Draft ETSI EN 319 531 V1.0.0 (2018-05)

EUROPEAN STANDARD

Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Registered Electronic Mail Service Providers

Reference

DEN/ESI-0019531

Keywords

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

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 draft European Standard (EN) has been produced by ETSI Technical Committee Electronic Signatures and Infrastructures (ESI), and is now submitted for the combined Public Enquiry and Vote phase of the ETSI standards EN Approval Procedure.

Proposed national transposition dates	
Date of latest announcement of this EN (doa):	3 months after ETSI publication
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	6 months after doa
Date of withdrawal of any conflicting National Standard (dow):	6 months after doa

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

Business and administrative relationships among companies, public administrations and private citizens are more and more implemented electronically. Trust is essential for their success and continued development of electronic services. It is therefore important that any entity using electronic services have suitable security controls and mechanisms in place to protect their transactions and to ensure trust and confidence with their partners.

Electronic signatures are commonly used worldwide to ensure authenticity and integrity of electronic documents, making it possible to transform traditional paper-based processes into electronic ones providing a comparable or even higher level of assurance. As communication is becoming predominantly internet-based, secure and provable exchange of documents is essential to the full digital transformation.

An electronic registered delivery service (ERDS hereinafter) provides secure and reliable delivery of electronic messages between parties, producing evidence of the delivery process for legal accountability. Evidence can be seen as a declaration by a trusted party that a specific event related to the delivery process (submission of a message, relay of a message, delivery of a message, refusal of a message, etc.) happened at a certain time. Evidence can be immediately delivered to the interested party (together with the message or separately) or can be kept in a repository for later access. It is common practice to implement evidence as digitally signed data. Registered electronic mail (REM hereinafter) is a specific type of electronic registered delivery, which builds on the formats, protocols and mechanisms used in ordinary e-mail messaging.

In a number of national, regional or sector-specific communities electronic registered delivery and registered electronic mail services are already in place, and even more are being developed. 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 adversely affect interoperability between implementations which are based on different models.

The documents covering ERDS contain the general concepts and requirements which apply to all kinds of electronic registered delivery services. Since REM is a specific type of electronic registered delivery, the documents covering REM service build on the corresponding documents covering ERDS by referencing the necessary provisions, and define the interpretation and specific requirements which apply only to registered electronic mail.

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.1] (Regulation (EU) No 910/2014, or Regulation hereinafter) provides a legal framework to facilitate cross-border recognition between existing national legal systems related to electronic registered delivery services. That framework aims to open new market opportunities for European Union trust service providers to offer new pan-European electronic registered delivery services. The Regulation defines the so-called qualified electronic registered delivery service (QERDS hereinafter), which is a special type of ERDS, where both the service and its provider need to meet a number of additional requirements that the regular ERDSs and their providers do not need to meet.

The framework of ERDS standards aims to cover the common and worldwide-recognized requirements to address electronic registered delivery in a secure and reliable way, independent of the applicable legislative framework. The documents contain generic requirements which can be applied in any geographic region. At the same time, the framework of ERDS standards aims to support demonstrating compliance to the Regulation (EU) No 910/2014 [i.1] (and related secondary legislation), both for non-qualified and qualified electronic registered delivery services. Specific clauses are included defining requirements applicable only to qualified electronic registered delivery services, especially in the documents covering policy and security requirements. Specific clauses are included to this effect, especially in the documents covering policy and security requirements. However, the legal effects are outside the scope of the present document.

1 Scope

The present document specifies generally applicable policy and security requirements for Registered Electronic Mail Service Provider (REMSP), including the services they provide.

The present document is applicable to:

- The policy and security requirements of REMS and EU REMS qualified providers.
- The general and security requirements of REMS and EU REMS qualified.

The present document does not specify interconnection requirements.

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 of services implemented according to the present document are outside the scope of the present document.

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 319 401: "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers".

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

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

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

3 Definitions, abbreviations and notation

3.1 Definitions

For the purposes of the present document, the terms and definitions given in ETSI EN 319 401 [1], ETSI EN 319 521 [2] and the following apply:

Store and Forward (S&F): style of operation of a REMS in which the user content provided by the sender is conveyed to the recipient by value, and explicit acceptance is not required from the recipient

NOTE: For a more detailed description of the REM Store and Forward style of operation, see clause 4.2.2 of ETSI EN 319 532-1 [i.2].

Store and Notify (S&N): style of operation of a REMS in which first a reference to the user content is conveyed to the recipient, and acceptance is required from the recipient before consignment of the user content itself

NOTE: For a more detailed description of the REM Store and Notify style of operation, see clause 4.2.2 of ETSI EN 319 532-1 [i.2].

3.2 Abbreviations

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

ERDS	Electronic Registered Delivery Services
IMAP	Internet Message Access Protocol
POP	Post Office Protocol
QERDS	Qualified Electronic Registered Delivery Services
QERDSP	Qualified Electronic Registered Delivery Services Provider
QREMS	Qualified Registered Electronic Mail Service
QREMSP	Qualified Registered Electronic Mail Service Provider
REM	Registered E-Mail
REMS	Registered Electronic Mail Service
REMSP	Registered Electronic Mail Service Provider
S&N	Store and Notify
SMTP	Simple Mail Transfer Protocol

3.3 Notation

The requirements identified in the present document include:

a) requirements applicable to any REMS. Such requirements are indicated by clauses without any additional marking;

b) requirements applicable under certain conditions. Such requirements are indicated by clauses marked by "[CONDITIONAL]";

c) requirements that include several choices which ought to be selected according to the applicable situation. Such requirements are indicated by clauses marked by "[CHOICE]";

d) <the 3 letters REQ> - <4-5 letters type of service, whether or REMS or EU qualified (QREMS) > < the clause number> - <2 digit number – incremental>.optional<1 lowercase letter> to distinct elements from a list>.

All REMS and REMSP requirements apply to QREMS and QREMSP.

4 General provision on policies and practices

4.1 REMS Practice statement

4.1.1 Common provisions

- **REQ-REMS-4.1.1-01** All REQ-ERDS requirements from ETSI EN 319 521 [2], clause 4.1.1 shall apply.

In addition, the following REMSP and REMS-specific requirements apply:

- **REQ-REMS-4.1.1-02** The REMS practice statement shall describe the procedures used by the REMSP for identifying and authenticating users of the REMS.

- **REQ-REMS-4.1.1-03** The REM practice statement shall describe how the users can submit and receive messages through the REMS.

- **REQ-REMS-4.1.1-04** The REMS practice statement shall describe which user agents are supported by the REMS.

- **REQ-REMS-4.1.1-05** The REMS practice statement shall state whether the REMS supports S&N style or not for messages submitted within this REMS.

- **REQ-REMS-4.1.1-06** The REMS practice statement shall state whether the REMS supports S&N style or not for messages relayed by another REMS.

- **REQ-REMS-4.1.1-07** [CONDITIONAL] If the REMS support S&N style, REM practice statement shall describe how the recipient can accept or reject the incoming message.

- **REQ-REMS-4.1.1-08** [CONDITIONAL] If the REMS support S&N style, the method of determining the time period for acceptance/rejection shall be specified in the REM policy or REM practice statement.

NOTE: This time period can be determined by legislation, policy rules, or parameters given by the sender.

- **REQ-REMS-4.1.1-09** [CONDITIONAL] If more than one REMS interoperates to deliver a user content between users subscribed to different REMSs, each REMS practice statement shall state whether the REMS supports relaying messages to other REMS, and if applicable, on what conditions.

- **REQ-REMS-4.1.1-10** [CONDITIONAL] If more than one REMS interoperates to deliver a user content between users subscribed to different REMSs, each REMS practice statement shall state whether the REMS supports accepting relayed messages from other REMS, and if applicable, on what conditions.

- **REQ-REMS-4.1.1-11** [CONDITIONAL] If more than one REMS interoperates to deliver a user content between users subscribed to different REMSs, each REMS practice statement shall state whether the REMS supports relaying messages to other non-REM ERDS, and if applicable, on what conditions.

- **REQ-REMS-4.1.1-12** [CONDITIONAL] If more than one REMS interoperates to deliver a user content between users subscribed to different REMSs, each REMS practice statement shall state whether the REMS supports accepting relayed messages from other non-REM ERDS, and if applicable, on what conditions.

- **REQ-REMS-4.1.1-13** REMS practice statement shall define how the evidence components are to be interpreted.

- **REQ-REMS-4.1.1-14** REM practice statement shall describe how the provided evidences are accessible to the users (e.g. sent in message, downloadable from web, collected by a central repository, etc.).

4.1.2 Practice statement for EU QREMSP

In addition, the following EU QEREMSP and EU QREMS-specific requirements apply:

- **REQ-QREMS-4.1.2-01** All REQ-QERDS requirements from ETSI EN 319 521 [2], clause 4.1.2 shall apply.

4.2 Terms and conditions

- **REQ-REMS-4.2-01** All REQ-ERDS requirements from ETSI EN 319 521 [2], clause 4.2 shall apply.

4.3 Information security policy

- **REQ-REMS-4.3-01** All requirements from ETSI EN 319 401 [1], clause 6.3 shall apply.

4.4 REM nature

- **REQ-REMS-4.4-01** The REMS shall provide the option for all its users to send and receive messages in MIME format.

- **REQ-REMS-4.4-02** The REMS should provide the option for all its users to send message over SMTP and receive messages over IMAP or POP.

- **REQ-REMS-4.4-03** [CONDITIONAL] If the REMS support interconnection with other REMS, the REMS shall relay REM messages in the format specified in ETSI EN 319 532-3 [3].

4.5 REM styles of operation

- **REQ-REMS-4.5-01** REMS shall support S&F style of operation.

- **REQ-REMS-4.5-02** REMS may support S&N style of operation.

- **REQ-REMS-4.5-03** The REMS shall recognize a relayed REMS notification, and shall always process it in S&F style (i.e. it shall not create another REMS notification referring to the first REMS notification).

5 General provision on REMS

5.1 Message integrity and confidentiality

5.1.1 Common provisions

- **REQ-REMS-5.1.1-01** All requirements from ETSI EN 319 521 [2], clause 5.1.1 shall apply.

5.1.2 Provisions for EU QERDSP

In addition, the following EU QREMSP and EU QREMDS-specific requirements apply.

- **REQ-REMS-5.1.2-01** All REQ-QERDS requirements from ETSI EN 319 521 [2], clause 5.1.2 shall apply.

5.2 Sender and receiver identification and authentication

5.2.1 Provisions for EU QREMSP Initial identity validation

- **REQ-QREMS-5.2.1-01** All REQ-QERDS requirements from ETSI EN 319 521 [2], clause 5.2.1 shall apply.

5.2.2 Provisions for EU QREMS authentication

In addition, the following EU QEREMSP and EU QREMS-specific requirements apply:

- **REQ-QREMS-5.2.2-01** All REQ-ERDS requirements from ETSI EN 319 521 [2], clause 5.2.2 shall apply.