ETSI EN 319 532-1 V1.1.1 (2018-09)

Electronic Signatures and Infrastructures (ESI);
Registered Electronic Mail (REM) Services;
Part 1: Framework and architecture

Reference
DEN/ESI-0019532-1

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

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 1 of a multi-part deliverable covering Registered Electronic Mail (REM) Services, as identified below:

Part 1: **"Framework and architecture";**

Part 2: "Semantic contents";

Part 3: "Formats";

Part 4: "Interoperability profiles".

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

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 present document is one of a set of interrelated documents (framework of ERDS standards hereinafter) ETSI has produced to facilitate a consistent form of electronic registered delivery service inside and outside Europe, especially with regard to the form of evidence provided, in order to maximize interoperability even between domains governed by different policy rules. This set of documents includes the following deliverables:

- ETSI EN 319 522 [i.16]: a multi-part deliverable providing technical specifications for Electronic Registered Delivery Services.
- ETSI EN 319 532 [i.17]: a multi-part deliverable providing technical specifications for Registered Electronic Mail Services.
- ETSI EN 319 521 [i.18]: providing Policy and Security Requirements for Electronic Registered Delivery Service Providers.
- ETSI EN 319 531 [i.19]: providing Policy and Security Requirements for Registered Electronic Mail Service Providers.
- ETSI TS 119 524 [i.20]: a multi-part deliverable providing requirements for Testing Conformance and Interoperability of Electronic Registered Delivery Services.
- ETSI TS 119 534 [i.21]: a multi-part deliverable providing requirements for Testing Conformance and Interoperability of Registered Electronic Mail Services.

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.4] (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.4] (and related secondary legislation), both for non-qualified and qualified electronic registered delivery services. Specific clauses are included defining requirements for qualified services only, especially in the documents covering policy and security requirements. However, the legal effects of services implemented according to the framework of ERDS standards are outside the scope of the documents [i.16] to [i.21].

The present document is part 1 of ETSI EN 319 532 [i.17], which is a multi-part deliverable covering Registered Electronic Mail (REM) Services, as detailed in the Foreword. ETSI EN 319 522 contains the general concepts and requirements which apply to all kinds of ERDSs. Since registered electronic mail is a specific type of electronic registered delivery, the general provisions given in ETSI EN 319 522 apply to registered electronic mail as well. Hence, parts 1 and 2 of ETSI EN 319 532 are aligned with ETSI EN 319 522, and they reference the necessary provisions of the corresponding part.

1 Scope

The present document specifies the logical model and basic concepts of registered electronic mail (REM) service.

The present document relies on ETSI EN 319 522-1 [1] for all concepts and requirements which are generally applicable to all electronic registered delivery services, and defines the interpretation and specific requirements which apply only to registered electronic mail.

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".

2.2 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 319 532-2: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) Services; Part 2: Semantic Contents".

[i.2] ETSI EN 319 532-3: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) Services; Part 3: Formats".

[i.3] ETSI EN 319 532-4: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) Services; Part 4: Interoperability profiles".

[i.4] Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[i.5] ETSI EN 319 522-2: "Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 2: Semantic Contents".

[i.6] ETSI TS 119 612: "Electronic Signatures and Infrastructures (ESI); Trusted Lists".

[i.7] IETF RFC 5751: "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification".

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

[i.9] IETF RFC 1939: "Post Office Protocol - Version 3".

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

[i.11] IETF RFC 5246: "The Transport Layer Security (TLS) Protocol Version 1.2".

[i.12] IETF RFC 4422: "Simple Authentication and Security Layer (SASL)".

[i.13] IETF RFC 3207: "SMTP Service Extension for Secure SMTP over Transport Layer Security".

[i.14] IETF RFC 2595: "Using TLS with IMAP, POP3 and ACAP".

[i.15] IETF RFC 7817: "Updated Transport Layer Security (TLS) Server Identity Check Procedure for Email-Related Protocols".

[i.16] ETSI EN 319 522 (all parts): "Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services".

[i.17] ETSI EN 319 532 (all parts): "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) Services".

[i.18] ETSI EN 319 521: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Electronic Registered Delivery Service Providers".

[i.19] ETSI EN 319 531: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Registered Electronic Mail Service Providers".

[i.20] ETSI TS 119 524 (all parts): "Electronic Signatures and Infrastructures (ESI); Testing Conformance and Interoperability of Electronic Registered Delivery Services".

[i.21] ETSI TS 119 534 (all parts): "Electronic Signatures and Infrastructures (ESI); Testing Conformance and Interoperability of Registered Electronic Mail Services".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

consignment: act of making the user content available to the recipient within the boundaries of the electronic registered delivery service

Electronic Registered Delivery Service Provider (ERDSP): entity which provides electronic registered delivery service

NOTE: It can be a Trust Service Provider as defined in Regulation (EU) No 910/2014 [i.4].

ERD dispatch: ERD message which contains the user content, some ERDS relay metadata and ERDS evidence

ERD event: relevant event in the electronic delivery process, which may be attested by an ERDS evidence

ERD message: data composed of an optional user content, ERDS relay metadata and zero or more ERDS evidence

ERD payload: ERD message which contains the user content and some ERDS relay metadata

ERD User Agent/Application (ERD-UA): system consisting of software and/or hardware components by which senders and recipients participate in the exchange of data with electronic registered delivery service providers

Electronic Registered Delivery Service (ERDS): electronic service that makes it possible to transmit data between the sender and recipients by electronic means and provides evidence relating to the handling of the transmitted data, including proof of sending and receiving the data, and that protects transmitted data against the risk of loss, theft, damage or any unauthorized alteration

NOTE: An electronic registered delivery service is provided by one ERDSP. ERDSPs can cooperate in transferring data from a sender to a recipient when they are subscribed to different ERDSPs (see 4-corner and extended models in clauses 4.3 and 4.4 of ETSI EN 319 522-1 [1]).

ERDS evidence: data generated by the electronic registered delivery service, which aims to prove that a certain event has occurred at a certain time

ERDS handover metadata: data related to the user content which is generated by the electronic registered delivery service and handed over to the ERD user agent/application of the recipient

ERDS receipt: ERD message which contains ERDS evidence and some ERDS relay metadata

ERDS relay metadata: data related to the user content which is generated by the electronic registered delivery service for the purpose of relaying to another electronic registered delivery service

ERDS serviceinfo: ERD message which contains some ERDS relay metadata

handover: act of having the user content successfully cross the border of the recipient's electronic registered delivery service towards the recipient's ERD user agent/application

original message: data including user content and submission metadata

recipient: natural or legal person to which the user content is addressed

Registered Electronic Mail (REM): enhanced form of e-mail transmitted by registered electronic mail service

Registered Electronic Mail Service (REMS): electronic registered delivery service which builds on the formats, protocols and mechanisms used in ordinary e-mail messaging

Registered Electronic Mail Service Provider (REMSP): entity which provides registered electronic mail service

NOTE: It can be a Trust Service Provider as defined in Regulation (EU) No 910/2014 [i.4].

REM dispatch: ERD dispatch in the form of a REM envelope

REM envelope: signed data structure generated by the registered electronic mail service which contains any of the user content, ERDS relay metadata and/or ERDS evidence

REM interoperability domain: homogeneous operational space consisting of a set of REMSPs able to properly interoperate among themselves

REM interoperability domain rules: set of rules defining a REM interoperability domain

REM message: ERD message in the form of a REM envelope

REMS notification: ERDS serviceinfo or ERDS receipt, in the form of a REM envelope, which includes a reference to the user content to be delivered

REM payload: ERD payload in the form of a REM envelope

REMS receipt: ERDS receipt in the form of a REM envelope

sender: natural or legal person that has submitted the user content

submission metadata: data submitted to the electronic registered delivery service together with the user content

user content: original data produced by the sender which has to be delivered to the recipient

3.2 Abbreviations

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

CSI	Common Service Interface
ERD	Electronic Registered Delivery
ERD-UA	ERD User Agent/Application
ERDS	Electronic Registered Delivery Service
ERDSP	Electronic Registered Delivery Service Provider
ESMTP	Extended SMTP
EU	European Union
I-REMS	Intermediate REMS
IMAP	Internet Message Access Protocol
MIME	Multipurpose Internet Mail Extensions
PDF	Portable Document Format
POP	Post Office Protocol
POP3	Post Office Protocol version 3
R-REMS	Recipient's REMS
REM	Registered Electronic Mail
REMID	REM Interoperability Domain
REMS	Registered Electronic Mail Service
REMSP	Registered Electronic Mail Service Provider
S&F	Store and Forward
S&N	Store and Notify
S-REMS	Sender's REMS
S/MIME	Secure/Multipurpose Internet Mail Extensions
SASL	Simple Authentication and Security Layer
SMTP	Simple Mail Transfer Protocol
TL	Trusted List

NOTE: As per ETSI TS 119 612 [i.6].

TLS	Transport Layer Security
TSP	Trust Service Provider
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
XML	eXtensible Mark-up Language

4 REM logical model

4.1 Introduction

Registered electronic mail service (REMS henceforth) is a specific type of electronic registered delivery service (ERDS henceforth), which builds on the formats, protocols and mechanisms used in ordinary e-mail messaging. The logical model of ERDS in general, as described in clause 4 of ETSI EN 319 522-1 [1], is applicable to REMS. See clause 4.1 of ETSI EN 319 522-1 [1] for an introduction to ERDS.

The next clauses describe the interpretation of the general ERDS model as applied in the specific case of REM. Clause 4.2 further specifies the black-box model described in clause 4.2 of ETSI EN 319 522-1 [1], focusing on the outer interfaces of the REMS. Clause 4.3 further specifies the 4-corner model described in clause 4.3 of ETSI EN 319 522-1 [1], explaining the interaction between the services of different REMSPs. Clause 4.4 further specifies the extended model described in clause 4.4 of ETSI EN 319 522-1 [1], providing the details about the interaction of the REMS with other REMSs in the case when more than 2 providers take part in the delivery process.

4.2 Black-box model

4.2.1 Functional viewpoint

In the simplest case, a REMS can be represented as a black box, conveying messages between a sender and a recipient and producing the appropriate ERDS evidence. Figure 1 below provides a simple representation.

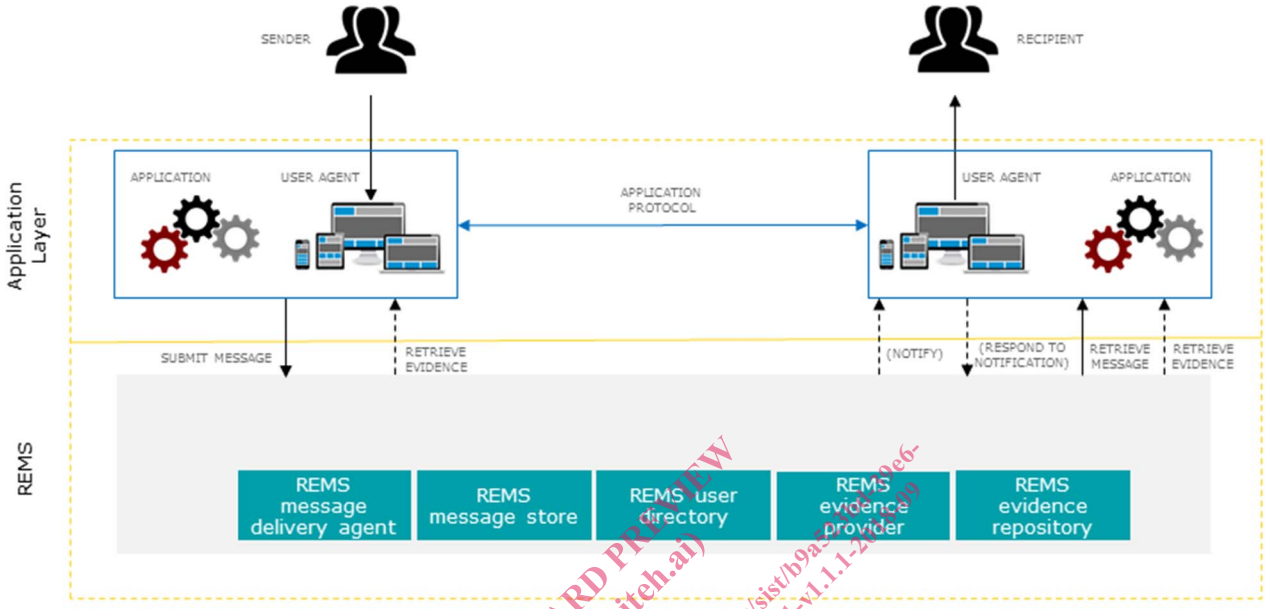

Figure 1: Black-box REM model

The REMS is typically accessed by a "user agent" (i.e. an application directly interacting with a user), which can be an ordinary email client software or a tailored REM software, or by a generic application (i.e. automated system), which can be e.g. a document management system, accounting system, etc. In any case, the client software can use the standard email protocols (i.e. SMTP and POP/IMAP) and web protocols (i.e. HTTP) to access the REMS. Use of other protocols is also possible, but it is outside the scope of the present document.

As required for all ERDSs, the sender and recipients each have a unique identifier, by which they are referred in REM messages and ERDS evidence. For REMS the unique identifier of users is an email address, as required by clause 5 of ETSI EN 319 532-3 [i.2].

For the purpose of message submission certain metadata needs to be given by the sender to the REMS, e.g. recipient addresses, requested style of operation, delivery options. This metadata is conveyed in the header of the email message. Further specification of the content and format of the metadata can be found in ETSI EN 319 532-2 [i.1] and ETSI EN 319 532-3 [i.2].

The logical model presented in figure 1 refines the functionality of the REMS into separate components, which were historically also referred to as "roles". The general ERDS model applies to REM as well. For the description of the ERDS components see clause 4.2.1 of ETSI EN 319 522-1 [1].

The following components of REMS correspond to the general ERDS components as specified in table 1.

Table 1: Mapping of REMS components and ERDS components

Component of REMS	Corresponding ERDS component
REMS message delivery agent	ERDS Message delivery system
REMS evidence provider	ERDS Evidence provider
REMS evidence repository	ERDS Evidence repository
REMS user directory	ERDS User directory