



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](https://docbox.etsi.org/ESI/Open/Latest%20Drafts/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>

0
1

Reference

DEN/ESI-0019532-1

Keywords

<keywords>

2

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 noticeThe present document can be downloaded from:
<http://www.etsi.org/standards-search>

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

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
<https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx>

If you find errors in the present document, please send your comment to one of the following services:
<https://portal.etsi.org/People/CommiteeSupportStaff.aspx>

Copyright Notification

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.

© European Telecommunications Standards Institute 2017.
All rights reserved.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.
3GPP™ and **LTE™** are Trade Marks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.
GSM® and the GSM logo are Trade Marks registered and owned by the GSM Association.

4	Contents	
5	Intellectual Property Rights	5
6	Foreword.....	5
7	Modal verbs terminology	5
8	Introduction	5
9	1 Scope	6
10	2 References	6
11	2.1 Normative references	6
12	2.2 Informative references	6
13	3 Definitions and abbreviations.....	7
14	3.1 Definitions	7
15	3.2 Abbreviations.....	8
16	4 REM logical model	9
17	4.1 Introduction.....	9
18	4.1.1 Services and providers related to ERD.....	9
19	4.1.2 General description of REM service	11
20	4.2 Black-box model.....	11
21	4.2.1 Functional viewpoint.....	11
22	4.2.2 Sequence viewpoint.....	12
23	4.2.2.1 REM styles of operation	12
24	4.2.2.2 REM Store and Forward style of operation	13
25	4.2.2.3 REM Store and Notify style of operation	14
26	4.3 4-corner model.....	17
27	4.3.1 Functional viewpoint.....	17
28	4.3.2 Sequence viewpoint.....	18
29	4.3.2.1 REM S&F to S&F interaction	18
30	4.3.2.2 REM S&F to S&N interaction.....	20
31	4.3.2.3 REM S&N to S&F interaction.....	22
32	4.4 Extended model	24
33	4.4.1 Functional viewpoint.....	24
34	4.4.2 Sequence viewpoint.....	25
35	4.4.2.1 Multi-hop sequence over S&F nodes only	25
36	4.4.2.2 Multi-hop sequence involving a S&N node	26
37	4.5 Roles within a REMS	27
38	5 REM interfaces.....	28
39	6 REM events and evidence	30
40	6.1 Overview	30
41	6.2 Events and evidence.....	30
42	6.2.1 A. Events related to the submission	30
43	6.2.2 B. Events related to the relay between REMSs	30
44	6.2.3 C. Events related to the acceptance/rejection by the recipient	31
45	6.2.4 D. Events related to the consignment	32
46	6.2.5 E. Events related to the handover to the recipient	32
47	6.2.6 F. Events related to connections with non-ERDS systems.....	33
48	7 Shared infrastructure of REM	33
49		
50		

51 Intellectual Property Rights

52 IPRs essential or potentially essential to the present document may have been declared to ETSI. The information
 53 pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found
 54 in ETSI SR 000 314: "*Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in*
 55 *respect of ETSI standards*", which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web
 56 server (<https://ipr.etsi.org>).

57 Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee
 58 can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web
 59 server) which are, or may be, or may become, essential to the present document.

60 Foreword

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

64 The present document is part 1 of a multi-part deliverable covering Registered Electronic Mail (REM) Services, as
 65 identified below:

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

67 Part 2: "Semantic contents";

68 Part 3: "Formats";

69 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

70

71 Modal verbs terminology

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

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

76 Introduction

77 **EDITORIAL NOTE: introduction to be completed**

78

79 1 Scope

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

83 The present document is part 1 of a multi-part deliverable covering Registered Electronic Mail (REM) Services, as
84 identified below:

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

86 Part 2: "Semantic contents";

87 Part 3: "Formats";

88 Part 4: "Interoperability profiles";

89 The general concepts and requirements of electronic registered delivery are described ETSI EN 319 522 covering
90 Electronic Registered Delivery Services, which is also a multi-part deliverable. Since registered electronic mail is a
91 specific type of electronic registered delivery, the general provisions given in ETSI EN 319 522 apply to registered
92 electronic mail as well. Hence, parts 1, 2 and 3 of EN 319 532 are aligned with EN 319 522, and they reference the
93 necessary provisions of the corresponding part.

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

97 2 References

98 2.1 Normative references

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

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

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

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

107 [1] ETSI EN 319 522-1: "Electronic Signatures and Infrastructures (ESI); Electronic Registered
108 Delivery Services; Part 1: Framework and Architecture".

109 2.2 Informative references

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

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

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

117 [i.1] ETSI TR 119 001: "Electronic Signatures and Infrastructures (ESI); The framework for
118 standardization of signatures; Definitions and abbreviations"

119	[i.2]	ETSI EN 319 532-2: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) Services; Part 2: Semantic Contents"
120		
121	[i.3]	ETSI EN 319 532-3: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) Services; Part 3: Formats"
122		
123	[i.4]	ETSI EN 319 532-4: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) Services; Part 4: Interoperability profiles"
124		
125	[i.5]	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.
126		
127		
128	[i.6]	ETSI EN 319 522-2: "Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 2: Semantic Contents"
129		
130	[i.7]	ETSI TS 119 612: "Electronic Signatures and Infrastructures (ESI); Trusted Lists"
131	[i.8]	IETF RFC 5751: "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification".
132		
133	[i.9]	IETF RFC 5321: "Simple Mail Transfer Protocol"
134	[i.10]	IETF RFC 1939: "Post Office Protocol - Version 3"
135	[i.11]	IETF RFC 3501: "INTERNET MESSAGE ACCESS PROTOCOL - VERSION 4rev1"
136	[i.12]	IETF RFC 5246: "The Transport Layer Security (TLS) Protocol Version 1.2"
137	[i.13]	IETF RFC 4422: "Simple Authentication and Security Layer (SASL)"
138	[i.14]	IETF RFC 3207: "SMTP Service Extension for Secure SMTP over Transport Layer Security"
139	[i.15]	IETF RFC 2595: "Using TLS with IMAP, POP3 and ACAP"
140	[i.16]	IETF RFC 7817: "Updated Transport Layer Security (TLS) Server Identity Check Procedure for Email-Related Protocols"
141		

142 3 Definitions and abbreviations

143 3.1 Definitions

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

145 **electronic registered delivery service:** electronic service that makes it possible to transmit data between the sender and
 146 recipients by electronic means and provides evidence relating to the handling of the transmitted data, including proof of
 147 sending and receiving the data, and that protects transmitted data against the risk of loss, theft, damage or any
 148 unauthorised alterations

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

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

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

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

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

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

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

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

- 158 **submission metadata:** data submitted to the electronic registered delivery service together with the user content
- 159 **ERDS relay metadata:** data related to the user content which is generated by the electronic registered delivery service
160 for the purpose of relaying to another electronic registered delivery service
- 161 **ERDS handover metadata:** data related to the user content which is generated by the electronic registered delivery
162 service and handed over to the ERD user agent/application of the recipient
- 163 **original message:** data structure including the user content and the submission metadata
- 164 **recipient:** natural or legal person to which the user content is addressed
- 165 **sender:** natural or legal person that submits the user content
- 166 **ERDS evidence:** data generated within the electronic registered delivery service, which aims to prove that a certain
167 event has occurred at a certain time
- 168 **ERD event:** a relevant step in the electronic delivery process, which may be attested by an ERDS evidence
- 169 **ERD user agent/application:** system consisting of software and/or hardware components by which senders and
170 recipients participate in the exchange of data with electronic registered delivery service providers
- 171 **consignment:** the act of making the user content available to the recipient within the boundaries of the electronic
172 registered delivery service
- 173 **handover:** the act of having the user content successfully cross the border of the recipient's electronic registered
174 delivery service towards the recipient's ERD user agent/application
- 175 **EDITORIAL NOTE:** The following definitions of data structures have not yet been thoroughly discussed and are
176 subject to change.
- 177 **ERD message:** data structure generated by the electronic registered delivery service, which contains any of the user
178 content, ERDS relay metadata and/or ERDS evidence
- 179 **ERD dispatch:** ERD message which contains the user content, some ERDS relay metadata and ERDS evidence
- 180 **ERD payload:** ERD message which contains the user content and some ERDS relay metadata
- 181 **ERDS serviceinfo:** ERD message which contains some ERDS relay metadata
- 182 **ERDS receipt:** ERD message which contains ERDS evidence and some ERDS relay metadata
- 183 **REM envelope:** signed data structure generated by the registered electronic mail service provider which contains any of
184 the user content, ERDS relay metadata and/or ERDS evidence
- 185 **REM message:** ERD message in the form of a REM envelope
- 186 **REM dispatch:** ERD dispatch in the form of a REM envelope
- 187 **REMS notification:** ERDS serviceinfo in the form of a REM envelope, which includes a reference to the user content
188 to be delivered
- 189 **REMS receipt:** ERDS receipt in the form of a REM envelope
- 190 **REM interoperability domain:** homogeneous operational space consisting of a set of REMSPs able to properly
191 interoperate among themselves
- 192 **REM interoperability domain rules:** set of rules defining a REM interoperability domain

193

194 3.2 Abbreviations

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

196	CSI	Common Service Interface
197	EU	European Union

198	EUMS	EU Member State
199	ERD	electronic registered delivery
200	ERDS	electronic registered delivery service
201	ERDSP	electronic registered delivery service provider
202	ERD-UA	ERD user agent/application
203	I-ERDS	intermediate ERDS
204	R-ERDS	recipient's ERDS
205	S-ERDS	sender's ERDS
206	REM	registered electronic mail
207	REMS	registered electronic mail service
208	REMSP	registered electronic mail service provider
209	I-REMS	intermediate REMS
210	R-REMS	recipient's REMS
211	S-REMS	sender's REMS
212	S&F	Store and Forward
213	S&N	Store and Notify
214	MIME	Multipurpose Internet Mail Extensions
215	S/MIME	Secure/Multipurpose Internet Mail Extensions
216	PDF	Portable Document Format
217	SOAP	Simple Object Access Protocol
218	SMTP	Simple Mail Transfer Protocol
219	ESMTP	Extended SMTP
220	IMAP	Internet Message Access Protocol
221	POP	Post Office Protocol
222	POP3	Post Office Protocol version 3
223	TLS	Transport Layer Security
224	SASL	Simple Authentication and Security Layer
225	TL	Trusted List
226	NOTE:	As per TS 119 612 Error! Reference source not found..
227	TSP	Trust Service Provider
228	URI	Uniform Resource Identifier
229	XML	Extendable Mark-up Language

230 4 REM logical model

231 4.1 Introduction

232 4.1.1 Services and providers related to ERD

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

235 An electronic registered delivery service (ERDS) is generally understood to be a service that makes it possible to
 236 transmit data between the sender and recipients by electronic means and provides evidence relating to the handling of
 237 the transmitted data, including proof of sending and receiving the data, and that protects the transmitted data against the
 238 risk of loss, theft, damage or any unauthorised alterations. An electronic registered delivery service provider (ERDSP)
 239 is a legal entity which provides ERDS. The ERDSP is usually an organization, and it is responsible for the correctness
 240 of operations and issued evidence. The users of the service are usually clients or subscribers of only one of the ERDSPs,
 241 and they can send and receive data communicating only through their chosen service provider.

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

248 The concept of ERDS can be interpreted in two different ways.

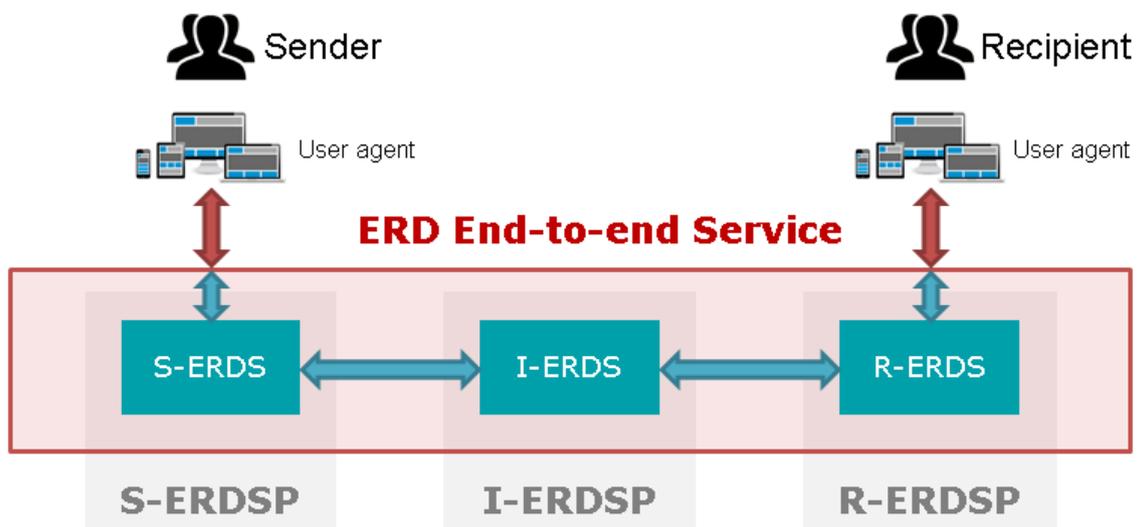
- 249 a) From the user's point of view the service is provided by the collaboration of multiple ERDSPs. It works just
 250 like international phone calls: when a user in Rome calls a phone number in Oslo, they do not need to know
 251 which operator that number belongs to and which countries the call will go through. Similarly, when the
 252 sender submits a message through a registered delivery service, they will receive proof of sending and receipt
 253 of that message, regardless of which service providers were involved in the performance of the service.
 254 Henceforth, this is called an electronic registered delivery end-to-end service.
- 255 b) From a compliance point of view there are certain requirements a service must fulfil in order to be considered
 256 an electronic registered delivery service. These requirements are formulated so that they apply to one single
 257 ERDSP. (Otherwise, conformance assessment would not be feasible.) Henceforth, the service provided by one
 258 single ERDSP is called an electronic registered delivery service.

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

- 260 1) Sender's ERDS (S-ERDS): this component service is responsible for allowing the submission of the message
 261 for the sender, with proper tracking of this event. It is also responsible for forwarding the message to the next
 262 actor, as appropriate.
- 263 2) Intermediate ERDS (I-ERDS): this component service is responsible for receiving a forwarded message and
 264 forwarding it again according to the routing rules established in the collaboration of service providers, with
 265 proper tracking of the relevant events. Multiple I-ERDS components can participate in the delivery of a
 266 particular message.
- 267 3) Recipient's ERDS (R-ERDS): this component service is responsible for receiving a forwarded message and
 268 delivering it to the recipient, with proper tracking of the relevant events.

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

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



275

276

Figure 1: Services and providers related to ERD

277 Notations used in the figure:

- 278 • In figure 1 the grey boxes represent the service providers (ERDSPs). They might also provide other services
 279 beside ERDS, but that is not shown in the figure.
- 280 • Each green box inside a grey box represents the service provided by the enclosing ERDSP. The green boxes
 281 correspond to the interpretation b) of the ERDS concept as described above (from a compliance point of view).

- 282 • The outer red box, enclosing all three green boxes, represents the electronic registered delivery end-to-end
283 service. This corresponds to the interpretation a) of the ERDS concept as described above (from the user's
284 point of view).
- 285 • The red arrows represent the external interface of the ERD end-to-end service, as it is perceived by the users.
- 286 • The green arrows represent the interface of the ERDS provided by one single provider. The figure illustrates
287 that this interface involves communication with the users, and also communication between the service
288 providers.

289 In the context of EU legislation, Regulation (EU) No 910/2014 [i.5] defines the terms '*electronic registered delivery*
290 *service*' and '*qualified electronic registered delivery service*', and specifies requirements for the latter. The Regulation
291 mentions the possibility of more than one provider participating in the provision of the service, but does not give any
292 stipulations regarding the possible different interpretations of the ERDS concept, as described above. However, the
293 requirements for a '*qualified electronic registered delivery service*' include identification of the sender and addressee
294 (recipient). In a general scenario, such as the one illustrated in figure 1, these requirements cannot be met by any single
295 provider alone, but they can be fulfilled by the collaboration of the ERDSPs. In consequence, in such a multi-provider
296 scenario, **the ERD end-to-end service, as defined in interpretation a) above**, could be able to satisfy the
297 requirements of a '*qualified electronic registered delivery service*' according to the Regulation.

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

300 4.1.2 General description of REM service

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

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

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

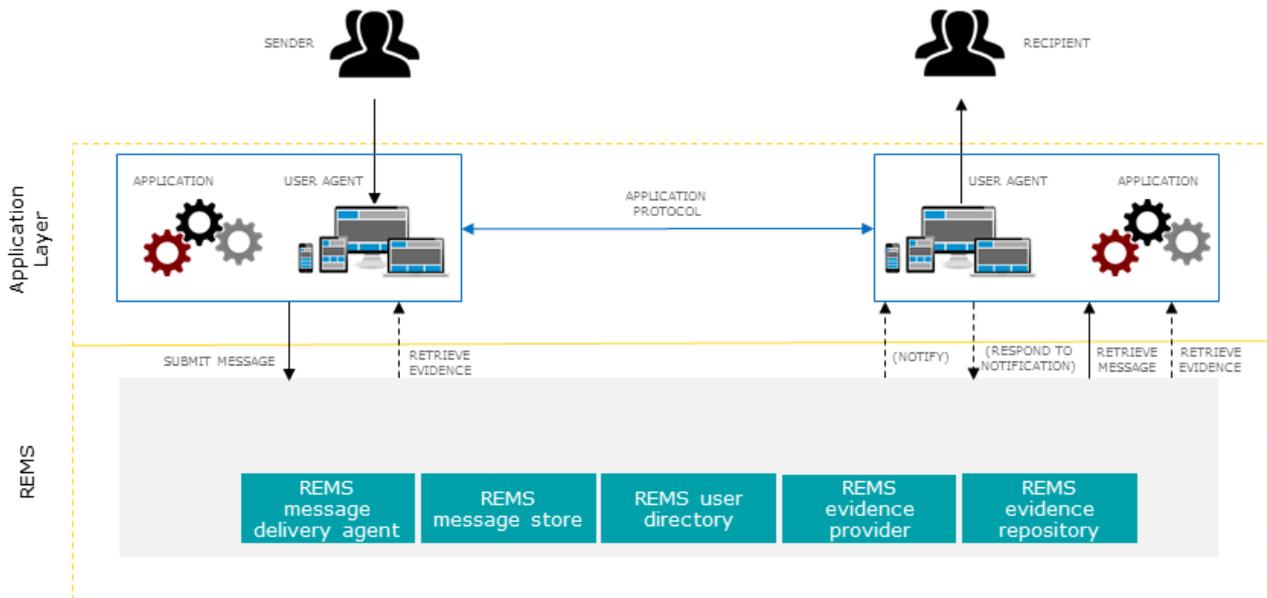
309 When the sender and the recipient are subscribers of different REMSPs, the REMSPs can collaborate to provide the
310 **REM end-to-end service, which is a specific type of ERD end-to-end service** as described in item a) of clause 4.1.1
311 above.

312 The next clauses describe the interpretation of the general ERDS model as applied in the specific case of REM. Clause
313 4.2 further specifies the black-box model described in clause 4.2 of ETSI EN 319 522-1 [1], focusing on the outer
314 interfaces of the REMS. Clause 4.3 further specifies the 4-corner model described in clause 4.3 of ETSI EN 319 522-1
315 [1], explaining the interaction between the services of different REMSPs. Clause 4.4 further specifies the extended
316 model described in clause 4.4 of ETSI EN 319 522-1 [1], providing the details about the interaction of the REMS with
317 other REMSs or ERDSs in the case when more than 2 providers take part in the delivery process.

318 4.2 Black-box model

319 4.2.1 Functional viewpoint

320 In the simplest case, a REMS can be represented as a black box, conveying messages between a sender and a recipient
321 and producing the appropriate evidences. The figure 2 below provides a simple representation.



322
323 **Figure 2: Black-box REM model**

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

329 As required for all ERDSs, the sender and recipients each have a unique identifier, by which they are referred in REM
330 messages and evidences. For REMS the unique identifier of users is an email address.

331 For the purpose of message submission certain metadata needs to be given by the sender to the REMS, e.g. recipient
332 addresses, requested style of operation, delivery options. This metadata is conveyed in the header of the email message.
333 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
334 [i.3].

335 4.2.2 Sequence viewpoint

336 4.2.2.1 REM styles of operation

337 From a procedural point of view, there are multiple alternative ways to deliver a message to a recipient.

338 One aspect is whether an explicit acceptance is required before the consignment of the user content to the recipient
339 occurs. In this aspect there are two alternatives:

- 340 • Acceptance is required: in this case the recipient must actively respond to the ERDSP before consignment, and
341 the user content is consigned only if the response was positive.
- 342 • Acceptance is not required: in this case the consignment of the user content will be performed without waiting
343 for any action of the recipient.

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

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

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

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

349 EXAMPLE 2: storing a file in the recipient’s mailbox, to be downloaded later by the email client via POP3.

- 350 • By reference: a reference to the user content is conveyed to the ERD-UA of the recipient, and the complete
351 user content itself is forwarded or downloaded only upon a request of the recipient.

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

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

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

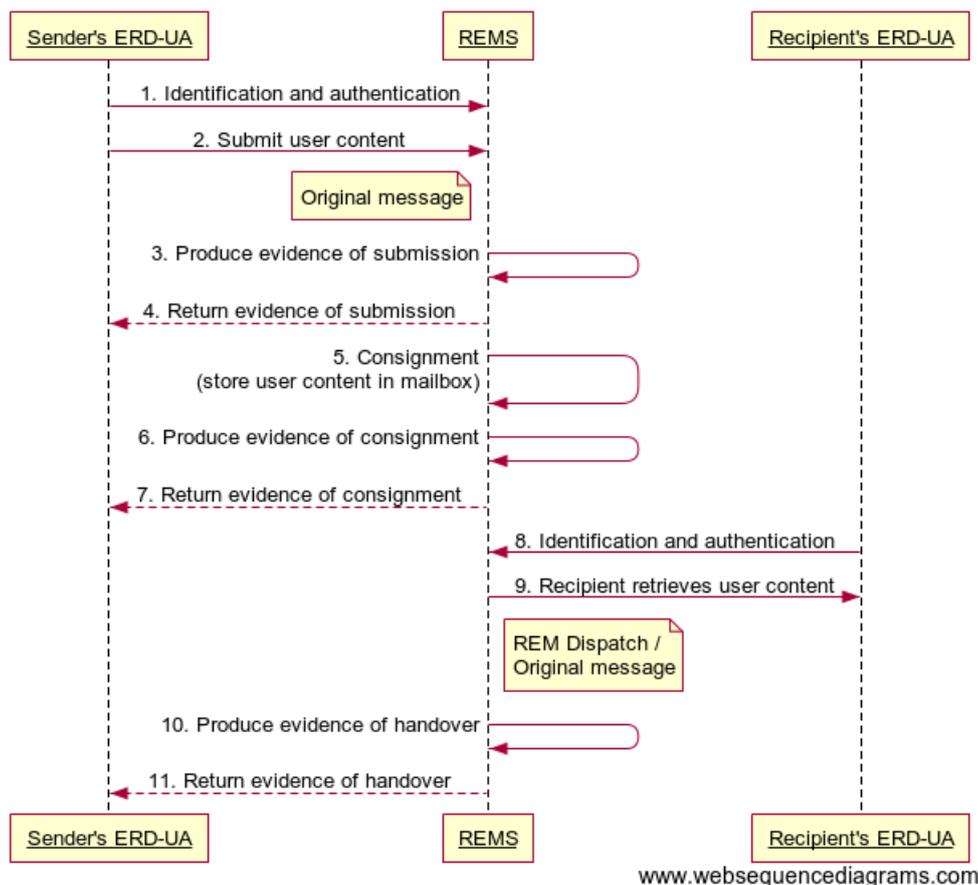
357 The two REM styles of operation are: "Store and Forward" (S&F) and "Store and Notify" (S&N).

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

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

369 4.2.2.2 REM Store and Forward style of operation

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



372

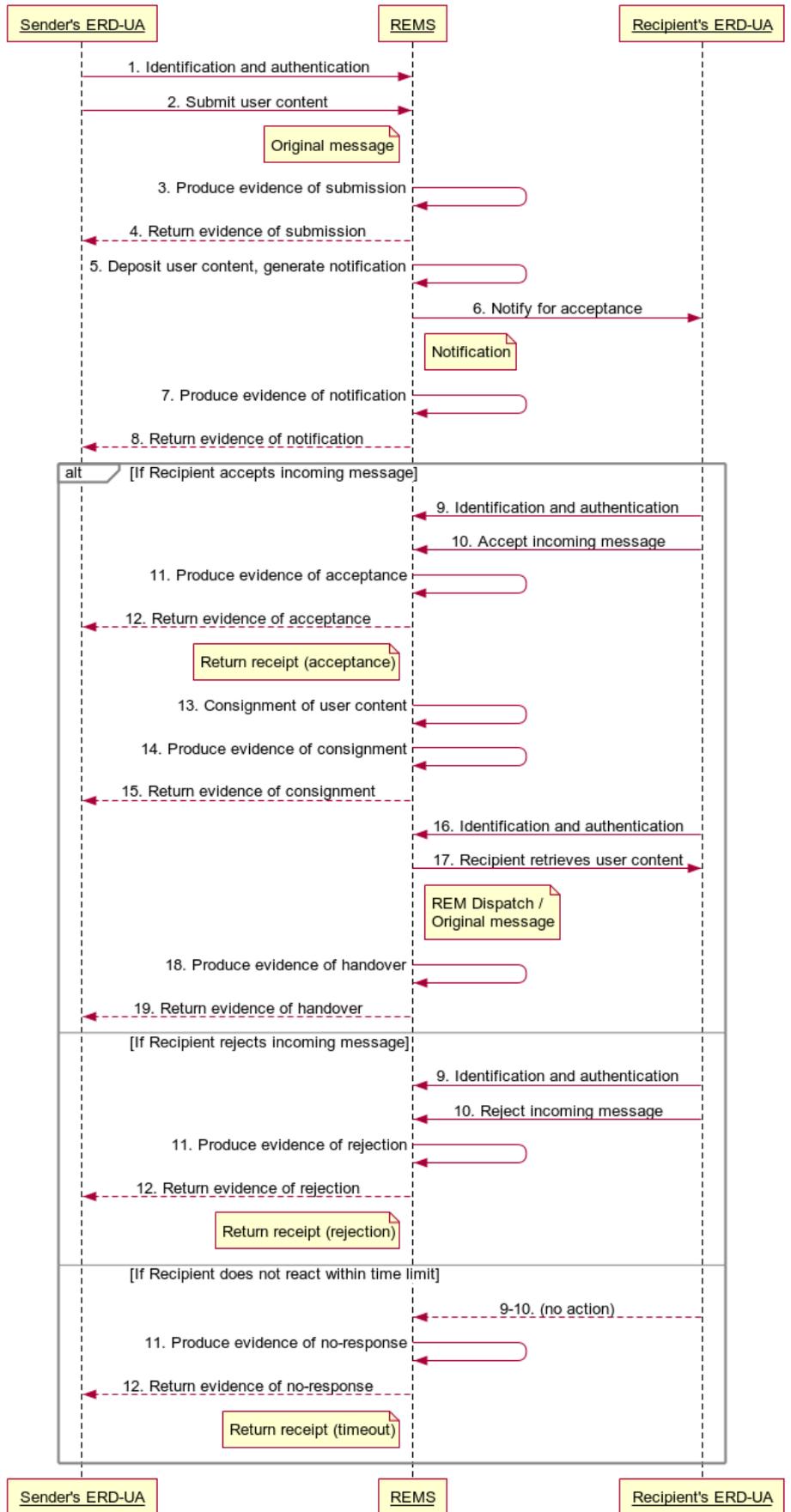
373

Figure 3: REM Store and Forward sequence of actions

- 374 1. The sender (either a user or a system) identifies and authenticates herself to the REM service.
- 375 2. The sender (either a user or a system) prepares the user content, specifies one or more recipients, and submits
376 it to the REM service. This step might in some cases merge with step 1 (e.g. if the original message in which
377 the user content is submitted contains a digital signature which is used to identify the sender)
- 378 3. The REM service tracks the event that the user content has been submitted. This is done producing an
379 "attestation of submission" (submission evidence), e.g. a signed file containing the basic information of the
380 event.
- 381 4. The evidence of submission may optionally be sent back to the sender. See NOTE below.
- 382 5. The REM service stores the user content in the recipient's mailbox. It may also store additional related
383 information (metadata, e.g. sender's identity, submission time, etc.) and evidence (e.g. submission evidence
384 produced in step 3.) along with the user content. These may be enveloped together in one single bundle, called
385 a REM dispatch, or may also be stored separately.
- 386 6. The REM service tracks the event that the user content has been made available to the recipient(s). Again, this
387 is done producing one or more attestation (consignment evidence).
- 388 7. The evidence of consignment may optionally be sent back to the sender. See NOTE below.
- 389 8. The recipient (either a user or a system) identifies and authenticates herself to the REMS.
- 390 9. The recipient (either a user or a system) retrieves the user content (either enveloped in a REM dispatch, or
391 separately), and optionally may also retrieve metadata and/or evidence (either enveloped in a REM dispatch,
392 or separately).
- 393 10. The REM service tracks the event that the user content has been handed over to the recipient. In some cases
394 this is done producing one or more attestation (handover evidence).
- 395 11. The evidence of handover may optionally be sent back to the sender. See NOTE below.
- 396 NOTE: In steps 4, 7, 11 sending the evidence right after its generation to the user is only one of the possible ways
397 of providing the evidence, and there are other alternatives as well, e.g.: the evidence can be stored by the
398 REMS for later on-demand access, it can be forwarded to an external evidence repository, etc.

399 4.2.2.3 REM Store and Notify style of operation

400 The sequence of actions in S&N style of operation is depicted in figure 4, and detailed below. For simplicity, failure
401 cases are not considered in this sequence.



www.websequencediagrams.com

402

403

Figure 4: REM Store and Notify sequence of actions

- 404 1. The sender (either a user or a system) identifies and authenticates herself to the REM service.
- 405 2. The sender (either a user or a system) prepares the user content, specifies one or more recipients, and submits
406 it to the REM service. This step might in some cases merge with step 1 (e.g. if the original message in which
407 the user content is submitted contains a digital signature which is used to identify the sender)
- 408 3. The REM service tracks the event that the user content has been submitted. This is done producing an
409 "attestation of submission" (submission evidence), e.g. a signed file containing the basic information of the
410 event.
- 411 4. The evidence of submission may optionally be sent back to the sender. See NOTE 2 below.
- 412 5. The REM service stores the user content (and optionally metadata and/or evidence along with it, optionally
413 enveloped in a REM dispatch) in a temporary storage where it is not accessible yet to the recipient, and
414 generates a notification for the recipient, containing a reference (e.g. a URL) to the user content.
- 415 6. The REM service sends the notification to the recipient. It may be sent as an ERD message or using any other
416 channel. Notifications sent through other channels (e.g. SMS, push notification) are outside the scope of the
417 present document.
- 418 7. The REM service tracks the event that the notification has been sent. It may produce a corresponding
419 attestation (notification evidence).
- 420 8. The evidence of notification may be sent back to the sender. See NOTE 2 below.

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

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

- 425 9. The recipient (either a user or a system) identifies and authenticates herself to the REMS.
- 426 10. The recipient performs an explicit action to confirm the acceptance of the incoming message by any means
427 provided by the REM service (e.g. sending a reply message, visiting a URL, clicking on a button, signing an
428 acknowledgment of receipt, etc.).
- 429 11. The REM service tracks the event that the message has been accepted by that particular recipient. This is done
430 producing a corresponding attestation (evidence of acceptance).
- 431 12. The evidence of acceptance, optionally along with additional data (e.g. acknowledgment of receipt signed by
432 the recipient), may be sent back to the sender. See NOTE 2 below.
- 433 13. The REM service stores the user content in the recipient's mailbox. It may also store additional related
434 information (metadata, e.g. sender's identity, submission time, etc.) and evidence (e.g. evidence produced in
435 step 3, step 7, step 10 or step 11) along with the user content. These may be enveloped together in one single
436 bundle, called a REM dispatch, or may also be stored separately.
- 437 Alternatively, the user content (and any accompanying metadata) may also be made available for download
438 directly through the channel in which the acceptance was performed (e.g. on the website of the REMS). The
439 user content is considered to be consigned regardless of the channel provided that it is available for the
440 recipient any time upon proper authentication.
- 441 14. The REM service tracks the event that the user content has been made available to the recipient(s). Again, this
442 is done producing one or more attestation (consignment evidence).
- 443 15. The evidence of consignment may be sent back to the sender. See NOTE 2 below.
- 444 16. The recipient (either a user or a system) identifies and authenticates herself to the REMS.
- 445 17. The recipient (either a user or a system) retrieves the user content (either enveloped in a REM dispatch, or
446 separately), and optionally may also retrieve metadata and/or evidence (either enveloped in a REM dispatch,
447 or separately).
- 448 18. The REM service tracks the event that the user content has been handed over to the recipient. In some cases,
449 this is done producing one or more attestation (handover evidence).

450 19. The evidence of handover may be sent back to the sender. See NOTE 2 below.

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

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

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

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

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

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

461 9., 10. The recipient takes no action.

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

465 12. The evidence of no-response, optionally along with additional data, may be sent back to the sender. See NOTE
466 2 below.

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

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

474 4.3 4-corner model

475 4.3.1 Functional viewpoint

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

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

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

487 This clause focuses on the interaction between two REMSs that communicate directly with each other, as illustrated in
488 figure 5.

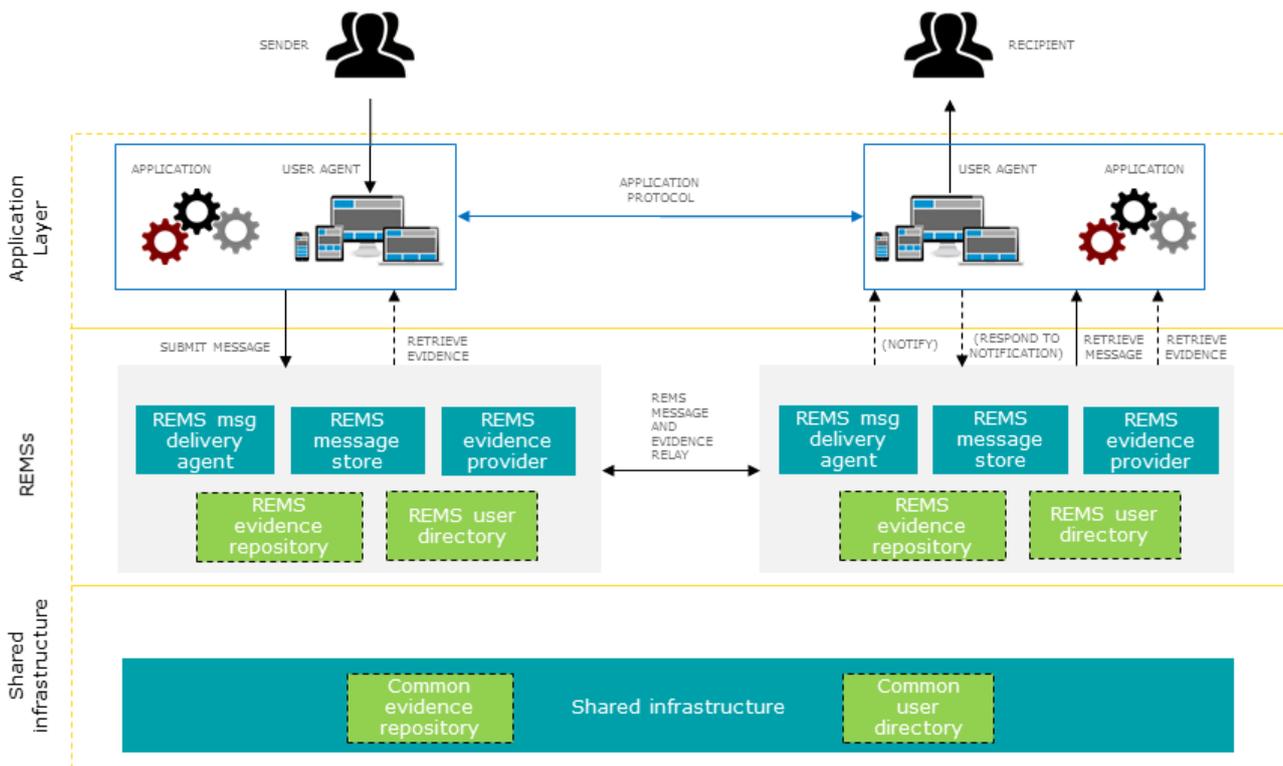


Figure 5: 4-corner REM model

489

490

491

492 Similarly to interconnected ERDSs in general, a shared infrastructure may assist the communication of interconnected
 493 REMSs. This may provide functions such as Message routing, Trust establishment, Capability management,
 494 Governance support, as described in clause 4.3.1 of ETSI EN 319 522-1 [1].

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

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

499

- S&F to S&F, as described in clause 4.3.2.1;

500

- S&F to S&N, as described in clause 4.3.2.2;

501

- 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;

502

503

- 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.

504

505

506

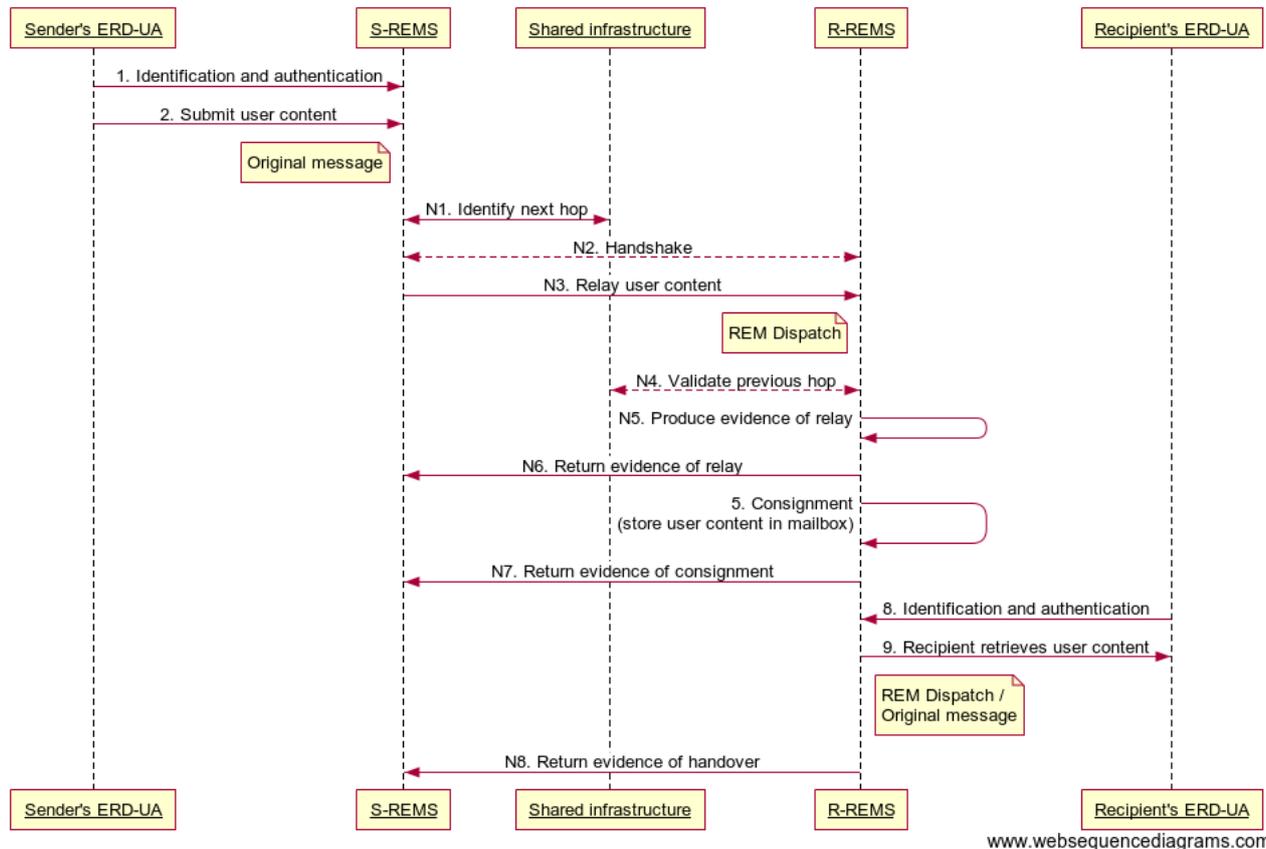
507 4.3.2 Sequence viewpoint

508 4.3.2.1 REM S&F to S&F interaction

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

511 The sequence of actions in S&F to S&F interaction is depicted in figure 6, and detailed below. For simplicity, failure
 512 cases are not considered in this sequence. The REMSs may track each relevant event in the sequence by producing a
 513 corresponding evidence, as detailed in clause 4.2.2.2, but for an easier overview, the production of these evidences is

514 not shown in the figure. The produced evidence may also be sent to the user, or may be provided in other ways, as
 515 described in clause 4.2.2.2. The optional returning of evidence to users is not shown in the figure.



516

517

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

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

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

527 1, 2, 3, 4. The user content is submitted, as in clause 4.2.2.2.

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

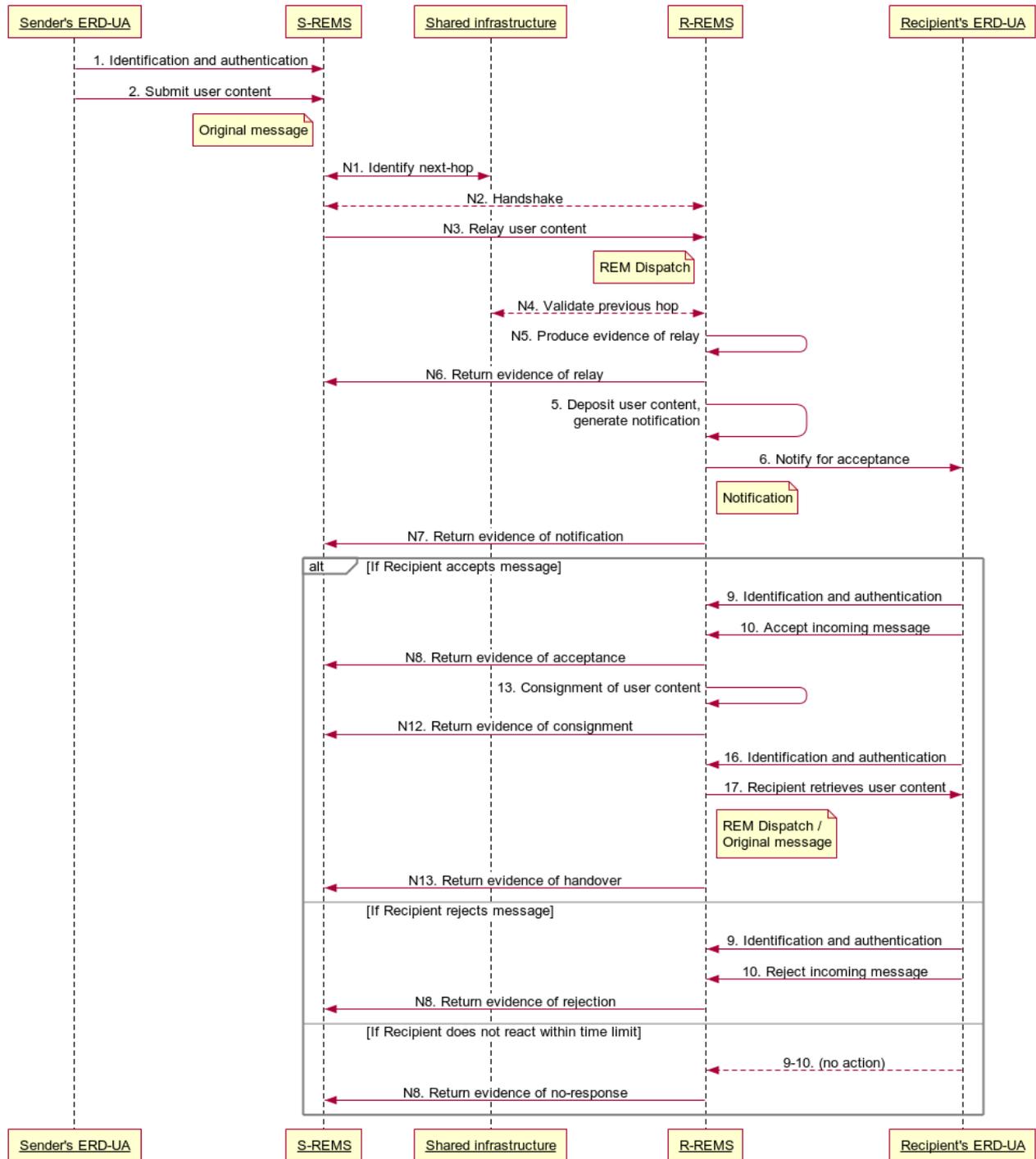
- 531 - S-REMS needs to identify the recipient's REMS. This may be possible using the recipient's mailbox
 532 address, as an email address contains the provider domain.
- 533 - S-REMS needs to find a mail route to the R-REMS. This may be possible using DNS lookups, as it is
 534 done in the case of regular email messages. In the 4-corner model (clause 4.3) it is assumed that the REM
 535 message can be forwarded directly to R-REMS. In the extended model (clause 4.4) it is assumed that the
 536 REM message is forwarded through a number of intermediate REMSs.
- 537 - S-REMS needs to check the capabilities of the REMSs along the mail route (e.g. supported style of
 538 operation, supported policies, etc.) in order to find a suitable route.

- 539 - S-REMS needs to establish a trust relationship with the next-hop REMS along the mail route. This may
540 be done, for instance, using Trusted Lists, as defined in ETSI TS 119 612 [i.7].
- 541 N2. The REMS performs a handshake with the next-hop REMS. This may include negotiation on different aspects
542 (capabilities, supported style of operation, ERDS evidence, level of authentication of end entities, fees, etc.).
543 Handshake may not be necessary in closed systems where this information is defined a priori or available
544 through a centralised infrastructure.
- 545 N3. The REMS relays the REM message to the next-hop REMS. It may also relay additional related information
546 (metadata, e.g. sender's identity, submission time, etc.) and evidence (e.g. submission evidence produced in
547 step 3.) along with it.
- 548 N4. The REMS that received the relayed REM message may also look up the relaying REMS in the shared
549 infrastructure, and get information (e.g. certificates), establish trust, etc.
- 550 N5. If the REM message has been successfully received and the validation of the relaying REMS reported no
551 problems, then the REMS tracks this event by producing a corresponding evidence of relay.
- 552 N6. The evidence of relay is returned to the relaying REMS, as an indication that the responsibility of handling the
553 relayed REM message has been taken over by the next REMS.
- 554 5, 6. The user content is consigned, as in clause 4.2.2.2.
- 555 N7. The evidence of consignment needs to be relayed back to the previous REMS along the mail route, so that it
556 can close its transaction, and the sender may also need this attestation.
- 557 7. The evidence of consignment may be returned to the sender, as in clause 4.2.2.2.
- 558 8, 9, 10. The user content is handed over to the recipient, as in clause 4.2.2.2.
- 559 N8. The evidence of handover needs to be relayed back to the previous REMS along the mail route, in case the
560 sender needs this attestation.
- 561 11. The evidence of handover may be returned to the sender, as in clause 4.2.2.2.

562 4.3.2.2 REM S&F to S&N interaction

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

567 The sequence of actions in S&F to S&N interaction is depicted in figure 7, and detailed below. For simplicity, failure
568 cases are not considered in this sequence. The REMSs may track each relevant event in the sequence by producing a
569 corresponding evidence, as detailed in clause 4.2.2.3, but for an easier overview, the production of these evidences is
570 not shown in the figure. The produced evidence may also be sent to the user, or may be provided in other ways, as
571 described in clause 4.2.2.3. The optional returning of evidence to users is not shown in the figure.



www.websequencediagrams.com

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

572

573

574 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.
 575 Therefore, the indices of the actions relevant for the REM end-to-end service are kept the same as in figure 4. The new
 576 actions depicted in figure 7 are the communication steps between the REMSs, or in other words, communications
 577 internal to the REM delivery network. These are indexed with 'N#'. The steps of the process are as detailed below.

578 1, 2, 3, 4. The user content is submitted, as in clause 4.2.2.3.

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

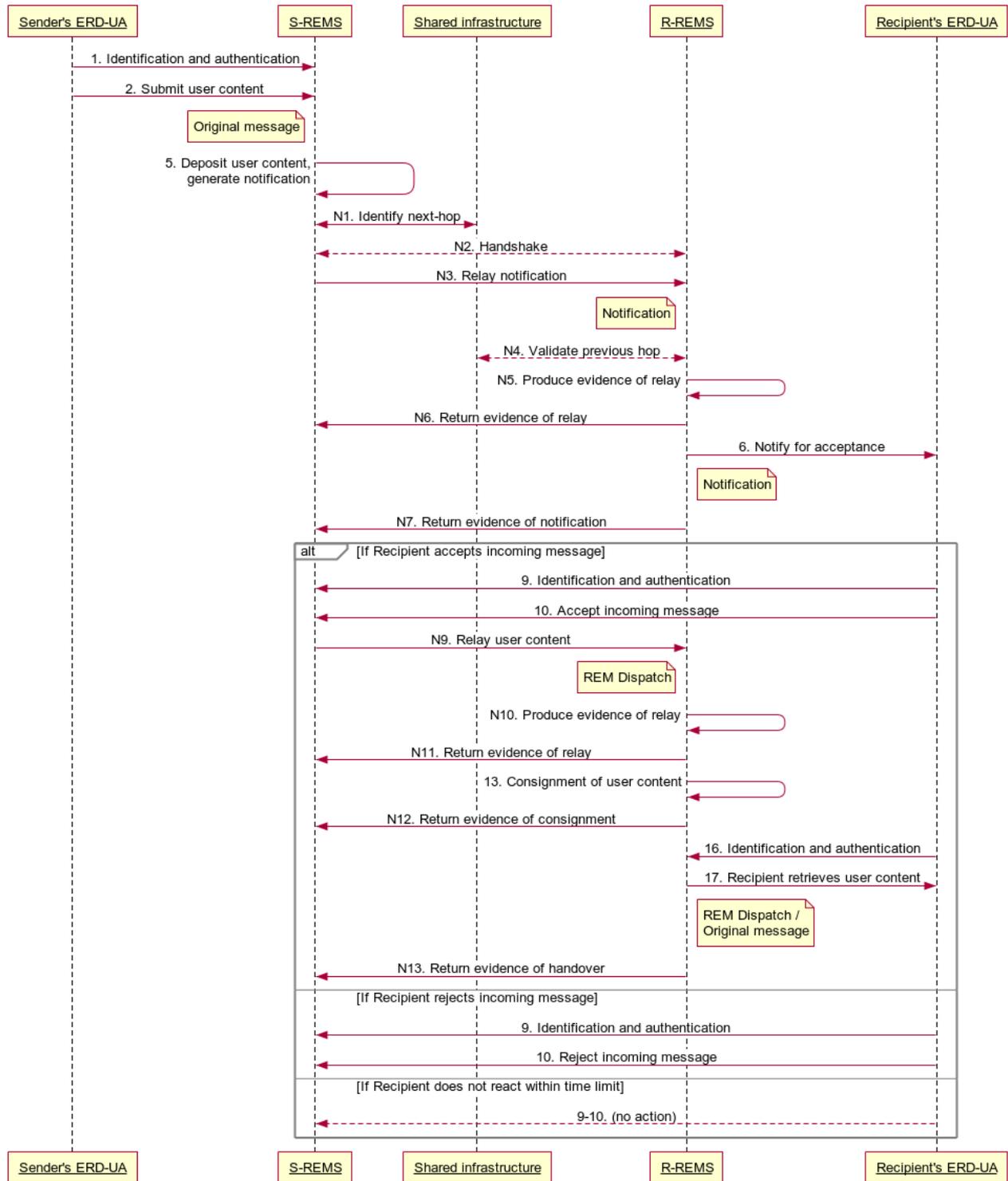
581 5, 6, 7. The user content is deposited in a temporary storage and a notification is sent, as in clause 4.2.2.3.

- 582 N7. The evidence of notification needs to be relayed back to the previous REMS along the mail route, in case the
583 sender needs this attestation.
- 584 8. The evidence of notification may be returned to the sender, as in clause 4.2.2.3.
- 585 9, 10, 11. The recipient accepts/rejects/does not respond to the incoming message, and the result is tracked as in
586 clause 4.2.2.3.
- 587 N8. The evidence of the acceptance/rejection/no-response needs to be relayed back to the previous REMS along
588 the mail route, in case the sender needs this attestation.
- 589 12. The evidence of acceptance/rejection/no-response may be returned to the sender, as in clause 4.2.2.3.
- 590 **Conditional:** if the recipient accepted the incoming message:
- 591 13, 14. The user content is consigned, as in clause 4.2.2.3.
- 592 N12. The evidence of consignment needs to be relayed back to the previous REMS along the mail route, so that it
593 can close its transaction, and the sender may also need this attestation.
- 594 15. The evidence of consignment may be returned to the sender, as in clause 4.2.2.3.
- 595 16, 17, 18. The recipient retrieves the user content, as in clause 4.2.2.3.
- 596 N13. The evidence of handover needs to be relayed back to the previous REMS along the mail route, in case the
597 sender needs this attestation.
- 598 19. The evidence of handover may be returned to the sender, as in clause 4.2.2.3.

599 4.3.2.3 REM S&N to S&F interaction

600 This clause describes the case when the sender's REMS operates in S&N style and the recipient's REMS operates in
601 S&F style in the handling of a particular user content. Instead of the user content itself, at first the notification is relayed
602 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
603 the acceptance/rejection process of the S&N style as described in clause 4.2.2.3, except that the user content is not
604 consigned directly to the recipient's mailbox but relayed to R-REMS first. (The user content may also be handed over
605 directly to the recipient, but this is not detailed in this clause.) The notification is always handled by a S&F sub-
606 component even if the REMS normally acts in S&N style, so the sequence is the same also when the R-REMS operates
607 in S&N style.

608 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
609 figure 8, and detailed below. For simplicity, failure cases are not considered in this sequence. The REMSs may track
610 each relevant event in the sequence by producing a corresponding evidence, as detailed in clause 4.2.2.3, but for an
611 easier overview, the production of these evidences is not shown in the figure. The produced evidence may also be sent
612 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
613 is not shown in the figure.



www.websequencediagrams.com

614

615

Figure 8: 4-corner S&N to S&F sequence

616 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.
 617 Therefore, the indices of the actions relevant for the REM end-to-end service are kept the same as in figure 4. The new
 618 actions depicted in figure 8 are the communication steps between the REMSs, or in other words, communications
 619 internal to the REM delivery network. These are indexed with 'N#'. The steps of the process are as detailed below.

620 1, 2, 3, 4. The user content is submitted, as in clause 4.2.2.3.

621 5. The user content is deposited in a temporary storage and a notification is generated, as in clause 4.2.2.3.

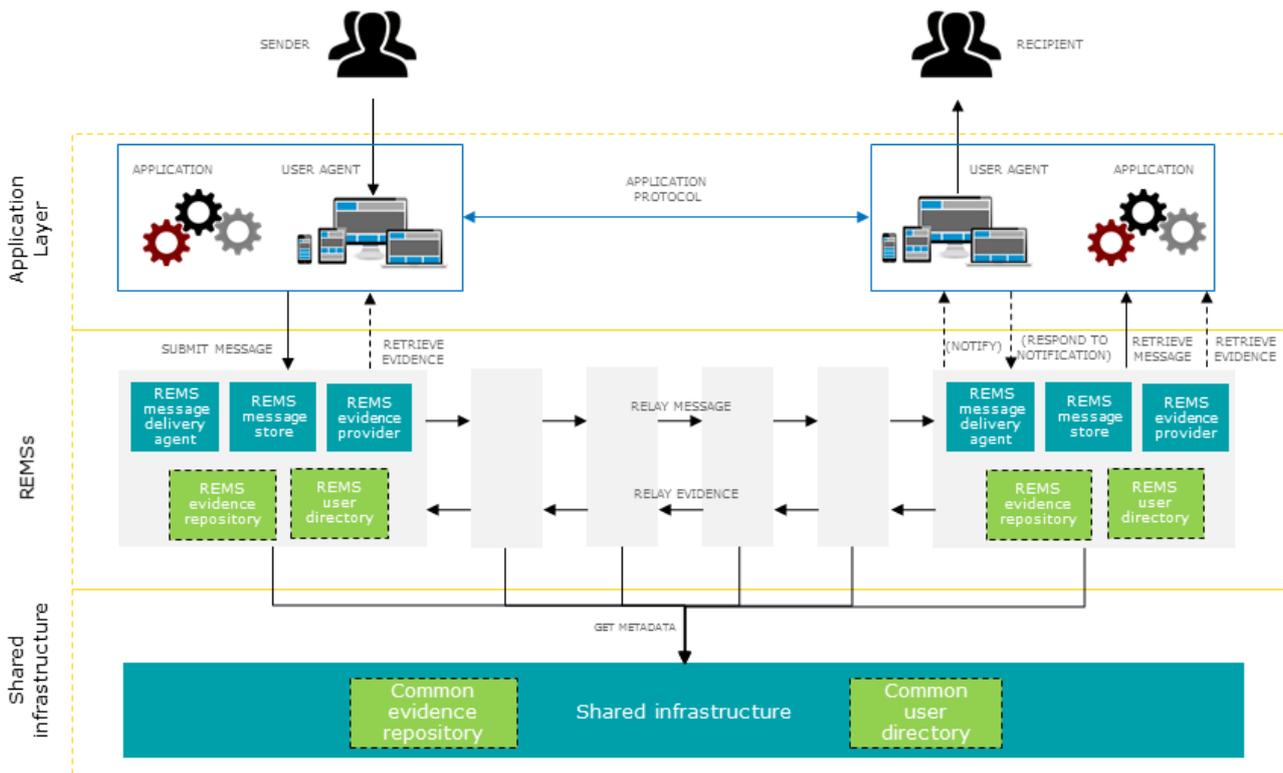
- 622 N1, N2, N3, N4, N5, N6. The S-REMS relays the notification, as in clause 4.3.2.1. (The REM message in the
623 description of steps N1-N6. is in this case a REMS notification.)
- 624 6, 7. The R-REMS interprets the incoming REMS notification (containing the reference to the user content). Then it
625 notifies the recipient using any channel they have agreed on, and tracks this event, as in clause 4.2.2.3.
- 626 N7. The evidence of notification needs to be relayed back to the previous REMS along the mail route, in case the
627 sender needs this attestation.
- 628 8. The evidence of notification may be returned to the sender, as in clause 4.2.2.3.
- 629 9, 10, 11. The recipient accepts/rejects/does not respond to the incoming message, communicating directly with S-
630 REMS when needed, and the result is tracked as in clause 4.2.2.3.
- 631 12. The evidence of acceptance/rejection/no-response may be returned to the sender, as in clause 4.2.2.3.
- 632 **Conditional:** if the recipient accepted the incoming message:
- 633 N9. The REMS relays the user content to the next-hop REMS. It may also relay additional related information
634 (metadata, e.g. sender's identity, submission time, etc.) and evidence (e.g. submission evidence produced in
635 step 3.) along with it. The REMS may also hand over the user content directly to the recipient. (This is not
636 shown in the figure.)
- 637 N10. If the REM message has been successfully received and the validation of the relaying REMS reported no
638 problems, then the REMS tracks this event by producing a corresponding evidence of relay.
- 639 N11. The evidence of relay is returned to the relaying REMS, as an indication that the responsibility of handling the
640 relayed REM message has been taken over by the next REMS.
- 641 13, 14. The user content is consigned, as in clause 4.2.2.3.
- 642 N12. The evidence of consignment needs to be relayed back to the previous REMS along the mail route, so that it
643 can close its transaction, and the sender may also need this attestation.
- 644 15. The evidence of consignment may be returned to the sender, as in clause 4.2.2.3.
- 645 16, 17, 18. The recipient retrieves the user content, as in clause 4.2.2.3.
- 646 N13. The evidence of handover needs to be relayed back to the previous REMS along the mail route, in case the
647 sender needs this attestation.
- 648 19. The evidence of handover may be returned to the sender, as in clause 4.2.2.3.

649 4.4 Extended model

650 4.4.1 Functional viewpoint

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

655 This clause focuses on the interactions between the different REMSs in the case when more than 2 REMSs take part in
656 the delivery process.



657
658 **Figure 9: Extended REM model**

659 When the sender and the recipient are subscribed to different REMSs then the respective REMSs communicate in order
660 to forward the user content, along with some metadata associated to it, and to provide evidence to the users about every
661 relevant event during the process. This communication may happen indirectly, involving a number of intermediate
662 REMSs as well, which may provide routing assistance, trust gateway, and other auxiliary functions.

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

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

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

674 Each of the REMSs involved in the delivery process may operate in S&F or S&N style (or may support both).
675 However, in any chain of REMSs only one REMS can act effectively according to the S&N style, since the notification
676 is always handled by a S&F sub-component. Therefore, all the REMSs along the chain after the first S&N REMS shall
677 behave as S&F ones. The interactions between any two adjacent REMSs follow one of the patterns described in clause
678 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
679 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
680 side of) the S&N REMS are like in clause 4.3.2.3. These two options are detailed in the next clause.

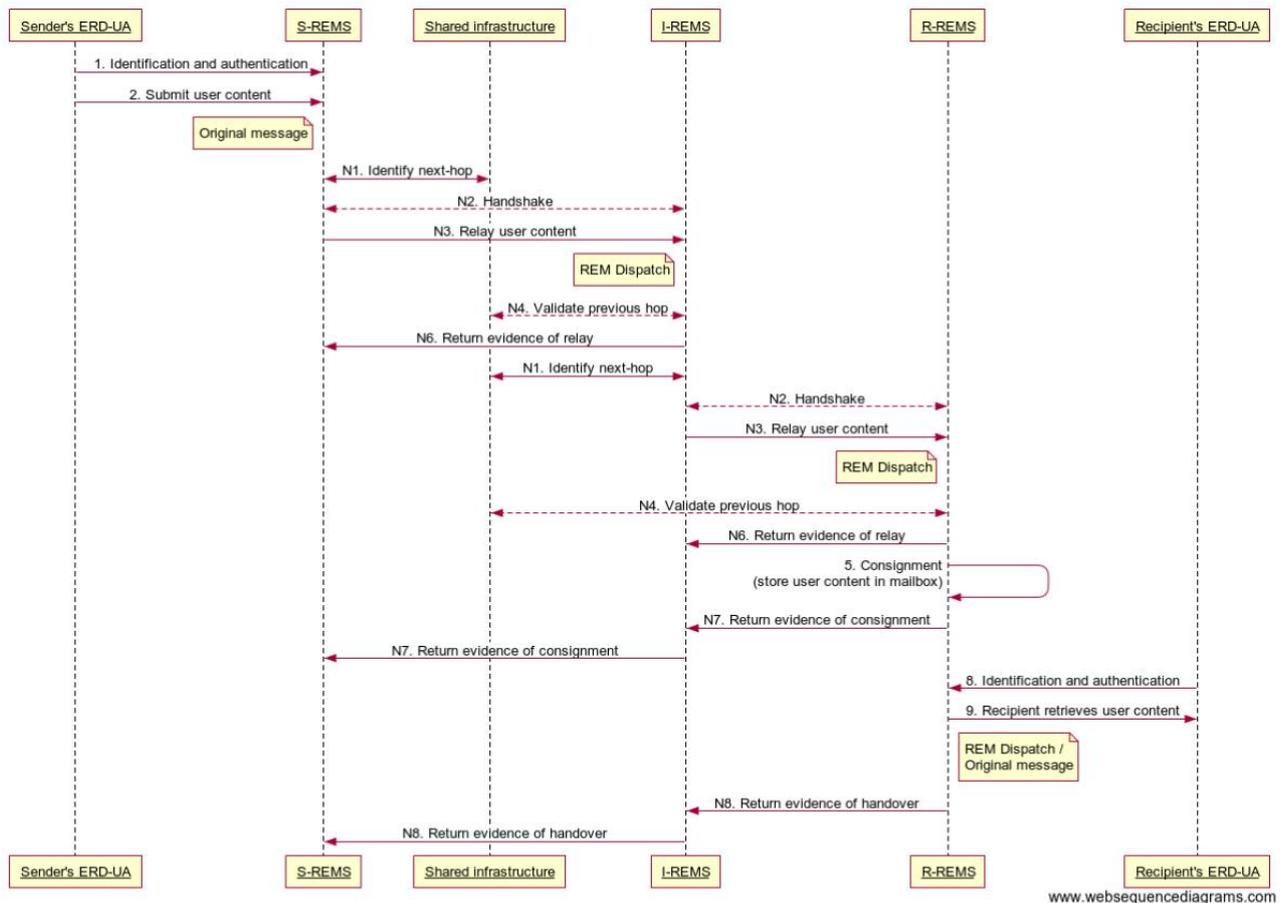
681 4.4.2 Sequence viewpoint

682 4.4.2.1 Multi-hop sequence over S&F nodes only

683 When all REMSs in the chain operate in S&F style, the user content itself will be relayed along the chain to R-REMS,
684 and the evidences will be relayed backwards along the chain to S-REMS. The interactions with the users are still the
685 same as defined in clause 4.2.2.2 for Store & Forward style in the black-box model. The communication between any

686 two adjacent REMSs follows the pattern described in clause 4.3.2.1. The sequence of steps N1, N2, N3, N4, N5, N6.
 687 will be repeated as many times as needed to relay the user content. Steps N7. and N8. will be repeated individually as
 688 many times as needed to relay any evidence.

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



695

696

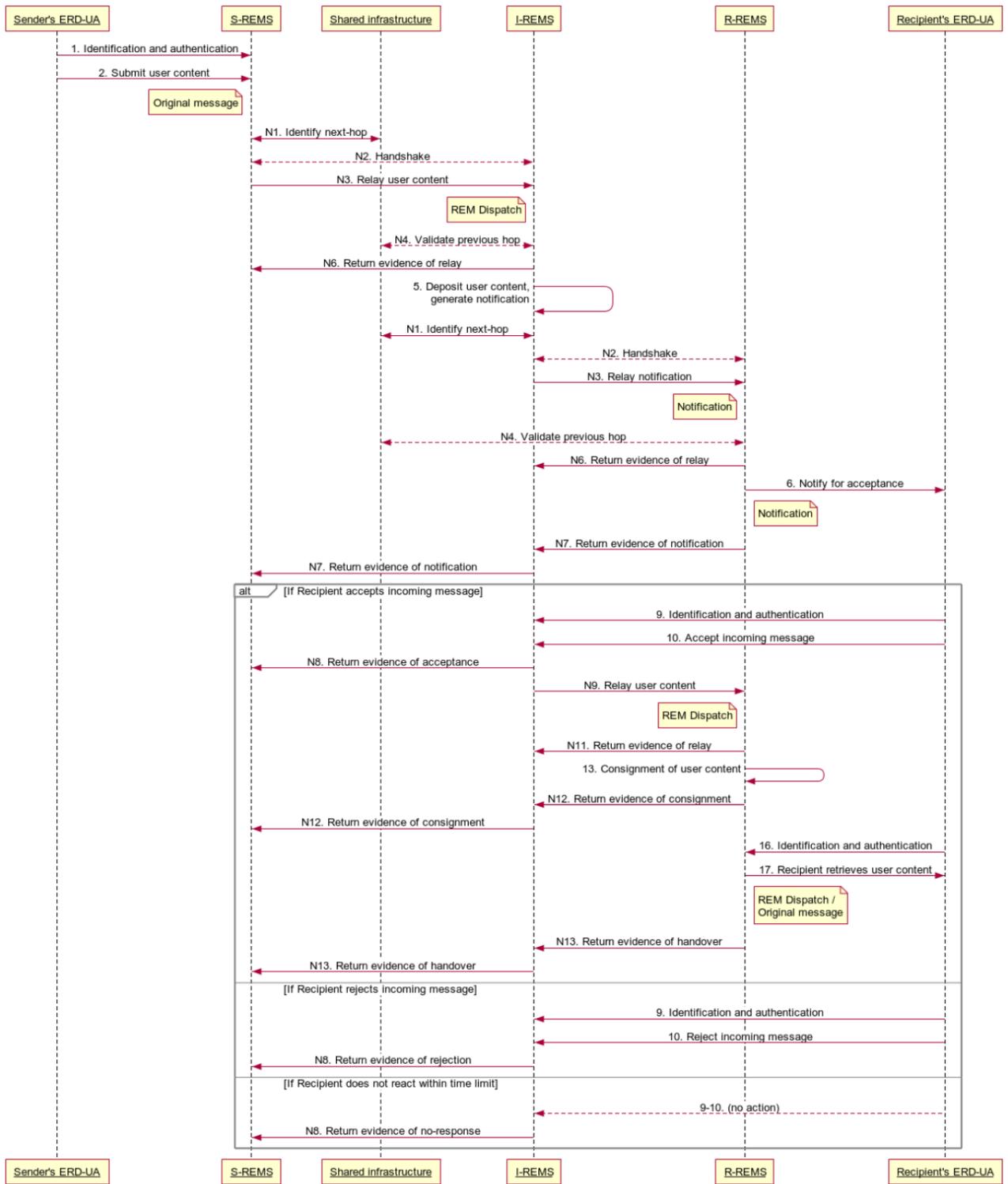
Figure 10: extended S&F to S&F to S&F sequence

697 4.4.2.2 Multi-hop sequence involving a S&N node

698 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
 699 REMS, where it will be stored temporarily, and from there the REMS notification will be relayed along the chain to R-
 700 REMS. Any evidence will be relayed backwards along the chain to S-REMS. The interactions with the users are still the
 701 same as defined in clause 4.2.2.3 for Store & Notify style in the black-box model. The communication between any two
 702 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
 703 communication between any two adjacent REMSs after (on the recipient's side of) the S&N REMS follows the pattern
 704 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
 705 relay the user content up to the S&N node, and to relay the REMS notification from there up to R-REMS. The sequence
 706 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-
 707 REMS. Steps N7., N8., N12. and N13. will be repeated individually as many times as needed to relay any evidence.

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

713 may be provided in other ways, as described in clause 4.2.2.3. The optional returning of evidence to users is not shown
 714 in the figure.



www.websequencediagrams.com

715

716

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

717

4.5 Roles within a REMS

718 The logical model refines the functionality of the REMS into separate components, which were historically also referred
 719 to as “roles”. The general ERDS model applies to REM as well. For the description of the ERDS components see clause
 720 4.2.1 of ETSI EN 319 522-1 [1].

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

722 **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

723

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

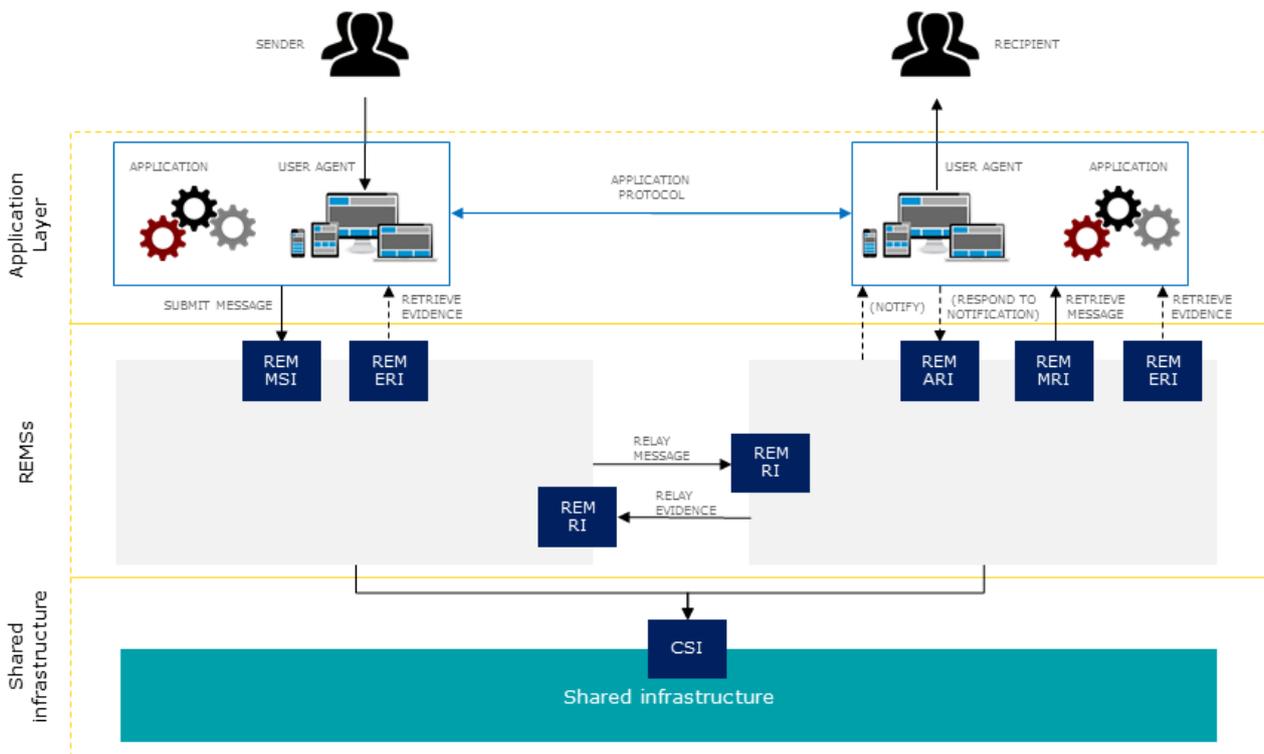
727 The REMS **shall** include the following core roles: REMS message delivery agent, REMS message store, and REMS
 728 evidence provider.

729 5 REM interfaces

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

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

737



738

739

740

Figure 12: Interfaces of REMS

Table 2: Requirements for REM interfaces

741

Name of interface	Corresponding ERDS interface in EN 319 522-1 [1]	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 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. through a token from a third party). This interface shall implement confidentiality and integrity preserving measures.	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.
REM MRI: Message Retrieval Interface	ERDS MERI: 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. 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 MSI. 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).
REM ERI: Evidence Retrieval Interface		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.
REM RI: Relay Interface	ERDS RI: Relay Interface: this interface allows ERD messages to be relayed between ERDS. This interface shall implement 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 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.
REM ARI: Acceptance/Rejection Interface	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. 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: ERD-UA 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.

Name of interface	Corresponding ERDS interface in EN 319 522-1 [1]	Specific requirements for REM
CSI: Common Service Interface	CSI: Common Service Interface: this interface gives access to message routing functions, trust management functions, capability management functions, governance functions.	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.).

742

743

6 REM events and evidence

744

6.1 Overview

745

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

746

747

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.

748

749

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.

750

751

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

752

6.2 Events and evidence

753

6.2.1 A. Events related to the submission

754

755

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

756

757

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

758

759

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.

760

761

762

763

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.

764

Table 3: Events related to the submission

Event type in 319 522-1	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 delivering 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.6] clause 8.3.3 about possible reasons.

765

6.2.2 B. Events related to the relay between REMSs

766

767

768

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.

769 **Relay** is the handing over of a REM message from one REMS (sending REMS henceforth) to another REMS (receiving
770 REMS henceforth) through the **REM RI: Relay Interface**. When the **REM RI** is provided using SMTP then this
771 transaction is an SMTP transaction.

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

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

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

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

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

788 **Table 4: Events related to relay between REMSs**

Event type in 319 522-1	Related interface	Issuing REMS	Interpretation
B.1. RelayAcceptance	REM RI	Receiving REMS	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.
B.2. RelayRejection	REM RI	Receiving REMS	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 [i.6] clause 8.3.3 about possible reasons.
B.3. RelayFailure	REM RI	Sending REMS	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.

789 6.2.3 C. Events related to the acceptance/rejection by the recipient

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

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

797 The notification shall be relayed to the R-REMS. Upon receiving a notification addressed to one of its subscribers, R-
798 REMS shall notify the subscriber. R-REMS may use any channel to notify the recipient. R-REMS should issue
799 evidence about the successful or unsuccessful notification of the recipient.

800

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

Event type in 319 522-1	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 identification and authentication, has performed an explicit action by which they indicated that they accept the message to be delivered.
C.4. ConsignmentRejection	REM ARI	Notifying REMS	The recipient, upon proper identification and authentication, has performed an explicit action by which they indicated that they reject 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.

801

6.2.4 D. Events related to the consignment

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

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

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

812

Table 6: Events related to the consignment

Event type in 319 522-1	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	R-REMS could not make the user content available to the recipient within a given time period.
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.

813

6.2.5 E. Events related to the handover to the recipient

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

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

820 When the **REM MRI** is provided using IMAP/POP3, then this transaction is an IMAP/POP3 transaction, which may
821 involve handover of more than one message containing user content. When IMAP is used, fetching only the headers of
822 the message (without the mail body) does not constitute handover. When the **REM MRI** is provided using HTTP, then
823 download of the message by the HTTP client is considered as handover.

824 NOTE: In ETSI TS 102 640-1 download of the message was defined to be a separate event from retrieval of the
 825 message. This standard considers those two cases as one, consequently there is no separate download
 826 event defined.

827 **Table 7: Events related to the handover to the recipient**

Event type in 319 522-1	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.

828 6.2.6 F. Events related to connections with non-ERDS systems

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

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

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

Event type in 319 522-1	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.

836

837 7 Shared infrastructure of REM

838 When the registered mail delivery involves multiple REM services of multiple providers, usually some shared
 839 infrastructure is used in the discovery, identification and assessment of the services, as specified in clauses 4.3.1 and
 840 4.4.1.

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

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

845 History

Document history		
V0.0.4	October 2017	Stable draft for public review

846