Draft ETSI EN 319 532-2 V1.0.0 (2018-05)

Electronic Signatures and Infrastructures (ESI);
Registered Electronic Mail (REM) Services;
Part 2: Semantic contents

Reference
DEN/ESI-0019532-2

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

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.

The present document is part 2 of a multi-part deliverable. Full details of the entire series can be found in part 1 [2].

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 the 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.10]: a multi-part deliverable providing technical specifications for Electronic Registered Delivery Services.
- ETSI EN 319 532 [i.11]: a multi-part deliverable providing technical specifications for Registered Electronic Mail Services.
- ETSI EN 319 521 [i.12]: providing Policy and Security Requirements for Electronic Registered Delivery Service Providers.
- ETSI EN 319 531 [i.13]: providing Policy and Security Requirements for Registered Electronic Mail Service Providers.
- ETSI TS 119 524 [i.14]: a multi-part deliverable providing requirements for Testing Conformance and Interoperability of Electronic Registered Delivery Services.
- ETSI TS 119 534 [i.15]: 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.2] (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 (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.10] to [i.15].

The present document is part 2 of ETSI EN 319 532 [i.11], which is a multi-part deliverable covering Registered Electronic Mail (REM) Services, as detailed in the Foreword. ETSI EN 319 522 [i.10] 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 [i.10] apply to registered electronic mail as well. Hence, parts 1 and 2 of ETSI EN 319 532 [i.11] are aligned with ETSI EN 319 522 [i.11], and they reference the necessary provisions of the corresponding part.

1 Scope

The present document defines the semantic content of messages and evidence used in registered electronic mail (REM) service.

The present document relies on ETSI EN 319 522-2 [1] for all semantic contents 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 nonspecific. 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 319 522-2: "Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 2: Semantic contents".

[2] ETSI EN 319 532-1: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) 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 nonspecific. 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 319 532-3: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) Services; Part 3: Formats".

[i.2] 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.3] ETSI TS 119 612: "Electronic Signatures and Infrastructures (ESI); Trusted Lists".

[i.4] IETF RFC 5321: "Simple Mail Transfer Protocol".

[i.5] IETF RFC 1939: "Post Office Protocol - Version 3".

[i.6] IETF RFC 3501: "INTERNET MESSAGE ACCESS PROTOCOL - VERSION 4rev1".

[i.7] IETF RFC 5246: "The Transport Layer Security (TLS) Protocol Version 1.2".

[i.8] IETF RFC 4422: "Simple Authentication and Security Layer (SASL)".

[i.9] ETSI EN 319 522-1: "Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 1: Framework and Architecture".

[i.10] ETSI EN 319 522 (all parts): "Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services".

[i.11] ETSI EN 319 532 (all parts): "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) Services".

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

[i.13] ETSI EN 319 531: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Registered Electronic Mail Service Providers".

[i.14] ETSI TS 119 524 (all parts): "Electronic Signatures and Infrastructures (ESI); Testing Conformance and Interoperability of Electronic Registered Delivery Services".

[i.15] 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 terms and definitions given in ETSI EN 319 532-1 [2] apply.

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI EN 319 532-1 [2] apply.

4 Overview

4.1 ERDS and REM data structures

Registered electronic mail (REM) service is a specific type of electronic registered delivery (ERD) service.

The semantic content flowing across the interfaces of ERD services in general, as specified in clause 4 of ETSI EN 319 522-2 [1], shall apply to REM services as well. The present document specifies how to interpret the ERD concepts in the specific case of REM. The interfaces of the REM service shall comply with the requirements stated in clause 5 of ETSI EN 319 532-1 [2].

The naming convention used in the present deliverable is the following. A term contains "ERD" or "ERDS" when it refers to a general concept defined by ETSI EN 319 522-1 [i.9] or ETSI EN 319 522-2 [1]. A term contains "REM" or "REMS" when it refers to a REM-specific concept defined in ETSI EN 319 532-1 [2] or in the present document. Terms referring to constructs whose content is completely generated by the service are prefixed with "ERDS" or "REMS", while terms referring to constructs whose content includes user generated data are prefixed with "ERD" or "REM".

The ERDS objects flowing across the interfaces can contain the types of information detailed below. Their interpretation in the REM specific case are the following:

- **user content:** original data produced by the sender which has to be delivered to the recipient. This can consist of one or more files. When the user content is submitted within an email message, the body of the message and the body of all attachments - if any - are considered to be the user content.

- **submission metadata:** data submitted to the electronic registered delivery service together with the user content. This can include any accompanying information that the sender specifies in relation to the submitted content. When the user content is submitted in the form of an email message, the headers of the message and the headers of attachments - if any - are considered to be part of the submission metadata. This includes headers specified by the sender and headers added by any servers the email passes through before reaching the boundary of the sender's REMS. Other data specified in the SMTP transaction (e.g. sender and recipient addresses) are also part of the submission 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. This may contain a transformation of the submission metadata and also additional data. In REM the ERDS relay metadata is the header of the relayed message (or any parts thereof).

- **ERDS evidence:** data generated by the electronic registered delivery service, which aims to prove that a certain event has occurred at a certain time. This is the same in REMS as for any other type of ERDS.

- **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. When the user content is handed over in the form of an email message, headers of the message (or any parts thereof) are considered to be part of the ERDS handover metadata.

The ERD service builds up data structures using the above information for the purpose of storage or communication between ERDSs or with end users. The various data structures are the following:

- **ERD message:** data composed of an optional user content, ERDS relay metadata and zero or more ERDS evidence. This is generated or assembled by the electronic registered delivery service. ERD message is a collective term, which includes the following subtypes: ERD dispatch, ERD payload, ERDS serviceinfo, ERDS receipt.

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

- **ERD payload:** ERD message which contains the user content and some ERDS relay metadata. ERD payload does not contain ERDS evidence.

- **ERDS serviceinfo:** ERD message which contains only some ERDS relay metadata.

- **ERDS receipt:** ERD message which contains ERDS evidence and some ERDS relay metadata. It does not contain the user content.

An additional data structure can appear on the interfaces of the ERDS, which is not built by the ERDS, but comes from the outside:

- **original message:** data including user content and submission metadata. For the purpose of submission, the ERD user agent / application of the sender builds up a data structure, e.g. an email message. Any servers forwarding the message can modify this before it reaches the systems of the ERDS (e.g. add extra headers, correct format errors, etc.). The original message is the resulting data structure, which passes through the ERDS MSI: Message Submission Interface provided by the sender's ERDS.

In addition, the following objects specific for REM are introduced:

- **REMS introduction:** data generated by the REMS containing information for the users about the data structure it is included in. This may be formatted text or plaintext. This is intended to be displayed to the user upon receipt of a REM message, and it can provide guidelines on how to interpret or use the various parts of the content of the REM message.

- **REMS extension:** data generated by the REMS in machine-readable form containing additional information for other REMSs or the ERD-UA of users. The content and format of REMS extension can be defined by application-specific or sector-specific rules; it is outside the scope of the present deliverable.

- **REM envelope:** signed data structure generated by the registered electronic mail service which contains any of the REMS introduction, user content, ERDS relay metadata, ERDS evidence and/or REMS extension. The REM envelope should be generated in the format specified in ETSI EN 319 532-3 [i.1]. The REM envelope shall bear the digital signature of the generating REMS.

All ERD messages can be structured as REM envelopes. Consequently, the following REM message types are defined:

- **REM message:** ERD message in the form of a REM envelope.
- **REM dispatch:** ERD dispatch in the form of a REM envelope.
- **REM payload:** ERD payload 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. A REMS notification shall not contain the user content. A REMS notification may contain optional ERDS evidence.
- **REMS receipt:** ERDS receipt in the form of a REM envelope. A REMS receipt shall not contain the user content.

NOTE: If a REMS conveys ERDS evidence and also a reference to the user content in the same REM message then the REMS notification will be an instance of ERDS receipt. On the other hand, a REMS notification not containing ERDS evidence will be an instance of ERDS serviceinfo. A REMS receipt always contains evidence, so it is always an instance of ERDS receipt, but it does not contain a reference to the user content.

The basic components (REMS introduction, user content, ERDS relay metadata, ERDS evidence, REMS extension) within each of the subtypes of REM message that are used in REM (REM dispatch, REM payload, REMS notification, REMS receipt) **shall** have the cardinality as defined in table 1.

Table 1: cardinality of components in REM messages

Type of message		REMS introduction	user content	ERDS relay metadata	ERDS evidence	REMS extension
REM message	REM dispatch	1	1	1	1..n	0..n
	REM payload	1	1	1	0	0..n
	REMS notification	1	0	1	0..n	0..n
	REMS receipt	1	0	1	1..n	0..n

4.2 Typical flows of REM messages

4.2.1 Introduction

The clauses below show how the data structures specified in clause 4.1 typically flow between the sender, the recipient and the REMSs. The 4-corner model (see clause 4.3 of ETSI EN 319 532-1 [2]) is used for this illustration, but this does not preclude the participation of more service providers in the delivery process, as in the extended model (see clause 4.4 of ETSI EN 319 532-1 [2]). When more than two REMSs are involved, the same objects flow to or from any intermediate REMS as between S-REMS and R-REMS depicted in the figures.

4.2.2 Use of data structures in Store and Forward style

Figure 1 shows the types of objects typically appearing on the interfaces when all REMSs are operating in Store and Forward style (see clause 4.3.2.1 of ETSI EN 319 532-1 [2] for the sequence of messages in this case). The optional REMS extension components are not shown in the figure.

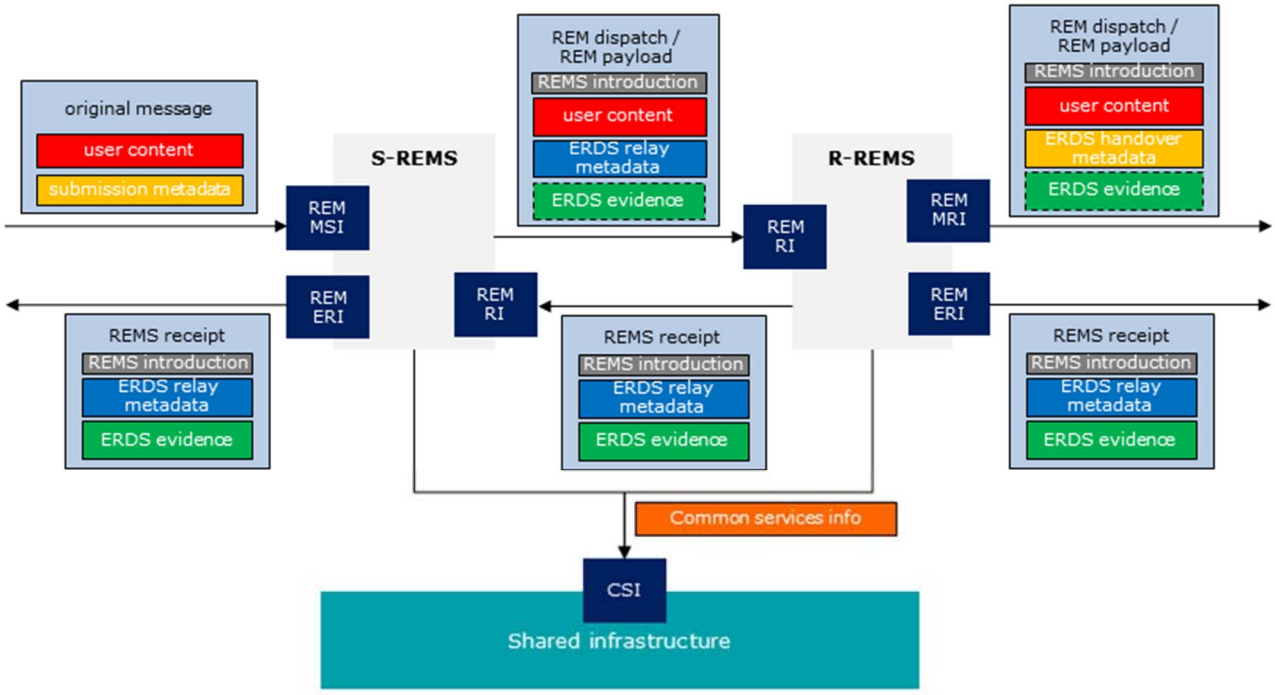

Figure 1: Typical flow of REM messages in Store and Forward style

In S&F style objects relayed between REMSs - through the REM RI: Relay Interface - shall always be in the form of REM dispatch, REM payload or REMS receipt. Objects forwarded to the recipient through the REM MRI: Message Retrieval Interface should be in the form of REM dispatch or REM payload. Objects forwarded to the sender or recipient through the REM ERI: Evidence Retrieval Interface may be in the form of REMS receipt.

NOTE: The use of these REM messages between a REMS and its end users is only recommended by the present document, but not mandated (e.g. R-REMS is allowed to convey the user content and related ERDS evidence to the recipient in separate data structures).

When the user content is handed over to the recipient enveloped in a REM dispatch or REM payload, then the ERDS handover metadata is identical to the ERDS relay metadata, otherwise it can be different.

Different REM messages relating to the same user content may contain a different subset of the ERDS relay metadata relating to that user content.

4.2.3 Use of data structures in Store and Notify style

Figure 2 shows the types of objects typically appearing on the interfaces when the sender's REMS is operating in Store and Notify style (see clause 4.3.2.3 of ETSI EN 319 532-1 [2] for the sequence of messages in this case). Only those objects are shown in the figure that are used before the recipient responds to the notification. The optional REMS extension components are not shown in the figure.

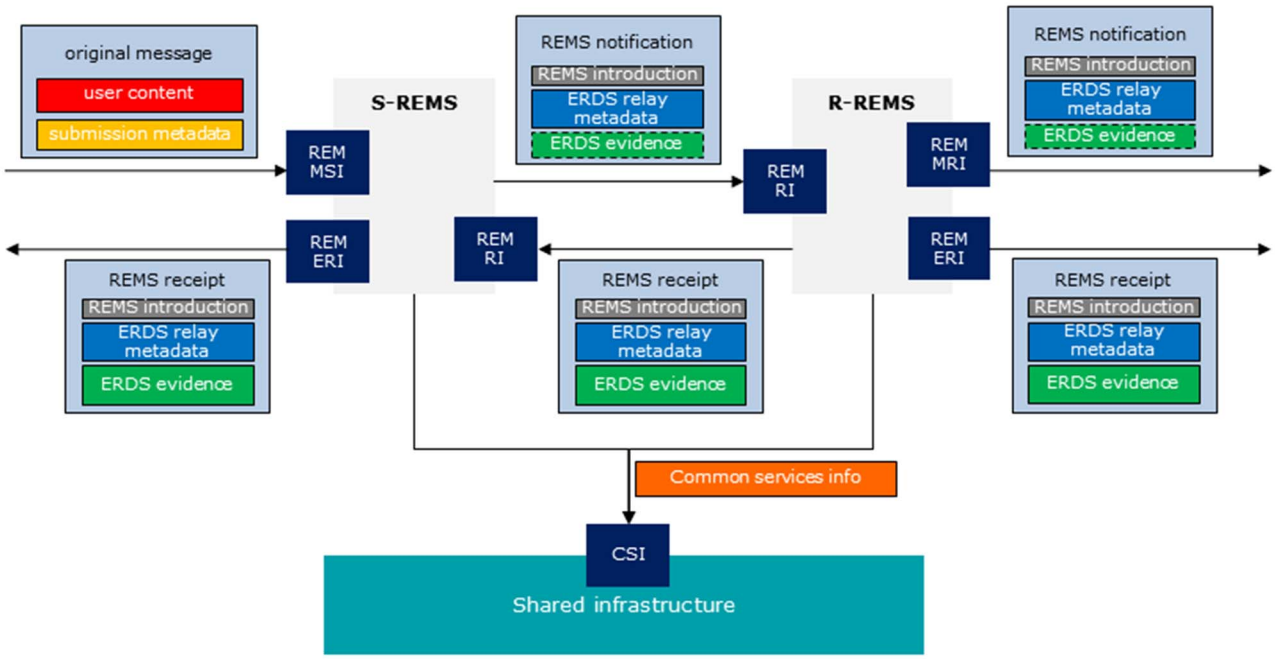

Figure 2: Typical flow of REM messages in Store and Notify style

In S&N style, before acceptance by the recipient, the object containing the reference to the user content relayed - through the REM RI: Relay Interface - by the S&N REMS (S-REMS in the figure) and any subsequent REMSs to the next REMS shall be in the form of REMS notification. The object forwarded to the recipient by R-REMS in order to notify about the incoming message may be in the form of REMS notification, or it may be in any other form as agreed between R-REMS and the recipient.

If the recipient accepts the incoming message based on the notification then the REM dispatch or REM payload may be forwarded to the recipient in the same way as in S&F style. The data structures used in this communication are as shown in figure 1. The same rules apply: the object forwarded between REMSs shall be a REM dispatch or REM payload, the object handed over by R-REMS to the recipient should be a REM dispatch or REM payload.

Alternatively, once the recipient signalled acceptance, the user content may be handed over by S-REMS directly to the recipient. (This option is not shown in the figures.) In this case, the object handed over to the recipient should be a REM dispatch or REM payload.

Objects forwarded to the sender or recipient through the REM ERI: Evidence Retrieval Interface may be in the form of REMS receipt.

When the sender's REMS operates in S&F style and the recipient's REMS operates in S&N style, the same rules apply as above, mutatis mutandis.

When the user content is handed over to the recipient enveloped in a REM dispatch or REM payload, then the ERDS handover metadata is identical to the ERDS relay metadata, otherwise it can be different.

Different REM messages relating to the same user content may contain a different subset of the ERDS relay metadata relating to that user content.

5 Identification of end entities in REM

A REMS needs to generate, exchange and validate attributes to support the identification and authentication of end entities like sender, recipient or a delegate. All provisions for identification and authentication in ERDS specified in clause 5 of ETSI EN 319 522-2 [1] shall apply to REM as well.

It is possible to provide REM service to users whose real-world identity is not established by the service provider. Even in that case, authentication of these users can be necessary, for instance in order to provide access to the mailbox or to provide access to evidence relating to a submitted user content.

In cases where the real-world identity of end users is established by the service provider, this identification can be performed in two manners:

1) Performing a full check of identity attributes and association with the real-world entity for each operation the user performs in the system; or

2) Performing a full check of identity attributes and association with the real-world entity once at the time of enrolment, and issuing or registering a method for authenticating the user, which is then used in each operation the user performs in the system.

REMS may provide information on the assurance level and method of both initial identity verification and authentication.

Initial identity verification of end users performed at their enrolment is out of scope of the present document.

The protocols used by regular email and often used by REM services as well - namely SMTP [i.4], IMAP [i.6] and POP3 [i.5] - all support user authentication based on the Simple Authentication and Security Layer (SASL), defined in IETF RFC 4422 [i.8], and also support secure communication over TLS [i.7]. When authentication is performed based on SASL or TLS then the REMS should include in the authentication components sufficient information about the mechanism such that the reported level of assurance is justified.

6 REM metadata content

6.1 Introduction

ERDS relay metadata defined in clause 6 of ETSI EN 319 522-2 [1] shall apply to REM as well.

In addition, components defined in the next clause apply.

6.2 Metadata components

6.2.1 Acceptance/rejection interface location

Description	Acceptance/rejection interface location
Format	URL
Meaning	In a REMS notification generated by a REMS operating in S&N style this component contains the location where the recipient can respond to the notification, and accept or reject the delivery of the user content referred to by the REMS notification.
Requirements	This component shall always be present in a REMS notification. This component should not be present in any other REM message. The content of this component **shall** be provided by the S&N REMS generating the REMS notification. R-REMS and intermediate REMSs **shall** propagate this component as received from the previous REMS in the delivery chain.

7 Digital signatures in REM

The requirements for digital signatures in ERDS specified in clause 7 of ETSI EN 319 522-2 [1] shall apply to REM as well. In addition, the following requirements apply.

The REM message shall bear the digital signature of the generating REMS.

The digital signature on the REM message shall cover all the basic components, as defined in clause 4.1, that are included in the REM message, except for the ERDS metadata (i.e. not only the mandatory components, but also the optional ones that are present, and all occurrences of a component that is included in multiple instances).

For more detailed requirements on the format of digital signatures applied in REM, see ETSI EN 319 532-3 [i.1] clause 8.

8 REM evidence set and components

ERDS evidence set and components defined in clause 8 of ETSI EN 319 522-2 [1] shall apply to REM services as well.

9 Common service interface content

9.1 Introduction

The common service interface (CSI) is the abstract interface through which the shared infrastructure assisting the delivery in a multi-provider scenario is accessible. The shared infrastructure is an abstract entity, which can include several distinct actors. The Common Service Interface can include several distinct interfaces in reality, as different functions of the CSI can be provided by different entities. The CSI can be used, among others, for the four purposes described in clause 4.3.1 of ETSI EN 319 522-1 [i.9]:

1) Message routing;
2) Trust establishment;
3) Capability management;
4) Governance support.

These purposes are described in the following clauses, with trust establishment and governance in the same clause.

It is possible to provide basic REM services with a lightweight shared infrastructure, consisting of:

- Routing information provided in public DNS, and
- Trust information provided in Trusted Lists, as defined in ETSI TS 119 612 [i.3].

If more sophisticated policy constraints or capability negotiations are needed then extensions to the above elements or further elements can be necessary in the shared infrastructure.

9.2 REM message routing

The requirements and explanations given in clause 9.2 of ETSI EN 319 522-2 [1] shall apply to REM, with the following amendments.

In REM, the identifier of a recipient is an email address. The REMS may use the Domain Name System (DNS) to find the server providing the REM RI (Relay Interface) of the REMS responsible for the domain identified in the domain part of the recipient's address. The REMS may attempt to forward the REM message directly to the identified server, or may use a different routing strategy.

Multi-hop routing of a REM message via a path of one or more intermediate REMSs is out of scope of the present document.

NOTE: One possibility to configure such multi-hop routing is to ensure that DNS lookups, as described above, for the recipient's domain by any server in the path always yield the next-hop server along the path.

9.3 REM trust establishment and governance

The requirements and explanations given in clause 9.3 of ETSI EN 319 522-2 [1] shall apply to REM, with the following amendments.

The REMS should use Trusted List (TL) to establish trust with other REMSs.

NOTE: This TL can be e.g. the European Trusted List system established pursuant to the Regulation (EU) No 910/2014 [i.2], or it can be a different TL set up specifically for a trust domain of REM services.

The REMS should ensure publication of information about itself in a TL to facilitate trust establishment by other REMSs.

Further details on the trust information about REMS in a TL can be found in clause 9.3 of ETSI EN 319 532-3 [i.1].

9.4 Capability management

9.4.1 Introduction

Capability management provides the functionality to resolve the unique identifier of a recipient into:

1) Identification of the R-REMS of which the recipient is a subscriber.

2) Metadata for the capabilities of the identified REMS.

3) Metadata for the capabilities of the recipient in the R-REMS.

9.4.2 Resolving recipient identification to ERDS identification

In REM, the identifier of a recipient is an email address. The domain part of this email address shall identify the REMS responsible for that domain (of which the recipient is a subscriber): R-REMS.

If the REMS supports receiving relayed messages from other REMS (i.e. it can act as I-REMS or R-REMS in a chain of REMSs) using SMTP, then the REMS should ensure that the hostname of the server providing the REM RI is available in MX records of the DNS to all other REMSs, which need to relay messages to this REMS. The hostname provided should be the same as the one included in a URI contained in the Service supply point of the TL entry (see clause 9.3 of ETSI EN 319 532-3 [i.1]), if the REMS uses TL to publish trust information about itself and the Service supply point element is present.

9.4.3 Recipient metadata

The requirements and explanations given in clause 9.4.3 of ETSI EN 319 522-2 [1] shall apply.

9.4.4 REMS capability metadata

The requirements and explanations given in clause 9.4.4 of ETSI EN 319 522-2 [1] shall apply to REMS provision, with the following amendments.

The REMS capabilities shall specify whether the REMS supports Store and Notify (S&N) style of operation within the "Supported mode of consignment" capability field according to the following rule: when either "**Consented**" or "**Consented signed**" or both are present, it means S&N style is supported; when neither of them are present, it means that S&N style is not supported.

If the REMS uses TL to publish trust information about itself, the REMS capability metadata may also be accessible using the TL; for more details see clause 9.4 of ETSI EN 319 532-3 [i.1].

History

Document history			
V1.0.0	May 2018	EN Approval Procedure	AP 20180823: 2018-05-25 to 2018-08-23