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

STABLE DRAFT FOR PUBLIC REVIEW UNTIL 29 DECEMBER 2017

Download the template for comments:
https://docbox.etsi.org/ESI/Open/Latest_Drafts/Template-for-comments.doc

Send comments ONLY to E-SIGNATURES_COMMENTS@list.etsi.org

CAUTION: This DRAFT document is provided for information and is for future development work within the ETSI Technical Committee ESI only. ETSI and its Members accept no liability for any further use/implementation of this Specification. Approved and published specifications and reports shall be obtained exclusively via the ETSI Documentation Service at http://www.etsi.org/standards-search
Contents

1 Intellectual Property Rights

2 Foreword

3 Modal verbs terminology

4 Introduction

5 Scope

6 References

7 Definitions and abbreviations

8 REM logical model

9 REM logical model

10 REM interfaces

11 REM events and evidence

12 Shared infrastructure of REM

ETSI
Intellectual Property Rights

IPRs essential or potentially essential to the present document 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.

Foreword

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

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";

<table>
<thead>
<tr>
<th>Proposed national transposition dates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date of latest announcement of this EN (doa):</td>
</tr>
<tr>
<td>Date of latest publication of new National Standard or endorsement of this EN (dop/e):</td>
</tr>
<tr>
<td>Date of withdrawal of any conflicting National Standard (dow):</td>
</tr>
</tbody>
</table>

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

EDITORIAL NOTE: introduction to be completed
1 Scope

The present document describes the logical model and basic concepts of Registered Electronic Mail (REM) service. Registered Electronic Mail is a specific type of electronic registered delivery service, which builds on the formats, protocols and mechanisms used in ordinary e-mail messaging.

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";

The general concepts and requirements of electronic registered delivery are described ETSI EN 319 522 covering Electronic Registered Delivery Services, which is also a multi-part deliverable. 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, 2 and 3 of EN 319 532 are aligned with EN 319 522, and they reference the necessary provisions of the corresponding part.

As a consequence, 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 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 319 522-1: "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 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 TR 119 001: "Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures; Definitions and abbreviations"
3 Definitions and abbreviations

3.1 Definitions

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

**electronic registered delivery service**: 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 unauthorised alterations.

**EDITORIAL NOTE**: THIS TERM MAY NEED TO BE CHANGED

**electronic registered delivery service provider**: entity which provides electronic registered delivery service.

NOTE: it can be a Trust Service Provider as defined in Regulation (EU) No 910/2014 [i.5]

**registered electronic mail**: enhanced form of e-mail transmitted by registered electronic mail service.

**registered electronic mail service**: electronic registered delivery service which builds on the formats, protocols and mechanisms used in ordinary e-mail messaging.

**registered electronic mail service provider**: entity which provides registered electronic mail service.

NOTE: it can be a Trust Service Provider as defined in Regulation (EU) No 910/2014 [i.5]

**user content**: the original data produced by the sender which has to be delivered to the recipient.
submission metadata: data submitted to the electronic registered delivery service together with the user content

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 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

original message: data structure including the user content and the submission metadata

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

sender: natural or legal person that submits the user content

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

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

ERD user agent/application: 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

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

handover: the 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

EDITORIAL NOTE: The following definitions of data structures have not yet been thoroughly discussed and are subject to change.

ERD message: data structure generated by the electronic registered delivery service, which contains any of the user content, ERDS relay metadata and/or ERDS evidence

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

ERDS serviceinfo: ERD message which contains some ERDS relay metadata

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

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

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

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

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

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

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

3.2 Abbreviations

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

CSI  Common Service Interface

EU  European Union
4 REM logical model

4.1 Introduction

4.1.1 Services and providers related to ERD

EDITORIAL NOTE: The material contained in this clause is still in progress and has not yet been fully agreed upon, so it is subject to changes.

An electronic registered delivery service (ERDS) is generally understood to be a 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 the transmitted data against the risk of loss, theft, damage or any unauthorised alterations. An electronic registered delivery service provider (ERDSP) is a legal entity which provides ERDS. The ERDSP is usually an organization, and it is responsible for the correctness of operations and issued evidence. The users of the service are usually clients or subscribers of only one of the ERDSPs, and they can send and receive data communicating only through their chosen service provider.

Each ERDSP can implement the communication between its own subscribers internally. In real life scenarios the users also need to communicate with the subscribers of other service providers. The ERDSPs can collaborate to allow exchange of messages among all their subscribers. However, they need to make some extra effort in order to achieve this, e.g. they need to interconnect their systems, establish routing and trust relationships, etc. In the end, through all these measures they can provide a higher level of service: electronic registered delivery reaching the clients of multiple providers.

The concept of ERDS can be interpreted in two different ways.
a) From the user’s point of view the service is provided by the collaboration of multiple ERDSPs. It works just like international phone calls: when a user in Rome calls a phone number in Oslo, they do not need to know which operator that number belongs to and which countries the call will go through. Similarly, when the sender submits a message through a registered delivery service, they will receive proof of sending and receipt of that message, regardless of which service providers were involved in the performance of the service. Henceforth, this is called an electronic registered delivery end-to-end service.

b) From a compliance point of view there are certain requirements a service must fulfil in order to be considered an electronic registered delivery service. These requirements are formulated so that they apply to one single ERDSP. (Otherwise, conformance assessment would not be feasible.) Henceforth, the service provided by one single ERDSP is called an electronic registered delivery service.

In general, the service provided by one single ERDSP can perform one or more of 3 roles in the delivery process:

1) Sender’s ERDS (S-ERDS): this component service is responsible for allowing the submission of the message for the sender, with proper tracking of this event. It is also responsible for forwarding the message to the next actor, as appropriate.

2) Intermediate ERDS (I-ERDS): this component service is responsible for receiving a forwarded message and forwarding it again according to the routing rules established in the collaboration of service providers, with proper tracking of the relevant events. Multiple I-ERDS components can participate in the delivery of a particular message.

3) Recipient’s ERDS (R-ERDS): this component service is responsible for receiving a forwarded message and delivering it to the recipient, with proper tracking of the relevant events.

In special cases, some roles can be omitted or can be combined into one. When the S-ERDS and R-ERDS can communicate directly then I-ERDS is not needed. When the sender and recipient are subscribers of the same ERDSP then the ERDS provided by that ERDSP can perform the roles of both S-ERDS and R-ERDS, and there is no need for forwarding the message at all.

Figure 1 shows an example where the sender and the recipient are subscribers of different ERDSPs, and the registered message is transferred through a third ERDSP as well.

![Figure 1: Services and providers related to ERD](image)

Notations used in the figure:

- In figure 1 the grey boxes represent the service providers (ERDSPs). They might also provide other services beside ERDS, but that is not shown in the figure.

- Each green box inside a grey box represents the service provided by the enclosing ERDSP. The green boxes correspond to the interpretation b) of the ERDS concept as described above (from a compliance point of view).
In the context of EU legislation, Regulation (EU) No 910/2014 [1,5] defines the terms ‘electronic registered delivery service’ and ‘qualified electronic registered delivery service’, and specifies requirements for the latter. The Regulation mentions the possibility of more than one provider participating in the provision of the service, but does not give any stipulations regarding the possible different interpretations of the ERDS concept, as described above. However, the requirements for a ‘qualified electronic registered delivery service’ include identification of the sender and addressee (recipient). In a general scenario, such as the one illustrated in figure 1, these requirements cannot be met by any single provider alone, but they can be fulfilled by the collaboration of the ERDSPs. In consequence, in such a multi-provider scenario, the ERD end-to-end service, as defined in interpretation a) above, could be able to satisfy the requirements of a ‘qualified electronic registered delivery service’ according to the Regulation.

In the present document, henceforth, the term ‘electronic registered delivery service’ and the acronym ‘ERDS’ are used solely in the sense of interpretation b) as described above, meaning the service provided by one single ERDSP.

**4.1.2 General description of REM service**

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 [1], is applicable to REMS.

Since REMS is a specific type of ERDS, the considerations in clause 4.1.1 also apply to REMS.

In the present document, henceforth, the term ‘registered electronic mail service’ and the acronym ‘REMS’ are used solely in the sense of a specific type of ERDS as described in item b) of clause 4.1.1 above, meaning the service provided by one single REMSP. All requirements specified in the present document shall be applied to the service provided by one single REMSP.

When the sender and the recipient are subscribers of different REMSPs, the REMSPs can collaborate to provide the REM end-to-end service, which is a specific type of ERD end-to-end service as described in item a) of clause 4.1.1 above.

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 or ERDSs 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 evidences. The figure 2 below provides a simple representation.
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 may 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 evidences. For REMS the unique identifier of users is an email address.

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 EN 319 532-2 [i.2] and EN 319 532-3 [i.3].

### 4.2.2 Sequence viewpoint

#### 4.2.2.1 REM styles of operation

From a procedural point of view, there are multiple alternative ways to deliver a message to a recipient. One aspect is whether an explicit acceptance is required before the consignment of the user content to the recipient occurs. In this aspect there are two alternatives:

- Acceptance is required: in this case the recipient must actively respond to the ERDSP before consignment, and the user content is consigned only if the response was positive.

- Acceptance is not required: in this case the consignment of the user content will be performed without waiting for any action of the recipient.

The delivery process in the two alternatives above is described in clause 4.2.2 of ETSI EN 319 522-1 [1].

Another aspect is whether the user content is conveyed to the recipient by value or by reference. In this aspect the two alternatives are:

- By value: the complete user content itself is conveyed to the ERD-UA of the recipient.

  **EXAMPLE 1:** sending a file in the body of an HTTP POST request.

  **EXAMPLE 2:** storing a file in the recipient’s mailbox, to be downloaded later by the email client via POP3.
By reference: a reference to the user content is conveyed to the ERD-UA of the recipient, and the complete user content itself is forwarded or downloaded only upon a request of the recipient.

EXAMPLE 1: sending a link (URL) to a document stored on an online server in the body of an HTTP POST request.

EXAMPLE 2: sending a link (URL) to a document stored on an online server in an email message.

The two aspects described above are independent, so in a general ERDS any combination of them could be applied. However, in REM only certain combinations are allowed, which are characterized by two styles of operation.

The two REM styles of operation are: "Store and Forward" (S&F) and "Store and Notify" (S&N).

In S&F style the user content provided by the sender is conveyed to the recipient by value, and acceptance is not required. This is typically performed by storing the user content in the recipient’s mailbox. The action of the REM service provider which makes the user content available to the recipient is called consignment. Once the user content is consigned, no other action is required from the recipient to access the user content besides identification and authentication.

In S&N style the user content provided by the sender is conveyed to the recipient by reference first, and acceptance is required. This is typically performed by sending a notification (possibly on a different channel or even multiple channels, e.g. email, SMS, push notification) to the recipient about the incoming message, containing a reference (e.g. a URL) to the user content. At this point the user content is not yet accessible to the recipient. The recipient needs to respond to the notification (on any channel provided by the REMSP) and either accept or reject the incoming message. If the recipient accepts the message, then the user content is consigned (made available to the recipient).

4.2.2.2 REM Store and Forward style of operation

The sequence of actions in S&F style of operation is depicted in figure 3, and detailed below. For simplicity, failure cases are not considered in this sequence.

![Figure 3: REM Store and Forward sequence of actions](www.websequence diagrams.com)
1. The sender (either a user or a system) identifies and authenticates herself to the REM service.

2. The sender (either a user or a system) prepares the user content, specifies one or more recipients, and submits it to the REM service. This step might in some cases merge with step 1 (e.g. if the original message in which the user content is submitted contains a digital signature which is used to identify the sender).

3. The REM service tracks the event that the user content has been submitted. This is done producing an "attestation of submission" (submission evidence), e.g. a signed file containing the basic information of the event.

4. The evidence of submission may optionally be sent back to the sender. See NOTE below.

5. The REM service stores the user content in the recipient's mailbox. It may also store additional related information (metadata, e.g. sender's identity, submission time, etc.) and evidence (e.g. submission evidence produced in step 3.) along with the user content. These may be enveloped together in one single bundle, called a REM dispatch, or may also be stored separately.

6. The REM service tracks the event that the user content has been made available to the recipient(s). Again, this is done producing one or more attestation (consignment evidence).

7. The evidence of consignment may optionally be sent back to the sender. See NOTE below.

8. The recipient (either a user or a system) identifies and authenticates herself to the REMS.

9. The recipient (either a user or a system) retrieves the user content (either enveloped in a REM dispatch, or separately), and optionally may also retrieve metadata and/or evidence (either enveloped in a REM dispatch, or separately).

10. The REM service tracks the event that the user content has been handed over to the recipient. In some cases this is done producing one or more attestation (handover evidence).

11. The evidence of handover may optionally be sent back to the sender. See NOTE below.

NOTE: In steps 4, 7, 11 sending the evidence right after its generation to the user is only one of the possible ways of providing the evidence, and there are other alternatives as well, e.g.: the evidence can be stored by the REMS for later on-demand access, it can be forwarded to an external evidence repository, etc.

4.2.2.3 REM Store and Notify style of operation

The sequence of actions in S&N style of operation is depicted in figure 4, and detailed below. For simplicity, failure cases are not considered in this sequence.
Figure 4: REM Store and Notify sequence of actions
1. The sender (either a user or a system) identifies and authenticates herself to the REM service.

2. The sender (either a user or a system) prepares the user content, specifies one or more recipients, and submits it to the REM service. This step might in some cases merge with step 1 (e.g. if the original message in which the user content is submitted contains a digital signature which is used to identify the sender).

3. The REM service tracks the event that the user content has been submitted. This is done producing an "attestation of submission" (submission evidence), e.g. a signed file containing the basic information of the event.

4. The evidence of submission may optionally be sent back to the sender. See NOTE 2 below.

5. The REM service stores the user content (and optionally metadata and/or evidence along with it, optionally enveloped in a REM dispatch) in a temporary storage where it is not accessible yet to the recipient, and generates a notification for the recipient, containing a reference (e.g. a URL) to the user content.

6. The REM service sends the notification to the recipient. It may be sent as an ERD message or using any other channel. Notifications sent through other channels (e.g. SMS, push notification) are outside the scope of the present document.

7. The REM service tracks the event that the notification has been sent. It may produce a corresponding attestation (notification evidence).

8. The evidence of notification may be sent back to the sender. See NOTE 2 below.

The following part of the sequence depends upon the action of the recipient. One of three alternatives may occur: the recipient accepts the message; the recipient rejects the message; the recipient does not respond within a predetermined time limit. If the user content is addressed to multiple recipients, this applies to each recipient.

**Alternative 1:** if the recipient accepts the message:

9. The recipient (either a user or a system) identifies and authenticates herself to the REMS.

10. The recipient performs an explicit action to confirm the acceptance of the incoming message by any means provided by the REM service (e.g. sending a reply message, visiting a URL, clicking on a button, signing an acknowledgment of receipt, etc.).

11. The REM service tracks the event that the message has been accepted by that particular recipient. This is done producing a corresponding attestation (evidence of acceptance).

12. The evidence of acceptance, optionally along with additional data (e.g. acknowledgment of receipt signed by the recipient), may be sent back to the sender. See NOTE 2 below.

13. The REM service stores the user content in the recipient’s mailbox. It may also store additional related information (metadata, e.g. sender’s identity, submission time, etc.) and evidence (e.g. evidence produced in step 3, step 7, step 10 or step 11) along with the user content. These may be enveloped together in one single bundle, called a REM dispatch, or may also be stored separately.

Alternatively, the user content (and any accompanying metadata) may also be made available for download directly through the channel in which the acceptance was performed (e.g. on the website of the REMS). The user content is considered to be consigned regardless of the channel provided that it is available for the recipient any time upon proper authentication.

14. The REM service tracks the event that the user content has been made available to the recipient(s). Again, this is done producing one or more attestation (consignment evidence).

15. The evidence of consignment may be sent back to the sender. See NOTE 2 below.

16. The recipient (either a user or a system) identifies and authenticates herself to the REMS.

17. The recipient (either a user or a system) retrieves the user content (either enveloped in a REM dispatch, or separately), and optionally may also retrieve metadata and/or evidence (either enveloped in a REM dispatch, or separately).

18. The REM service tracks the event that the user content has been handed over to the recipient. In some cases, this is done producing one or more attestation (handover evidence).
The evidence of handover may be sent back to the sender. See NOTE 2 below.

**Alternative 2:** if the recipient rejects the message:

9. The recipient (either a user or a system) identifies and authenticates herself to the REMS.

10. The recipient performs an explicit action to confirm the rejection of the incoming message by any means provided by the REM service (e.g. sending a reply message, visiting a URL, clicking on a button, signing a statement of rejection, etc.).

11. The REM service tracks the event that the message has been rejected by that particular recipient. This is done producing a corresponding attestation (evidence of rejection).

12. The evidence of rejection, optionally along with additional data, may be sent back to the sender. See NOTE 2 below.

**Alternative 3:** if the recipient does not respond within a predetermined time limit:

9., 10. The recipient takes no action.

11. The REM service tracks the event that the predetermined acceptance time period for that particular recipient has elapsed without any response. This is done producing a corresponding attestation (evidence of no-response).

12. The evidence of no-response, optionally along with additional data, may be sent back to the sender. See NOTE 2 below.

**NOTE 1:** The time period available for acceptance/rejection can be determined by legislation, policy rules, or parameters given by the sender. The method of determining this time period can be specified in the REM policy or REM practice statement of any provider providing S&N style of operation.

**NOTE 2:** In steps 4, 8, 12, 15, 19 sending the evidence right after its generation to the user is only one of the possible ways of providing the evidence, and there are other alternatives as well, e.g.: the evidence can be stored by the REMS for later on-demand access, it can be forwarded to an external evidence repository, etc.

### 4.3 4-corner model

#### 4.3.1 Functional viewpoint

When the sender and recipient are clients of the same REMS then no further communication between different parties is needed, and clause 4.2 describes all the interactions that are subject to standardization. (Data flows and processing internal to one REMS is outside the scope of the present document.) However, this is not always the case.

When the sender and the recipient are subscribed to different REMSs then the respective REMSs communicate in order to forward the user content, along with some metadata associated to it, and to provide evidence to the users about every relevant event during the process. This communication may happen directly, in which case only 2 REMSs are involved. This 4-corner model is described in this clause. In other cases, the communication may happen indirectly, involving a number of intermediate REMSs as well, which is described in the next clause 4.4.

The interaction of the individual services of the REMSPs provides the REM end-to-end service, including user content delivery and evidence provision. The interface between the users of the service and the REMSs they communicate with is the same as described in the black-box model above.

This clause focuses on the interaction between two REMSs that communicate directly with each other, as illustrated in figure 5.
Similarly to interconnected ERDSs in general, a shared infrastructure may assist the communication of interconnected REMSs. This may provide functions such as Message routing, Trust establishment, Capability management, Governance support, as described in clause 4.3.1 of ETSI EN 319 522 [1].

In REM the identifier of a user shall be an email address, which includes a domain specific part. The routing of REM messages may be based on the DNS records associated with the domain of the recipient address, just like in regular email messaging. In that case, it is possible that the Common user directory, as depicted in the figure, is not necessary.

REMSs operating in different styles of operation can interoperate in a range of combinations, such as:

- S&F to S&F, as described in clause 4.3.2.1;
- S&F to S&N, as described in clause 4.3.2.2;
- S&N to S&F, where a reference to the user content is relayed to the recipient’s REMS and delivered there using a S&F service, as described in clause 4.3.2.3;
- S&N to S&N, where a reference to the user content stored by the sender’s REMS is relayed to the recipient’s REMS, which normally operates in S&N style, but upon recognizing that the incoming message is a notification only, it will act in S&F style. The message flow in this case is identical to the one described in clause 4.3.2.3.

### 4.3.2 Sequence viewpoint

#### 4.3.2.1 REM S&F to S&F interaction

This clause describes the case when the sender’s REMS and the recipient’s REMS both operate in S&F style in the handling of a particular user content.

The sequence of actions in S&F to S&F interaction is depicted in figure 6, and detailed below. For simplicity, failure cases are not considered in this sequence. The REMSs may track each relevant event in the sequence by producing a corresponding evidence, as detailed in clause 4.2.2.2, but for an easier overview, the production of these evidences is...
not shown in the figure. The produced evidence may also be sent to the user, or may be provided in other ways, as described in clause 4.2.2.2. The optional returning of evidence to users is not shown in the figure.

The interactions with the users are the same as defined in clause 4.2.2.2 for Store & Forward style in the black-box model. Therefore, the indices of the actions relevant for the REM end-to-end service are kept the same as in figure 3. The new actions depicted in figure 6 are the communication steps between the REMSs, or in other words, communications internal to the REM delivery network. These are indexed with ‘N#’. The steps of the process are as detailed below.

NOTE: Steps N#. of the sequence are defined in a general way so that they can be reused in the extended model (see clause 4.4), where REM message relay is performed over a chain of multiple REMSs. The 4-corner model is a special case of this where only two REMSs are involved, namely the sender’s REMS and the recipient’s REMS.

1, 2, 3, 4. The user content is submitted, as in clause 4.2.2.2.

N1. Sender’s REMS (S-REMS) needs to find out how to reach the recipient’s REMS (R-REMS). In the general case this happens through a common infrastructure (Shared infrastructure). This is an abstract entity, which may correspond to several distinct actors. This step may involve multiple actions:

- S-REMS needs to identify the recipient’s REMS. This may be possible using the recipient’s mailbox address, as an email address contains the provider domain.

- S-REMS needs to find a mail route to the R-REMS. This may be possible using DNS lookups, as it is done in the case of regular email messages. In the 4-corner model (clause 4.3) it is assumed that the REM message can be forwarded directly to R-REMS. In the extended model (clause 4.4) it is assumed that the REM message is forwarded through a number of intermediate REMSs.

- S-REMS needs to check the capabilities of the REMSs along the mail route (e.g. supported style of operation, supported policies, etc.) in order to find a suitable route.
- S-REMS needs to establish a trust relationship with the next-hop REMS along the mail route. This may be done, for instance, using Trusted Lists, as defined in ETSI TS 119 612 [i.7].

N2. The REMS performs a handshake with the next-hop REMS. This may include negotiation on different aspects (capabilities, supported style of operation, ERDS evidence, level of authentication of end entities, fees, etc.). Handshake may not be necessary in closed systems where this information is defined a priori or available through a centralised infrastructure.

N3. The REMS relays the REM message to the next-hop REMS. It may also relay additional related information (metadata, e.g. sender's identity, submission time, etc.) and evidence (e.g. submission evidence produced in step 3.) along with it.

N4. The REMS that received the relayed REM message may also look up the relaying REMS in the shared infrastructure, and get information (e.g. certificates), establish trust, etc.

N5. If the REM message has been successfully received and the validation of the relaying REMS reported no problems, then the REMS tracks this event by producing a corresponding evidence of relay.

N6. The evidence of relay is returned to the relaying REMS, as an indication that the responsibility of handling the relayed REM message has been taken over by the next REMS.

5, 6. The user content is consigned, as in clause 4.2.2.2.

N7. The evidence of consignment needs to be relayed back to the previous REMS along the mail route, so that it can close its transaction, and the sender may also need this attestation.

7. The evidence of consignment may be returned to the sender, as in clause 4.2.2.2.

8, 9, 10. The user content is handed over to the recipient, as in clause 4.2.2.2.

N8. The evidence of handover needs to be relayed back to the previous REMS along the mail route, in case the sender needs this attestation.

11. The evidence of handover may be returned to the sender, as in clause 4.2.2.2.

4.3.2.2 REM S&F to S&N interaction

This clause describes the case when the sender’s REMS operates in S&F style and the recipient’s REMS operates in S&N style in the handling of a particular user content. The user content is relayed to the R-REMS in the same manner as detailed in clause 4.3.2.1. The R-REMS performs the acceptance/rejection process of the S&N style as described in clause 4.2.2.3, except that the evidences are not returned directly to the sender but relayed back through S-REMS.

The sequence of actions in S&F to S&N interaction is depicted in figure 7, and detailed below. For simplicity, failure cases are not considered in this sequence. The REMSs may track each relevant event in the sequence by producing a corresponding evidence, as detailed in clause 4.2.2.3, but for an easier overview, the production of these evidences is not shown in the figure. The produced evidence may also be sent to the user, or may be provided in other ways, as described in clause 4.2.2.3. The optional returning of evidence to users is not shown in the figure.
The interactions with the users are the same as defined in clause 4.2.2.3 for Store & Notify style in the black-box model. Therefore, the indices of the actions relevant for the REM end-to-end service are kept the same as in figure 4. The new actions depicted in figure 7 are the communication steps between the REMSs, or in other words, communications internal to the REM delivery network. These are indexed with ‘N#’. The steps of the process are as detailed below.

1, 2, 3, 4. The user content is submitted, as in clause 4.2.2.3.

N1, N2, N3, N4, N5, N6. The user content is relayed, as in clause 4.3.2.1. (The REM message in the description of steps N1-N6. is in this case a REM dispatch.)

5, 6, 7. The user content is deposited in a temporary storage and a notification is sent, as in clause 4.2.2.3.

**Figure 7: 4-corner S&F to S&N sequence**
The evidence of notification needs to be relayed back to the previous REMS along the mail route, in case the sender needs this attestation.

The evidence of notification may be returned to the sender, as in clause 4.2.2.3.

9. 10. 11. The recipient accepts/rejects/does not respond to the incoming message, and the result is tracked as in clause 4.2.2.3.

The evidence of the acceptance/rejection/no-response needs to be relayed back to the previous REMS along the mail route, in case the sender needs this attestation.

12. The evidence of acceptance/rejection/no-response may be returned to the sender, as in clause 4.2.2.3.

**Conditional:** if the recipient accepted the incoming message:

13. 14. The user content is consigned, as in clause 4.2.2.3.

N12. The evidence of consignment needs to be relayed back to the previous REMS along the mail route, so that it can close its transaction, and the sender may also need this attestation.

15. The evidence of consignment may be returned to the sender, as in clause 4.2.2.3.

16, 17, 18. The recipient retrieves the user content, as in clause 4.2.2.3.

N13. The evidence of handover needs to be relayed back to the previous REMS along the mail route, in case the sender needs this attestation.

19. The evidence of handover may be returned to the sender, as in clause 4.2.2.3.

### 4.3.2.3 REM S&N to S&F interaction

This clause describes the case when the sender’s REMS operates in S&N style and the recipient’s REMS operates in S&F style in the handling of a particular user content. Instead of the user content itself, at first the notification is relayed to the R-REMS in a manner similar to the relay of the user content as detailed in clause 4.3.2.1. The S-REMS performs the acceptance/rejection process of the S&N style as described in clause 4.2.2.3, except that the user content is not consigned directly to the recipient’s mailbox but relayed to R-REMS first. (The user content may also be handed over directly to the recipient, but this is not detailed in this clause.) The notification is always handled by a S&F sub-component even if the REMS normally acts in S&N style, so the sequence is the same also when the R-REMS operates in S&N style.

The sequence of actions in S&N to S&F interaction – which is also applicable in the S&N to S&N case – is depicted in figure 8, and detailed below. For simplicity, failure cases are not considered in this sequence. The REMSs may track each relevant event in the sequence by producing a corresponding evidence, as detailed in clause 4.2.2.3, but for an easier overview, the production of these evidences is not shown in the figure. The produced evidence may also be sent to the user, or may be provided in other ways, as described in clause 4.2.2.3. The optional returning of evidence to users is not shown in the figure.
The interactions with the users are the same as defined in clause 4.2.2.3 for Store & Notify style in the black-box model. Therefore, the indices of the actions relevant for the REM end-to-end service are kept the same as in figure 4. The new actions depicted in figure 8 are the communication steps between the REMSs, or in other words, communications internal to the REM delivery network. These are indexed with 'N#'. The steps of the process are as detailed below.

1. The user content is submitted, as in clause 4.2.2.3.

2. The user content is deposited in a temporary storage and a notification is generated, as in clause 4.2.2.3.
N1, N2, N3, N4, N5, N6. The S-REMS relays the notification, as in clause 4.3.2.1. (The REM message in the description of steps N1-N6. is in this case a REMS notification.)

6. 7. The R-REMS interprets the incoming REMS notification (containing the reference to the user content). Then it notifies the recipient using any channel they have agreed on, and tracks this event, as in clause 4.2.2.3.

N7. The evidence of notification needs to be relayed back to the previous REMS along the mail route, in case the sender needs this attestation.

8. The evidence of notification may be returned to the sender, as in clause 4.2.2.3.

9, 10, 11. The recipient accepts/rejects/does not respond to the incoming message, communicating directly with S-REMS when needed, and the result is tracked as in clause 4.2.2.3.

12. The evidence of acceptance/rejection/no-response may be returned to the sender, as in clause 4.2.2.3.

Conditional: if the recipient accepted the incoming message:

N9. The REMS relays the user content to the next-hop REMS. It may also relay additional related information (metadata, e.g. sender’s identity, submission time, etc.) and evidence (e.g. submission evidence produced in step 3.) along with it. The REMS may also hand over the user content directly to the recipient. (This is not shown in the figure.)

N10. If the REM message has been successfully received and the validation of the relaying REMS reported no problems, then the REMS tracks this event by producing a corresponding evidence of relay.

N11. The evidence of relay is returned to the relaying REMS, as an indication that the responsibility of handling the relayed REM message has been taken over by the next REMS.

13, 14. The user content is consigned, as in clause 4.2.2.3.

N12. The evidence of consignment needs to be relayed back to the previous REMS along the mail route, so that it can close its transaction, and the sender may also need this attestation.

15. The evidence of consignment may be returned to the sender, as in clause 4.2.2.3.

16, 17, 18. The recipient retrieves the user content, as in clause 4.2.2.3.

N13. The evidence of handover needs to be relayed back to the previous REMS along the mail route, in case the sender needs this attestation.

19. The evidence of handover may be returned to the sender, as in clause 4.2.2.3.

4.4 Extended model

4.4.1 Functional viewpoint

In the general scenario, the delivery process may go through several chained REMSs, as presented in figure 9. The interaction of the individual services of the REMSPs provides the REM end-to-end service, including user content delivery and evidence provision. The interface between the users of the service and the REMSs they communicate with is the same as described in the black-box model above.

This clause focuses on the interactions between the different REMSs in the case when more than 2 REMSs take part in the delivery process.
When the sender and the recipient are subscribed to different REMSs then the respective REMSs communicate in order to forward the user content, along with some metadata associated to it, and to provide evidence to the users about every relevant event during the process. This communication may happen indirectly, involving a number of intermediate REMSs as well, which may provide routing assistance, trust gateway, and other auxiliary functions.

In the most general case a service provider acting as a REMSP could also be able to communicate using other formats and protocols which are different from REM, and thus provide interconnection with other types of ERDSs. An intermediate ERDS could also provide such protocol conversion, thereby acting as a gateway between a REM and a non-REM ERDS.

The present document (and also part 2 and part 3 of the present deliverable) describes the interactions between REMSs building on the email-based REM formats and protocols only. Communication with other non-REM ERDSs is out of scope of the present document. See ETSI EN 319 522-1 [1] for guidance in that area.

Similarly to interconnected ERDSs in general, a shared infrastructure may assist the communication of interconnected REMSs. In a multi-ERDS delivery scenario, some components which are normally implemented by an ERDS (dotted boxes in the figure) might be moved to the shared infrastructure, like for instance: shared user directory, shared evidence repository.

Each of the REMSs involved in the delivery process may operate in S&F or S&N style (or may support both).

However, in any chain of REMSs only one REMS can act effectively according to the S&N style, since the notification is always handled by a S&F sub-component. Therefore, all the REMSs along the chain after the first S&N REMS shall behave as S&F ones. The interactions between any two adjacent REMSs follow one of the patterns described in clause 4.3.2. If there is no S&N REMS in the chain, then all interactions are as in clause 4.3.2.1. Otherwise, all interactions before (on the sender’s side of) the S&N REMS are like in clause 4.3.2.2, and all interactions after (on the recipient’s side of) the S&N REMS are like in clause 4.3.2.3. These two options are detailed in the next clause.

### 4.4.2 Sequence viewpoint

#### 4.4.2.1 Multi-hop sequence over S&F nodes only

When all REMSs in the chain operate in S&F style, the user content itself will be relayed along the chain to R-REMS, and the evidences will be relayed backwards along the chain to S-REMS. The interactions with the users are still the same as defined in clause 4.2.2.2 for Store & Forward style in the black-box model. The communication between any...
two adjacent REMSs follows the pattern described in clause 4.3.2.1. The sequence of steps N1, N2, N3, N4, N5, N6 will be repeated as many times as needed to relay the user content. Steps N7 and N8 will be repeated individually as many times as needed to relay any evidence.

As an example, the complete flow of communications involving 3 REMSs, each operating in S&F style, is depicted in figure 10. For simplicity, failure cases are not considered in this sequence. The REMSs may track each relevant event in the sequence by producing a corresponding evidence, as detailed in clause 4.2.2.2, but for an easier overview, the production of these evidences is not shown in the figure. The produced evidence may also be sent to the user, or may be provided in other ways, as described in clause 4.2.2.2. The optional returning of evidence to users is not shown in the figure.

![Figure 10: extended S&F to S&F to S&F sequence](image)

### 4.4.2.2 Multi-hop sequence involving a S&N node

When one of the REMSs in the chain operate in S&N style, the user content itself will be relayed along the chain to this REMS, where it will be stored temporarily, and from there the REMS notification will be relayed along the chain to R-REMS. Any evidence will be relayed backwards along the chain to S-REMS. The interactions with the users are still the same as defined in clause 4.2.2.3 for Store & Notify style in the black-box model. The communication between any two adjacent REMSs before (on the sender’s side of) the S&N REMS follows the pattern described in clause 4.3.2.2, and the communication between any two adjacent REMSs after (on the recipient’s side of) the S&N REMS follows the pattern described in clause 4.3.2.3. The sequence of steps N1, N2, N3, N4, N5, N6 will be repeated as many times as needed to relay the user content up to the S&N node, and to relay the REMS notification from there up to R-REMS. The sequence of steps N9, N10, N11 will be repeated as many times as needed to relay the user content from the S&N node up to R-REMS. Steps N7, N8, N12, and N13 will be repeated individually as many times as needed to relay any evidence.

As an example, the complete flow of communications involving 3 REMSs, the middle one operating in S&N style, is depicted in figure 11. For simplicity, failure cases are not considered in this sequence. The S&N REMS may also hand over the user content directly to the recipient, but this is not shown in the figure. The REMSs may track each relevant event in the sequence by producing a corresponding evidence, as detailed in clause 4.2.2.3, but for an easier overview, the production of these evidences is not shown in the figure. The produced evidence may also be sent to the user, or
may be provided in other ways, as described in clause 4.2.2.3. The optional returning of evidence to users is not shown in the figure.

Figure 11: extended S&F to S&N to S&F sequence

4.5 Roles within a REMS

The logical model 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>
<thead>
<tr>
<th>Component of REMS</th>
<th>Corresponding ERDS component</th>
</tr>
</thead>
<tbody>
<tr>
<td>REMS message delivery agent</td>
<td>ERDS Message delivery system</td>
</tr>
<tr>
<td>REMS evidence provider</td>
<td>ERDS Evidence provider</td>
</tr>
<tr>
<td>REMS evidence repository</td>
<td>ERDS Evidence repository</td>
</tr>
<tr>
<td>REMS user directory</td>
<td>ERDS User directory</td>
</tr>
</tbody>
</table>

In addition to the general ERDS components, a REMS also provides a REMS message store component. A REMS message store is allocated to the senders and recipients, and is securely accessible by senders and recipients respectively to retrieve REM messages addressed to them.

The REMS shall include the following core roles: REMS message delivery agent, REMS message store, and REMS evidence provider.

## 5 REM interfaces

Since REMS is a specific type of ERDS, the ERD interfaces described in ETSI EN 319 522-1 [1] clause 5 can also be applied to REM. However, in ERDSs the transport mechanisms can vary and therefore only a high-level abstraction of the interfaces is specified in ETSI EN 319 522-1 [1]. On the other hand, in REM the transport mechanisms are mostly based on regular email messaging, so a more fine-grained specification is given for REM interfaces in this clause.

Figure 12 illustrates the interfaces of the REM services. The 4-corner model is used for this illustration, but any REMS can provide all the presented interfaces. Detailed specification of the interfaces, and their relation to the abstract ERDS interfaces, is provided below in table 2.

![Figure 12: Interfaces of REMSs](image-url)
### Table 2: Requirements for REM interfaces

<table>
<thead>
<tr>
<th>Name of interface</th>
<th>Corresponding ERDS interface in EN 319 522-1 [1]</th>
<th>Specific requirements for REM</th>
</tr>
</thead>
<tbody>
<tr>
<td>REM MSI: Message Submission Interface</td>
<td>ERDS MSI: Message Submission Interface: this interface is used by the sender's ERD-UA to submit messages (ERD Original Message) to the sender's ERDS, for them to be forwarded to the recipient(s). This interface shall require identification and authentication, either direct (e.g. through credential check) or indirect (e.g. though a token from a third party). This interface shall implement confidentiality and integrity preserving measures.</td>
<td>The REM MSI shall be provided. Requirements on ERDS MSI shall apply to REM MSI. The REM MSI should be provided using SMTP [i.9] over TLS [i.12]. See also [i.14] and [i.16]. Other protocols may be used only if they create a secure channel providing confidentiality, integrity and authenticity of data sent through the channel (e.g. TLS). Example: HTTPS may be used. NOTE: Authentication can rely on the features provided by SASL [i.13], TLS (e.g. certificate-based authentication), or S/MIME [i.8] digital signature over the submitted message.</td>
</tr>
<tr>
<td>REM MRI: Message Retrieval Interface</td>
<td>ERDS MRI: Message and Evidence Retrieval Interface: this interface is used to retrieve (user content and the associated evidence. This interface requires identification and authentication, either direct (e.g. through credential check) or indirect (e.g. though a token from a third party). This interface shall implement confidentiality and integrity preserving measures.</td>
<td>The REM MRI shall be provided. Requirements on ERDS MERI shall apply to REM MRI. The REM MRI should be provided using IMAP [i.11] over TLS or POP3 [i.10] over TLS. Other protocols may be used only if they create a secure channel providing confidentiality, integrity and authenticity of data sent through the channel (e.g. TLS). Example: HTTPS may be used. NOTE: Authentication can rely on the features provided by SASL [i.13] or TLS (e.g. certificate-based authentication).</td>
</tr>
<tr>
<td>REM ERI: Evidence Retrieval Interface</td>
<td>ERDS RI: Relay Interface: this interface allows ERD messages to be relayed between ERDS. This interface shall implement confidentiality and integrity preserving measures.</td>
<td>The REM ERI shall be provided. Requirements on ERDS MERI shall apply to REM ERI. The REM ERI may use the same channel as the REM MRI, but may also use separate channels.</td>
</tr>
<tr>
<td>REM RI: Relay Interface</td>
<td>ERDS RI: Relay Interface: this interface allows ERD messages to be relayed between ERDS. This interface shall implement confidentiality and integrity preserving measures.</td>
<td>The REM RI should be provided. Requirements on ERDS RI shall apply to REM RI. The REM RI should be provided using SMTP over TLS. Other protocols may be used only if they create a secure channel providing confidentiality, integrity and authenticity of data sent through the channel (e.g. TLS). Example: HTTPS may be used. Implementation of this interface should follow the requirements defined in clause 5 of ETSI EN 319 532-4 [i.4]. The ERDS RI may be provided using other protocols. NOTE: This can be useful when the REMS communicates with other non-REM ERDSs.</td>
</tr>
<tr>
<td>REM ARI: Acceptance/Rejection Interface</td>
<td>This interface can be provided by non-REM ERDS as well, but it is not specified in EN 319 522-1 [1]. This interface is used by the recipient to respond to a REMS notification and signal the acceptance or rejection of the incoming message.</td>
<td>The REM ARI shall be provided when the REMS operates in S&amp;N style. The REM ARI may be provided using any techniques. The REMS should include in the REMS notification sufficient information so that the recipient can use the REM ARI.</td>
</tr>
<tr>
<td>-</td>
<td>ERD-UA MEPI: ERD-UA Message and Evidence Push Interface</td>
<td>In regular email messaging the user agent acts as a client towards the mail service provider. Hence, in REM pushing a message to an ERD-UA is not typical. For this reason, no corresponding REMS interface is defined for the ERD-UA MEPI.</td>
</tr>
<tr>
<td>Name of interface</td>
<td>Corresponding ERDS interface in EN 319 522-1 [1]</td>
<td>Specific requirements for REM</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>CSI: Common Service Interface</td>
<td>CSI: Common Service Interface: this interface gives access to message routing functions, trust management functions, capability management functions, governance functions.</td>
<td>Interoperable REMS (which communicates with other REMS) should use CSI. CSI can be a set of distinct interfaces providing different functions. The REMS may provide some functions that can be used in place of the CSI (e.g. publication of capabilities, routing information, etc.).</td>
</tr>
</tbody>
</table>

### 6 REM events and evidence

#### 6.1 Overview

The event types listed in clause 6.1 of EN 319 522-1 [1] shall apply.

The definitions of the event types in clause 6.2 of EN 319 522-1 [1] shall apply, as further specified in clause 6.2 of the present document.

The requirements on the production of evidence for each event type as defined in clause 6.1 of ETSI EN 319 522-1 [1] shall apply.

Additional requirements for REM on the production of evidence for each event type are specified in clause 6.2 of the present document.

#### 6.2 Events and evidence

##### 6.2.1 A. Events related to the submission

**Submission** is the transaction in which the original message, coming from the outside, passes through the **REMS**: **Message Submission Interface** of by the REMS. The transaction may involve authentication of the sender.

In REM the original message is the payload of the transaction as received by the system under the responsibility of the REMSP.

When the **REMS** is provided using SMTP then this transaction is an SMTP transaction. The client may be a user agent or a mail transfer agent.

After submission the REMS may inspect the submitted original message to decide about its acceptance (e.g. it may validate the digital signature – if any – over the message, may verify that headers of the message correspond to the authenticated user, may check whether the message complies with the policy rules, etc.). The decision of the REMS shall be one of the events listed in table 3.

<table>
<thead>
<tr>
<th>Event type in 319 522-1</th>
<th>Related interface</th>
<th>Issuing REMS</th>
<th>Interpretation</th>
</tr>
</thead>
<tbody>
<tr>
<td>A.1. SubmissionAcceptance</td>
<td>REM MSI</td>
<td>S-REMS</td>
<td>The REMS has accepted the submitted original message, and the REMSP takes responsibility for delivering it to all specified recipients respecting the policy rules and all delivery options given by the sender.</td>
</tr>
<tr>
<td>A.2. SubmissionRejection</td>
<td>REM MSI</td>
<td>S-REMS</td>
<td>The REMS has rejected the submitted original message. The REMS shall inform the sender about the reason(s) for the rejection. See ETSI EN 319 522-2 [1.6] clause 8.3.3 about possible reasons.</td>
</tr>
</tbody>
</table>

##### 6.2.2 B. Events related to the relay between REMSs

A REMS may communicate with other REMSs or ERDSs in order to forward user content to recipients not subscribed to the REMS, or to deliver user content from senders not subscribed to the REMS. When a REMS interoperates with another REMS then it shall provide evidence corresponding to the events described in this clause.
**Relay** is the handing over of a REM message from one REMS (sending REMS henceforth) to another REMS (receiving REMS henceforth) through the REM RI: Relay Interface. When the REM RI is provided using SMTP then this transaction is an SMTP transaction.

After a successful relay of a REM message containing user content the REMSP operating the receiving REMS shall take over the responsibility of handling the user content according to the requirements in the present document and the policy rules. The receiving REMS may inspect the REM message to decide about its acceptance (e.g. it may verify trust in the sending REMS, check the compliance of the REM message with policy rules, etc.). The receiving REMS shall issue evidence about its decision over the relayed user content, and shall convey this evidence to the sending REMS. If the receiving REMS rejects the relayed user content, then the REMSP operating the sending REMS shall be responsible again for handling the relayed user content according to the requirements.

If the relay of a REM message containing user content has failed then the responsibility of handling the user content according to the requirements in the present document and the policy rules shall remain with the REMSP operating the sending REMS. The sending REMS shall issue evidence about the failure of the relay.

The REMS shall track the relay of each user content under its responsibility (regardless of whether it is enveloped in a REM dispatch or not), regardless of whether it is the sender’s REMS or an intermediary REMS.

The REMS shall track the relay of each REMS notification (about S&N style of operation see clause 4.2.2.3) under its responsibility, regardless of whether it was generated by this REMS or previously relayed by another REMS.

The REMS need not track the relay of REM messages containing only evidence, i.e. need not issue evidence about it (but may log it for instance).

### Table 4: Events related to relay between REMSs

<table>
<thead>
<tr>
<th>Event type in 319 522-1</th>
<th>Related interface</th>
<th>Issuing REMS</th>
<th>Interpretation</th>
</tr>
</thead>
<tbody>
<tr>
<td>B.1. RelayAcceptance</td>
<td>REM RI</td>
<td>Receiving REMS</td>
<td>The receiving REMS has accepted the relayed REM message, and the REMSP takes responsibility for handling it according to the requirements in the present document and the policy rules.</td>
</tr>
<tr>
<td>B.2. RelayRejection</td>
<td>REM RI</td>
<td>Receiving REMS</td>
<td>The receiving REMS has rejected the relayed REM message. The receiving REMS shall inform the sending REMS about the reason(s) for the rejection. See ETSI EN 319 522-2 [1.6] clause 8.3.3 about possible reasons.</td>
</tr>
<tr>
<td>B.3. RelayFailure</td>
<td>REM RI</td>
<td>Sending REMS</td>
<td>The sending REMS was unable to relay the REM message to the receiving REMS within a given time period, or the receiving REMS did not return evidence about the acceptance or rejection of the REM message within that time period.</td>
</tr>
</tbody>
</table>

**6.2.3 C. Events related to the acceptance/rejection by the recipient**

When a REMS operates in S&N style or interoperates with another REMS operating in S&N style then it shall provide evidence corresponding to the events described in this clause.

In the most general case the user content can be forwarded through a chain of REMSs. Only one of these can effectively operate in S&N style (see clause 4.4.1) (notifying REMS henceforth). The notifying REMS shall generate the notification, and shall track the response of the recipient. A time period can be specified for the response of the recipient by legislation, policy rules or parameters given by the sender. The notifying REMS shall issue evidence about the appropriate one of the events regarding the response of the recipient.

The notification shall be relayed to the R-REMS. Upon receiving a notification addressed to one of its subscribers, R-REMS shall notify the subscriber. R-REMS may use any channel to notify the recipient. R-REMS should issue evidence about the successful or unsuccessful notification of the recipient.
### 6.2.4 D. Events related to the consignment

Consignment is the operation of R-REMS which makes the user content available to the recipient such that no other action is required from the recipient to access the user content besides identification and authentication. Hence, consignment is considered to be performed internally by the REMS, not through any outer interfaces. R-REMS shall issue evidence about the successful or unsuccessful consignment of each user content, regardless of whether it is consigned inside a REM dispatch or separately.

**EXAMPLE:** Consignment can be performed by storing the message in a mailbox which the recipient can access with authentication.

R-REMS may optionally notify the recipient about the consigned user content. This may be done using any channel they agreed upon, it need not use any of the standardised interfaces. R-REMS may also issue evidence about the successful or unsuccessful notification of the recipient about the consigned user content.

### 6.2.5 E. Events related to the handover to the recipient

Handover is the transaction in which the user content (either enveloped in a REM dispatch, or separately) passes through the REM MRI: Message Retrieval Interface of the REMS, from the REMS to the recipient’s ERD-UA. The transaction involves authentication of the user performing the handover. In this transaction, related metadata and/or evidence may also be handed over along with the user content (either enveloped in a REM dispatch, or separately).

**NOTE:** Handover is often performed using a user agent or other application, which connects as a client to the server providing the REM MRI.

When the REM MRI is provided using IMAP/POP3, then this transaction is an IMAP/POP3 transaction, which may involve handover of more than one message containing user content. When IMAP is used, fetching only the headers of the message (without the mail body) does not constitute handover. When the REM MRI is provided using HTTP, then download of the message by the HTTP client is considered as handover.
NOTE: In ETSI TS 102 640-1 download of the message was defined to be a separate event from retrieval of the message. This standard considers those two cases as one, consequently there is no separate download event defined.

Table 7: Events related to the handover to the recipient

<table>
<thead>
<tr>
<th>Event type in 319 522-1</th>
<th>Related interface</th>
<th>Issuing REMS</th>
<th>Interpretation</th>
</tr>
</thead>
<tbody>
<tr>
<td>E.1. ContentHandover</td>
<td>REM MRI</td>
<td>R-REMS</td>
<td>The user content has successfully passed through the REM MRI from the REMS to the client under the responsibility of the recipient.</td>
</tr>
<tr>
<td>E.2. ContentHandoverFailure</td>
<td>REM MRI</td>
<td>R-REMS</td>
<td>The user content did not pass through the REM MRI within a given time period.</td>
</tr>
</tbody>
</table>

6.2.6 F. Events related to connections with non-ERDS systems

The REMSP may provide interconnection with services that are not ERDS (e.g. physical mail, regular email, sector-specific delivery system, etc.) and as such unable to provide ERDS evidence about the events occurring under their responsibility. When a user content is received from such a service or is relayed to such a service then it cannot be considered that the delivery of this user content has been provided by an ERDS. Still, in some cases allowing communication between such systems has value for the users and so can be desirable.

If the REMSP provides this feature, it should issue evidence corresponding to the events described in this clause.

Table 8: Events related to connections with non-ERDS systems

<table>
<thead>
<tr>
<th>Event type in 319 522-1</th>
<th>Related interface</th>
<th>Issuing REMS</th>
<th>Interpretation</th>
</tr>
</thead>
<tbody>
<tr>
<td>F.1. RelayToNonERDS</td>
<td>n/a</td>
<td>Relaying REMS</td>
<td>The REMS has successfully relayed the user content to the given non-ERDS system.</td>
</tr>
<tr>
<td>F.2. RelayToNonERDSFailure</td>
<td>n/a</td>
<td>Relaying REMS</td>
<td>The REMS was unable to relay the user content to the non-ERDS system within a given time period.</td>
</tr>
<tr>
<td>F.3. ReceivedFromNonERDS</td>
<td>n/a</td>
<td>Receiving REMS</td>
<td>The REMS has received the user content from a non-ERDS system, therefore all information related to its sending, like the sender's identifier and the sending time, cannot be trusted per se.</td>
</tr>
</tbody>
</table>

7 Shared infrastructure of REM

When the registered mail delivery involves multiple REM services of multiple providers, usually some shared infrastructure is used in the discovery, identification and assessment of the services, as specified in clauses 4.3.1 and 4.4.1.

This is an abstract entity, which may consist of multiple distinct actors in reality. Its abstract interface is called CSI: Common Service Interface, which may also include several distinct interfaces in reality, as different functions of the CSI may be provided by different entities.

For further information see clause 9 of EN 319 532-2 [i.2].

History

<table>
<thead>
<tr>
<th>Document history</th>
</tr>
</thead>
<tbody>
<tr>
<td>V0.0.4 October 2017</td>
</tr>
</tbody>
</table>