ETSI EN 319 532-4 V1.1.1 (2018-09)

EUROPEAN STANDARD

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

Reference

DEN/ESI-0019532-4

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

Important notice

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

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

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

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Copyright Notification

ETSI

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

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

Foreword

This European Standard (EN) has been produced by ETSI Technical Committee Electronic Signatures and Infrastructures (ESI).

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

National transposition dates	
Date of adoption of this EN:	23 August 2018
Date of latest announcement of this EN (doa):	30 November 2018
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	31 May 2019
Date of withdrawal of any conflicting National Standard (dow):	31 May 2019

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 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.), and protects against risk of loss, theft, damage and any illegitimate modification. The present document aims to cover the common and worldwide-recognized requirements to address electronic registered delivery in a secure and reliable way. 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 semantic defined in ETSI EN 319 532-1 [4] and ETSI EN 319 532-2 [5]. It deals with issues relating authentication, authenticity and integrity of the information, with the purpose to address the achievement of interoperability across REM service providers, implemented according the aforementioned specifications.

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

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.

More specifically, the present document:

a) Defines generalities on profiling.

b) Defines constraints for SMTP profile.

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".

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 5751: "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 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".

3 Definitions, abbreviations and terminology

3.1 Definitions

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

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI EN 319 532-1 [4] apply.

3.3   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 [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/or 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", while 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, as well as technical standard and service interoperability aspects.

More specifically, the present document specifies a profile for REM service that use the same formats (S/MIME based) and the same transport protocols (SMTP). This is rather an intra-operability profile acting, theoretically, on a pure and homogeneous environment.

4.2   Compliance requirements

Requirements are grouped in three different categories, each one having 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 **Nº** 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/or 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 on the same formats. Under this basis, although many aspects defined here are valid and reusable in other contexts, format and protocols, all the sentences of the present part of the document mainly refer to interactions among REM services providers using - as 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 lies in the fact 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 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 operations.

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 further detailed in 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. As an example, SMTP on TLS according to IETF RFC 7817 [i.13] or SSL plus 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. As an 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 measures 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 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) and, for the purpose of
the present profile, the following three main elements shall be considered:

   1)   Routing

   2)   Trusting

   3)   Capability discovery

   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 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 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 identifier "Id" defined inside the Evidence root element structure 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 in REM message with a list of REM-*ReasonIdentifier* header fields, each with the corresponding URI value.

NOTE: Item Nº 4 in table 7 facilitates achieving of interoperability that, however, 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)   An 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 fields constraints, present in table 6 of ETSI EN 319 532-3 [6], clause 6.2.3.2 shall apply. An encoding according to the parameter: charset="UTF-8" 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 fields constraints, present in table 6 of ETSI EN 319 532-3 [6], clause 6.2.3.3 shall apply. An encoding according to the parameter: charset="UTF-8" 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-paragra-Type	Clause 6.2.4.2	M	a	

Implementation guidance:

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

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

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

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	

Implementation guidance:

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

b)   The value of 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 Content-Disposition and/or 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 his/her message submission.				
NOTE 2:	Rationale: The sender is made aware on whether the recipient was/was not made available (within the boundaries of 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 on whether the recipient was/was not made available (within the boundaries of recipient's REMS) of the notification the sender's REMS generated in relation to 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 back to the sender a REM receipt including the evidence relevant to the event of 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 back to the sender one REMS receipt 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 B1	Conditional	a, b, c	see note
2	RelayRejection	Clause 6.2.2 B2	Conditional	a, b, c	see note
3	RelayFailure	Clause 6.2.2 B3	Conditional	d, e	see note
NOTE:	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:

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

    II)   The sender's REMS will assume that a REM dispatch or payload has been accepted by the recipient's REMS if any other contrary indication (e.g. REMS evidence 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 REM receipt including the RelayAcceptance or the RelayRejection evidence.

    c)   In the cases addressed in the previous item 1, the sender's REMS shall build a REM receipt including the RelayRejection evidence (and/or any other contrary indication to the relay, like SMTP DSN) and shall send it back to the sender.

Implementation guidance for 3:

    d)   RelayFailure shall be generated if there is not an 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 REM, if any other contrary indication (e.g. REMS evidence and or SMTP DSN) is received within a predefined time period.

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

    e)   The sender's REMS shall build a REM receipt, including the RelayFailure evidence (and/or 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 so far. More in detail, the following clauses list all Evidence components that are required to ensure interoperability, including those that 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.

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: 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 1
2	Event identifier=SubmissionAcceptance or SubmissionRejection	G03	M		see note 1
3	Reason identifier	G04	M		
4	Reason code	G04	M (1..N)	a	
5	Evidence version	G02	M		see note 1
6	Event time	G05	M		see note 1
7	Evidence issuer policy identifier	R01	M (1..N)		see note 1
8	Evidence issuer details	R02	M		see note 1
9	Sender's identifier	I02	M		see note 1
10	Recipient's identifier	I06	M (1..N)		see note 1
11	Sender 's identity assurance details	I10	O	b	
12	User content information	M02	M		see note 1
13	Reply-to	MD09	M	c	see note 1
14	Submission date and time	M03	M		see note 1
15	Message type	MD13	R	d	
16	Signature	R03	M		see note 1
17	Message Identifier	M01	M		see note 1
NOTE: This requirement is present as 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 when submission is regularly accepted no Reason code is necessary. Multiple Reason codes may be present depending on the reasons that caused the evidence's triggering event.

b)   If this field is not present it means that 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.

c)   This field shall be present containing the email address of the original sender, unless the applicable REMIDs explicitly require that no Reply-to is necessary.

d)   This field should be present according to the semantic of ETSI EN 319 522-2 [2], clause 6.2.13.

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	Message type	MD13	R	b	
14	Signature	R03	M		see note
15	Message Identifier	M01	M		see note
NOTE: This requirement is present as 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 when consignment regularly occurred no Reason code is necessary. Multiple Reason codes may be present depending on the reasons that caused the evidence's triggering event.

b) This field should be present according to the semantic of ETSI EN 319 522-2 [2], clause 6.2.13.

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	Message type	MD13	R	b	
15	Signature	R03	M		see note
16	Message Identifier	M01	M		see note
NOTE: This requirement is present as 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 when download regularly occurred no Reason code is necessary. Multiple Reason codes may be present depending on the reasons that caused the evidence's triggering event.

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

c) This field should be present according to the semantic of ETSI EN 319 522-2 [2], clause 6.2.13.

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	Message Type	MD13	R	b	
13	Signature	R03	M		see note
14	Message Identifier	M01	M		see note
15	External ERDS	M05	M		see note
NOTE: This requirement is present as 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 when the relay to the recipient's REMS regularly occurred no Reason code is necessary. Multiple Reason codes may be present depending on the reasons that caused the evidence's triggering event.

b) This field should be present according to the semantic of ETSI EN 319 522-2 [2], clause 6.2.13.

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	Message Type	MD13	R	b	
13	Signature	R03	M		see note
14	Message Identifier	M01	M		see note
15	External ERDS	M05	M		see note
NOTE: This requirement is present as 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 when relay to the recipient's REMS failed no Reason code is necessary. Multiple Reason codes may be present depending on the reasons that caused the evidence's triggering event.

    b)   This field should be present according to the semantic of ETSI EN 319 522-2 [2], clause 6.2.13.

Annex A (informative):
REM best practices

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

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 5751 [i.11]).

History

Document history			
V1.0.0	May 2018	EN Approval Procedure	AP 20180823: 2018-05-25 to 2018-08-23
V1.1.1	September 2018	Publication	