ETSI EN 319 532-4 V1.1.1 (2018-09)

EUROPEAN STANDARD

Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) Services; Part 4: Interoperability profiles

Reference

DEN/ESI-0019532-4

Keywords

e-delivery services, registered e-delivery services, registered electronic mail

ETSI

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

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

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

Important notice

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

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
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

Copyright Notification

Contents

Intellectual Property Rights

Essential patents

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

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

Trademarks

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

Foreword

This European Standard (EN) has been produced by ETSI Technical Committee Electronic Signatures and Infrastructures (ESI).

The present document is part 4 of a multi-part deliverable. Full details of the entire series can be found in part 1 [4].

National transposition dates	
Date of adoption of this EN:	23 August 2018
Date of latest announcement of this EN (doa):	30 November 2018
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	31 May 2019
Date of withdrawal of any conflicting National Standard (dow):	31 May 2019

Modal verbs terminology

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

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

Introduction

Registered Electronic Mail (REM) is a particular instance of An Electronic Registered Delivery Service (ERDS). Standard email, used as backbone, makes interoperability smooth and increases usability. At the same time, the application of additional security mechanisms ensures integrity, confidentiality and non-repudiation (of submission, consignment, handover, etc.), and protects against risk of loss, theft, damage and any illegitimate modification.

The present document aims to cover the common and worldwide-recognized requirements to address electronic registered delivery in a secure and reliable way. Particular attention is paid to the Regulation (EU) No 910/2014 [i.1]. However, the legal effects are outside the scope of the present document.

1 Scope

The present document specifies the interoperability profiles of the Registered Electronic Mail (REM) messages according to the formats defined in ETSI EN 319 532-3 [6] and the concepts and semantic defined in ETSI EN 319 532-1 [4] and ETSI EN 319 532-2 [5]. It deals with issues relating authentication, authenticity and integrity of the information, with the purpose to address the achievement of interoperability across REM service providers, implemented according the aforementioned specifications.

The present document covers all the options to profile REM services for both styles of operation: S&N and S&F.

The mandatory requirements defined in the aforementioned referenced REM services specifications are not normally repeated here but, when necessary, the present document contains some references to them.

More specifically, the present document:

a) Defines generalities on profiling.

b) Defines constraints for SMTP profile.

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

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

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

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

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

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

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

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

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

[10] IETF RFC 3207 (2002): "SMTP Service Extension for Secure SMTP over Transport Layer Security".

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] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[i.2] ISO/IEC TR 10000:1998: "Information technology - Framework and taxonomy of International Standardized Profiles".

[i.3] IETF RFC 6698: "The DNS-Based Authentication of Named Entities (DANE), Transport Layer Security (TLS) Protocol: TLSA".

[i.4] IETF RFC 7208: "Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1".

[i.5] IETF RFC 6376: "DomainKeys Identified Mail (DKIM) Signatures".

[i.6] NIST Special Publication 800-177: "Trustworthy Email".

[i.7] NIST Special Publication 800-45: "Guidelines on Electronic Mail Security, Version 2".

[i.8] IPJ - The Internet Protocol Journal - November 2016, Volume 19, Number 3: "Comprehensive Internet E-Mail Security: Review of email vulnerabilities and security threats".

[i.9] IETF RFC 4035: "Protocol Modifications for the DNS Security Extensions".

[i.10] IETF RFC 7489: "Domain-based Message Authentication, Reporting, and Conformance (DMARC)".

[i.11] IETF RFC 5751: "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification".

[i.12] ETSI EN 319 521: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Electronic Registered Delivery Service Providers".

[i.13] IETF RFC 7817: "Updated Transport Layer Security (TLS) Server Identity Check Procedure for Email-Related Protocols".

3 Definitions, abbreviations and terminology

3.1 Definitions

For the purposes of the present document, the terms and definitions given in ETSI EN 319 532-1 [4] apply.

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI EN 319 532-1 [4] apply.

3.3 Terminology

Since Registered Electronic Email Services are specific types of Electronic Registered Delivery Services, the present document uses the terms and definitions from ETSI EN 319 521 [i.12] and ETSI EN 319 522 [1], [2] and [3].

ETSI EN 319 532-2 [5], clause 4.1 specifies the usage of prefixes ERD versus REM or ERDS versus REMS for naming concepts and/or structures.

The naming convention used in the present document is that constructs whose content is completely generated by the REMS are prefixed with "ERDS" or "REMS", while constructs whose content includes user generated data is prefixed with "ERD" or "REM".

4 General requirements

4.1 Introduction

The present document provides one profile as intended in ISO/IEC TR 10000 [i.2]: *"the identification of chosen classes, conforming subsets, options and parameters of base standards, or International Standardized Profiles necessary to accomplish a particular function"*. In the present document the concept of profile embraces references like architectural, protocol detail, semantic and implementation aspects, as well as technical standard and service interoperability aspects.

More specifically, the present document specifies a profile for REM service that use the same formats (S/MIME based) and the same transport protocols (SMTP). This is rather an intra-operability profile acting, theoretically, on a pure and homogeneous environment.

4.2 Compliance requirements

Requirements are grouped in three different categories, each one having its corresponding identifier. Table 1 defines these categories and their identifiers.

Table 1: Requirements categories

Identifier	Requirement to implement
M	System **shall** implement the element
R	System **should** implement the element
O	System **may** implement the element

All the requirements shall be defined in tabular form.

Table 2: Requirements template

Nº	Service/Protocol element	EN reference	Requirement	Implementation guidance	Notes

Column **Nº** shall identify a unique number for the requirements. This number shall start from 1 in each clause. The eventual references to it would also include the clause number to avoid any ambiguity.

Column **Service/Protocol element** shall identify the service element or protocol element the requirement applies to.

Column **EN Reference** shall reference the relevant clause of the standard where the element is defined. The reference is to ETSI EN 319 522-1 [1], ETSI EN 319 522-2 [2], ETSI EN 319 532-1 [4] or ETSI EN 319 532-3 [6] except where explicitly indicated otherwise.

Column **Requirement** shall contain an identifier, as defined in table 1.

Column **Implementation guidance** shall contain numbers referencing notes and/or letters referencing additional requirements. It is intended either to explain how the requirement is implemented or to include any other information not mandatory.

Column **Notes** shall contain additional notes to the requirement.

NOTE: Within a REMID, a provision different from the ones specified in the present document is viable if and only if such REMID does not envisage to interoperate with other REMIDs.

5 SMTP interoperability profile

5.1 General requirements

This clause defines a profile for interoperability among REMSPs based on SMTP relay protocol and on the same formats. Under this basis, although many aspects defined here are valid and reusable in other contexts, format and protocols, all the sentences of the present part of the document mainly refer to interactions among REM services providers using - as transfer protocol for REM messages - SMTP and its related updates, extensions and improvements (e.g. ESMTP or SMTP-AUTH, etc.).

In particular the concepts defined in IETF RFC 5321 [7], clause 2.3.1 regarding envelope and content of the Mail Objects, and the concepts defined in IETF RFC 5322 [8], clause 2.2 and IETF RFC 2045 [9] regarding the collection of header fields, structure, formats and message representation shall apply.

5.2 Style of operation

From an interoperability standpoint, no impact is expected to occur because of the adopted style of operation by REMS (Store-And-Forward vs. Store-And-Notify). Therefore, the present document shall deal with both on the same profile.

The reason for that lies in the fact that any REM message exchanged between two REMSPs (even REM messages that contain a reference to the REM Object in a Store-And-Notify context) is conveyed using the Relay Interface that, within the present interoperability profile, is based on the SMTP protocol. Henceforth protocols, message formats and evidence formats are the same in the two cases.

Then, all the REMS operating under Store-And-Notify style of operation also need a REMS operating under Store-And-Forward style of operation that represents a common layer between the two styles of operations.

Differences only arise in the set of mandatory evidence, which is specified within the two styles of operations, as described in clause 5.5.

5.3 REMS - interfaces constraints

5.3.1 Introduction

The next clauses profile the interfaces specified in ETSI EN 319 522-1 [1] and further detailed in ETSI EN 319 532-1 [4], clause 5.

5.3.2 REM MSI: Message Submission Interface

Table 3: REM message submission interface

Nº	Service/Protocol element	ETSI EN 319 532-1 [4] reference	Requirement	Implementation guidance	Notes
1	Any protocol, provided that it is secured	Clause 5	M	a	

Implementation guidance:

a) The Message Submission Interface shall be implemented with a protocol that shall secure the communication from the originating mail User Agent to the SMTP server. More specifically this protocol shall ensure proper identification and authentication of the user, confidentiality of the communication, authenticity and integrity of the submitted data. As an example, SMTP on TLS according to IETF RFC 7817 [i.13] or SSL plus check of credential over SMTP-AUTH may be used.

5.3.3 REM MRI-ERI: Message and Evidence Retrieval Interface

Table 4: REM message and evidence retrieval interface

Nº	Service/Protocol element	ETSI EN 319 532-1 [4] reference	Requirement	Implementation guidance	Notes
1	Any protocol, provided that it is secured	Clause 5	M	a	

Implementation guidance:

a) The Message and Evidence Retrieval Interface shall be implemented with a protocol that shall secure the communication from the sender/recipient mail User Agent to the REMSP server. More specifically this protocol shall ensure proper identification and authentication of the user, confidentiality of the communication, authenticity and integrity of the retrieved data. As an example, IMAP or POP or HTTP on TLS according to IETF RFC 7817 [i.13] or SSL may be used.

5.3.4 REM RI: Relay Interface

Table 5: REM relay interface

Nº	Service/Protocol element	ETSI EN 319 532-1 [4] reference	Requirement	Implementation guidance	Notes
1	SMTP on TLS	Clause 5	M	a	see note
NOTE: This is a profile for SMTP relay protocol among REMSPs and it is reflected in this requirement.					

Implementation guidance:

a) The Relay Interface shall be implemented using SMTP protocol securing the communication from the sender REMSP server to the recipient REMSP server using TLS according to IETF RFC 3207 [10].

NOTE: Particular attention has to be paid to measures preserving confidentiality, authenticity, integrity, identification and authentication. TLS and the best practices recommended in Annex A give the necessary provision to accomplish these requirements. Further IETF work about MTA-to-MTA (TLS everywhere) dialogue is actually under a draft status and not added as reference in the present document. However, it is a desirable practice in addition to opportunistic STARTTLS/DANE (see NIST Special Publication 800-177 [i.6] for more details).

5.3.5 CSI: Common Service Interface

The services used throughout this interface are not necessarily provided by a REMS (see note) and, for the purpose of the present profile, the following three main elements shall be considered:

1) Routing

2) Trusting

3) Capability discovery

NOTE 1: For this reason, the prefix REM is omitted before the definition of the interface.

ETSI EN 319 532-2 [5], clause 9 shall identify the semantic requirements that apply to CSI.