

STN	Elektronické podpisy a infraštruktúry (ESI) Registrované služby elektronickej pošty (REM) Časť 3: Formáty	STN EN 319 532-3 V1.2.1 87 9532
------------	--	---

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

Táto norma obsahuje anglickú verziu európskej normy.
This standard includes the English version of the European Standard.

Táto norma bola oznámená vo Vestníku ÚNMS SR č. 10/19

Obsahuje: EN 319 532-3 V1.2.1:2019

129288

ETSI EN 319 532-3 V1.2.1 (2019-04)



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

Reference

REN/ESI-0019532-3v121

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 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/CommitteeSupportStaff.aspx>

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.

The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2019.

All rights reserved.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members.

3GPP™ and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.

oneM2M™ logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners.

GSM® and the GSM logo are trademarks registered and owned by the GSM Association.

Contents

Intellectual Property Rights	4
Foreword.....	4
Modal verbs terminology.....	4
Introduction	5
1 Scope	6
2 References	6
2.1 Normative references	6
2.2 Informative references.....	7
3 Definition of terms, abbreviations and terminology.....	7
3.1 Terms.....	7
3.2 Abbreviations	7
3.3 Terminology	8
4 Message formats.....	8
4.1 Introduction	8
4.2 Internet Message Format in the REM services.....	8
4.3 REM message - Structure Definition.....	10
5 REMS - identification formats	15
6 REMS - relay metadata formats	15
6.1 General requirements	15
6.2 REM message structure	16
6.2.1 REMS relay metadata MIME Header Fields	16
6.2.2 signed data MIME Header Fields	19
6.2.3 REMS introduction MIME Header Fields-Body	19
6.2.3.1 General requirements	19
6.2.3.2 multipart/alternative: free text subsection Header Fields	19
6.2.3.3 multipart/alternative: HTML subsection Header Fields	20
6.2.3.4 Introduction body formats	20
6.2.4 original message MIME Header Fields	20
6.2.4.1 original message general requirements	20
6.2.4.2 original message - MIME section Header Fields	20
6.2.4.3 original message - MIME section Body formats.....	21
6.2.5 REMS extensions MIME Header Fields.....	21
6.2.6 ERDS evidence MIME Header Fields.....	22
6.2.6.1 General requirements	22
6.2.6.2 Header Fields for XML ERDS evidence usage.....	22
6.2.6.3 Header Fields for PDF ERDS evidence usage	23
6.2.7 REMS signature MIME Header Fields-Body	23
7 REMS - evidence set formats	24
8 REMS - signatures formats	24
8.1 General	24
8.2 Signatures individually signing ERDS Evidence	25
8.3 Signatures on REM messages	25
9 Common Service Interface formats.....	25
9.1 General requirements	25
9.2 Routing information	25
9.3 Trust information.....	26
9.4 Capability management	26
Annex A (informative): REM message examples	28
History	35

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 3 of a multi-part deliverable. Full details of the entire series can be found in part 1 [10].

National transposition dates	
Date of adoption of this EN:	9 April 2019
Date of latest announcement of this EN (doa):	31 July 2019
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	31 January 2020
Date of withdrawal of any conflicting National Standard (dow):	31 January 2020

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.5]. However, the legal effects are outside the scope of the present document.

1 Scope

The present document specifies the formats for messages that are produced and handled by a Registered Electronic Mail (REM) service according to the concepts and semantic defined in ETSI EN 319 522 parts 1 [7] and 2 [8] and ETSI EN 319 532 parts 1 [10] and 2 [11]. More specifically, the present document:

- a) Specifies how the general ERDS concepts like user content and metadata are identified and mapped in the standard email structure.
- b) Specifies how the aforementioned concepts are mapped in the REM service messaging structures.
- c) Specifies how the ERDS evidence set is plugged inside the REM service messaging structures.
- d) Specifies additional mechanisms like digital signature and other security controls.

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] IETF RFC 8118: "The application/pdf Media Type".
- [2] IETF RFC 2183: "Communicating Presentation Information in Internet Messages: The Content-Disposition Header Field".
- [3] IETF RFC 5751: "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification".
- [4] IETF RFC 5322: "Internet Message Format".
- [5] IETF RFC 2854: "The 'text/html' Media Type".
- [6] IETF RFC 7303: "XML Media Types".
- [7] ETSI EN 319 522-1: "Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 1: Framework and Architecture".
- [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 EN 319 532-1: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) Services; Part 1: Framework and Architecture".
- [11] ETSI EN 319 532-2: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) Services; Part 2: Semantic contents".
- [12] IETF RFC 2045: "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies".

- [13] IETF RFC 2046: "Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types".
- [14] IETF RFC 5321: "Simple Mail Transfer Protocol".
- [15] 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 6648: "Deprecating the "X-" Prefix and Similar Constructs in Application Protocols".
- [i.4] ETSI EN 319 521: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Electronic Registered Delivery Service Providers".
- [i.5] 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.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 319 142-1: "Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures".
- [i.8] 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.9] IETF RFC 6931: "Additional XML Security Uniform Resource Identifiers (URIs)".

koniec náhľadu – text ďalej pokračuje v platenej verzii STN