ETSI TS 102 640-2 V1.1.1 (2008-10)

Technical Specification

Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Architecture, Formats and Policies; Part 2: Data Requirements and Formats for Signed Evidences for REM

ETSI

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

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or
perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF).
In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive
within ETSI Secretariat.

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

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

ETSI

Contents

Intellectual Property Rights

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 (http://webapp.etsi.org/IPR/home.asp).

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.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Electronic Signatures and Infrastructures (ESI).

The present document is part 2 of a multi-part deliverable covering Registered Electronic Mail (REM); Architecture, Formats and Policies, as identified below:

Part 1: "Architecture";

Part 2: "Data Requirements and Formats for Signed Evidences for REM";

Part 3: "Information Security Policy Requirements for REM Management Domains".

Introduction

Business and administrative relationships among companies, public administrations and private citizens, are the more and more implemented electronically. Trust is becoming essential for their success and continued development of electronic services. It is therefore important that any entity using electronic services have suitable security controls and mechanisms in place to protect their transactions and to ensure trust and confidence with their partners.

Electronic mail is a major tool for electronic business and administration. Additional security services are necessary for e-mail to be trusted. In some European Union Member States (Italy, Belgium, etc.) regulation(s) and application(s) are already in place on mails transmitted by electronic means providing origin authentication and proof of delivery. A range of Registered E-Mail ("REM") services is already established and their number is set to grow significantly over the next few years. Without the definition of common standards there will be no consistency in the services provided, making it difficult for users to compare them. Under these circumstances, users might be prevented from easily changing to alternative providers, damaging free competition. Lack of standardization might also affect interoperability between REM based systems implemented based on different models. The present Technical Specification is to ensure a consistent form of service across Europe, especially with regard to the form of evidence provided, in order to maximize interoperability even between e-mail domains governed by different policy rules.

In order to move towards the general recognition and readability of evidence provided by registered e-mail services, it is necessary to specify technical formats, as well as procedures and practices for handling REM, and the ways the electronic signatures are applied to it. In this respect, the electronic signature is an important security component to protect the information and to provide trust in electronic business. It is to be noted that a simple "electronic signature" would be insufficient to provide the required trust to an information exchange. Therefore the present Technical Specification assumes the usage of at least an Advanced Electronic Signature, with the meaning of article 2(2) of EU Directive 1999/93/EC [1].

1   Scope

The basic Registered E-Mail service purpose is to provide users, in addition to the usual services supplied by the ordinary e-mail service providers, with a set of evidences suitable to uphold assertions of acceptance (i.e. of "shipment"), of delivery/non delivery, of receipt, etc. of e-mails sent/delivered through such service.

The present document provides:

   a)   Rules for building a REM-MD Envelope and, consequently, a REM Dispatch or a REM-MD Message.

   b)   Syntax and semantics of REM-MD Evidences to be produced by a REM Management Domain.

   c)   Rules on the signature to be used within REM-MD Envelopes.

REM-MD Evidence formats are deemed to comply with legal, regulatory or contractual requirements to provide legal validity and enforceability under domestic or international law.

The structure of the present document is as follows:

   •   Clause 2 contains the list of normative and informative references.

   •   Clause 3 includes definitions of the relevant concepts to the present document and abbreviations.

   •   Clause 4 contains the generic REM-MD Envelope structure.

   •   Clause 5 contains the definition of REM-MD Evidences produced by REM-MDs, in terms of content and semantics. Specific syntaxes are addressed by annexes.

   •   Clause 6 deals with digital signatures to be applied by REM-MD for building REM-MD Envelopes.

   •   Annex A provides ASN.1 syntax for REM-MD Evidences.

   •   Annex B provides xml syntax for REM-MD Evidences.

   •   Annex C provides pdf syntax for REM-MD Evidences.

   •   Annex D specifies identifiers and codes for reporting events reasons in REM-MD Evidences.

   •   Annex E provides the ASN.1 definition for REM-MD Evidences encoded in ASN.1.

   •   Annex F provides the XML schema for REM-MD Evidences encoded in XML.

2   References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific.

   •   For a specific reference, subsequent revisions do not apply.

   •   Non-specific reference may be made only to a complete document or a part thereof and only in the following cases:

        -   if it is accepted that it will be possible to use all future changes of the referenced document for the purposes of the referring document;

        -   for informative references.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

For online referenced documents, information sufficient to identify and locate the source shall be provided. Preferably, the primary source of the referenced document should be cited, in order to ensure traceability. Furthermore, the reference should, as far as possible, remain valid for the expected life of the document. The reference shall include the method of access to the referenced document and the full network address, with the same punctuation and use of upper case and lower case letters.

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

2.1 Normative references

The following referenced documents are indispensable for the application of the present document. For dated references, only the edition cited applies. For non-specific references, the latest edition of the referenced document (including any amendments) applies.

[1] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

[2] IETF RFC 3852: "Cryptographic Message Syntax (CMS)".

[3] ETSI TS 101 733: "Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)".

[4] ETSI TS 101 903: "XML Advanced Electronic Signatures (XAdES)".

[5] ETSI TS 102 176-1: "Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms".

[6] ETSI TS 102 231: "Electronic Signatures and Infrastructures (ESI); Provision of harmonized Trust-service status information".

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

[8] IETF RFC 2311: "S/MIME Version 2 Message Specification".

[9] IETF RFC 2822: "Internet Message Format".

[10] ITU-T Recommendations X.680-683: "Information technology - Abstract Syntax Notation One (ASN.1)".

[11] ITU-T Recommendation X.690: "Information technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)".

[12] OASIS Digital Signature Services (DSS) TC: "Digital Signature Service Core Protocols, Elements, and Bindings Version 1.0".

[13] IETF RFC 3061 (2001): "A URN Namespace of Object Identifiers".

[14] IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

[15] AFNOR AC Z74-600-3 (2005): "Electronic attestations of anteriority, deposit, withdrawal and receipt - Part 3 : format of attestations".

[16] ETSI TS 102 904: "Electronic Signatures and Infrastructures; Profiles of XML Advanced Electronic Signatures based on TS 101 903 (XAdES)".

2.2   Informative references

The following referenced documents are not essential to the use of the present document but they assist the user with regard to a particular subject area. For non-specific references, the latest version of the referenced document (including any amendments) applies.

[i.1]   ETSI TR 102 605: "Electronic Signatures and Infrastructures (ESI); Registered E-Mail".

[i.2]   ETSI TS 102 640-1: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Architecture, Formats and Policies; Part 1: Architecture".

[i.3]   ETSI TS 102 640-3: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Architecture, Formats and Policies; Part 3: Information Security Policy Requirements for REM Management Domains".

[i.4]   IETF RFC 822: "Standard for the format of ARPA internet text messages".

[i.5]   IETF RFC 2045: "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies".

[i.6]   IETF RFC 2046: "Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types".

[i.7]   IETF RFC 3986: "Uniform Resource Identifier (URI): Generic Syntax".

[i.8]   ISO 32000-1 (2008): "Document management - Portable document format - Part 1: PDF 1.7".

3   Definitions and abbreviations

3.1   Definitions

For the purposes of the present document, the terms and definitions given in TS 102 640-1 [i.2], TS 102 640-3 [i.3] and the following apply:

Long Term Storage: role that supports the integrity of data and the authenticity of a signature over the period required to store data for evidential purposes that can be used by the Message Archive

Message archive: optional role that supports storage of REM Objects and REM-MD Evidences, as required for later use for evidential or any other legally admitted purposes, at the relevant REM-MD for an indefinite or definite time period, to be accessed once or many times by one or more entities

Original Message: e-mail message generated by the Sender's User Agent or under the Sender's technical/legal responsibility (i.e. outside of the REM-MD), which may be signed by the Sender

NOTE: It has to be conveyed to the Recipient either by value (in the Store & Forward Style of operations) or by reference (in the Store & Notify Style of operations).

REM Dispatch: REM-MD Envelope containing the Original Message and related REM-MD Evidence

REM Message Store: role that supports the storage of REM Objects

NOTE: In other words the set of mailboxes of the users.

REM Object: message object handled by a REM-MD. This is a REM-MD Message, REM-Dispatch or Original message

REM Objects Relay Interface: interface that supports REM objects relaying between disparate REM-MD

REM Recipient: physical or legal entity legally responsible for the mailbox to which the original message is addressed

REM Sender: physical or legal entity legally responsible for the mailbox from which the original message has been sent

REM Third Party: party authorized to access REM Objects and REM-MD Evidence for specific purposes

REM User Agent (REM-UA): entity by which Senders, Recipients participate in the exchange of REM Objects and Third Parties may access REM Objects

REM-Management Domain (REM-MD): set of technical and physical components, personnel, policies and processes that provide REM services

    NOTE: A REM-MD is operated under the responsibility of a single management entity.

REM-MD Envelope: signed structure generated by the REM-MD which envelopes an Original message and/or REM-MD Evidence

REM-MD Evidence: signed data created within a REM-MD, which proves that a certain event has occurred at a certain time

    NOTE: It may be signed directly or indirectly by placing it within a REM-MD Envelope.

REM-MD Evidence Provider: role that issues REM-MD Evidences

REM-MD Evidence Verifier: role that supports the verification of REM-MD Evidences

REM-MD Message: RFC 822 [i.4] message generated by the REM-MD under the REM-MD sole technical/legal responsibility (i.e. inside of the REM-MD)

    NOTE: It must be signed by the entity legally responsible for the REM-MD. It may be understood by the recipient/sender as a "receipt" or a "notification". A REM-MD Message carries an REM-MD Envelope containing REM-MD Evidence.

REM-MD Message Gateway: role that supports the transfer of REM objects to conventional e-mail (e.g. Internet) services and physical postal delivery services

REM-MD Message Transfer Agent: role that supports the transfer of REM Objects to Recipient's and Sender's Message Store either directly or via the REM-MD Message and Evidence Relay Interface into another REM-MD or via a Message Gateway

REM-MD Repository: role that supports the storage of Original Messages, REM-MD Evidences and any other, which must be accessed by reference

REM-MD Repository Retrieval Interface: interface of REM-MD towards REM UA used in the Store and Notify Style of Operation by the Recipient for downloading REM Objects from REM-MD Repository

    NOTE: It can also be used by Senders for downloading REM-MD Evidences.

REM-MD Sender Message Submission Interface: interface of REM-MD towards sender REM UA used by the REM Sender to submit Original Messages to her REM-MD, for them to be forwarded to the Recipients

REM-MD Sender/Recipient Message Store Retrieval Interface: interface of REM-MD towards REM UA used by REM Senders or REM Recipients to fetch REM Objects addressed to them

REM-MD Third Party Evidence Retrieval Interface: interface that supports REM-MD Evidences and REM Objects retrieval by users that are parties external to the usual message flow

3.2 Abbreviations

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

AdES	Advanced Electronic Signature
CAdES	CMS Advanced Electronic Signatures
CMS	Cryptographic Message Syntax
OID	Object Identifier
QES	Qualified Electronic Signature
REM	Registered E-Mail
REM-MD	REM Management Domain
REM-PD	REM Policy Domain
REM-UA	REM User Agent
RSRI	Reference Store Retrieval Interface

S&F	Store and Forward
S&N	Store and Notify
URI	Uniform Resource Identifier
XAdES	XML Advanced Electronic Signature

4　　REM-MD Envelope Structure Implementation

This clause provides a specification for the structure of a REM-MD Envelope. A REM-MD Envelope does not exist as a self-standing object, since it always appear in the context of a REM-MD Message or a REM Dispatch.

A REM-MD Message or a REM Dispatch may flow between REM-MDs, and optionally from REM-MDs to REM User Agents, as defined in TS 102 640-1 [i.2]. No specifications are provided in the present document on how the generic REM-MD Message or REM Dispatch should be tailored according to the specific mode of operation and interface it flows through.

A REM-MD Envelope is a structure for encapsulating REM-MD Evidence and/or Original Message. Moreover it contains:

1) An (optional) introductory message-part displayed by the mail client application and in which the REM-MD explains the purpose of the current message and gives some details on the other parts attached to it. The present document may also contain references to objects stored in a REM-MD Repository.

2) A signature applied by the REM-MD (the signature covers both the Original Message, when present, and the REM-MD Evidence).

A REM-MD Envelope is structured with a Message Header containing the Header Fields followed by Message Body containing one or more Body Parts as defined in MIME (RFC 2045 [i.5]). The Message Body will 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 multipart/mixed MIME message will 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-MD Envelope will therefore be the signature of the REM-MD over the rest of the MIME parts that appear in the REM-MD Envelope

This generic structure with all its elements can be further depicted as follow.

REM-MD Envelope	Headers				MIME message headers profiled for a **multipart/signed** MIME message (see clause 4.1)
	Body (signed data)	Headers			MIME part headers profiled for a **multipart/mixed** message (see clause 4.2)
		Body	REM-MD Introduction MIME section 0..1	Headers	MIME part headers profiled for a text/plain or a **multipart/alternative** MIME content (see clause 4.4)
				Body	In the case of **text/plain** the body contains a message created by the REM-MD, which is intended to be displayed automatically upon display of the REM-MD Message/REM Dispatch. Text may contain URIs

						In the case of **multipart/alternative** the body contains: a. a part headers profiled for an inline body content. The present document contains a message created by the REM-MD, which is intended to be displayed automatically upon display of the REM-MD Message/REM Dispatch. Text may contain URIs (see clause 4.4.1) b. a part profiled for **message/external-body** (RFC 2046 [i.6], clause 5.2.3). The present document contains an URI for automatic processing of access by reference to a message in a REM-MD Repository (see clause 4.4.2)
				Original Message MIME section 0..1	Headers	MIME part headers profiled for an enveloped **message/rfc822** message (see clause 4.5)
					Body	Optional full, self-contained RFC-822 message as submitted by the sender. (the Original Message). Only present in REM Dispatch
				REM-MD Evidence MIME section 0..N	Headers	MIME part headers profiled for an **application/octet-stream**, **application/xml** or **application/pdf** (see clause 4.6)
					Body	Optional REM-MD Evidence as required by the specific content-type
		REM-MD Signature	Headers			MIME part headers profiled to S/MIME **application/pkcs7-signature** signature on the whole REM-MD Message/REM Dispatch (see clause 4.3)
			Body			S/MIME Signature generated by the Sender's REM-MD covering the whole structure

Figure 1: REM-MD Envelope generic template

This figure presents the full structure including parts in grey which should be filled to build a REM Dispatch or a REM-MD Message.

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

4.1 REM-MD Message/REM Dispatch Headers constraints

Content-Type	The value for this header MUST be "multipart/signed". The 'protocol' parameter value MUST be "application/x-pkcs7-signature". The 'micalg' parameter value SHOULD be conformant to TS 102 176-1 [5]
MIME-Version	The value for this header MUST be "1.0"
Message-ID	This value SHOULD be an UID (see note) NOTE: Identifier that is unique over the time.
Date	This value MUST be compliant with clause 3.3 of RFC 2822 [9]
From	This value SHOULD be either a REM-MD 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 REM-MD (e.g. "on behalf of user@rem_md_x.com <service_rem_md_x@rem_md_x.com>")
To	This value MUST be compliant with clause 3.6.3 of RFC 2822 [9]. The value for this header shall match the value of the 'To' header field in the Original Message
Subject	This value 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-MD Message/REM Dispatch 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-MD Message is a delivery receipt)

The header of each REM-MD Envelope may contain optional Extension Header Fields. The purpose of these headers is to give immediate access to important identification information, which is already present in the REM-MD Evidence, instead of forcing REM-MDs to go through the REM-MD Evidence.

The syntax of these optional parameters is the following:

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

where:

- <component> is related to the name of a REM-MD Evidence Component (see clause 5.2).

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

4.2 REM-MD Message/REM Dispatch Data Headers Constraints

Content-Type	The value for this field MUST be: "multipart/mixed"

4.3 REM-MD Signature Headers Constraints

Content-Type	The value for this header MUST be: "**application/x-pkcs7-signature; name=smime.p7s**". The value of the 'name' parameter SHOULD be "smime.p7s"
Content-Transfer-Encoding	The value for this header MUST be: "base64"
Content-Disposition	The value for this header MUST be: "attachment" The value of the 'filename' parameter SHOULD be "smime.p7s"
Content-Description	The value for this header MAY be: "S/MIME Cryptographic Signature"

4.4 REM-MD Introduction Headers Constraints

Content-Type	The value for this field MUST be: "**text/plain**" or "**multipart/alternative**"
Content-Disposition (only for "text/plain")	The value of this header MUST be "inline" as it is intended to be displayed automatically upon display of the message in mail client
Content-Transfer-Encoding (only for "text/plain")	The value for this field MUST be: 7bit

4.4.1 Multipart/alternative: Free text subsection Header constraints

Content-Type	The value for this field MUST be: "text/plain"
Content-Disposition	The value of this header MUST 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 MUST be: 7bit

4.4.2 Multipart/alternative: Structured subsection Header constraints

Content-Type	The value for this field MUST be: "**message/external-body**" access-type=X-REM-<rem-access-type>-ACCESS; (1) expiration="<date-of-expiration>" - OPTIONAL <two consecutive CRLFs as per RFC 2045 [i.5]> See also note 1 for the rem-access-type
X-REM-ACCESS-URI	<access-uri-value> (2) See note 2
Content-Type	The value for this field MUST be "**message/rfc822**"
Content-ID	<original-mime-message-id> This field must contain a UID for the referenced object as per RFC 2045 [i.5]
NOTE 1: X-REM-<rem-access-type>-ACCESS is one of the recommended access protocol when the Original Message has to be accessed by reference (e.g. X-REM-HTTPS-ACCESS).	
NOTE 2: X-REM-ACCESS-URI contains the full URI (containing optionally, if required, authentication information according to RFC 3986 [i.7]) referencing the REM-MD Evidence.	

4.5 Original Message MIME Section Headers Constraints

Content-Type	The value for this field MUST be: "message/rfc822"; name=AttachedMimeMessage
Content-Transfer-Encoding:	7bit
Content-Disposition	The value for this field MUST be: "attachment"; filename=AttachedMimeMessage

4.6 REM-MD Evidence MIME Section Headers Constraints

4.6.1 ASN.1 Format

Content-Type	The value for this header will be "application/octet-stream" The value of the 'name' parameter will be "<REM EVIDENCE_NAME>.aso" The value of the 'charset' parameter MUST be "UTF-8"
Content-Transfer-Encoding	The value of this header MUST be "quoted-printable"
Content-Disposition	The value of this header will be "attachment" The value of the 'filename' parameter will match the value of the 'name' parameter of the Content-Type header

4.6.2 XML Format

Content-Type	The value for this header will be "application/xml" The value of the 'name' parameter will be "<REM EVIDENCE_NAME>.xml" The value of the 'charset' parameter MUST be "UTF-8"
Content-Transfer-Encoding	The value of this header MUST be "quoted-printable"
Content-Disposition	The value of this header will be "attachment" The value of the 'filename' parameter will match the value of the 'name' parameter of the Content-Type header

4.6.3 PDF Format

Content-Type	The value for this header will be "application/pdf" The value of the 'name' parameter will be "<REM EVIDENCE_NAME>.pdf"
Content-Transfer-Encoding	The value of this header will be "base64"
Content-Disposition	The value of this header will be "attachment" The value of the 'filename' parameter will match the value of the 'name' parameter of the Content-Type header

5 REM-MD Evidence Content and Semantics

This clause provides the content and semantics for REM-MD Evidences, which are trusted statements produced by REM-MDs, according to the flows described in TS 102 640-1 [i.2]. One REM-MD Evidence can address more Events among those described individually in TS 102 640-1 [i.2], clause 6.

In clause 5.1 the list of REM-MD Evidences is presented in detail.

REM-MD Evidences are described with reference to a set of building blocks called "REM-MD Evidence components". In clause 5.2 REM-MD Evidence Components are listed and described in terms of content and semantics. This clause is divided in the following three clauses:

    i)   Clause 5.2.1 presents a synoptic Template of REM-MD Evidence Components.

    ii)   Clause 5.2.2 provides a detailed description and explanation of all REM-MD Evidence Components that are described in terms of content and semantics.

    iii)   Clause 5.2.3 describes formats and values of the REM-MD Evidence Components, providing elements such as Time and Data format, Exception Codes, etc.

Specific syntaxes allowed for REM-MD Evidences are provided in annexes A, B and C.

5.1 REM-MD Evidences

In this clause the REM-MD Evidences provided by REM-MD are described. They correspond to events mentioned in TS 102 640-1 [i.2], clause 6 as described in the following table.

Event (TS 102 640-1 [i.2], clause 6.2)	REM-MD Evidence
6.2.1 Event A.1 - S-REM-MD Acceptance	5.1.1 SubmissionAcceptanceRejection
6.2.1 Event A.2 - S- REM-MD Rejection	
6.2.2 Event B.1 - R-REM-MD Acceptance	5.1.2 RelayToREMMDAcceptanceRejection
6.2.2 Event B.2 - R-REM-MD Rejection	
6.2.2 Event B.3 - Expiration of time to deliver to R-REM-MD	5.1.3 RelayToREMMDFailure
6.2.3 Event C.1 - Message Delivery	5.1.4 DeliveryNonDeliveryToRecipient
6.2.3 Event C.2 - Expiration of time to deliver message	
6.2.3 Event D.1 - Notification Delivery	
6.2.3 Event D.2 - Expiration of time to deliver notification	

Event (TS 102 640-1 [i.2], clause 6.2)	REM-MD Evidence
6.2.3 Event E.1 (REM-MD Repository) - Download	5.1.5 DownloadNonDownloadByRecipient
6.2.3 Event E.2 (REM-MD Repository) - Expiration of time for download	
6.2.3 Event E.4 (REM-MD Repository) - Download by a recipient's delegate	
6.2.3 Event F.1 (mailbox) - Retrieval	5.1.6 RetrievalNonRetrievalByRecipient
6.2.3 Event F.2 (mailbox) - Expiration of time for Retrieval	
6.2.3 Event F.3 (mailbox) - Retrieval by a recipient's delegate	
6.2.3 Event E.3 - Rejection of download by recipient	5.1.7 AcceptanceRejectionByRecipient
6.2.4 Event H.1 - Successful forwarding for Ordinary e-mail	5.1.8 RelayToNonREMSystem
6.2.4 Event H.2 - Unsuccessful forwarding for Ordinary e-mail	
6.2.4 Event G.1 - Successful forwarding for Printing	
6.2.4 Event G.2 - Unsuccessful forwarding for Printing	
6.2.4 Event I.1 - E-Mail message received from a regular e-mail system	5.1.9 **Error! Bookmark not defined.**ReceivedByNonREMSystem

In order to facilitate interoperability within the REM community, and based on the outcomes published in TR 102 605 [i.1] of a survey performed among a large number of interviewees, each REM-MD Evidence type is indicated as "M" (mandatory), "R" (recommended) or "O" (optional).

A few of these REM-MD Evidence types can be issued by, or with the support of, external providers, therefore, where applicable, locutions like "issued under the responsibility of" are used instead of "issued by".

In the following paragraphs for each REM-MD Evidence the basic content is specified by means of MANDATORY "REM-MD Evidence Components" the content of which is specified in clause 5.2. Additional "REM-MD Evidence Components" MAY be used where applicable, either chosen from those listed in clause 5.2.1, or additional ones applicable within a predefined set of REM-MDs, like a REM-PD.

Parties other than the "Primary REM-MD Evidence Recipient" may also rely on any REM-MD Evidence.

It should be noted that different forms of REM-MD Evidence may be directly provided by the sender itself, for instance by electronically signing the message before sending. This sender's signature provides an additional reliable information on the message origin and authenticity, provided that the certificate supporting the signature is issued by a Certification Authority that is acknowledged as trusted (see note) and, preferably, that the signature is issued by means of a Secure Signature Creation Device with the meaning of article 2(6) of the Directive 1999/93/EC [1]. However, this is outside the scope of the present document.

NOTE: As an example, in the European Union, Certification Authorities issuing Qualified Certificates, as defined in the European Directive 1999/93/EC [1] article 2(10), are trusted since article 3(3) of the same Directive mandates that they are supervised in the EUMS they reside in.

5.1.1   SubmissionAcceptanceRejection

Description	REM-MD Evidence of submitted message acceptance / Rejection
Optionality	M
Purpose	to prove that a certain Original Message was / was not successfully submitted, at the time indicated in the REM-MD Evidence, to the sender's REM-MD by the sender authenticated by the same sender's REM-MD.
Related event	successful / unsuccessful acceptance by sender's REM-MD of an Original Message submitted to the same REM-MD by the authenticated message sender.
Responsible for Issuance	sender's REM-MD.
Primary Intended Recipient	message sender and message recipient.
REM-MD Evidence Components	<table><tr><th>Id</th><th>Component</th><th># Iter</th></tr><tr><td>G00</td><td>REM-MD Evidence Identifier</td><td>1</td></tr><tr><td>G01</td><td>REM-MD Evidence Type = "SubmissionAcceptanceRejection"</td><td>1</td></tr><tr><td>G02</td><td>REM Event</td><td>1</td></tr><tr><td>G03</td><td>Reason code</td><td>0..N</td></tr><tr><td>G04</td><td>REM-MD Evidence Version</td><td>1</td></tr><tr><td>G05</td><td>Event Time</td><td>1</td></tr><tr><td>G06</td><td>Transaction log information</td><td>0..1</td></tr><tr><td>R01</td><td>REM-MD Evidence issuer Policy Identifier</td><td>1..N</td></tr><tr><td>R02</td><td>REM-MD Evidence issuer Details</td><td>1</td></tr><tr><td>R03</td><td>Signature by issuing REM-MD</td><td>0..1</td></tr><tr><td>I00</td><td>Sender's details</td><td>1</td></tr><tr><td>I01</td><td>Recipient's details</td><td>1..N</td></tr><tr><td>I04</td><td>Sender Authentication details</td><td>0..1</td></tr><tr><td>M00</td><td>REM-MD Message/REM Dispatch details</td><td>1</td></tr><tr><td>M01</td><td>Reply-to</td><td>0..1</td></tr><tr><td>M03</td><td>Message Submission Time</td><td>0..1</td></tr></table>

5.1.2   RelayToREMMDAcceptanceRejection

Description	REM-MD Evidence that a successfully received REM-MD Message/REM Dispatch was accepted / rejected by the recipient's REM-MD
Optionality	It SHOULD be sent to the sender's REM-MD. It MAY be sent back to the sender.
Purpose	to prove that one REM-MD Message/REM Dispatch sent by the sender's REM-MD was successfully received by the recipient's REM-MD that accepted / rejected it. NOTE: This REM-MD Evidence is applicable when the received message comes from another REM-MD. The case when it comes from an ordinary e-mail server is covered in clause 5.1.9.
Related event	The REM-MD Message/REM Dispatch was sent by the sender's REM-MD and received by the recipient's REM-MD that accepted / rejected it.
Responsible for Issuance	Recipient's REM-MD
Primary Intended Recipient	sender's REM-MD
REM-MD Evidence Components	

Id	Component	# Iter
G00	REM-MD Evidence Identifier	1
G01	REM-MD Evidence Type = "RelayToREMMDAcceptanceRejection"	1
G02	REM Event	1
G03	Reason code	0..N
G04	REM-MD Evidence Version	1
G05	Event Time	1
G06	Transaction log information	0..N
R01	REM-MD Evidence issuer Policy Identifier	1..N
R02	REM-MD Evidence issuer Details	1
R03	Signature by issuing REM-MD	0..1
I00	Sender's details	1
I01	Recipient's details	1..N
M00	REM-MD Message/REM Dispatch details	1
M01	Reply-to	0..1
M02	Notification Message Tag	1

5.1.3   RelayToREMMDFailure

Description	REM-MD Evidence of non delivery of a REM-MD Message/REM Dispatch to the recipient's REM-MD within a given time period			
Optionality	R			
Purpose	to prove that it was impossible to deliver a REM-MD Message/REM Dispatch within a given time period to the recipient's REM-MD due to technical errors and/or other problems.			
Related event	This REM-MD Evidence can be issued to specify that a problem was encountered when trying to forward a REM-MD Message/REM Dispatch to the recipient's REM-MD; the following cases can occur: 1) the sender's REM-MD was not able to identify the recipient's REM-MD; 2) the recipient's REM-MD is unreachable; 3) the recipient's REM-MD had malfunctions that prevented the REM-MD Message/REM Dispatch delivery. The referred to given time period may be set law, by statutory requirements, by internal rules, in any case it is reflected in the REM-MD's or in the REM-PD's policies.			
Responsible for Issuance	Sender's REM-MD. NOTE: This REM-MD Evidence is generated by the sender's REM-MD that, where applicable, may take in account also the replies from the recipient's REM-MD.			
Primary Intended Recipient	Sender			
REM-MD Evidence Components	Id	Component	# Iter	
	G00	REM-MD Evidence Identifier	1	
	G01	REM-MD Evidence Type = "RelayToREMMDFailure"	1	
	G02	REM Event	1	
	G03	Reason code	0..N	
	G04	REM-MD Evidence Version	1	
	G05	Event Time	1	
	G06	Transaction log information	0..N	
	R01	REM-MD Evidence issuer Policy Identifier	1..N	
	R02	REM-MD Evidence issuer Details	1	
	R03	Signature by issuing REM-MD	0..1	
	I00	Sender's details	0..1	
	I01	Recipient's details	1..N	
	I03	Recipient referred to by the REM-MD Evidence	1	
	M00	REM-MD Message/REM Dispatch details	1	
	M01	Reply-to	0..1	
	M02	Notification Message Tag	1	

5.1.4   DeliveryNonDeliveryToRecipient

Description	**REM-MD Evidence of delivery / non delivery within a given time period of a REM-MD Message/REM Dispatch to the recipient's or, OPTIONALLY, to a recipient's delegate mailbox**			
Optionality	**M**			
Purpose	To prove that the REM-MD Message/REM Dispatch was delivered to the recipient's mailbox or, OPTIONALLY, to a delegate's mailbox at a specific time or that it was not possible to deliver it within a given time period. This time period may be set law, by statutory requirements, by internal rules, in any case it is reflected in the REM-MD's or in the REM-PD's policies. NOTE 1: The time period can be any, even zero, in which case the recipient's REM-MD will not retry to deliver the REM-MD Message/REM Dispatch if the first attempt fails. NOTE 2: The REM-MD, or REM-PD, policies shall specify if the delivery can be performed into a delegate's mailbox and the details of the delegation mechanism and how and for how long the related documentation would be kept.			
Related event	1) The recipient's REM-MD successfully deposited / was not able to deposit within a given time period a REM-MD Message/REM Dispatch into the recipient's or, OPTIONALLY, a delegate's REM mailbox. In this case the REM-MD that creates this evidence is the recipient's REM-MD. 2) The sender's REM-MD did not receive within a given time period from the recipient's REM-MD a REM-MD Evidence of successful/unsuccessful delivery. In this case it is the sender's REM-MD that creates this REM-MD Evidence with the suitable reason code.			
Responsible for Issuance	Recipient's REM-MD or sender's REM-MD.			
Primary Intended Recipient	Sender			
REM-MD Evidence Components	**Id**	**Component**	**# Iter**	
	G00	REM-MD Evidence Identifier	1	
	G01	REM-MD Evidence Type = "DeliveryNonDeliveryToRecipient"	1	
	G02	REM Event	1	
	G03	Reason code	0..N	
	G04	REM-MD Evidence Version	1	
	G05	Event Time	1	
	G06	Transaction log information	0..N	
	R01	Evidence issuer Policy Identifier	1..N	
	R02	Evidence issuer Details	1	
	R03	Signature by issuing REM-MD	1	
	I00	Sender's details	0..1	
	I01	Recipient's details	0..N	
	I02	Recipient's delegate details	0..N	
	I03	Recipient referred to by the Evidence	0..1	
	M00	REM-MD Message/REM Dispatch details	1	
	M01	Reply-to	0..1	
	M02	Notification Message Tag		

5.1.5 DownloadNonDownloadByRecipient

Description	Evidence of download / non download within a given time period - of a REM-MD Message/REM Dispatch by the recipient's or, OPTIONALLY, a recipient's delegate
Optionality	M
Purpose	To prove that the REM-MD Message/REM Dispatch at a specific time was downloaded by the recipient or, OPTIONALLY, by an Entity Delegated by the Recipient, or non downloaded within a given retention period that expired at the specified time.
Related event	The recipient or, OPTIONALLY, a delegate successfully downloaded / did not download within a given time period a REM-MD Message/REM Dispatch from a REM-MD Repository under the responsibility of the sender's or recipient's REM-MD, depending on the download mechanism.
Responsible for Issuance	Recipient's or sender's REM-MD. NOTE: The REM-MD issuing the signature, that is also the REM-MD responsible for the RSRI, can be the recipient's REM-MD or of the sender's REM-MD, depending on the download mechanism.
Primary Intended Recipient	Sender

REM-MD Evidence Components	Id	Component	# Iter	
	G00	REM-MD Evidence Identifier	1	
	G01	REM-MD Evidence Type = "DownloadNonDownloadByRecipient"	1	
	G02	REM Event	1	
	G03	Reason code	0..N	
	G04	REM-MD Evidence Version	1	
	G05	Event Time	1	
	G06	Transaction log information	0..N	
	R01	Evidence issuer Policy Identifier	1..N	
	R02	Evidence issuer Details	1	
	R03	Signature by issuing REM-MD	1	
	I00	Sender's details	0..1	
	I01	Recipient's details	0..N	
	I02	Recipient's delegate details	0..N	
	I03	Recipient referred to by the Evidence	0..1	
	I05	Recipient Authentication details	0..1	
	M00	REM-MD Message/REM Dispatch details	1	

5.1.6 RetrievalNonRetrievalByRecipient

Description	Evidence of retrieval / non retrieval within a given period - by the recipient or, OPTIONALLY, by a recipient's delegate			
Optionality	O			
Purpose	To prove that the REM-MD Message/REM Dispatch present in the recipient's mailbox was retrieved / non retrieved within a given period - by the recipient or, OPTIONALLY, by a recipient's delegate. Retrieval of the REM-MD Message/REM Dispatch from the mailbox, upon user authentication, can be implemented in two ways: a) the recipient's (or his/her delegate's) User Agent (a desktop client such as Microsoft Outlook or Mozilla Thunderbird), downloads messages from the mailbox at the REM-MD's; b) an ad hoc webmail application accesses the related mailbox and messages data, for example: sender, subject, send date, size, etc, are fetched and displayed on the webmail page; the recipient or his/her delegate is now aware of the REM-MD Message/REM Dispatch existence.			
Related event	The REM-MD Message/REM Dispatch held in the recipient's mailbox is retrieved / not retrieved within a given period - by the recipient or, OPTIONALLY, by a recipient's delegate.			
Responsible for Issuance	Recipient's REM-MD.			
Primary Intended Recipient	Sender			
REM-MD Evidence Components	**Id**	**Component**	**# Iter**	
	G00	REM-MD Evidence Identifier	1	
	G01	REM-MD Evidence Type = "RetrievalNonRetrievalByRecipient"	1	
	G02	REM Event	1	
	G03	Reason code	0..N	
	G04	REM-MD Evidence Version	1	
	G05	Event Time	1	
	G06	Transaction log information	0..N	
	R01	Evidence issuer Policy Identifier	1..N	
	R02	Evidence issuer Details	1	
	R03	Signature by issuing REM-MD	1	
	I00	Sender's details	0..1	
	I01	Recipient's details	0..N	
	I02	Recipient's delegate details	0..N	
	I03	Recipient referred to by the Evidence	0..1	
	I05	Recipient Authentication details	0..1	
	M00	REM-MD Message/REM Dispatch details	1	
	M01	Reply-to	0..1	
	M02	Notification Message Tag	1	

5.1.7   AcceptanceRejectionByRecipient

Description	Evidence of acceptance / rejection by the recipient, or, OPTIONALLY, a delegate, of a REM-MD Message/REM Dispatch			
Optionality	O			
Purpose	To prove that the REM-MD Message/REM Dispatch was accepted / rejected by the recipient or, OPTIONALLY, by a delegate. This REM-MD Evidence, differently from DownloadNonDownloadByRecipient and RetrievalNonRetrievalByRecipient, implies an explicit act of the recipient who declares to accept/reject the message.			
Related event	The recipient or, OPTIONALLY, a delegate communicated to the sender's REM-MD or the recipient's REM-MD his/her will to accept/reject a REM-MD Message/REM Dispatch. This REM-MD Evidence may apply both to S&N and S&F operation modes.			
Responsible for Issuance	Recipient's REM-MD			
Primary Intended Recipient	Sender			
REM-MD Evidence Components	**Id**	**Component**	**# Iter**	
	G00	REM-MD Evidence Identifier	1	
	G01	REM-MD Evidence Type = "AcceptanceRejectionByRecipient"	1	
	G02	REM Event	1	
	G03	Reason code	0..N	
	G04	REM-MD Evidence Version	1	
	G05	Event Time	1	
	G06	Transaction log information	0..N	
	R01	Evidence issuer Policy Identifier	1..N	
	R02	Evidence issuer Details	1	
	R03	Signature by issuing REM-MD	1	
	I00	Sender's details	0..1	
	I01	Recipient's details	0..N	
	I02	Recipient's delegate details	0..N	
	I03	Recipient referred to by the Evidence	0..1	
	I05	Recipient Authentication details	0..1	
	M00	REM-MD Message/REM Dispatch details	1	
	M02	Notification Message Tag	1	

5.1.8   RelayToNonREMSystem

Description	Evidence that a REM-MD Message/REM Dispatch was successfully / unsuccessfully forwarded to a non-REM external system
Optionality	O
Purpose	To prove that a certain REM-MD Message/REM Dispatch was successfully / unsuccessfully forwarded by the sender's or recipient's REM-MD to a non REM external system NOTE: Depending on the statutory or contractual agreements, the sender's REM-MD MAY forward a REM-MD Message/REM Dispatch to a non REM external system if it is not able to forward it to the recipient's REM-MD via REM. Under similar agreement the recipient's REM-MD MAY behave similarly if it cannot deposit the REM-MD Message/REM Dispatch into the recipient's REM mailbox. The involved REM-MD MAY / MAY NOT issue REM-MD Evidence types related to the various events (e.g. "non delivery" and "forwarding to ordinary e-mail") depending on the applicable Policy.
Related event	The message was successfully / unsuccessfully forwarded by the sender's or recipient's REM-MD to a non REM external system.
Responsible for Issuance	Sender's or recipient's REM-MD
Primary Intended Recipient	Sender
REM-MD Evidence Components	<table><tr><th>Id</th><th>Component</th><th># Iter</th><th></th></tr><tr><td>G00</td><td>REM-MD Evidence Identifier</td><td>1</td><td></td></tr><tr><td>G01</td><td>REM-MD Evidence Type = "SubmissionAcceptanceRejection"</td><td>1</td><td></td></tr><tr><td>G02</td><td>REM Event</td><td>1</td><td></td></tr><tr><td>G03</td><td>Reason code</td><td>0..N</td><td></td></tr><tr><td>G04</td><td>REM-MD Evidence Version</td><td>1</td><td></td></tr><tr><td>G05</td><td>Event Time</td><td>1</td><td></td></tr><tr><td>G06</td><td>Transaction log information</td><td>0..N</td><td></td></tr><tr><td>R01</td><td>Evidence issuer Policy Identifier</td><td>1..N</td><td></td></tr><tr><td>R02</td><td>Evidence issuer Details</td><td>1</td><td></td></tr><tr><td>R03</td><td>Signature by issuing REM-MD</td><td>1</td><td></td></tr><tr><td>I00</td><td>Sender's details</td><td>0..1</td><td></td></tr><tr><td>I01</td><td>Recipient's details</td><td>0..N</td><td></td></tr><tr><td>I03</td><td>Recipient referred to by the Evidence</td><td>0..1</td><td></td></tr><tr><td>I05</td><td>Recipient Authentication details</td><td>0..1</td><td></td></tr><tr><td>M00</td><td>REM-MD Message/REM Dispatch details</td><td>1</td><td></td></tr><tr><td>M01</td><td>Reply-to</td><td>0..1</td><td></td></tr><tr><td>M02</td><td>Notification Message Tag</td><td>1</td><td></td></tr><tr><td>M04</td><td>Forwarded to external system</td><td>1</td><td></td></tr></table>

5.1.9   ReceivedByNonREMSystem

Description	Evidence that a message was successfully received from a regular (i.e. non REM) e-mail system			
Optionality	O			
Purpose	To prove that a certain message was not received from a REM-MD but from an ordinary e-mail server, therefore all information on message origin is not per se trustable. NOTE 1: This REM-MD Evidence will most likely be merged in the REM-MD Message/REM Dispatch that the recipient's REM-MD SHALL generate. NOTE 2: This REM-MD Evidence is generated when the message comes from an ordinary e-mail server and the recipient's REM-MD policy provides accepting ordinary e-mails sent to its own users.			
Related event	The REM-MD received the message from a regular e-mail gateway.			
Responsible for Issuance	Recipient's REM-MD			
Primary Intended Recipient	Recipient			
REM-MD Evidence Components	NOTE: All information related to sender and other recipients, in addition to the one this Evidence is delivered, is simply claimed by the sender, being not a REM-MD Message/REM Dispatch.			
	Id	**Component**	**# Iter**	
	G00	REM-MD Evidence Identifier	1	
	G01	REM-MD Evidence Type = "SubmissionAcceptanceRejection"	1	
	G02	REM Event	1	
	G03	Reason code	0..N	
	G04	REM-MD Evidence Version	1	
	G05	Event Time	1	
	G06	Transaction log information	0..N	
	R01	Evidence issuer Policy Identifier	1..N	
	R02	Evidence issuer Details	1	
	R03	Signature by issuing REM-MD	1	
	I00	Sender's details	0..1	
	I01	Recipient's details	0..N	
	I03	Recipient referred to by the Evidence	0..1	
	M00	REM-MD Message/REM Dispatch details	1	
	M01	Reply-to	0..1	

5.2   REM-MD Evidence Components

5.2.1   REM-MD Evidence Components Template

This clause provides a generic template for REM-MD Evidence Components.

Applications that implement REM-MD functions SHALL process for each REM-MD Evidence the components indicated in clause 5.1 and MAY process other components.

Component Class		Id	Component
REM-MD Evidence	Core Components	G00	REM-MD Evidence Identifier
		G01	REM-MD Evidence Type
		G02	REM Event
		G03	Reason code (see note below) NOTE: Preferably there would be only one (when applicable) G03 listing all remarked exceptions reason codes, but it cannot be excluded that one single message collects more than one G03.
		G04	REM-MD Evidence Version
		G05	Event Time
		G06	Transaction log information
	REM-MD Components	R01	Evidence issuer Policy Identifier
		R02	Evidence issuer Details
		R03	Signature by issuing REM-MD
	Identity Related Components	I00	Sender's details
		I01	Recipient's details
		I02	Recipient's delegate details
		I03	Recipient referred to by the Evidence
		I04	Sender Authentication details
		I05	Recipient Authentication details
	Messaging Components	M00	REM-MD Message/REM Dispatch details
		M01	Reply-to
		M02	Notification Message Tag
		M03	Message Submission Time
		M04	Forwarded to external system
	Extended	Enn	Space for private or public extensions to be added in the future by a set of users or by standardization bodies

Figure 2: REM-MD Evidence generic template

NOTE: Private or public Components, as well as additional Groups, may be added as extensions by a set of users or by standard bodies. These Components SHALL not be CRITICAL outside the relevant domain.

5.2.2   Components description

5.2.2.1   Core Components

5.2.2.1.1   G00 - REM-MD Evidence Identifier

Description	This field specifies a unique identifier for REM-MD Evidence within the issuing REM-MD.
Format	Text.
Meaning	Used to keep track of issued REM-MD Evidence, for possible later retrieval.
Note	

5.2.2.1.2   G01 - REM-MD Evidence Type

Description	This field specifies the type of the REM-MD Evidence. The evidence type must be unambiguously identified.
Format	The identification of the type of evidence strongly depends on the syntax selected for encoding such evidence. Annexes A, B and C specify formats for evidences in different syntaxes and provide details on how this identification is performed.
Meaning	The REM-MD Evidence belongs to the given type.
Note	

5.2.2.1.3   G02 - REM Event

Description	This field specifies the REM event (as in TS 102 640-1 [i.2], clause 6.2) in front of which the REM-MD Evidence has been issued.
Format	The identification of the event reported by the evidence strongly depends on the syntax selected for encoding such evidence. Annexes A, B and C specify formats for evidences in different syntaxes and provide details on how this identification is performed. Values from table in clause 5.2.3.2.
Meaning	The event belongs to the given type.
Note	

5.2.2.1.4   G03 - Reason code

Description	This field indicates a Reason code for further specifying the event which caused the issuance of the REM-MD Evidence.
Format	The identification of the reason reported by the evidence strongly depends on the syntax selected for encoding such evidence. Annex D shows a table with the encodings of the identified reasons for the different syntaxes. Values from table in clause 5.2.3.3.
Meaning	Reason code(s) are typically associated to a negative event (failure to deliver, rejection, …) Reason Codes specified in clause 5.2.3.3. Reason clauses are to be used.
Note	A single REM-MD Evidence may allow for more reason code components.

5.2.2.1.5   G04 - REM-MD Evidence Version

Description	This field specifies the version of the standard to which the REM-MD Evidence adheres.
Format	Text.
Meaning	Used to keep track of REM-MD Evidence version.
Note	A reference to the relevant ETSI standard version SHOULD be used.

5.2.2.1.6   G05 - Event Time

Description	This field specifies the time on which the REM-MD Evidence has been produced by the REM-MD.
Format	DATE TIME.
Meaning	Date and time when the REM-MD Evidence has been produced.
Note	

5.2.2.1.7   G06 - Transaction log information

Description	This field contains the log of all SMTP related events regarding the specific event to which the containing REM-MD Evidence refers to.
Format	Free text, depending on the applicable Policy.
Meaning	This field contains a list of log records related to the implementation of the event addressed by the containing REM-MD Evidence. These records are the ones required by, and are formatted as per, the applicable Policy.
Note	If more Policies are to be complied with, each requiring a specific log content and format, multiple instances of G06 are possible.

5.2.2.2   REM-MD Components

5.2.2.2.1   R01 - Evidence issuer Policy Identifier

Description	This field specifies the Identifier of one Policy that applies to the related REM-MD Evidence issuance.
Format	one of the widespread formats used for identification: OID or URI.
Meaning	This field indicates the Identifier of the Policy under which the REM-MD operates. It may be a Policy common to an entire REM Policy Domain, or a Policy specific to the related REM-MD, or any other applicable Policy.
Note	Multiple instances of G04 are possible where more Policies are applicable to the REM-MD Evidence at issue, for example: 1) a REM-PD Policy; 2) a REM-MD specific Policy; 3) a Policy applicable to the exchange of REM-MD Messages/REM Dispatches between the issuing REM-MD and the REM-MD to the environment of which the REM-MD Evidence will be forwarded.

5.2.2.2.2   R02 - Evidence Issuer Details

Description	This field specifies several details of the REM-MD Evidence issuer.
Format	Structured.
Meaning	REM-MD Evidence Issuer Commercial information, like commercial name, address, etc.
Note	This name must be the one under which the Sender's REM-MD is registered at the relevant Authority, be it the Chamber of Commerce or the Authority governing the REM-PD.

5.2.2.2.3   R03 - Signature by issuing REM-MD

Description	If present, this field contains the Signature issued by the REM-MD or by an external Signature Provider.
Format	Details provided in clause 6 REM Signatures.
Meaning	Signature issued by the REM-MD or its provider on the REM-MD Evidence.
Note	1) This signature on the REM-MD Evidence, where present, would be additional to the S/MIME signature over the entire REM-MD Message/REM Dispatch that SHALL always be present. It is required if the REM-MD Evidence is to be exhibited separately from the REM-MD Message/REM Dispatch it belongs to. 2) If this signature is generated by an external provider on behalf of the REM-MD, in the signing certificate either the subject SHALL specify the related REM-MD, or an extension SHALL assert that the signature was issued by the Provider on behalf of that REM-MD. In other words a reliable information on what is the REM-MD responsible for the issuance of the evidence SHALL be specified. 3) The signature format can be any of the above, thus the REM-MD application that receives a REM-MD Evidence SHALL be able to handle all of them.

5.2.2.3   Identity Components

5.2.2.3.1   I00 - Sender's details

Description	This field specifies the Sender's details.
Format	Structured.
Meaning	Sender's mailbox identifier and any other information related to sender's identity as defined in the applicable Policy Identifier. Includes: • Electronic address (mandatory). • Postal address (optional). • Digital certificate info (optional). • Signature detail (optional).
Note	The sender's identity will be provided as defined in the Policy the related REM-MDs, or REM-PD, abide by. For example it can be name and surname, or social security ID, or fiscal code. The mailbox identifier should be the one under which the sender has been authenticated by the REM-MD at issue.

5.2.2.3.2   I01 - Recipient's details

Description	This field specifies the recipient's details.
Format	Structured.
Meaning	recipient's mailbox identifier and any other information related to recipient identity as defined in the applicable Policy Identifier. Includes: • Electronic address (mandatory). • Postal address (optional). • Digital certificate info (optional). • Signature detail (optional).
Note	The recipient's identity will be provided as defined in the Policy the related REM-MDs, or REM-PD, abide by. For example it can be name and surname, or social security ID, or fiscal code. The mailbox identifier should be the one under which the recipient has been authenticated by the REM-MD at issue.

5.2.2.3.3   I02 - Recipient's delegate details

Description	This field specifies the recipient's delegate details.
Format	Structured.
Meaning	In case the recipient's REM-MD allows for delegation, this component will be used to provide recipient's delegate mailbox identifier and any other information related to recipient's delegate identity as defined in the applicable Policy Identifier. Includes: • Electronic address (mandatory). • Postal address (optional). • Digital certificate info (optional). • Signature detail (optional).
Note	The recipient's delegate identity will be provided as defined in the Policy the related REM-MDs, or REM-PD, abide by. For example it can be name and surname, or social security ID, or fiscal code. The mailbox identifier should be the one under which the recipient has been authenticated by the REM-MD at issue.

5.2.2.3.4   I03 -Recipient referred to by the Evidence

Description	This component indicates the REM-MD Message/REM Dispatch recipient, among the various ones indicated via I03, the REM-MD Evidence refers to.
Format	Integer.
Meaning	When several recipients are defined in the REM-MD Evidence (several I03 components will be present), this component is used to indicate which of them is the one the REM-MD Evidence refers to.
Note	

5.2.2.3.5   I04 - Sender Authentication details

Description	Information on Sender's authentication.
Format	Structured.
Meaning	This component provides information on sender's authentication, including authentication mechanism.
Note	Represent the following classes of authentication: a) Basic: Using basic authentication mechanisms such as passwords; or b) Enhanced: Using enhanced authentication such two factor authentication mechanisms linked to a one time password; or c) AdES: Using advanced electronic signatures; or d) AdES-Plus: Using advanced electronic signatures issued by means of Secure Signature Creation Devices (as defined in Directive 1999/93/EC [1]) or equivalent secure cryptographic device; e) QES: Using advanced electronic signatures issued by means of Secure Signature Creation Devices and supported by Qualified Certificates (as defined in Directive 1999/93/EC [1]). NOTE: See also TS 102 640-3 [i.3], clause 6.3 on "Sender / Recipient Authentication". The default class of authentication is Basic. In case authentication mechanism has value of c), d) e) the sender's PKCS#7 detached (*.p7s) MUST be present. In case authentication mechanism has value a) the sender's UID MAY be added. Extensibility fields may be used to enable the REM-MD to include any. other relevant details of the authentication used.

5.2.2.3.6   I05 - Recipient Authentication details

Description	Information on recipient's authentication.
Format	Structured.
Meaning	This component provides information on recipient's authentication, including authentication mechanism.
Note	Represent the following classes of authentication: a) Basic: Using basic authentication mechanisms such as passwords; or b) Enhanced: Using enhanced authentication such two factor authentication mechanisms linked to a one time password; or c) AdES: Using advanced electronic signatures; or d) AdES-Plus: Using advanced electronic signatures issued by means of Secure Signature Creation Devices (as defined in Directive 1999/93/EC [1]) or equivalent secure cryptographic device; e) QES: Using advanced electronic signatures issued by means of Secure Signature Creation Devices and supported by Qualified Certificates (as defined in Directive 1999/93/EC [1]). NOTE: See also TS 102 640-3 [i.3], clause 6.3 on "Sender / Recipient Authentication"). The default class of authentication is Basic. In case authentication mechanism has value of c), d) e) the sender's PKCS#7 detached (*.p7s) MUST be present. In case authentication mechanism has value a) the sender's UID MAY be added. Extensibility fields may be used to enable the REM-MD to include any other relevant details of the authentication used.

5.2.2.4   Messaging Components

5.2.2.4.1   M00 - REM-MD Message/REM Dispatch details

Description	REM-MD Message/REM Dispatch details, including Message identifier.
Format	Structured.
Meaning	Message info, like message Id, message subject, etc.
Note	An identifier, based on the hash computed as indicated in the subsequent numbered items list, is created by the sender's REM-MD to be added to all REM-MD Evidences, except in the evidence described in clause 5.1.9, in which case the identifier is created by the Recipient's REM-MD. The hashing algorithm SHALL be specified (e.g. "SHA-1", "SHA256") Indications in TS 102 176-1 [5] is to be taken as a reference as regards the hashing algorithm. 1) **When conveying the Original Message**: the hash is computed over the entire Original Message, attachments included, to ensure a tight coupling between the Original Message itself and all other information related to all related REM-MD Messages/REM Dispatches. 2) **When conveying a notification:** the hash is computed over the concatenation of the text of the notification message and the entire stored Original Message. This mechanism is RECOMMENDED for three years effective from the publication date of the present document. After this interim period this mechanism SHALL be implemented. This interim period has the purpose to provide existing REM implementations, that do not build this Identifier based on this digest, sufficient time to implement this provision.

5.2.2.4.2   M01 - Reply-to

Description	Message Reply-to header.
Format	e-mail address in text.
Meaning	Message reply-to header, as in the original message.
Note	

5.2.2.4.3   M02 - Notification Message Tag

Description	Notification Tag.
Format	Boolean, 'true' for notification 'false' for not notification.
Meaning	This tag specifies whether the associated message includes the Original Message, or it is a notification message with a reference to the Original Message.
Note	

5.2.2.4.4   M03 - Message Submission Time

Description	This field specifies the message submission time.
Format	DATE TIME.
Meaning	Date and time when the sender submitted the original message.
Note	This field may differ from Event Time in SubmissionAcceptanceRetrieval REM-MD Evidence, since message submission does not necessarily coincide with message acceptance/refusal.

5.2.2.4.5   M04 - Forwarded to external system

Description	This component is used when the message is forwarded to a system outside the REM borders.
Format	Text.
Meaning	Provides a description of the external system to which the message has been forwarded (non REM e-mail system, ordinary paper mail system, etc.).
Note	

5.2.3   REM-MD Evidence Components formats and values

REM-MD Evidence Data Elements are elementary pieces of information used to make up the REM-MD Evidence Components.

5.2.3.1　Free text

Information in free text SHALL be written in UK English. Text in other languages MAY be added.

5.2.3.2　Events

In accordance with TS 102 640-1 [i.2], clause 6.2.

Table 1

Events
S-REM-MD Acceptance
S- REM-MD Rejection
R-REM-MD Acceptance
R-REM-MD Rejection
Expiration of time to deliver to R-REM-MD
REM-MD Message / REM Dispatch Delivery
Expiration of time to deliver REM-MD Message / REM Dispatch
Download
Expiration of time for download
Download by a recipient's delegate
Retrieval
Expiration of time for Retrieval
Retrieval by a recipient's delegate
Rejection of download by recipient
Successful forwarding for Ordinary e-mail
Unsuccessful forwarding for Ordinary e-mail
Successful forwarding for Printing
Unsuccessful forwarding for Printing
Message received from a regular e-mail system

5.2.3.3　Reasons

Appropriate codes for reasons will be provided in annexes A, B and C.

5.2.3.3.1　Reasons related to Sender's Submission

Table 2

Reason
Message accepted
Invalid message format
Malware found in REM-MD Message/REM Dispatch
Invalid sender's signature format
Sender's signing certificate expired or revoked
Sender's REM-PD or REM-MD policy violation, e.g.: max message size exceeded, invalid attachment formats, etc.
Other

5.2.3.3.2   Reasons related to the Relay to the recipient's REM-MD

Table 3

Reason
REM-MD Message/REM Dispatch successfully delivered to, and accepted by, the Recipient's REM-MD
REM-MD Message/REM Dispatch successfully delivered to, but rejected by, the Recipient's REM-MD for: Invalid message format
REM-MD Message/REM Dispatch successfully delivered to, but rejected by, the Recipient's REM-MD for: Malware found in REM-MD Message/REM Dispatch
REM-MD Message/REM Dispatch successfully delivered to, but rejected by, the Recipient's REM-MD for: Invalid message signature format
REM-MD Message/REM Dispatch successfully delivered to, but rejected by, the Recipient's REM-MD for: Signing certificate expired or revoked
REM-MD Message/REM Dispatch successfully delivered to, but rejected by, the Recipient's REM-MD for: Recipient's REM-PD or REM-MD policy violation, e.g.: max message size exceeded, invalid attachment formats, sender's REM-MD (or regular e-mail server) non accepted
REM-MD Message/REM Dispatch non delivered to the Recipient's REM-MD for: Recipient's REM-MD malfunction
REM-MD Message/REM Dispatch non delivered to the Recipient's REM-MD for: Recipient's REM-MD not identified in the Internet
REM-MD Message/REM Dispatch non delivered to the Recipient's REM-MD for: Recipient's REM-MD unreachable
REM-MD Message/REM Dispatch non delivered to the Recipient's REM-MD for: Unknown Recipient
Other

5.2.3.3.3   Delivery/download related reasons

Table 4

Reason
REM-MD Message/REM Dispatch successfully delivered to /downloaded by | the recipient
REM-MD Message/REM Dispatch successfully delivered to /downloaded by | a recipient's delegate
The sender's REM-MD received within a given period no information on delivery from the recipient's REM-MD
Invalid REM-MD Message/REM Dispatch format
Malware found in REM-MD Message/REM Dispatch
Mailbox full
Technical malfunction
Attachment formats non accepted
REM-MD Message/REM Dispatch rejection by the Recipient
Retention period expired without downloading / successful delivery
Other

5.2.3.3.4   Retrieval reasons

Table 5

Reason
REM-MD Message/REM Dispatch successfully retrieved by the recipient
REM-MD Message/REM Dispatch successfully retrieved by a recipient's delegate
Invalid REM-MD Message/REM Dispatch format
Malware found in REM-MD Message/REM Dispatch
Technical malfunction
Attachment formats non accepted
Retention period expired without retrieval
Other

5.2.3.3.5   Reasons related to forwarding REM Message to a non REM external system

Table 6

Reason
Successful
Regular e-mailing system unreachable
Regular e-mailing system non operational
Regular e-mailing system rejected submission
NOTE: Reason codes provided by the e-mailing system can be specified.
Printing system unreachable
Printing system non operational
Printing buffer full
Other

6   REM Signatures

Clauses above have discussed the structure of the REM-MD Messages/REM Dispatches and the range of REM-MD Evidences suitable to uphold certain assertions, which are provided to the users in addition to the services provided by ordinary e-mail systems.

This clause focuses on the usage of electronic signatures within REM-MD Messages/REM Dispatches.

Clause 6.1 identifies the different types of electronic signatures that may appear within the REM-MD Messages/REM Dispatches, and general rules that govern their presence within one REM-MD Message/REM Dispatch.

Clause 6.2 specifies common requirements on all the types of signatures within a REM-MD Message/REM Dispatch.

Clause 6.3 specifies requirements on signatures applied to individual REM-MD Evidence objects within a REM-MD Message/REM Dispatch.

Clause 6.4 specifies requirements on signatures placed in the REM-MD Message/REM Dispatch to protect all the parts of a REM-MD Message/REM Dispatch including the Original Message and REM-MD Evidence objects added.

6.1   Electronic signatures within REM-MD Messages/REM Dispatches

Within a REM-MD Message/REM Dispatch the following electronic signatures may appear:

- Signatures generated by a REM-MD or by the delegated entity on individual REM-MD Evidence.

- S/MIME signature protecting all the MIME parts (including not only REM-MD Evidences) that constitute a REM-MD Message/REM Dispatch. This signature is generated by a REM-MD.

Senders MAY sign the original message submitted to the recipient, supporting the signature with their certificates - qualified or not qualified. These signatures are outside of the scope of the present document.

If a REM-MD Message/REM Dispatch contains REM-MD Evidences, these have to be signed by the REM-MD in charge of generating them. This may be done by individually signing each REM-MD Evidence and make these signatures part of the REM-MD Evidences themselves or by generating a S/MIME signature on all the parts of the REM-MD Message/REM Dispatch. The present document does not preclude the co-existence of both types of signatures, as the first one secures the REM-MD Evidences and the second one also secures other parts of the REM-MD Message/REM Dispatch.

If a REM-MD Message/REM Dispatch contains references to a REM-MD Repository within a REM-MD, then the REM-MD generating the REM-MD Message/REM Dispatch will generate an S/MIME signature on all the parts of the REM-MD Message/REM Dispatch. REM-MD Evidences may also be individually signed.

6.2 Common Requirements on Signatures

The following requirements apply to all type of signatures applied by the REM-MD:

1) Electronic signatures MUST be Advanced Electronic Signatures (AdES) as per specifications TS 101 903 (XAdES) [4] or TS 101 733 (CAdES) [3].

2) These electronic signatures MAY include a signed property containing the explicit identifier of the Electronic Signature Policy governing the signing and verifying processes.

   It is recommended, however, that signature policy requirements, or the signature policy identifier, be included in REM Practice Statement (see TS 102 640-3 [i.3], clause 6.1).

3) These electronic signatures MUST include a signed property containing the signing time claimed by the REM-MD.

NOTE: All the REM-MD Evidences carry one or more date and time elements. If the REM-MD signature is known to be valid the REM-MD Evidence signer's time indications may also be trusted. This time should not, however, be used to check signature validity.

4) These electronic signatures MUST include a signed property protecting the signing certificate.

5) Once generated a signature time-stamp MAY be computed and added to these electronic signatures.

6.3 Requirements on Signatures Applied to REM-MD Evidence

The following clauses specify requirements for signature applied to REM-MD Evidence objects for the three data formats supported: XML, ASN.1 and PDF applying the common requirements in the context of specific data formats.

6.3.1 XML Signatures

The following requirements apply to XML Signatures applied to REM-MD Evidence encoded in XML:

1) The signature MUST be an XML Advanced Electronic Signature as specified in TS 101 903 (XAdES) [4].

2) The signature MUST be an enveloped signature as specified in clause 10 of W3C Recommendation for XML Signature syntax and Processing [7].

3) Signature Policy employed MAY be identified in the property `SignaturePolicyIdentifier`.

4) The signing certificate MUST be protected. It is RECOMMENDED that this be achieved using the XAdES attribute xades:SigningCertificate. However, this MAY be achieved by ds:KeyInfo/X509Data/X509Certificate present AND ds:KeyInfo included in the signature.

5) The signature MUST include `xades:SigningTime`.

6) The signature may include a time-stamp of the signature in `xades:SignatureTimeStamp`.

6.3.2 ASN.1 Signatures

The following requirements apply to Signatures applied to REM-MD Evidence encoded in ASN.1:

1) The signature MUST be an Advanced Electronic Signature as specified in TS 101 733 (CAdES) [3].

2) The signature MUST be an "`Enveloping with data`" signature as specified in clause 5.2 of RFC 3852 Cryptographic Message Syntax [2].

3) The signature policy employed MAY be identified in the `signature-policy-identifier` signed attribute.

4) The signing certificate MUST be protected using signed attribute `ESS-signing-certificate-v2` as defined in TS 101 733 [3].

5) The signature MUST include signed attribute `signing-time`.

6) The signature may include a time-stamp of the signature in the Unsigned attribute `signature-time-stamp.`

6.3.3   PDF Signatures

It is recommended that PDF documents are protected by signatures employing CAdES signatures as defined in clause 6.3.2, carried within a SIG object as defined in clause 12.8 of ISO 32000-1 [i.8].

NOTE: Profiles for the used of Advanced Electronic Signatures in PDF are under development in ETSI.

6.4   Electronic signatures on REM-Message

Signatures applied to REM-MD Messages/REM Dispatches to protect all parts of the message shall meet the following requirements:

1) The signature MUST be placed in the message using S/MIME multipart/signed as defined in RFC 2311 [8].

The signature MUST be encoded.

Annex A (normative):
REM-MD Evidence Implementation in ASN.1

This annex defines the syntax for REM-MD Evidence when ASN.1 is used.

This clause specifies the ASN.1 structures to be used when implementing an ASN.1-version of the evidences.

The ASN.1 syntax used in this annex is the 1988 version, as defined by ITU-T Recommendations X.680-683 [10] with the addition of "UTF8String" type imported from the hybrid ASN.1 module of RFC 5280 [14]. These additions are imported so as to enhance interoperability by avoiding ambiguity concerning signature algorithms and digest calculation. The following schema requires the use of a "relaxed compiler" to accommodate these two special types.

The ASN.1 in this annex may be converted into the 1997 syntax by using the Information Object Classes introduced by that version to replace the type "ANY DEFINED BY" (this type not being supported by the 1997 version) and removing the importation of "UTF8String" type, plus amending the module header appropriately.

The ASN.1 implementation of the evidences must be encoded by using the Distinguished Encoding Rules defined by ITU-T Recommendation X.690 [11].

The header of the ASN.1 module is specified as follows.

```
-REM-v1-88syntax { itu-t(0) identified-organization(4) etsi(0)
  tsl-specification (1234) id-mod(0) v1-88syntax (1) }
DEFINITIONS EXPLICIT TAGS ::=

BEGIN

-- EXPORTS All
IMPORTS
  -- Internet X.509 Public Key Infrastructure - Certificate and CRL Profile: RFC
  Extensions
    FROM PKIX1Explicit88 { iso(1) identified-organization(3) dod(6) internet(1)
      security(5) mechanisms(5) pkix(7) id-mod(0) id-pkix1-explicit(18) }
  -- Cryptographic Message Syntax (CMS): RFC 3852
  ContentInfo
    FROM CryptographicMessageSyntax2004 { iso(1) member-body(2) us(840) rsadsi(113549)
      pkcs(1) pkcs-9(9) smime(16) modules(0) cms-2004(24) }
  -- Provision of harmonized Trust-service status information (TSL) - ETSI TS 102 231 V2.1.1
  NonEmptyURI, MultiLangString, MultiLangAddress, ElectronicAddresses
    FROM ETSI-TSL-v2-88syntax { itu-t(0) identified-organization(4) etsi(0)
      tsl-specification (2231) id-mod(0) v2-88syntax (1) }
  -- AFNOR - AuthorizedCertificate
  AuthorizedCertificate
    FROM EEvidencesCommon { iso(1) member-body(2) fr(250) type-org(1)
      aFNORStandardisation(127) letter(26) standard(74600) asn1-modules(3) common(0) }
;
```

Clause A.1 defines the general structure for REM-MD Evidences and provides details for their elements.

Clause A.2 specifies the different types of REM-MD Evidences as defined in clause 5.1.

A.1   REM-MD Evidence Structure

Clause 5.2.1 shows a template for REM-MD Evidence. The present clause defines the ASN.1 syntax for REM-MD Evidences.

Below follows the root for all the OIDs defined in the present document.

```
id-rem OBJECT IDENTIFIER ::= { ETSI-REM-v1-88syntax }
```

Below follows the asn1 definition for REM-MD Evidences.

```
REMEvidence ::= SEQUENCE {

    version                             Version,
    eventCode                           INTEGER OPTIONAL,
    eventReasons                        EventReasons OPTIONAL,
    evidenceIdentifier                  UTF8String (SIZE (1..MAX)),
    evidenceIssuerPolicyID              PolicyIdentifier OPTIONAL,
    evidenceIssuerDetails               EntityDetails,
    senderAuthenticationDetails     [0] AuthenticationDetails OPTIONAL,
    recipientAuthenticationDetails  [1] AuthenticationDetails OPTIONAL,
    eventTime                           GeneralizedTime,
    submissionTime                      GeneralizedTime OPTIONAL,
    replyTo                             UTF8String OPTIONAL,
    senderDetails                       UserDetails,
    recipientsDetails                   UserDetails OPTIONAL,
    recipientsDelegatesDetails      [2] RecipientsDelegatesDetails OPTIONAL,
    evidenceRefersToRecipient       [3] INTEGER OPTIONAL,
    messageDetails                  [4] MessageDetails OPTIONAL,
    notificationDetails             [5] MessageDetails OPTIONAL,
    forwardedToExternalSystem       [6] UTF8String OPTIONAL,
    transactionLogInformation       [7] TransactionLogInformation OPTIONAL,
    extensions                      [8] Extensions OPTIONAL

}
```

Field version for the present document is as follows:

```
Version ::= INTEGER { v1(1) }
```

Clauses below further develop the elements of a REM-MD Evidence.

A.1.1   Field eventCode

This field has the semantics of G02 data element as specified in clause 5.2.2.1.3. Its content is an integer.

The present document has identified a number of events, whose identifiers are defined below.

1) Acceptance of some REM-MD Message/REM Dispatch by some entity.

2) Rejection of some REM-MD Message/REM Dispatch by some entity.

3) Delivery of some REM-MD Message/REM Dispatch to some entity.

4) Non delivery of some REM-MD Message/REM Dispatch to some entity within a certain period of time.

5) Download of some REM-MD Message/REM Dispatch by recipient or recipient's delegate from a REM's REM-MD Repository.

6) No download of some REM-MD Message/REM Dispatch by recipient or recipient's delegate from a REM's REM-MD Repository within a certain period of time.

7) Retrieval of some REM-MD Message/REM Dispatch by recipient from recipient's mailbox.

8) Non retrieval of some REM-MD Message/REM Dispatch by recipient from recipient's mailbox within a certain period of time.

9) Rejection of download of a message by recipient.

10) Forward of REM-MD Message/REM Dispatch to a regular e-mail system.

11) Forward of REM-MD Message/REM Dispatch to a printing system to be subsequently sent via physical registered mail.

12) Reception of a message from a regular e-mail system.

A.1.2 Field eventReasons

This field has the semantics of G03 data element as specified in clause 5.2.2.1.4.

It is an instance EventReasons type, which is defined below.

```
EventReasons ::= SEQUENCE SIZE (1..MAX) OF {
    eventReason EventReason
}
EventReason ::= SEQUENCE {
    code    INTEGER,
    details UTF8String OPTIONAL,
}
```

Field eventReasons contains a list of eventReason elements.

eventReason's field code contains the reason code as an integer. Annex D of the present document shows the codes for event reasons already identified by the present document.

eventReason's optional field details contain a string with additional details.

A.1.3 Field evidenceIssuerPolicyID

This field has the semantics of R01 data element as specified in clause 5.2.2.2.1. It is an instance PolicyIdentifier type, which is defined below.

```
PolicyIdentifier ::= CHOICE {
    oid    OBJECT IDENTIFIER,
    uri    NonEmptyURI }
```

The content of this field will be a choice between an OID and an URI, as both mechanisms may be used for identifying a policy.

Field oid, if present, shall contain an OID and field uri, if present shall contain an URI.

A.1.4 Field evidenceIdentifier

This field has the semantics of G00 data element as specified in clause 5.2.2.1.1. It contains a unique identifier of the REM-MD Evidence for the REM-MD Evidence Issuer.

All the REM-MD Evidences generated by a certain REM-MD Evidence Issuer must have different identifiers. The present document does not specify any further restriction on the values of this element.

A.1.5 Field evidenceIssuerDetails

This field has the semantics of R02 data element as specified in clause 5.2.2.2.2. It is an instance of EntityDetails type, which is defined below.

```
EntityDetails ::= SEQUENCE {
    entityName              MultiLangString,
    postalAddress           MultiLangAddress,
    unitName            [1] MultiLangString OPTIONAL,
    electronicAddress   [2] ElectronicAddresses OPTIONAL
}
```

Field entityName contains the Name of the entity, as specified in TS 102 231 [6].

Field postalAddress contains the postal address of the entity, as specified in TS 102 231 [6].

Optional field unitName, if present, contains the name of the Unit within the entity, as specified in TS 102 231 [6].

Optional field `electronicAddress`, if present, contains the e-mail address of the entity.

A.1.6 Field `senderAuthenticationDetails`

This field has the semantics of I04 data element as specified in clause 5.2.2.3.5. It is an instance `AuthenticationDetails` type, which is defined below.

```
AuthenticationDetails ::= SEQUENCE {
    authenticationTime          GeneralizedTime,
    authenticationMethod        INTEGER,
    additionalDetails           AdditionalDetails OPTIONAL
}
AdditionalDetails ::= SEQUENCE SIZE (1..MAX) OF ContentInfo
```

Field `authenticationTime` indicates the time when the sender was authenticated.

Field `authenticationMethod` contains info on the method used for authenticating the sender. The following methods and codes have already been identified:

- `"1"`. Basic: Using basic mechanisms such as passwords.

- `"2"`. Enhanced: Using enhanced authentication such two factor mechanisms linked to a one time password.

- `"3"`. AdES: Using advanced electronic signatures.

- `"4"`. AdES-Plus: Using advanced electronic signatures with Secure Signature Creation Devices (as defined in Directive 1999/93/EC [1]) or equivalent secure cryptographic device.

- `"5"`. QES: Using advanced electronic signatures with Secure Signature Creation Devices and Qualified Certificates (as defined in Directive 1999/93/EC [1]).

Optional field `additionalDetails` contains additional details on the authentication process. It may contain, for instance, the token presented by the sender to the sender's REM-MD. If signature has been used for authentication, one of the elements of the sequence may be the sender's signature itself.

A.1.7 Field `recipientAuthenticationDetails`

This field has the semantics of I05 data element as specified in clause 5.2.2.3.6. It is an instance of type `AuthenticationDetails`.

A.1.8 Field `eventTime`

This field has the semantics of G05 data element as specified in clause 5.2.2.1.6. It is an instance of `GeneralizedTime`.

A.1.9 Field `submissionTime`

This field has the semantics of M03 data element as specified in clause 5.2.2.4.4. It is an instance of `GeneralizedTime`.

A.1.10 Field `replyTo`

This field has the semantics of M01 data element as specified in clause 5.2.2.4.2.

A.1.11 Field `senderDetails`

This field has the semantics of I00 data element as specified in clause 5.2.2.3.1. It is an instance of `UserDetails` type, which is defined below.

```
UserDetails ::= SEQUENCE {
    electronicAdress            ElectronicAddresses,
    postalAddress           [1] MultiLangAddress OPTIONAL,
    certificateDetails          AuthorizedCertificate OPTIONAL
}
```

Field `electronicAddress` contains details of sender's electronic mail address. See TS 102 231 [6] for details.

Field `postalAddress` contains details of sender's postal address. See TS 102 231 [6] for details.

Element `certificateDetails` in field AuthorizedCertificate contains details of the user's certificate. See [15] for details.

A.1.12 Field `recipientsDetails`

This field has the semantics of I01 data element as specified in clause 5.2.2.3.2. It is an instance of `UserDetails` type.

A.1.13 Field `recipientsDelegatesDetails`

This element has the semantics of I02 data element as specified in clause 5.2.2.3.3. It is an instance of `UserDetails` type, which is defined below.

```
RecipientsDelegatesDetails ::= SEQUENCE SIZE (1..MAX) OF RecipientsDelegateDetails

RecipientsDelegateDetails ::= SEQUENCE {
    delegateDetails         UserDertails,
    delegatingRecipients    ListOfIntegers
}

ListOfIntegers ::= SEQUENCE SIZE (1..MAX) OF INTEGER
```

`RecipientsDelegateDetails`'s `delegateDetails` field contains the details of the delegate in question.

`RecipientsDelegateDetails`'s `delegatingRecipients` field contains a list of integers that identify the recipients that have delegated in this entity. First Recipient in `recipientsDetails` is assigned number 1. If this element is absent, then the delegate will act as delegated of all the recipients.

A.1.14 Field `evidenceRefersToRecipient`

This field has the semantics of I03 data element as specified in clause 5.2.2.3.4. Its value references one of the recipients in `recipientsDetails` field. First recipient in the list of recipients is assigned number 1.

A.1.15 Field `messageDetails`

This element has the semantics of M00 data element as specified in clause 5.2.2.4.1. It is an instance of `MessageDetails` type, which is defined below.

```
MessageDetails ::= SEQUENCE {
    isNotification                  BOOLEAN,
    messageSubject                  UTF8String,
    uaMessageIdentifier         [1] UTFS8tring OPTIONAL,
    messageIdentifierByREMMD     [2] UTFS8tring,
    hashAlgorithm                   OBJECT IDENTIFIER OPTIONAL,
    hash                            BIT STRING OPTIONAL
}
```

`isNotification` indicates whether the message whose details are provided is a REM Notification or not.

Optional `messageSubject`'s content is the value of the Subject field of the referred message.

Optional `uaMessageIdentifier` field contains an identifier as computed by the user's UA.

Element `messageIdentifierByREMMD` contains an identifier computed by a REM-MD. This identifier shall be unique for this REM-MD.

Finally, `hashAlgorithm` and `hash` contain the referred message's digest algorithm and the digest value identifier respectively.

A.1.16 Field `forwardedToExternalSystem`

This field the semantics of M04 data element as specified in clause 5.2.2.4.5.

A.1.17 Field `transactionLogInformation`

This field has the semantics of G06 data element as specified in clause 5.2.2.2.3. It provides a placeholder that issuers of evidences may use for including pieces of the log file content within them.

It is an instance of `TransactionLogInformation` type, which is defined below.

```
TransactionLogInformation ::= SEQUENCE SIZE (1..MAX)OF {
    transactionLog  UTF8String
}
```

Field `transactionLogInformation` contains a sequence of `transactionLog` elements, each one containing an instance of log information.

A.1.18 Field `extensions`

This element has the semantics of Enn data element. This element is a placeholder for further standardized or private extensions.

A.2   REM-MD Evidences

All the evidences specified in clause 5.1 of the present document will be instances of `EncapsulatedContentInfo` type as defined in RFC 3852 [2].

The `eContentType` field identifies the type of evidence as shown below.

```
id-rem-evidenceTypes OBJECT IDENTIFIER ::= { id-rem 1 }

id-rem-evidenceTypes-summbissionAcceptanceRejection OBJECT IDENTIFIER ::= { id-rem-evidenceTypes 1 }
-- OID for SubmissionAcceptanceRejection evidence as specified in 5.1.1

id-rem-evidenceTypes-relayREMMDAcceptanceRejection OBJECT IDENTIFIER ::= { id-rem-evidenceTypes 2 }
-- OID for RelayREMMDAcceptanceRejection evidence as specified in 5.1.2

id-rem-evidenceTypes-relayREMMDFailure OBJECT IDENTIFIER ::= { id-rem-evidenceTypes 3 } -- OID for
RelayREMMDFailure evidence as specified in 5.1.3

id-rem-evidenceTypes-deliveryNonDeliveryToRecipient OBJECT IDENTIFIER ::= { id-rem-evidenceTypes 4 }
-- OID for DeliveryNonDeliveryToRecipient evidence as specified in 5.1.4

id-rem-evidenceTypes-downloadNonDownloadByRecipient OBJECT IDENTIFIER ::= { id-rem-evidenceTypes 5 }
-- OID for DownloadNonDownloadByRecipient evidence as specified in 5.1.5

id-rem-evidenceTypes-retrievalNonRetrievalByRecipient OBJECT IDENTIFIER ::= { id-rem-evidenceTypes 6
} -- OID for RetrievalNonRetrievalByRecipient evidence as specified in 5.1.6

id-rem-evidenceTypes-acceptanceRejectionByRecipient OBJECT IDENTIFIER ::= { id-rem-evidenceTypes 7 }
-- OID for AcceptanceRejectionByRecipient evidence as specified in 5.1.7

id-rem-evidenceTypes-relayToNonREMSystem OBJECT IDENTIFIER ::= { id-rem-evidenceTypes 8 } -- OID for
RelayToNonREMSystem evidence as specified in 5.1.8

id-rem-evidenceTypes-receivedFromNonREMSystem OBJECT IDENTIFIER ::= { id-rem-evidenceTypes 9 } --
OID for ReceivedFromNonREMSystem evidence as specified in 5.1.9
```

The `eContent` field will be an encapsulated instance of `REMEvidence` type defined in clause B.1. Clauses below specify the contents of each type of evidence by defining further constraints for the different fields of `REMEvidence`.

Constraints are expressed in tables organized as follows:

- Column **Field** identifies the profiled field. Should an evidence could carry more than one instance of the same element, then the usual array syntax of an integer index within square brackets is used for enumerating the different instances. Array index numbering starts at 1.

- Column **Mandatory / Optional** specifies requirements on the field. The following codes may appear:

    - M: This means that the field is mandatory.

    - O: This means that presence or absence of the field is optional.

    - C: This means that the presence of the field depends on certain conditions that are further developed in column **Additional Profile Properties**.

- Column **Nbr. Occurrences** identifies the number of occurrences of the element.

- Column **Additional Profile Properties** specifies additional requirements on the field: values, conditions, etc. Terms shall, may and should used in these cells have the meaning as specified in TS 102 904 [16].

A.2.1   Evidence submissionAcceptanceRejection

The table below shows the contents of this element.

Field	Mand. Opt.	Number occurrences	Additional profile properties
Version	M	1	Value: "1" for this version
eventCode	M	1	Value if acceptance: "Acceptance" Value if rejection: "Rejection"
eventReasons	C	0..1	If value of eventCode is "Acceptance" then this element shall not appear. If value of eventCode is "Rejection" then one single instance of this element shall appear. The values of their eventReason children shall contain the codes identifying the reason(s) why the REM-MD rejected the message submitted by the sender.
evidenceIssuerPolicyID	O	0..1	
evidenceIdentifier	M	1	Value as computed by the Evidence issuer.
evidenceIssuerDetails	M	1	
senderAuthenticationDetails	C	0..1	If the sender has been authenticated by the REM-MD, then this element shall be present. Its contents will indicate the authentication process details. If the sender has not been authenticated by the REM-MD, then this element shall not be present.
eventTime	M	1	
submissionTime	M	1	
replyTo	O	0..1	
senderDetails	M	1	
recipientsDetails	C	0..1	If the evidence is generated for delegated entities only, then this element shall not appear. If the evidence is generated for recipients, then this element shall appear.
recipientsDelegatesDetails	C	0..1	If the evidence is generated for delegated entities only, then this element shall appear. If the evidence is generated for recipients only, then this element shall appear.
messageDetails	M	1	The contents of this element shall be as follows: messageSubject shall be present. uaMessageIdentifier may be present. messageIdentifierByREMMD shall be present. After the period mentioned in the normative part, hashAlgorithm and hash shall be present. Implementations may include it before the expiration of such a period Field isNotification shall be "false".
requiredReceiptType	C	0..1	Should messageDetails's hashAlgorithm and hash be present, this element shall not be present. Should messageDetails's hashAlgorithm and hash be not be present, this element shall be present. Field isNotification's value shall be "false".
transactionLogInformation	O	0..1	
Extensions	O	0..1	

A.2.2   Evidence RelayREMMDAcceptanceRejection

The table below shows the contents of this element.

Element / Attribute	Mand. Opt.	Number occurrences	Additional profile properties
Version	M	1	Value: "1" for this version
eventCode	M	1	Value if acceptance by recipient's REM-MD: "Acceptance" Value if rejection by recipient's REM-MD: "Rejection"
eventReasons	C	0..1	If value of eventCode is "Acceptance" then this element shall not appear. If value of eventCode is "Rejection" then one single instance of this element shall appear. The values of their eventReason children shall contain the codes identifying the reason(s) why the REM-MD rejected the message submitted by the sender.
evidenceIdentifier	M	1	Value as computed by the Evidence issuer.
evidenceIssuerPolicyID	O	0..1	
evidenceIssuerDetails	M	1	
eventTime	M	1	If recipient's REM-MD has accepted the message this element shall indicate when the acceptance occurred. If recipient's REM-MD has rejected the message this element shall indicate when the rejection occurred.
replyTo	O	0..1	
senderDetails	M	1	
recipientsDetails	C	0..1	If the evidence is generated for delegated entities only, then this element shall not appear. If the evidence is generated for recipients, then this element shall appear.
recipientsDelegatesDetails	C	0..1	If the evidence is generated for delegated entities only, then this element shall appear. If the evidence is generated for recipients only, then this element shall appear.
evidenceRefersToRecipient	C	0..1	If the evidence only refers to some recipient / delegate then this element shall appear. If the evidence refers to all the recipients / delegates then this element shall not appear.
messageDetails	M	1	The contents of this element shall be as follows: messageSubject shall be present. uaMessageIdentifier may be present. messageIdentifierByREMMD shall be present. After the period mentioned in the normative part, hashAlgorithm and hash shall be present. Implementations may include it before the expiration of such a period Field isNotification's value shall be "false".
requiredReceiptType	C	0..1	Should messageDetails's hashAlgorithm and hash be present, this element shall not be present. Should messageDetails's hashAlgorithm and hash be not be present, this element shall be present.
transactionLogInformation	O	0..1	
Extensions	O	0..1	

A.2.3   Evidence RelayREMMDFailure

The table below shows the contents of this element.

Element / Attribute	Mand. Opt.	Number occurrences	Additional profile properties
Attribute version	M	1	Value: "1" for this version
eventCode	M	1	For this evidence the value of this code is always: "DeliveryExpiration"
eventReasons	M	1	The values of their eventReason children shall contain the codes identifying the reason(s) why the sender's REM-MD could not delivery the message to recipient's REM-MD.
evidenceIdentifier	M	1	Value as computed by the Evidence issuer.
evidenceIssuerPolicyID	O	0..1	
evidenceIssuerDetails	M	1	
eventTime	M	1	This element will contain the message delivery expiration time.
replyTo	O	0..1	
senderDetails	M	1	
reipientsDetails	C	0..1	If the evidence is generated for delegated entities only, then this element shall not appear. If the evidence is generated for recipients, then this element shall appear.
reipientsDelegatesDetails	C	0..1	If the evidence is generated for delegated entities only, then this element shall appear. If the evidence is generated for recipients only, then this element shall appear.
evidenceRefersToRecipient	C	0..1	If the evidence only refers to some recipient / delegate then this element shall appear. If the evidence refers to all the recipients / delegates then this element shall not appear.
messageDetails	M	1	The contents of this element shall be as follows: messageSubject shall be present. uaMessageIdentifier may be present. messageIdentifierByREMMD shall be present. After the period mentioned in the normative part, hashAlgorithm and hash shall be present. Implementations may include it before the expiration of such a period Attribute isNotification shall be "false".
requiredReceiptType	C	0..1	Should messageDetails's hashAlgorithm and hash be present, this element shall not be present. Should messageDetails's hashAlgorithm and hash be not be present, this element shall be present. Field isNotification's value shall be "false".
transactionLogInformation	O	0..1	
Extensions	O	0..1	

A.2.4 Evidence DeliveryNonDeliveryToRecipient

The table below shows the contents of this element.

Element / Attribute	Mand. Opt.	Number occurrences	Additional profile properties
Attribute version	M	1	Value: "1" for this version
eventCode	M	1	Value if message (which may be a notification) has been delivered to recipient or recipient's delegates: "Delivery" Value if message (which may be a notification) has not been delivered to recipient or recipient's delegates: "DeliveryExpiration".
eventReasons	C	0..1	If value of eventCode is "Delivery" then this element shall not appear. If value of eventCode is "DeliveryExpiration" then one single instance of this element shall appear. The values of their eventReason children shall contain the codes identifying the reason(s) why the message could not be delivered to the recipient or the recipient's delegates.
evidenceIdentifier	M	1	Value as computed by the Evidence issuer.
evidenceIssuerPolicyID	O	0..1	
evidenceIssuerDetails	M	1	
reipientAuthenticationDetails	C	0..1	If the recipient has been authenticated by the REM-MD, then this element shall be present. Its contents will indicate the authentication process details. If the recipient has not been authenticated by the REM-MD, then this element shall not be present.
eventTime	M	1	If message (which may be a notification) has been delivered to recipient or recipient's delegates then this element will contain the delivery time. If message (which may be a notification) has not been delivered to recipient or recipient's delegates before the arrival of the delivery expiration time, then this element will contain the delivery expiration time.
replyTo	O	0..1	
senderDetails	M	1	
reipientsDetails	C	0..1	If the evidence is generated for delegated entities only, then this element shall not appear. If the evidence is generated for recipients, then this element shall appear.
reipientsDelegatesDetails	C	0..1	If the evidence is generated for delegated entities only, then this element shall appear. If the evidence is generated for recipients only, then this element shall appear.
evidenceRefersToRecipient	C	0..1	If the evidence only refers to some recipient / delegate then this element shall appear. If the evidence refers to all the recipients / delegates then this element shall not appear.

Element / Attribute	Mand. Opt.	Number occurrences	Additional profile properties
messageDetails[1]	M	1	This evidence shall contain one or two messageDetails elements. The contents of the first one will be as follows: messageSubject shall be present. uaMessageIdentifier may be present. messageIdentifierByREMMD shall be present. After the period mentioned in the normative part, hashAlgorithm and hash shall be present. Implementations may include it before the expiration of such a period. The value of field isNotification shall be "false".
messageDetails[2]	C	0..1	This element shall be present when the message delivered is a notification. In these cases the contents of this element will be as follows: messageSubject shall be present and will contain the subject of the notification itself. uaMessageIdentifier shall not be present. messageIdentifierByREMMD shall be present. hashAlgorithm and hash shall not be present The value of field isNotification shall be "true".
requiredReceiptType	C	0..1	Should messageDetails[1]'s hashAlgorithm and hash be present, this element shall not be present. Should messageDetails[1]'s hashAlgorithm and hash be not present, this element shall be present.
transactionLogInformation	O	0..1	
Extensions	O	0..1	

A.2.5 Evidence DownLoadNonDownloadByRecipient

The table below shows the contents of this element.

Element / Attribute	Mand. Opt.	Number occurrences	Additional profile properties
Attribute version	M	1	Value: "1" for this version
eventCode	M	1	Value if message has been downloaded by the recipient (or recipient's delegates) from a REM-MD's REM-MD Repository: "Download" Value if message has not been downloaded by the recipient or recipient's delegates before a certain giving time: "DownloadExpiration".
eventReasons	C	0..1	If value of eventCode is "Download" then this element shall not appear. If value of eventCode is "DownloadExpiration" then one single instance of this element shall appear. The values of their eventReason children shall contain the codes identifying the reason(s) why the message could not be downloaded by the recipient or the recipient's delegates.
evidenceIdentifier	M	1	Value as computed by the Evidence issuer.
evidenceIssuerPolicyID	O	0..1	
evidenceIssuerDetails	M	1	
reipientAuthentionDetails	C	0..1	If the recipient (or recipient's delegates) has been authenticated by the REM-MD, then this element shall be present. Its contents will indicate the authentication process details. If the recipient has not been authenticated by the REM-MD, then this element shall not be present.
eventTime	M	1	If message (which may be a notification) has been downloaded by the recipient or recipient's delegates then this element will contain the download time. If message (which may be a notification) has not been downloaded by the recipient or recipient's delegates before the arrival of the download expiration time, then this element will contain the download expiration time.
replyTo	O	0..1	
senderDetails	M	1	
reipientsDetails	C	0..1	If the evidence is generated for delegated entities only, then this element shall not appear. If the evidence is generated for recipients, then this element shall appear.
reipientsDelegatesDetails	C	0..1	If the evidence is generated for delegated entities only, then this element shall appear. If the evidence is generated for recipients only, then this element shall appear.
evidenceRefersToRecipient	C	0..1	If the evidence only refers to some recipient / delegate then this element shall appear. If the evidence refers to all the recipients / delegates then this element shall not appear.

Element / Attribute	Mand. Opt.	Number occurrences	Additional profile properties
messageDetails	M	1	The contents of this element will be as follows: `messageSubject` shall be present. `uaMessageIdentifier` may be present. `messageIdentifierByREMMD` shall be present. After the period mentioned in the normative part, `hashAlgorithm` and `hash` shall be present. Implementations may include it before the expiration of such a period. Should a notification be downloaded, field `isNotification`'s value shall be `"true"`, otherwise it shall be `"false"`.
requiredReceiptType	C	0..1	Should `messageDetails`'s `hashAlgorithm` and `hash` be present, this element shall not be present. Should `messageDetails`'s `hashAlgorithm` and `hash` be not present, this element shall be present.
transactionLogInformation	O	0..1	
Extensions	O	0..1	

A.2.6   Evidence RetrievalNonRetrievalByRecipient

The table below shows the contents of this element.

Element / Attribute	Mand. Opt.	Number occurrences	Additional profile properties
Attribute version	M	1	Value: `"1"` for this version
eventCode	M	1	Value if message has been retrieved from mailbox: `"Retrieval"` Value if message has not been retrieved from mailbox before a giving time: `"RetrievalExpiration"`.
eventReasons	C	0..1	If value of `eventCode` is `"Retrieval"` then this element shall not appear. If value of `eventCode` is `"RetrievalExpiration"` then one single instance of this element shall appear. The values of their `eventReason` children shall contain the codes identifying the reason(s) why the message could not be retrieved from the mailbox.
evidenceIdentifier	M	1	Value as computed by the Evidence issuer.
evidenceIssuerPolicyID	O	0..1	
evidenceIssuerDetails	M	1	
reipientAuthenticationDetails	C	0..1	If the recipient (or recipient's delegates) has been authenticated by the REM-MD, then this element shall be present. Its contents will indicate the authentication process details. If the recipient has not been authenticated by the REM-MD, then this element shall not be present.
eventTime	M	1	If message (which may be a notification) has been retrieved by the recipient or recipient's delegates from mailbox then this element shall contain the retrieval time. If message (which may be a notification) has not been retrieved by the recipient or recipient's delegates from mailbox then this element shall contain the retrieval expiration time.

Element / Attribute	Mand. Opt.	Number occurrences	Additional profile properties
replyTo	O	0..1	
senderDetails	M	1	
reipientsDetails	C	0..1	If the evidence is generated for delegated entities only, then this element shall not appear. If the evidence is generated for recipients, then this element shall appear.
reipientsDelegatesDetails	C	0..1	If the evidence is generated for delegated entities only, then this element shall appear. If the evidence is generated for recipients only, then this element shall appear.
evidenceRefersToRecipient	C	0..1	If the evidence only refers to some recipient / delegate then this element shall appear. If the evidence refers to all the recipients / delegates then this element shall not appear.
messageDetails	M	1	The contents of this element will be as follows: messageSubject shall be present. uaMessageIdentifier may be present. messageIdentifierByREMMD shall be present. After the period mentioned in the normative part, hashAlgorithm and hash shall be present. Implementations may include it before the expiration of such a period. If the message delivered to the recipient is the message sent by the sender (with optionally some additional evidences), then the value of field isNotification shall be "false". If the message delivered to the recipient is a notification, then the value of field isNotification shall be "false".
requiredReceiptType	C	0..1	Should messageDetails's hashAlgorithm and hash be present, this element shall not be present. Should messageDetails's hashAlgorithm and hash be not present and the value of messageDetails's isNotification field is "false", this element shall be present.
transactionLogInformation	O	0..1	
extensions	O	0..1	

A.2.7 Evidence AcceptanceRejectionByRecipient

The table below shows the contents of this element.

Element / Attribute	Mand. Opt.	Number occurrences	Additional profile properties
Attribute version	M	1	Value: `"1"` for this version
eventCode	M	1	Value if recipient (or recipient's delegate) has accepted the message: `"Acceptance"` Value if recipient (or recipient's delegates) has rejected the message: `"Rejection"`.
eventReasons	C	0..1	If value of eventCode is `"Acceptance"` then this element shall not appear. If value of eventCode is `"Rejection"` then one single instance of this element shall appear. The values of their `eventReason` children shall contain the codes identifying the reason(s) why the message could not be retrieved from the mailbox.
evidenceIdentifier	M	1	Value as computed by the Evidence issuer.
evidenceIssuerPolicyID	O	0..1	
evidenceIssuerDetails	M	1	
reipientAuthenticationDetails	C	0..1	If the recipient (or recipient's delegates) has been authenticated by the REM-MD, then this element shall be present. Its contents will indicate the authentication process details. If the recipient has not been authenticated by the REM-MD, then this element shall not be present.
eventTime	M	1	If recipient (or recipient's delegates) has accepted the message this element shall contain the acceptance time. If recipient (or recipient's delegates) has rejected the message this element shall contain the rejection time.
replyTo	O	0..1	
senderDetails	M	1	
reipientsDetails	C	0..1	If the evidence is generated for delegated entities only, then this element shall not appear. If the evidence is generated for recipients, then this element shall appear.
reipientsDelegatesDetails	C	0..1	If the evidence is generated for delegated entities only, then this element shall appear. If the evidence is generated for recipients only, then this element shall appear.
evidenceRefersToRecipient	C	0..1	If the evidence only refers to some recipient / delegate then this element shall appear. If the evidence refers to all the recipients / delegates then this element shall not appear.
messageDetails	M	1	The contents of this element will be as follows: `messageSubject` shall be present. `uaMessageIdentifier` may be present. `messageIdentifierByREMMD` shall be present. After the period mentioned in the normative part, `hashAlgorithm` and `hash` shall be present. Implementations may include it before the expiration of such a period.

Element / Attribute	Mand. Opt.	Number occurrences	Additional profile properties
requiredReceiptType	C	0..1	Should `messageDetails`'s `hashAlgorithm` and `hash` be present, this element shall not be present. Should `messageDetails`'s `hashAlgorithm` and `hash` be not present, this element shall be present. The value of field `isNotification` shall be "false".
transactionLogInformation	O	0..1	
extensions	O	0..1	

A.2.8   Evidence RelayToNonREMSystem

The table below shows the contents of this element.

Element / Attribute	Mand. Opt.	Number occurrences	Additional profile properties
Attribute version	M	1	Value: "1" for this version.
eventCode	O	0..1	Already identified values for this element: Value if message has been forwarded to regular e-mail: "ForwardedToRegularEMail" Value if message has been received from regular e-mail: "ForwardedToPrintingSystem".
evidenceIdentifier	M	1	Value as computed by the Evidence issuer.
evidenceIssuerPolicyID	O	0..1	
evidenceIssuerDetails	M	1	
eventTime	M	1	This element shall contain the message forwarding time.
replyTo	O	0..1	
senderDetails	M	1	
reipientsDetails	C	0..1	If the evidence is generated for delegated entities only, then this element shall not appear. If the evidence is generated for recipients, then this element shall appear.
evidenceRefersToRecipient	C	0..1	If the evidence only refers to some recipient / delegate then this element shall appear. If the evidence refers to all the recipients / delegates then this element shall not appear.
messageDetails	M	1	The contents of this element will be as follows: `messageSubject` shall be present. `uaMessageIdentifier` shall not be present. `messageIdentifierByREMMD` shall be present. `hashAlgorithm` and `hash` shall be present Field `isNotification` shall be "false".
forwardedToExternalSystem	M	1	
transactionLogInformation	O	0..1	
Extensions	O	0..1	

A.2.9 Evidence ReceivedFromNonREMSystem

The table below shows the contents of this element.

Element / Attribute	Mand. Opt.	Number occurrences	Additional profile properties
Attribute version	M	1	Value: "1" for this version.
evidenceIdentifier	M	1	Value as computed by the Evidence issuer.
evidenceIssuerPolicyID	O	0..1	
evidenceIssuerDetails	M	1	
eventTime	M	1	This element shall contain the message reception time.
replyTo	O	0..1	
senderDetails	M	1	
evidenceRefersToRecipient	C	0..1	If the evidence only refers to some recipient / delegate then this element shall appear. If the evidence refers to all the recipients / delegates then this element shall not appear.
messageDetails	M	1	The contents of this element will be as follows: messageSubject shall be present. uaMessageIdentifier shall not be present. messageIdentifierByREMMD shall be present. hashAlgorithm and hash shall be present Field isNotification shall be "false".
transactionLogInformation	O	0..1	
extensions	O	0..1	

Annex B (normative):
REM-MD Evidence Implementation in xml

This annex defines the syntax for REM-MD Evidence when xml is used.

Clause B.1 defines the general structure for REM-MD Evidences and provides details for their elements.

Clause B.2 specifies the different types of REM-MD Evidences as defined in clause 5.1.

B.1   REM-MD Evidence Structure

The table below shows the namespaces' URIs and prefixes used throughout the present annex.

Namespace's URI	Namespace's prefix
http://uri.etsi.org/REM#	rem
http://www.w3.org/2001/XMLSchema	xs
http://www.w3.org/2000/09/xmldsig#	ds
http://uri.etsi.org/02231/v2#	tsl
http://uri.etsi.org/01903/v1.3.2#	xades
urn:oasis:names:tc:dss:1.0:core:schema	dss

Clause 5.2.1 shows a template for REM-MD Evidence. The present clause defines a xml schema for REM-MD Evidences.

```
<xsd:complexType name="InternationalNamesType">
<xs:complexType name="REMEvidenceType">
   <xs:sequence>
       <xs:element ref="rem:EventCode" minOccurs="0" />
       <xs:element ref="rem:EventReasons" minOccurs="0"/>
       <xs:element name="EvidenceIdentifier" type="xs:string" />
       <xs:element name="EvidenceIssuerPolicyID" type="xs:anyURI" minOccurs="0"/>
       <xs:element ref="rem:EvidenceIssuerDetails"/>
       <xs:element ref="rem:SenderAuthenticationDetails" minOccurs="0"/>
       <xs:element ref="rem:RecipientAuthenticationDetails" minOccurs="0"/>
       <xs:element name="EventTime" type="xs:dateTime" />
       <xs:element name="SubmissionTime" type="xs:dateTime" minOccurs="0" />
       <xs:element name="ReplyTo" type="xs:string" minOccurs="0" />
       <xs:element ref="rem:SenderDetails" />
       <xs:element ref="rem:RecipientsDetails" minOccurs="0" />
       <xs:element ref="rem:RecipientsDelegatesDetails" minOccurs="0" />
       <xs:element name="EvidenceRefersToRecipient" type="xs:integer"
         minOccurs="0" />
       <xs:element ref="rem:MessageDetails" minOccurs="0" maxOccurs="2" />
       <xs:element name="ForwardedToExternalSystem" type="xs:string" minOccurs="0" />
       <xs:element ref="rem:TransactionLogInformation" minOccurs="0"/>
       <xs:element ref="rem:Extensions" minOccurs="0"/>
       <xs:element ref="ds:Signature" minOccurs="0"/>
   </xs:sequence>
   <xs:attribute name="version" type="xs:integer" use="required"/>
   <xs:attribute name="Id" type="ID" use="optional"/>
</xs:complexType>
```

Attribute `version` identifies the version of the evidence syntax. Value for the present specification in "1". has the semantics of data element G04 specified in clause 5.2.2.1.5.

Attribute `Id` allows the evidence be referenced from XML documents by an URI.

Clauses below further develop the elements of a REM-MD Evidence.

B.1.1 Element `<rem:EventCode>`

This element has the semantics of G02 data element as specified in clause 5.2.2.1.3. Its content is an URI.

The present document has identified a number of events, whose identifiers are defined below.

- `"http:uri.etsi.org/REM/Event#Acceptance"`: Acceptance of some REM Message by some entity.

- `"http:uri.etsi.org/REM/Event#Rejection"`: Rejection of some REM Message by some entity.

- `"http:uri.etsi.org/REM/Event#Delivery"`: Delivery of some REM Message to some entity.

- `"http:uri.etsi.org/REM/Event#DeliveryExpiration"`: Non delivery of some REM Message to some entity within a certain period of time.

- `"http:uri.etsi.org/REM/Event#Download"`: Download of some REM Message by recipient or recipient's delegate from a REM's REM-MD Repository.

- `"http:uri.etsi.org/REM/Event #DownloadExpiration"`: No download of some REM Message by recipient or recipient's delegate from a REM's REM-MD Repository within a certain period of time.

- `"http:uri.etsi.org/REM/Event#Retrieval"`: Retrieval of some REM Message by recipient from recipient's mailbox.

- `"http:uri.etsi.org/REM/Event#NonRetrievalExpiration"`: Non retrieval of some REM Message by recipient from recipient's mailbox within a certain period of time.

- `"http:uri.etsi.org/REM/Event#Rejection"`: Rejection of download of a message by recipient.

- `"http:uri.etsi.org/REM/Event#ForwardedToRegularEMail"`: Forward of REM Message to a regular e-mail system.

- `"http:uri.etsi.org/REM/Event#ForwardedToPrintingSystem"`: Forward of REM Message to a printing system to be subsequently sent via physical registered mail.

- `"http:uri.etsi.org/REM/Event#ReceivedFromRegularEMail"`: Reception of a message from a regular e-mail system.

B.1.2 Element `<rem:EventReasons>`

This element has the semantics of G03 data element as specified in clause 5.2.2.1.4. Below follows the xml schema for this element.

```
<xs:element name="EventReasons" type="rem:EventReasonsType"/>
<xs:complexType name="EventReasonsType">
    <xs:sequence>
        <xs:element ref="rem:EventReason" maxOccurs="unbounded"/>
    </xs:sequence>
</xs:complexType>
<xs:element name="EventReason" type="rem:EventReasonType"/>
<xs:complexType name="EventReasonType">
    <xs:sequence>
        <xs:element name="code" type="xs:anyURI"/>
        <xs:element name="Details" type="xs:string" minOccurs="0"/>
    </xs:sequence>
</xs:complexType>
```

Element `<rem:EventReasons>` contains a list of `<rem:EventReason>` elements.

`<rem:EventReason>`'s `<rem:Code>` child contains the reason code as an URI. Annex D of the present document shows the codes for the reasons identified by the present document.

`<rem:EventReason>`'s `<rem:Details>` optional child contains a string with additional details.

B.1.3   Element `<EvidenceIssuerPolicyID>`

This element has the semantics of R01 data element as specified in clause 5.2.2.2.2.1.

The value of this element is an URI identifying the aforementioned policy. Should the policy be identified by an OID, the content of this element MUST be an URN generated as specified in RFC 3061 [13].

B.1.4   Element `<EvidenceIdentifier>`

This element has the semantics of G00 data element as specified in clause 5.2.2.1.1. It contains a unique identifier of the REM-MD Evidence for the REM-MD Evidence Issuer.

All the REM-MD Evidences generated by a certain REM-MD Evidence Issuer MUST have different identifiers. The present document does not specify any further restriction on the values of this element.

B.1.5   Element `<rem:EvidenceIssuerDetails>`

This element has the semantics of R02 data element as specified in clause 5.2.2.2.2.

Below follows the xml schema for this element.

```
<xs:element name="EvidenceIssuerDetails" type="rem:EntityDetailsType"/>
<xs:complexType name="EntityDetailsType">
    <xs:sequence>
        <xs:element name="EntityName" type="tsl:InternationalNamesType"/>
        <xs:element ref="tsl:PostalAddress"/>
        <xs:element name="UnitName" type="tsl:InternationalNamesType" minOccurs="0"/>
        <xs:element ref="tsl:ElectronicAddress" minOccurs="0"/>
    </xs:sequence>
</xs:complexType>
```

Element `<EntityName>` contains the Name of the entity, as specified in TS 102 231 [6].

Element `<tsl:PostalAddress>` contains the postal address of the entity, as specified in TS 102 231 [6].

Optional element `<UnitName>`,if present, contains the name of the Unit within the entity, as specified in TS 102 231 [6].

Optional element `<tsl:ElectronicAddress>`,if present, contains the e-mail address of the entity.

B.1.6   Element `<rem:SenderAuthenticationDetails>`

This element has the semantics of I04 data element as specified in clause 5.2.2.3.5. This element, if present indicates the method used by sender's REM-MD for authenticating the sender.

Below follows the xml schema for this element.

```
<xs:element name="SenderAuthenticationDetals" type="rem:AuthenticationDetailsType"/>
<xs:complexType name="AuthenticationDetailsType">
    <xs:sequence>
        <xs:element name="AuthenticationTime" type="xs:dateTime"/>
        <xs:element name="AuthenticationMethod" type="xs:anyURI"/>
        <xs:element name="AdditionalDetails" type="xades:AnyType" minOccurs="0" />
    </xs:sequence>
</xs:complexType>
```

Element `<rem:AuthenticationTime>` indicates the time when the sender was authenticated.

Element `<rem:AuthenticationMethod>` contains info on the method used for authenticating the sender. The following methods and identifiers have already been identified:

- `"http:uri.etsi.org/REM/AuthMethod#Basic"`: Basic: Using basic mechanisms such as passwords for use of signature.

- `"http:uri.etsi.org/REM/AuthMethod#Enhanced"`. Enhanced: Using enhanced authentication such two factor mechanisms linked to a one time password.

- `"http:uri.etsi.org/REM/AuthMethod#AdES"`. AdES: Using advanced electronic signatures.

- `"http:uri.etsi.org/REM/AuthMethod#AdES-Plus"`. AdES-Plus: Using advanced electronic signatures with Secure Signature Creation Devices (as defined in Directive 1999/93/EC [1]) or equivalent secure cryptographic device.

- `"http:uri.etsi.org/REM/AuthMethod#QES"`. QES: Using advanced electronic signatures with Secure Signature Creation Devices and Qualified Certificates (as defined in Directive 1999/93/EC [1]).

Optional element `<rem:AdditionalDetails>` contains additional details on the authentication process. It may contain, for instance, the token presented by the sender to the sender's REM-MD. If the token is the sender's signature itself, then it shall appear within a `<dss:SignatureObject>` element defined in the core of the OASIS DSS core protocol [12], with the following restrictions:

- When the sender's signature is a CMS or PKCS#7 signature, the child of this element will be a `<dss:Base64Signature>` encapsulating its BER-encoded value.

- Should the sender's signature be a XML signature, the child of this element would be a `<ds:Signature>` element.

- This element shall not have any child different to the ones mentioned in this bulleted list.

B.1.7   Element `<rem:RecipientAuthenticationDetails>`

This element has the semantics of I05 data element as specified in clause 5.2.2.3.6. This element, if present indicates the method used by recipient's REM-MD for authenticating the recipient.

Below follows the xml schema for this element.

```
<xs:element name="RecipientAuthenticationDetails" type="rem:AuthenticationDetailsType />
```

B.1.8   Element `<rem:EventTime>`

This field has the semantics of G05 data element as specified in clause 5.2.2.1.6.

B.1.9   Element `<rem:SubmissionTime>`

This field has the semantics of M03 data element as specified in clause 5.2.2.4.4.

B.1.10 Element `<rem:ReplyTo>`

This element has the semantics of M01 data element as specified in clause 5.2.2.4.2.

B.1.11 Element `<rem:SenderDetails>`

This element has the semantics of I00 data element as specified in clause 5.2.2.3.1.

Below follows the xml schema for this element:

```
<xs:element name="SenderDetails" type="rem:UserDetailsType" />
<xs:complexType name="UserDetailsType">
    <xs:sequence>
        <xs:element ref="tsl:ElectronicAddress"/>
        <xs:element ref="tsl:PostalAddress" minOccurs="0"/>
        <xs:element ref="rem:CertificateDetails" minOccurs="0"/>
    </xs:sequence>
</xs:complexType>
<xs:complexType name="UserDetailsListType">
    <xs:sequence>
        <xs:element name="UserDetails" maxOccurs="unbounded"/>
    </xs:sequence>
</xs:complexType>

<xs:element name="CertificateDetails" type="rem:CertificateDetailsType"/>
<xs:complexType name="CertificateDetailsType">
    <xs:choice>
        <xs:element name="X509Certificate" type="xs:base64Binary"/>
        <xs:element name="CertID" type="xades:CertIDType"/>
        <xs:element ref="rem:CertIDAndSignature"/>
    </xs:choice>
</xs:complexType>

<xs:element name="CertIDAndSignature" type="rem:CertIDAndSignatureType" />
<xs:complexType name="CertIDAndSignatureType">
    <xs:sequence>
        <xs:element name="IssuerSerial" type="ds:X509IssuerSerialType"/>
        <xs:element name="tbsCertificateDigestDetails" type="xades:DigestAlgAndValueType"/>
        <xs:element ref="rem:CertSignatureDetails"/>
    </xs:sequence>
</xs:complexType>

<xs:element name="CertSignatureDetails" type=="rem:CertSignatureDetailsType" />
<xs:complexType name="CertSignatureDetailsType">
    <xs:sequence>
        <xs:element ref="ds:SignatureMethod"/>
        <xs:element ref="ds:SignatureValue"/>
    </xs:sequence>
</xs:complexType>
```

Element `<tsl:ElectroniAddress>` contains details of sender's electronic mail address. See TS 102 231 [6] for details.

Element `<tsl:ElectroniAddress>` contains details of sender's postal address. See TS 102 231 [6] for details.

Element `<rem:CertificateDetails>` contains details of the user's certificate. These may be one of the following:

- User's X509 certificate itself within element `<rem:X509Certificate>`.

- User's X509 certificate identifier within element `<rem:CertID>`. This is an instance of `xades:CertIDType`. See TS 101 903 [4] for more details.

- User's X509 certificate identifier with signature value incorporated within `<rem:CertIDAndSignature>`. Its contents are as indicated below:

  - `<rem:IssuerSerial>` is an instance of `<ds:X509IssuerSerial>` containing the certificate's issuer's name and the serial number. See XML Sig for more details.

  - `<rem:tbsCertificateDigestDetails>` contains the digest algorithm and digest value of the to-be-signed field of the user's certificate.

  - `<rem:CertSignatureDetails>` contains the signature algorithm and the signature value of the user's certificate.

B.1.12 Element `<rem:RecipientsDetails>`

This element has the semantics of I01 data element as specified in clause 5.2.2.3.2.

Below follows the xml schema for this element:

```
<xs:element name="RecipientsDetails" type="rem:UserDetailsListType" />
<xs:complexType name="UserDetailsListType">
    <xs:sequence>
        <xs:element name="UserDetails" maxOccurs="unbounded"/>
    </xs:sequence>
</xs:complexType>
```

Semantics of this element are similar to the semantics of `<rem:SenderDetails>` but referred to the recipient user.

B.1.13 Element `<rem:RecipientsDelegatesDetails>`

This element has the semantics of I02 data element as specified in clause 5.2.2.3.3.

Below follows the xml schema for this element:

```
<xs:element name="RecipientsDelegatesDetails" type="rem:RecipientsDelegatesType" />
<xs:complexType name="RecipientsDelegatesType">
    <xs:sequence maxOccurs="unbounded">
        <xs:element ref="rem:Delegate"/>
    </xs:sequence>
</xs:complexType>
<xs:element name="Delegate" type="rem:RecipientsDelegateType" />
<xs:complexType name="RecipientsDelegateType">
    <xs:sequence>
        <xs:element name="DelegateDetails" type="rem:UserDetailsType"/>
        <xs:element name="DelegatingRecipients" type="rem:ListOfIntegers" minOccurs="0"/>
    </xs:sequence>
</xs:complexType>
<xs:simpleType name="ListOfIntegers">
    <xs:list itemType="xs:integer"/>
</xs:simpleType>
```

`<rem:Delegate>`'s `<rem:DelegateDetails>` element contains the details of the delegate in question.

`<rem:Delegate>`'s `<rem:DelegatingRecipients>` element contains a list of integers that identify the recipients that have delegated in this entity. First Recipient in `<rem:SendersDetails>` is assigned number 1. If this element is absent, then the delegate will act as delegated of all the recipients.

B.1.14 Element `<EvidenceRefersToRecipient>`

This element has the semantics of I03 data element as specified in clause 5.2.2.3.4. Its value references one of the recipients in `<rem:RecipientsDetails>` element. First recipient in the list of recipients is assigned number 1.

B.1.15 Element `<rem:MessageDetails>`

This element has the semantics of M00 data element as specified in clause 5.2.2.4.1.

Below follows the xml schema for this element:

```
<xs:element name="MessageDetails" type="rem:MessageDetailsType"/>
<xs:complexType name="MessageDetailsType">
    <xs:sequence>
        <xs:element name="MessageSubject" type="xs:string" minOccurs="0" />
        <xs:element name="UAMessageIdentifier" type="xs:string" minOccurs="0"/>
        <xs:element name="MessageIdentifierByREMMD" type="xs:string" />
        <xs:element ref="ds:DigestMethod" minOccurs="0"/>
        <xs:element ref="ds:DigestValue" minOccurs="0"/>
    </xs:sequence>
    <xs:attribute name="isNotification" type="xs:boolean" use="required"/>
</xs:complexType>
```

Optional `<rem:MessageSubject>`'s content is the value of the Subject field of the referred message.

Optional `<rem:UAMessageIdentifier>` element contains an identifier as computed by the user's UA.

Element `<rem:MessageIdentifierByREMMD>` contains an identifier computed by a REM-MD. This identifier shall be unique for this REM-MD.

Finally, `<ds:DigestValue>` and `<ds:DigestMethod>` contain the referred message's digest value and the digest algorithm identifier respectively.

B.1.16 Element `<rem:ForwardedToExternalSystem>`

This element the semantics of M04 data element as specified in clause 5.2.2.4.5.

B.1.17 Element `<rem:TransactionLogInformation>`

This element has the semantics of G06 data element as specified in clause 5.2.2.2.3. This element is a placeholder that issuers of evidences may use for including pieces of the log file content within them.

Below follows the xml schema for this element.

```
<xs:element name="TransactionLogInformation" type="rem:TransactionLogInformationType"/>
<xs:complexType name="TransactionLogInformationType">
    <xs:sequence>
        <xs:element ref="rem:TransactionLog" maxOccurs="unbounded"/>
    </xs:sequence>
</xs:complexType>
<xs:element name="TransactionLog" type="xades:AnyType"/>
```

Element `<rem:TransactionLogInformation>` contains a sequence of `<rem:TransactionLog>` elements, each one containing an instance of log information.

The present document does not mandate any particular format for the content of `<rem:TransactionLog>` elements.

B.1.18 Element `<rem:Extensions>`

This element has the semantics of Enn data element. This element is a placeholder for further standardized or private extensions.

B.1.19 Element `<ds:Signature>`

This element has the semantics of R03 data element as specified in clause 5.2.2.2.3. Should this element be present, it will contain the enveloped signature of the Evidence, profiled as indicated in clause 6 of the present document.

B.2   REM-MD Evidences

This clause defines formats for different types of Evidences, which are listed in the xml schema below.

```
<xs:element name="SubmissionAcceptanceRejection" type="rem:REMEvidenceType" />
<xs:element name="RelayREMMDAcceptanceRejection" type="rem:REMEvidenceType" />
<xs:element name="RelayREMMDFailure" type="rem:REMEvidenceType" />
<xs:element name="DeliveryNonDeliveryToRecipient" type="rem:REMEvidenceType"/>
<xs:element name="DownloadNonDownloadByRecipient" type="rem:REMEvidenceType"/>
<xs:element name="RetrievalNonRetrievalByRecipient" type="rem:REMEvidenceType"/>
<xs:element name="AcceptanceRejectionByRecipient" type="rem:REMEvidenceType"/>
<xs:element name="RelayToNonREMSystem" type="rem:REMEvidenceType"/>
<xs:element name="ReceivedFromNonREMSystem" type="rem:REMEvidenceType"/>
```

Each clause below specifies one Evidence type by profiling the contents of the REMEvidenceType shown above.

Constraints are expressed in tables organized as follows:

- Column **Element / Attribute** identifies the profiled element or attribute. Should an evidence could carry more than one instance of the same element, then the usual array syntax of an integer index within square brackets is used for enumerating the different instances. Array index numbering starts at 1.

- Column **Mandatory / Optional** specifies requirements on the element / attribute. The following codes may appear:

  - M: This means that the element / attribute is mandatory.

  - O: This means that presence or absence of the element / attribute is optional.

  - C: This means that the presence of the element / attribute depends on certain conditions that are further developed in column **Additional Profile Properties**.

- Column **Nbr. Occurrences** identifies the number of occurrences of the element.

- Column **Additional Profile Properties** specifies additional requirements on the element / attribute: values, conditions, etc. Terms shall, may and should used in these cells have the meaning as specified in TS 102 904 [16].

B.2.1 Evidence <SubmissionAcceptanceRejection>

The table below shows the contents of this element.

Element / Attribute	Mand. Opt.	Number occurrences	Additional profile properties
Attribute version	M	1	Value: "1" for this version
rem:EventCode	M	1	Value if acceptance: "Acceptance" Value if rejection: "Rejection".
rem:EventReasons	C	0..1	If value of rem:EventCode is "Acceptance" then this element shall not appear. If value of rem:EventCode is "Rejection" then one single instance of this element shall appear. The values of their rem:EventReason children shall contain the codes identifying the reason(s) why the REM-MD rejected the message submitted by the sender.
rem:EvidenceIssuerPolicyID	O	0..1	
rem:EvidenceIdentifier	M	1	Value as computed by the Evidence issuer.
rem:EvidenceIssuerDetails	M	1	
rem:SenderAuthenticationDetails	C	0..1	If the sender has been authenticated by the REM-MD, then this element shall be present. Its contents will indicate the authentication process details. If the sender has not been authenticated by the REM-MD, then this element shall not be present.
rem:EventTime	M	1	
rem:SubmissionTime	M	1	
replyTo	O	0..1	
rem:SenderDetails	M	1	
rem:RecipientsDetails	C	0..1	If the evidence is generated for delegated entities only, then this element shall not appear. If the evidence is generated for recipients, then this element shall appear.
rem:RecipientsDelegatesDetails	C	0..1	If the evidence is generated for delegated entities only, then this element shall appear. If the evidence is generated for recipients only, then this element shall appear.
rem:MessageDetails	M	1	The contents of this element shall be as follows: <rem:MessageSubject> shall be present. <rem:UAMessageIdentifier> may be present. <rem:MessageIdentifierByREMMD> shall be present. After the period mentioned in the normative part, <ds:DigestMethod> and <ds:DigestValue> shall be present. Implementations may include it before the expiration of such a period Attribute isNotification shall be "false".
rem:TransactionLogInformation	O	0..1	
rem:Extensions	O	0..1	
ds:Signature	C	0..1	

B.2.2 Evidence <RelayREMMDAcceptanceRejection>

The table below shows the contents of this element.

Element / Attribute	Mand. Opt.	Number occurrences	Additional profile properties
Attribute version	M	1	Value: "1" for this version.
rem:EventCode	M	1	Value if acceptance by recipient's REM-MD: "Acceptance" Value if rejection by recipient's REM-MD: "Rejection"
rem:EventReasons	C	0..1	If value of rem:EventCode is "Acceptance" then this element shall not appear. If value of rem:EventCode is "Rejection" then one single instance of this element shall appear. The values of their rem:EventReason children shall contain the codes identifying the reason(s) why the REM-MD rejected the message submitted by the sender.
rem:EvidenceIdentifier	M	1	Value as computed by the Evidence issuer.
rem:EvidenceIssuerPolicyID	O	0..1	
rem:EvidenceIssuerDetails	M	1	
rem:EventTime	M	1	If recipient's REM-MD has accepted the message this element shall indicate when the acceptance occurred. If recipient's REM-MD has rejected the message this element shall indicate when the rejection occurred.
replyTo	O	0..1	
rem:SenderDetails	M	1	
rem:RecipientsDetails	C	0..1	If the evidence is generated for delegated entities only, then this element shall not appear. If the evidence is generated for recipients, then this element shall appear.
rem:RecipientsDelegatesDetails	C	0..1	If the evidence is generated for delegated entities only, then this element shall appear. If the evidence is generated for recipients only, then this element shall appear.
rem:EvidenceRefersToRecipient	C	0..1	If the evidence only refers to some recipient / delegate then this element shall appear. If the evidence refers to all the recipients / delegates then this element shall not appear.
rem:MessageDetails	M	1	The contents of this element shall be as follows: <rem:MessageSubject> shall be present. <rem:UAMessageIdentifier> may be present. <rem:MessageIdentifierByREMMD> shall be present. After the period mentioned in the normative part, <ds:DigestMethod> and <ds:DigestValue> shall be present. Implementations may include it before the expiration of such a period Attribute isNotification's value shall be "false".
rem:TransactionLogInformation	O	0..1	
rem:Extensions	O	0..1	
ds:Signature	C	0..1	

B.2.3   Evidence <RelayREMMDFailure>

The table below shows the contents of this element.

Element / Attribute	Mand. Opt.	Number occurrences	Additional profile properties
Attribute version	M	1	Value: "1" for this version.
rem:EventCode	M	1	For this evidence the value of this code is always: "DeliveryExpiration"
rem:EventReasons	M	1	The values of their rem:EventReason children shall contain the codes identifying the reason(s) why the sender's REM-MD could not delivery the message to recipient's REM-MD.
rem:EvidenceIdentifier	M	1	Value as computed by the Evidence issuer.
rem:EvidenceIssuerPolicyID	O	0..1	
rem:EvidenceIssuerDetails	M	1	
rem:EventTime	M	1	This element will contain the message delivery expiration time.
replyTo	O	0..1	
rem:SenderDetails	M	1	
rem:RecipientsDetails	C	0..1	If the evidence is generated for delegated entities only, then this element shall not appear. If the evidence is generated for recipients, then this element shall appear.
rem:RecipientsDelegatesDetails	C	0..1	If the evidence is generated for delegated entities only, then this element shall appear. If the evidence is generated for recipients only, then this element shall appear.
rem:EvidenceRefersToRecipient	C	0..1	If the evidence only refers to some recipient / delegate then this element shall appear. If the evidence refers to all the recipients / delegates then this element shall not appear.
rem:MessageDetails	M	1	The contents of this element shall be as follows: <rem:MessageSubject> shall be present. <rem:UAMessageIdentifier> may be present. <rem:MessageIdentifierByREMMD> shall be present. After the period mentioned in the normative part, <ds:DigestMethod> and <ds:DigestValue> shall be present. Implementations may include it before the expiration of such a period Attribute isNotification shall be "false".
rem:TransactionLogInformation	O	0..1	
rem:Extensions	O	0..1	
ds:Signature	C	0..1	

B.2.4   Evidence <DeliveryNonDeliveryToRecipient>

The table below shows the contents of this element.

Element / Attribute	Mand. Opt.	Number occurrences	Additional profile properties
Attribute version	M	1	Value: "1" for this version.
rem:EventCode	M	1	Value if message (which may be a notification) has been delivered to recipient or recipient's delegates: "Delivery" Value if message (which may be a notification) has not been delivered to recipient or recipient's delegates: "DeliveryExpiration"
rem:EventReasons	C	0..1	If value of rem:EventCode is "Delivery" then this element shall not appear. If value of rem:EventCode is "DeliveryExpiration" then one single instance of this element shall appear. The values of their rem:EventReason children shall contain the codes identifying the reason(s) why the message could not be delivered to the recipient or the recipient's delegates.
rem:EvidenceIdentifier	M	1	Value as computed by the Evidence issuer.
rem:EvidenceIssuerPolicyID	O	0..1	
rem:EvidenceIssuerDetails	M	1	
rem:RecipientAuthenticationDetails	C	0..1	If the recipient has been authenticated by the REM-MD, then this element shall be present. Its contents will indicate the authentication process details. If the recipient has not been authenticated by the REM-MD, then this element shall not be present.
rem:EventTime	M	1	If message (which may be a notification) has been delivered to recipient or recipient's delegates then this element will contain the delivery time. If message (which may be a notification) has not been delivered to recipient or recipient's delegates before the arrival of the delivery expiration time, then this element will contain the delivery expiration time.
replyTo	O	0..1	
rem:SenderDetails	M	1	
rem:RecipientsDetails	C	0..1	If the evidence is generated for delegated entities only, then this element shall not appear. If the evidence is generated for recipients, then this element shall appear.
rem:RecipientsDelegatesDetails	C	0..1	If the evidence is generated for delegated entities only, then this element shall appear. If the evidence is generated for recipients only, then this element shall appear.
rem:EvidenceRefersToRecipient	C	0..1	If the evidence only refers to some recipient / delegate then this element shall appear. If the evidence refers to all the recipients / delegates then this element shall not appear.
rem:MessageDetails[1]	M	1	This evidence shall contain one or two rem:MessageDetails elements. The contents of the first one will be as follows: <rem:MessageSubject> shall be present. <rem:UAMessageIdentifier> may be present. <rem:MessageIdentifierByREMMD> shall be present.

Element / Attribute	Mand. Opt.	Number occurrences	Additional profile properties
			After the period mentioned in the normative part, `<ds:DigestMethod>` and `<ds:DigestValue>` shall be present. Implementations may include it before the expiration of such a period. The value of attribute `isNotification` shall be `"false"`.
`rem:MessageDetails[2]`	C	0..1	This element shall be present when the message delivered is a notification. In these cases the contents of this element will be as follows: `<rem:MessageSubject>` shall be present and will contain the subject of the notification itself. `<rem:UAMessageIdentifier>` shall not be present. `<rem:MessageIdentifierByREMMD>` shall be present. `<ds:DigestMethod>` and `<ds:DigestValue>` shall not be present The value of attribute `isNotification` shall be `"true"`.
`rem:TransactionLogInformation`	O	0..1	
`rem:Extensions`	O	0..1	
`ds:Signature`	C	0..1	

B.2.5   Evidence <DownLoadNonDownloadByRecipient>

The table below shows the contents of this element.

Element / Attribute	Mand. Opt.	Number occurrences	Additional profile properties
Attribute version	M	1	Value: `"1"` for this version.
`rem:EventCode`	M	1	Value if message has been downloaded by the recipient (or recipient's delegates) from a REM-MD's REM-MD Repository: `"Download"` Value if message has not been downloaded by the recipient or recipient's delegates before a certain giving time: `"DownloadExpiration"`.
`rem:EventReasons`	C	0..1	If value of `rem:EventCode` is `"Download"` then this element shall not appear. If value of `rem:EventCode` is `"DownloadExpiration"` then one single instance of this element shall appear. The values of their `rem:EventReason` children shall contain the codes identifying the reason(s) why the message could not be downloaded by the recipient or the recipient's delegates.
`rem:EvidenceIdentifier`	M	1	Value as computed by the Evidence issuer.
`rem:EvidenceIssuerPolicyID`	O	0..1	
`rem:EvidenceIssuerDetails`	M	1	
`rem:RecipientAuthentionDetails`	C	0..1	If the recipient (or recipient's delegates) has been authenticated by the REM-MD, then this element shall be present. Its contents will indicate the authentication process details. If the recipient has not been authenticated by the REM-MD, then this element shall not be present.

Element / Attribute	Mand. Opt.	Number occurrences	Additional profile properties
`rem:EventTime`	M	1	If message (which may be a notification) has been downloaded by the recipient or recipient's delegates then this element will contain the download time. If message (which may be a notification) has not been downloaded by the recipient or recipient's delegates before the arrival of the download expiration time, then this element will contain the download expiration time.
`replyTo`	O	0..1	
`rem:SenderDetails`	M	1	
`rem:RecipientsDetails`	C	0..1	If the evidence is generated for delegated entities only, then this element shall not appear. If the evidence is generated for recipients, then this element shall appear.
`rem:RecipientsDelegatesDetails`	C	0..1	If the evidence is generated for delegated entities only, then this element shall appear. If the evidence is generated for recipients only, then this element shall appear.
`rem:EvidenceRefersToRecipient`	C	0..1	If the evidence only refers to some recipient / delegate then this element shall appear. If the evidence refers to all the recipients / delegates then this element shall not appear.
`rem:MessageDetails`	M	1	The contents of this element will be as follows: `<rem:MessageSubject>` shall be present. `<rem:UAMessageIdentifier>` may be present. `<rem:MessageIdentifierByREMMD>` shall be present. After the period mentioned in the normative part, `<ds:DigestMethod>` and `<ds:DigestValue>` shall be present. Implementations may include it before the expiration of such a period. Should a notification be downloaded, attribute `isNotification`'s value shall be "true", otherwise it shall be "false".
`rem:TransactionLogInformation`	O	0..1	
`rem:Extensions`	O	0..1	
`Ds:Signature`	C	0..1	

B.2.6   Evidence <RetrievalNonRetrievalByRecipient>

The table below shows the contents of this element.

Element / Attribute	Mand. Opt.	Number occurrences	Additional profile properties
Attribute version	M	1	Value: "1" for this version.
rem:EventCode	M	1	Value if message has been retrieved from mailbox: "Retrieval" Value if message has not been retrieved from mailbox before a giving time: "RetrievalExpiration".
rem:EventReasons	C	0..1	If value of rem:EventCode is "Retrieval" then this element shall not appear. If value of rem:EventCode is "RetrievalExpiration" then one single instance of this element shall appear. The values of their rem:EventReason children shall contain the codes identifying the reason(s) why the message could not be retrieved from the mailbox.
rem:EvidenceIdentifier	M	1	Value as computed by the Evidence issuer.
rem:EvidenceIssuerPolicyID	O	0..1	
rem:EvidenceIssuerDetails	M	1	
rem:RecipientAuthenticationDetails	C	0..1	If the recipient (or recipient's delegates) has been authenticated by the REM-MD, then this element shall be present. Its contents will indicate the authentication process details. If the recipient has not been authenticated by the REM-MD, then this element shall not be present.
rem:EventTime	M	1	If message (which may be a notification) has been retrieved by the recipient or recipient's delegates from mailbox then this element shall contain the retrieval time. If message (which may be a notification) has not been retrieved by the recipient or recipient's delegates from mailbox then this element shall contain the retrieval expiration time.
replyTo	O	0..1	
rem:SenderDetails	M	1	
rem:RecipientsDetails	C	0..1	If the evidence is generated for delegated entities only, then this element shall not appear. If the evidence is generated for recipients, then this element shall appear.
rem:RecipientsDelegatesDetails	C	0..1	If the evidence is generated for delegated entities only, then this element shall appear. If the evidence is generated for recipients only, then this element shall appear.
rem:EvidenceRefersToRecipient	C	0..1	If the evidence only refers to some recipient / delegate then this element shall appear. If the evidence refers to all the recipients / delegates then this element shall not appear.
rem:MessageDetails	M	1	The contents of this element will be as follows: <rem:MessageSubject> shall be present.

Element / Attribute	Mand. Opt.	Number occurrences	Additional profile properties
			`<rem:UAMessageIdentifier>` may be present. `<rem:MessageIdentifierByREMMD>` shall be present. After the period mentioned in the normative part, `<ds:DigestMethod>` and `<ds:DigestValue>` shall be present. Implementations may include it before the expiration of such a period. If the message delivered to the recipient is the message sent by the sender (with optionally some additional evidences), then the value of attribute `isNotification` shall be "false". If the message delivered to the recipient is a notification, then the value of attribute `isNotification` shall be "false".
`rem:TransactionLogInformation`	O	0..1	
`rem:Extensions`	O	0..1	
`ds:Signature`	C	0..1	

B.2.7   Evidence <AcceptanceRejectionByRecipient>

The table below shows the contents of this element.

Element / Attribute	Mand. Opt.	Number occurrences	Additional profile properties
Attribute version	M	1	Value: "`1`" for this version.
`rem:EventCode`	M	1	Value if recipient (or recipient's delegate) has accepted the message: "`Acceptance`" Value if recipient (or recipient's delegates) has rejected the message: "`Rejection`".
`rem:EventReasons`	C	0..1	If value of `rem:EventCode` is "`Acceptance`" then this element shall not appear. If value of `rem:EventCode` is "`Rejection`" then one single instance of this element shall appear. The values of their `rem:EventReason` children shall contain the codes identifying the reason(s) why the message could not be retrieved from the mailbox.
`rem:EvidenceIdentifier`	M	1	Value as computed by the Evidence issuer.
`rem:EvidenceIssuerPolicyID`	O	0..1	
`rem:EvidenceIssuerDetails`	M	1	
`rem:RecipientAuthenticationDetails`	C	0..1	If the recipient (or recipient's delegates) has been authenticated by the REM-MD, then this element shall be present. Its contents will indicate the authentication process details. If the recipient has not been authenticated by the REM-MD, then this element shall not be present.
`rem:EventTime`	M	1	If recipient (or recipient's delegates) has accepted the message this element shall contain the acceptance time. If recipient (or recipient's delegates) has rejected the message this element shall contain the rejection time.

Element / Attribute	Mand. Opt.	Number occurrences	Additional profile properties
replyTo	O	0..1	
rem:SenderDetails	M	1	
rem:RecipientsDetails	C	0..1	If the evidence is generated for delegated entities only, then this element shall not appear. If the evidence is generated for recipients, then this element shall appear.
rem:RecipientsDelegatesDetails	C	0..1	If the evidence is generated for delegated entities only, then this element shall appear. If the evidence is generated for recipients only, then this element shall appear.
rem:EvidenceRefersToRecipient	C	0..1	If the evidence only refers to some recipient / delegate then this element shall appear. If the evidence refers to all the recipients / delegates then this element shall not appear.
rem:MessageDetails	M	1	The contents of this element will be as follows: <rem:MessageSubject> shall be present. <rem:UAMessageIdentifier> may be present. <rem:MessageIdentifierByREMMD> shall be present. After the period mentioned in the normative part, <ds:DigestMethod> and <ds:DigestValue> shall be present. Implementations may include it before the expiration of such a period.
rem:TransactionLogInformation	O	0..1	
rem:Extensions	O	0..1	
ds:Signature	C	0..1	

B.2.8 Evidence <RelayToNonREMSystem>

The table below shows the contents of this element.

Element / Attribute	Mand. Opt.	Number occurrences	Additional profile properties
Attribute version	M	1	Value: "1" for this version.
rem:EventCode	O	0..1	Already identified values for this element: Value if message has been forwarded to regular e-mail: "ForwardedToRegularEMail" Value if message has been received from regular e-mail: "ForwardedToPrintingSystem".
rem:EvidenceIdentifier	M	1	Value as computed by the Evidence issuer.
rem:EvidenceIssuerPolicyID	O	0..1	
rem:EvidenceIssuerDetails	M	1	
rem:EventTime	M	1	This element shall contain the message forwarding time.
replyTo	O	0..1	
rem:SenderDetails	M	1	
rem:RecipientsDetails	C	0..1	If the evidence is generated for delegated entities only, then this element shall not appear. If the evidence is generated for recipients, then this element shall appear.

Element / Attribute	Mand. Opt.	Number occurrences	Additional profile properties
rem:EvidenceRefersToRecipient	C	0..1	If the evidence only refers to some recipient / delegate then this element shall appear. If the evidence refers to all the recipients / delegates then this element shall not appear.
rem:MessageDetails	M	1	The contents of this element will be as follows: `<rem:MessageSubject>` shall be present. `<rem:UAMessageIdentifier>` shall not be present. `<rem:MessageIdentifierByREMMD>` shall be present. `<ds:DigestMethod>` and `<ds:DigestValue>` shall be present Attribute `isNotification` shall be "false".
rem:ForwardedToExternalSystem	M	1	
rem:TransactionLogInformation	O	0..1	
rem:Extensions	O	0..1	
ds:Signature	C	0..1	

B.2.9   Evidence <ReceivedFromNonREMSystem>

The table below shows the contents of this element.

Element / Attribute	Mand. Opt.	Number occurrences	Additional profile properties
Attribute version	M	1	Value: "1" for this version.
rem:EvidenceIdentifier	M	1	Value as computed by the Evidence issuer.
rem:EvidenceIssuerPolicyID	O	0..1	
rem:EvidenceIssuerDetails	M	1	
rem:EventTime	M	1	This element shall contain the message reception time.
replyTo	O	0..1	
rem:SenderDetails	M	1	
rem:EvidenceRefersToRecipient	C	0..1	If the evidence only refers to some recipient / delegate then this element shall appear. If the evidence refers to all the recipients / delegates then this element shall not appear.
rem:MessageDetails	M	1	The contents of this element will be as follows: `<rem:MessageSubject>` shall be present. `<rem:UAMessageIdentifier>` shall not be present. `<rem:MessageIdentifierByREMMD>` shall be present. `<ds:DigestMethod>` and `<ds:DigestValue>` shall be present Attribute `isNotification` shall be "false".
rem:TransactionLogInformation	O	0..1	
rem:Extensions	O	0..1	
ds:Signature	C	0..1	

Annex C (normative):
REM-MD Evidence Implementation in pdf

This annex specifies mechanisms for generating human readable REM-MD Evidences based in PDF documents.

For generating REM-MD Evidence in PDF the following process is recommended:

1) Generate the REM-MD Evidence using the XML syntax as indicated in annex B.

2) Generate an XFA file where the XML data object is the XML-encoded REM-MD Evidence generated in step 1.

3) Generate a PDF/A-1 file from the XFA generated in step 2. This format is suitable for long term preservation of the information.

4) Should the REM-MD Evidences be individually signed, sign the PDF/A-1 file generated in step 3 using normal PDF signatures (PDF/A-1 & PDF 1.4).

NOTE: At the time of writing of the present document, work is being carried for specifying full integration of XAdES and CAdES signatures within PDF files. XFA is a forms architecture which may be used to create PDF forms. It can be used to carry XML data and map this to a PDF form fields. It is recommended that the XFA template maps the XML data element names directly to form field names and that specifies an appropriate display of pages that presents the form field data supported by text describing the meaning of each field in an appropriate language.

Annex D (normative):
Event reason identifiers and codes

Element `<rem:EventReason>` in XML evidences and field `eventReason` in ASN.1 identify the event reason. In XML evidences the content of the element is an URI. In ASN.1 evidences the field is an integer.

The table below lists all the event reasons identified in the present document, and shows the correspondence between the URI and the integer values.

Identifier as URI	Ident. as integer
http:uri.etsi.org/REM/EventReason#InvalidMessageFormat	1
http:uri.etsi.org/REM/EventReason#MalwareFound	2
http:uri.etsi.org/REM/EventReason#InvalidUserSignature	3
http:uri.etsi.org/REM/EventReason#UserCertExpiredOrRevoked	4
http:uri.etsi.org/REM/EventReason#PolicyViolation	5
http:uri.etsi.org/REM/EventReason#R_REMMD_Malfunction	6
http:uri.etsi.org/REM/EventReason#R_REMMD_NotIdenified	7
http:uri.etsi.org/REM/EventReason#R_REMMD_Unreachable	8
http:uri.etsi.org/REM/EventReason#S_REMMD_ReceivedNoDeliveryInfoFromR_REMMD	9
http:uri.etsi.org/REM/EventReason#UnknownRecipient	10
http:uri.etsi.org/REM/EventReason#MailboxFull	11
http:uri.etsi.org/REM/EventReason#TechnicalMalfunction	12
http:uri.etsi.org/REM/EventReason#AttachementFormatNotAccepted	13
http:uri.etsi.org/REM/EventReason#RecipientRejection	14
http:uri.etsi.org/REM/EventReason#RetentionPeriodExpired	15
http:uri.etsi.org/REM/EventReason#RegularEmailUnreachable	16
http:uri.etsi.org/REM/EventReason#RegularEmailNonOperational	17
http:uri.etsi.org/REM/EventReason#RegularEmailRejection	18
http:uri.etsi.org/REM/EventReason#PrintingSystemUnreachable	19
http:uri.etsi.org/REM/EventReason#PrintingSystemNonOperational	20
http:uri.etsi.org/REM/EventReason#PrintingBufferFull	21
http:uri.etsi.org/REM/EventReason#Other	22

Annex E (normative):
ASN.1 module for Evidences encoded in ASN.1

```
ETSI-REM-v1-88syntax { itu-t(0) identified-organization(4) etsi(0)
  tsl-specification (1234) id-mod(0) v1-88syntax (1) }
DEFINITIONS EXPLICIT TAGS ::=

BEGIN

-- EXPORTS All
IMPORTS
  -- Internet X.509 Public Key Infrastructure - Certificate and CRL Profile: RFC 5280
  Extensions
    FROM PKIX1Explicit88 { iso(1) identified-organization(3) dod(6) internet(1)
      security(5) mechanisms(5) pkix(7) id-mod(0) id-pkix1-explicit(18) }
  -- Cryptographic Message Syntax (CMS): RFC 3852
  ContentInfo
    FROM CryptographicMessageSyntax2004 { iso(1) member-body(2) us(840) rsadsi(113549)
      pkcs(1) pkcs-9(9) smime(16) modules(0) cms-2004(24) }
  -- Provision of harmonized Trust-service status information (TSL) - ETSI TS 102 231 V2.1.1
  NonEmptyURI, MultiLangString, MultiLangAddress, ElectronicAddresses
    FROM ETSI-TSL-v2-88syntax { itu-t(0) identified-organization(4) etsi(0)
      tsl-specification (2231) id-mod(0) v2-88syntax (1) }
  -- AFNOR - AuthorizedCertificate
  AuthorizedCertificate
    FROM EEvidencesCommon { iso(1) member-body(2) fr(250) type-org(1)
      aFNORStandardisation(127) letter(26) standard(74600) asn1-modules(3) common(0) }
;

id-rem OBJECT IDENTIFIER ::= { ETSI-REM-v1-88syntax }

id-rem-evidenceTypes OBJECT IDENTIFIER ::= { id-rem 1 }

id-rem-evidenceTypes-summbmissionAcceptanceRejection OBJECT IDENTIFIER ::= { id-rem-evidenceTypes 1 }
-- OID for SubmissionAcceptanceRejection evidence

id-rem-evidenceTypes-relayREMMDAcceptanceRejection OBJECT IDENTIFIER ::= { id-rem-evidenceTypes 2 }
-- OID for RelayREMMDAcceptanceRejection evidence

id-rem-evidenceTypes-RelayREMMDFailure OBJECT IDENTIFIER ::= { id-rem-evidenceTypes 3 } -- OID for
RelayREMMDFailure evidence

id-rem-evidenceTypes-DeliveryNonDeliveryToRecipient OBJECT IDENTIFIER ::= { id-rem-evidenceTypes 4 }
-- OID for DeliveryNonDeliveryToRecipient evidence

id-rem-evidenceTypes-DownloadNonDownloadByRecipient OBJECT IDENTIFIER ::= { id-rem-evidenceTypes 5 }
-- OID for DownloadNonDownloadByRecipient evidence

id-rem-evidenceTypes-RetrievalNonRetrievalByRecipient OBJECT IDENTIFIER ::= { id-rem-evidenceTypes 6
} -- OID for RetrievalNonRetrievalByRecipient evidence

id-rem-evidenceTypes-AcceptanceRejectionByRecipient OBJECT IDENTIFIER ::= { id-rem-evidenceTypes 7 }
-- OID for AcceptanceRejectionByRecipient evidence

id-rem-evidenceTypes-RelayToNonREMSystem OBJECT IDENTIFIER ::= { id-rem-evidenceTypes 8 } -- OID for
RelayToNonREMSystem evidence

id-rem-evidenceTypes-ReceivedFromNonREMSystem OBJECT IDENTIFIER ::= { id-rem-evidenceTypes 9 } --
OID for ReceivedFromNonREMSystem evidence


REMEvidence ::= SEQUENCE {

    version                       Version,
    eventCode                     INTEGER OPTIONAL,
    eventReasons                  EventReasons OPTIONAL,
    evidenceIdentifier            UTF8String (SIZE (1..MAX)),
    evidenceIssuerPolicyID        PolicyIdentifier OPTIONAL,
    evidenceIssuerDetails         EntityDetails,
    senderAuthenticationDetails   [0] AuthenticationDetails OPTIONAL,
    recipientAuthenticationDetails [1] AuthenticationDetails OPTIONAL,
    eventTime                     GeneralizedTime,
    submissionTime                GeneralizedTime OPTIONAL,
    replyTo                       UTF8String OPTIONAL,
```

```
    senderDetails                     UserDetails,
    recipientsDetails                 UserDetails OPTIONAL,
    recipientsDelegatesDetails    [2] RecipientsDelegatesDetails OPTIONAL,
    evidenceRefersToRecipient     [3] INTEGER OPTIONAL,
    messageDetails                [4] MessageDetails OPTIONAL,
    notificationDetails           [5] MessageDetails OPTIONAL,
    forwardedToExternalSystem     [6] UTF8String OPTIONAL,
    transactionLogInformation     [7] TransactionLogInformation OPTIONAL,
    extensions                    [8] Extensions OPTIONAL

}

Version ::= INTEGER { v1(1) }


EventReasons ::= SEQUENCE SIZE (1..MAX) OF {
    eventReason EventReason
}

EventReason ::= SEQUENCE {
    code    INTEGER,
    details UTF8String OPTIONAL
}

PolicyIdentifier ::= CHOICE {
    oid    OBJECT IDENTIFIER,
    uri    NonEmptyURI }

EntityDetails ::= SEQUENCE {
    entityName          MultiLangString,
    postalAddress       MultiLangAddress,
    unitName        [1] MultiLangString OPTIONAL,
    electronicAddress [2] ElectronicAddresses OPTIONAL
}

AuthenticationDetails ::= SEQUENCE {
    authenticationTime      GeneralizedTime,
    authenticationMethod    INTEGER,
    additionalDetails       AdditionalDetails OPTIONAL
}

AdditionalDetails ::= SEQUENCE SIZE (1..MAX) OF ContentInfo

UserDetails ::= SEQUENCE {
    electronicAdress    ElectronicAddresses,
    postalAddress       [1] MultiLangAddress OPTIONAL,
    certificateDetails  AuthorizedCertificate OPTIONAL
}

RecipientsDelegatesDetails ::= SEQUENCE SIZE (1..MAX) OF RecipientsDelegateDetails

RecipientsDelegateDetails ::= SEQUENCE {
    delegateDetails         UserDetails,
    delegatingRecipients    ListOfIntegers
}

ListOfIntegers ::= SEQUENCE SIZE (1..MAX) OF INTEGER


MessageDetails ::= SEQUENCE {
    isNotification              BOOLEAN,
    messageSubject              UTF8String,
    uaMessageIdentifier         [1] UTF8String OPTIONAL,
    messageIdentifierByREMMD    [2] UTF8String,
    hashAlgorithm               OBJECT IDENTIFIER OPTIONAL,
    hash                        BIT STRING OPTIONAL
}

TransactionLogInformation ::= SEQUENCE SIZE (1..MAX)OF {
    transactionLog  UTF8String
}

END
```

Annex F (normative):
XML Schema for Evidences encoded in XML

```xml
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema targetNamespace="uri.etsi.org/REM#" xmlns:rem="uri.etsi.org/REM#"
xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:tsl="http://uri.etsi.org/02231/v2#"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:xades="http://uri.etsi.org/01903/v1.3.2#"
elementFormDefault="qualified" attributeFormDefault="unqualified">

    <xs:import namespace="http://uri.etsi.org/01903/v1.3.2#"
schemaLocation="http://uri.etsi.org/01903/v1.3.2/XAdES.xsd"/>
    <xs:import namespace="http://uri.etsi.org/02231/v2#" schemaLocation="xxxx??"/> <!—At the time of
writing the present document no definitive URI is known for the xml schema of TS 102 231 v2.1.1 -->
    <xs:import namespace="http://www.w3.org/2000/09/xmldsig#"
schemaLocation="http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/xmldsig-core-schema.xsd"/>

    <xs:element name="SubmissionAcceptanceRejection" type="rem:REMEvidenceType"/>
    <xs:element name="RelayREMMDAcceptanceRejection" type="rem:REMEvidenceType"/>
    <xs:element name="RelayREMMDFailure" type="rem:REMEvidenceType"/>
    <xs:element name="DeliveryNonDeliveryToRecipient" type="rem:REMEvidenceType"/>
    <xs:element name="DownloadNonDownloadByRecipient" type="rem:REMEvidenceType"/>
    <xs:element name="RetrievalNonRetrievalByRecipient" type="rem:REMEvidenceType"/>
    <xs:element name="AcceptanceRejectionByRecipient" type="rem:REMEvidenceType"/>
    <xs:element name="RelayToNonREMSystem" type="rem:REMEvidenceType"/>
    <xs:element name="ReceivedFromNonREMSystem" type="rem:REMEvidenceType"/>


    <xs:complexType name="REMEvidenceType">
        <xs:sequence>
            <xs:element ref="rem:EventCode" minOccurs="0"/>
            <xs:element ref="rem:EventReasons" minOccurs="0"/>
            <xs:element name="EvidenceIdentifier" type="xs:string"/>
            <xs:element name="EvidenceIssuerPolicyID" type="xs:anyURI" minOccurs="0"/>
            <xs:element ref="rem:EvidenceIssuerDetails"/>
            <xs:element ref="rem:SenderAuthenticationDetails" minOccurs="0"/>
            <xs:element ref="rem:RecipientAuthenticationDetails" minOccurs="0"/>
            <xs:element name="EventTime" type="xs:dateTime"/>
            <xs:element name="SubmissionTime" type="xs:dateTime" minOccurs="0"/>
            <xs:element ref="ReplyTo" type="xs:string" minOccurs="0"/>
            <xs:element ref="rem:SenderDetails"/>
            <xs:element ref="rem:RecipientsDetails" minOccurs="0"/>
            <xs:element ref="rem:RecipientsDelegatesDetails" minOccurs="0"/>
            <xs:element name="EvidenceRefersToRecipient" type="xs:integer" minOccurs="0"/>
            <xs:element ref="rem:MessageDetails" minOccurs="0" maxOccurs="2"/>
            <xs:element ref="ForwardedToExternalSystem" type="xs:string" minOccurs="0"/>
            <xs:element ref="rem:TransactionLogInformation" minOccurs="0"/>
            <xs:element ref="rem:Extensions" minOccurs="0"/>
            <xs:element ref="ds:Signature" minOccurs="0"/>
        </xs:sequence>
        <xs:attribute name="version" type="xs:integer" use="required"/>
        <xs:attribute name="Id" type="xs:ID" use="optional"/>
    </xs:complexType>

    <xs:element name="EventCode" type="xs:anyURI"/>
    <xs:element name="EventReasons" type="rem:EventReasonsType"/>


    <xs:complexType name="EventReasonsType">
        <xs:sequence>
            <xs:element ref="rem:EventReason" maxOccurs="unbounded"/>
        </xs:sequence>
    </xs:complexType>
    <xs:element name="EventReason" type="rem:EventReasonType"/>
    <xs:complexType name="EventReasonType">
        <xs:sequence>
            <xs:element name="code" type="xs:anyURI"/>
            <xs:element name="Details" type="xs:string" minOccurs="0"/>
        </xs:sequence>
    </xs:complexType>
    <xs:element name="TransactionLogInformation" type="rem:TransactionLogInformationType"/>
    <xs:complexType name="TransactionLogInformationType">
        <xs:sequence>
            <xs:element ref="rem:TransactionLog" maxOccurs="unbounded"/>
        </xs:sequence>
    </xs:complexType>
    <xs:element name="TransactionLog" type="xades:AnyType"/>
```

ETSI

```xml
    <xs:element name="SenderDetails" type="rem:UserDetailsType" />
    <xs:element name="RecipientsDetails" type="rem:UserDetailsListType" />
    <xs:complexType name="UserDetailsType">
        <xs:sequence>
            <xs:element ref="tsl:ElectronicAddress"/>
            <xs:element ref="tsl:PostalAddress" minOccurs="0"/>
            <xs:element ref="rem:CertificateDetails" minOccurs="0"/>
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="UserDetailsListType">
        <xs:sequence>
            <xs:element name="UserDetails" maxOccurs="unbounded"/>
        </xs:sequence>
    </xs:complexType>
    <xs:element name="CertificateDetails" type="rem:CertificateDetailsType"/>
    <xs:complexType name="CertificateDetailsType">
        <xs:choice>
            <xs:element name="X509Certificate" type="xs:base64Binary"/>
            <xs:element name="CertID" type="xades:CertIDType"/>
            <xs:element ref="rem:CertIDAndSignature"/>
        </xs:choice>
    </xs:complexType>
    <xs:element name="CertIDAndSignature" type="rem:CertIDAndSignatureType"/>
    <xs:complexType name="CertIDAndSignatureType">
        <xs:sequence>
            <xs:element name="IssuerSerial" type="xades:DigestAlgAndValueType"/>
            <xs:element name="tbsCertificateDigestDetails" type="xades:DigestAlgAndValueType"/>
            <xs:element ref="rem:CertSignatureDetails"/>
        </xs:sequence>
    </xs:complexType>
    <xs:element name="CertSignatureDetails" type="rem:CertSignatureDetailsType"/>
    <xs:complexType name="CertSignatureDetailsType">
        <xs:sequence>
            <xs:element ref="ds:SignatureMethod"/>
            <xs:element ref="ds:SignatureValue"/>
        </xs:sequence>
    </xs:complexType>

    <xs:element name="RecipientsDelegatesDetails" type="rem:RecipientsDelegatesType" />
    <xs:complexType name="RecipientsDelegatesType">
        <xs:sequence maxOccurs="unbounded">
            <xs:element name="DelegateDetails" type="rem:UserDetailsType"/>
            <xs:element name="DelegatingRecipients" type="rem:ListOfIntegers"/>
        </xs:sequence>
    </xs:complexType>
    <xs:simpleType name="ListOfIntegers">
        <xs:list itemType="xs:integer"/>
    </xs:simpleType>

    <xs:element name="MessageDetails" type="rem:MessageDetailsType"/>
    <xs:complexType name="MessageDetailsType">
        <xs:sequence>
            <xs:element name="MessageSubject" type="xs:string" />
            <xs:element name="UAMessageIdentifier" type="xs:string" minOccurs="0"/>
            <xs:element name="MessageIdentifierByREMMD" type="xs:string"/>
            <xs:element ref="ds:DigestMethod" minOccurs="0"/>
            <xs:element ref="ds:DigestValue" minOccurs="0"/>
        </xs:sequence>
        <xs:attribute name="isNotification" type="xs:boolean" use="required"/>
    </xs:complexType>

    <xs:element name="EvidenceIssuerDetails" type="rem:EntityDetailsType"/>
    <xs:complexType name="EntityDetailsType">
        <xs:sequence>
            <xs:element name="EntityName" type="tsl:InternationalNamesType"/>
            <xs:element ref="tsl:PostalAddress"/>
            <xs:element name="UnitName" type="tsl:InternationalNamesType" minOccurs="0"/>
            <xs:element ref="tsl:ElectronicAddress" minOccurs="0"/>
        </xs:sequence>
    </xs:complexType>

    <xs:element name="SenderAuthenticationDetails" type="rem:AuthenticationDetailsType"/>
    <xs:element name="RecipientAuthenticationDetails" type="rem:AuthenticationDetailsType"/>
    <xs:complexType name="AuthenticationDetailsType">
        <xs:sequence>
            <xs:element name="AuthenticationTime" type="xs:dateTime"/>
            <xs:element name="AuthenticationMethod" type="xs:anyURI"/>
```

ETSI

```
            <xs:element name="AdditionalDetails" type="xades:AnyType" minOccurs="0"/>
        </xs:sequence>
    </xs:complexType>

    <xs:element name="Extensions" type="rem:ExtensionsListType"/>
    <xs:complexType name="ExtensionsListType">
        <xs:sequence maxOccurs="unbounded">
            <xs:element ref="rem:Extension"/>
        </xs:sequence>
    </xs:complexType>
    <xs:element name="Extension" type="rem:ExtensionType"/>
    <xs:complexType name="ExtensionType">
        <xs:complexContent>
            <xs:extension base="xades:AnyType">
                <xs:attribute name="isCritical" type="xs:boolean" use="optional" default="true"/>
            </xs:extension>
        </xs:complexContent>
    </xs:complexType>
</xs:schema>
```

Annex G (informative):
Bibliography

IETF RFC 3501: "Internet Message Access Protocol - Version 4rev".

History

Document history		
V1.1.1	October 2008	Publication