ETSI TS 119 534-1 V1.1.1 (2019-02)

Electronic Signatures and Infrastructures (ESI);
Testing Conformance and Interoperability of Registered Electronic Mail Services;
Part 1: Testing conformance

Reference

DTS/ESI-0019534-1

Keywords

conformance, registered electronic mail, testing

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

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

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

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

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

Contents

Intellectual Property Rights

Essential patents

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

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

Trademarks

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

Foreword

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

The present document is part 1 of a multi-part deliverable covering Registered Electronic Mail Services, as identified below:

Part 1: **"Testing conformance";**

Part 2: "Test suites for interoperability testing of providers using same format and transport protocols";

Part 3: "Test suites for interoperability testing of providers using different format and transport protocols".

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

The present document defines the set of checks to be performed for testing conformance in the provision of Registered Electronic Mail Services against the specific technical requirements defined in ETSI EN 319 532-3 [1] and against technical requirements for the provision of the service defined in ETSI EN 319 532-1 [2].

More specifically, the present document defines test assertions for testing conformance regarding:

1) The construction of MIME and SMIME headers (clause 5) and bodies (clause 6) in ETSI EN 319 532-3 [1].
2) The construction of REM messages (clause 7).
3) The generation of digital signatures in REM messages and ERDS evidence (clause 8)
4) Some aspects of the Common Service Interface (clause 9).
5) The structure and contents of ERDS evidence (clause 10).
6) Relevant aspects of the provision of the service, namely: the generation of ERDS evidence following certain events, and the security measures in the relevant interfaces defined in ETSI EN 319 532-3 [1], clause 11.

The present document does not define the checks to be performed for testing conformance in the provision of Registered Electronic Mail Services against technical requirements defined in none of the technical specifications on which ETSI EN 319 532-3 [1] is built.

2 References

2.1 Normative references

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

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

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

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

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

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

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

[4] IETF RFC 5322 (October 2008): "Internet Message Format".

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

[6] OASIS Standard: "Test Assertions Model Version 1.0".

[7] ETSI TS 119 524-1: "Electronic Signatures and Infrastructures (ESI); Testing Conformance and Interoperability of Electronic Registered Delivery Services; Part 1: Testing conformance".

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

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

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

2.2 Informative references

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

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

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

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

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

[i.3] IETF RFC 2046: "Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types".

[i.4] IETF RFC 6931 (April 2013): "Additional XML Security Uniform Resource Identifiers (URIs)".

[i.5] ETSI EN 319 142-1: "Electronic Signatures and Infrastructures (ESI);PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures".

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

[i.7] ETSI EN 319 522-4-3: "Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 4: Bindings; Sub-part 3: Capability/requirements bindings".

[i.8] IETF RFC 5321: "Simple Mail Transfer Protocol".

[i.9] IETF RFC 5246: "The Transport Layer Security (TLS) Protocol Version 1.2".

[i.10] IETF RFC 3501: "Internet Message Access Protocol - Version 4rev1".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in ETSI EN 319 532-1 [2] apply.

3.2 Symbols

Void.

3.3 Abbreviations

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

ARI	Acceptance/Rejection Interface
CA	Certification Authority
CSI	Common Service Infrastructure
ERDS	Electronic Registered Delivery Service

ERDSP	Electronic Registered Delivery Service Provider
ERD-UA	Electronic Registered Delivery - User Agent
ERI	Evidence Retrieval Interface
IMAP	Internet Mail Access Protocol
MEPI	Message and Evidence Push Interface
MERI	Message and Evidence Retrieval Interface
MRI	Message Retrieval Interface
MSI	Message Submission Interface
POP	Post Office Protocol
REM	Registered Electronic Mail
REMS	Registered Electronic Mail Service
REMSP	Registered Electronic Mail Service Provider
RI	Relay Interface
R-REMS	Recipient's REMS
S&N	Store and Notify
S/MIME	Secure/Multipurpose Internet Mail Extensions
SMIME	Secure Multipurpose Internet Mail Extensions
SMTP	Simple Mail Transfer Protocol
S-REMS	Sender's REMS
TL	Trusted List
TLS	Transport Layer Security
TSP	Trust Service Provider
UID	Unique IDentifier
URI	Uniform Resource Identifier
URL	Universal Resource Locator
UTF	Unicode Transformation Format
XML	eXtensible Mark-up Language

4 Overview

The present clause describes the main aspects of the technical approach used for specifying the whole set of tests to be performed for testing conformance against ETSI EN 319 532-3 [1] with the scope defined in clause 1 of the present document.

No tests are included testing conformance on requirements not specified in ETSI EN 319 532-3 [1].

The tests are defined using recent developments in testing fields. The selected technology is the test assertions as specified in OASIS Standard [6]. In consequence, the tests will be defined as test assertions.

Each test assertion defined in the present document will include:

1) Unique **identifier** for further referencing. The identifiers of the assertions defined within the present document will start with one code identifying the set of requirements the assertion corresponds to.

2) Reference to the **Normative source** for the test.

3) The **Target** of the assertion. In the normative part, this field identifies services whose technical implementation conforms to the requirements specified in ETSI EN 319 532-3 [1].

4) **Predicate** fully and unambiguously defining the assertion to be tested by tools claiming conformance to the present document.

5) **Prescription level**. Three levels are defined: mandatory, recommended and optional.

6) **Tag**. If assigned to test assertions it allows their categorization and grouping.

5 Test assertions for SMIME section header fields specified by ETSI EN 319 532-3

5.1 Introduction

This clause defines the whole set of assertions required for testing compliance of the requirements defined by ETSI EN 319 532-3 [1] for the header fields present in the following REM messages' MIME section headers:

1) The outermost MIME section header.

2) The signed data MIME section header.

3) The REMS introduction MIME section header.

4) The original message MIME section header.

5) The REMS extension MIME section header.

6) The ERDS evidence MIME section header.

7) The REMS signature MIME section header.

5.2 Test assertions for fields in the outermost MIME section header

REMS/HEADER/OUT/FIELD/TA_01	
TA Id	REMS/HEADER/OUT/FIELD/TA_01
Normative source	ETSI EN 319 532-3 [1], clause 6.2.1 Content-Type The value for this header field shall be "multipart/signed": • 'protocol' parameter value shall be "application/pkcs7-signature" • 'micalg' parameter value should be conformant to ETSI TS 119 312 [i.2] • 'boundary' parameter value should be conformant to IETF RFC 2046 [i.3], section 5.1.1
Target	Conformance to outermost MIME section header
Predicate	The value of 'Content-Type' field of the outermost MIME section header is "multipart/signed"
Prescription level	Mandatory
Tag	Conformance, REMS, REMSP, REMS relay metadata

REMS/HEADER/OUT/FIELD/TA_02	
TA Id	REMS/HEADER/OUT/FIELD/TA_02
Normative source	ETSI EN 319 532-3 [1], clause 6.2.1 Content-Type The value for this header field shall be "multipart/signed": • 'protocol' parameter value shall be "application/pkcs7-signature" • 'micalg' parameter value should be conformant to ETSI TS 119 312 [i.2] • 'boundary' parameter value should be conformant to IETF RFC 2046 [i.3], section 5.1.1
Target	Conformance to outermost MIME section header
Predicate	The value of parameter 'protocol' of 'Content-Type' field is "application/pkcs7-signature"
Prescription level	Mandatory
Tag	Conformance, REMS, REMSP, REMS relay metadata

REMS/HEADER/OUT/FIELD/TA_03	
TA Id	REMS/HEADER/OUT/FIELD/TA_03
Normative source	ETSI EN 319 532-3 [1], clause 6.2.1 Content-Type The value for this header field shall be "multipart/signed": • 'protocol' parameter value shall be "application/pkcs7-signature" • 'micalg' parameter value should be conformant to ETSI TS 119 312 [i.2] • 'boundary' parameter value should be conformant to IETF RFC 2046 [i.3], section 5.1.1
Target	Conformance to outermost MIME section header
Predicate	The value of parameter 'micalg' of 'Content-Type' field is conformant to ETSI TS 119 312 [i.2]
Prescription level	Recommended
Tag	Conformance, REMS, REMSP, REMS relay metadata

REMS/HEADER/OUT/FIELD/TA_04	
TA Id	REMS/HEADER/OUT/FIELD/TA_04
Normative source	ETSI EN 319 532-3 [1], clause 6.2.1 Content-Type The value for this header field shall be "multipart/signed": • 'protocol' parameter value shall be "application/pkcs7-signature" • 'micalg' parameter value should be conformant to ETSI TS 119 312 [i.2] • 'boundary' parameter value should be conformant to IETF RFC 2046 [i.3], section 5.1.1
Target	Conformance to outermost MIME section header
Predicate	The value of parameter 'boundary' of 'Content-Type' field is conformant to IETF RFC 2046 [i.3]
Prescription level	Recommended
Tag	Conformance, REMS, REMSP, REMS relay metadata

REMS/HEADER/OUT/FIELD/TA_05	
TA Id	REMS/HEADER/OUT/FIELD/TA_05
Normative source	ETSI EN 319 532-3 [1], clause 6.2.1 Content-Type Presence Mandatory
Target	Conformance to outermost MIME section header
Predicate	The 'Content-Type' field of the outermost MIME section header is present
Prescription level	Mandatory
Tag	Conformance, REMS, REMSP, REMS relay metadata

REMS/HEADER/OUT/FIELD/TA_06	
TA Id	REMS/HEADER/OUT/FIELD/TA_06
Normative source	ETSI EN 319 532-3 [1], clause 6.2.1 MIME-Version The value for this header field shall be "1.0"
Target	Conformance to outermost MIME section header
Predicate	The value of 'MIME-Version' field of the outermost MIME section header is "1.0"
Prescription level	Mandatory
Tag	Conformance, REMS, REMSP, REMS relay metadata

REMS/HEADER/OUT/FIELD/TA_07	
TA Id	REMS/HEADER/OUT/FIELD/TA_07
Normative source	ETSI EN 319 532-3 [1], clause 6.2.1 MIME-Version Presence Mandatory
Target	Conformance to outermost MIME section header
Predicate	The 'MIME-Version' field of the outermost MIME section header is present
Prescription level	Mandatory
Tag	Conformance, REMS, REMSP, REMS relay metadata

REMS/HEADER/OUT/FIELD/TA_08	
TA Id	REMS/HEADER/OUT/FIELD/TA_08
Normative source	ETSI EN 319 532-3 [1], clause 6.2.1 Message-ID The value for this header field should be an UID as defined in IETF RFC 5322 [4]
Target	Conformance to outermost MIME section header
Predicate	The value of 'Message-ID' field of the outermost MIME section header is an UID as defined in IETF RFC 5322 [8]
Prescription level	Recommended
Tag	Conformance, REMS, REMSP, REMS relay metadata

REMS/HEADER/OUT/FIELD/TA_09	
TA Id	REMS/HEADER/OUT/FIELD/TA_09
Normative source	ETSI EN 319 532-3 [1], clause 6.2.1 Message-ID Presence Mandatory
Target	Conformance to outermost MIME section header
Predicate	The 'Message-ID' field of the outermost MIME section header is present
Prescription level	Mandatory
Tag	Conformance, REMS, REMSP, REMS relay metadata

REMS/HEADER/OUT/FIELD/TA_10	
TA Id	REMS/HEADER/OUT/FIELD/TA_10
Normative source	ETSI EN 319 532-3 [1], clause 6.2.1 Date The value for this header field shall be compliant with clause 3.3 of IETF RFC 5322 [4]
Target	Conformance to outermost MIME section header
Predicate	The value of 'Date' field of the outermost MIME section header is compliant with clause 3.3 of IETF RFC 5322 [4]
Prescription level	Mandatory
Tag	Conformance, REMS, REMSP, REMS relay metadata

REMS/HEADER/OUT/FIELD/TA_11	
TA Id	REMS/HEADER/OUT/FIELD/TA_11
Normative source	ETSI EN 319 532-3 [1], clause 6.2.1 Date Presence Mandatory
Target	Conformance to outermost MIME section header
Predicate	The 'Date' field of the outermost MIME section header is present
Prescription level	Mandatory
Tag	Conformance, REMS, REMSP, REMS relay metadata

REMS/HEADER/OUT/FIELD/TA_12	
TA Id	REMS/HEADER/OUT/FIELD/TA_12
Normative source	ETSI EN 319 532-3 [1], clause 6.2.1 From The value for this header field should be either a REMSP service address (e.g. "<service_rem_md_x@rem_md_x.com>" or a transformation of the original From field to show the role of the REMSP (e.g. "on behalf of user@rem_md_x.com <service_rem_md_x@rem_md_x.com>")
Target	Conformance to outermost MIME section header
Predicate	The value of 'From' field of the outermost MIME section header is either a REMSP service address or a transformation of the original 'From' field to show the role of the REMSP
Prescription level	Recommended
Tag	Conformance, REMS, REMSP, REMS relay metadata

REMS/HEADER/OUT/FIELD/TA_13	
TA Id	REMS/HEADER/OUT/FIELD/TA_13
Normative source	ETSI EN 319 532-3 [1], clause 6.2.1 From Presence Mandatory
Target	Conformance to outermost MIME section header
Predicate	The 'From' field of the outermost MIME section header is present
Prescription level	Mandatory
Tag	Conformance, REMS, REMSP, REMS relay metadata

REMS/HEADER/OUT/FIELD/TA_14	
TA Id	REMS/HEADER/OUT/FIELD/TA_14
Normative source	ETSI EN 319 532-3 [1], clause 6.2.1 To In case of a REM dispatch or REM payload the value for this header field shall match the value of the 'To' header field in the original message. In case of a REM message carrying evidence for the sender, the value for this header field may match the value of the 'From' header field in the original message
Target	Conformance to outermost MIME section header
Prerequisite	The header is part of a REM Dispatch or REM payload
Predicate	The value of 'To' field of the outermost MIME section header matches the value of the To header field in the original message
Prescription level	Mandatory
Tag	Conformance, REMS, REMSP, REMS relay metadata

REMS/HEADER/OUT/FIELD/TA_15	
TA Id	REMS/HEADER/OUT/FIELD/TA_15
Normative source	ETSI EN 319 532-3 [1], clause 6.2.1 To In case of a REM dispatch the value for this header field shall match the value of the 'To' header field in the original message. In case of a REM message carrying evidence for the sender, the value for this header field may match the value of the 'From' header field in the original message
Target	Conformance to outermost MIME section header
Prerequisite	The header is part of REM message carrying evidence for the sender
Predicate	The value of 'To' field of the outermost MIME section header matches the value of the 'From' header field in the original message
Prescription level	Optional
Tag	Conformance, REMS, REMSP, REMS relay metadata

REMS/HEADER/OUT/FIELD/TA_16	
TA Id	REMS/HEADER/OUT/FIELD/TA_16
Normative source	ETSI EN 319 532-3 [1], clause 6.2.1 To Presence Mandatory
Target	Conformance to outermost MIME section header
Predicate	The 'To' field of the outermost MIME section header is present
Prescription level	Mandatory
Tag	Conformance, REMS, REMSP, REMS relay metadata

REMS/HEADER/OUT/FIELD/TA_17	
TA Id	REMS/HEADER/OUT/FIELD/TA_17
Normative source	ETSI EN 319 532-3 [1], clause 6.2.1 Cc REMS should assign a value to this header field only for REM dispatch. In such case, the value shall match the value of the 'Cc' header field in the original message
Target	Conformance to outermost MIME section header
Predicate	The value of 'Cc' field of the outermost MIME section header matches the value of the 'Cc' header field in the original message
Prescription level	Optional
Tag	Conformance, REMS, REMSP, REMS relay metadata

REMS/HEADER/OUT/FIELD/TA_18	
TA Id	REMS/HEADER/OUT/FIELD/TA_18
Normative source	ETSI EN 319 532-3 [1], clause 6.2.1 Cc Presence Optional
Target	Conformance to outermost MIME section header
Predicate	The 'Cc' field of the outermost MIME section header is present
Prescription level	Optional
Tag	Conformance, REMS, REMSP, REMS relay metadata

REMS/HEADER/OUT/FIELD/TA_19	
TA Id	REMS/HEADER/OUT/FIELD/TA_19
Normative source	ETSI EN 319 532-3 [1], clause 6.2.1 Subject The value for this header field should be transformed as follows starting from the Subject header field contained in the original sender's message, in order to indicate the role that the REM message has within the flow: REM <event identifier>: <original subject> (E.g.: "REM `ContentConsignment`: subject_of_original_message")
Target	Conformance to outermost MIME section header
Predicate	The value of 'Subject' field of the outermost MIME section header is the result of transforming the 'Subject' field in the original message as follows: REM <event identifier>: <original 'Subject' field>
Prescription level	Recommended
Tag	Conformance, REMS, REMSP, REMS relay metadata

REMS/HEADER/OUT/FIELD/TA_20	
TA Id	REMS/HEADER/OUT/FIELD/TA_20
Normative source	ETSI EN 319 532-3 [1], clause 6.2.1 Subject Presence Mandatory
Target	Conformance to outermost MIME section header
Predicate	The 'Subject' field of the outermost MIME section header is present
Prescription level	Mandatory
Tag	Conformance, REMS, REMSP, REMS relay metadata

REMS/HEADER/OUT/FIELD/TA_21	
TA Id	REMS/HEADER/OUT/FIELD/TA_21
Normative source	ETSI EN 319 532-3 [1], clause 6.2.1 ReplyTo In the case of a REM dispatch or REM payload the value for this header field shall match the value of the 'From' header field in the original message. In the case of a REM message carrying evidence for the sender, this header field should not appear, and if it appears, its value should be the REM service address
Target	Conformance to outermost MIME section header
Prerequisite	The header is part of a REM dispatch or REM payload
Predicate	The value of 'ReplyTo' field of the outermost MIME section header matches the value of the 'From' header field in the original message
Prescription level	Mandatory
Tag	Conformance, REMS, REMSP, REMS relay metadata