ETSI TS 102 640-2 V2.2.1 (2011-09)

Electronic Signatures and Infrastructures (ESI);
Registered Electronic Mail (REM);
Part 2: Data requirements, Formats and Signatures for REM

Reference
RTS/ESI-000071-2

Keywords
e-commerce, electronic signature, email, security,
trust services

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

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://ipr.etsi.org).

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

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. Full details of the entire series can be found in part 1 [i.2].

Introduction

Business and administrative relationships among companies, public administrations and private citizens, are 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 has 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. At the time of writing the present document, in some European Union Member States (Italy, Belgium, etc.) regulation(s) and application(s) are being developed**, if not 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 document 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 doccument assumes the usage of at least an Advanced Electronic Signature, with the meaning of article 2(2) of EU Directive 1999/93/EC [1] issued with a Secure Signature Creation Device, with the meaning of article 2(6) of the same Directive.

The summarised scope of each part and sub-part can be found in part 1 [i.2] of this multi-part deliverable.

1 Scope

The basic purpose of a Registered E-Mail service is to provide users, in addition to the usual services supplied by the ordinary e-mail service providers, with a set of evidence 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 Evidence 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 Evidence 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.
- Clause 7 provides a profiling of the service information for listing within a TSL.
- Annex A provides ASN.1 syntax for REM-MD Evidence.
- Annex B provides xml syntax for REM-MD Evidence.
- Annex C provides PDF syntax for REM-MD Evidence.
- Annex D provides a profiling for the SAML assertion to be used in REM-MD Evidence.
- Annex E specifies identifiers and codes for reporting events reasons in REM-MD Evidence.
- Annex F provides the ASN.1 definition for REM-MD Evidence encoded in ASN.1.
- Annex G provides the XML schema for REM-MD Evidence encoded in XML.
- Annex H provides a bibliography.

2 References

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

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

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

2.1 Normative references

The following referenced documents are necessary for the application of the present document.

[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: "Electronic Signatures and Infrastructures (ESI); 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 5751: "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification".

[9] IETF RFC 5322: "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)".

[17] ETSI TS 102 778: "Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles".

[18] ETSI TS 102 778-2: "Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 2: PAdES Basic - Profile based on ISO 32000-1".

[19] ETSI TS 102 778-3: "Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 3: PAdES Enhanced - PAdES-BES and PAdES-EPES Profiles".

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

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

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

[22] IETF RFC 4395: "Guidelines and Registration Procedures for New URI Schemes".

2.2 Informative references

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

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

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

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

[i.4] Void.

[i.5] Void.

[i.6] IETF RFC 2045: "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies".

[i.7] IETF RFC 2046: "Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types".

[i.8] STORK D5.1.8.b - Interface Specification, 31/7/2009.

NOTE: Available at: https://www.eid-stork.eu/index.php?option=com_processes&Itemid=&act=streamDocument&did=960, (last visited on 8th August, 2010).

[i.9] ETSI TS 102 640-4: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 4: REM-MD Conformance Profiles".

[i.10] ETSI TS 102 640-5: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 5: REM-MD Interoperability Profiles".

[i.11] ETSI TS 102 640-6-1: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 6: Interoperability Profiles; Sub-part 1: REM-MD UPU PReM Interoperability Profile".

[i.12] ETSI TS 102 640-6-2: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 6: Interoperability Profiles; Sub-part 2: REM-MD BUSDOX Interoperability Profile".

[i.13] ETSI TS 102 640-6-3: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 6: Interoperability Profiles; Sub-part 3: REM-MD SOAP Binding Profile".

[i.14] ISO/IEC 27001: "Information technology - Security techniques - Information security management systems - Requirements".

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] apply.

Throughout the present document a number of verbal forms are used, whose meaning is defined below:

- **may**, **need not:** indicate a course of action permissible within the limits of the present document.
- **shall, shall not:** indicate requirements strictly to be followed in order to conform to the present document and from which no deviation is permitted.

- **should, should not:** indicate that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required, or that (in the negative form) a certain possibility or course of action is deprecated but not prohibited.

3.2 Abbreviations

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

ADeS	Advanced Electronic Signature
ASN 1	Abstract Syntax Notation 1
EUMS	EU Member States
IANA	Internet Assigned Numbers Authority
MIME	Multipurpose Internet Mail Extensions
OID	Object IDentifier
PDF	Portable Document Format
QES	Qualified Electronic Signature
REM-MD	REM Management Domain
REM-PD	REM Policy Domain (defined in part 1)
R-REM-MD	Recipient's REM-MD
RSRI	REM-MD Repository Retrieval Interface
S&F	Store and Forward
S&N	Store and Notify
S/MIME	Secure/Multipurpose Internet Mail Extensions
SAML	Security Assertion Markup Language
SMTP	Simple Mail Transfer Protocol
SOAP	Simple Object Access Porotocol
S-REM-MD	Sender's REM-MD
STORK QAA	Quality Authentication Assurance
TrST	Trust Service Token

NOTE: As per TS 102 231 [6].

TSL	Trust-service Status List
UA	User Agent (defined in part 1)
URI	Uniform Resource Identifier
XML	Extendable Mark-up Language

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 actual message **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.6]). 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 multi-part/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 in figure 1.

<table>
<tr><td rowspan="11">REM-MD Envelope</td><td>Headers</td><td colspan="6">MIME message headers profiled for a multipart/signed MIME message (see clause 4.1)</td></tr>
<tr><td rowspan="10">Body</td><td rowspan="10">(signed data)</td><td>Headers</td><td colspan="5">MIME part headers profiled for a multipart/mixed message (see clause 4.2)</td></tr>
<tr><td rowspan="9">Body</td><td rowspan="3">REM-MD Introduction MIME section 0..1</td><td>Headers</td><td colspan="4">MIME part headers profiled for a multipart/alternative MIME content (see clause 4.4)</td></tr>
<tr><td rowspan="4">Body</td><td rowspan="2">Plain text introduction</td><td>Headers</td><td colspan="2">MIME part headers profiled for text/plain (see clause 4.4)</td></tr>
<tr><td>Body</td><td colspan="2">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</td></tr>
<tr><td rowspan="2">Html introduction</td><td>Headers</td><td colspan="2">MIME part headers profiled for text/html (see clause 4.4.2)</td></tr>
<tr><td>Body</td><td colspan="2">A message created by the REM-MD, which is intended to be displayed automatically upon display of the REM-MD Message/REM Dispatch. Html may contain URIs</td></tr>
<tr><td rowspan="2">Original Message MIME section 0..1</td><td>Head</td><td colspan="4">MIME part headers profiled for an enveloped message/rfc5322 message (see clause 4.5)</td></tr>
<tr><td>Body</td><td colspan="4">Optional full, self-contained RFC 5322 [9] message as submitted by the sender. (the Original Message). Only present in REM Dispatch</td></tr>
<tr><td rowspan="2">REM-MD Extensions MIME section 0..N</td><td>Headers</td><td colspan="4">MIME part headers profiled for application/xml (see clause 4.7)</td></tr>
<tr><td>Body</td><td colspan="4">Optional xml attachment to be used by possible extensions</td></tr>
<tr><td>REM-MD Evidenc</td><td>Headers</td><td colspan="4">MIME part headers profiled for an application/octet-stream, application/xml or application/pdf (see clause 4.7.1)</td></tr>
</table>

					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

Figure 1 presents the full structure including parts in grey which **should** be present in 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 **shall** be "multipart/signed". The 'protocol' parameter value **shall** be "application/pkcs7-signature". The 'micalg' parameter value **should** be conformant to TS 102 176-1 [5].
MIME-Version	The value for this header **shall** be "1.0".
Message-ID	This value **should** be an UID as defined in RFC 5322 [9].
Date	This value **shall** be compliant with clause 3.3 of RFC 5322 [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 **shall** be compliant with clause 3.6.3 of RFC 5322 [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).
Reply-To	The value for this header **shall** match the value of the 'From' header field in the Original Message.

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 either the REM-MD Evidence or REM-MD message, instead of forcing REM-MDs to go through the REM-MD Evidence.

The syntax of these optional parameters is one of the following:

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

where <value> **shall** be:

- "Dispatch" for a REM Dispatch (i.e. the Original Message by the sender is included)
- "Message" for any other REM-MD Message (i.e. a return receipt or a message generated by REM-MD containing URI references to REM Object or REM-MD Evidence)

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

where:

- <component> is a label (possibly related to the name of a REM-MD Evidence Component or subcomponent - see clause 5.2).
- <value> is a correspondent value for the component.

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

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

4.2 REM-MD Message/REM Dispatch Data Headers Constraints

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

4.3 REM-MD Signature Headers Constraints

The fields defined in the following table and their respective values shall adhere to the sections 3.2.1 and 3.4.3 of RFC 5751 [8].

Content-Type	The value for this header shall be: "application/pkcs7-signature; name=smime.p7s". The parameter 'name' should be present and its value should be "smime.p7s".
Content-Transfer-Encoding	This header **should** be present.The value for this header **shall** be: "base64".
Content-Disposition	The value for this header **shall** 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".

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

4.4 REM-MD Introduction Headers Constraints

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

The order chosen for the following alternative parts finishes with the most preferred choice from the email clients, as reported RFC 2046 [i.7] (the best choice is the LAST part of a type supported by the recipient system's local environment).

4.4.1 Multipart/alternative: Free text subsection Header constraints

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

4.4.2 Multipart/alternative: Html subsection Header constraints

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

This "alternative" part **shall** contain the same information of the Free Text part and the HTML **shall** not contain active code.

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

4.5 Original Message MIME Section Headers Constraints

Content-Type	The value for this field **shall** be: "message/rfc5322"; `name=AttachedMimeMessage`
Content-Transfer-Encoding:	`7bit`
Content-Disposition	The value for this field **shall** be: "attachment"; filename=`AttachedMimeMessage`
X-REM-Section-Type	The value of this optional field **should** be "rem_message/original".

This clause contains the Original Message and makes only sense when the message has to be conveyed to the Recipient by value (in the Store & Forward Style of operations).

4.6 REM-MD Extensions MIME Section Headers Constraints

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

The structure of this optional attachment is not defined here, since it is left for any possible extensions to be agreed on a peer-to-peer basis (e.g. Automatic processing of download URI in S&N style of operation, insertion of Electronic PostMark, etc.).

4.7 REM-MD Evidence MIME Section Headers Constraints

4.7.1 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 **shall** be "UTF-8"
Content-Transfer-Encoding	The value of this header **shall** 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

4.7.2 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 **shall** be "UTF-8"
Content-Transfer-Encoding	The value of this header **shall** 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

4.7.3 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 Evidence, 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 Evidence is presented in detail.

REM-MD Evidence are described with reference to a set of building blocks called "REM-MD Evidence components". In clause 0 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 Evidence are provided in annexes A, B and C.

5.1 REM-MD Evidence

In this clause the REM-MD Evidence 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	0 5.1.1 SubmissionAcceptanceRejection
6.2.1 Event A.2 - S- REM-MD Rejection	
6.2.2 Event B.1 - R-REM-MD Acceptance	0 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	0 5.1.3 RelayToREMMDFailure
6.2.3 Event C.1 - Message Delivery	0 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	0 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	0 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	0 5.1.7 AcceptanceRejectionByRecipient
6.2.4 Event H.1 - Successful forwarding for Ordinary e-mail	0 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 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 clauses 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	

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	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
I04	Sender Authentication details	0..1
M00	REM-MD Message/REM Dispatch details	1
M01	Reply-to	1
M03	Message Submission Time	1

5.1.2 RelayToREMMDAcceptanceRejection

<table>
<tr><td>Description</td><td>REM-MD Evidence that a successfully received REM-MD Message/REM Dispatch was accepted/rejected by the recipient's REM-MD</td></tr>
<tr><td>Optionality</td><td>It should be sent to the sender's REM-MD.
It may be sent back to the sender.</td></tr>
<tr><td>Purpose</td><td>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.</td></tr>
<tr><td>Related event</td><td>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.</td></tr>
<tr><td>Responsible for Issuance</td><td>Recipient's REM-MD.</td></tr>
<tr><td>Primary Intended Recipient</td><td>Sender's REM-MD.</td></tr>
<tr><td>REM-MD Evidence Components</td><td>
<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 = "RelayToREMMDAcceptanceRejection"</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..N</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>I03</td><td>Recipient referred to by the REM-MD Evidence</td><td>1</td></tr>
<tr><td>M00</td><td>REM-MD Message/REM Dispatch details</td><td>1</td></tr>
<tr><td>M02</td><td>Notification Message Tag</td><td>0..1</td></tr>
<tr><td>M03</td><td>Message Submission Time</td><td>1</td></tr>
</table>
</td></tr>
</table>

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. 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	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
		M02	Notification Message Tag	0..1
		M03	Message Submission Time	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 can be set in accordance with law, statutory requirements or local policy. The rules governing this time period **shall** be indicated in the REM-MD Practice Statement or REM Policy (see part 3).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. 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	0..1
I00	Sender's details	1
I01	Recipient's details	1..N
I02	Recipient's delegate details	0..N
I03	Recipient referred to by the Evidence	1
M00	REM-MD Message/REM Dispatch details	1
M02	Notification Message Tag	0..1
M03	Message Submission Time	1

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 (see note).			
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	0..1
		I00	Sender's details	1
		I01	Recipient's details	1..N
		I02	Recipient's delegate details	0..N
		I03	Recipient referred to by the Evidence	1
		I05	Recipient Authentication details	0..1
		M00	REM-MD Message/REM Dispatch details	1
		M03	Message Submission Time	1
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.				

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	0..1
I00	Sender's details	1
I01	Recipient's details	1..N
I02	Recipient's delegate details	0..N
I03	Recipient referred to by the Evidence	1
I05	Recipient Authentication details	0..1
M00	REM-MD Message/REM Dispatch details	1
M01	Reply-to	1
M02	Notification Message Tag	0..1
M03	Message Submission Time	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	0..1
	I00	Sender's details	1
	I01	Recipient's details	1..N
	I02	Recipient's delegate details	0..N
	I03	Recipient referred to by the Evidence	1
	I05	Recipient Authentication details	0..1
	M00	REM-MD Message/REM Dispatch details	1
	M02	Notification Message Tag	0..1
	M03	Message Submission Time	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. 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

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	0..1
I00	Sender's details	1
I01	Recipient's details	1..N
I02	Recipient's delegate details	0..N
I03	Recipient referred to by the Evidence	1
I05	Recipient Authentication details	0..1
M00	REM-MD Message/REM Dispatch details	1
M01	Reply-to	1
M02	Notification Message Tag	0..1
M03	Message Submission Time	1
M04	Forwarded to external system	1

5.1.9 ReceivedFromNonREMSystem

<table>
<tr><td>Description</td><td>Evidence that a message was successfully received from a regular (i.e. non REM) e-mail system</td></tr>
<tr><td>Optionality</td><td>O</td></tr>
<tr><td>Purpose</td><td>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.
This REM-MD Evidence will most likely be merged in the REM-MD Message/REM Dispatch that the recipient's REM-MD SHALL generate (see note).</td></tr>
<tr><td>Related event</td><td>The REM-MD received the message from a regular e-mail gateway.</td></tr>
<tr><td>Responsible for Issuance</td><td>Recipient's REM-MD</td></tr>
<tr><td>Primary Intended Recipient</td><td>Recipient</td></tr>
<tr><td>REM-MD Evidence Components</td><td>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.
It is recommended that the REM-MD Message or REM Dispatch including such evidence contains in the REM-MD Introduction a disclaimer like the following:
"On YYYY-MM-DD at hh:mm:ss (+ECT) the message having as subject "<original_subject>" was received, seemingly sent from address "xxxx@yyy.zz".
The REM-MD issuing this REM Dispatch takes commitment only on the time this message was received and that the information displayed in the attached Evidence have been transposed from the original message without any change. No other commitment is taken by the REM-MD."
<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..N</td></tr>
<tr><td>R01</td><td>Evidence issuer Policy Identifier</td><td>1..N</td></tr>
<tr><td>R02</td><td>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>I03</td><td>Recipient referred to by the Evidence</td><td>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>1</td></tr>
</table>
</td></tr>
<tr><td colspan="2">NOTE: 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.</td></tr>
</table>

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.

REM-MD Evidence	Component Class	Id	Component
	Core Components	G00	REM-MD Evidence Identifier
		G01	REM-MD Evidence Type
		G02	REM Event
		G03	Reason code (see note)
		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

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.

Figure 2: REM-MD Evidence generic template

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.
Usage Requirements	

5.2.2.1.2 G01 - REM-MD Evidence Type

Description	This field specifies the type of the REM-MD Evidence. The evidence type **shall** 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 evidence in different syntaxes and provide details on how this identification is performed.
Meaning	The REM-MD Evidence belongs to the given type.
Usage Requirements	

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 evidence 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.
Usage Requirements	

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 E 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, etc.) Reason Codes specified in clause 5.2.3.3. Reason clauses are to be used. Absence of Reason code means by default a positive event.
Usage Requirements	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.
Usage Requirements	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.
Usage Requirements	

5.2.2.1.7 G06 - Transaction log information

Description	This field contains the log of the transaction, specific to the transport protocol, regarding the 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.
Usage Requirements	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.
Usage Requirements	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.
Usage Requirements	This name **shall** 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 on the REM-MD Evidence under the responsibility of the REM-MD.
Format	Details provided in clause 6.
Meaning	Signature issued by the REM-MD or its provider on the REM-MD Evidence.
Usage Requirements	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).
Usage Requirements	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. Electronic address should be provided in such a way to fit to different kinds of communication infrastructures (SMTP, Web Services, etc.) hence it has to deal with multiple e-address schemes, which differ from e-mail addresses as defined by RFC 5322 [9]. REM end entity addresses shall be expressed as an URI according to RFC 3986 [21]. The URI scheme SHOULD be registered by IANA, according to RFC 4395 [22]. Example of possible values are: - "mailto" for SMTP based REM service addresses; - "http" or "https" for REM service addresses, as used for SOAP endpoints with http(s) binding. A REM end entity address shall be unique within the REM-PD it belongs. Each REM user in a REM-PD federation is identified by the tuple REM Address - Scheme Name. A REM address shall be validated according to its REM-MD policies. The information provided by the mandatory Scheme information URI (TS 102 231 [6], clause 5.3.7) shall specify how to perform such a validation and the specific mechanism required to locate the specific REM-MD the recipient belongs to.

NOTE: Use of IANA coded schemes is recommended, not mandated. This is not to exclude non listed schemes.

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).
Usage Requirements	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. At least one I01 component is present in each evidence, even if delegate recipient is present. The mailbox identifier **should** be the one under which the recipient has been authenticated by the REM-MD at issue. Electronic address should be provided in such a way to fit to different kinds of communication infrastructures (SMTP, Web Services, etc.) hence it has to deal with multiple e-address schemes, which differ from e-mail addresses as defined by RFC 5322 [9] and his successors. REM end entity addresses shall be expressed as an URI according to RFC 3986 [21]. The URI scheme SHOULD be registered by IANA, according to RFC 4395 [22]. Example of possible values are: - "mailto" for SMTP based REM service addresses; - "http" or "https" for REM service addresses, as used for SOAP endpoints with http(s) binding. A REM end entity address shall be unique within the REM-PD it belongs. Each REM user in a REM-PD federation is identified by the tuple REM Address - Scheme Name. A REM address shall be validated according to its REM-MD policies. The information provided by the mandatory Scheme information URI (TS 102 231 [6], clause 5.3.7) shall specify how to perform such a validation and the specific mechanism required to locate the specific REM-MD the recipient belongs to.

NOTE: Use of IANA coded schemes is recommended, not mandated. This is not to exclude non listed schemes.

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).
Usage Requirements	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.
Usage Requirements	

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.
Usage Requirements	Represent the following classes of authentication: a) Basic: Using basic authentication mechanisms such as passwords. The user **may** authenticate using passwords if protected and only used with an authenticated server. (e.g. using TLS/SSL); 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 to recognised standards such as given in TS 102 640-3 [i.3], clause 6.4.3; 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]). (See note). The default class of authentication is a) Basic. In case authentication mechanism has value of c), d) e) the sender's PKCS#7 detached (*.p7s) **shall** 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.
NOTE: See also TS 102 640-3 [i.3], clause 6.3 on "Sender/Recipient Authentication".	

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. Recipient authentication details refer either to recipient or to its delegate, according to which of the two is acting.
Usage Requirements	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]). (See note). The default class of authentication is Basic. In case authentication mechanism has value of c), d) e) the sender's PKCS#7 detached (*.p7s) **shall** 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.
NOTE: See also TS 102 640-3 [i.3], clause 6.3 on "Sender/Recipient Authentication").	

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, containing in particular: Message subject Message Identifier by UA Message Identifier by REM-MD Hash Algorithm Hash Value
Usage Requirements	The hashing algorithm shall also be specified (e.g. "SHA-1", "SHA256") in the REM Practice statement or REM Policy (see TS 102 640-3 [i.3], clause 6.1). Guidance on hashing algorithms is given in TS 102 176-1 [5]. Hash value shall be computed according to the following rules: 1) When the message is a REM Dispatch or a REM-MD message conveying a receipt: the hash is computed over the entire Original Message submitted by the sender, 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 the message is a REM-MD Message conveying a notification (S&N mode of operation): the hash is computed over the text of the notification message.

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.
Usage Requirements	

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. The default value for this component is "false".
Usage Requirements	

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.
Usage Requirements	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.).
Usage Requirements	

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 (see note)
Printing system unreachable
Printing system non operational
Printing buffer full
Other
NOTE: Reason codes provided by the e-mailing system can be specified.

6 REM Signatures

Clauses above have discussed the structure of the REM-MD Messages/REM Dispatches and the range of REM-MD Evidence 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 each REM-MD Evidence individually.
- S/MIME signature protecting all the MIME parts (including not only REM-MD Evidence) 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 Evidence, 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 Evidence 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 Evidence 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 Evidence **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 **should** be Advanced Electronic Signatures (AdES) as per specifications TS 101 903 (XAdES) [4] or TS 101 733 (CAdES) [3] or TS 102 778 [17] (PAdES).

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 **should** include a signed property containing the signing time claimed by the REM-MD.

NOTE: All the REM-MD Evidence 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 **should** 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 **should** be an XML Advanced Electronic Signature as specified in TS 101 903 (XAdES) [4].

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

2) The signature **should** be an "`Enveloping with data`" signature as specified in clause 5.2 of RFC 3852 [2].

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

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

5) The signature **should** 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 PAdES signatures. The signature profile specified in TS 102 778-2 [18] may be used. It is recommended that systems migrate to use TS 102 778-3 [19] by 2012.

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 **shall** be placed in the message using S/MIME multipart/signed as defined in RFC 5751 [8].

7 Profiling for REM Service information in Trusted-Service Status List

The use of TSL (TS 102 231 [6]) for building trust between different REM system is specified in clause 7 of TS 102 640-1 [i.2]. This clause specifies a profiling for REM services defined within a TSL.

The section describing a REM service **shall** be populated in conformance to TS 102 231 [6] with the restrictions defined in the following table.

TSL field	Optionality	Value (see TS 102 231 [6])
Service type identifier	M	Set to http://uri.etsi.org/TrstSvc/Svctype/REM.
Service digital identity	M	the TSP X.509 certificate associated to the key used to sign the REM-MD Evidences and optionally the corresponding X509SKI element.
Service Supply Point	M	This element provides information for access to the MD-RI (REM-MD Message and Evidence Relay Interface) defined in TS 102 640-1 [i.2]. Depending on the implemented protocol, the element **shall** provide a pointer to a web service or to a smtp server. Via appropriate conventions, a file containing service metadata information **may** be reachable based on this pointer.
TSP service definition URI	O	If present, this URI **shall** point to published general information relevant to the users like public certificates, addresses, etc.
Service information extensions	O	If present, extensions **shall not** be set as critical (see note).
NOTE: Use of extension is discouraged as they can create barriers to interoperability.		

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 evidence.

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 evidence **shall** 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.

```
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, LanguageTag, CountryCode
    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 EEvidenceCommon { 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 Evidence and provides details for their elements.

Clause A.2 specifies the different types of REM-MD Evidence 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 Evidence.

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

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

Below follows the ASN.1 definition for REM-MD Evidence.

```
REMEvidence ::= SEQUENCE {
    version                          Version,
    eventCode                        INTEGER OPTIONAL,
    eventReasons                     EventReasons OPTIONAL,
    evidenceIdentifier               UTF8String (SIZE (1..MAX)),
    evidenceIssuerPolicyID           [1] PolicyIdentifiers OPTIONAL,
    evidenceIssuerDetails            EntityDetails,
    senderAuthenticationDetails      [2] AuthenticationDetails OPTIONAL,
    recipientAuthenticationDetails   [3] AuthenticationDetails OPTIONAL,
    eventTime                        GeneralizedTime,
    submissionTime                   GeneralizedTime OPTIONAL,
    replyTo                          UTF8String OPTIONAL,
    senderDetails                    EntityDetails,
    recipientsDetails                EntityDetailsList,
    recipientsDelegatesDetails       [4] RecipientsDelegatesDetails OPTIONAL,
    evidenceRefersToRecipient        [5] INTEGER OPTIONAL,
    senderMessageDetails             [6] MessageDetails OPTIONAL,
    notificationDetails              [7] MessageDetails OPTIONAL,
    forwardedToExternalSystem        [8] UTF8String OPTIONAL,
    transactionLogInformation        [9] TransactionLogInformation OPTIONAL,
    extensions                       [10] 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 ::= 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 `PolicyIdentifiers` type, which is defined below.

```
PolicyIdentifiers ::= SEQUENCE SIZE (1..MAX) OF PolicyIdentifier

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

The content of this field will be a sequence of policies identifiers. Each policy identifier is 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 Evidence generated by a certain REM-MD Evidence Issuer **shall** 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 {
    namesPostalAddresses     [1] NamesPostalAddresses OPTIONAL,
    electronicAddresses      [2] ChoiceOfElectronicAddresses OPTIONAL,
    certificateDetails       [3] AuthorizedCertificate OPTIONAL,
    otherInformation         [4] ANY OPTIONAL
}

NamesPostalAddresses ::= SEQUENCE SIZE (1..MAX) OF NamePostalAddress

NamePostalAddress ::= SEQUENCE{
    entityName      [1] EntityName OPTIONAL,
    postalAddress   [2] PostalAddress OPTIONAL
}
```

```
EntityName ::= SEQUENCE {
    languageTag     [1] LanguageTag OPTIONAL,
    nameInstance    [2] UTF8String (SIZE (1..MAX))
}

PostalAddress ::= SEQUENCE {
  languageTag           LanguageTag,
  streetAddress         MultiLineStreetAddress,
  locality              UTF8String (SIZE (1..MAX)),
  stateOrProvince       [1] UTF8String (SIZE (1..MAX)) OPTIONAL,
  postalCode            UTF8String (SIZE (1..MAX)),
  countryName           CountryCode
}

MultiLineStreetAddress ::= SEQUENCE SIZE (1..MAX) OF UTF8String(SIZE (1..MAX))

ChoiceOfElectronicAddresses ::= SEQUENCE SIZE (1..MAX) OF
ChoiceOfElectronicAddress

ChoiceOfElectronicAddress ::= CHOICE {
     regularElectronicAddress          NonEmptyURI,
     attributedElectronicAddress       AttributedElectronicAddress
}
AttributedElectronicAddress ::= SEQUENCE {
        address         [1] NonEmptyURI,
        scheme          [2] IA5String(SIZE (1..MAX)),
        displayName     [3] UTF8String (SIZE (1..MAX))
}
```

When present, optional `namesPostalAddresses` field contains a list of `namePostalAddress` fields. Each `namePostalAddresss` **may** contain the entity's name (`entityName` field) and/or the postal address (`postalAddress` field) in a specific language, which is indicated by the corresponding `languageTag` fields within the types. Field `entityName` allows for more than one string for the name. Field `postalAddress` allows for more than one string for indicating details of the street.

When present, optional `ElectronicAddress` field contains the entity's electronic address (for instance an e-mail address, although not necessarily).

Field `certificateDetails` is an instance of `AuthorizedCertificate` type that contains details of the user's certificate. See [15] for details.

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". Strong: Using Strong authentication using client certificate via mutual SSL.
- "4". AdES: Using advanced electronic signatures.
- "5". AdES-Plus: Using advanced electronic signatures with Secure Signature Creation Devices (as defined in Directive 1999/93/EC [1]) or equivalent secure cryptographic device.
- "6". 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 `EntityDetails` type, which has been defined in clause A.1.5.

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 `EntityDetailsList` type, which is defined below.

```
EntityDetailsList ::= SEQUENCE SIZE (1..MAX) OF EntityDetails
```

Each `entityDetails` field contains the details of one of the recipients of the message.

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         EntityDetails,
    delegatingRecipients    ListOfIntegers
}

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

Field `delegateDetails` contains the details of the delegate in question.

Field `delegatingRecipients` 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 Fields senderMessageDetails and notificationMessageDetails

Fields `senderMessageDetails` and `notificationMessageDetails` are instances of `MessageDetails` type, which is defined below.

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

Field `isNotification` indicates whether the message whose details are provided is a notification (a message containing a pointer to the sender's message) or not. Absence of this field means that the message is not a notification.

If present, optional `messageSubject` field contains the value of the Subject field of the message.

If present, optional `uaMessageIdentifier` field contains an identifier as computed by the user's UA.

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

Finally, optional fields `hashAlgorithm` and `hash`, if present contain the message's digest algorithm identifier and the digest value computed on the sender's message respectively.

A.1.15.1 Field `senderMessageDetails`

Field `senderMessageDetails` has the semantics of M00 data element as specified in clause 5.2.2.4.1 when it contains details of the sender's message. As it has been said before this field is an instance of `MessageDetails` type.

Evidence not reporting events on notifications **shall** contain the `senderMessageDetails` field.

When this field is present in an evidence, the following requirements apply to their children fields:

- Field `isNotification` **may** be present (in which case its value **shall** be `"false"`) or not (as absence of this attribute means that the details do not correspond to a notification).
- Field `messageSubject` **shall** be present.
- Field `uaMessageIdentifier` **may** be present.
- Field `messageIdentifierByREMMD` **shall** be present.
- Fields `hashAlgorithm` and `hash` **shall** be present.

A.1.15.2 Field `notificationMessageDetails`

Field `notificationMessageDetails` has the semantics of M00 data element as specified in clause 5.2.2.4.1 when it contains the details of a notification (a message containing a pointer to the sender's message). This field is an instance of `MessageDetails` type.

Evidence reporting events on notifications **shall** contain the `notificationDetails` field. In addition, if evidence issuers have access to the sender's message details, then these evidence **should** also contain the `senderMessageDetails` field.

When this field is present in an evidence, the following requirements apply to their children fields:

- Field `isNotification` **shall** be present and its value **shall** be `"true"`.
- Field `messageSubject` **shall** be absent.
- Field `uaMessageIdentifier` **shall** be absent.
- Field `messageIdentifierByREMMD` **shall** be present.
- Fields `hashAlgorithm` and `hash` **shall** be present.

A.1.16 Field forwardedToExternalSystem

This field has 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 evidence **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 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.

Each extension in an evidence is designated as either critical or non-critical by the `critical` Boolean field. If this attribute is present, then the extension is designated as critical. An extension using system **shall** reject the evidence if it encounters a critical extension it does not recognize. A non-critical extension **may** be ignored if it is not recognized.

A.2 REM-MD Evidence

All the evidence 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-sumbmissionAcceptanceRejection 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 be able to 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 requirements
`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`	M	1	
`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.
`senderMessageDetails`	M	1	This field **shall** be present. The requirements for its children fields are specified in clause A.1.15.1.
`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 requirements
`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`	M	1	
`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.
`senderMessageDetails`	C	0..1	If the evidence is not an evidence on a notification, this field **shall** be present. If the evidence is an evidence on a notification and the issuer of the evidence has access to the details of the sender's message this field **should** be present. If the issuer does not have access to the details of sender's message this field **shall** be absent. If present, the requirements for its children fields are specified in clause A.1.15.1.
`notificationMessageDetails`	C	0..1	If the evidence is an evidence on a notification, this field **shall** be present. If the evidence is not an evidence on a notification this field **shall** be absent. If present, the requirements for its children fields are specified in clause A.1.15.2.
`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 requirements
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 deliver 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	
recipientsDetails	M	1	
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** be absent.
senderMessageDetails	C	0..1	If the evidence is not an evidence on a notification, this field **shall** be present. If the evidence is an evidence on a notification and the issuer of the evidence has access to the details of the sender's message this field **should** be present. If present, the requirements for its children fields are specified in clause A.1.15.1.
notificationMessageDetails	C	0..1	If the evidence is an evidence on a notification, this field **shall** be present. If the evidence is not an evidence on a notification this field **shall** be absent. If present, the requirements for its children fields are specified in clause A.1.15.2.
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 requirements
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".

Element/Attribute	Mand. Opt.	Number occurrences	Additional requirements
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	
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** be absent.
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	
recipientsDetails	M	1	
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.
senderMessageDetails	C	0..1	If the evidence is not an evidence on a notification, this field **shall** be present. If the evidence is an evidence on a notification and the issuer of the evidence has access to the details of the sender's message this field **should** be present. If the issuer does not have access to the details of sender's message this field **shall** be absent. If present, the requirements for its children fields are specified in clause A.1.15.1.
notificationMessageDetails	C	0..1	If the evidence is an evidence on a notification, this field **shall** be present. If the evidence is not an evidence on a notification this field **shall** be absent. If present, the requirements for its children fields are specified in clause A.1.15.2.
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 requirements
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	
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.
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	
recipientsDetails	M	1	
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.
senderMessageDetails	M	1	This field **shall** be present. The requirements for its children fields are specified in clause A.1.15.1.
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 requirements
`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	
`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.
`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	
`senderDetails`	M	1	
`recipientsDetails`	M	1	
`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.
`senderMessageDetails`	C	0..1	If the evidence is not an evidence on a notification, this field **shall** be present. If the evidence is an evidence on a notification and the issuer of the evidence has access to the details of the sender's message this field **should** be present. If the issuer does not have access to the details of sender's message this field **shall** be absent. If present, the requirements for its children fields are specified in clause A.1.15.1.

Element/Attribute	Mand. Opt.	Number occurrences	Additional requirements
notificationMessageDetails	C	0..1	If the evidence is an evidence on a notification, this field **shall** be present. If the evidence is not an evidence on a notification this field **shall** be absent. If present, the requirements for its children fields are specified in clause A.1.15.2.
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 requirements
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	
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.
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	
recipientsDetails	M	1	
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.

Element/Attribute	Mand. Opt.	Number occurrences	Additional requirements
senderMessageDetails	C	0..1	If the evidence is not an evidence on a notification, this field **shall** be present. If the evidence is an evidence on a notification and the issuer of the evidence has access to the details of the sender's message this field **should** be present. If the issuer does not have access to the details of sender's message this field **shall** be absent. If present, the requirements for its children fields are specified in clause A.1.15.1.
notificationMessageDetails	C	0..1	If the evidence is an evidence on a notification, this field **shall** be present. If the evidence is not an evidence on a notification this field **shall** be absent. If present, the requirements for its children fields are specified in clause A.1.15.2.
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 requirements
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	
recipientsDetails	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.
senderMessageDetails	C	0..1	If the evidence is not an evidence on a notification, this field **shall** be present. If the evidence is an evidence on a notification and the issuer of the evidence has access to the details of the sender's message this field **should** be present. If the issuer does not have access to the details of sender's message this field **shall** be absent. If present, the requirements for its children fields are specified in clause A.1.15.1.

Element/Attribute	Mand. Opt.	Number occurrences	Additional requirements
notificationMessageDetails	C	0..1	If the evidence is an evidence on a notification, this field **shall** be present. If the evidence is not an evidence on a notification this field **shall** be absent. If present, the requirements for its children fields are specified in clause A.1.15.2.
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 requirements
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	
recipientsDetails	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	This field **shall** be present. The requirements for its children fields are specified in clause A.1.15.1.
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 Evidence and provides details for their elements.

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

B.1 REM-MD Evidence Structure

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

Namespace's URI	Namespace's prefix
http://uri.etsi.org/02640/v1#	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 Evidence.

```
<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:choice minOccurs="0">
                <xs:element name="ReplyTo" type="xs:string"/>
                <xs:element name="ReplyToAddress" type="rem:AttributedElectronicAddressType"/>
        </xs:choice>
        <xs:element ref="rem:SenderDetails" />
        <xs:element ref="rem:RecipientsDetails" />
        <xs:element ref="rem:RecipientsDelegatesDetails" minOccurs="0" />
        <xs:element name="EvidenceRefersToRecipient" type="xs:integer"
          minOccurs="0" />
        <xs:element ref="rem:SenderMessageDetails" minOccurs="0" />
        <xs:element ref="rem:NotificationMessageDetails" minOccurs="0" />
        <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:string" 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 is **`"1.2.1"`**. It 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/02640/Event#Acceptance": Acceptance of some REM Message by some entity.
- "http:uri.etsi.org/02640/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 5.2.2.2.1.

Below follows the xml schema for this element.

```
<xs:element name="EvidenceIssuerPolicyID" type="rem:EvidenceIssuerPolicyIDType"/>
<xs:complexType name="EvidenceIssuerPolicyIDType">
    <xs:sequence>
        <xs:element name="PolicyID" type="xs:anyURI" maxOccurs="unbounded"/>
    </xs:sequence>
</xs:complexType>
```

The content of this element is a sequence of URIs each one identifying one of the applicable policies. Should one of these policies be identified by an OID, the content of this element **shall** 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 Evidence generated by a certain REM-MD Evidence Issuer **shall** 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. It is based on <rem:EntityDetailsType>, described in the following:

```
<xs:element name="EvidenceIssuerDetails" type="rem:EntityDetailsType"/>
```

B.1.5.1 Element <rem:AttributedElectronicAddress>

To be able to support different formats of e-addresses, this element is defined as an alternative to the <tsl:electronicAddress> as defined in TS 102 231 [6], which provides no possibility to outline the scheme of an e-address value as well as an optional "Display Name" as in use by standard e-mail (see RFC 5322 [9] for details).

```
<xs:complexType name="AttributedElectronicAddressType">
    <xs:simpleContent>
        <xs:extension base="tsl:NonEmptyURIType">
            <xs:attribute name="scheme" type="xs:QName" default="mailto">
                <xs:annotation>
                    <xs:documentation>Defaults to mailto, if not present</xs:documentation>
                </xs:annotation>
            </xs:attribute>
            <xs:attribute name="DisplayName" type="tsl:NonEmptyString"/>
        </xs:extension>
    </xs:simpleContent>
  </xs:complexType>
```

Element <rem:AttributedElectronicAddress> carries the mandatory, non-empty e-address in the format xs:anyURI. The @scheme attribute **shall** outline the scheme of the e-address value in the form of xs:string. tsl:NonEmptyURIType and tsl:NonEmptyStringType are defined in TS 102 231 [6].

<rem:AttributedElectronicAddress> attribute scheme is a mandatory, non-empty attribute of type xs:string, outlining the scheme of the e-address.

<rem:AttributedElectronicAddress> attribute DisplayName is an optional attribute of type xs:string, carrying a "display-name" related to the e-address.

B.1.5.2 Element <EntityDetailsType>

Below follows the xml schema for this element:

```
<xs:element name="EvidenceIssuerDetails" type="rem:EntityDetailsType"/>

<xs:complexType name="EntityDetailsType">
        <xs:sequence>
                <xs:element ref="rem:NamesPostalAddresses" minOccurs="0"/>
                <xs:choice minOccurs="0" maxOccurs="unbounded">
                        <xs:element ref="rem:AttributedElectronicAddress"/>
                        <xs:element ref="tsl:ElectronicAddress"/>
                </xs:choice>
                <xs:element ref="rem:CertificateDetails" minOccurs="0"/>
                <xs:element ref="xades:Any" minOccurs="0"/>
        </xs:sequence>
</xs:complexType>

<xs:element name="NamesPostalAddresses" type="rem:NamesPostalAddressListType"/>
<xs:complexType name="NamesPostalAddressListType">
    <xs:sequence>
        <xs:element ref="rem:NamePostalAddress" maxOccurs="unbounded"/>
    </xs:sequence>
</xs:complexType>

<xs:element name="NamePostalAddress" type="rem:NamePostalAddressType"/>
<xs:complexType name="NamePostalAddressType">
    <xs:sequence>
        <xs:element ref="rem:EntityName" minOccurs="0"/>
        <xs:element ref="rem:PostalAddress" minOccurs="0"/>
    </xs:sequence>
</xs:complexType>

<xs:element name="EntityName" type="rem:EntityNameType"/>
<xs:complexType name="EntityNameType">
    <xs:sequence>
        <xs:element name="Name" type="xs:string" maxOccurs="unbounded"/>
    </xs:sequence>
    <xs:attribute ref="xml:lang" use="optional"/>
</xs:complexType>

<xs:element name="PostalAddress" type="rem:PostalAddressType"/>
<xs:complexType name="PostalAddressType">
    <xs:sequence>
        <xs:element name="StreetAddress" type="tsl:NonEmptyString" maxOccurs="unbounded"/>
        <xs:element name="Locality" type="tsl:NonEmptyString"/>
        <xs:element name="StateOrProvince" type="tsl:NonEmptyString" minOccurs="0"/>
        <xs:element name="PostalCode" type="tsl:NonEmptyString"/>
        <xs:element name="CountryName" type="tsl:NonEmptyString"/>
    </xs:sequence>
    <xs:attribute ref="xml:lang" use="optional"/>
</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>
```

When present, optional <NamesPostalAddresses> element contains a list of <NamePostalAddresss> elements. Each <NamePostalAddresss> **may** contain the entity's name (<EntityName> element) and/or the postal address (<PostalAddress> element) in a specific language, which is indicated by their optional lang attributes. <EntityName> allows for more than one string for the name. <PostalAddress> allows for more than one string for indicating details of the street.

When present, optional <tsl:ElectronicAddress> element contains the entity's electronic address (for instance an e-mail address, although not necessarily).

When present, optional <CertificateDetails> element contains the entity's certificate details. These **may** be one of the following:

- Entity's X509 certificate itself within element <rem:X509Certificate>.
- Entity's X509 certificate identifier within element <rem:CertID>. This is an instance of xades:CertIDType. See TS 101 903 [4] for more details.
- Entity'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.1.6 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="SenderAuthenticationDetails" type="rem:AuthenticationDetailsType"/>
<xs:complexType name="AuthenticationDetailsType">
    <xs:sequence>
        <xs:choice>
            <xs:sequence>
                <xs:element name="AuthenticationTime" type="xs:dateTime"/>
                <xs:element name="AuthenticationMethod" type="xs:anyURI"/>
            </xs:sequence>
            <xs:element ref="saml:Assertion"/>
        </xs:choice>
        <xs:element name="AdditionalDetails" type="xades:AnyType" minOccurs="0"/>
    </xs:sequence>
</xs:complexType>
```

Authentication datails can be expressed directly (with the couple <rem:AuthenticationMethod>, < rem:AuthenticationTime>) or, alternatively, with a SAML assertion.

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

Element <rem:AuthenticationMethod> indicates 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#Strong". Strong authentication using client certificate via mutual SSL.
- "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.

When choosing <saml:assertion> instead, the profiling defined in appendix D **shall** be adopted.

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.

The original `rem:REMEvidenceType` contains an element `<ReplyTo>` of type `xs:String`. To deal with the `rem:ElectronicAddressType` for the "reply-to" information, the `rem:REMEvidenceType` is extended by the element `<ReplyToAddress>`. As outlined above, implementations of the present document **shall** always provide this child element instead of `<rem:ReplyTo>` and then **shall** provide a value of "2" in the `@version` attribute of the top element of type `rem:REMEvidenceType`.

```
<xs:complexType name="REMEvidenceType">
        <xs:complexContent>
            <xs:extension base="rem:REMEvidenceType">
                <xs:sequence>
                    <xs:element name="ReplyToAddress" type="rem:ExtendedElectronicAddressType"
minOccurs="0"/>
                </xs:sequence>
            </xs:extension>
        </xs:complexContent>
    </xs:complexType>
```

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:EntityDetailsType" />
```

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:EntityDetailsListType" />
<xs:complexType name="EntityDetailsListType">
    <xs:sequence>
        <xs:element name="EntityDetails" type="rem:EntityDetailsType" maxOccurs="unbounded"/>
    </xs:sequence>
</xs:complexType>
```

Each `<EntityDetails>` element contains the details of one of the recipients of the message.

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 Elements <rem:senderMessageDetails> and <rem:notificationMessageDetails>

Elements <rem:senderMessageDetails> and <rem:notificationMessageDetails> are instances of MessageDetails type, whose xml schema is shown below:

```
<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="optional"/>
</xs:complexType>
```

Optional attribute isNotification indicates whether the details corresponds to notification (a message containing a pointer to the sender's message) or not. Absence of this attribute means that the message is not a notification.

If present, optional <rem:MessageSubject> element contains the value of the Subject field of the message.

If present, 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:DigestMethod> and <ds:DigestValue> optional elements contain, when they are present, the message's digest algorithm identifier and the digest value computed on the sender's message respectively.

B.1.15.1 Element <rem:senderMessageDetails>

Element <rem:senderMessageDetails> has the semantics of M00 data element as specified in clause 5.2.2.4.1 when it contains details of the sender's message. As it has been said before this field is an instance of MessageDetails type. Below follows its XML schema definition:

```
<xs:element name="SenderMessageDetails" type="rem:MessageDetailsType"/>
```

Evidence not reporting events on notifications **shall** contain the <rem:senderMessageDetails> element.

When this element is present in an evidence, the following requirements apply to their children and attributes:

- Attribute `IsNotification` **may** be present (in which case its value **shall** be `"false"`) or not (as absence of this attribute means that the details do not correspond to a notification).
- Element `<rem:MessageSubject>` **shall** be present.
- Element `<rem:UAMessageIdentifier>` **may** be present.
- Element `<rem:MessageIdentifierByREMMD>` **shall** be present.
- Elements `<ds:DigestMethod>` and `<ds:DigestValue>` **shall** be present.

B.1.15.2 Element <rem:notificationMessageDetails>

Element `<rem:notificationMessageDetails>` has the semantics of M00 data element as specified in clause 5.2.2.4.1 when it contains the details of a notification (a message containing a pointer to the sender's message). This field is an instance of `MessageDetails` type. Below follows its XML schema definition:

```
<xs:element name="NotificationMessageDetails" type="rem:MessageDetailsType"/>
```

Evidence reporting events on notifications **shall** contain the `<rem:notificationMessageDetails>` element. In addition, if evidence issuers have access to the sender's message details, then these evidence **should** also contain the `<rem:senderMessageDetails>` element.

When this element is present in an evidence, the following requirements apply to their children and attributes:

- Attribute `IsNotification` **shall** be present and its value **shall** be `"true"`.
- Element `<rem:MessageSubject>` **shall** be absent.
- Element `<rem:UAMessageIdentifier>` **shall** be absent.
- Element `<rem:MessageIdentifierByREMMD>` **shall** be present.
- Elements `<ds:DigestMethod>` and `<ds:DigestValue>` **shall** be present.

B.1.16 Element <rem:ForwardedToExternalSystem>

This element has 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 evidence 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.

Below follows the xml schema for this element:

```
<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"/>
        </xs:extension>
    </xs:complexContent>
</xs:complexType>
```

This element contains a list of extensions.

Each extension in an evidence is designated as either critical or non-critical by the `isCritical` boolean attribute. If this attribute is absent, then the extension is designated as non critical.

An extension using system **shall** reject the evidence if it encounters a critical extension it does not recognize. A non-critical extension **may** be ignored if it is not recognized.

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.

B.2 REM-MD Evidence

This clause defines formats for different types of Evidence, 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 requirements
`Attribute version`	M	1	Value: `"2"` 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`	M	1	
`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 not** appear.
`rem:SenderMessageDetails`	M	1	This element **shall** be present. The requirements for its attributes and children elements are specified in clause B.1.15.1.
`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 requirements
Attribute version	M	1	Value: "2" for this version.
rem:EventCode	M	1	Value if acceptance by receiving REM-MD: "Acceptance". Value if rejection by receiving 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 to be relayed.
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	M	1	
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 not** 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:SenderMessageDetails	C	0..1	If the evidence is not an evidence on a notification, this element **shall** be present. If the evidence is an evidence on a notification and the issuer of the evidence has access to the details of the sender's message this element **should** be present. If the issuer does not have access to the details of sender's message this element **shall** be absent. If present, the requirements for its children elements and attributes are specified in clause B.1.15.1.
rem:NotificationMessageDetails	C	0..1	If the evidence is an evidence on a notification, this element **shall** be present. If the evidence is not an evidence on a notification this element **shall** be absent. If present, the requirements for its attributes and children elements are specified in clause B.1.15.2.
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 requirements
Attribute version	M	1	Value: "2" 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 sending REM-MD could not deliver the message to the receiving 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	M	1	
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:SenderMessageDetails	C	0..1	If the evidence is not an evidence on a notification, this element **shall** be present. If the evidence is an evidence on a notification and the issuer of the evidence has access to the details of the sender's message this element **should** be present. If the issuer does not have access to the details of sender's message this element **shall** be absent. If present, the requirements for its children elements and attributes are specified in clause B.1.15.1.
rem:NotificationMessageDetails	C	0..1	If the evidence is an evidence on a notification, this element **shall** be present. If the evidence is not an evidence on a notification this element **shall** be absent. If present, the requirements for its attributes and children elements are specified in clause B.1.15.2.
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 requirements
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:RecipientAuthentication Details	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	M	1	
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.

Element/Attribute	Mand. Opt.	Number occurrences	Additional requirements
rem:SenderMessageDetails	C	0..1	If the evidence is not an evidence on a notification, this element **shall** be present. If the evidence is an evidence on a notification and the issuer of the evidence has access to the details of the sender's message this element **should** be present. If the issuer does not have access to the details of sender's message this element **shall** be absent. If present, the requirements for its children elements and attributes are specified in clause B.1.15.1.
rem:NotificationMessageDetails	C	0..1	If the evidence is an evidence on a notification, this element **shall** be present. If the evidence is not an evidence on a notification this element **shall** be absent. If present, the requirements for its attributes and children elements are specified in clause B.1.15.2.
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 requirements
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 requirements
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	M	1	
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:SenderMessageDetails	M	1	This element **shall** be present. The requirements for its attributes and children elements are specified in clause B.1.15.1.
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 requirements
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	M	1	
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.

Element/Attribute	Mand. Opt.	Number occurrences	Additional requirements
rem:SenderMessageDetails	C	0..1	If the evidence is not an evidence on a notification, this element **shall** be present. If the evidence is an evidence on a notification and the issuer of the evidence has access to the details of the sender's message this element **should** be present. If the issuer does not have access to the details of sender's message this element **shall** be absent. If present, the requirements for its children elements and attributes are specified in clause B.1.15.1.
rem:NotificationMessageDetails	C	0..1	If the evidence is an evidence on a notification, this element **shall** be present. If the evidence is not an evidence on a notification this element **shall** be absent. If present, the requirements for its attributes and children elements are specified in clause B.1.15.2.
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 requirements
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.

Element/Attribute	Mand. Opt.	Number occurrences	Additional requirements
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.
replyTo	O	0..1	
rem:SenderDetails	M	1	
rem:RecipientsDetails	M	1	
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:senderMessageDetails	C	0..1	If the evidence is not an evidence on a notification, this element **shall** be present. If the evidence is an evidence on a notification and the issuer of the evidence has access to the details of the sender's message this element **should** be present. If the issuer does not have access to the details of sender's message this element **shall** be absent. If present, the requirements for its children elements and attributes are specified in clause B.1.15.1.
rem:notificationMessageDetails	C	0..1	If the evidence is an evidence on a notification, this element **shall** be present. If the evidence is not an evidence on a notification this element **shall** be absent. If present, the requirements for its attributes and children elements are specified in clause B.1.15.2.
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 requirements
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

Element/Attribute	Mand. Opt.	Number occurrences	Additional requirements
			forwarding time.
replyTo	O	0..1	
rem:SenderDetails	M	1	
rem:RecipientsDetails	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:SenderMessageDetails	C	0..1	If the evidence is not an evidence on a notification, this element **shall** be present. If the evidence is an evidence on a notification and the issuer of the evidence has access to the details of the sender's message this element **should** be present. If the issuer does not have access to the details of sender's message this element **shall** be absent. If present, the requirements for its children elements and attributes are specified in clause B.1.15.1.
rem:NotificationMessageDetails	C	0..1	If the evidence is an evidence on a notification, this element **shall** be present. If the evidence is not an evidence on a notification this element **shall** be absent. If present, the requirements for its attributes and children elements are specified in clause B.1.15.2.
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 requirements
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:RecipientsDetails	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:SenderMessageDetails	M	1	This element **shall** be present. The requirements for its attributes and children elements are specified in clause B.1.15.1.
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 Evidence 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 Evidence be signed, sign the PDF/A-1 file generated in step 3 using PDF signatures as specified in clause 6.3.3.

NOTE: The XFA forms architecture may be used to create PDF documents mapping the XML data to PDF form fields. It is recommended that the XFA template maps the XML data element names directly to form fields with equivalent names and that PDF includes text associated with the form fields describing the meaning of each field in an appropriate language.

Annex D (normative): SAML token profiling

Format details and semantics are described in OASIS SAML V2.0 core specification [20]. In the following a profiling for `saml2:Assertion` is provided.

NOTE: The definition of this token is aligned to and in many parts conformant with the specification of the SAML Assertion defined in the STORK D5.8.1b Interface Specification [i.8]. A major difference is the introduction of a new assertion attribute. Besides the QAA authentication level defined by STORK, a REM-MD may also provide a sender's QAA registration level.

D.1 Element <saml2:Issuer>

This mandatory element **shall** contain the URI that identifies the issuing REM-MD. (it is expected that this URI be the one which identify the REM-MD in a TSL `<tsl:ServiceSupplyPoint>`).

D.2 Element <ds:Signature >

Mandatory element; in order to use the SAML assertion as transferable token in other contexts, the assertion must be signed by the issuing REM-MD. An XML Signature authenticates the issuing REM-MD and ensures message integrity (signature over complete assertion). The signature must be an enveloped signature and applied to the `saml2:Assertion` element and all its children. The signature must contain a single `ds:Reference` containing the `saml2:Assertion/ID` attribute value and must be signed using the certificate defined within the REM-MD's TSL entry).

D.3 Element <saml2:Subject>

Only the element `saml2:NameID` and `saml2:SubjectConfirmation` are used.

D.3.1 Element <saml2:Subject/saml2:NameId >

Mandatory identifier that represents the Subject. The attribute `SPNameQualifier` **shall not** be used.

D.3.2 Element <saml2:Subject/saml2:SubjectConfirmation>

This mandatory element provides means for verification of the correspondence between the SAML subject (sender) with the party whom the relying party is communicating with (destination REM-MD).

Attribute "method" **shall** be present with a value of "`urn:oasis:names:tc:SAML:2.0:cm:sender-vouches`", which denotes that the issuing REM-MD vouches for the subject confirmation of the sender.

Elements `<saml2:Subject>/<saml2:SubjectConfirmation>/<saml2:BaseId>`, `.<saml2:NameId>`, `.<saml2:EncryptedID>` **shall not** be used.

D.3.2.1 Element <saml2:Subject/saml2:SubjectConfirmation/ saml2:SubjectConfirmationData>

This mandatory element specifies additional data allowing the SAML subject (sender) to be confirmed. Rules for attributes of this element.

Table D.1: SubjectConfirmationData attributes of a sender's SAML assertion

Attribute	Support	Notes
`@NotBefore`	**shall**	Subject (sender) cannot be confirmed before this time.
`@NotOnOrAfter`	**shall**	Subject cannot be confirmed on or after this time.
`@Recipient`	**shall**	URI reference of the REM-MD this assertion is being sent to.
`@InResponseTo`	**shall not**	Id of the Request that requested this assertion.
`@Address`	**shall not**	IP address of user that this assertion was issued to.

D.4 Element <saml2:Conditions>

This mandatory element specifies conditions that must be evaluated when using the `saml2:Assertion`. Following attributes **shall** be provided.

Table D.2: Conditions Attributes of an Authentication Response

Attribute	Support	Notes
`@NotBefore`	**shall**	Assertion not valid before this time.
`@NotOnOrAfter`	**shall**	Assertion not valid on or after this time.

Element `<saml2:Advice>` **shall not** be used.

Element `<saml2:OneTimeUse>` **shall not** be used.

D.4.1 Element <saml2:Conditions/saml2:AudienceRestriction>

Mandatory element; used to restrict the audience of this assertion to the specific destination domain by outlining its URI reference. This URI must be identical to the URI value defined within the TSL.

D.5 Element <saml2:AuthnStatement>

Mandatory element; it's attribute `SessionIndex` **shall not** be used.

Element `<saml2:AuthnStatement>`/`<saml2:SubjectLocality>` **shall not** be used.

D.5.1 Element <saml2:AuthnStatement/saml2:AttributeStatement>

This optional element contains several `saml2:Attribute` child elements carrying information associated with the SAML subject (sender).

At least one `<saml2:Attribute>` **shall** be provided.

To provide information about the end entity's initial registration process strength, the following `<saml2:Attribute>` element is defined and **may** be provided:

@Name = `"http:uri.etsi.org/REM /AuthenticationMethod"`

@NameFormat = **"**`urn:oasis:names:tc:SAML:2.0:attrname-format:uri`**"**

@FriendlyName m= `"Authentication Method"`

<saml2:AttributeValue>: The value of the elements denotes the registration strength level in the format xs**:**anyURI with possible values defined in clause B.1.6.

Annex E (normative): Event reason identifiers and codes

Element <rem:EventReason> in XML evidence and field eventReason in ASN.1 identify the event reason. In XML evidence the content of the element is an URI. In ASN.1 evidence 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 F (normative): ASN.1 module for Evidence 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, LanguageTag, CountryCode
    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 EEvidenceCommon { 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-sumbmissionAcceptanceRejection 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


REMEvidence ::= SEQUENCE {
    version                         Version,
    eventCode                       INTEGER OPTIONAL,
    eventReasons                    EventReasons OPTIONAL,
    evidenceIdentifier              UTF8String (SIZE (1..MAX)),
    evidenceIssuerPolicyID          [1] PolicyIdentifiers OPTIONAL,
    evidenceIssuerDetails           EntityDetails,
    senderAuthenticationDetails     [2] AuthenticationDetails OPTIONAL,
    recipientAuthenticationDetails  [3] AuthenticationDetails OPTIONAL,
    eventTime                       GeneralizedTime,
    submissionTime                  GeneralizedTime OPTIONAL,
    replyTo                         UTF8String OPTIONAL,
    senderDetails                   EntityDetails,
```

```
    recipientsDetails               EntityDetailsList,
    recipientsDelegatesDetails      [4] RecipientsDelegatesDetails OPTIONAL,
    evidenceRefersToRecipient       [5] INTEGER OPTIONAL,
    senderMessageDetails            [6] MessageDetails OPTIONAL,
    notificationDetails             [7] MessageDetails OPTIONAL,
    forwardedToExternalSystem       [8] UTF8String OPTIONAL,
    transactionLogInformation       [9] TransactionLogInformation OPTIONAL,
    extensions                      [10] Extensions OPTIONAL
}

Version ::= INTEGER { v1(1) }

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

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

PolicyIdentifiers ::= SEQUENCE SIZE (1..MAX) OF PolicyIdentifier

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

EntityDetails ::= SEQUENCE {
    namesPostalAddresses     [1] NamesPostalAddresses OPTIONAL,
    electronicAddresses      [2] ChoiceOfElectronicAddresses OPTIONAL,
    certificateDetails       [3] AuthorizedCertificate OPTIONAL,
    otherInformation         [4] ANY OPTIONAL
}

NamesPostalAddresses ::= SEQUENCE SIZE (1..MAX) OF NamePostalAddress

NamePostalAddress ::= SEQUENCE {
    entityName        [1] EntityName OPTIONAL,
    postalAddress     [2] PostalAddress OPTIONAL
}

EntityName ::= SEQUENCE {
    languageTag       [1] LanguageTag OPTIONAL,
    nameInstance      [2] UTF8String (SIZE (1..MAX))
}

PostalAddress ::= SEQUENCE {
  languageTag         LanguageTag,
  streetAddress       MultiLineStreetAddress,
  locality            UTF8String (SIZE (1..MAX)),
  stateOrProvince     [1] UTF8String (SIZE (1..MAX)) OPTIONAL,
  postalCode          UTF8String (SIZE (1..MAX)),
  countryName         CountryCode
}

MultiLineStreetAddress ::= SEQUENCE SIZE (1..MAX) OF UTF8String (SIZE (1..MAX))

ChoiceOfElectronicAddresses ::= SEQUENCE SIZE (1..MAX) OF
ChoiceOfElectronicAddress

ChoiceOfElectronicAddress ::= CHOICE {
     regularElectronicAddress          NonEmptyURI,
     attributedElectronicAddress       AttributedElectronicAddress
}
AttributedElectronicAddress ::= SEQUENCE {
        address         [1] NonEmptyURI,
        scheme          [2] IA5String(SIZE (1..MAX)),
        displayName     [3] UTF8String (SIZE (1..MAX))
}

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

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

EntityDetailsList ::= SEQUENCE SIZE (1..MAX) OF  EntityDetails
```

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

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

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

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

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

END
```

Annex G (normative): XML Schema for Evidence encoded in XML

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xml="http://www.w3.org/XML/1998/namespace"
xmlns:xades="http://uri.etsi.org/01903/v1.3.2#" xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:tsl="http://uri.etsi.org/02231/v2#" xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" xmlns:rem="http://uri.etsi.org/02640/v1#"
targetNamespace="http://uri.etsi.org/02640/v1#" 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://www.w3.org/XML/1998/namespace"
schemaLocation="http://www.w3.org/2001/xml.xsd"/>
    <xs:import namespace="http://uri.etsi.org/02231/v2#"
schemaLocation="http://uri.etsi.org/02231/v3.1.2/ts_102231v030102_xsd.xsd"/>
    <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:import namespace="urn:oasis:names:tc:SAML:2.0:assertion" schemaLocation="http://docs.oasis-
open.org/security/saml/v2.0/saml-schema-assertion-2.0.xsd"/>

<!-- List of evidence -->
    <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"/>

<!-- EvidenceType definition -->
    <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 ref="rem:EvidenceIssuerPolicyID" 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"/>
            <!-- ReplyTo type changed from xs:string to rem:AttributedElectronicAddressType in
version #2 -->
            <xs:choice minOccurs="0">
                <xs:element name="ReplyTo" type="xs:string"/>
                <xs:element name="ReplyToAddress" type="rem:AttributedElectronicAddressType"/>
            </xs:choice>
            <xs:element ref="rem:SenderDetails"/>
            <xs:element ref="rem:RecipientsDetails"/>
            <xs:element ref="rem:RecipientsDelegatesDetails" minOccurs="0"/>
            <xs:element name="EvidenceRefersToRecipient" type="xs:integer" minOccurs="0"/>
            <xs:element ref="rem:SenderMessageDetails" minOccurs="0"/>
            <xs:element ref="rem:NotificationMessageDetails" minOccurs="0"/>
            <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:string" use="required"/>
        <xs:attribute name="Id" type="xs:ID" use="optional"/>
    </xs:complexType>

<!-- EventCode -->
    <xs:element name="EventCode" type="xs:anyURI"/>

<!-- EventReasons -->
    <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>

<!-- EvidenceIssuerPolicyID-->
    <xs:element name="EvidenceIssuerPolicyID" type="rem:EvidenceIssuerPolicyIDType"/>
    <xs:complexType name="EvidenceIssuerPolicyIDType">
        <xs:sequence>
            <xs:element name="PolicyID" type="xs:anyURI" maxOccurs="unbounded"/>
        </xs:sequence>
    </xs:complexType>

<!-- EntityDetailsType -->
    <xs:element name="EvidenceIssuerDetails" type="rem:EntityDetailsType"/>
    <xs:complexType name="EntityDetailsType">
        <xs:sequence>
            <xs:element ref="rem:NamesPostalAddresses" minOccurs="0"/>
            <xs:choice minOccurs="0" maxOccurs="unbounded">
                <xs:element ref="rem:AttributedElectronicAddress"/>
                <xs:element ref="tsl:ElectronicAddress"/>
            </xs:choice>
            <xs:element ref="rem:CertificateDetails" minOccurs="0"/>
            <xs:element ref="xades:Any" minOccurs="0"/>
        </xs:sequence>
    </xs:complexType>
    <!-- AttributedElectronicAddressType - introduced in Version #2 as an alternative to
tsl:ElectronicAddress -->
    <xs:complexType name="AttributedElectronicAddressType">
        <xs:simpleContent>
            <xs:extension base="tsl:NonEmptyURIType">
                <xs:attribute name="scheme" type="xs:QName" default="mailto">
                    <xs:annotation>
                        <xs:documentation>Defaults to mailto, if not present</xs:documentation>
                    </xs:annotation>
                </xs:attribute>
                <xs:attribute name="DisplayName" type="tsl:NonEmptyString"/>
            </xs:extension>
        </xs:simpleContent>
    </xs:complexType>
    <xs:element name="AttributedElectronicAddress" type="rem:AttributedElectronicAddressType"/>
    <xs:element name="NamesPostalAddresses" type="rem:NamesPostalAddressListType"/>
    <xs:complexType name="NamesPostalAddressListType">
        <xs:sequence>
            <xs:element ref="rem:NamePostalAddress" maxOccurs="unbounded"/>
        </xs:sequence>
    </xs:complexType>
    <xs:element name="NamePostalAddress" type="rem:NamePostalAddressType"/>
    <xs:complexType name="NamePostalAddressType">
        <xs:sequence>
            <xs:element ref="rem:EntityName" minOccurs="0"/>
            <xs:element ref="rem:PostalAddress" minOccurs="0"/>
        </xs:sequence>
    </xs:complexType>
    <xs:element name="EntityName" type="rem:EntityNameType"/>
    <xs:complexType name="EntityNameType">
        <xs:sequence>
            <xs:element name="Name" type="tsl:NonEmptyString" maxOccurs="unbounded"/>
        </xs:sequence>
        <xs:attribute ref="xml:lang" use="optional"/>
    </xs:complexType>
    <xs:element name="PostalAddress" type="rem:PostalAddressType"/>
    <xs:complexType name="PostalAddressType">
        <xs:sequence>
            <xs:element name="StreetAddress" type="tsl:NonEmptyString" maxOccurs="unbounded"/>
            <xs:element name="Locality" type="tsl:NonEmptyString"/>
            <xs:element name="StateOrProvince" type="tsl:NonEmptyString" minOccurs="0"/>
            <xs:element name="PostalCode" type="tsl:NonEmptyString"/>
            <xs:element name="CountryName" type="tsl:NonEmptyString"/>
        </xs:sequence>
        <xs:attribute ref="xml:lang" use="optional"/>
    </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>

<!-- AuthenticationDetailsType -->
    <xs:element name="SenderAuthenticationDetails" type="rem:AuthenticationDetailsType"/>
    <xs:element name="RecipientAuthenticationDetails" type="rem:AuthenticationDetailsType"/>
    <xs:complexType name="AuthenticationDetailsType">
        <xs:sequence>
            <xs:choice>
                <xs:sequence>
                    <xs:element name="AuthenticationTime" type="xs:dateTime"/>
                    <xs:element name="AuthenticationMethod" type="xs:anyURI"/>
                </xs:sequence>
                <!-- saml:Assertion - introduced in Version #2 as an alternative to
rem:AuthenticationTime/Method -->
                <xs:element ref="saml:Assertion"/>
            </xs:choice>
            <xs:element name="AdditionalDetails" type="xades:AnyType" minOccurs="0"/>
        </xs:sequence>
    </xs:complexType>

<!-- EntityDetailsListType -->
    <xs:element name="SenderDetails" type="rem:EntityDetailsType"/>
    <xs:element name="RecipientsDetails" type="rem:EntityDetailsListType"/>
    <xs:complexType name="EntityDetailsListType">
        <xs:sequence>
            <xs:element name="EntityDetails" type="rem:EntityDetailsType" maxOccurs="unbounded"/>
        </xs:sequence>
    </xs:complexType>

<!-- RecipientsDelegatesDetailsType -->

    <xs:element name="RecipientsDelegatesDetails" type="rem:RecipientsDelegatesType"/>
    <xs:complexType name="RecipientsDelegatesType">
        <xs:sequence maxOccurs="unbounded">
            <xs:element name="DelegateDetails" type="rem:EntityDetailsType"/>
            <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="SenderMessageDetails" type="rem:MessageDetailsType"/>
    <xs:element name="NotificationMessageDetails" 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="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"/>
    <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"/>
            </xs:extension>
        </xs:complexContent>
    </xs:complexType>
</xs:schema>
```

Annex H (informative): Bibliography

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

History

Document history		
V1.1.1	October 2008	Publication
V2.1.1	January 2010	Publication
V2.2.1	September 2011	Publication