# Draft ETSI EN 319 532-3 V0.0.5 (2017-10)

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

STABLE DRAFT FOR PUBLIC REVIEW UNTIL 29 DECEMBER 2017

Download the template for comments:

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

Send comments ONLY to E-SIGNATURES_COMMENTS@list.etsi.org

CAUTION: This DRAFT document is provided for information and is for future development work within the ETSI Technical Committee ESI only. ETSI and its Members accept no liability for any further use/implementation of this Specification. Approved and published specifications and reports shall be obtained exclusively via the ETSI Documentation Service at http://www.etsi.org/standards-search

0

1

Reference

DEN/ESI-0019532-3

Keywords

<keywords>

2

*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*

### *Copyright Notification*

# Contents

# Intellectual Property Rights

## Essential patents

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

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

## Trademarks

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

# Foreword

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

The present document is part 3 of a multi-part deliverable covering Registered Electronic Mail (REM) Services, as identified below:

Part 1: "Framework and architecture";

Part 2: "Semantic contents";

**Part 3: "Formats";**

Part 4: "Interoperability profiles";

| 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.

# Executive summary

Editorial Note: this section will be completed in the next developments of the present document.

# Introduction

Editorial Note: this section will be completed in the next developments of the present document.

# 1 Scope

The basic purpose of Registered Electronic Mail (REM) is to provide a service for the transmission of information among parties, counting on an evidence set, related to the communication steps, suitable to uphold proof of acceptance, of sending, of delivery/non-delivery, receiving/retrieval of the conveyed data. The email standards used as backbone, including a set of additional security mechanisms, make smooth the interoperability and, at the same time, protect the integrity, the confidentiality and the loss exposition of the carried information.

The present document specifies the formats for the contents of the different messages that are produced and handled by the REM service. More specifically:

a) Describes how the general ERDS concepts like “user content” and “metadata” are identified and mapped in the standard email structure

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

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

e) Defines the additional mechanisms, like “digital signature” and security features, that are fundamental to the achievement of the scope.

The specifications defined in the present document aims to cover the common and worldwide-recognized requirements to address **electronic delivery** in a secure and reliable way. Particular attention is paid to all the articles and requirements of the Regulation (EU) No 910/2014 [i.12]. Anyway, the legal effects of services implemented according to the present document are outside the scope of the same.

# 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 1: 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 319 122-1: "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures ".

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

[5] W3C Recommendation: "XML Signature Syntax and Processing".

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

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

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

[9] OASIS Standard Specification "Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0", 15 March 2005.

NOTE 1: Available at: http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf

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

[11] ETSI EN 319 531: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Registered Electronic Mail Services Providers".

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

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

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

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

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

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

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

[19] IETF RFC 5321: "Simple Mail Transfer Protocol"

## 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 1: 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 TR 102 605: "Electronic Signatures and Infrastructures (ESI); Registered E-Mail".

[i.2] European Commission CEF Digital, eID eIDAS Profile Technical Specifications version 1.1, especially the parts “eIDAS Message Format_v1.1-2” and “eIDAS SAML Attribute Profile v1.1_2”

NOTE 2: Available at: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eID+eIDAS+profile.

[i.3] ETSI EN 319 532-4: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) Services; Part 4: Interoperability profiles".

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

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

[i.6] ETSI EN 319 522-4-3: "Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 4-3: Capability and requirements bindings".

[i.7] ETSI TS 119 312: "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites".

[i.8] ETSI TS 119 612: "Electronic Signatures and Infrastructures (ESI); Trusted Lists".

| | |
|---|---|
| [i.9] | ETSI TS 119 524: "Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Testing Conformance and Interoperability of Electronic Registered Delivery Services.". |
| [i.10] | ETSI TS 119 534: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) Services; Testing Conformance and Interoperability of Electronic Registered Mail Services". |
| [i.11] | ETSI TR 119 500: "Electronic Signatures and Infrastructures (ESI); Business Driven Guidance for Trust Application Service Providers". |
| [i.12] | 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. |

# 3 Definitions, abbreviations and terminology

## 3.1 Definitions

For the purposes of the present document, the terms and definitions given in the following document apply.

ETSI EN 319 532-1 [15]

## 3.2 Abbreviations

For the purposes of the present document, the abbreviations given in the following document apply:

ETSI EN 319 532-1 [15]

Furthermore, together with those included in the aforementioned documents, the following abbreviations apply:

| | |
|---|---|
| UA | User Agent |

## 3.3 Terminology

Due to the parallelism that there is between Registered Email Services and Electronic Delivery Registered Services, the present document uses the terms and definitions coming from ETSI EN 319 521 [10] and ETSI EN 319 522 [12] [13] [14] family of documents. To indicate this affinity, when applicable, “ERD” prefix is inherited and used together the terms and their meanings coming from ETSI EN 319 532-2 [16] Clauses 3,4 and - transitively - from its relevant connected normative references. When, for the purpose of the present document - due to the REM peculiarity or for clarity - this is not possible or opportune, the “REM” prefix is used instead in any definition. The key of interpretation is to consider “REM” prefix paired with “RED” and “REMS” (i.e. REM Service) with “ERDS”.

NOTE: The prefix REM (without S) is used when the related object is relevant or may be relevant to something generated “outside” the REM Service. Conversely, the REMS prefix is used when it refers to an object that is produced by the REM Service.

# 4 Message formats

## 4.1 Introduction

The present section defines and explains how metadata and contents composing an electronic communication are formatted in the ambit of REM. This description mainly refers to the rational that lead to schemas and format definitions of  ETSI EN 319 522-3 [14] that are reviewed in the REM perspective. Further implicit references are to ETSI EN 319 532-2 [16] Section 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” (that represents the “payload”) and “metadata” components.

As outlined in ETSI EN 319 522-2 [13] Section 4, referring to the ERDS general perimeter, the “user content” is the Sender’s content that is intended to be delivered to a recipient. Whereas the “submission”, “relay” or “handover” metadata, related to the “user content”, are provided for purposes of identification of itself and/or of Sender/Recipient(s), and/or also for discovery of service capabilities.

The next sections describe how these meaningful concepts have been mapped first in email and later in REM ambits starting with a description example for a graphical individuation of the components, and following with the format specifications.

## 4.2 Internet Message Format in the REM context example

In email area (that, generally speaking, represents the constitutional element of REM) the aforementioned concepts like “user content” and “metadata” have, respectively, a correspondence with the elements of “Mail Object” as defined in IETF RFC 5321 [19] Section 2.3.1, joined up with the definitions contained in ETSI EN 319 522-1 [12] Section 3.1, ETSI EN 319 522-2 [13] Clause 4, ETSI EN 319 532-2 [16] Clause 4.

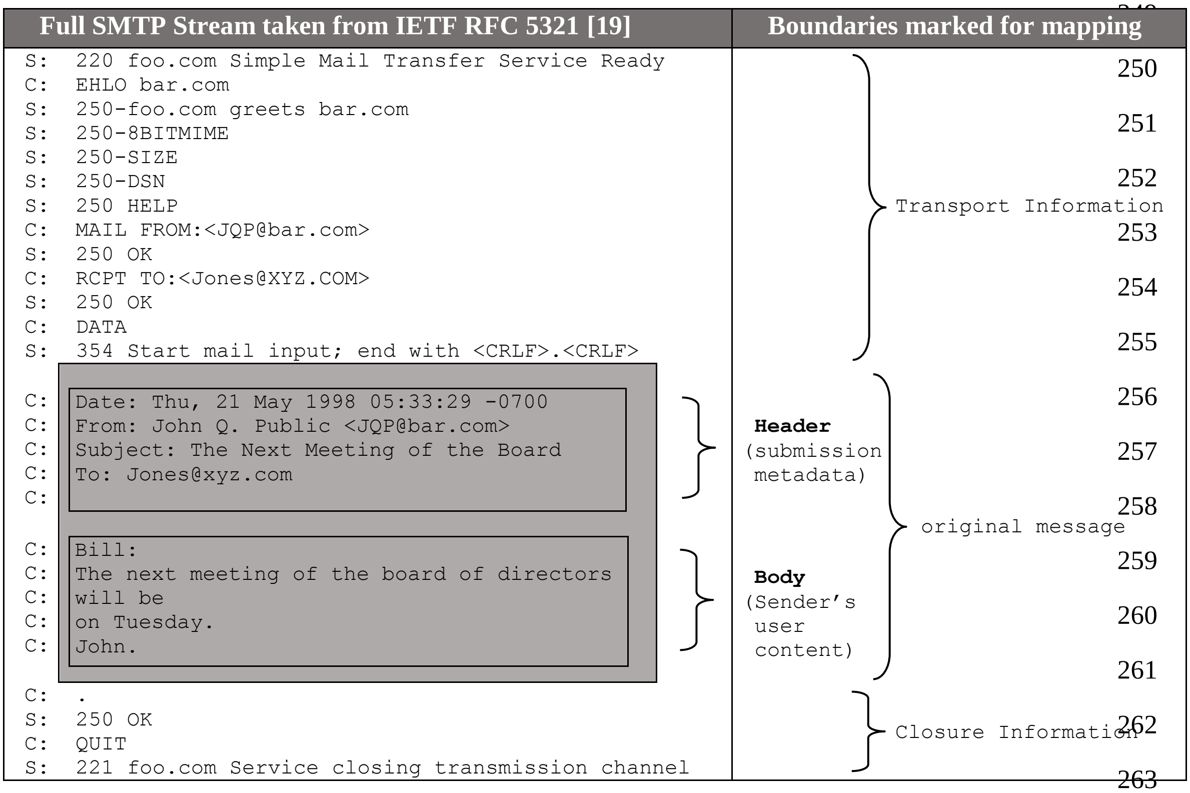
Therefore, for the purpose of the present document the terminology and principles defined in Clause 3.3 shall apply.

The following table illustrates the root of terms (if any), used in the next sections, and the intended meaning in the REM context.

| **Root definitions (from ETSI EN 319 522-2** [13]**)** | **REM equivalent definition** | **Notes** |
|---|---|---|
| *user content* | **user content** | This is the **Body** of the “Mail Object” as intended in IETF RFC 5321 [19] Section 2.3.1. It is generated by the Sender under the Sender's technical/legal responsibility. See also ETSI EN 319 532-2 [16] Clause 4<br>NOTE 1: From some view point, also the **subject** and perhaps the **addresses** Header elements could be considered part(s) of the user content (as contents that the sender specifies together the Body of the message). This theoretical view is masked by the applications that is normal used by the sender like email client and/or webmail. To maintain coherence with widely recognized separation Header/Body, defined also in email international standards, and to simplify the exposition in the present document, these elements of the Header are considered outside the user contents. |
| *submission metadata* | **submission metadata** | This is the **Header** of the “Mail Object” as intended in IETF RFC 5321 [19] Section 2.3.1. See Figure 3, Figure 4, Figure 7 and also definitions in ETSI EN 319 532-2 [16] Clause 4 |
| | **original message** | This is composed of **Header** + **Body** as intended in IETF RFC 5321 [19] Section 2.3.1. It is generated by the Sender's 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. See Figure 3, Figure 4, Figure 7 and also definitions in ETSI EN 319 532-2 [16] Clause 4<br>NOTE 2: 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 [17]. |
| *ERDS relay metadata* | **REMS relay metadata** | This is the **Header** (as intended in IETF RFC 5321 [19]) of the new object (according to the REM message structure) generated under the responsibility of the REM Service, used to envelop the **original message**. Also the REMS introduction is considered part of the REMS relay metadata. See from Figure 3 to Figure 7 and also definitions in ETSI EN 319 532-2 [16] Clause 4 |

| | | |
|---|---|---|
| *ERDS evidence* | **ERDS evidence** | One of the methods usable to transport the ERDS evidence in RM is an attachment **Body Part** (as intended in IETF RFC 2045 [17]) of the new object (according to the REM message structure) generated under the responsibility of the REM Service, used to envelop the **original message**. See from Figure 3 to Figure 6 and also definitions in ETSI EN 319 532-2 [16] Clause 4 |
| *ERDS serviceInfo* | **REMS notification** | See Figure 6 for the structure of this object and definitions in EN 319 532-1 [15] Clause 3.1. The difference with ERDS serviceInfo is that a REMS notification achieves the recipient. Furthermore, it may carries optionally the relevant evidence. |
| *ERD message* | **REM message** | See from Figure 3 to Figure 7 for all the possible structures in parts (as intended in IETF RFC 2045 [17]) |
| *ERD payload* | **ERD payload** | See Figure 7 for the structure of this object and also definition in ETSI EN 319 521 [10] Clause 3 and ETSI EN 319 522-1 [12] Clause 3 |
| *ERD dispatch* | **REM dispatch** | See Figure 4 for the structure of this object and also definition in ETSI EN 319 521 [10] Clause 3 and ETSI EN 319 522-1 [12] Clause 3. It is a new object (according to the REM message structure) generated under the responsibility of the REM Service, used to envelop the **original message**, plus the **original message** itself. So, the REM dispatch, as a whole, is not totally generated under the responsibility of REM Service.<br>NOTE 3: Due to the aforementioned reason on the responsibility, this definition has only the “REM” prefix instead of “REMS”. |
| | **transport metadata** | This is the Transport Information and the Closure Information conveyed in a typical SMTP session (see Figure 1). It wraps the **original message** inside the SMTP transaction and it contains commands and answer information flowing between client/server dialogue, as intended in IETF RFC 5321 [19]<br>NOTE 4: Further considerations regarding specific protocol elements like Transport and Closure are out of scope for the present document and are, in some measure, managed in ETSI EN 319 532-4 [i.3] Clause 5.3.5 - CSI. |

In the email ambit, (that is the basis of REM), the aforementioned concepts apply to the messaging stream as outlined in the next informative example of Figure 1.



```
S:  220 foo.com Simple Mail Transfer Service Ready
C:  EHLO bar.com
S:  250-foo.com greets bar.com
S:  250-8BITMIME
S:  250-SIZE
S:  250-DSN
S:  250 HELP
C:  MAIL FROM:<JQP@bar.com>
S:  250 OK
C:  RCPT TO:<Jones@XYZ.COM>
S:  250 OK
C:  DATA
S:  354 Start mail input; end with <CRLF>.<CRLF>

C:  Date: Thu, 21 May 1998 05:33:29 -0700
C:  From: John Q. Public <JQP@bar.com>
C:  Subject: The Next Meeting of the Board
C:  To: Jones@xyz.com
C:

C:  Bill:
C:  The next meeting of the board of directors
C:  will be
C:  on Tuesday.
C:  John.
C:  .
S:  250 OK
C:  QUIT
S:  221 foo.com Service closing transmission channel
```

**Figure 1: Boundaries in email stream example**

In the previous example, taken from IETF RFC 5321 [19], the **original message** represents the main interesting part to examine in the present document.

To do a parallel with the definitions contained in ETSI EN 319 522, the “Transport Information” and “Closure Information” sections are set apart and represent the “transport metadata”.

NOTE 5: Further considerations regarding specific protocol elements like Transport and Closure are out of scope for the present document and are, in some measure, managed  in ETSI EN 319 532-4 [i.3] Clause 5.3.5 - CSI.

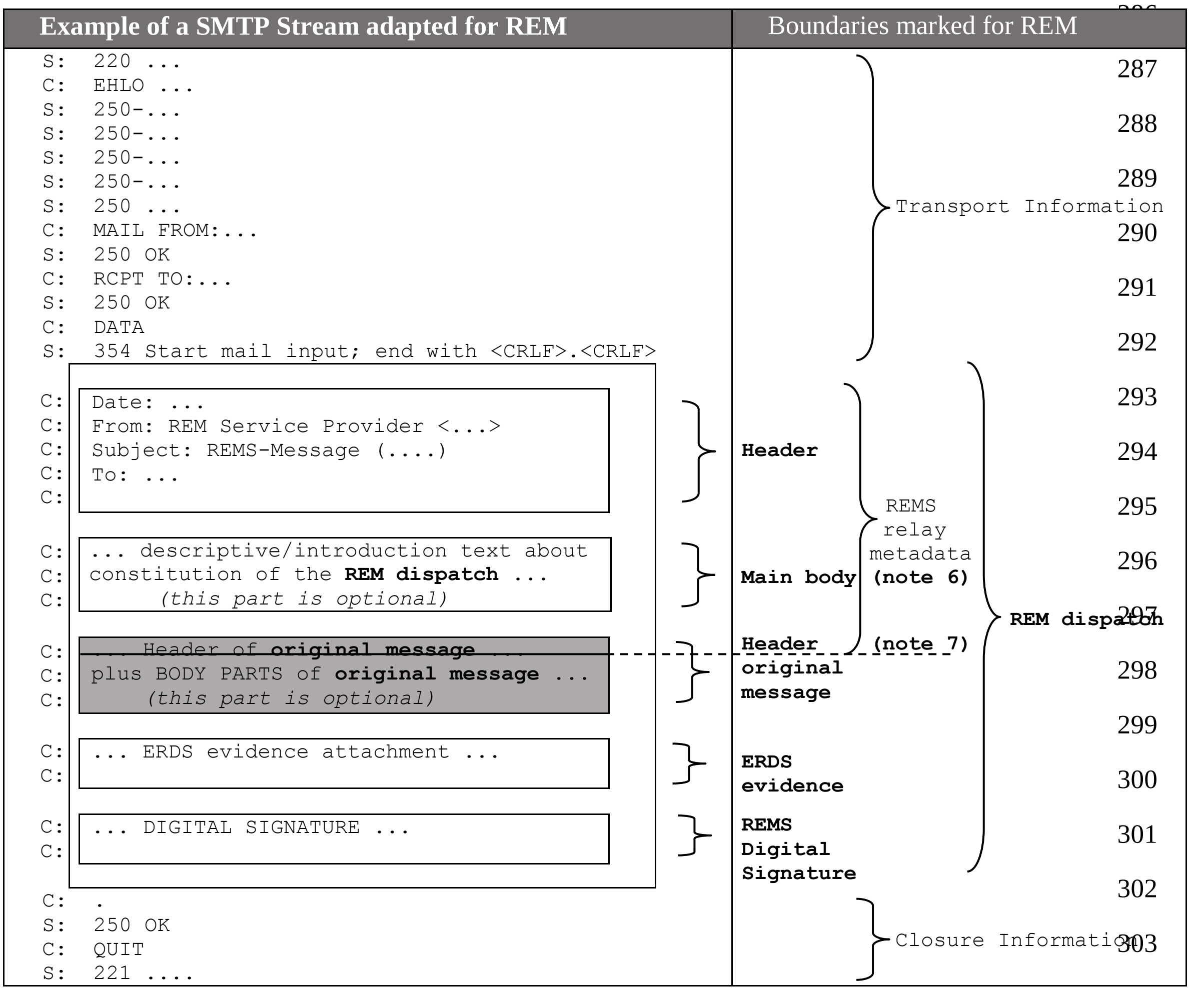
Whereas, the Header section contains the content metadata (referred in the present document as “submission metadata”). Finally, the Body section is the Sender’s user content.

Header and Body, together, form the “**original message**” and they represent the real object that is intended to be conveyed to the Recipient(s). Therefore, the **original message** contains some metadata.

The Figure 1 above represents the place where the object under description is located along the protocol stream.

Another important feature specific of REM is that, exactly the same standard wrapping mechanism, like that described above it is also used to create the “digital signed vector” composing the REM message structure. For example, in case of the **REM dispatch**, this vector is used to transport, as attachments, the **original message**, together the other REM message components, giving the possibility to make available the entire content comprehensible and usable by all the interested parts (from the Sender’s service provider up to the Recipient).

The following informative representation exemplifies this further step, by showing encapsulating of the **original message** in a **REM dispatch**.



```
S:  220 ...
C:  EHLO ...
S:  250-...
S:  250-...
S:  250-...
S:  250-...
S:  250 ...
C:  MAIL FROM:...
S:  250 OK
C:  RCPT TO:...
S:  250 OK
C:  DATA
S:  354 Start mail input; end with <CRLF>.<CRLF>

C:  Date: ...
C:  From: REM Service Provider <...>
C:  Subject: REMS-Message (....)
C:  To: ...
C:

C:  ... descriptive/introduction text about
C:  constitution of the REM dispatch ...
C:       (this part is optional)

C:  ... Header of original message ...
C:  plus BODY PARTS of original message ...
C:       (this part is optional)

C:  ... ERDS evidence attachment ...
C:

C:  ... DIGITAL SIGNATURE ...
C:
C:  .
S:  250 OK
C:  QUIT
S:  221 ....
```

NOTE 6: The main Body Part of the REM message, when present, is the place where to put some explanatory/introduction text indicating the constitution of the message and / or elements to recognize the nature of the attachments (original message and / or ERDS evidence) and / or the description of eventual changes applied to some header of the submission metadata (see also Figure 3).

NOTE 7: The Header of the original message (originally called "submission metadata") changes his nature after it is picked up by REMS and becomes part of the "REMS relay metadata".

**Figure 2: Enveloping of REM dispatch in email stream example**

So the **original message** it is wrapped inside a "Body part" of a new digitally signed message used to protect the Sender's message up to the Recipient. Since the wrapping and the digital signature of the **original message** are realized by means of standard processes, the Recipients may access (and verify the REMS digital signature) of the Sender's message using normal email clients.

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

Like the previous example, the Figure 2 above represents the place where the REM dispatch is located inside the protocol stream.

Due to the peculiarity to have an auto-consistent REM message separated from "Transport/Closure Information" - parts of the communication stream - the entire set of REM definitions may work also with another type of transfer protocol.

NOTE 8: This separation ensures that REM messages are completely unrelated to underlying protocol stream.

In fact, the protocol involves only the "Transport Information" and "Closure Information" of the stream leaving the **REM message** unchanged, and using it as the new "*Payload*" of the entire REM service transaction. All the REM logic is defined inside the **REM message** object. How outlined in ETSI EN 319 532-4 [i.3] Clause 7, this makes REM, theoretically, independent from the particular transmission subsystem. Contemporarily, by means of this universal and standard enveloping modality, REM is recognizable by any standard email client of the initiator and/or the final users.

An important further distinction is that the transmission of information between the Sender's REMS and Recipient's REMS 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 another means (e.g. by a **ERD payload** or regular email message or through a link where download it in the case of S&N style of operation). Whereas, the interrelated evidence is sent apart to the Recipient, by a subsequent **REM message** containing the **ERDS evidence** attachment.

The final consideration that can be outlined in this section is that, for particular management purposes, the REM Service could add/modify some header field to the **submission metadata** during the enveloping process. Anyway, these changes should be limited to something that is proven as essential for the good working of the process and should be fully defined in the specific REM implementation.

NOTE 9: E.g. update of the Message-ID header if it not present or it needs to be normalized to a universal recognized identifier format, inside the context of the provided service. The original identifier, if specified, is assigned to some new X-Header of the submission metadata and to the X-REM-UAMessageIdentifier header of the REM message. A new regularized and **universal unique** Message-ID is assigned to the submission metadata.

Furthermore, any of the aforementioned changes, needed for the said purposes, shall be clearly indicated to the Sender and Recipient of the REM dispatch or the REM payload as outlined in the point 1) of the next section.

NOTE 10: The "REMS introduction MIME section" descriptive text (see Figure 3 of next section), for example, is one of the places where to put such indication. Alternatively, the contract with the users represents another place where to indicate this systematic practice.

## 4.3 REM message - Structure Implementation

This clause provides a specification for the structure of a **REM message** based on the MIME format (see IETF RFC 2045 [17]). A REM message does not exist as a self-standing object, since it always appear in the context of one of a REM dispatch, a REMS receipt, a REMS notification or a REM payload.

A REM message may flow between REMSP, and optionally from REMSPs to REM User Agents, as defined in ETSI EN 319 532-1 [15]. No specifications are provided in the present document on how the generic REM message should be tailored according to the specific mode of operation and interface it flows through.

A REM message is a structure for encapsulating ERDS evidence and/or **original message**. Moreover, it contains:

1) An (optional) introductory message-part displayed by the mail client application and in which the REMSP explains the purpose of the current message and gives some details on the other parts attached to it and, eventually, if some element of the **submission metadata** has been modified (see note 9 and note 10 in Clause 4.2). The actual message may also contain references to objects stored in a REMSP Repository.

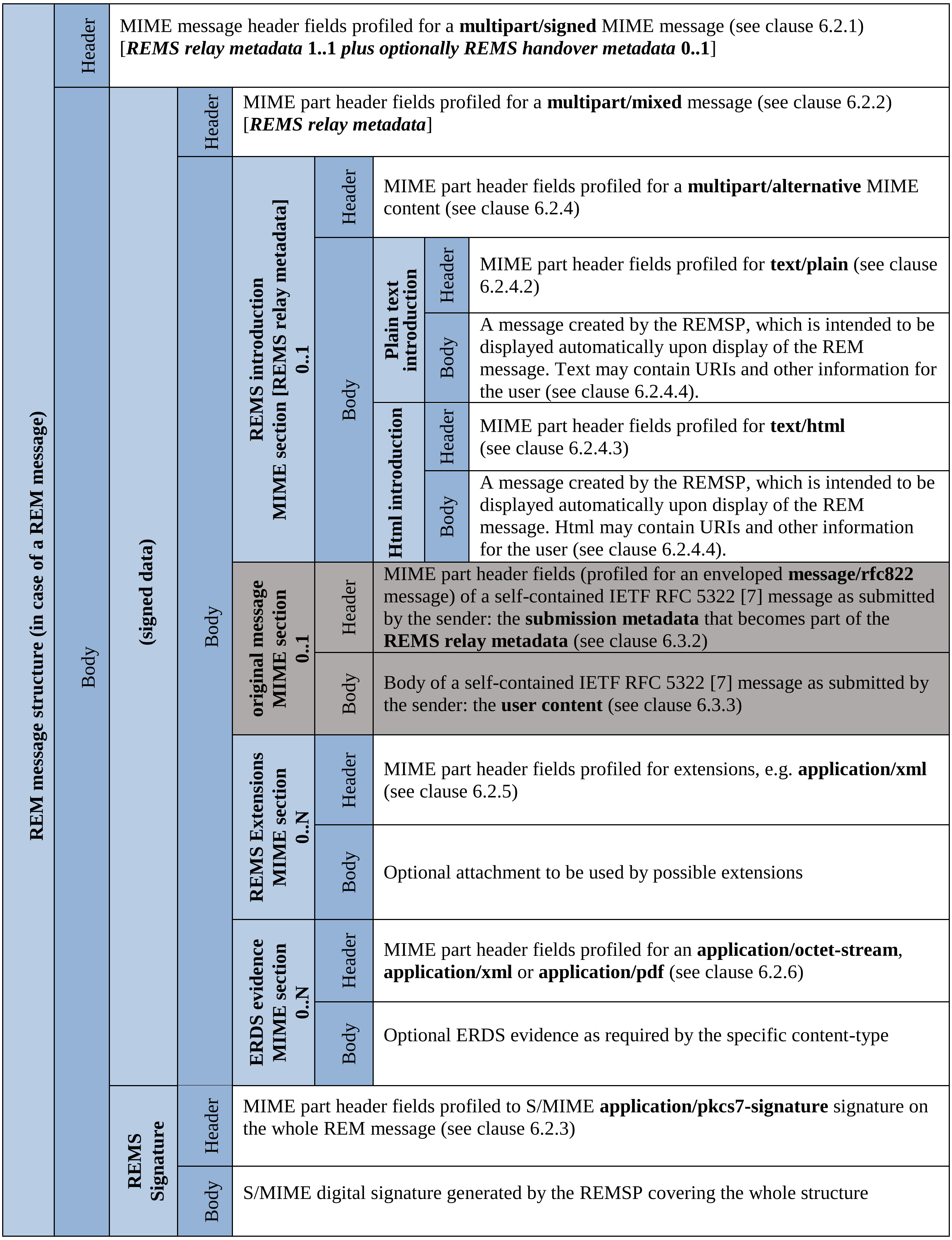
2) A mandatory digital signature applied by the REMSP (the signature covers both the **original message**, when present, and the ERDS evidence).

3) An (optional) REMS Extensions part that may be used to host an electronic time stamps certifying the accuracy of the date and time of the event (sending, receipt or eventual changes) related to the current message. Note that, when a current time stamp (it is typically a structured information, as an example in a XML file), or a generic current time reference is associated to a REM message, all the date/time values - relevant to the current time - present in REMS headers and/or ERDS evidence fields shall be aligned with the same exact value of the applied current time stamp (or current time reference). It is not admitted to have misaligned current time reference values among the significant time references (in any format, timezone etc. they are) present in each REM message

NOTE 1: The extension place-holder has a multiple cardinality. Time stamp is just an example to cover the regulation requirement. Other extensions with other purposes may be contemporarily present. This is one of the possibilities. Another one is to host the time stamp in the signature as indicate in Clause 8.3.

A REM message shall be structured with a Message Header containing the Header Fields followed by Message Body containing one or more Body Parts as defined in MIME (see IETF RFC 2045 [17]). The Message Body shall take the form of a multipart/mixed MIME structure in which every MIME-body-part contains one of the aforementioned elements (except the signature element). This multi-part/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 REMSP over the rest of the MIME parts that appear in the REM message.

This generic structure with all its elements is further depicted in Figure 3.



**REM message structure (in case of a REM message)**

Header

MIME message header fields profiled for a **multipart/signed** MIME message (see clause 6.2.1) [***REMS relay metadata* 1..1 *plus optionally REMS handover metadata* 0..1**]

Body

**(signed data)**

Header

MIME part header fields profiled for a **multipart/mixed** message (see clause 6.2.2) [***REMS relay metadata***]

Body

**REMS introduction MIME section [REMS relay metadata] 0..1**

Header

MIME part header fields profiled for a **multipart/alternative** MIME content (see clause 6.2.4)

Body

**Plain text introduction**

Header

MIME part header fields profiled for **text/plain** (see clause 6.2.4.2)

Body

A message created by the REMSP, which is intended to be displayed automatically upon display of the REM message. Text may contain URIs and other information for the user (see clause 6.2.4.4).

**Html introduction**

Header

MIME part header fields profiled for **text/html** (see clause 6.2.4.3)

Body

A message created by the REMSP, which is intended to be displayed automatically upon display of the REM message. Html may contain URIs and other information for the user (see clause 6.2.4.4).

**original message MIME section 0..1**

Header

MIME part header fields (profiled for an enveloped **message/rfc822** message) of a self-contained IETF RFC 5322 [7] message as submitted by the sender: the **submission metadata** that becomes part of the **REMS relay metadata** (see clause 6.3.2)

Body

Body of a self-contained IETF RFC 5322 [7] message as submitted by the sender: the **user content** (see clause 6.3.3)

**REMS Extensions MIME section 0..N**

Header

MIME part header fields profiled for extensions, e.g. **application/xml** (see clause 6.2.5)

Body

Optional attachment to be used by possible extensions

**ERDS evidence MIME section 0..N**

Header

MIME part header fields profiled for an **application/octet-stream**, **application/xml** or **application/pdf** (see clause 6.2.6)

Body

Optional ERDS evidence as required by the specific content-type

**REMS Signature**

Header

MIME part header fields profiled to S/MIME **application/pkcs7-signature** signature on the whole REM message (see clause 6.2.3)

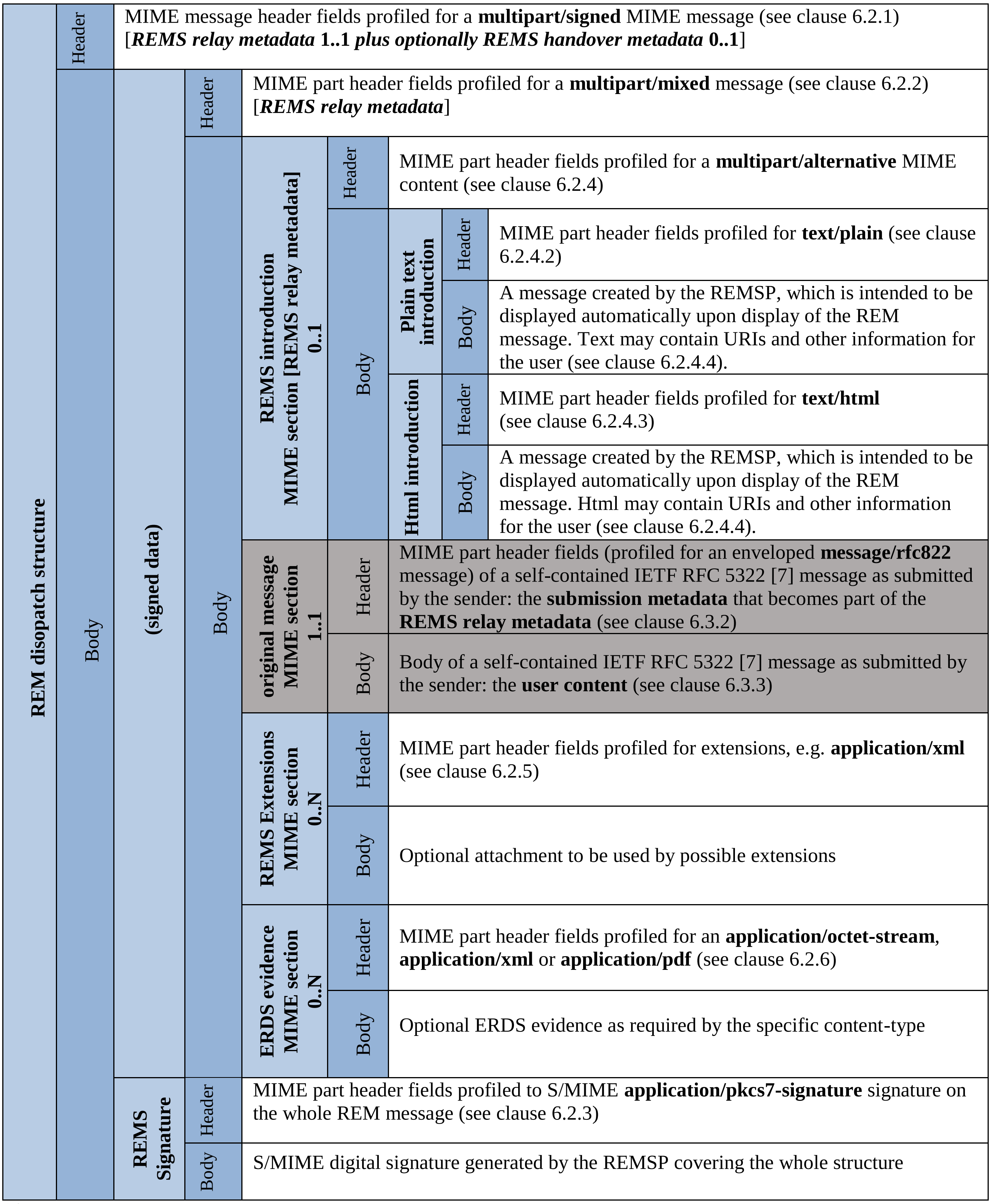
Body

S/MIME digital signature generated by the REMSP covering the whole structure

**Figure 3: REM message generic template**

Figure 3 - without the grey part - presents the full skeleton of a generic REM message. When it includes the grey part (the **original message** MIME section) it represents the structure of a REM dispatch or a REM payload.

The following figures shall present the full definition and profiling of the REM message. They are built starting from the ERD message affine structure, defined in Table 1 of  ETSI EN 319 522-2 [13] Clause 4, with the emphasis of REM specific aspects and peculiarities.



MIME message header fields profiled for a **multipart/signed** MIME message (see clause 6.2.1) [***REMS relay metadata* 1..1 *plus optionally REMS handover metadata* 0..1**]

MIME part header fields profiled for a **multipart/mixed** message (see clause 6.2.2) [***REMS relay metadata***]

MIME part header fields profiled for a **multipart/alternative** MIME content (see clause 6.2.4)

MIME part header fields profiled for **text/plain** (see clause 6.2.4.2)

A message created by the REMSP, which is intended to be displayed automatically upon display of the REM message. Text may contain URIs and other information for the user (see clause 6.2.4.4).

MIME part header fields profiled for **text/html** (see clause 6.2.4.3)

A message created by the REMSP, which is intended to be displayed automatically upon display of the REM message. Html may contain URIs and other information for the user (see clause 6.2.4.4).

MIME part header fields (profiled for an enveloped **message/rfc822** message) of a self-contained IETF RFC 5322 [7] message as submitted by the sender: the **submission metadata** that becomes part of the **REMS relay metadata** (see clause 6.3.2)

Body of a self-contained IETF RFC 5322 [7] message as submitted by the sender: the **user content** (see clause 6.3.3)

MIME part header fields profiled for extensions, e.g. **application/xml** (see clause 6.2.5)

Optional attachment to be used by possible extensions

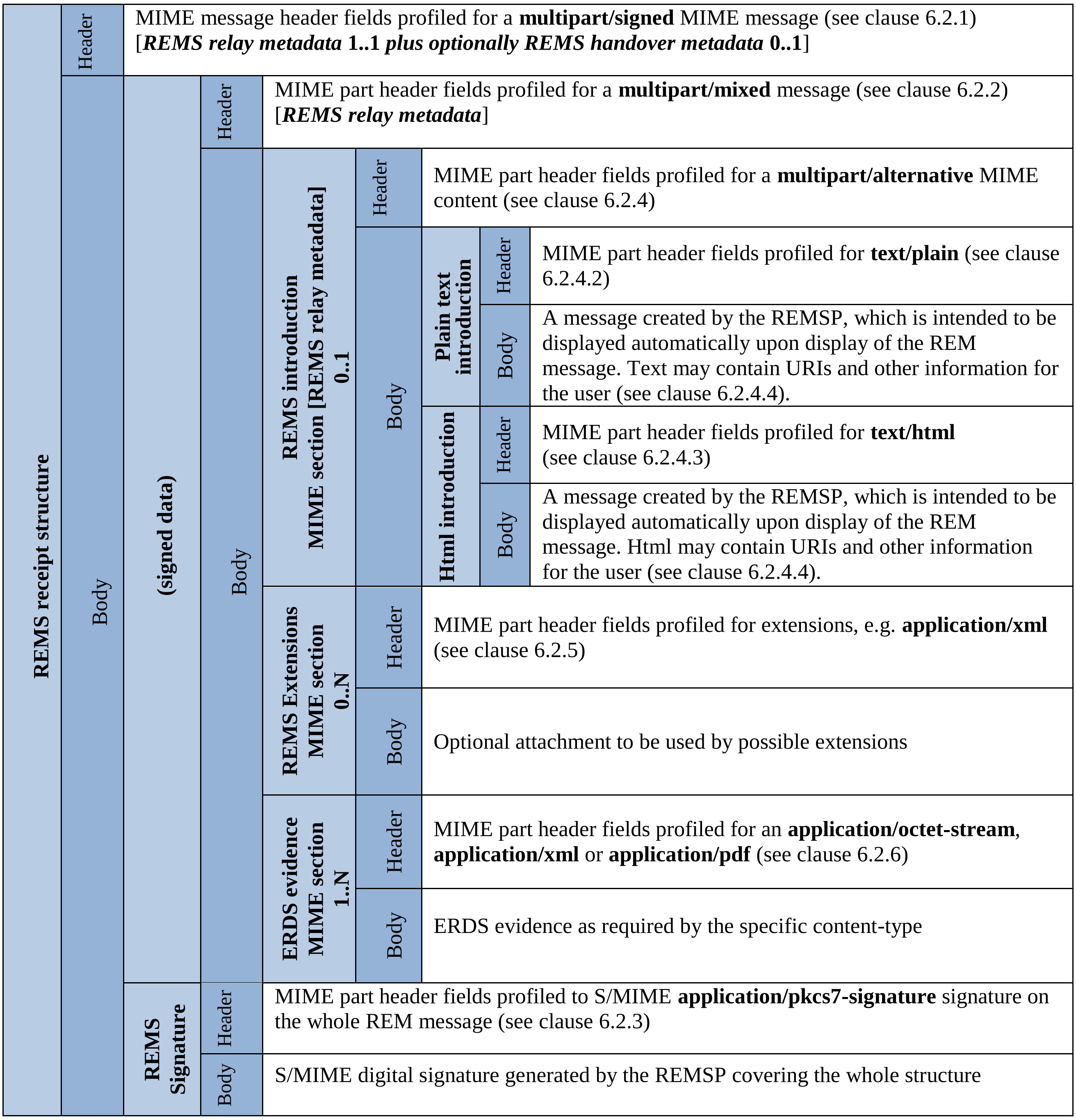
MIME part header fields profiled for an **application/octet-stream**, **application/xml** or **application/pdf** (see clause 6.2.6)

Optional ERDS evidence as required by the specific content-type

MIME part header fields profiled to S/MIME **application/pkcs7-signature** signature on the whole REM message (see clause 6.2.3)

S/MIME digital signature generated by the REMSP covering the whole structure

**Figure 4: REM dispatch structure**

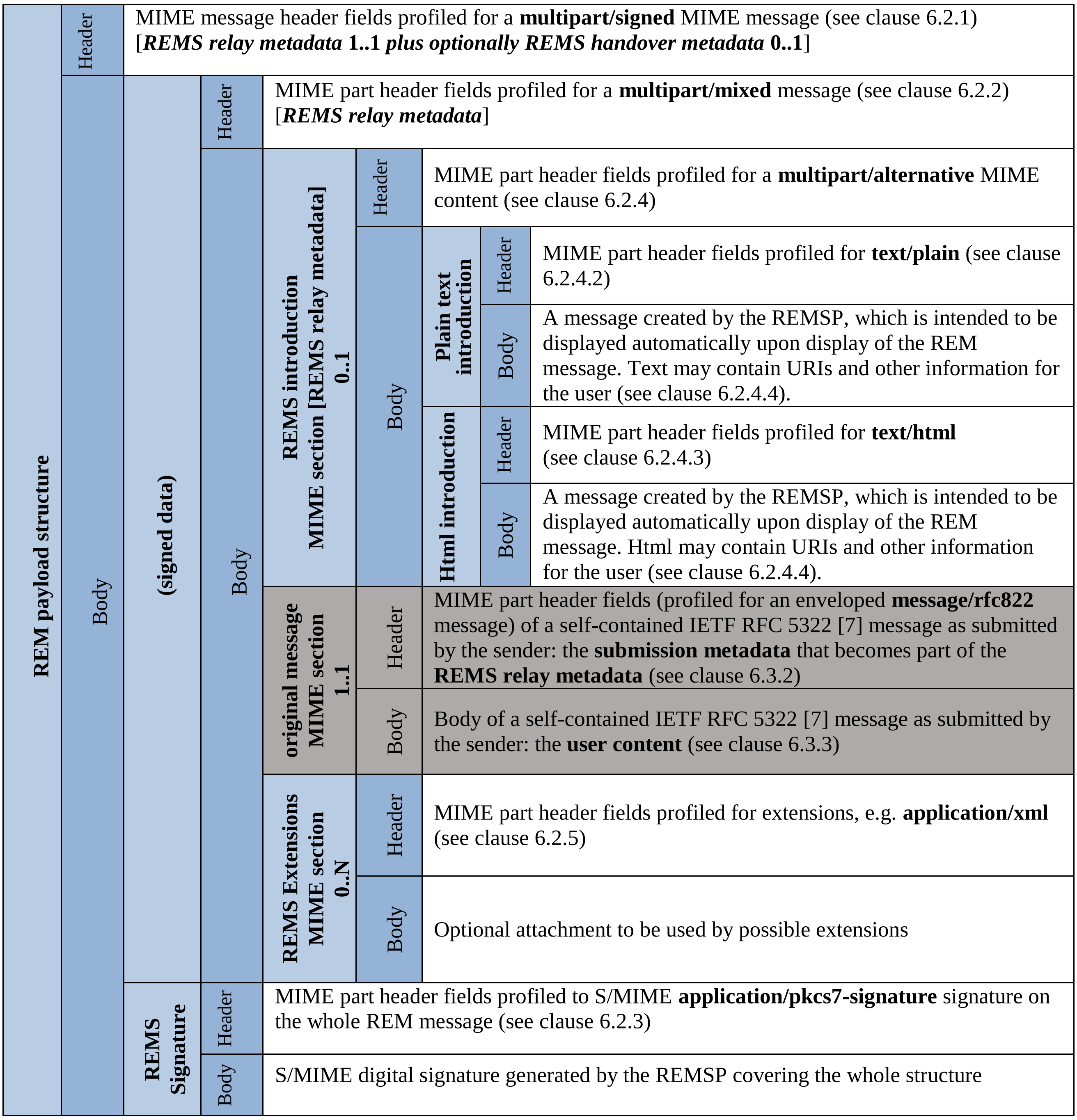


| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **REMS receipt structure** | Header | | | | | | | MIME message header fields profiled for a **multipart/signed** MIME message (see clause 6.2.1)<br>[***REMS relay metadata* 1..1 *plus optionally REMS handover metadata* 0..1**] |
| | Body | **(signed data)** | Header | | | | | MIME part header fields profiled for a **multipart/mixed** message (see clause 6.2.2)<br>[***REMS relay metadata***] |
| | | | Body | **REMS introduction MIME section [REMS relay metadata] 0..1** | Header | | | MIME part header fields profiled for a **multipart/alternative** MIME content (see clause 6.2.4) |
| | | | | | Body | **Plain text introduction** | Header | MIME part header fields profiled for **text/plain** (see clause 6.2.4.2) |
| | | | | | | | Body | A message created by the REMSP, which is intended to be displayed automatically upon display of the REM message. Text may contain URIs and other information for the user (see clause 6.2.4.4). |
| | | | | | | **Html introduction** | Header | MIME part header fields profiled for **text/html**<br>(see clause 6.2.4.3) |
| | | | | | | | Body | A message created by the REMSP, which is intended to be displayed automatically upon display of the REM message. Html may contain URIs and other information for the user (see clause 6.2.4.4). |
| | | | | **REMS Extensions MIME section 0..N** | Header | | | MIME part header fields profiled for extensions, e.g. **application/xml** (see clause 6.2.5) |
| | | | | | Body | | | Optional attachment to be used by possible extensions |
| | | | | **ERDS evidence MIME section 1..N** | Header | | | MIME part header fields profiled for an **application/octet-stream**, **application/xml** or **application/pdf** (see clause 6.2.6) |
| | | | | | Body | | | ERDS evidence as required by the specific content-type |
| | | **REMS Signature** | Header | | | | | MIME part header fields profiled to S/MIME **application/pkcs7-signature** signature on the whole REM message (see clause 6.2.3) |
| | | | Body | | | | | S/MIME digital signature generated by the REMSP covering the whole structure |

**Figure 5: REMS receipt structure**

<table>
<tr><td rowspan="13">**REMS notification structure**</td><td>Header</td><td colspan="7">MIME message header fields profiled for a **multipart/signed** MIME message (see clause 6.2.1)<br>[***REMS relay metadata* 1..1 *plus optionally REMS handover metadata* 0..1**]</td></tr>
<tr><td rowspan="12">Body</td><td rowspan="10">**(signed data)**</td><td>Header</td><td colspan="5">MIME part header fields profiled for a **multipart/mixed** message (see clause 6.2.2)<br>[***REMS relay metadata***]</td></tr>
<tr><td rowspan="9">Body</td><td rowspan="5">**REMS introduction MIME section [REMS relay metadata] 0..1**</td><td>Header</td><td colspan="3">MIME part header fields profiled for a **multipart/alternative** MIME content (see clause 6.2.4)</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 6.2.4.2)</td></tr>
<tr><td>Body</td><td>A message created by the REMSP, which is intended to be displayed automatically upon display of the REM message. Text may contain URIs and other information for the user (see clause 6.2.4.4).</td></tr>
<tr><td rowspan="2">**Html introduction**</td><td>Header</td><td>MIME part header fields profiled for **text/html**<br>(see clause 6.2.4.3)</td></tr>
<tr><td>Body</td><td>A message created by the REMSP, which is intended to be displayed automatically upon display of the REM message. Html may contain URIs and other information for the user (see clause 6.2.4.4).</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">Optional attachment to be used by possible extensions</td></tr>
<tr><td rowspan="2">**ERDS evidence MIME section 0..N**</td><td>Header</td><td colspan="3">MIME part header fields profiled for an **application/octet-stream**, **application/xml** or **application/pdf** (see clause 6.2.6)</td></tr>
<tr><td>Body</td><td colspan="3">Optional 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 6.2.3)</td></tr>
<tr><td>Body</td><td colspan="5">S/MIME digital signature generated by the REMSP covering the whole structure</td></tr>
</table>

**Figure 6: REMS notification structure**



- **REM payload structure**
  - Header: MIME message header fields profiled for a **multipart/signed** MIME message (see clause 6.2.1) [***REMS relay metadata* 1..1 *plus optionally REMS handover metadata* 0..1**]
  - Body
    - **(signed data)**
      - Header: MIME part header fields profiled for a **multipart/mixed** message (see clause 6.2.2) [***REMS relay metadata***]
      - Body
        - **REMS introduction MIME section [REMS relay metadata] 0..1**
          - Header: MIME part header fields profiled for a **multipart/alternative** MIME content (see clause 6.2.4)
          - Body
            - **Plain text introduction**
              - Header: MIME part header fields profiled for **text/plain** (see clause 6.2.4.2)
              - Body: A message created by the REMSP, which is intended to be displayed automatically upon display of the REM message. Text may contain URIs and other information for the user (see clause 6.2.4.4).
            - **Html introduction**
              - Header: MIME part header fields profiled for **text/html** (see clause 6.2.4.3)
              - Body: A message created by the REMSP, which is intended to be displayed automatically upon display of the REM message. Html may contain URIs and other information for the user (see clause 6.2.4.4).
        - **original message MIME section 1..1**
          - Header: MIME part header fields (profiled for an enveloped **message/rfc822** message) of a self-contained IETF RFC 5322 [7] message as submitted by the sender: the **submission metadata** that becomes part of the **REMS relay metadata** (see clause 6.3.2)
          - Body: Body of a self-contained IETF RFC 5322 [7] message as submitted by the sender: the **user content** (see clause 6.3.3)
        - **REMS Extensions MIME section 0..N**
          - Header: MIME part header fields profiled for extensions, e.g. **application/xml** (see clause 6.2.5)
          - Body: Optional attachment to be used by possible extensions
    - **REMS Signature**
      - Header: MIME part header fields profiled to S/MIME **application/pkcs7-signature** signature on the whole REM message (see clause 6.2.3)
      - Body: S/MIME digital signature generated by the REMSP covering the whole structure

**Figure 7: REM payload structure**

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..1 shall occur exactly once.

The following clauses aim at further profiling/constraining each header of this generic message structure. The present document does not impose any constraint on those header fields not listed in the tables below [6.2].

NOTE 2: Jointly with the previous structures, see also Table 1 of  ETSI EN 319 522-2 [13] Clause 4 and Table 1 of ETSI EN 319 532-2 [16] Clause 4.1.

# 5 REMS - identification formats

The present section of the document aims to provide details about REMS identification formats. For this purpose the content and relevant specifications defined in ETSI EN 319 522-2 [13] Clause 5, the identity components defined in Table 6 of ETSI EN 319 522-2 [13] Clause 8.1 and the formats defined in ETSI EN 319 522-3 [14] Clause 5 shall apply.

# 6 REMS - relay metadata formats

## 6.1 Introduction

The present section intends to detail the REMS relay metadata formats. For this purpose the content and relevant components defined in ETSI EN 319 522-2 [13] Clauses 6.1, 6.2 shall apply.

The composition of the REM message headers is derived starting from the template structure of Figure 3.

Furthermore, the next table contains a mapping between the general semantic content of ERDS and the same concepts applied to REM headers.

| **Semantic content (from ETSI EN 319 522-2** [13]**)** | **Mapping to IETF RFC 5322 [7] header elements** |
|---|---|
| Metadata version | X-REM-MetadataVersion header field (see  Clause 6.2.1). This value shall be compliant with the correspondent format defined in ETSI EN 319 522-2 [13] Clause 6.2.1 - MD01 |
| Relay date and time | X-REM-RelayDate header field (see  Clause 6.2.1). The format of this optional value shall be compliant with the correspondent format defined in ETSI EN 319 522-2 [13] Clause 6.2.2 - MD02 and with clause 3.3 of IETF RFC 5322 [7]. |
| Expiry date and time | X-REM-ExpirationDate header field (see  Clause 6.2.1). The format of this optional value shall be compliant with with the correspondent format defined in ETSI EN 319 522-2 [13] Clause 6.2.3 - MD03and clause 3.3 of IETF RFC 5322 [7]. |
| Recipient required authentication level | X-REM-RecipientAuthenticationLevel header field (see  Clause 6.2.1). This optional value shall be compliant with the correspondent format defined in ETSI EN 319 522-2 [13] Clause 6.2.4 - MD04. |
| Applicable policy | X-REM-ApplicablePolicy header field (see  Clause 6.2.1). This optional value shall be compliant with the correspondent format defined in ETSI EN 319 522-2 [13] Clause 6.2.5 – MD05. |
| Mode of consignment | X-REM-ModeOfConsignment header field (see  Clause 6.2.1). This optional value shall be compliant with the correspondent format defined in ETSI EN 319 522-2 [13] Clause 6.2.6 – MD06. |
| Scheduled delivery | X-REM-ScheduledDelivery header field (see  Clause 6.2.1). The format of this optional value shall be compliant with the correspondent format defined in ETSI EN 319 522-2 [13] Clause 6.2.7 - MD07 and with clause 3.3 of IETF RFC 5322 [7]. |
| Sender’s identifier | X-REM-SenderIdentityData header field (see  Clause 6.2.1). This optional value shall be compliant with the correspondent format defined in ETSI EN 319 522-2 [13] Clause 6.2.8 - MD08 |

| | |
|---|---|
| Sender’s replyto address | ”Reply-To” header field (see  Clause 6.2.1 below). This value shall be compliant with the correspondent format defined in ETSI EN 319 522-2 [13] Clause 6.2.9 - MD09 |
| Recipient’s identifier | X-REM-RecipientIdentityData header field (see  Clause 6.2.1). This optional value shall be compliant with the correspondent format defined in ETSI EN 319 522-2 [13] Clause 6.2.10 – MD10. |
| ERD Message identifier | ”Message-ID” header field (see  Clause 6.2.1 below). This value shall be compliant with the correspondent format defined in ETSI EN 319 522-2 [13] Clause 6.2.11 - MD011 |
| In reply to | X-REM-InReplyTo header field (see  Clause 6.2.1). This optional value shall be compliant with the correspondent format defined in ETSI EN 319 522-2 [13] Clause 6.2.12 – MD12 |
| User content information: Content type | ”Content-Type” header field (see  Clause 6.2.1 below). |
| User content information: Subject | ”Subject” header field (see  Clause 6.2.1 below). |
| ERD Message type | X-REM-MessageType header field (see  Clause 6.2.1). This optional value shall be compliant with the correspondent format defined in ETSI EN 319 522-2 [13] Clause 6.2.13 – MD13 |
| User content information:Message digest | X-REM-hashValue header field (see  Clause 6.2.1). This optional value shall be compliant with the correspondent format defined in ETSI EN 319 522-2 [13] Clause 6.2. |
| User content information:Message original identifier | X-REM-UAMessageIdentifier header field (see  Clause 6.2.1). This optional value shall be compliant with the correspondent format defined in ETSI EN 319 522-2 [13] Clause 6.2. |
| User content information: AttachmentInformation | X-REM-AttachmentInformation header field (see  Clause 6.2.1). This optional value shall be compliant with the correspondent format defined in ETSI EN 319 522-2 [13] Clause 6.2. Furthermore, it is related to attachment information natively contained in the MIME headers. |
| Signature | See headers in Clause 6.2.3 |
| Extensions | Other metadata may be specified with the mechanism defined in the Clause 6.2.1. This optional value shall be compliant with the correspondent format defined in ETSI EN 319 522-2 [13] Clause 6.2.15 - MD015 |

# 6.2 REMS - whole Headers formats

## 6.2.1 REM message - Headers formats

| | |
|---|---|
| Content-Type | The value for this header shall be "multipart/signed".<br>The 'protocol' parameter value shall be "application/pkcs7-signature".<br>The 'micalg' parameter value should be conformant to TS 119 312 [i.7].<br>The ‘boundary’ parameter value should be conformant to IETF RFC 2046 [18] |
| MIME-Version | The value for this header shall be "1.0". |
| Message-ID | The value for this header should be an UID as defined in IETF RFC 5322 [7]. |
| Date | The value for this header shall be compliant with clause 3.3 of IETF RFC 5322 [7]. |
| From | The value for this header should be either a REMSP service address (e.g. "<service_rem_md_x@rem_md_x.com>" or a transformation of the original From field to show the role of the REMSP (e.g. "on behalf of user@rem_md_x.com <service_rem_md_x@rem_md_x.com>"). |
| To | The value for this header shall be compliant with clause 3.6.3 of IETF RFC 5322 [7]. In the case of a REM dispatch the value for this header shall match the value of the 'To' header field in the **original message**. In the case of a REM message carrying evidence for the Sender, the value for this header may match the value of the 'From' header field in the **original message**. |
| Cc | The value for this optional header shall be compliant with clause 3.6.3 of IETF RFC 5322 [7]. REMS should assign a value to this header only in case of REM dispatch and, in such case, the value shall match the value of the 'Cc' header field in the **original message**. |
| Subject | The value for this header should be transformed starting from the Subject header field contained in the original sender's message, in order to indicate the role that the REM message has within the flow. (E.g.: "REM dispatch: subject_of_original_message" if the message is an envelope for the original sender's message, "REM Delivery Receipt: subject_of_original_message" if the REM message is a delivery receipt). |
| Reply-To | The value for this header shall be compliant with clause 3.6.3 of IETF RFC 5322 [7]. In the case of a REM dispatch the value for this header shall match the value of the ‘From' header field in the **original message**. In the case of a REM message carrying evidence for the Sender, this header field should not appear, and if it appears, its value should be the REMS service address. |

The header of each REM message may inherit also other header fields (e.g. return-path, received, etc) from the **original message** that are relevant for a particular profile or a peer-to-peer agreement. Furthermore, the header of each REM message may contain optional Extension Header Fields. The purpose of these headers is to give immediate access to important identification information, which is so already present in either the ERDS evidence or REM message, instead of forcing recipient REMSPs to go through the ERDS evidence.

NOTE 1: To be more accurate, here, REMSP is intended as the software implementing the REM services.

The syntax of these optional parameters is according to the following specification:

```
X-REM-Msg-Type: <value>
```

where <value> shall be:

- "Dispatch" for a REM dispatch (i.e. the **original message** by the sender is included)
- "Receipt" for a REMS receipt
- "Notification" for a REMS notification
- "Payload" for a REM payload

```
X-REM-<component>: <value>
```

where:

- <component> is a label (possibly related to the identification code of a ERDS relay metadata Component or subcomponent or a ERDS evidence Component or subcomponent - see clause 7.2 for a full list of these components and their codes - e.g. G01, G02, etc).

NOTE 2: - See Table 3 in ETSI EN 319 522-2 [13] Clauses 6.1 for a full list of identification codes  of ERDS relay metadata components - e.g. MD01, MD02, etc.
- See Table 6 in ETSI EN 319 522-2 [13] Clauses 7.1 for a full list of identification codes of ERDS evidence components - e.g. G01, R01, I01, etc.

- <value> is a correspondent value for the component.

As an example, with the aforementioned mechanism, the following headers field may be introduced:

| | |
|---|---|
| X-REM-G02: | <Evidence identifier value> |
| X-REM-R01: | <Evidence issuer policy identifier> |

The following specific headers field may be also introduced:

| | |
|---|---|
| X-REM-hashAlgorithm: | <algorithm used in hash computation> |
| X-REM-hashValue: | <sender's Message Hash> |
| X-REM-UAMessageIdentifier: | < identifier of the **original message** submitted by the UA> |

In case the <value> to assign to any aforementioned headers is in a structured or non-textual format, a base64 encoding should be used to correctly represent it, in a unique header, according to the IETF RFC 2046 [18] specification.

## 6.2.2 REM message - signed data Headers formats

| | |
|---|---|
| Content-Type | This header shall be present and the value for it shall be: "multipart/mixed" |

## 6.2.3 REMS - signature Headers formats

The fields defined in the following table and their respective values shall adhere to the sections 3.2.1 and 3.4.3 of RFC 5751 [6].

| | |
|---|---|
| Content-Type | This header shall be present and the value for it shall be: "application/pkcs7-signature; name=smime.p7s".<br>The parameter 'name' should be present and its value should be "smime.p7s". |
| Content-Transfer-Encoding | This header should be present. The value for this header shall be: "base64". |
| Content-Disposition | This header shall be present and the value for it shall be: "attachment".<br>The value of the 'filename' parameter should be "smime.p7s". |
| Content-Description | The value for this header may be: "S/MIME Cryptographic Signature". |

Even if sender REMSPs have to include the field Content-Disposition and fill in the name/filename parameters, recipient REMSPs shall be able to correctly interpret incoming messages without Content-Disposition and/or name/filename parameters.

NOTE: To be more accurate, here, REMSP is intended as the software implementing the REM services.

## 6.2.4 REMS - introduction Headers-Body formats

### 6.2.4.1 Introduction

This optional MIME part shall be structured as follows and in the next inner sub-parts:

| | |
|---|---|
| Content-Type | The value for this field shall be: "**multipart/alternative**" |
| X-REM-Section-Type | The value of this optional field should be "rem_message/introduction" |

NOTE: The order chosen for the following two parts (body of the “multipart/alternative” header defined in the previous section - and so mutually substitutable) ends with the choice that the email clients usually interpret as preferred, as indicated in IETF RFC 2046 [18] (the best choice is the LAST part of a type supported by the recipient system's local environment).

#### 6.2.4.2 multipart/alternative: free text subsection Headers formats

| | |
|---|---|
| Content-Type | The value for this field shall be: "text/plain".<br>The value of the 'charset' parameter should be "UTF-8". |
| Content-Disposition | The value of this header shall be "inline" as it is intended to be displayed automatically upon display of the message in mail client. |
| Content-Transfer-Encoding | The value for this field should be: 7bit, 8bit or quoted-printable. |

#### 6.2.4.3 multipart/alternative: HTML subsection Headers formats

| | |
|---|---|
| Content-Type | The value for this field shall be: "text/html;".<br>The value of the 'charset' parameter should be "UTF-8". |
| Content-Transfer-Encoding | The value for this field should be: 7bit, 8bit or quoted-printable. |

#### 6.2.4.4 Introduction body formats

The optional “introduction text” for the REM message is positioned in two different places represented by the body parts of the two previous clauses 6.2.4.2 for plain-text and 6.2.4.3 for HTML. Its informational content shall be equivalent in both formats plain text and HTML and the HTML shall not contain active code.

If the present part contains some URL, it shall be indicated explicitly in the visible text. The printed part (that is the Hypertext visible to the user) shall be the same as the hidden part (that is the real location where the web browser is redirected clicking on it).

NOTE: As indicated in the note 10 in Clause 4.2 at page 15, the introduction text represents one of the places where to indicate to the users of the REM service any eventual and necessary rectification applied to some header of submission metadata by the REMS.

### 6.2.5 REMS - extensions MIME section Headers formats

This optional MIME part shall be structured as follows:

| | |
|---|---|
| Content-Type | The value for this header should be "application/xml".<br>The value of the ‘name' parameter should be "<REM_EXTENTION_NAME>.xml".<br>The value of the ‘charset' parameter should be "UTF-8". |
| Content-Transfer-Encoding | The value of this header shall be "quoted-printable" or "base64" or "binary". |
| Content-Disposition | The value of this header shall be "attachment".<br>The value of the ‘filename' parameter shall match the value of the ‘name' parameter of the Content-Type header. |
| X-REM-Section-Type | The value of this optional field should be "rem_message/extension". |
| X-REM-Extension-Code | The value of this optional field is not defined here. It should be in accordance with the type of the attachment, in order to allow for automatic processing. |

The structures and or the names or type-extensions of these optional attachments are not defined here, since they are left for any possible extensions to be agreed on a peer-to-peer basis (e.g. automatic processing of download URI in S&N style of operation, insertion of Electronic PostMark, etc.) or to cover particular requirements coming in the future.

In particular, one of these extensions may be used to associate an electronic time stamp (see note 1 in Clause 4.3 at page 15) to the REM message certifying the date and time of sending, receiving and/or any change/transformation of the message transmitted from the sender to the recipient.

In case one extension is used to transport information relevant to the “time” to which the event (Message or Evidence) is referring, all the time references present in REM message (e.g. G05 - Event Time defined in Table 6 of ETSI EN 319 522-2 [13] Clauses 8.1) shall report a unique and aligned time value to that provided by the **electronic time stamp**.

This unique value shall be the official certified time reference related to the event (e.g. the precise date/time of taking in charge/transferring the responsibility about a digital communication).

NOTE: The Event Time above is intended as a UTC date and time.

## 6.2.6 ERDS evidence - MIME section Headers formats

### 6.2.6.1 Introduction

The present section defines the specific headers provided for the ERDS evidence contained inside a REM message (see Clause 7 for the whole Evidence set and from Figure 3 to Figure 6 for the applications of the ERDS evidence inside a REM message). The header set shall be structured as follows.

According to the interoperability profiles, **XML** is the preferred format to choose for the Evidence attachment.

NOTE 1: Making that choice, it facilitates the interoperability in open or between heterogeneous services interactions.

**PDF** Evidence format, although valid, it is thought more for final human usage rather than in situations where interoperability has to be addressed or automatic processes have to take some decision based on Evidence content. XML format is better suited for these last cases, where the automatic processing of the evidence content prevails over its immediate human interpretation. For the aforementioned reasons, the detailed specification of PDF evidence format is out of scope of the present specification and it is left to specific implementations of REMS.

The tag < REM_EVIDENCE_NAME> present in the next two tables should be instantiated, time to time, with the name of the evidence to which it relates. These names, should assume the value of G02 code (see note 2 below) according to the event (see note 3 below) to which the evidence is referring (e.g. SubmissionAcceptance.xml, SubmissionRejection.xml, etc.).

NOTE 2: See the definition of G02 - Event identifier code in ETSI EN 319 522-2 [13] Clause 7.2.2.

NOTE 3: See the full list of the ERDS event in ETSI EN 319 522-1 [12] Table 1.

According to the structure of Figure 3, more than one evidence is allowed be attached to each REM message. **These (optional) additional Evidence attachments** (eventually different - in terms of semantic/content/name - from all the Evidence set provided with the present technical specification) obey to peer-to-peer and/or interoperability agreements and/or specific profiles. In any case, these eventual additional evidence attachments should be specified, in the MIME header structure, according with their type, in a similar way of that defined for XML and PDF below.

### 6.2.6.2 XML format

| | |
|---|---|
| Content-Type | The value for this header shall be "application/xml"<br>The value of the 'name' parameter shall be "<REM_EVIDENCE_NAME>.xml"<br>The value of the 'charset' parameter shall be "UTF-8" |
| Content-Transfer-Encoding | The value of this header shall be "quoted-printable" |
| Content-Disposition | The value of this header shall be "attachment"<br>The value of the 'filename' parameter shall match the value of the 'name' parameter of the Content-Type header |
| X-REM-Section-Type | The value of this optional field should be "rem_message/xml_evidence". |

### 6.2.6.3 PDF format

| | |
|---|---|
| Content-Type | The value for this header shall be "application/pdf"<br>The value of the 'name' parameter shall be "<REM EVIDENCE_NAME>.pdf" |
| Content-Transfer-Encoding | The value of this header shall be "base64" or "binary" |
| Content-Disposition | The value of this header shall be "attachment"<br>The value of the 'filename' parameter shall match the value of the 'name' parameter of the Content-Type header |
| X-REM-Section-Type | The value of this optional field should be "rem_message/pdf_evidence". |

## 6.3 REMS - user content formats

### 6.3.1 Introduction

This section contains the MIME headers definitions and formats for the **original message** packaging and makes only sense when the message has to be conveyed to the Recipient by value (in the Store & Forward Style of operations).

The whole MIME for the **original message** (see Figure 3, Figure 4 and Figure 7 for the applications inside a REM message) shall be structured as follows.

### 6.3.2 original message - MIME section Headers formats

| | |
|---|---|
| Content-Type | The value for this field shall be: "message/rfc822".<br>The 'name' parameter value shall be "AttachedMimeMessage". |
| Content-Transfer-Encoding: | The value of this header shall be "binary" |
| Content-Disposition | The value for this field shall be: "attachment".<br>The value of the ‘filename' parameter shall match the value of the ‘name' parameter of the Content-Type header. |
| X-REM-Section-Type | The value of this optional field should be "rem_message/original". |

NOTE: These header fields are parts of the submission metadata that converge inside the REMS relay metadata.

### 6.3.3 original message - MIME section Body formats

It contains the “**user content**” (that represents the “payload”) as the Sender submits it.

NOTE 1: From the formal viewpoint, the user content is part of the original message but is not part of the REMS relay metadata (object of the current section of the present document). Anyway, it is introduced here to define the place where it appears inside the entire morphology and to maintain the coherence with MIME structure description.

Some change is admitted on the submission metadata part (Header of the **original message**), but only if it is limited to what is effectively necessary for the good working of the REM exchange of information (e.g. the MessageID as also previously mentioned, see notes 9 and 10 in Clause 4.2 at page 15). Furthermore, any necessary change shall be clearly pointed out to the Sender (e.g in the Evidence) and to the Recipient (e.g in the Evidence and/or in the introduction message defined in 6.2.4.4).

NOTE 2: The order, inside the MIME structure of the REM Message - where this and also the other header fields of clauses 6.2.x, appear - is not necessarily that identified in the present description (in fact this description is ordered to maintain a logical coherence with the other parts of the entire technical specification).

# 7 REMS - evidence set and components formats

## 7.1 ERDS evidence set overview

The present section aims to provide the components and the format details of the ERDS evidence set relevant for REM. For this purpose the ERDS events listed in the Table 1 of ETSI EN 319 522-1 [12] and the application to REM detailed in ETSI EN 319 532-1 [15] Clause 6 shall apply.

For the same purpose, also the general semantic defined in ETSI EN 319 522-2 [13] Clause 7 shall apply.

## 7.2 ERDS evidence components

Specifications on evidence content and relevant components defined in ETSI EN 319 522-2 [13] Clauses 7.1, 7.2, 7.3 shall apply.

## 7.3 ERDS evidence set structure

Specification for the structure of ERDS evidence set provided in Table 13 of ETSI EN 319 522-2 [13] Clause 7.4 - Requirements for components of evidence shall apply. Such definitions have to be mapped from the ERDS general context to REMS according to the content of the previous clauses.

## 7.4 ERDS evidence XML formats

The present section intends to provide the XML format details about the ERDS evidence set relevant to REM. For this purpose the definitions present in ETSI EN 319 522-3 [14] Clause 5 shall apply.

Furthermore, other mappings or adaptations are admitted or could be provided in next version of the present document or in other documents as agreements among interested parties.

# 8 REMS - signatures formats

## 8.1 Introduction

The present section intends to provide the format details about the signatures involved in the REM messages. For this purpose the general definitions present in ETSI EN 319 522-2 [13] Clause 7 shall apply.

The algorithms and key lengths used to generate digital signatures should be as specified in ETSI TS 119 312 [i.7].

Within a REM message the following digital signatures are applied:

- Signatures generated by a REMSP or by the delegated entity on each ERDS evidence individually.
- S/MIME signature protecting all the MIME parts that constitute a REM message. This signature is generated by a REMSP.

NOTE: Senders may additionally sign the **original message** submitted to the recipient, supporting the signature with own certificates. These signatures are outside of the scope of the present document.

All the above signatures may coexists, each securing one part of the REM message.

Next sub clauses specify the details relevant to formats of the signatures that apply on the different parts composing a REM message.

## 8.2 Signatures individually signing REMS Evidences

For this type of signatures requirements specified in ETSI EN 319 522-2 [13] Clause 7.2 and ETSI EN 319 522-3 [14] Clause 5.2.2.26 shall apply.

In addition, in case PDF evidence format is used, it is recommended that it is protected by PAdES digital signatures as defined in EN 319 142-1 [8].

## 8.3 Signatures on REM messages

For signatures that sign all the components of REM messages the general requirements specified in ETSI EN 319 522-2 [13] Clause 7.2 for this type of signatures shall apply.

In addition, the following requirements shall apply:

1) The signature shall be applied to the message using S/MIME multipart/signed as defined in RFC 5751 [6]. 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 [13] clause 8.2.9.

NOTE: 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 EN 319 122-1 [1].

3) This digital signature should be a CAdES baseline signature as specified in ETSI EN 319 122-1 [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.
Once the CAdES-B-B baseline signature has been generated, it should be augmented to a CAdES-B-T baseline signature by incorporation into the digital signature of the unsigned attribute `signature-time-stamptamp`, containing a time-stamp token computed as specified in ETSI EN 319 122-1.
The signing certificate of this digital signature shall meet the requirements specified in in ETSI EN 319 522-2 [13] clause 9.3.

# 9 Common Service Interface formats

The present section of the document aims to provide formats about the Common Service Interface (CSI) procedures. These include techniques to resolve the identification of recipients, collect metadata for capabilities of the recipient REMS, identification and routing information of the recipient REMS, provide metadata capabilities of sender REMS, evaluate trust among interoperable REMS. For this purpose all or parts of the concepts defined in ETSI EN 319 522-2 [13] Clause 9 - Common Services Interface Content, and ETSI EN 319 522-3 [14] Clause 6 - Service Discovery Format should apply.

In particular:

1) The preferred **routing** strategy should be throughout DNS, even if other techniques may be used, according to the interoperability profile or peer-to-peer agreements between REMSP.

2) The preferred **trusting** strategy should be according to the concepts defined in ETSI EN 319 522-2 [13] Clause 9.3 - ERDS trust establishment and governance and the formats defined in ETSI EN 319 522-3 [14] Clause 6.

3) The preferred **discovery** strategy should be according to ETSI EN 319 522-3 [14] Clauses 6.1 (SML) and 6.2 (SMP).

Furthermore, other protocols or adaptations of the aforementioned processes are admitted, according to specifications provided in future version of the present document or in other documents as agreements among interested parties.

The “identification” of the recipient is possible also before the delivery of the REM message from the sender’s REMSSP to the recipient’s REMSP by means of the aforementioned discovery techniques or according to peer-to-peer protocols agreed between REMSP.

# Annex A (informative): REM message examples

```
From sender@senderdomain.eu  Thu Dec 15 13:01:36 2016
Return-Path: <sender@senderdomain.eu>
Reply-To: "Sender common name" <sender@senderdomain.eu>
From: "On behalf of: sender@senderdomain.eu" <rem-message@s-rems.eu>
To: <recipient@r-rems.eu>
Subject: REM MESSAGE: purchase order n. 1237
Date: Thu, 15 Dec 2016 13:01:34 +0100
Message-ID: <76A0CF65.00566CE0.025BE6B4.85251369.rem-message@s-rems.eu>
X-REM-Msg-Type: Dispatch
X-REM-G02: 6C64B129829AC96401AD6740A55936FB58E4C67A
X-REM-hashAlgorithm: sha-256
X-REM-hashValue: D9CD8155764C3543F10FAD8A480D743137466F8D55213C8EAEFCD12F06D43A80
X-REM-UAMessageIdentifier: <00be01d30072$fde7b950$f9b72bf0$@de>
MIME-Version: 1.0
Content-Type: multipart/signed;
        boundary="----=_Part_25506461_161465589.1481803294404";
        protocol="application/pkcs7-signature";
        micalg=sha-1


This is a multi-part message in MIME format.

------=_Part_25506461_161465589.1481803294404
Content-Type: multipart/mixed;
        boundary="----=_Part_25506459_1876869085.1481803294402"


------=_Part_25506459_1876869085.1481803294402
Content-Type: multipart/alternative;
        boundary="----=_Part_25506458_953555057.1481803294401"


------=_Part_25506458_953555057.1481803294401
Content-Type: text/plain;
        charset="UTF-8"
Content-Transfer-Encoding: quoted-printable
...
...

Editorial note: A complete example will be provided in the next versions of the present document.
```

# Annex B (normative): Event reason identifiers and codes

The present section provides further details in respect to the Clause 7 on ERDS evidence formats. For this purpose the reasons and the relevant codes listed in ETSI EN 319 522-2 [13] Clause 8.3.3 and related annexes shall apply.

# Annex C (normative): XML Schema for Evidence encoded in XML

The present section provides further details in respect to the Clause 7 on ERDS evidence formats. For this purpose the XML formats the relevant schema definitions defined in ETSI EN 319 522-3 [14] Clause 5.2.2 and related annexes and attachments shall apply.

# History

| Document history | | |
|---|---|---|
| V0.0.1 | March 2017 | Version for ESI comments |
| V0.0.2 | June 2017 | Version for ESI comments |
| V0.0.3 | September 2017 | Version for ESI comments |
| V 0.0.4 | October 2017 | Version for public comments |
| V 0.0.5 | October 2017 | Version for public comments |