ETSI EN 319 532-3 V1.2.1 (2019-04)

Electronic Signatures and Infrastructures (ESI);
Registered Electronic Mail (REM) Services;
Part 3: Formats

Reference

REN/ESI-0019532-3v121

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

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

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

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 3 of a multi-part deliverable. Full details of the entire series can be found in part 1 [10].

National transposition dates	
Date of adoption of this EN:	9 April 2019
Date of latest announcement of this EN (doa):	31 July 2019
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	31 January 2020
Date of withdrawal of any conflicting National Standard (dow):	31 January 2020

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.5]. However, the legal effects are outside the scope of the present document.

1 Scope

The present document specifies the formats for messages that are produced and handled by a Registered Electronic Mail (REM) service according to the concepts and semantic defined in ETSI EN 319 522 parts 1 [7] and 2 [8] and ETSI EN 319 532 parts 1 [10] and 2 [11]. More specifically, the present document:

a) Specifies how the general ERDS concepts like user content and metadata are identified and mapped in the standard email structure.

b) Specifies how the aforementioned concepts are mapped in the REM service messaging structures.

c) Specifies how the ERDS evidence set is plugged inside the REM service messaging structures.

d) Specifies additional mechanisms like digital signature and other security controls.

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] IETF RFC 8118: "The application/pdf Media Type".

[2] IETF RFC 2183: "Communicating Presentation Information in Internet Messages: The Content-Disposition Header Field".

[3] IETF RFC 5751: "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification".

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

[5] IETF RFC 2854: "The 'text/html' Media Type".

[6] IETF RFC 7303: "XML Media Types".

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

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

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

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

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

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

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

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

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

2.2 Informative references

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

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

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

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

[i.2] ETSI TS 119 312: "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites".

[i.3] IETF RFC 6648: "Deprecating the "X-" Prefix and Similar Constructs in Application Protocols".

[i.4] ETSI EN 319 521: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Electronic Registered Delivery Service Providers".

[i.5] 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.6] ETSI EN 319 122-1: "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures".

[i.7] ETSI EN 319 142-1: "Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures".

[i.8] ETSI EN 319 522-4-3: "Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 4: Bindings; Sub-part 3: Capability/requirements bindings".

[i.9] IETF RFC 6931: "Additional XML Security Uniform Resource Identifiers (URIs)".

3 Definition of terms, abbreviations and terminology

3.1 Terms

For the purposes of the present document, the terms given in ETSI EN 319 532-1 [10] apply.

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI EN 319 532-1 [10] apply.

3.3 Terminology

Since Registered Electronic Mail Services are specific types of Electronic Registered Delivery Services, the present document uses the terms and definitions from ETSI EN 319 521 [i.4] and ETSI EN 319 522 [7], [8] and [9].

ETSI EN 319 532-2 [11], 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 is prefixed with "ERDS" or "REMS", while constructs whose content includes user generated data is prefixed with "ERD" or "REM".

4 Message formats

4.1 Introduction

The present clause defines and explains how metadata and contents are formatted in REM messages. Schemas and format definitions of ETSI EN 319 522-3 [9] are reviewed in the REM perspective. Further implicit references are to ETSI EN 319 532-2 [11], clause 4 describing the contents.

To define the formats involved in communication exchanges in the REM (and so email) scope, it is necessary to individuate and distinguish fundamental parts like user content and metadata components.

As outlined in ETSI EN 319 522-2 [8], clause 4, the user content is the content generated or provided by the sender, that is intended to be delivered to a recipient. Metadata related to the user content, e.g. in the case of submission, relay or handover events, are provided for purposes of handling and processing a message, e.g. message identification, identification of sender/recipient(s), or also for service capabilities discovery.

Annex A describes how these meaningful concepts have been mapped first in email and later in REMSs provision context starting with a description example for a graphical individuation of the components. Next clauses describe how ERD concepts are mapped on REM following with the format specifications.

4.2 Internet Message Format in the REM services

In the context of email and REM services provision the concepts like user content and metadata have a correspondence with the elements of Mail Object as defined in IETF RFC 5321 [14], clause 2.3.1 and with the definitions contained in ETSI EN 319 522-1 [7], clause 3.1, ETSI EN 319 522-2 [8], clause 4, and ETSI EN 319 532-2 [11], clause 4.

Table 1 illustrates the root of terms (if any), used in the next clauses, and the intended meaning in the REM context.

Table 1: ERD to REM terms mapping

Root definition (from ETSI EN 319 522-2 [8])	REM equivalent definition	Detailed definition
user content	**user content**	This is the body of the Mail Object as defined in IETF RFC 5321 [14], clause 2.3.1 (note 1). It is generated by the sender under the sender's technical/legal responsibility. See also ETSI EN 319 532-2 [11], clause 4.
submission metadata	**submission metadata**	This is the header section of the Mail Object as defined in IETF RFC 5321 [14], clause 2.3.1. See Figure 1, Figure 4 and also definitions in ETSI EN 319 532-2 [11], clause 4.
	original message	This is composed of header + body as defined in IETF RFC 5321 [14], clause 2.3.1. It is generated by the sender's ERD user agent or under the sender's technical/legal responsibility (and outside the responsibility of the service), which may be eventually digitally signed by the sender (note 1). See Figure 1, Figure 4 and also definitions in ETSI EN 319 532-2 [11], clause 4.

Root definition (from ETSI EN 319 522-2 [8])	REM equivalent definition	Detailed definition
ERDS relay metadata	**REMS relay metadata**	This is the header section (as defined in IETF RFC 5321 [14]) of the REM message. Also the REMS introduction is considered part of the REMS relay metadata. See from Figure 1 to Figure 4 and also definitions in ETSI EN 319 532-2 [11], clause 4.
ERDS handover metadata	**REMS handover metadata**	The same of mapping of REMS relay metadata with the semantic defined in ETSI EN 319 532-2 [11], clause 4.
ERDS evidence	**ERDS evidence**	One of the methods usable to transport the ERDS evidence in REM is an attachment body part (as defined in IETF RFC 2045 [12]) of the REM message. See from Figure 1 to Figure 3 and also definitions in ETSI EN 319 532-2 [11], clause 4.
ERDS serviceInfo	**REMS notification**	See Figure 3 for the structure of this object and definitions in ETSI EN 319 532-1 [10], clause 3.1. The difference from ERDS serviceInfo is that a REMS notification always contains a reference to the user content. Furthermore, it may optionally carry the relevant evidence.
ERD message	**REM message**	See from Figure 1 to Figure 4 for all the possible structures in parts (as defined in IETF RFC 2045 [12]).
ERD payload	**REM payload**	See Figure 4 for the structure of this object and also definition in ETSI EN 319 521 [i.4], clause 3 and ETSI EN 319 522-1 [7], clause 3.
ERD dispatch	**REM dispatch**	See Figure 1 for the structure of this object and also definition in ETSI EN 319 521 [i.4], clause 3 and ETSI EN 319 522-1 [7], clause 3 and further details in ETSI EN 319 532-2 [11], clause 4. It is a new object (according to the REM message structure) generated by the REM Service enclosing the original message and other contents generated by the REM Service, who is responsible only for part of its contents (it is not responsible for the contents of the original message).
	transport metadata	When the original message is submitted over SMTP, this is the transport information and the closure information conveyed in a typical SMTP session (see Figure A.1). It wraps the original message inside the SMTP transaction and it contains commands and answer information flowing during the client/server communication, as defined in IETF RFC 5321 [14] (note 2).

NOTE 1: The term **body**, in the context of the present document, indicates also a "possibly structured" body part including one or more attachments, according to MIME standard specification, as provided in IETF RFC 2045 [12], clause 2.6.

NOTE 2: Further considerations regarding specific protocol elements like transport and closure are out of scope for the present document and are managed in ETSI EN 319 532-4 [i.1], clause 5.3.5 - CSI.

In the email ambit, (that is the basis of REM), the aforementioned concepts apply to the messaging stream.

Figure A.1 shows an example of where the constructs shown in Table 1 are located along the protocol stream.

An important feature specific for REM is that exactly the standard wrapping mechanism shown in Figure A.1 is also used to incorporate a digital signature into a REM message structure for getting a signed REM message (see Figure A.2). For example, in case of the REM dispatch, it is used to transport the original message together with the other REM message components as attachments and digital signatures, giving the possibility to make available the entire content in a comprehensible and usable way to all interested parties from the sender's REMS up to the recipient (see Figure A.1).

See Figure A.2 as an example representing this further step, by showing the encapsulation of the original message in a REM dispatch and, similarly the previous example of Figure A.1, where it is located inside the protocol stream.

The same wrapping mechanism shall be used for enveloping the remaining objects relevant to the REM messages.

As the REM message contents are separated from the transport information/closure information parts in the communication stream, the entire set of REM messages as specified in the present document may also be properly transported by other underlying transport protocols.

NOTE 1: This separation ensures that REM messages are completely unrelated to the underlying protocol stream.

In fact, the underlying protocol only deals with the transport information and closure information of the stream and the REM message remains unchanged. All the REM logic is defined inside the REM message. This makes REM independent from the particular underlying transport protocol. In addition, as REM messages use this universal and standard enveloping, any standard email client of the initiator and/or the final users can process them.

The transmission of information between the sender's REMS and recipient's REMS typically happens according to the "attached" or "detached" forms. In the first case the original message is conveyed inside a REM dispatch. In the latter, it is transmitted using other means (e.g. by a REM payload). The ERDS evidence related to events occurred during the transfer of this original message is sent separately to the recipient, e.g. by a subsequent REM receipt.

The REM Service could add/modify some header fields to the submission metadata during the enveloping process. Anyway, these changes should be limited to what is proven as essential for the good working of the process and should be fully defined in the specific REM implementation.

NOTE 2: Update of the Message-ID header field can be one of these changes (if it is not present or it needs to be normalized to a universal recognized identifier format, inside the context of the provided service). In such cases, the original identifier, if specified, is assigned to some new custom header field of the submission metadata and to the REM-UAMessageIdentifier: header field of the REM message. A new regularized and universal unique Message-ID is assigned to the submission metadata.

Furthermore, any of the aforementioned changes (additions/modifications of header fields) shall be clearly indicated to the sender and recipient of the REM dispatch or the REM payload.

NOTE 3: The "REMS introduction MIME section" descriptive text - see clause 6.2.3.4 - is one of the places where the REMS can put such an indication. Alternatively, the contract with the users represents another place where the REMS can indicate this systematic practice.

4.3 REM message - Structure Definition

This clause specifies the structure of a REM message based on the MIME format (see IETF RFC 2045 [12]). A REM message does not exist as a self-standing object, since it always appears in the context of either a REM dispatch, a REMS receipt, a REMS notification or a REM payload.

A REM message may flow between different REMSs, and from a REMS to ERD user agents, as defined in ETSI EN 319 532-1 [10]. It is out of scope of the present document to define how the generic REM message is tailored to the specific mode of operation and interface it flows through.

See the description preceding Figure A.3 for examples of REM message components.

A REM message shall be structured as a message header section containing the header fields followed by a message body composed of several body parts as defined in MIME (IETF RFC 2045 [12]). The message body shall take the form of multipart signed/mixed/alternative MIME sections, in which every MIME-body-part is structured as defined in Figure A.3. This multipart/mixed MIME message shall constitute the signed MIME-body-part of a multipart/signed S/MIME message. The S/MIME signature contained in the last MIME part of the REM message shall therefore be the digital signature of the REMS over the rest of the MIME parts that appear in the REM message.

See Figure A.3 as an example representing this generic structure with all its elements. The different types of REM messages are built as indicated in Table 1 of ETSI EN 319 532-2 [11], clause 4.1, which in turn is derived from Table 1 of ETSI EN 319 522-2 [8], clause 4.

The REM dispatch shall be structured as in Figure 1.

The REMS receipt shall be structured as in Figure 2.

The REMS notification shall be structured as in Figure 3 and shall be generated by REMS according to the flow requirements of ETSI EN 319 532-1 [10], clause 4 and ETSI EN 319 532-2 [11], clause 4.

The REM payload shall be structured as in Figure 4.

They are built starting from the ERD message structure, defined in Table 1 of ETSI EN 319 522-2 [8], clause 4, with the emphasis of REM specific aspects and peculiarities.

The cardinality numbers present in the boxes shall indicate the number of occurrences of any MIME part:

- **0..1** indicates an optional part;
- **0..N** indicates an optional part that may occur any number of times;
- Parts not otherwise indicated by cardinality numbers or remarked for clarity with **1** shall occur exactly once.

<table>
<tr><td rowspan="15">REM dispatch structure</td><td>Header</td><td colspan="6">MIME header fields profiled for a multipart/signed MIME message (see clause 6.2.1)
[REMS relay metadata 1 plus optionally REMS handover metadata 0..1]</td></tr>
<tr><td rowspan="14">Body</td><td rowspan="12">(signed data MIME section)</td><td>Header</td><td colspan="5">MIME part header fields profiled for a multipart/mixed message (see clause 6.2.2)
[REMS relay metadata]</td></tr>
<tr><td rowspan="11">Body</td><td rowspan="3">REMS introduction MIME section [REMS relay metadata] 1</td><td>Header</td><td colspan="3">MIME part header fields profiled for a multipart/alternative MIME content (see clause 6.2.3)</td></tr>
<tr><td rowspan="4">Body</td><td rowspan="2">Plain text introduction</td><td>Header</td><td>MIME part header fields profiled for text/plain (see clause 6.2.3.2)</td></tr>
<tr><td>Body</td><td>A message created by the REMS, to be displayed automatically upon display of the REM message. Text may contain information for the user (see clause 6.2.3.4)</td></tr>
<tr><td rowspan="2">HTML introduction</td><td>Header</td><td>MIME part header fields profiled for text/html (see clause 6.2.3.3)</td></tr>
<tr><td>Body</td><td>A message created by the REMS, to be displayed automatically upon display of the REM message. HTML may contain URIs and other information for the user (see clause 6.2.3.4)</td></tr>
<tr><td rowspan="2">original message MIME section 1</td><td>Header</td><td colspan="3">MIME part header fields profiled for an enveloped message/rfc822 message (see clause 6.2.4.2)</td></tr>
<tr><td>Body</td><td colspan="3">Header and Body of a self-contained IETF RFC 5322 [4] message as submitted by the sender: the submission metadata that becomes part of the REMS relay metadata and the user content (see clause 6.2.4.3)</td></tr>
<tr><td rowspan="2">REMS Extensions MIME section 0..N</td><td>Header</td><td colspan="3">MIME part header fields profiled for extensions, e.g. application/xml (see clause 6.2.5)</td></tr>
<tr><td>Body</td><td colspan="3">Attachment to be used by possible extensions</td></tr>
<tr><td rowspan="2">ERDS evidence MIME section 1..N</td><td>Header</td><td colspan="3">MIME part header fields profiled for an application/xml or application/pdf (see clause 6.2.6)</td></tr>
<tr><td>Body</td><td colspan="3">ERDS evidence as required by the specific content-type</td></tr>
<tr><td rowspan="2">REMS signature</td><td>Header</td><td colspan="5">MIME part header fields profiled to S/MIME application/pkcs7-signature signature on the whole REM message (see clause 6.2.7)</td></tr>
<tr><td>Body</td><td colspan="5">S/MIME digital signature generated by the REMS covering the whole structure</td></tr>
</table>

Figure 1: REM dispatch structure