

Draft **ETSI EN 319 532-1** V1.0.0 (2018-05)



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

Reference

DEN/ESI-0019532-1

Keywords

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

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

The present document can be downloaded from:

<http://www.etsi.org/standards-search>

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status.

Information on the current status of this and other ETSI documents is available at

<https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx>

If you find errors in the present document, please send your comment to one of the following services:

<https://portal.etsi.org/People/CommitteeSupportStaff.aspx>

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.

The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2018.

All rights reserved.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members.

3GPP™ and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.

oneM2M logo is protected for the benefit of its Members.

GSM® and the GSM logo are trademarks registered and owned by the GSM Association.

Contents

Intellectual Property Rights	4
Foreword.....	4
Modal verbs terminology.....	4
Introduction	5
1 Scope	7
2 References	7
2.1 Normative references	7
2.2 Informative references.....	7
3 Definitions and abbreviations.....	8
3.1 Definitions.....	8
3.2 Abbreviations	10
4 REM logical model	10
4.1 Introduction	10
4.2 Black-box model	11
4.2.1 Functional viewpoint	11
4.2.2 Sequence viewpoint	12
4.2.2.1 REM styles of operation.....	12
4.2.2.2 REM Store and Forward style of operation.....	13
4.2.2.3 REM Store and Notify style of operation.....	14
4.3 4-corner model	17
4.3.1 Functional viewpoint	17
4.3.2 Sequence viewpoint	18
4.3.2.1 REM S&F to S&F interaction.....	18
4.3.2.2 REM S&F to S&N interaction	20
4.3.2.3 REM S&N to S&F interaction	22
4.4 Extended model.....	24
4.4.1 Functional viewpoint	24
4.4.2 Sequence viewpoint	26
4.4.2.1 Multi-hop sequence over S&F nodes only.....	26
4.4.2.2 Multi-hop sequence involving a S&N node.....	27
5 REM interfaces.....	29
6 REM events and evidence	31
6.1 Overview	31
6.2 Events and evidence	31
6.2.1 A. Events related to the submission.....	31
6.2.2 B. Events related to the relay between REMSs.....	32
6.2.3 C. Events related to the acceptance/rejection by the recipient.....	32
6.2.4 D. Events related to the consignment.....	33
6.2.5 E. Events related to the handover to the recipient.....	34
6.2.6 F. Events related to connections with non-ERDS systems	34
History	35

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 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".

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

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the [ETSI Drafting Rules](#) (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Introduction

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

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

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

In a number of national, regional or sector-specific communities electronic registered delivery and registered electronic mail services are already in place, and even more are being developed. Without the definition of common standards there will be no consistency in the services provided, making it difficult for users to compare them. Under these circumstances, users might be prevented from easily changing to alternative providers, damaging free competition. Lack of standardization might also adversely affect interoperability between implementations which are based on different models.

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

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

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

Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [i.4] (Regulation (EU) No 910/2014, or Regulation hereinafter) provides a legal framework to facilitate cross-border recognition between existing national legal systems related to electronic registered delivery services. That framework aims to open new market opportunities for European Union trust service providers to offer new pan-European electronic registered delivery services. The Regulation defines the so-called qualified electronic registered delivery service (QERDS hereinafter), which is a special type of ERDS, where both the service and its provider need to meet a number of additional requirements that the regular ERDSs and their providers do not need to meet.

The framework of ERDS standards aims to cover the common and worldwide-recognized requirements to address electronic registered delivery in a secure and reliable way, independent of the applicable legislative framework. The documents contain generic requirements which can be applied in any geographic region. At the same time, the framework of ERDS standards aims to support demonstrating compliance to the Regulation (EU) No 910/2014 [i.4] (and related secondary legislation), both for non-qualified and qualified electronic registered delivery services. Specific clauses are included defining requirements for qualified services only, especially in the documents covering policy and security requirements. However, the legal effects of services implemented according to the framework of ERDS standards are outside the scope of the documents [i.16] to [i.21].

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

1 Scope

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

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

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at <https://docbox.etsi.org/Reference/>.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are necessary for the application of the present document.

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

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

- [i.1] ETSI EN 319 532-2: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) Services; Part 2: Semantic Contents".
- [i.2] ETSI EN 319 532-3: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) Services; Part 3: Formats".
- [i.3] ETSI EN 319 532-4: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) Services; Part 4: Interoperability profiles".
- [i.4] Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.
- [i.5] ETSI EN 319 522-2: "Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 2: Semantic Contents".
- [i.6] ETSI TS 119 612: "Electronic Signatures and Infrastructures (ESI); Trusted Lists".
- [i.7] IETF RFC 5751: "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification".

- [i.8] IETF RFC 5321: "Simple Mail Transfer Protocol".
- [i.9] IETF RFC 1939: "Post Office Protocol - Version 3".
- [i.10] IETF RFC 3501: "Internet Message Access Protocol - Version 4rev1".
- [i.11] IETF RFC 5246: "The Transport Layer Security (TLS) Protocol Version 1.2".
- [i.12] IETF RFC 4422: "Simple Authentication and Security Layer (SASL)".
- [i.13] IETF RFC 3207: "SMTP Service Extension for Secure SMTP over Transport Layer Security".
- [i.14] IETF RFC 2595: "Using TLS with IMAP, POP3 and ACAP".
- [i.15] IETF RFC 7817: "Updated Transport Layer Security (TLS) Server Identity Check Procedure for Email-Related Protocols".
- [i.16] ETSI EN 319 522 (all parts): "Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services".
- [i.17] ETSI EN 319 532 (all parts): "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) Services".
- [i.18] ETSI EN 319 521: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Electronic Registered Delivery Service Providers".
- [i.19] ETSI EN 319 531: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Registered Electronic Mail Service Providers".
- [i.20] ETSI TS 119 524 (all parts): "Electronic Signatures and Infrastructures (ESI); Testing Conformance and Interoperability of Electronic Registered Delivery Services".
- [i.21] ETSI TS 119 534 (all parts): "Electronic Signatures and Infrastructures (ESI); Testing Conformance and Interoperability of Registered Electronic Mail Services".

3 Definitions and abbreviations

3.1 Definitions

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

ERDS serviceinfo: ERD message which contains some ERDS relay metadata

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

original message: data including user content and submission metadata

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3.2 Abbreviations

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

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

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

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

4 REM logical model

4.1 Introduction

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

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

4.2 Black-box model

4.2.1 Functional viewpoint

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

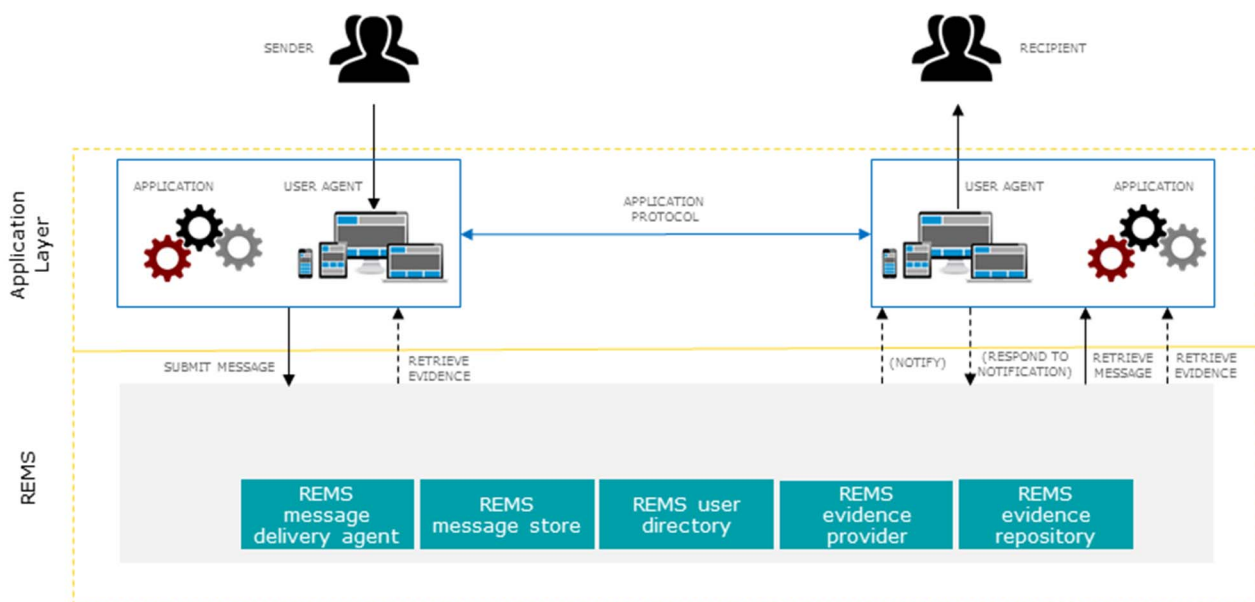


Figure 1: Black-box REM model

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

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

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

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

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

Table 1: Mapping of REMS components and ERDS components

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

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. In addition, the REMS **may** include the REMS evidence repository and the REMS user directory.

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 acceptance by the recipient 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 ERDS shall require the recipient to actively respond to the ERDS before consignment, and shall consign the user content only if the response was positive.
- Acceptance is not required: in this case the ERDS may perform the consignment of the user content without waiting for any action of the recipient.

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 shall be 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 shall be conveyed to the ERD-UA of the recipient, and the complete user content itself shall be forwarded or downloaded only upon a request of the recipient.

EXAMPLE 3: Sending a link (URL) to a document stored on an online server in the body of an HTTP POST request.

EXAMPLE 4: 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 shall be conveyed to the recipient by value, and acceptance shall not be required. 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 shall be required from the recipient to access the user content besides identification and authentication.

EXAMPLE 5: This is typically performed by storing the user content in the recipient's mailbox.

In **S&N style** the user content provided by the sender shall be conveyed to the recipient by reference first, and acceptance shall be required. Acceptance may be implicit (e.g. downloading a document can imply accepting it). If the recipient accepts the message, then the user content shall be consigned (made available to the recipient).

EXAMPLE 6: 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.

A REMS **shall** support S&F style of operation. A REMS **may** support S&N style of operation.

4.2.2.2 REM Store and Forward style of operation

A typical sequence of actions in S&F style of operation is depicted in figure 2, and detailed below. For simplicity, failure cases are not considered in this sequence. (Success and failure cases are specified in the event types and possible reasons, see clause 6 below and ETSI EN 319 522-2 [i.5], clause 8.3.3.)

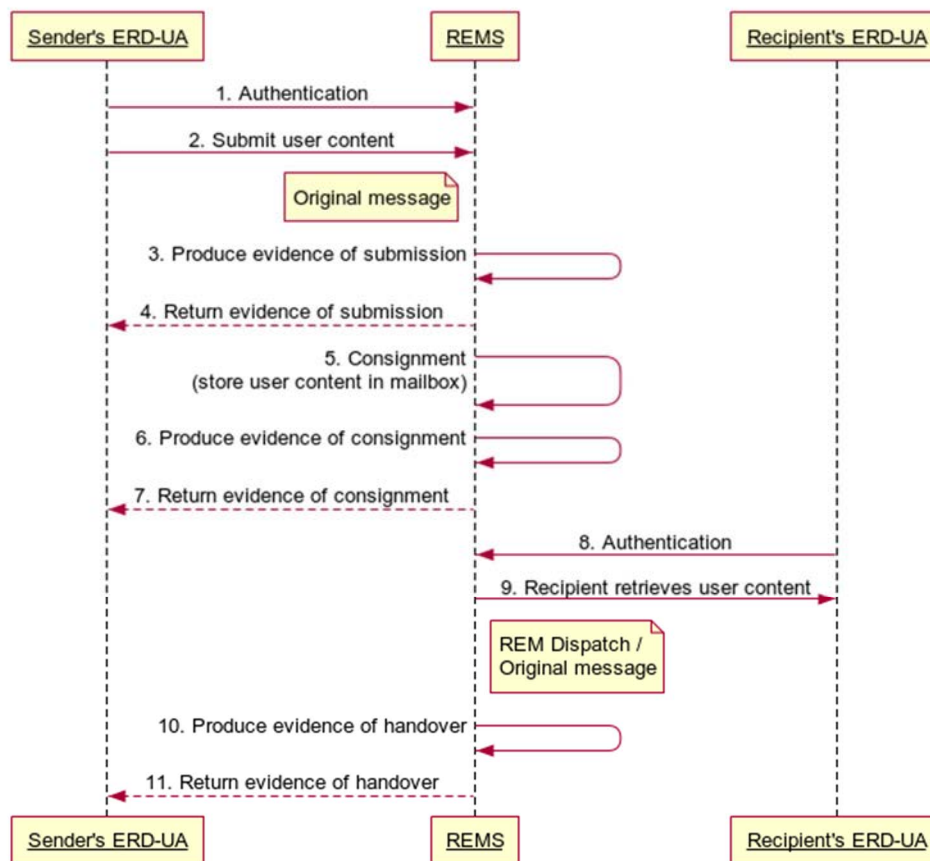


Figure 2: REM Store and Forward sequence of actions

1. The sender (either a user or a system) 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 can 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 and authenticate the sender).
3. The REM service tracks the event that the user content has been submitted. This is done producing an "attestation of submission" (ERDS evidence of submission), e.g. a signed file containing the basic information of the event.
4. The ERDS 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 can also store additional related information (metadata, e.g. sender's identity, submission time, etc.) and ERDS evidence (e.g. submission evidence produced in step 3) along with the user content. These can be enveloped together in one single bundle, called a REM dispatch, or can 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 (ERDS evidence of consignment).
7. The ERDS evidence of consignment can optionally be sent back to the sender. See note below.
8. The recipient (either a user or a system) 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 can also retrieve metadata and/or ERDS 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 (ERDS evidence of handover).
11. The ERDS evidence of handover can optionally be sent back to the sender. See note below.

NOTE: In steps 4, 7 and 11 sending the ERDS evidence right after its generation to the user is only one of the possible ways of providing the ERDS evidence, and there are other alternatives as well, e.g. the ERDS 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

A typical sequence of actions in S&N style of operation is depicted in figure 3, and detailed below. For simplicity, failure cases are not considered in this sequence. (Success and failure cases are specified in the event types and possible reasons, see clause 6 below and ETSI EN 319 522-2 [i.5], clause 8.3.3.)

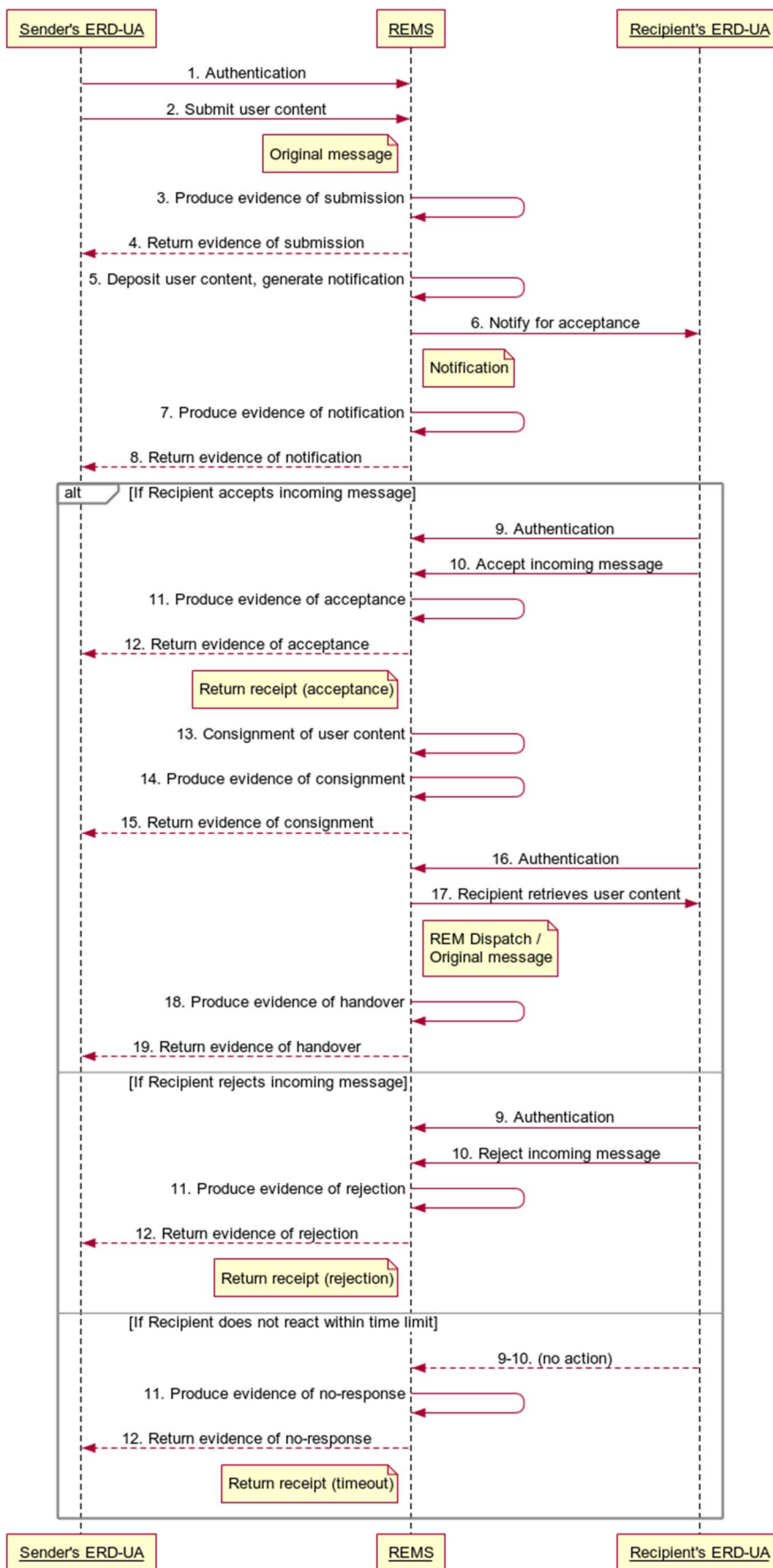


Figure 3: REM Store and Notify sequence of actions

1. The sender (either a user or a system) 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 can 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 and authenticate the sender).
3. The REM service tracks the event that the user content has been submitted. This is done producing an "attestation of submission" (ERDS evidence of submission), e.g. a signed file containing the basic information of the event.
4. The ERDS evidence of submission can optionally be sent back to the sender. See note 2 below.
5. The REM service stores the user content (and optionally metadata and/or ERDS 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 can 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 can produce a corresponding attestation (ERDS evidence of notification).
8. The ERDS evidence of notification can 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 can 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 separately.

Alternative 1: if the recipient accepts the message:

9. The recipient (either a user or a system) authenticates herself to the REMS.
10. The recipient performs an 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 (ERDS evidence of acceptance).
12. The ERDS evidence of acceptance, optionally along with additional data (e.g. acknowledgment of receipt signed by the recipient), can be sent back to the sender. See note 2 below.
13. The REM service stores the user content in the recipient's mailbox. It can also store additional related information (metadata, e.g. sender's identity, submission time, etc.) and ERDS evidence (e.g. ERDS evidence produced in step 3, step 7, step 10 or step 11) along with the user content. These can be enveloped together in one single bundle, called a REM dispatch, or can also be stored separately.

Alternatively, the user content (and any accompanying metadata) can 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 (ERDS evidence of consignment).
15. The ERDS evidence of consignment can be sent back to the sender. See note 2 below.
16. The recipient (either a user or a system) 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 can also retrieve metadata and/or ERDS 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 (ERDS evidence of handover).
19. The ERDS evidence of handover can 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) authenticates herself to the REMS.
10. The recipient performs an 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 (ERDS evidence of rejection).
12. The ERDS evidence of rejection, optionally along with additional data, can be sent back to the sender. See note 2 below.

Alternative 3: if the recipient does not respond within a predetermined time limit (see note 1 below):

- 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 (ERDS evidence of no-response).
12. The ERDS evidence of no-response, optionally along with additional data, can 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 and 19 sending the ERDS evidence right after its generation to the user is only one of the possible ways of providing the ERDS evidence, and there are other alternatives as well, e.g. the ERDS 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 clause 4.4.

The interaction of the individual services of the REMSPs ensures the end-to-end user content delivery and evidence provision. The interface between the users of the services 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 4.

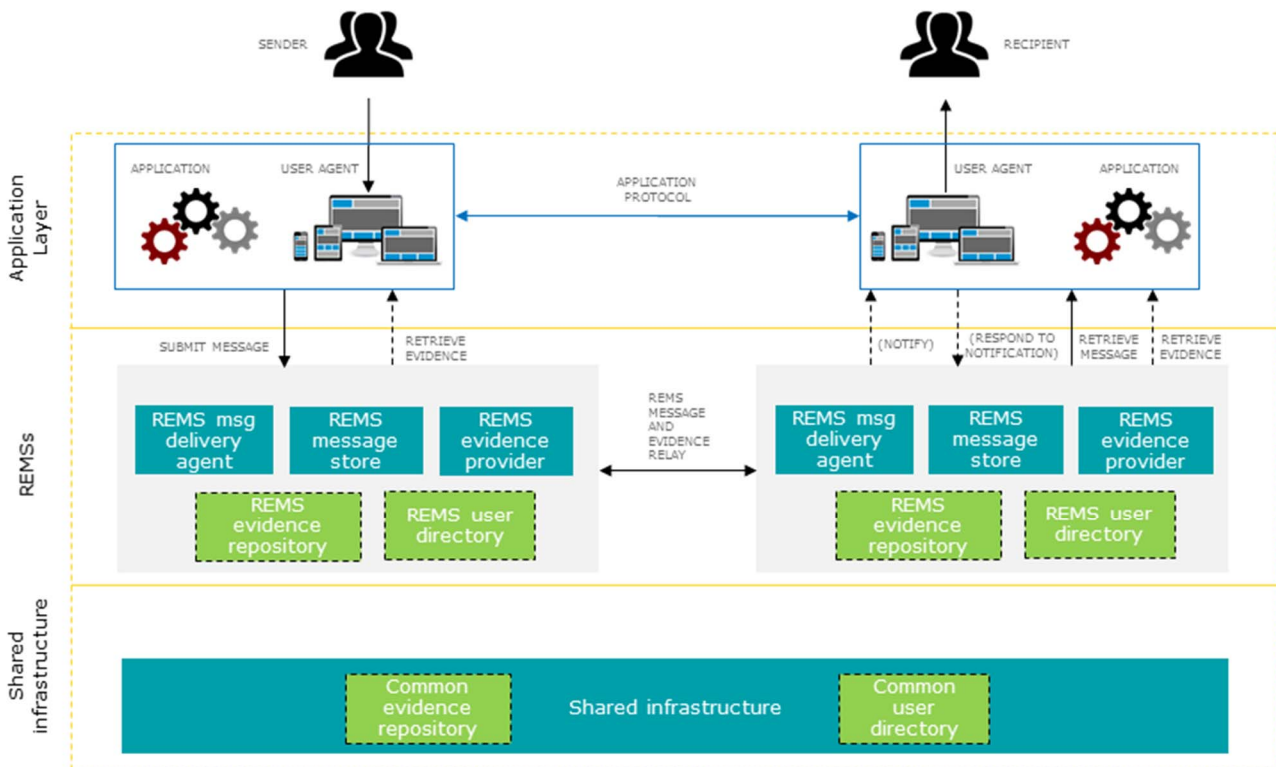


Figure 4: 4-corner REM model

Similarly to interconnected ERDSs in general, a shared infrastructure can assist the communication of interconnected REMSs. This is an abstract entity, which can consist of multiple distinct actors in reality. This can 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 [1].

In REM, as required by clause 5 of ETSI EN 319 532-3 [i.2], the identifier of a user is 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 figure 4, is not necessary.

REMSs operating in different styles of operation may 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. R-REMS shall recognize if the incoming message is a notification, and in that case it shall act in S&F style, i.e. it shall process the notification and notify the recipient, and shall not generate another notification with a reference to the first notification. 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.

A typical sequence of actions in S&F to S&F interaction is depicted in figure 5, and detailed below. For simplicity, failure cases are not considered in this sequence. (Success and failure cases are specified in the event types and possible reasons, see clause 6 below and ETSI EN 319 522-2 [1.5], clause 8.3.3.) The REMSs can track each relevant event in the sequence by producing a corresponding ERDS 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 5. The produced evidence can also be sent to the user, or can 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 5.

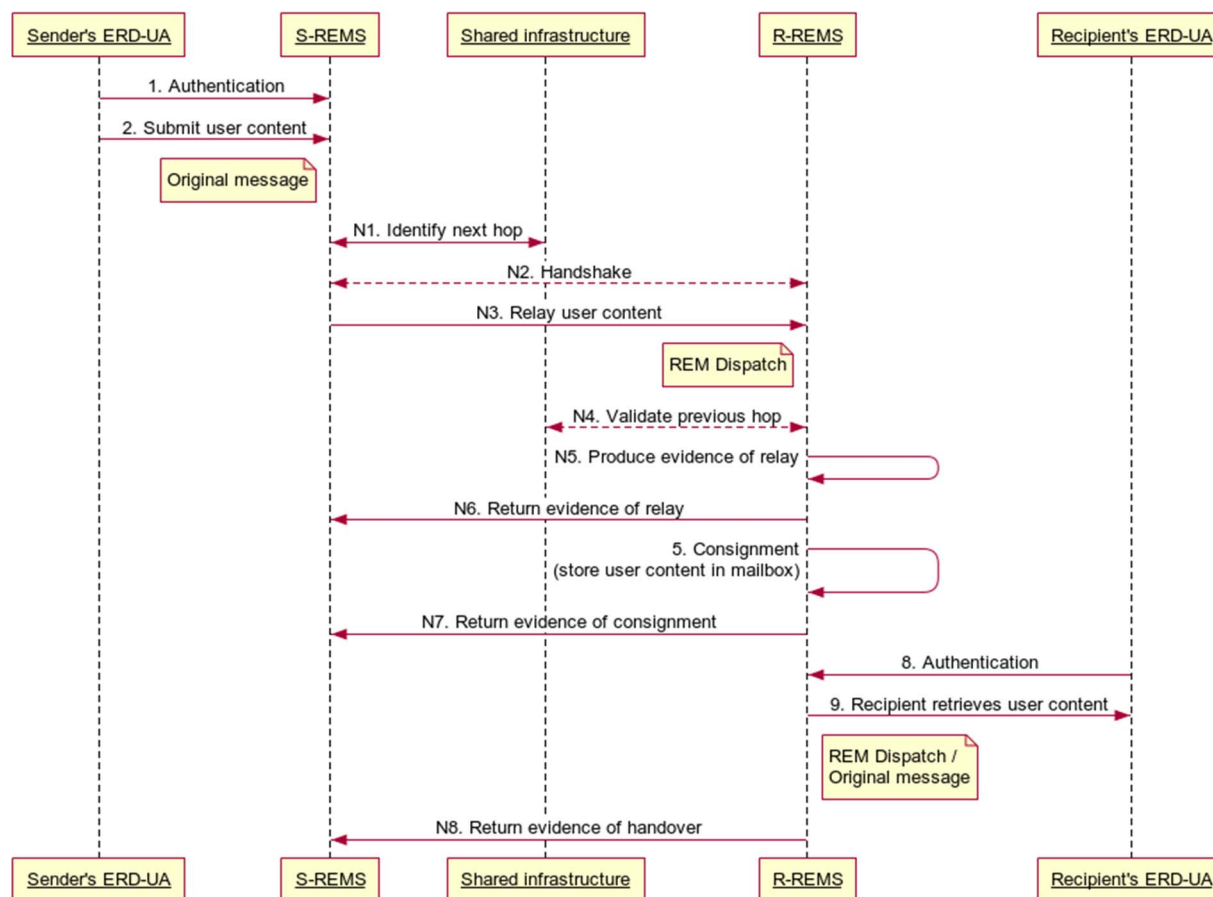


Figure 5: 4-corner S&F to S&F sequence

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 users are kept the same as in figure 2. The new actions depicted in figure 5 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 can correspond to several distinct actors. This step can involve multiple actions:

- S-REMS needs to determine the recipient's REMS. This can 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 can be possible using DNS lookups, as it is done in the case of regular email messages, or using other techniques. 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 can be done, for instance, using Trusted Lists, as defined in ETSI TS 119 612 [i.6].
- N2. The REMS performs a handshake with the next-hop REMS. This can include negotiation on different aspects (capabilities, supported style of operation, ERDS evidence, level of authentication of end entities, fees, etc.). Handshake can be omitted 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 can also relay additional related information (metadata, e.g. sender's identity, submission time, etc.) and ERDS evidence (e.g. ERDS evidence of submission produced in step 3) along with it.
- N4. The REMS that received the relayed REM message can 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 ERDS 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 might also need this attestation.
7. The ERDS evidence of consignment can 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 ERDS 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 ERDS 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.

A typical sequence of actions in S&F to S&N interaction is depicted in figure 6, and detailed below. For simplicity, failure cases are not considered in this sequence. (Success and failure cases are specified in the event types and possible reasons, see clause 6 below and ETSI EN 319 522-2 [i.5] clause 8.3.3.) The REMSs can track each relevant event in the sequence by producing a corresponding ERDS 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 6. 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 6.

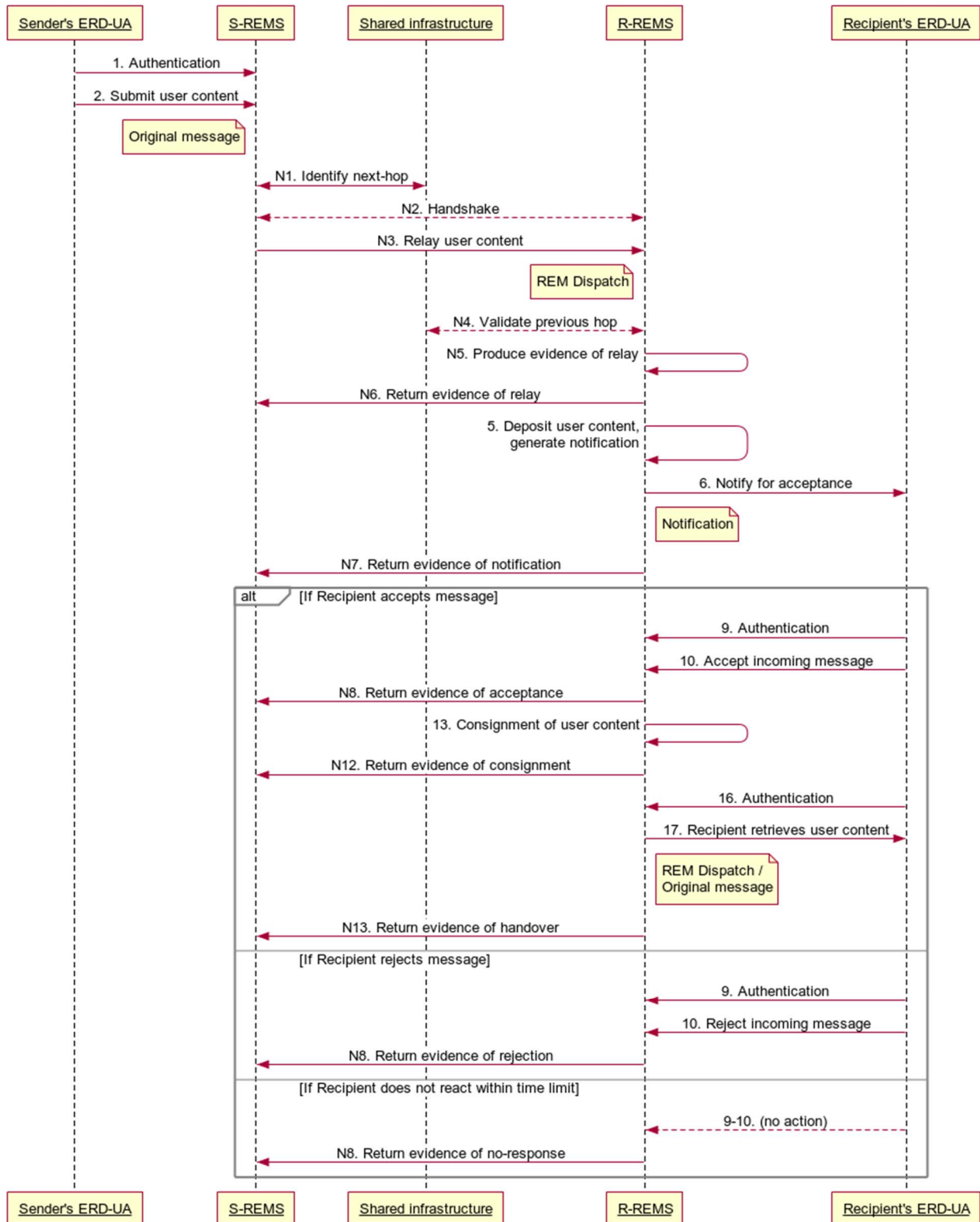


Figure 6: 4-corner S&F to S&N sequence

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 users 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.

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. The evidence produced in step N5. is an ERDS evidence.)

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

N7. The ERDS 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 ERDS evidence of notification can 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.

N8. The ERDS 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 ERDS evidence of acceptance/rejection/no-response can 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 ERDS 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 might also need this attestation.

15. The ERDS evidence of consignment can 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 ERDS 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 ERDS evidence of handover can 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 can 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.

A typical 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 7, and detailed below. For simplicity, failure cases are not considered in this sequence. (Success and failure cases are specified in the event types and possible reasons, see clause 6 below and ETSI EN 319 522-2 [i.5], clause 8.3.3.) The REMSs can track each relevant event in the sequence by producing a corresponding ERDS 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 7. 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 7.

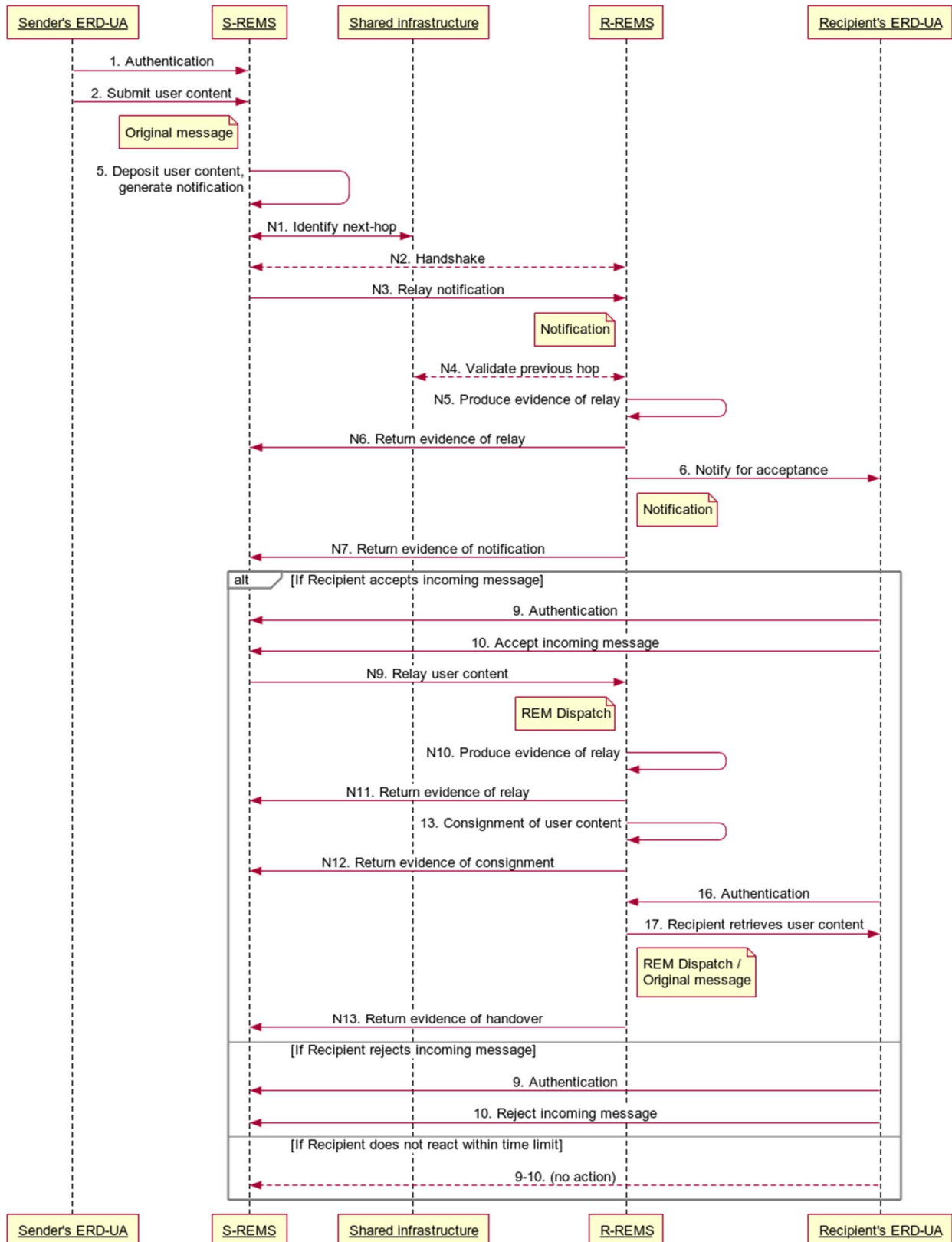


Figure 7: 4-corner S&N to S&F sequence

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 users are kept the same as in figure 3. The new actions depicted in figure 7 are the communication steps between the REMs, 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.
5. 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. The evidence produced in step N5. is typically not an ERDS evidence, as this relay operation does not involve the user content. Still, S-REMS typically needs some kind of authentic response whether the relay was successful or not.)
- 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 ERDS 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 ERDS evidence of notification can 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 can 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 can also relay additional related information (metadata, e.g. sender's identity, submission time, etc.) and ERDS evidence (e.g. ERDS evidence of submission produced in step 3) along with it. The REMS can also hand over the user content directly to the recipient. (This is not shown in figure 7.)
- 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 ERDS evidence of relay.
- N11. The ERDS 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 ERDS 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 might also need this attestation.
15. The ERDS evidence of consignment can 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 ERDS 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 ERDS evidence of handover can 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 8. The interaction of the individual services of the REMSPs ensures the end-to-end user content delivery and evidence provision. The interface between the users of the services 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.

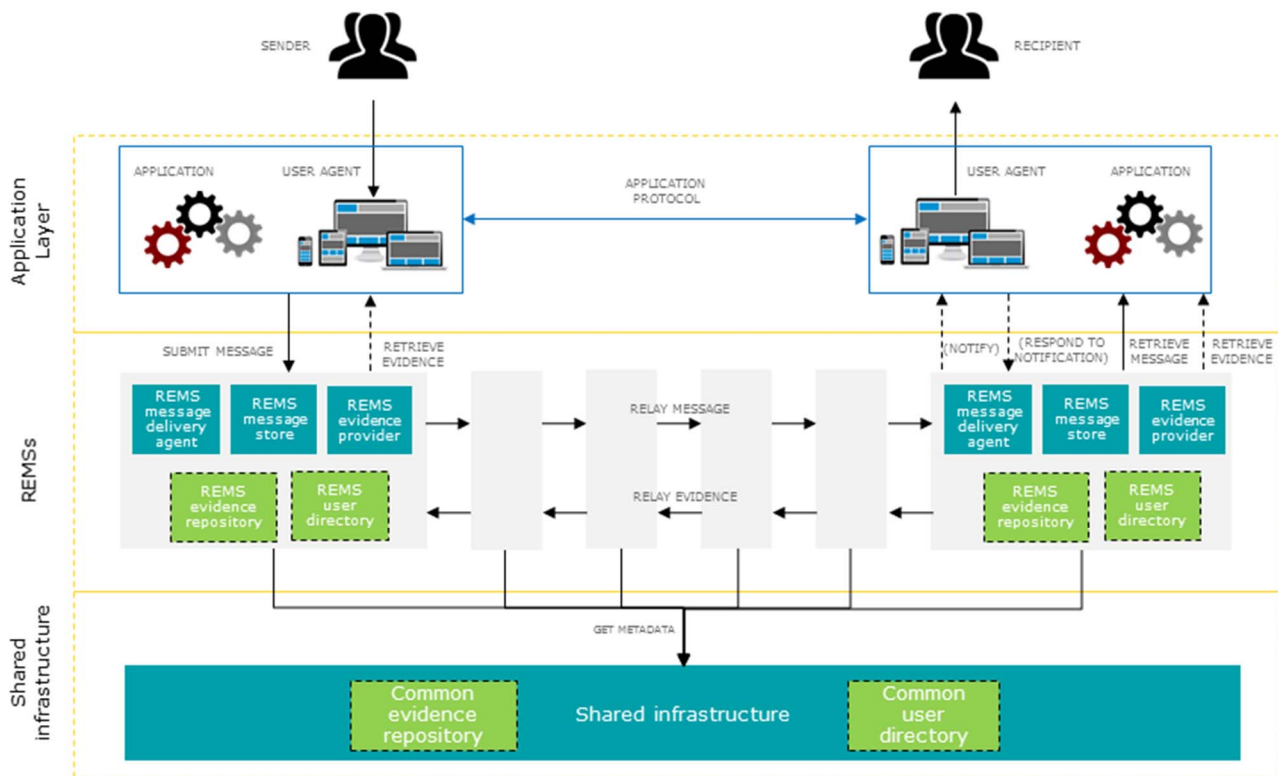


Figure 8: Extended REM model

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 [i.1] and part 3 [i.2] of the present multi-part 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 can assist the communication of interconnected REMSs. This is an abstract entity, which can consist of multiple distinct actors in reality. In a multi-ERDS delivery scenario, some components which are normally implemented by an ERDS (dotted boxes in figure 8) can 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 may act effectively according to the S&N style, since the notification shall always be 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 ERDS 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 ERDS evidence.

As an example, the complete flow of communications involving 3 REMSs, each operating in S&F style, is depicted in figure 9. For simplicity, failure cases are not considered in this sequence. (Success and failure cases are specified in the event types and possible reasons, see clause 6 below and ETSI EN 319 522-2 [i.5], clause 8.3.3.) The REMSs can track each relevant event in the sequence by producing a corresponding ERDS evidence, as detailed in clause 4.2.2.2, but for an easier overview, the production of these evidences is not shown in figure 9. The produced evidence can also be sent to the user, or can be provided in other ways, as described in clause 4.2.2.2. The optional returning of evidence to users is not shown in figure 9.

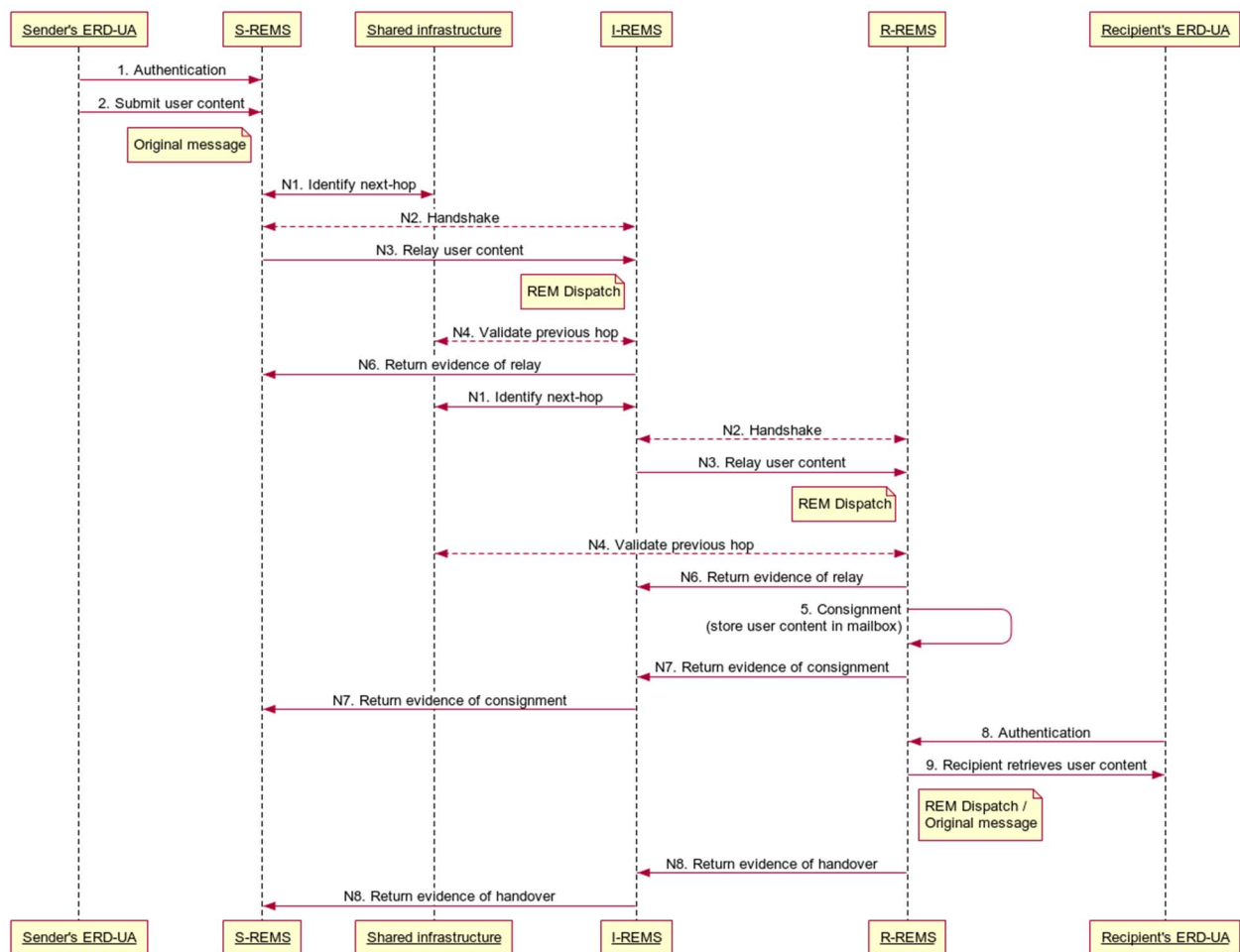


Figure 9: Extended S&F to S&F to S&F sequence

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 ERDS 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 ERDS evidence.

As an example, the complete flow of communications involving 3 REMSs, the middle one operating in S&N style, is depicted in figure 10. For simplicity, failure cases are not considered in this sequence. (Success and failure cases are specified in the event types and possible reasons, see clause 6 below and ETSI EN 319 522-2 [i.5], clause 8.3.3.) The S&N REMS can also hand over the user content directly to the recipient, but this is not shown in figure 10. The REMSs can track each relevant event in the sequence by producing a corresponding ERDS evidence, as detailed in clause 4.2.2.3, but for an easier overview, the production of these evidences is not shown in figure 10. The produced evidence can also be sent to the user, or can be provided in other ways, as described in clause 4.2.2.3. The optional returning of evidence to users is not shown in figure 10.

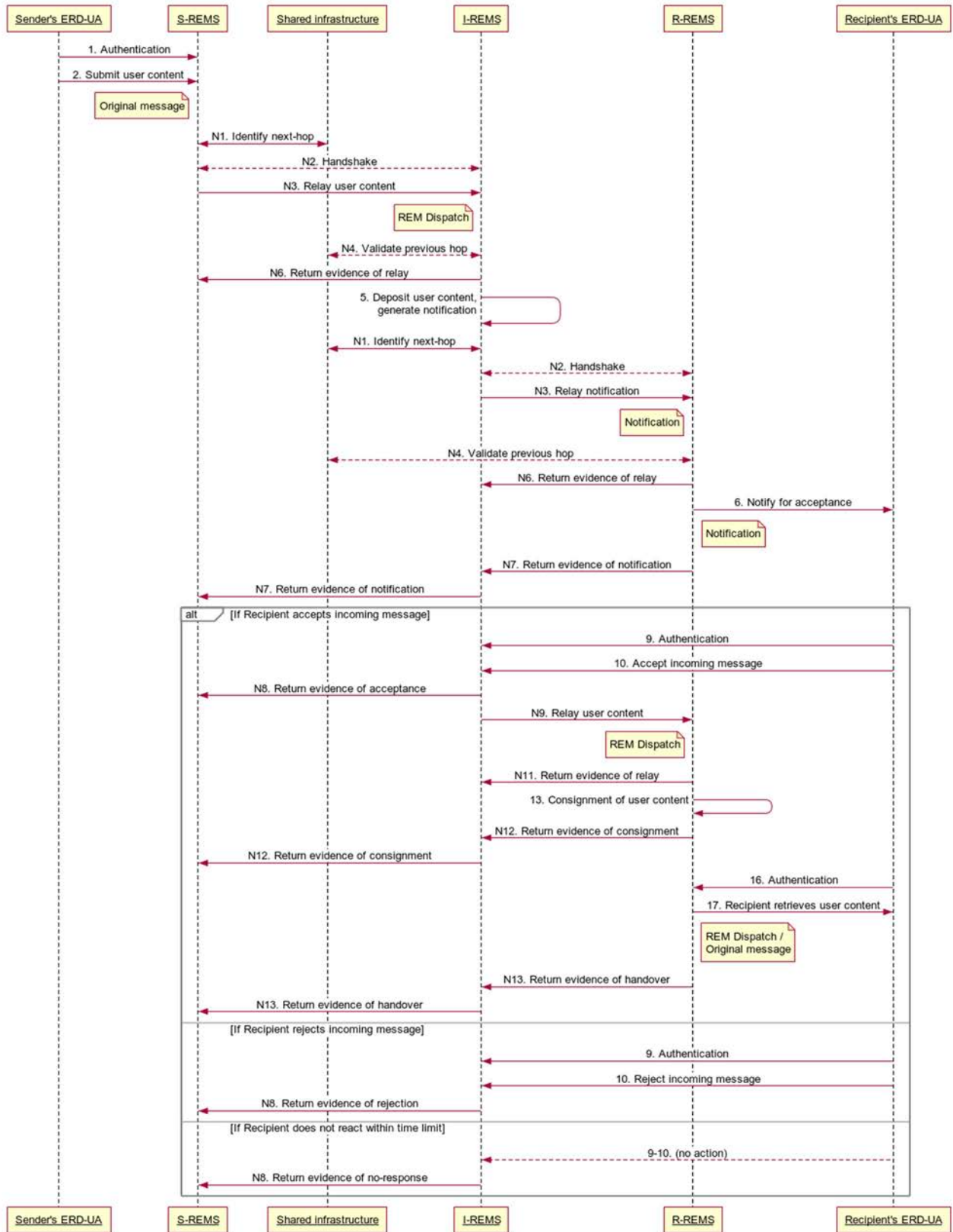


Figure 10: Extended S&F to S&N to S&F sequence

5 REM interfaces

Since REMS is a specific type of ERDS, the ERD interfaces described in clause 5 of ETSI EN 319 522-1 [1] 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 11 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.

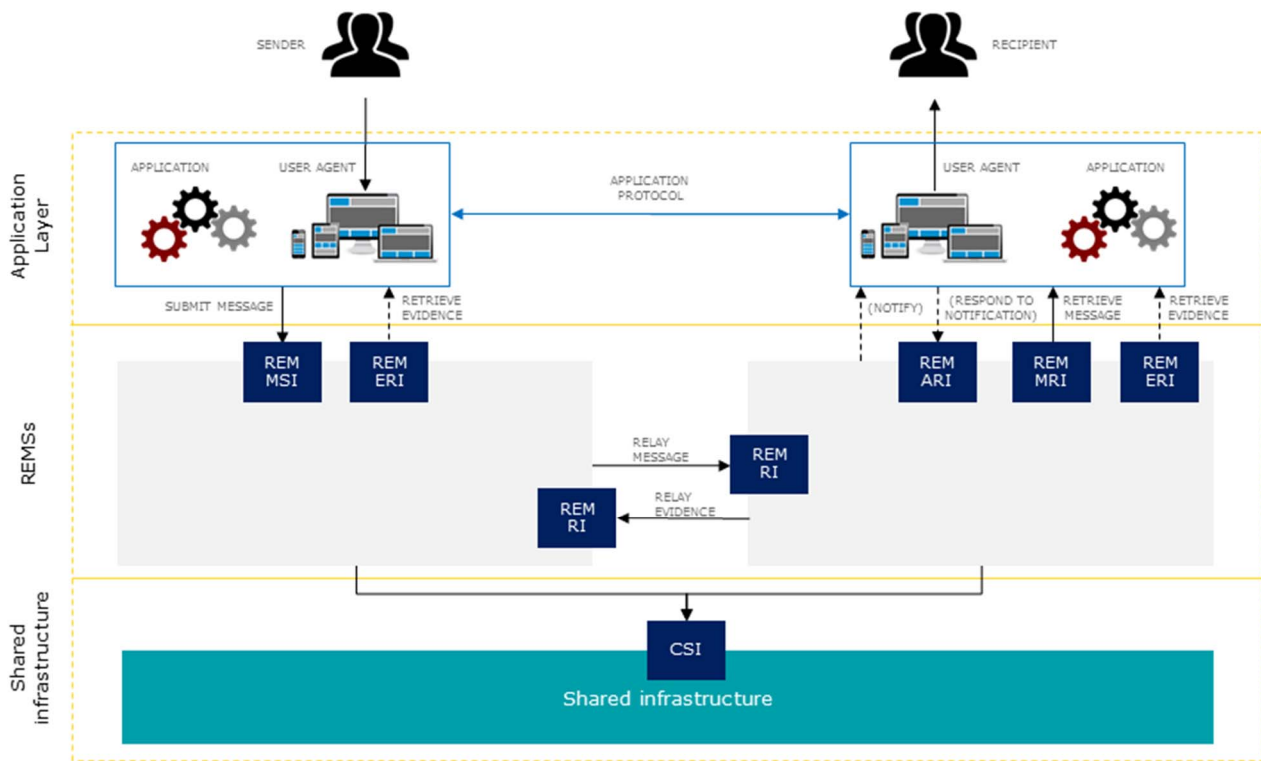


Figure 11: Interfaces of REMS

Table 2: Requirements for REM interfaces

Name of interface	Corresponding ERDS interface in ETSI ETSI EN 319 522-1 [1]	Additional specific requirements for REM
REM MSI (Message Submission Interface)	ERDS MSI (Message Submission Interface): this interface is used by the sender's ERD-UA to submit original messages 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. through a token from a third party). This interface shall implement confidentiality and integrity preserving measures.	<p>The REM MSI shall be provided.</p> <p>Requirements on ERDS MSI shall apply to REM MSI.</p> <p>The REM MSI should be provided using SMTP [i.8] over TLS [i.11]. See also [i.13], [i.14] and [i.15]. 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 creates such a secure channel.</p> <p>See note 1.</p>

Name of interface	Corresponding ERDS interface in ETSI ETSI EN 319 522-1 [1]	Additional specific requirements for REM
REM MRI (Message Retrieval Interface)	ERDS MERI (Message and Evidence Retrieval Interface): this interface is used by the ERD-UA to retrieve user content, handover metadata and associated evidence (pull mode). This interface shall require identification and authentication, either direct (e.g. through credential check) or indirect (e.g. through a token from a third party). This interface shall implement confidentiality and integrity preserving measures.	The REM MRI shall be provided. Requirements on ERDS MERI shall apply to REM MRI. The REM MRI should be provided using IMAP [i.10] over TLS or POP3 [i.9] 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 creates such a secure channel. See note 2.
REM ERI (Evidence Retrieval Interface)	This interface shall implement confidentiality and integrity preserving measures.	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. See note 2.
REM RI (Relay Interface)	ERDS RI (Relay Interface): this interface allows ERD messages to be relayed between ERDS. This interface shall implement authentication, confidentiality and integrity preserving measures.	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 creates such a secure channel. Implementation of this interface should follow the requirements defined in clause 5 of ETSI EN 319 532-4 [i.3]. A REMS may provide more than one REM RI. The REM RI may be provided using other protocols. See note 3.
REM ARI (Acceptance/Rejection Interface)	This interface can be provided by non-REM ERDS as well, but it is not specified in ETSI ETSI EN 319 522-1 [1].	This interface is used by the recipient to respond to a notification and signal the acceptance or rejection of the incoming message. The REM ARI shall be provided when the REMS operates in S&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.
-	ERD-UA MEPI (Message and Evidence Push Interface)	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.
CSI (Common Service Interface)	CSI (Common Service Interface): this interface gives access to message routing functions, trust management functions, capability management functions, governance functions.	An 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.).
<p>NOTE 1: Authentication in the REM MSI may rely on the features provided by SASL [i.12], TLS (e.g. certificate-based authentication), S/MIME [i.7] digital signature over the submitted message, or other mechanisms.</p> <p>NOTE 2: Authentication in the REM MRI and REM ERI may rely on the features provided by SASL [i.12], TLS (e.g. certificate-based authentication), or other mechanisms.</p> <p>NOTE 3: Providing a REM RI using other protocols can be useful when the REMS communicates with other non-REM ERDSs.</p>		

NOTE 1: The REM MSI, REM MRI, REM ERI and REM RI interfaces are required to implement confidentiality preserving measures. Independently, the sender can ensure the confidentiality of the user content by applying end-to-end encryption before submission. In this case the confidentiality of the user content would have additional protection even outside the secure channels of these interfaces, and even REMSPs would not be able to read the user content.

NOTE 2: The REMS will authenticate the sender and provide ERDS evidence associated to the authenticated user about the relevant ERD events. Independently, the sender can ensure the integrity and authenticity of the user content by applying a digital signature to it before submission. In this case the digital signature of the sender becomes part of the user content, and can give assurance to the recipient(s) in addition to that provided by the ERDS evidence.

6 REM events and evidence

6.1 Overview

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

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

The requirements on the production of ERDS 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 ERDS 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 **REM MSI (Message Submission Interface)** of the REMS. The transaction involves 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 **REM MSI** 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 can validate the digital signature - if any - over the message, can verify that headers of the message correspond to the authenticated user, can 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 3: Events related to the submission

Event type in ETSI EN 319 522-1 [1]	Related interface	Issuing REMS	Interpretation
A.1. SubmissionAcceptance	REM MSI	S-REMS	The REMS has accepted the submitted original message, and the REMSP takes responsibility for trying to deliver it to all specified recipients respecting the policy rules and all delivery options given by the sender.
A.2. SubmissionRejection	REM MSI	S-REMS	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 [i.5], clause 8.3.3 about possible reasons.

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 ERDS evidence corresponding to the events described in this clause.

Relay is the handing over of a REM message containing user content 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 can verify trust in the sending REMS, check the compliance of the REM message with policy rules, etc.). The receiving REMS shall issue ERDS evidence about its decision over the relayed user content, and shall convey this ERDS 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 ERDS evidence about the failure of the relay.

The REMS shall issue the above mentioned ERDS evidences about the relay of each user content (regardless of whether it is enveloped in a REM dispatch or not) under its responsibility regardless of whether it is the sender's REMS or an intermediary REMS.

The REMS need not issue ERDS evidence about the relay of REM messages which do not contain user content (but may log them for instance).

Table 4: Events related to relay between REMSs

Event type in ETSI EN 319 522-1 [1]	Related interface	Issuing REMS	Interpretation
B.1. RelayAcceptance	REM RI	Receiving REMS	The receiving REMS has accepted the relayed REM message containing user content, and the REMSP takes responsibility for handling it according to the requirements in the present document and the policy rules.
B.2. RelayRejection	REM RI	Receiving REMS	The receiving REMS has rejected the relayed REM message containing user content. The receiving REMS shall inform the sending REMS about the reason(s) for the rejection. See ETSI EN 319 522-2 [i.5], clause 8.3.3 about possible reasons.
B.3. RelayFailure	REM RI	Sending REMS	The sending REMS was unable to relay the REM message containing user content to the receiving REMS within a given time period, or the receiving REMS did not return ERDS evidence about the acceptance or rejection of the REM message within that time period.

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 ERDS 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 ERDS evidence about exactly one of the events regarding the response of each of the recipients (C.3, C.4, C.5 in table 5) for each user content.

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 ERDS evidence about the successful or unsuccessful notification of the recipient (C.1, C.2 in table 5).

Table 5: Events related to the acceptance/rejection by the recipient

Event type in ETSI EN 319 522-1 [1]	Related interface	Issuing REMS	Interpretation
C.1. NotificationForAcceptance	n/a	R-REMS	R-REMS has notified the recipient about the availability of a message at the notifying REMS.
C.2. NotificationForAcceptanceFailure	n/a	R-REMS	R-REMS could not notify the recipient about the availability of a message at the notifying REMS within a given time period.
C.3. ConsignmentAcceptance	REM ARI	Notifying REMS	The recipient, upon proper authentication, has performed an action by which she indicated that she accepts the message to be delivered.
C.4. ConsignmentRejection	REM ARI	Notifying REMS	The recipient, upon proper authentication, has performed an action by which she indicated that she rejects the message to be delivered.
C.5. AcceptanceRejectionExpiry	REM ARI	Notifying REMS	The predetermined time period for acceptance/rejection has elapsed without any response from 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 authentication. Consignment is considered to be performed internally by the REMS, not through any outer interfaces. R-REMS **shall** issue ERDS evidence about the successful or unsuccessful consignment of each user content, regardless of whether it is consigned inside a REM dispatch or separately. If the user content was relayed by another REMS then the R-REMS shall make the ERDS evidence of successful or unsuccessful consignment available to the relaying REMS.

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

When the REMS relays a user content to another REMS, it shall monitor whether the other REMS provides ERDS evidence of the successful or unsuccessful consignment of the user content within a given time period. If the other REMS does not provide such ERDS evidence within this time period then the REMS **shall** issue ERDS evidence about the failure of consignment, indicating the time period. If the user content was relayed by another REMS then the REMS shall make this evidence available to the relaying REMS.

NOTE: The time period available for the confirmation of successful or unsuccessful consignment 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 the REMS.

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 ERDS evidence about the successful or unsuccessful notification of the recipient about the consigned user content.

Table 6: Events related to the consignment

Event type in ETSI EN 319 522-1 [1]	Related interface	Issuing REMS	Interpretation
D.1. ContentConsignment	n/a	R-REMS	R-REMS has made the user content available to the recipient.
D.2. ContentConsignmentFailure	n/a	R-REMS	The REMS could not make the user content available to the recipient within a given time period, or the REMS did not receive ERDS evidence within a given time period about the successful or unsuccessful consignment of the user content from the other REMS to which it had relayed the user content.
D.3. ConsignmentNotification	n/a	R-REMS	R-REMS has notified the recipient about the consigned user content.
D.4. ConsignmentNotificationFailure	n/a	R-REMS	R-REMS could not notify the recipient about the consigned user content within a given time period.

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 ERDS evidence may also be handed over along with the user content (either enveloped in a REM dispatch, or separately).

NOTE 1: 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 2: Historically, download of the message was defined to be a separate event from retrieval of the message. The present document considers those two cases as one, consequently there is no separate download event defined.

The REMS **may** issue ERDS evidence about the successful or unsuccessful handover.

Table 7: Events related to the handover to the recipient

Event type in ETSI EN 319 522-1 [1]	Related interface	Issuing REMS	Interpretation
E.1. ContentHandover	REM MRI	R-REMS	The user content has successfully passed through the REM MRI from the REMS to the client under the responsibility of the recipient.
E.2. ContentHandoverFailure	REM MRI	R-REMS	The user content did not pass through the REM MRI within a given time period.

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

The REMS may support 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 REMS supports this feature, it should issue ERDS evidence corresponding to the events described in this clause.

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

Event type in ETSI EN 319 522-1 [1]	Related interface	Issuing REMS	Interpretation
F.1. RelayToNonERDS	n/a	Relaying REMS	The REMS has successfully relayed the user content to the given non-ERDS system.
F.2. RelayToNonERDSFailure	n/a	Relaying REMS	The REMS was unable to relay the user content to the non-ERDS system within a given time period.
F.3. ReceivedFromNonERDS	n/a	Receiving REMS	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.

History

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