ICS 35.240.30 SLOVENSKÁ TECHNICKÁ NORMA Október 2022

STN

Elektronické podpisy a infraštruktúry (ESI) Registrované služby elektronickej pošty (REM) Časť 4: Profily interoperability

STN
EN 319 532-4
V1.2.1

87 9532

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

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. 09/22

Obsahuje: EN 319 532-4 V1.2.1:2022

obsahuje
farebné
strany

135463

ETSI EN 319 532-4 V1.2.1 (2022-05)

EUROPEAN STANDARD

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

Reference

REN/ESI-0019532-4v121

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 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

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

If you find a security vulnerability in the present document, please report it through our Coordinated Vulnerability Disclosure Program:
https://www.etsi.org/standards/coordinated-vulnerability-disclosure

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.
No recommendation as to products and services or vendors is made or should be implied.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are 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 Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, 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.

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.

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:	2 May 2022
Date of latest announcement of this EN (doa):	31 August 2022
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	28 February 2023
Date of withdrawal of any conflicting National Standard (dow):	28 February 2023

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 a 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.). It protects against the risk of loss, theft, damage and any illegitimate modification.

The present document covers the common and worldwide-recognized requirements to address electronic registered delivery securely and reliably. 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 semantics defined in ETSI EN 319 532-1 [4] and ETSI EN 319 532-2 [5]. It deals with issues relating to authentication, authenticity and integrity of the information, with the purpose to address the achievement of interoperability across REM service providers, implemented according to 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.

The present document also specifies a REM baseline supporting the technical interoperability amongst service providers in different regulatory frameworks.

NOTE: Specifically but not exclusively, REM baseline specified in the present document aims at supporting implementations of interoperable REM services by use of Trusted List Frameworks to constitute Trusted domains and qualified REM services (instances of electronic registered delivery services) by use of EU Trusted List system as per Regulation (EU) No 910/2014 [i.1].

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".

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

[12] ETSI TS 119 612 (V2.2.1): "Electronic Signatures and Infrastructures (ESI); Trusted Lists".

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

[14] ETSI EN 319 132-1: "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures".

[15] eIDAS Technical Specifications: "SAML Attribute Profile" - Version 1.2", 31 August 2019.

NOTE: Available at https://ec.europa.eu/cefdigital/wiki/download/attachments/82773108/eIDAS%20SAML%20Attribute%20Profile%20v1.2%20Final.pdf?version=2&modificationDate=1571068651772&api=v2.

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".

[i.14] IETF RFC 2046: "Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types".

[i.15] ETSI TR 119 001 (V1.2.1): "Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures; Definitions and abbreviations".