set to the appropriate URI of table 3 of ETSI EN 319 522-3 [3], clause 5.2.2.7 according to one of the reasons, summarized in the 'URI code' cell of table C.28 for REM baseline, as prescribed in clauses C.4.5.1, C.4.5.2 and C.4.5.3.

II. first `Details`: field set to the appropriate 'Details code' value, from the second column of table C.28.

III. second `Details`: field set to the appropriate 'reason details' textual description of the event reason, got from the third column of table C.28. Other possible `Details` components shall appear after the two canonical elements, as for the previous prescription.

EXAMPLE 1:

```
<tns:EventReasons>
<tns:EventReason>
    <Code>http://uri.etsi.org/19522/EventReason/MessageAccepted</Code>
    <Details>RA01</Details>
    <Details>Message accepted</Details>
    <Details>[...] optional rows with text, if any, with further details [...]</Details>
    <Details>[...] ... [...]</Details>                    </tns:EventReason>
</tns:EventReasons>
```

e) The `EventTime` element shall be set with the time raising the event (see instant time T0 in figure B.9, figure B.10, figure B.11 and figure B.12).

f) The `EvidenceIssuerPolicyID` element shall be set at least with the following URIs (see clause D.1.3):

I. http://uri.etsi.org/19532/v1#/REMbaseline.

II. <URI of the "en" International/English page of the REMID policy specified in CSISchemePolicyCommunityRules element of CapabilityAndSecurityInformation> (e.g. https://CC-remid-authority.cc/remid-policy-en.html).

g) The EvidenceIssuerDetails element shall be set as follows, according to eIDAS TS SAML Attribute Profile [15], clauses 2.3.2 and 2.3.4 of which an excerpt is copied below for information:

```
<tns:EvidenceIssuerDetails>
      <tns:Identity>
         <saml:Attribute
            FriendlyName="LegalName"
            Name="http://eidas.europa.eu/attributes/legalperson/LegalName"
            NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
            <saml:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xsi:type="elp:LegalNameType">"LEGAL NAME OF THE SERVICE PROVIDER"
            </saml:AttributeValue>
         </saml:Attribute>
      </tns:Identity>
   </tns:EvidenceIssuerDetails>
```

Where:

- The value *"LEGAL NAME OF THE SERVICE PROVIDER"* shall be set to the same value used in the ERDSGoverningBody ERDSMetadata element (see point c.3.3.2 of table C.8).
- The other attribute values shall be set as per the excerpt above.

NOTE 2: The namespace prefixes `tns`, `saml`, `xsi`, `elp` are not fixed and have the usual role in an XML.

h) The SenderDetails/Sender's Identity attributes element shall be set as follows, according to eIDAS TS SAML Attribute Profile [15], clauses 2.2.2 and 2.2.3 of which an excerpt is copied below for information (see also the best practices at statement 3) of the clause D.4.2):

I. I01: this component shall be used only for users belonging to qualified REMSP and according to the presence requirement summarized in table C.27 (and possibly, to further arrangements at **REMID policy** intended to reinforce its adoption during the issuing of the ERDS evidence).

```
      <tns:Identity>
          <saml:Attribute
              FriendlyName="PersonIdentifier"
              Name="http://eidas.europa.eu/attributes/naturalperson/PersonIdentifier"
              NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
              <saml:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance" xsi:type="enp:PersonIdentifierType">"Source CC"/"Dest CC"/"userid"
              </saml:AttributeValue>
          </saml:Attribute>
      </tns:Identity>
```

Where:

- The value "Source CC"/"Dest CC"/"userid" should be set as follows:
  - "Source CC": the Country Code of the «user» (the sender in this case)
  - "Dest CC": the Country Code of the REMSP (the pertinent EU MS of the **sender**'s REMSP in this case)
  - "userid": the sha256 digest (transformed in uppercase) of the user's email (picked up in lowercase)

EXAMPLE 2: ES/IT/466FA5C7D106870115F12BABFE65B7A3647E828B65BA0EBE5B5D38691DCC8F78

ES for a *Spanish* user
IT for an *Italian* REMSP
466FA5C7D106870115F12BABFE65B7A3647E828B65BA0EBE5B5D38691DCC8F78
for the *sender@s-rems.rem* email

- The other attribute values shall be set as per the excerpt above.

NOTE 3: The namespace prefixes tns, saml, xsi, enp are not fixed and have the usual role in an XML.

NOTE 4: If the issuer of the ERDS evidence is the **sender**'s REMSP, it is, by definition, the entity to which the sender is "registered". Therefore, the **sender**'s REMSP has all the information to fill in the I01 component. And conversely, when the issuer of the ERDS evidence is the **recipient**'s REMSP, it has, as a starting point, the SubmissionAcceptance ERDS evidence attached to the REM dispatch which can be used as source information to fill in the I01 component.
Whereas, the user referred to by the I01 identity component - represented in a neutral way by a *natural person* saml attribute identifier - is used to represent both natural or legal persons (see note in eIDAS TS SAML Attribute Profile [15], clause 2.3.3).

II. I02: the value of this component represented below as "sender's email addr" shall contain only the clean addr-spec part of the email address (that is the local-part "@" domain without angle brackets "<" and ">") as defined in IETF RFC 5322 [8], clause 3.4 and 3.4.1 (see the example in figure C.5).
<Identifier IdentifierSchemeName="mailto">"sender's email addr"</Identifier>

i) The RecipientDetails/Recipient's Identity attributes element shall be set as follows, according to eIDAS TS SAML Attribute Profile [15], clauses 2.2.2 and 2.2.3 of which an excerpt is copied below for information (see also the best practices at statement 3) of the clause D.4.2):

I. I05: this component (one instance for each intended recipient) shall be used only for users belonging to qualified REMSP and according to the presence requirement summarized in table C.27 (and possibly, to further arrangements at **REMID policy** intended to reinforce its adoption during the issuing of the ERDS evidence).

```
<tns:Identity>
    <saml:Attribute
        FriendlyName="PersonIdentifier"
        Name="http://eidas.europa.eu/attributes/naturalperson/PersonIdentifier"
        NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
        <saml:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance" xsi:type="enp:PersonIdentifierType">
            "Source CC"/"Dest CC"/"userid"
        </saml:AttributeValue>
    </saml:Attribute>
</tns:Identity>
```

Where:

- The value "Source CC"/"Dest CC"/"userid" should be set as follows:
  - "Source CC": the Country Code of the «user» (the **recipient** in this case)
  - "Dest CC": the Country Code of the REMSP (the pertinent EU MS of the **recipient**'s REMSP in this case)
- "userid": sha256 digest (transformed in uppercase) of the user's email (picked up in lowercase).

EXAMPLE 3: `DE/DE/3A7D68B6BD4C5CF1EB8D3F22E58679419AC5BBA466650035E73B2F54349F9868`

`DE` for a *German* user
`DE` for a *German* REMSP
`3A7D68B6BD4C5CF1EB8D3F22E58679419AC5BBA466650035E73B2F54349F9868`
for the *recipient@r-rems.rem* email

- The other attribute values shall be set as per the excerpt above.

NOTE 5: The namespace prefixes `tns`, `saml`, `xsi`, `enp` are not fixed and have the usual role in an XML.

NOTE 6: If the issuer of the ERDS evidence is the **sender**'s REMSP, it usually does not have the information to fill in the I05 component (unless, for example, the case where S-REMS = R-REMS). Typically, such feature is not present except in instances where an ERDS evidence is issued after or as a consequence of another ERDS evidence coming from R-REMS (e.g. the issuing of a RelayFailure ERDS evidence as a result of a RelayRejection evidence): in such events, the triggering ERDS evidence, coming from R-REMS (and so having the I05 component, as explained below) can be used as source information to fill in the I05 component.
And conversely, when the issuer of the ERDS evidence is the **recipient**'s REMSP, it is, by definition, the entity to which the recipient is "registered". Therefore, the **recipient**'s REMSP has all the information to fill in the I05 component.
Whereas, the user referred to by the I01 identity component - represented in a neutral way by a *natural person* saml attribute identifier - is used to represent both natural or legal persons (see note in eIDAS TS SAML Attribute Profile [15], clause 2.3.3).

II. I06: the value of this component represented below as "recipient's email addr" shall contain only the clean addr-spec part of the email address (that is the local-part "@" domain without angle brackets "<" and ">") as defined in IETF RFC 5322 [8], clause 3.4 and 3.4.1 (see the example in figure C.5).
<Identifier IdentifierSchemeName="mailto">"recipient's email addr"</Identifier>

j) The SubmissionTime element shall be set with the time raising the initial delivery process (see instant time T0 in figure B.9) that have to be "copied" to the M03 element of any ERDS evidence according to the presence and cardinality requirements defined in table C.27 of the clause C.4.5.4.

k) The MessageIdentifier element shall be a UID generated according to IETF RFC 5322 [8], clause 3.6.4 (see also point a) above).

l) The UserContentInfo element shall be set as follows:

```
<tns:UserContentInfo>
   <AppLayerIdentifier>"UA message-ID"</AppLayerIdentifier>
   <ComposingParts>1</ComposingParts>
   <tns:PartsInfo>
      <tns:PartInfo>
         <Identifier>urn:oid:1.3.6.1.7</Identifier>
         <ContentType>message/rfc822</ContentType>
         <ds:DigestMethod Algorithm="URI of used algorithm"/>
         <ds:DigestValue>"base64 val computed with the DigestMethod"</ds:DigestValue>
      </tns:PartInfo>
   </tns:PartsInfo>
</tns:UserContentInfo>
```

Where, about the variable parts:

- The value of the element `"AppLayerIdentifier"` shall be set to the original message's Message-ID header taking care of the necessary transcoding of the not admitted characters in the values of XML elements (e.g. the '<' and '>' characters, systematically present in Message-ID headers, are translated in '< ' and '>' entities)

NOTE 7: `"AppLayerIdentifier"` element value has the same value as the header MD14/REM-UAMessageIdentifier, apart from the XML transcoding not used in email headers.

- The value of the attribute `PartInfo/DigestMethod Algorithm` shall be set according to clause C.4.5.1 table C.22 point c)/IV.

NOTE 8: `"DigestMethod Algorithm"` attribute value has the same value as the header MD14/REM-DigestAlgorithm.

- The value of the element `PartInfo/DigestValue` shall be set according to clause C.4.5.1 table C.22 point c)/V.

NOTE 9: `"DigestValue"` has the same value as the header MD14/REM-DigestValue.

NOTE 10: The namespace prefixes `tns` and `ds` are not fixed and have the usual role in an XML.

m) The Signature element shall include digital signature and time-stamp token as defined in clauses C.4.3 and C.4.4.

n) The Extension element shall be set according to clause C.3.2 table C.15 and table C.16.

o) The EvidenceRefersToRecipient element shall be set according to ETSI EN 319 522-3 [3], clause 5.2.2.21 (see clause C.4.5.3, table C.25 points a)II, h)I, h)II and i)II for specific usage of this element).

p) The Sender/AssuranceLevelsDetails element shall be set according to ETSI EN 319 522-3 [3], clause 4.3.14 selecting the choices of the XSD definitions to assume the following XML structure:

```
<AssuranceLevelsDetails>
    <GlobalAssuranceLevel>
        <AssuranceLevel>"assurance level URI"</AssuranceLevel>
        <PolicyID>"assurance level policy URI"</PolicyID>
    </GlobalAssuranceLevel>
    <tns:AuthenticationDetails>
        <AuthenticationTime>"authentication time"</AuthenticationTime>
        <AuthenticationMethod>"authentication method URI"</AuthenticationMethod>
    </tns:AuthenticationDetails>
</AssuranceLevelsDetails>
```

Where:

- The `"AssuranceLevel"` element value shall be set to the URI: `http://eidas.europa.eu/LoA/substantial`
- The `"PolicyID"` element value shall be set to a URI referencing the assurance levels definitions
- The "`AuthenticationTime`" element value should be set as follows:
  - The time of the session authentication, in case of web authentications or any case providing session mechanism.
  - The closest one authentication time to the submission event, in other cases, (i.e. when there are multiple authentications before the submission event).

q) The ExternalERDSDetails element refers to the counterpart service, in respect to the ERDS evidence issuer, and shall be set as follows, according to eIDAS TS SAML Attribute Profile [15], clauses 2.3.2 and 2.3.4 of which a fragment is copied below for information:

```
<tns:ExternalERDSDetails>
   <tns:Identity>
      <saml:Attribute
         FriendlyName="LegalName"
         Name="http://eidas.europa.eu/attributes/legalperson/LegalName"
         NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
         <saml:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="elp:LegalNameType">"LEGAL NAME OF THE SERVICE PROVIDER"
         </saml:AttributeValue>
      </saml:Attribute>
   </tns:Identity>
</tns:ExternalERDSDetails>
```

Where:

- The value *`"LEGAL NAME OF THE SERVICE PROVIDER"`* shall be set to the same value used in ERDSGoverningBody ERDSMetadata element of the "other party" of the transaction in respect to the issuer (see element g) above for the issuer counterpart, and point c.3.3.2 of table C.8).
- The other attribute values shall be set as per the excerpt above.

NOTE 11: The namespace prefixes `tns`, `saml`, `xsi`, `elp` are not fixed and they assume the classical role they have in an XML.

A complete example of ERDS evidence for SubmissionAcceptance event with some of the fields expressed as per the prescriptions of the present clause C.3 is illustrated in figure C.5.

```
<?xml version="1.0" encoding="UTF-8"?>
<!--
The present document is an XML example for ETSI EN 319 532-4 and represents:
  1. the namespaces definitions relevant to an ERDS evidence exemplification for REM baseline

  2. an ERDS evidence XML structure composed by:
     - Evidence
-->

<tns:Evidence version="EN319522v1.1.1"
     xmlns:tns="http://uri.etsi.org/19522/v1#"
     xmlns:ext="http://uri.etsi.org/19532/v1#"
     xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
     xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
     xmlns:elp="http://eidas.europa.eu/attributes/legalperson"
     xmlns:enp="http://eidas.europa.eu/attributes/naturalperson">

    <tns:EvidenceIdentifier>76A0CF65.00566CE0.025BE6B4.03B4A2C1.rem-service@s-
rems.rem</tns:EvidenceIdentifier>

    <tns:ERDSEventId>http://uri.etsi.org/19522/Event/SubmissionAcceptance</tns:ERDSEventId>

    <tns:EventReasons>
       <tns:EventReason>
          <Code>http://uri.etsi.org/19522/EventReason/MessageAccepted</Code>
          <Details>RA01</Details>
          <Details>Message accepted</Details>
       </tns:EventReason>
    </tns:EventReasons>

    <EventTime>2018-01-16T07:30:00Z</EventTime>

    <tns:EvidenceIssuerPolicyID>
       <PolicyID>http://uri.etsi.org/19532/v1#/REMbaseline</PolicyID>
       <PolicyID>https://CC-remid-authority.cc/remid-policy-en.html</PolicyID>
    </tns:EvidenceIssuerPolicyID>

    <tns:EvidenceIssuerDetails>
        <tns:Identity>
            <saml:Attribute
                  FriendlyName="LegalName"
                  Name="http://eidas.europa.eu/attributes/legalperson/LegalName"
                  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
                  <saml:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="elp:LegalNameType">S-REMS provider</saml:AttributeValue>
            </saml:Attribute>
        </tns:Identity>
    </tns:EvidenceIssuerDetails>

    <tns:SenderDetails>
        <tns:Identity>
            <saml:Attribute
                  FriendlyName="PersonIdentifier"
                  Name="http://eidas.europa.eu/attributes/naturalperson/PersonIdentifier"
                  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
                  <saml:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="enp:PersonIdentifierType">CC/CC/466FA5C7D106870115F12BABFE65B7A3647E828B65BA0EBE5B5D38691D
CC8F78</saml:AttributeValue>
            </saml:Attribute>
        </tns:Identity>
        <Identifier IdentifierSchemeName="mailto">sender@s-rems.rem</Identifier>
        <AssuranceLevelsDetails>
            <GlobalAssuranceLevel>
                <AssuranceLevel>http://eidas.europa.eu/LoA/substantial</AssuranceLevel>
                <PolicyID>https://CC-remid-authority.cc/rem-policy-cc#assurance-level-
policy</PolicyID>
            </GlobalAssuranceLevel>
            <tns:AuthenticationDetails>
                <AuthenticationTime>2018-01-16T07:25:00Z</AuthenticationTime>
                <AuthenticationMethod>https://CC-remid-authority.cc/rem-policy-cc#authentication-
method</AuthenticationMethod>
```

```
            </tns:AuthenticationDetails>
         </AssuranceLevelsDetails>
    </tns:SenderDetails>

    <tns:RecipientDetails>
        <Identifier IdentifierSchemeName="mailto">recipient@r-rems.rem</Identifier>
    </tns:RecipientDetails>

    <tns:SubmissionTime>2018-01-16T08:30:00Z</tns:SubmissionTime>

    <tns:MessageIdentifier>76A0CF65.00566CE0.025BE6B4.85251369.rem-service@s-
rems.rem</tns:MessageIdentifier>

    <tns:UserContentInfo>
       <AppLayerIdentifier>&lt;00be01d30072$fde7b950$f9b72bf0$@de&gt;</AppLayerIdentifier>
       <ComposingParts>1</ComposingParts>
       <tns:PartsInfo>
          <tns:PartInfo>
             <Identifier>urn:oid:1.3.6.1.7</Identifier>
             <ContentType>message/rfc822</ContentType>
             <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
             <ds:DigestValue>km8noxERawpFLnZ8ARP7p4zcktEFF9ABmw9SqpvIPc4=</ds:DigestValue>
          </tns:PartInfo>
       </tns:PartsInfo>
    </tns:UserContentInfo>
    <tns:Extensions>
       <tns:Extension isCritical="false">
          <ext:GeneralEvidenceInfo>
            <ext:Subject>Purchase order #1237</ext:Subject>
          </ext:GeneralEvidenceInfo>
       </tns:Extension>
    </tns:Extensions>
    <dsig:Signature {...} Id="abc000"><!-- THE XAdES-B-T SIGNATURE HERE ... -->
       <dsig:SignedInfo><!—{...}--></dsig:SignedInfo>
       <ds:SignatureValue {...} Id="abc111">{...}</ds:SignatureValue>
       <ds:KeyInfo>
          <ds:X509Data>
             <ds:X509Certificate>{...}</ds:X509Certificate>
             <ds:X509Certificate>{...}</ds:X509Certificate>
          </ds:X509Data>
       </ds:KeyInfo>
       <ds:Object>
          <xades:QualifyingProperties {...} Target="abc222">
             <xades:SignedProperties Id="abc333">
                <xades:SignedSignatureProperties>{...}</xades:SignedSignatureProperties>
             </xades:SignedProperties>
             <xades:UnsignedProperties>
                <xades:UnsignedSignatureProperties>
                   <xades:SignatureTimeStamp Id="abc444">{...}</xades:SignatureTimeStamp>
                </xades:UnsignedSignatureProperties>
             </xades:UnsignedProperties>
          </xades:QualifyingProperties>
       </ds:Object>
    </dsig:Signature>
</tns:Evidence>
```

Figure C.5: Detailed ERDS evidence example

C.4 Digital signatures and time-stamp

C.4.1 Overview

Clause C.4 specifies the minimum requirements for the digital signatures and time-stamp application in **REM messaging**.

NOTE 1: The implementation guidance of the tables of clause C.4 do not intend to establish a rigid schema of execution (e.g. comparable to a flow chart of a program). But rather, the whole purpose of them is to provide a high level description of the contexts and of the main points where and how digital signatures, time-stamps and other significant prescriptions of REM baseline have to be applied.

NOTE 2: Definitive failures arising during any best-effort activities are typically logged as permanent errors that interrupts the normal course of the REM transaction.

C.4.2 REM messages - digital signature provisions

Regarding digital signatures, signing all the components of REM messages, the requirements given and explained in ETSI EN 319 532-3 [6], clause 8.3 shall apply to REM baseline according to the provisions of the present clause.

Regarding the REM messages formats and EML structure composition, the requirements given and explained in ETSI EN 319 532-3 [6], clause 6 shall apply to REM baseline according to the provisions of the present clause.

The requirements on presence, cardinality and annotations, declined to the full set of events provided for in REM baseline, summarized in table C.26 shall apply.

Table C.19: Digital signature - REM messages

Nº	Service/Protocol element	ETSI EN 319 532-3 [6] main reference	Requirement	Implementation guidance	Notes
1	REM message digital signature	Clause 8.3	M	a), b)	

Implementation guidance:

a) The digital signature shall be a CAdES baseline signature according to the semantics specified in ETSI EN 319 522-2 [2], clause 8.2.9, and the baseline signature as specified in ETSI EN 319 122-1 [13], clause 6 (see time T5 in figure B.9, figure B.10, figure B.11, figure B.12).

b) The **REMID policy** should specify either if this digital signature includes the signed attribute signature-policy-identifier, containing the explicit identifier of the signature policy governing the local signing and validating processes or that the signature policy is directly specified inside the **REMID policy** and such attribute is not used (see also point II in clause C.2.3.5, clauses D.1.3 and D.2.2.3).

NOTE: Once the CAdES-B-B baseline signature has been generated, it is not necessary that it is augmented to a CAdES-B-T baseline signature for the incorporation of the time-stamp token since the time-stamp is applied only once per transaction in ERDS evidence (see the derived rationales from statement 1 of table B.13).

C.4.3 ERDS evidence - digital signature provisions

Regarding digital signatures, individually signing the XML structure of any ERDS evidence, the requirements given and explained in ETSI EN 319 522-2 [2], clause 7.2 shall apply to REM baseline according to the provisions of the present clause.

Table C.20: Digital signature - ERDS evidence

Nº	Service/Protocol element	ETSI EN 319 522-2 [2] main reference	Requirement	Implementation guidance	Notes
1	ERDS evidence digital signature	Clause 7.2	M	c), d)	

Implementation guidance:

c) The digital signature shall be a XAdES-B-B baseline signature specified in ETSI EN 319 132-1 [14] (see time T3 in figure B.9, figure B.10, figure B.11, figure B.12).

d) The **REMID policy** should specify either if this digital signature includes the signed attribute signature-policy-identifier, containing the explicit identifier of the signature policy governing the local signing and validating processes or that the signature policy is directly specified inside the **REMID policy** and such attribute is not used (see also point II in clause C.2.3.5, clauses D.1.3 and D.2.2.3).

C.4.4 ERDS evidence - time-stamp provisions

Regarding the time-stamp, incorporating the signature timestamp as an indirect time-stamp on the ERDS evidence itself, the requirements given and explained in ETSI EN 319 522-2 [2], clause 7.2 shall apply to REM baseline according to the provisions of the present clause.

Table C.21: Time-stamp - ERDS evidence

Nº	Service/Protocol element	ETSI EN 319 522-2 [2] main reference	Requirement	Implementation guidance	Notes
1	ERDS evidence time-stamp	Clause 7.2	M	e)	

Implementation guidance:

e) A signature time-stamp shall be added to the digital signature of evidence as follows:

Once the XAdES-B-B baseline signature has been generated, it shall be augmented to a XAdES-B-T baseline signature level, by incorporation into the digital signature of the unsigned attribute signature-timestamp, containing a time-stamp token computed as specified in ETSI EN 319 132-1 [14], clause 6 (see time T4 in figure B.9, figure B.10, figure B.11 and figure B.12).

NOTE: This time-stamp token supports requirements related to the time-stamping of ERDS evidence that different regulatory frameworks can define; in particular, this can support the requirements on time-stamping defined by the Regulation (EU) No 910/2014 [i.1], Article 44.

C.4.5 Specific applications

C.4.5.1 Submission event

With regards to the application of digital signatures and time-stamp to ERDS evidence, and digital signatures to REM messages during the submission event, the constraints of clause 5.5.1.1, elements 1 and 2, shall apply to REM baseline according to the provisions of the present clause (see ETSI EN 319 532-1 [4], clause 6.2.1 for a full description of the events mentioned in the present clause).

Table C.22: Submission - ERDS evidence signature and time-stamp

Nº	Service/Protocol element	ETSI EN 319 522-1 [1] main reference	Requirement	Implementation guidance	Notes
1	SubmissionAcceptance	Clause 6.2.1 A.1.	M	a), b), c), d), e), f), g)	Acceptance event
2	SubmissionRejection	Clause 6.2.1 A.2.	M	a), b), c), d), e), f), g), h)	Rejection event

Implementation guidance:

a) The "submission" event phase of the original message to the S-REMS (see time T0 in figure B.9 of clause B.3.2) is composed of a list of steps among which a number of checks. After the formal and security checks, the S-REMS has in charge the application of the digital signature and the time-stamp to the ERDS evidence for such event (composed as per clause C.3), and the application of the digital signature to both REM dispatch and REMS receipt. This process shall be framed, substantially, as follows:

I. If any of the formal or security checks fail, the submission acceptance process shall be interrupted; and the flow continues from point h) with a SubmissionRejection.

II. Otherwise, if all the checks of the previous step I. succeed, the flow shall continue with point b) assigning the value `http://uri.etsi.org/19522/Event/SubmissionAcceptance` to the `ERDSEventId` element of a SubmissionAcceptance ERDS evidence, and the `EventReason/Code` set to the URI `http://uri.etsi.org/19522/EventReason/MessageAccepted`.

b) The time reference T0 of the "submission" phase shall be set to the G05 `EventTime` element of the ERDS evidence according to the semantic of ETSI EN 319 522-2 [2], clause 8.2.5 (see time T0 in figure B.9 of clause B.3.2).

c) A "digest" of the entire "original message" shall be assigned to the digest child field of M02 (same as MD14) element of the ERDS evidence (see time T1 in figure B.9 of clause B.3.2) in the context of the following process:

   I. ComposingParts child field of an element of UserContentInfo shall be set to 1.

   II. Identifier child field of element of UserContentInfo shall be set to "urn:oid:1.3.6.1.7" (that represents the identifier for iso(1) org(3) dod(6) internet(1) mail(7) OID, as defined in IANA SMI OID numbers).

   III. ContentType child field of an element of UserContentInfo shall be set to "message/rfc822".

   IV. `DigestMethod` child field of an element of `UserContentInfo` shall be set to an algorithm, amongst those identified in the security policy as per the current best practice, in the form of a URI according to the element REM-DigestAlgorithm defined in ETSI EN 319 532-3 [6], table 2 (see also clause D.1.3).

   V. `DigestValue` child field of an element of `UserContentInfo` shall be set to the base64Binary encoded digest value of original message (candidate to be attached in the '`Content-Type: message/rfc822; name=AttachedMimeMessage`' MIME section of the REM dispatch) as computed using the digest algorithm indicated in the `DigestMethod` as mentioned earlier field. Such digest shall be calculated as follows:

      i. normalization of the original message (e.g. some operation like the canonization of the Message-ID, etc. can be performed on the original message before its inclusion in the REM dispatch: the digest is computed after any change on it)

      ii. binary digest, according to the attribute `PartInfo/DigestMethod Algorithm` (e.g. sha256) considering the original message as a 'CRLF terminated' file (i.e. provided also with final 0x0D0A bytes at the end-of-file)

NOTE 1: Once the original message is attached inside the REM dispatch as rfc822 message media type MIME part, two CRLFs/line breaks appear in the MIME stream at the end of such part: the first is composed by the 0x0D0A sequence representing the end-of-file of the original message, and the second CRLF is due to the requirement prescribed in IETF RFC 2046 [i.14], clause 5.1.1 (to have any boundary, and so also the epilogue of the original message, at the beginning of the line). The unambiguous individuation of the correct portion of the REM dispatch representing the original message (ending with the first CRLF) upon which re-compute the digest is fundamental during the check phases.

d) The XML structure of the ERDS evidence shall be filled with the necessary values (see time T2 in figure B.9 of clause B.3.2) as follows:

   I. `EvidenceIssuerPolicyID` element of the ERDS evidence shall have a URI set to `http://uri.etsi.org/19532/v1#/REMbaseline` and shall match the value of ERDSProfileSupported element of ERDSMetadata (see c.3.3.3 of table C.8 and clause D.1.3)

   II. All the other contents and elements of ERDS evidence shall be set according to clause C.3

e) A standard XAdES-B-B baseline digital signature is applied to the XML evidence structure according to the provisions of clause C.4.3 (see time T3 in figure B.9 of clause B.3.2).

f) A **standard time-stamp** is generated and applied on top of the XAdES-B-B augmenting the signature level to XAdES-B-T according to the provisions of clause C.4.4 (see time T4 in figure B.9 of clause B.3.2). The ERDS evidence XML structure is ready to be "released" by the process of signature and time-stamp.

g) If there are no errors the ERDS evidence XML structure shall be attached to the REM dispatch built according to clauses 5.4 and C.4.2, that can continue the flow with the relay event defined in clause C.4.5.2; and the same ERDS evidence XML structure shall be attached to a SubmissionAcceptance REMS receipt, built according to clauses 5.4 and C.4.2, to be sent back to the sender (see time T5 in figure B.9 of clause B.3.2).

h) If one of the previous steps fails, the REM service shall issue the ERDS evidence to attach to a REMS receipt that has to be sent back to the sender. This process shall be framed, substantially, in the best-effort way, as described in I. and II. for permanent failures, and in III. for transient failures:

I. The value `http://uri.etsi.org/19522/Event/SubmissionRejection` shall be set to the `ERDSEventId` element of the ERDS evidence; the appropriate `Code` and `Details` about the formal or security checks failed or any other error condition shall be set to the `EventReason` element (see the URIs of table 3 of ETSI EN 319 522-3 [3], clause 5.2.2.7 for the full list of Codes, and the columns DCode and RDetails of table C.28 of the present document for the relevant full list of Details). This is the case where there are no errors in the new execution of steps from b) to f) on such ERDS evidence: it shall be attached to a SubmissionRejection REMS receipt, built according to clauses 5.4 and C.4.2, to be sent back (in a best-effort way) to the sender.

II. The value `http://uri.etsi.org/19522/Event/SubmissionRejection` shall be set to the `ERDSEventId` element of the ERDS evidence; the appropriate `Code` and `Details` about the formal or security checks failed or any other error condition shall be set to the `EventReason` element (see the URIs of table 3 of ETSI EN 319 522-3 [3], clause 5.2.2.7 for the full list of Codes, and the columns DCode and RDetails of table C.28 of the present document for the relevant full list of Details). This is the case where there is a permanent error during the new execution of some step from b) to f) on such ERDS evidence: it may be further completed with the details of this additional error in the best-effort way; and it (even if not complete) shall be attached to a SubmissionRejection REMS receipt, built according to clauses 5.4 and C.4.2, to try to send it back (in a best-effort way) to the sender.

III. If there is some transient error on any step from b) to f), the process shall try to recover the error within a timeout fixed in the **REMID policy** (see clauses C.2.3.5 and D.1.3); if the error is back, the process shall continue with the step g); otherwise, in any case, the error is considered persistent, and the REM service shall issue the ERDS evidence to attach to a REMS receipt that has to be sent back to the sender. This process shall be framed, substantially, in the best-effort way, as described in I. or II.

NOTE 2: In both cases I. and II. above, there can be additional rules in local **REMID policy** that dispose of particular preservations and management practices on the REM dispatch in case of "security violations and threats" specified in the policy (see clause C.2.3.5). Anyway, none of these "additional" practices breaks the interoperability.

C.4.5.2 Relay event

With regards to the application of digital signatures and time-stamp to ERDS evidence, and digital signatures to REM messages during the relay event, the constraints of clause 5.5.1.3, elements 1, 2 and 3 shall apply to REM baseline according to the provisions of the present clause (see ETSI EN 319 532-1 [4], clause 6.2.2 for a full description of the events mentioned in the present clause).

Table C.23: Relay (R-REMS side) - ERDS evidence signature and time-stamp

Nº	Service/Protocol element	ETSI EN 319 522-1 [1] main reference	Requirement	Implementation guidance	Notes
1	RelayAcceptance	Clause 6.6.2 B.1.	M	a), b), c), d), e), f), g), i)	Relay event
2	RelayRejection	Clause 6.6.2 B.2.	M	a), b), c), d), e), f), g), h), i)	RelayRejection event

Implementation guidance:

a) The "accepting" event phase, at R-REMS side, of the "REM dispatch" relayed by S-REMS (see time T0 in figure B.10 of clause B.3.3) is composed of a list of steps among which a number of checks. After the formal and security checks, the R-REMS has in charge the application of the digital signature and the time-stamp to the ERDS evidence for such event (composed as per clause C.3), and the application of the digital signature to the REMS receipt. This process shall be framed, substantially, as follows:

I. If any of the formal or security checks fail the relay acceptance process shall be interrupted; and the flow continues from point h) with a RelayRejection.

II. Otherwise, if all the checks of the previous step I. succeed, the flow shall continue with point b) assigning the value `http://uri.etsi.org/19522/Event/RelayAcceptance` to the `ERDSEventId` element of a RelayAcceptance ERDS evidence, the `EventReason/Code` set to the URI `http://uri.etsi.org/19522/EventReason/S_ERDS_MessageSuccessfullyRelayed` and the `Extensions/RelayEvidenceRefersTo` element set to the recipient(s) that the evidence refers to, among all, the intended recipients (see note b of table C.27).

b) The time reference T0 of the "accepting" phase shall be set to the G05 `EventTime` element of the ERDS evidence according to the semantic of ETSI EN 319 522-2 [2], clause 8.2.5 (see time T0 in figure B.10 of clause B.3.3).

c) The "digest" of the "original message" contained in M02 ERDS evidence element of REM dispatch shall be assigned, by copy, to the digest child field of M02 (same as MD14) element of the ERDS evidence (see time T1 in figure B.10 of clause B.3.3) in the context of the following process:

I. ComposingParts child field of UserContentInfo element shall be set to 1.

II. Identifier child field of an element of UserContentInfo shall be set to "urn:oid:1.3.6.1.7" (that represents the identifier for iso(1) org(3) dod(6) internet(1) mail(7) OID, as defined in IANA SMI OID numbers).

III. ContentType child field of an element of UserContentInfo shall be set to "message/rfc822".

IV. DigestMethod child field of an element of UserContentInfo shall be set as a "copy" of the digest method taken from DigestMethod child field of an element of the ERDS evidence attached in REM dispatch.

V. DigestValue child field of an element of UserContentInfo shall be set to as a "copy" of the base64 encoded digest value of original message taken from ERDS evidence attached in REM dispatch (that has been computed using the digest algorithm indicated in the DigestMethod as mentioned earlier field).

d) The XML structure of the ERDS evidence shall be filled with the necessary values (see time T2 in figure B.10 of clause B.3.3) as follows:

I. `EvidenceIssuerPolicyID` element of the ERDS evidence shall have a URI set to `http://uri.etsi.org/19532/v1#/REMbaseline` and shall match the value of ERDSProfileSupported element of ERDSMetadata (see c.3.3.3 of table C.8 and clause D.1.3).

II. All the other contents and elements of ERDS evidence shall be set according to clause C.3.

e) A standard XAdES-B-B baseline digital signature is applied to the XML evidence structure according to the provisions of clause C.4.3 (see time T3 in figure B.10 of clause B.3.3).

f) A **standard time-stamp** is generated and applied on top of the XAdES-B-B augmenting the signature level to XAdES-B-T according to the provisions of clause C.4.4 (see time T4 in figure B.10 of clause B.3.3), and the ERDS evidence XML structure is ready to be "released" by the process of signature and time-stamp.

g) If there are no errors, the ERDS evidence XML structure shall be attached to a RelayAcceptance REMS receipt, built according to clauses 5.4 and C.4.2, to be sent back to the S-REMS (see time T5 in figure B.10 of clause B.3.3); and the REM dispatch can continue the flow with the consignment event defined in clause C.4.5.3.

h) If one of the previous steps fails, the REM service shall issue the ERDS evidence to attach to a REMS receipt that has to be sent back to the S-REMS. This process shall be framed, substantially, in the best-effort way, as described in I. and II. for permanent failures, and in III. for transient failures:

I. The value `http://uri.etsi.org/19522/Event/RelayRejection` shall be set to the `ERDSEventId` element of the ERDS evidence; the `Extensions/RelayEvidenceRefersTo` element shall be set to the recipient(s) to whom the evidence refers to (amongst all the intended recipients); the appropriate `Code` and `Details` about the formal or security checks failed or any other error condition shall be set to the `EventReason` element (see the URIs of table 3 of ETSI EN 319 522-3 [3], clause 5.2.2.7 for the full list of Codes, and the columns DCode and RDetails of table C.28 of the present document for the relevant full list of Details). This is the case where there are no errors in the new execution of steps from b) to f) on such ERDS evidence: it shall be attached to a RelayRejection REMS receipt, built according to clauses 5.4 and C.4.2, to be sent back (in a best-effort way) to the S-REMS.

II. The value `http://uri.etsi.org/19522/Event/RelayRejection` shall be set to the `ERDSEventId` element of the ERDS evidence; the `Extensions/RelayEvidenceRefersTo` element shall be set to the recipient(s) to whom the evidence refers to (amongst all the intended recipients); the appropriate `Code` and `Details` about the formal or security checks failed or any other error condition shall be set to the `EventReason` element (see the URIs of table 3 of ETSI EN 319 522-3 [3], clause 5.2.2.7 for the full list of Codes, and the columns DCode and RDetails of table C.28 of the present document for the relevant full list of Details). This is the case where there is a permanent error during the new execution of some step from b) to f) on such ERDS evidence: it may be further completed with the details of this additional error in the best-effort way; and it (even if not complete) shall be attached to a RelayRejection REMS receipt, built according to clauses 5.4 and C.4.2, to try to send it back (in a best-effort way) to the S-REMS.

III. If there is some transient error on any step from b) to f), the process shall try to recover the error within a timeout fixed in the **REMID policy** (see clauses C.2.3.5 and D.1.3); if the error is back, the process shall continue with the step g); otherwise, in any case, the error is considered persistent, and the REM service shall issue the ERDS evidence to attach to a REMS receipt that has to be sent back to the sender. This process shall be framed, substantially, in the best-effort way, as described in I. or II.

NOTE 1: In both cases I. and II. above, there can be additional rules in local **REMID policy** that dispose of particular preservations and management practices on the REM dispatch in case of "security violations and threats" specified in the policy (see clause C.2.3.5). Anyway, none of these "additional" practices breaks the interoperability.

NOTE 2: ERDS/REMS standard does not prescribe the intra-provider relay operation when R-REMS is the same of S-REMS. So, the particular case of recipient(s) unknown or unregistered when R-REMS = S-REMS it is not reported to the sender by an unsuccessful relay operation, since relay does not take place (indeed it is neither attempted), but it is reported through a ContentConsignmentFailure with the RD21 'Details code'. Vice versa, the case of recipient(s) unknown or unregistered, when R-REMS ≠ S-REMS, occurring through an unsuccessful try of relay (e.g. notified by a DSN), it is consistent with the RB10 'Details code' ("*ERD message **not relayed** to the Recipient's ERDSP for: Unknown Recipient*" 'reason details' semantic, according to ETSI EN 319 522-2 [2], clause 8.3.3.2 table 8); and it is reported to the sender through a RelayFailure with the RB10 'Details code' (see the scenario S4 of clause D.4.5 for an example). Finally, the case of recipient(s) unknown or unregistered when R-REMS ≠ S-REMS, occurring through a relay which takes place, it is not reported to the sender by an unsuccessful relay operation with the RB10 'Details code', since it is not consistent with its semantic (because the relay takes place), but it is reported through a chain of relay operations (RelayReject from R-REMS to S-REMS, and a RelayFailure from S-REMS to the sender) with the RB21 'Details code', as specified in the next statements (see the scenario S5 of clause D.4.5 for an example).

i) The case of the recipient(s) unknown or unregistered to R-REMS is identified by an EventReason element specifically defined for REM baseline and implemented as follows:

I. the 'URI code'/'reason details' identified by RB21 'Details code' shall apply (see table C.28 and the example 1 at point d) of clause C.3.4 for the disposition of EventReason relevant elements);

II. the RelayEvidenceRefersTo ERDS evidence element of RelayReject shall be used to reference, with the specific positional integer(s), the recipient(s) to whom the relay evidence refers to (amongst all the intended recipients) according to the point a) of clause C.3.2.2, table C.16.

NOTE 3: Void.

NOTE 4: Void.

Table C.24: Relay (S-REMS side) - ERDS evidence signature and time-stamp

N°	Service/Protocol element	ETSI EN 319 522-1 [1] main reference	Requirement	Implementation guidance	Notes
1	RelayFailure	Clause 6.2.2 B.3.	M	a), b), c), d), e), f), g), h), i)	RelayFailure event

Implementation guidance:

a) The "failing" event phase, at S-REMS side (e.g. on receiving a negative SMTP response from border, or no information within a given period on RelayAcceptance or RelayRjection is received), on trying to relay the "REM dispatch" to R-REMS (see time T0 in figure B.11 of clause B.3.3) is composed of a list of steps among which a number of checks. The responsibility to inform the sender remains to the S-REMS that has in charge the application of the digital signature and the time-stamp to the ERDS evidence for such event (composed as per clause C.3), and the application of the digital signature to the REMS receipt. This process shall be framed, substantially, as follows:

   I. The value `http://uri.etsi.org/19522/Event/RelayFailure` shall be set to the `ERDSEventId` element of a RelayFailure ERDS evidence, the `EventReason/Code` set to the appropriate URI according to the failure reason (see the URIs of table 3 of ETSI EN 319 522-3 [3], clause 5.2.2.7 for the full list of codes) and the `Extensions/RelayEvidenceRefersTo` element set to the recipient(s) that the evidence refers to, among all, the intended recipients.

   II. If the S-REMS receive a RelayRejection REMS receipts from R-REMS, a proper error code is set for the evidence (according to ETSI EN 319 522-3 [3], table 3) and the flow continues from point h) with a RelayFailure ERDS evidence.

   III. If the S-REMS was unable to relay the REM dispatch to R-REMS within a given time period specified in the **REMID policy**, a proper error code is set for the evidence (according to ETSI EN 319 522-3 [3], table 3) and the flow continues from point h) with a RelayFailure ERDS evidence.

   IV. If the S-REMS was unable to receive a RelayAcceptance REMS receipts, relevant to the aforementioned REM dispatch, within a given time period specified in the **REMID policy**, a proper error code is set for the evidence (according to ETSI EN 319 522-3 [3], table 3) and the flow continues from point h) with a RelayFailure ERDS evidence.

b) The time reference T0 of the "failing" event (relay rejection or unable to relay) shall be set to the G05 `EventTime` element of the ERDS evidence according to the semantic of ETSI EN 319 522-2 [2], clause 8.2.5 (see time T0 in figure B.11 of clause B.3.3).

c) The "digest" of the "original message" contained in M02 ERDS evidence element of REM dispatch (or of RelayRejection REMS receipt) shall be assigned, by copy, to the digest child field of M02 (same as MD14) element of RelayFailure ERDS evidence (see time T1 in figure B.11 of clause B.3.3) in the context of the following process:

   I. ComposingParts child field of UserContentInfo element shall be set to 1.

   II. Identifier child field of an element of UserContentInfo shall be set to "urn:oid:1.3.6.1.7" (that represents the identifier for iso(1) org(3) dod(6) internet(1) mail(7) OID, as defined in IANA SMI OID numbers).

   III. ContentType child field of an element of UserContentInfo shall be set to "message/rfc822".

   IV. DigestMethod child field of an element of UserContentInfo shall be set as a "copy" of the digest method taken from DigestMethod child field of an element of the ERDS evidence attached in REM dispatch.

   V. DigestValue child field of an element of UserContentInfo shall be set to as a "copy" of the base64 encoded digest value of original message taken from ERDS evidence attached in REM dispatch (that has been computed using the digest algorithm indicated in the aforementioned DigestMethod field).

d) The XML structure of the ERDS evidence shall be filled with the necessary values (see time T2 in figure B.11 of clause B.3.3) as follows:

   I. `EvidenceIssuerPolicyID` element of the ERDS evidence shall have a URI set to `http://uri.etsi.org/19532/v1#/REMbaseline` and shall match the value of ERDSProfileSupported element of ERDSMetadata (see c.3.3.3 of table C.8 and clause D.1.3).

   II. All the other contents and elements of ERDS evidence shall be set according to clause C.3.

e) A standard XAdES-B-B baseline digital signature is applied to the XML evidence structure according to the provisions of clause C.4.3 (see time T3 in figure B.11 of clause B.3.3).

f) A **standard time-stamp** is generated and applied on top of the XAdES-B-B, augmenting the signature level to XAdES-B-T according to the provisions of clause C.4.4 (see time T4 in figure B.11 of clause B.3.3); and the ERDS evidence XML structure is ready to be "released" by the process of signature and time-stamp.

g) If there are no errors, the ERDS evidence XML structure shall be attached to a RelayFailure REMS receipt, built according to clauses 5.4 and C.4.2, to be sent back to the sender (see time T5 in figure B.11 of clause B.3.3); and this flows of the entire REM transaction stops here.

h) If one of the previous steps fails, the REM service shall issue the ERDS evidence to attach to a REMS receipt that has to be sent back to the sender. This process shall be framed, substantially, in the best-effort way, as described in II. for permanent failures, and in III. for transient failures:

   I. Void.

   II. If either there is a permanent error during the execution of some step from b) to f) or the process achieved a given limit (see clauses C.2.3.5 and D.1.3) the event is logged as a permanent error to be properly managed by S-REMS according to the local **REMID policy**; and the flows of the transaction stops here.

   III. If there is some transient error on any step from b) to f), the process shall try to recover the error within a timeout fixed in the **REMID policy** (see clauses C.2.3.5 and D.1.3); if the error is back, the process shall continue with the step g); otherwise, in any case, the error is considered persistent, and the process shall be framed, substantially, as described in II.

NOTE 5: In case II. above, there can be additional rules in local **REMID policy** that dispose of particular preservations and management practices on the REM dispatch in case of "security violations and threats" specified in the policy (see clause C.2.3.5). Anyway, none of these "additional" practices breaks the interoperability.

NOTE 6: Taking into account note 2 above, the case of R-REMS ≠ S-REMS and recipient(s) unknown or unregistered can be reported to the sender through a chain of relay operations (RelayReject from R-REMS to S-REMS, and a RelayFailure from S-REMS to the sender), as specified in the next statements.

i) The case of the recipient(s) unknown or unregistered to R-REMS is identified by an EventReason element specifically defined for REM baseline and implemented as follows:

   I. The 'URI code'/'reason details' identified by RB21 'Details code' shall apply (see table C.28 and the example 1 at point d) of clause C.3.4 for the disposition of EventReason relevant elements).

   II. The RelayEvidenceRefersTo ERDS evidence element of RelayFailure shall be used to reference, with the specific positional integer(s), the recipient(s) to whom the relay evidence refers to (amongst all the intended recipients) according to the point a) of clause C.3.2.2, table C.16.

C.4.5.3 ContentConsignment event

With regards to the application of digital signatures and time-stamp to ERDS evidence, and digital signatures to REM messages during the consignment event, the constraints of clause 5.5.1.1, elements 3 and 4 shall apply to REM baseline according to the provisions of the present clause (see ETSI EN 319 532-1 [4], clause 6.2.4 for a full description of the events mentioned in the present clause).

Table C.25: Consignment - ERDS evidence signature and time-stamp

Nº	Service/Protocol element	ETSI EN 319 522-1 [1] main reference	Requirement	Implementation guidance	Notes
1	ContentConsignment	Clause 6.2.4 D.1.	M	a), b), c), d), e), f), g)	Consignment event
2	ContentConsignment Failure	Clause 6.2.4 D.2.	M	a), b), c), d), e), f), g), h), i)	ConsignmentFailure event

Implementation guidance:

a) The "consigning" event phase of the "REM dispatch" to the recipient (see time T0 in figure B.12 of clause B.3.4) is composed of a list of steps among which a number of checks. After the formal and security checks (if any), the R-REMS has in charge the application of the digital signature and the time-stamp to the ERDS evidence for such event (composed as per clause C.3), and the application of the digital signature to the REMS receipt. This process shall be framed, substantially, as follows:

   I. If any of the formal or security checks fail the content consignment process shall be interrupted; and the flow continues from point h) with a ContentConsignmentFailure. This also if the S-REMS was unable to receive a ContentConsignment/ ContentConsignmentFailure REMS receipts, relevant to the aforementioned REM dispatch, within a given time period specified in the **REMID policy**. In such case a proper error code is set for the evidence (according to ETSI EN 319 522-3 [3], table 3) and the flow continues from point h) with a ContentConsignmentFailure ERDS evidence.

   II. Otherwise, if all the checks of the previous step I. succeed, the flow shall continue with point b) assigning the value `http://uri.etsi.org/19522/Event/ContentConsignment` to the `ERDSEventId` element of a ContentConsignment ERDS evidence. The EventReason/Code set to the URI `http://uri.etsi.org/19522/EventReason/MessageConsignedToRecipient` and the `EvidenceRefersToRecipient` element set to the recipient that the evidence refers to among all the intended recipients.

b) The time reference T0 of the "consignment" phase shall be set to the G05 `EventTime` element of the ERDS evidence according to the semantic of ETSI EN 319 522-2 [2], clause 8.2.5 (see time T0 in figure B.12 of clause B.3.4).

c) The "digest" of the "original message" contained in M02 ERDS evidence element of REM dispatch shall be assigned, by copy, to the digest child field of M02 (same as MD14) element of the ERDS evidence (see time T1 in figure B.12 of clause B.3.4) in the context of the following process:

   I. ComposingParts child field of UserContentInfo element shall be set to 1.

   II. Identifier child field of an element of UserContentInfo shall be set to "urn:oid:1.3.6.1.7" (that represents the identifier for iso(1) org(3) dod(6) internet(1) mail(7) OID, as defined in IANA SMI OID numbers).

   III. ContentType child field of an element of UserContentInfo shall be set to "message/rfc822".

   IV. DigestMethod child field of an element of UserContentInfo shall be set as a "copy" of the digest method taken from DigestMethod child field of an element of the ERDS evidence attached in REM dispatch.

   V. DigestValue child field of an element of UserContentInfo shall be set to as a "copy" of the base64 encoded digest value of original message taken from ERDS evidence attached in REM dispatch (that has been computed using the digest algorithm indicated in the aforementioned DigestMethod field).

d) The XML structure of the ERDS evidence shall be filled with the necessary values (see time T2 in figure B.12 of clause B.3.4) as follows:

   I. `EvidenceIssuerPolicyID` element of the ERDS evidence shall have a URI set to `http://uri.etsi.org/19532/v1#/REMbaseline` and shall match the value of ERDSProfileSupported element of ERDSMetadata (see c.3.3.3 of table C.8 and clause D.1.3).

   II. All the other contents and elements of ERDS evidence shall be set according to clause C.3.

e) A standard XAdES-B-B baseline digital signature is applied to the XML evidence structure according to the provisions of clause C.4.3 (see time T3 in figure B.12 of clause B.3.4).

f) A **standard time-stamp** is generated and applied on top of the XAdES-B-B, augmenting the signature level to XAdES-B-T according to the provisions of clause C.4.4 (see time T4 in figure B.12 of clause B.3.4); and the ERDS evidence XML structure is ready to be "released" by the process of signature and time-stamp.

g) If there are no errors, the ERDS evidence XML structure shall be attached to a ContentConsignment REMS receipt, built according to clauses 5.4 and C.4.2, to be sent back to the sender (see time T5 in figure B.12 of clause B.3.4); and the REM dispatch is consigned to the user mailbox.

h) If one of the previous steps fails, the REM service shall issue the ERDS evidence to attach to a REMS receipt that has to be sent back to the sender. This process shall be framed, substantially, in the best-effort way, as described in I. and II. for permanent failures, and in III. for transient failures:

   I. The value `http://uri.etsi.org/19522/Event/ContentConsignmentFailure` shall be set to the `ERDSEventId` element of the ERDS evidence; the `EvidenceRefersToRecipient` element shall be set to the recipient to whom the evidence refers to (amongst all the intended recipients); the appropriate `Code` and `Details` about the formal or security checks failed or any other error condition shall be set to the `EventReason` element (see the URIs of table 3 of ETSI EN 319 522-3 [3], clause 5.2.2.7 for the full list of Codes, and the columns DCode and RDetails of table C.28 of the present document for the relevant full list of Details). This is the case where there are no errors in the new execution of steps from b) to f) on such ERDS evidence: it shall be attached to a ContentConsignmentFailure REMS receipt, built according to clauses 5.4 and C.4.2, to be sent back (in a best-effort way) to the sender.

   II. The value `http://uri.etsi.org/19522/Event/ContentConsignmentFailure` shall be set to the `ERDSEventId` element of the ERDS evidence; the `EvidenceRefersToRecipient` element shall be set to the recipient to whom the evidence refers to (amongst all the intended recipients); the appropriate `Code` and `Details` about the formal or security checks failed or any other error condition shall be set to the `EventReason` element (see the URIs of table 3 of ETSI EN 319 522-3 [3], clause 5.2.2.7 for the full list of Codes, and the columns DCode and RDetails of table C.28 of the present document for the relevant full list of Details). This is the case where there is a permanent error during the new execution of some step from b) to f) on such ERDS evidence: it may be further completed with the details of this additional error in the best-effort way; and it (even if not complete) shall be attached to a ContentConsignmentFailure REMS receipt, built according to clauses 5.4 and C.4.2, to try to send it back (in a best-effort way) to the sender.

   III. If there is some transient error on any step from b) to f), the process shall try to recover the error within a timeout fixed in the **REMID policy** (see clauses C.2.3.5 and D.1.3); if the error is back, the process shall continue with the step g); otherwise, in any case, the error is considered persistent, and the REM service shall issue the ERDS evidence to attach to a REMS receipt that has to be sent back to the sender. This process shall be framed, substantially, in the best-effort way, as described in I. or II.

NOTE 1: In both cases I. and II. above, there can be additional rules in local **REMID policy** that dispose of particular preservations and management practices on the REM dispatch in case of "security violations and threats" specified in the policy (see clause C.2.3.5). Anyway, none of these "additional" practices breaks the interoperability.

NOTE 2: The particular case of recipient(s) unknown or unregistered when R-REMS = S-REMS it is reported to the sender through one ContentConsignmentFailure for each recipient with the RD21 'Details code', as specified in the next statements.

i) The case of the recipient(s) unknown or unregistered to R-REMS is identified by an EventReason element specifically defined for REM baseline and implemented as follows:

   I. The 'URI code'/'reason details' identified by the RD21 'Details code' shall apply (see table C.28 and the example 1 at point d) of clause C.3.4 for the disposition of EventReason relevant elements).

   II. The I09 EvidenceRefersToRecipient ERDS evidence element of ContentConsignmentFailure shall be used to reference, with the specific positional integer, **the recipient** whose the consignment evidence refers to, among all the intended recipients, according to the point o) of clause C.3.4, table C.18.

NOTE 3: The cardinality of recipients referred to by any content consignment ERDS evidence is one: ContentConsignmentFailure identifies exactly one unknown recipient by the I09 EvidenceRefersToRecipient element.

C.4.5.4 Summary tables

With regards to the application of digital signatures and time-stamp to ERDS evidence and digital signatures to REM messages, the events and constraints of clauses C.4.5.1, C.4.5.2 and C.4.5.3 shall apply to REM baseline according to the provisions of the present clause (see ETSI EN 319 522-2 [2], clause 6.1, clause 8.3 and clause 8.4 for the full description; and ETSI EN 319 522-3 [3], clause 5.2.2.7 for the full list of codes).

Table C.26 and table C.27 within this clause define cardinality requirements and notes that apply, respectively, to the different REM message headers and ERDS evidence components.

Below follows a detailed explanation of the content of the aforementioned tables:

1) The first row contains the set of REM message types (in the case of table C.26) and the set of events on which an evidence may be issued (in the case of table C.27).

2) The first column contains the set of REM message headers (in the case of table C.26) and the set evidence components (in the case of table C.27) prescribed for REM baseline.

3) Each cell within table C.26 and table C.27 contains the cardinality requirements that apply to the header or the component identified by the row, in correspondence of the REM message or of the event identified by the column respectively.

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

   - **0:** The REM message (table C.26) or evidence (table C.27) associated with the event identified by the column shall not incorporate any header or component identified by the row, respectively.

   - **1:** The REM message (table C.26) or evidence (table C.27) associated with the event identified by the column shall incorporate exactly one instance of the header or component identified by the row, respectively.

   - **0..1:** The REM message (table C.26) or evidence (table C.27) associated with the event identified by the column shall incorporate zero or one instance of the header or component identified by the row, respectively.

   - ***:** The REM message (table C.26) or evidence (table C.27) associated with the event identified by the column shall incorporate zero or more instances of the header or component identified by the row, respectively.

   - **1..*:** The REM message (table C.26) or evidence (table C.27) associated with the event identified by the column shall incorporate one or more instances of the header or component identified by the row, respectively.

   - **2..*:** The REM message (table C.26) or evidence (table C.27) associated with the event identified by the column shall incorporate two or more instances of the header or component identified by the row, respectively.

In addition to the cardinality, some cells identify an explanatory note on their contents using letters enclosed in round brackets. Notes appear after the tables.

NOTE: There can be additional rules in local **REMID policy** that further tune the ranges of cardinalities of the following tables for either one or both of particular practices and behaviours specified in the policy (see clause C.2.3.5). Anyway, none of these "additional" tunings breaks the interoperability.

Table C.26: REM message headers: presence and cardinality in REM baseline

REM message / Code/Metadata (header) component name	REM SubmissionAcceptance	REM dispatch	REM SubmissionRejecttion	REM RelayAcceptance	REM RelayRejection	REM RelayFailure	REM ContentConsignment	REM ContentConsignmentFailure
MD01 REM-MetadataVersion	1	1	1	1	1	1	1	1
MD02 REM-RelayDate	0	0..1	0..1	0..1	0..1	0..1	0..1	0..1
MD03 REM-ExpirationDate	0	0	0	0	0	0	0	0
MD04 REM-RecipientAssuranceLevel	0..1	0..1	0..1	0..1	0..1	0..1	0..1	0..1
MD05 REM-ApplicablePolicy	0..*	0..*	0..*	0..*	0..*	0..*	0..*	0..*
MD06 REM-ModeOfConsignment	0..1	0..1	0..1	0..1	0..1	0..1	0..1	0..1
MD07 REM-ScheduledDelivery	0	0	0	0	0	0	0	0
MD08 REM-MD08	1 (a)	1 (a)	1 (a)	1 (a)	1 (a)	1 (a)	1 (a)	1 (a)
MD09 Reply-to	0..1	1	0..1	0..1	0..1	0..1	0..1	0..1
MD10 To	1	1	1	1	1	1	1	1
MD11 Message-ID	1	1	1	1	1	1	1	1
MD12 In-Reply-To	0..1	0..1	0..1	0..1	0..1	0..1	0..1	0..1
MD13 REM-MessageType	1	1	1	1	1	1	1	1
MD14 Content-Type, Subject, REM-DigestAlgorithm, REM-DigestValue, REM-UAMessageIdentifier	1	1	1	1	1	1	1	1
MD15 Extensions	0..1	0..1	0..1	0..1	0..1	0..1	0..1	0..1
/ Signature	1	1	1	1	1	1	1	1

NOTE:
(a) This element shall be as specified in ETSI EN 319 522-2 [2], table 5 and clause 6.2.8 about semantic, and ETSI EN 319 532-3 [6], table 2 and clause 6.2.1 about REM-<component>: <value> format definition.

Table C.27: ERDS evidence elements: presence and cardinality in REM baseline

Code/Evidence component name \ Event		SubmissionAcceptance	SubmissionRejecttion	RelayAcceptance	RelayRejection	RelayFailure	ContentConsignment	ContentConsignmentFailure
G01 EvidenceIdentifier		1	1	1	1	1	1	1
G02 Evidence version		1	1	1	1	1	1	1
G03 ERDSEventId		1	1	1	1	1	1	1
G04 EventReasons		1	1..*	1	1..*	1..*	1	1..*
G05 EventTime		1	1	1	1	1	1	1
R01 EvidenceIssuerPolicyID		2..*	2..*	2..*	2..*	2..*	2..*	2..*
R02 EvidenceIssuerDetails		1	1	1	1	1	1	1
R03 Signature		1	1	1	1	1	1	1
I01 SenderDetails/Sender's Identity attributes		0..1	0..1	0..1	0..1	0..1	0..1	0..1
I02 SenderDetails/Sender's Identifier		1	1	1	1	1	1	1
I05 RecipientDetails/Recipient's Identity attributes		0..*	0..*	0..*	0..*	0..*	0..*	0..*
I06 RecipientDetails/Recipient's Identifier		1..*	1..*	1..*	1..*	1..*	1..*	1..*
I09 EvidenceRefersToRecipient		0	0	0	0	0	1	1
I10 Sender/AssuranceLevelsDetails		1	1	1	1	1	1	1
I12 Recipient/AssuranceLevelsDetails		0	0	0	0	0	0	0
M01 MessageIdentifier		1	1	1	1	1	1	1
M02 UserContentInfo		1	1	1	1	1	1	1
M03 SubmissionTime		1	1	0..1	0..1	0..1	0..1	0..1
M04 ExternalSystem (*ForwardedToExternalSystem)*		0	0	0	0	0	0	0
M05 ExternalERDSDetails		0	0	1	1	1	0	0
E01	Extensions	0..1 (a)	0..1 (a)	0..1 (a)	0..1 (a)	0..1 (a)	0..1 (a)	0..1 (a)
	Extensions/Subject	0..1	0..1	0..1	0..1	0..1	0..1	0..1
	Extensions/UntrustedPathToRecipient	0..*	0..*	0..*	0..*	0..*	0..*	0..*
	Extensions/RelayEvidenceRefersTo	0	0	0..* (b)	0..* (b)	0..* (b)	0	0

NOTE:
(a) From XML syntactical viewpoint, the optionality of extensions is according to the present requirement. Whereas the definitive specific presence is conditioned to the semantic rationales as per clause C.3.4, table C.18 requirement n.16 and clauses C.3.2, C.4.5.1, C.4.5.2 and C.4.5.3.
(b) If this element is absent, the ERDS evidence shall be considered related to all the intended recipients.

Regarding the M04 ExternalSystem element, it is specified, inside XSD as *ForwardedToExternalSystem* (that, as name to use, takes precedence as per ETSI EN 319 522-3 [3], clauses 4.1 and 5.1). It is used in mixed situations where NonERDS users are involved as either one or both sender and recipients together a pure REM baseline interchange. So, inside ERDS Evidence, its usage is relevant to such NonERDS users. In the case of ReceivedFromNonERDS, RelayToNonERDS and RelayToNonERDSFailure events (the first two associated with specific REM dispatches from/to external systems, and the last associated with a REMS receipt), the *ForwardedToExternalSystem* element should be present in the relevant ERDS evidence XML structures, and should be set as follows:

- REM dispatch/ReceivedFromNonERDS ERDS evidence: *ForwardedToExternalSystem* set to the "Received" header of the original message, received from an external system, containing information on it.
- REM dispatch/RelayToNonERDS ERDS evidence: *ForwardedToExternalSystem* set to the MX-record of the NonERDS remote system where the REM dispatch is relayed.
- REMS receipt/RelayToNonERDSFailure ERDS evidence: *ForwardedToExternalSystem* set to the MX-record of the NonERDS remote system where the REM dispatch was tried to relay to.

Table C.28 summarizes the matching among codes, URIs and details identifying reasons causing events occurrences. Moreover, three new codes (RB21, RB22 and RD21) specific for REM baseline are defined (as suggested and granted by rows identified with code *RBXX* and *RDXX* of ETSI EN 319 522-2 [2], table 8 and table 10, respectively).

Below follows a detailed explanation of the content of table C.28.

The first row contains a short description of each column:

1st column) **Event**: the set of couples '(event code)'/'event name'.

2nd column) **DCode**: the set of 'Details code'

3rd column) **RDetails and URI code identifying EventReason**: the of couples 'reason details'/'URI code'

See the example 1 at point d) of clause C.3.4 for the disposition of 'Details code', 'reason details' and 'URI code' in the EventReason element.

Table C.28: Events - Details codes - Reason details/URI codes identifying reasons causing events occurrences

Event	DCode	RDetails and URI code identifying EventReason	Example(s)
(A.1) SubmissionAcceptance	RA01	Message **accepted** http://uri.etsi.org/19522/EventReason/MessageAccepted	See scenarios S1,S3,S4,S5,S6,S7 of clause D.4.5 examples.
(A.2) SubmissionRejection	RA02	**Invalid** message **format** http://uri.etsi.org/19522/EventReason/InvalidMessageFormat	See scenario S2 of clause D.4.5 examples.
	RA03	**Malware** found in ERD original message http://uri.etsi.org/19522/EventReason/MalwareFound	See scenario S2 of clause D.4.5 examples.
	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	See scenario S2 of clause D.4.5 examples.
	RA06	ERD message not accepted by the Sender's ERDSP for: Sender's ERDSP malfunction http://uri.etsi.org/19522/EventReason/S_ERDS_Malfunction	See scenario S2 of clause D.4.5 examples.
(B.1) RelayAcceptance	RB01	ERD message **successfully relayed** to the Recipient's ERDSP http://uri.etsi.org/19522/EventReason/S_ERDS_MessageSuccessfullyRelayed	See scenarios S1,S4,S5,S6,S7 of clause D.4.5 examples.
(B.2) RelayRejection (B.3) RelayFailure	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	See scenario S3 of clause D.4.5 examples.
	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	See scenario S3 of clause D.4.5 examples.
	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	See scenario S3 of clause D.4.5 examples.
	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	See scenario S3 of clause D.4.5 examples.
	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	See scenario S3 of clause D.4.5 examples.
	RB07	ERD message not relayed to the Recipient's ERDSP for: Recipient's **ERDSP malfunction** http://uri.etsi.org/19522/EventReason/R_ERDS_Malfunction	See scenario S4 of clause D.4.5 examples.
	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	See scenario S4 of clause D.4.5 examples.
	RB09	ERD message not relayed to the Recipient's ERDSP for: Recipient's **ERDSP unreachable** http://uri.etsi.org/19522/EventReason/R_ERDS_Unreachable	See scenario S4 of clause D.4.5 examples.
	RB10	ERD **message not relayed** to the Recipient's ERDSP for: **Unknown Recipient** http://uri.etsi.org/19522/EventReason/UnknownRecipient	See scenario S4 of clause D.4.5 examples.
	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	See scenario S5 of clause D.4.5 examples.
	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	See scenario S5 of clause D.4.5 examples.
(D.1) ContentConsignment	RD01	Message **successfully consigned** to the recipient http://uri.etsi.org/19522/EventReason/MessageConsignedToRecipient	See scenarios S1,S4,S5,S7 of clause D.4.5 examples.
(D.2) ContentConsignmentFailure	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	See scenario S6 of clause D.4.5 examples.
	RD04	Not consigned for **excessing recipient quota** http://uri.etsi.org/19522/EventReason/MessageNotConsignedForQuota	See scenario S6 of clause D.4.5 examples.
	RD05	Not consigned for **technical malfunction** http://uri.etsi.org/19522/EventReason/MessageNotConsignedForMalfunction	See scenario S7 of clause D.4.5 examples.
	RD06	Not consigned for message **type not accepted** by recipient http://uri.etsi.org/19522/EventReason/MessageNotConsignedForUnallowedType	See scenario S6 of clause D.4.5 examples.
	RD21	ERD message not consigned for: **Unregistered recipient** to Recipient's ERDSP http://uri.etsi.org/19522/EventReason/MessageNotConsignedForUnregisteredRecipient	See scenario S7 of clause D.4.5 examples.

Annex D (informative): REM baseline best practices

D.1 Global governance practices

D.1.1 General

This clause provides a collection of the main practices typically used for the governance during the REM baseline adoption, which was considered worth mentioning here.

D.1.2 Links with national laws

The Trusted List ETSI TS 119 612 [12] specifies many practices regarding the links with the local realities. In particular, the point (f) of 5.5.1.1 and the clauses 5.3.8 and 5.3.10 are relevant for qualified trust services within the REM baseline framework.

D.1.3 REMID policy elements

Another task regarding the governance practices is the **collection** of elements that need to be specified at the policy level, according to the resolution of the previous task, clause D.1.2, and the **publication** of such policy.

The implementation guidance b) of clause C.2.3.5 illustrates a method for the publication. Such practice is derived from clauses 5.3.9 and D.4 of ETSI TS 119 612 [12], where other details are defined.

The collection of elements present in the REMID policy regards service and security aspects and technical conditions that need to be specialized at the local level, without breaking the interoperability. The following elements are typically considered in the REMID policy, as an example, for specific content definition and for specific practices on them:

- CSIIssueDateTime (see point vi./c.3.1.8 of table C.6)
- CSINextUpdate (see point vii./c.3.1.8 of table C.6)
- Digital signature and optionally time-stamp of CapabilityAndSecurityInformation XML (see point c.3.1.11 of table C.6)
- Digital signature of REM messages (see point b) of table C.19)
- Digital signature of ERDS evidence XML structures (see point d) of table C.20)
- Digital certificates properties for digital signature of REM messages, ERDS evidence XML structures, CapabilityAndSecurityInformation XML structure, Transport Layer Security (TLS) (see clause D.2.2)
- EvidenceIssuerPolicyID/**CSISchemePolicyCommunityRules** (see points: b) of clause C.2.3.5, f) of table C.18, d) of table C.22, d) of table C.23, d) of table C.24 and d) of table C.25 for the URI where is published the **REMID policy**)
- "userid" either one or both of source and format when applicable to the local **REMID policy** (see points h) and i) of table C.18 and clause D.4.2)
- DigestMethod of entire original message (see point c)IV of table C.23)

EXAMPLE 1: *http://www.w3.org/2001/04/xmlenc#sha256*
as algorithm used to get the digest of whole "original message".

- Timeout for transient errors (see clause D.4.4)

- Relay-snd-dsp-wait timeout (see clause D.4.4)
- Relay-rcv-ra-wait timeout (see clause D.4.4)
- Relay-rcv-ca-wait timeout (see clause D.4.4)
- Cycle-number for persistent errors and final behaviours (see clause D.4.4)
- Number of historical elements that have to be maintained inside the `CSIPointersToOtherMetadata` list of URIs (see clause D.3)

EXAMPLE 2: 50 elements. Or any number of elements within a period of 30 months.

D.2 Registration and setup practices

D.2.1 General

This clause provides a collection of the main practices that are typically necessary for a service provider that wants to adopt the REM baseline, which was considered worth mentioning here.

D.2.2 Certificate and signature properties

D.2.2.1 Certificate significant elements

The **REMID policy** represents a place where define specific elements characterizing the certificates for all the digital signatures of REM messages and ERDS evidence XML structures and also certificates for TLS CSI used for the REMID level. Such elements include, for example, Certificate Name Check Conventions on SubjectAltName (SAN) extension and on Common Name (CN) elements. As well as other X509v3 extensions like key usage and certificate policies.

NOTE: In fact, regarding the certificates used to sign the S/MIME signature of the REM messages, the email/rfc822Name alternative of the SAN specifies the email address characterizing such digital signature (see note clause 5.5.1.3, table 18, item b). In other words, the email/rfc822Name represents the "signer" (set by using the rfc822Name alternative of the GeneralName CHOICE of the SAN X509v3 extension, according to IETF RFC 8550 [i.16], clause 4.4.3). And similarly, regarding the certificates used for TLS, the DNS/dNSName alternative of the SAN specifies the MX record of the hostnames characterizing the REM service (see also note 2 of clause C.2.3.4.4, table C.11, item c.3.5.1). In other words, the DNS/dNSName represents the "REMS" (set by using the dNSName alternative of the GeneralName CHOICE of the SAN X509v3 extension).

D.2.2.2 Certificate issuing path

The adoption of the following properties, involving the **digital certificate** signing **REM messages**, improves the user experience and facilitates the installation/configuration of REM systems:

1) Issued in the path of a top-level Root CA worldwide recognized by any Operating System and client browser:

   Signatures using certificates issued in the path of a top-level Root CA certificate, trusted by the common operating systems (and the relevant browsers through their own Root CA cache), are ideal for facilitating automatic verification in any user client (browser or application). Using this property, the usual email client retrieving and verifying incoming messages from REMS will not receive any warning. It would be unpleasant that, for a "qualified" service, a REMS's recipient receives an invalid signature warning each time a REM message is retrieved from a REMS.

Nevertheless, all the key-stores of the software applications implementing REMS contain, basically, all the top-level Root CA world-wide recognized by any Operating System or client browsers (and these key-stores are automatically updated contextually with the system updates). This property facilitates the setup and management of REM systems. In fact, in such a case, the digital signature's basic validation takes place without exceptions/software or execution interruptions. Vice versa, when the root CA are not in the key-store, either one or both of the software and the digital signature libraries could not work properly. In such a case, it would be necessary to update, as some new REMSP enters the circuit continuously, and with custom procedures, all the involved servers key-stores with the required custom Root CA. This greatly complicates the management of the systems and their reliability.

2) Used as "digital identity of REMS":
In fact, as illustrated in the rationales of table B.4, the digital certificate signing REM messages and ERDS evidence is used as digital identity of the relevant REMSP.

3) Set the aforementioned digital certificate on ServiceDigitalIdentity element of TL:
As illustrated in the definitions of table C.4, the digital certificate signing REM messages and ERDS evidence is represented from the ServiceDigitalIdentity element of TL.

4) Placement on the following certification path is:

   - top-level Root CA (recognized by OS and browsers)

   - - subordinate CA (with required/restricted purposes mentioned in statement 1 of table B.4)

   - - - REMS digital identity certificate (for message/evidence signature).

   The certification path illustrated above is obtained by putting together the aforementioned properties, and only the third certificate will be in TL.

   And furthermore, the "From:" email address, header of the S/MIME structure of a REM message, equal to the rfc822Name of the X509v3 SAN (SubjectAltName extension of digital certificate used to sign the S/MIME itself) completes the user experience improvements. In fact, using this property together that mentioned in point 1), the usual email client retrieving and verifying incoming messages from REMS will not receive any warning.

In other words, for the digital signature of REM messages, the classical S/MIME digital certificates, further ensured in TL, represent the ideal solution for both practicality and usability.

A slightly different situation occurs for the **digital signature** of **ERDS evidence** XML structures. There is no typical direct usage, of these XML objects, by the final users, using standard clients (in comparison to the REM messages that are directly used by normal email clients, and thus unrecognized certificates produce confounding warnings). But, as seen in the rationales of table B.4, the need to ensure this certificate in TL and the constraint to have only one public-key per service digital identity certificate leads to **use the same digital certificate** for the signature of both ERDS evidence XML structures and REM messages.

Similarly, for the **digital signature** of **CapabilityAndSecurityInformation** XML structure, the point c.3.1.12 of table C.6 and the same considerations done above for ERDS evidence leads to use, also for this digital signature, the aforementioned digital certificate.

Finally, the **digital certificate** for **Transport Layer Security (TLS)** is ensured in TL by reference, using the CapabilityAndSecurityInformation XML structure. So there is no special direction about the certificate issuing path of such certificate except what is laid down on the specific **REMID policy** for local requirements.

D.2.2.3 Digital signature - signature-policy-identifier

The **REMID policy** represents a place where define a given signature policy for all the digital signatures of ERDS evidence XML structures used for the REMID without the use of signature-policy-identifier attribute. Alternatively if, for all the REMSP adhering to such policy, the digital signature includes the signed attribute signature-policy-identifier (see clauses C.4.2 and C.4.3).

D.2.3 TL fulfilment

The filling out of TL during the registration and setup phases, implies a set of practices involving TLSO and the SP aiming to adopt REM baseline to REMSP is primarily listed in TL. Furthermore, the SP have to produce and publish, according to the local **REMID policy**, the CapabilityAndSecurityInformation XML structure, and this URI is referenced from the ServiceSupplyPoint element of TL.

Clauses D.1.3 and D.2.2 list the main attention points to consider in these phases.

D.2.4 Flow elements

Other elements on TL and CapabilityAndSecurityInformation are considered during registration and setup phases. These mainly consist in the proper configuration of the systems to respect the flows defined for REM baseline and all the further limits and constraints defined in the local **REMID policy** (see clause D.1.3).

D.3 Periodical practices

Regarding the particular cyclic practices worth mentioning for the REM baseline, there are the publication practices of CapabilityAndSecurityInformation and its digest. Furthermore, the maintaining of the historical files: the number and their digests. See periodical practices illustrated in points of c) and d) of table C.14 and point ix./c.3.1.8 of table C.6, clause C.2.3.4.1.

D.4 Run-time practices

D.4.1 General

Other the particular run-time and day-by-day practices that are worth to be mentioned for REM baseline are the usage of the validation procedures and tools set up for trust and interoperability (e.g. those seen in clauses D.2.2, D.2.3 and D.3 and the run-time part necessary to use the mechanisms illustrated in point of c) and d) of table C.14, verification of digital signatures and protocols/formats/flows consistency, anti-abuse operations, etc.).

D.4.2 Basic handshake

The main run-time **pre-relay operations** implemented by S-REMS foresee to perform the checks on trust and capabilities equivalence before the relay of a REM message to the R-REMS (see rationales of table B.2 and table B.7, and relevant prescriptions in clause C.2.3.3.3, clause C.2.3.4.1 point c.3.1.1 and c.3.1.3 of table C.6, clause C.2.3.4.3 table C.9 and clause C.2.3.4.5 table C.12).

Other practices involve:

1) Version of any trusting/interoperability elements and protocols (e.g. TL, ERDSMetadata, TLS, etc.).

2) Countries of source/destination detection, when required by **REMID policy** to compile the identity components (see points h) and i) of table C.18).

3) As stated in eIDAS TS SAML Attribute Profile [15], clause 2.2.3 the "userid" element is composed of any string of readable characters uniquely identifying the **identity** asserted in the origin country. The **REMID policy** fixes a solution for the "CC/CC/userid" element of the identity component according to the points h) and i) of clause C.3.4, table C.18.

EXAMPLE: The use of a well-known function, stated at **REMID policy** level, (e.g. SHA-256 hash) of the user's email address as "userid" element ensures the unicity of the "userid" to use for both I01 SenderDetails/Sender's Identity attributes and I05 RecipientDetails/Recipient's Identity attributes elements.

D.4.3 Content checks

The run-time **post-relay operations** (post or directly on-the-fly, on streaming basis, before full completion of relay-acceptance operation) implemented by R-REMS foresee to perform:

- formal checks on the received content REM message and ERDS evidence (e.g. see clause C.2.3.3.3);

NOTE: Further practices specified in **REMID policy** make sense like:

1) The sufficiency of the CAdES-S/MIME digital signature validation according to statement <<To establish trust in an ERDS based on information in a TL, an actor, which may be another ERDS, shall validate the ERDS's digital signature on an ERD message **or** ERD evidence >> of ETSI EN 319 522-4-3 [11], clause 7.2. A signed ERDS evidence is intrinsically ensured once it is enveloped in a REM message by the issuer REMS that - contextually - signs also the REM message.

2) The detailed steps to validate the trust as mentioned earlier by extracting the digital certificate, checking its formal validity and by its further validation against the REMS's digital identity on TL.

3) The detailed steps to validate the digest of the original message against the digest conveyed in the ERDS evidence (and MD14 REM-DigestValue metadata header).

4) Detailed steps to check the validity of the service and to validate the compliance between declared/expected service.

- formal checks on capability metadata and capability-based security (e.g. see clauses C.2.3.4.3 and C.2.3.4.5);
- security checks to detect service abuses or threats (e.g. viruses, malware, phishing etc) according to current best practices and local **REMID policy**.

D.4.4 Events checks

The run-time **post-relay operations** implemented by S-REMS and R-REMS foresee performing consistency checks, on an event basis to ensure that the required service is compliant with the REM baseline (e.g. correct messages, correct receipts, etc.), and every transaction is ended. In particular:

- Timeout for transient errors (i.e. temporary error on some step and try to recover within a timeout: see points h)III of table C.22, h)III of table C.23, h)III of table C.24 and h)III of table C.25).

EXAMPLE 1: 1 800 seconds.

- Relay-snd-dsp-wait timeout (i.e. S-REMS was unable to relay the REM dispatch to R-REMS within a given time period: see point a)III of table C.24).

EXAMPLE 2: 86 400 seconds.

- Relay-rcv-ra-wait timeout (i.e. S-REMS was unable to receive a RelayAcceptance REMS receipts within a given time period: see point a)IV of table C.24).

EXAMPLE 3: 86 400 seconds.

- Cycle-number for persistent errors and final behaviours (see point h)II table C.24).

EXAMPLE 4: 8 cycles (of transient errors): in this case they correspond to 4 hours).

- Relay-rcv-ca-wait timeout (i.e. S-REMS was unable to receive a ContentConsignment/ContentConsignmentFailure REMS receipts (after a RelayAcceptance has been received) within a given time period: see point a)I of table C.25).

EXAMPLE 5: 86 400 seconds.

NOTE: There may be particular situations that can be further tuned at **REMID policy** level. For instance when a ContentConsignement REMS receipt is received without receive the related RelayAcceptance REMS receipt. In such case, the usual behaviour is followed: consigning the ContentConsignement REMS receipt to the sender and, according to **REMID policy**, at Relay-rcv-ra-wait timeout a further RelayFailure REMS receipt (e.g. with code RB07 and with further specific Details messages) can be sent to the sender with purpose of tracking the event.

D.4.5 Complete set of examples

A full set of working examples miming significant scenarios identified by the folder "INFORMATIVE-EXAMPLES" are provided in the attachment en_31953204v010300a0.zip accompanying the present document.

Annex E (normative): XML schema files

E.1 XML Schema file location for namespace http://uri.etsi.org/19532/v1#

The XML Schema files for the present document are files "1953204CSIxmlSchema.xsd" and "1953204EvidencexmlSchema.xsd" and are contained in archive en_31953204v010300a0.zip which accompanies the present document and are also available at:

https://forge.etsi.org/rep/esi/x19_53204_rem_services/-/raw/v1.3.1/1953204CSIxmlSchema.xsd, and
https://forge.etsi.org/rep/esi/x19_53204_rem_services/-/raw/v1.3.1/1953204EvidencexmlSchema.xsd.

Annex F (informative): Change History

Date	Version	Information about changes
September 2018	1.1.1	Publication as ETSI EN 319 532-4.
October 2020	1.1.2	Early draft - update of the SMTP interoperability profile selecting a minimum set of requirements, in the form of a REM baseline, for implementation of REM services. This required to define precise details on Common Service Interface (CSI and secure routing), application of digital signatures on both ERDS evidence and REM messages, application of time-stamp on ERDS evidence. The update consisted of adding an informative Annex B with all the rationales derived from a number of other standards and a normative Annex C that leveraging the rationales of Annex B converged to the minimum set of requirements needed for the REM baseline. Finally, drafted a first skeleton for details on best practices as an informative Annex D.
January 2021	1.1.3	Stable draft - update of the version 1.1.2 with a number of further details on ERDS evidence, REM messages and XML particulars to fully complete the minimum set of requirements of REM baseline, and the application of the received comments. This required the update of Annexes B, C and D. Finally, fixed a number of minor editorial issues in clause 5 and adjusted, according to the new content, the usual informative preliminary, general and supplementary clauses at the beginning and the end of the present document.
October 2021	1.1.4	Stable draft - update version 1.1.3 with a number of fixes and adjustments to fix the issues identified in the Plugtests event on June/July 2021.
November 2021	1.1.5	Stable draft - update version 1.1.4 with a number of arrangements matured duringESI#75 and the follow-up discussions.
December 2021	1.1.6	Final draft - update version 1.1.5 with several arrangements due to comments received during the online discussions period.
January 2022	1.1.7	Publication for EN Approval Procedure.
May 2022	1.1.8	Final draft - update version 1.1.7 with a few of fixes due to the editorial comments received during the EN Approval Procedure.
May 2022	1.2.1	Publication of approved EN.
April 2023	1.2.2	Stable draft - update version 1.2.1 with: References and abbreviations: update of RFC versions and added a new RFC for S/MIME certificate handling (2.2); added a new abbreviation and an explanatory note (3.3). Clarifications: moved a requirement from the scope to the introduction (4.1); reworded/fixed text and notes for Implementation guidance (5.4.1: REM-Evidence-ID; 5.5.1.3: SAN for RelayAcceptance, RelayRejection and RelayFailure; C.2.3.4.4/c.3.5.1: TLS hanshake; C.3.4: removed misleading note on EvidenceIdentifier, fixed usage of EventReason/Details code, fixed I01/I02/I05/I06 identity codes settings; C.4.5.1: fixed the list of steps for submission events; C.4.5.2: fixed the list of steps for relay event; C.4.5.3: fixed the list of steps for consignment event), and for Service/Protocol elements (tables in C.2.3.4.1, C.2.3.4.2, C.2.3.4.4); reworded Overview B.3.1 of digital signatures and time-stamp rationales; fixed note on C.2.3.3.3: TLS and signing certificate expired; reworded Overview C.4.1 of digital signatures and time-stamp requirements with two clarification notes. Functionals: added a new RA06 reason code (propagated also to ETSI EN 319 522-2/522-3) for sender's ERDS malfunction (table C.28); D.1.3: added the Relay-rcv-ca-wait timeout; D.2.2.1: added a note clarifying SAN/rfc822Name and SAN/MX relationships; D.2.2.2: added text clarifying "From:" email address/SAN relationship; D.4.4: added text and note clarifying timeout tunings. Rationales: added statement relevant to TL TSP service supply point URI alternative (B.2.2.4/table B.8) for REMS capability and security metadata reference (alignment with table 14 of 532-3). Editorials: fixed typos in terms, names, Service/Protocol Elements, codes and figures (e.g. REM vs ERDS; REM vs REMS; evidence vs receipt; details vs Details; URI format of ServiceSupplyPoint; missing evidence in table C.27/note b; S-REMS missing in D.4.4; fixed numbering of REMS in figure B.1).

Date	Version	Information about changes
June 2023	1.2.3	Final draft - update version 1.2.2 with minor fixes and updated accordingly the ZIP file with the examples. Editorials: fixed typos in figures (e.g. a comma in figure B.5; B05 vs G05 in figure B.9, figure B.10, figure B.11 and figure B.12; name version of zip attachment; C.3.4/table C.18: realigned text in implementation guidance a. and reworded/fixed NOTE 4 and NOTE 6; figure C.5: fixed ERDS evidence signature element in the example; C.4.1/NOTE 2: fixed typo; C.4.5.2/ table C.24: fixed typos in implementation guidance h. and NOTE 5; table C.28: fixed scenarios references; D.2.2.2: fixed text in point 4.); updated the INFORMATIVE section of the ZIP attachment file: added new S8_Diagram scenario covering error cases, fixed typos in terms of the other 7 scenarios (from S1_Diagram to S7_Diagram), added a new option in S2_Diagram scenario covering the new RA06 reason code, fixed all EML S/MIME files (e.g. removing semicolon from S/MIME at the end of evidence declaration, generating new XAdES-BT digital signature of all attached ERDS evidence XMLs and generating new CAdES digital signature of all REM messages EMLs, accordingly), added new folder with details on XAdES-BT and CAdES signatures inside XML ERDS evidence and EML REM message, updated README_FIRST.txt with additional explanatory and clarification text covering the changes applied to the ZIP.
June 2023	1.2.4	Final draft - updated the present Annex E (Change History) with the explicit mention of the main changes.

History

Document history		
V1.1.1	September 2018	Publication
V1.2.1	May 2022	Publication
V1.3.0	October 2023	EN Approval Procedure AP 20240103: 2023-10-05 to 2024-01-03