Draft **ETSI EN 319 532-4** V0.0.4 (2017-10)

EUROPEAN STANDARD

Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) Services; Part 4: Interoperability profiles

0

1

Reference
DEN/ESI-0019532-4

Keywords
<keywords>

2

Important notice

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

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

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

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

Copyright Notification

ETSI

Contents

Intellectual Property Rights

Essential patents

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

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

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 public review before approval by TC ESI and submission for the combined Public Enquiry and Vote phase of the ETSI standards EN Approval Procedure.

The present document is part 4 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.

Executive summary

Editorial Note: this section will be completed in the next developments of the present document.

122

Introduction

124   Editorial Note: this section will be completed in the next developments of the present document.

125

1   Scope

The basic purpose of Registered Electronic Mail (REM) is to provide a service for the transmission of information among parties, counting on an evidence set, related to the communication steps, suitable to uphold proof of acceptance, of sending, of delivery/non-delivery, receiving/retrieval of the conveyed data. The email standards used as backbone, including a set of additional security mechanisms, make smooth the interoperability and, at the same time, protect the integrity, the confidentiality and the loss exposition of the carried information.

The present document defines the profiles of ETSI EN 319 532-3 [8] specification, taking in account concepts and semantic defined in ETSI EN 319 532-1 [6] and ETSI EN 319 532-2 [7], addressing issues relating authentication, authenticity and integrity of the information, with the purpose to address the achievement of interoperability across REM service providers, implemented according the aforementioned specifications and using the same or different formats and/or transport protocols.

The present document covers all the options to profile REM services for both styles of operation: S&N and S&F.

The mandatory requirements defined in the aforementioned referenced REM services specifications are not normally repeated here but, when necessary, the present document contains some references to them.

More specifically:

a) Defines generalities on profiling

b) Defines constraints for SMTP profile.

c) Defines mapping form SMTP/PReM interoperability profile.

The specifications defined in the present document aims to cover the common and worldwide-recognized requirements to address **electronic delivery** in a secure and reliable way. Particular attention is paid so that the present document cover the legal provisions of all the articles and requirements of the Regulation (EU) No 910/2014 [i.8]. Anyway, the legal effects of services implemented according to the present document are outside the scope of the same.

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 319 521: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Electronic Registered Delivery Services Providers".

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

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

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

168 [5]   ETSI EN 319 522-3: "Electronic Signatures and Infrastructures (ESI); Electronic Registered
169   Delivery Services; Part 3: Formats".

170 [6]   ETSI EN 319 532-1: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail
171   (REM) Services; Part 1: Framework and Architecture ".

172 [7]   ETSI EN 319 532-2: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail
173   (REM) Services; Part 2: Semantic Contents".

174 [8]   ETSI EN 319 532-3: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail
175   (REM) Services; Part 2: Formats".

176 [9]   IETF RFC 3207 (2002): "SMTP Service Extension for Secure SMTP over Transport Layer
177   Security".

178 [10]   ETSI TS 119 612: "Electronic Signatures and Infrastructures (ESI); Trusted Lists".

179

180 Editorial Note: the following reference refers to the actual specification of PReM. It should be updated with a new
181   one according to the note at Clause 6.

182 [11]   UPU S52-1: "Functional specification for postal registered electronic mail".

183

184

185

2.2   Informative references

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

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

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

194 [i.1]   ETSI TR 102 605: "Electronic Signatures and Infrastructures (ESI); Registered E-Mail".

195 [i.2]   ETSI EN 319 522-4-1: "Electronic Signatures and Infrastructures (ESI); Electronic Registered
196   Delivery Services; Part 4-1: Message delivery bindings".

197 [i.3]   ETSI EN 319 522-4-2: "Electronic Signatures and Infrastructures (ESI); Electronic Registered
198   Delivery Services; Part 4-2: Evidence and identification bindings".

199 [i.4]   ETSI EN 319 522-4-3: "Electronic Signatures and Infrastructures (ESI); Electronic Registered
200   Delivery Services; Part 4-3: Capability and requirements bindings".

201 [i.5]   ETSI TS 119 524: "Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery
202   Services; Testing Conformance and Interoperability of Electronic Registered Delivery Services.".

203 [i.6]   ETSI TS 119 534: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail
204   (REM) Services; Testing Conformance and Interoperability of Electronic Registered Mail
205   Services".

206 [i.7]   ETSI TR 119 500: "Electronic Signatures and Infrastructures (ESI); Business Driven Guidance for
207   Trust Application Service Providers".

208 [i.8]   Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on
209   electronic identification and trust services for electronic transactions in the internal market and
210   repealing Directive 1999/93/EC.

211   [i.9]   ISO/IEC 27001:2005: "Information technology - Security techniques - Information security
212   management systems - Requirements".

213   [i.10]   ISO/IEC TR 10000:1998: " Information technology — Framework and taxonomy of International
214   Standardized Profiles".

215   [i.11]   IETF RFC 5321: "Simple Mail Transfer Protocol".

216   [i.12]   IETF RFC 5322: "Internet Message Format".

217   [i.13]   IETF RFC 5751: "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message
218   Specification".

219   [i.14]   ISO 3166-1: "Codes for the representation of names of countries and their subdivisions -- Part 1:
220   Country codes".

221

222   Editorial Note: the following references will be eliminated/updated from here as the PReM interoperability profile
223   will be completed, as per the note in Clause 6.

224   [i.15]   ETSI TS 102 640-1: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail
225   (REM); Part 1: Architecture".

226   [i.16]   ETSI TS 102 640-2: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail
227   (REM); Part 2: Data requirements, Formats and Signatures for REM".

228   [i.17]   ETSI TS 102 640-5: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail
229   (REM); Part 5: REM-MD Interoperability Profiles".

230   [i.18]   ETSI TS 102 231: "Electronic Signatures and Infrastructures (ESI); Provision of harmonized
231   Trust-service status information".

232   [i.19]   ETSI TS 102 640-3: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail
233   (REM); Part 3: Information Security Policy Requirements for REM Management Domains".

234   [i.20]   ETSI TS 102 640-4: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail
235   (REM); Part 4: REM-MD Conformance Profiles".

236

3   Definitions, symbols and abbreviations

3.1   Definitions

For the purposes of the present document, the terms and definitions given in the following document apply.

    ETSI EN 319 532-1 [6]

3.2   Abbreviations

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

    ETSI EN 319 532-1 [6]

Furthermore, together with those included in the aforementioned documents, the following abbreviations apply:

REMID   REM interoperability domain
REMIDR   REM interoperability domain rules
UA   User Agent

250

3.3 Terminology

Due to the parallelism that there is between Registered Email Services and Electronic Delivery Registered Services, the present document uses the terms and definitions coming from ETSI EN 319 521 [1] and ETSI EN 319 522-* [3][4][5] family of documents. To indicate this affinity, when applicable, "ERD" prefix is inherited and used together the terms and their meanings coming from ETSI EN 319 532-2 [7] Clauses 3, 4 and - transitively - from its relevant connected normative references. When, for the purpose of the present document - due to the REM peculiarity or for clarity - this is not possible or opportune, the "REM" prefix is used instead in any definition. The key of interpretation is to consider "REM" prefix paired with "RED" and "REMS" (i.e. REM Service) with "ERDS".

NOTE: The prefix REM (without S) is used when the related object is relevant or may be relevant to something generated "outside" the REM Service. Conversely, the REMS prefix is used when it refers to an object that is produced by the REM Service.

262

263

4 Interoperability profile - general concepts

265

4.1 Introduction

The present document aims to provide a set of profiles in principle as intended in ISO/IEC TR 10000 [i.10], namely considering the essence of the profile definition there contained: "the identification of chosen classes, conforming subsets, options and parameters of base standards, or International Standardized Profiles necessary to accomplish a particular function". Furthermore, mainly due to the necessity to cover the interoperability profile relevant to REM service providers that use different formats and/or transport protocols (in particular SMTP vs. PReM), the concept of profile is extended to embrace other type of references (e.g. architectural, protocol detail, semantic and implementation aspects, as well as technical standard and service interoperability aspects).

And more specifically, other than the present section with generalities on profiling and conformance, two profiles are defined in the next sections:

a) The first for SMTP – it is rather a intra-operability profile acting, theoretically, on a pure and homogeneous environment.

b) The second is on PReM where interoperability between REM/SMTP and PReM/SOAP is addressed.

280

4.2 Compliance requirements

Requirements are grouped in three different categories, each one having its corresponding identifier. Table 1 defines these categories and their identifiers.

Table 1: Requirement categories

Identifier	Requirement to implement
M	System **shall** implement the element
R	System **should** implement the element
O	System **may** implement the element

285

All the requirements will be defined in tabular form.

287   **Table 2: Requirements template**

Nº	Service/Protocol element	EN reference	Requirement	Implementation guidance	Notes

288

289   Column **Nº** will identify a unique number for the requirements. This number will start from 1 in each clause. The
290   eventual references to it would also include the clause number to avoid any ambiguity.

291   Column **Service/Protocol element** will identify the service element or protocol element the requirement applies to.

292   Column **EN Reference** will reference the relevant clause of the standard where the element is defined. The reference is
293   to ETSI EN 319 522-1 [3], ETSI EN 319 522-2 [4], ETSI EN 319 532-1 [6] or ETSI EN 319 532-3 [8] except where
294   explicitly indicated otherwise.

295   Column **Requirement** will contain an identifier, as defined in table 1.

296   Column **Implementation guidance** will contain numbers referencing notes and/or letters referencing explanation of the
297   requirement. It is intended either to explain how the requirement is implemented or to include any other information not
298   mandatory.

299   Column **Notes** will contain additional notes to the requirement.

300   NOTE: Within one REMID may be in force provision different from the ones specified in the present document,
301   if and only if such REMID does not envisage to interoperate with other REMIDs.

302

5   SMTP interoperability profile

304

5.1   Introduction

306   This section of the document defines a profile for interoperability among REMSPs based on SMTP relay protocol.
307   Under this basis, although many aspects defined here are valid and reusable in other contexts, format and protocols, all
308   the sentences of the present part of the document mainly refer to interactions among REM services providers using - as
309   transfer protocol for REM messages - SMTP and its related updates, extensions and improvements (e.g. ESMTP or
310   SMTP-AUTH, etc.).

311

5.2   Style of operation

313   From an interoperability standpoint, no impact is expected to occur because of the adopted style of operation by a
314   REMS (Store and Forward vs. Store and Notify). Therefore, the present document shall deal with both on the same
315   profile..

316   The reason for that lies in the fact that any REM message exchanged between two REMSPs (even REM messages that
317   contain a reference to the REM Object in a Store-And-Notify context) is conveyed using the Relay Interface that, within
318   the present interoperability profile, is based on the SMTP protocol. Henceforth protocols, message formats and
319   evidence formats are the same in the two cases.

320   Then, all the Store-And-Notify systems also need a Store-And-Forward system that represents a common layer between
321   the two styles of operations.

322   Differences only arise in the set of mandatory evidence, which is specified within the two styles of operations, as
323   described in clause 5.6.

324

5.3   REMS - interfaces constraints

5.3.1   Introduction

The interfaces defined in ETSI EN 319 522-1 [3] and further detailed in ETSI EN 319 532-1 [6] Clause 5 are profiled as
follows in the next clauses of the present section.

5.3.2   ERDS MSI: Message Submission Interface

Nº	Service/Protocol element	ETSI EN 319 532-1 [6] reference	Requirement	Implementation guidance	Notes
1	Any protocol, provided that it is secured	Clause 5	M	a	

Implementation guidance:

a)   The Message Submission Interface **shall** be implemented using any protocol securing the communication from
     the originating mail User Agent to the SMTP server and paying special attention to identification,
     authentication, confidentiality, authenticity and integrity aspects. As an example, SMTP on TLS or SSL plus
     check of credential over SMTP-AUTH **may** be used.

5.3.3   ERDS MERI: Message and Evidence Retrieval Interface

Nº	Service/Protocol element	ETSI EN 319 522-1 [3] reference	Requirement	Implementation guidance	Notes
1	Any protocol, provided that it is secured	Clause 5	M	a	

Implementation guidance:

a)   The Message and Evidence Retrieval Interface **shall** be implemented using any protocol securing the
     communication from the sender/recipient mail User Agent to the REMSP server and paying special attention
     to identification, authentication, confidentiality, authenticity and integrity aspects. As an example IMAP or
     POP or HTTP on TLS or SSL **may** be used.

5.3.4   ERDS RI: Relay Interface

Nº	Service/Protocol element	ETSI EN 319 532-1 [6] reference	Requirement	Implementation guidance	Notes
1	SMTP on TLS	Clause 5	M	a	see note
NOTE: This is a profile for SMTP relay protocol among REMSPs and it is reflected in this requirement.					

Implementation guidance:

a)   The Relay Interface **shall** be implemented using SMTP protocol securing the communication from the sender
     REMSP server to the recipient REMSP server using TLS according to IETF RFC 3207 [9] taking so particular
     account on measures preserving confidentiality, authenticity and integrity.

5.3.5   CSI: Common Service Interface

The services used throughout this interface are not necessarily provided by a REMSP (see note) and, for the purpose of
the present profile, the following tree main elements shall be considered:

356   1.   Routing
357   2.   Trusting
358   3.   Discovery

359   NOTE: For this reason, the prefix ERDS is omitted before the definition of the interface.

360

Nº	Service/Protocol element	ETSI EN 319 532-3 [8] reference	Requirement	Implementation guidance	Notes
1	DNS	Clause 9	M	a	Routing i/f
2	TL	Clause 9	R	b	Trusting i/f
3	SML/SMP	Clause 9	O	c	Discovery i/f

361

362   Implementation guidance:

363   a)   The Routing Interface, part of CSI, **shall** be implemented using DNS protocol.

364   b)   The Trusting Interface, part of CSI, **should** be implemented using TL protocol.

365   c)   The Discovery Interface, part of CSI, **may** be implemented using SML/SMP protocols.

366   Editorial Note: The three interfaces above will be further specified more in depth, in the next developments of the
367   present document.

368

5.4   REMS - whole Headers constraints

5.4.1   REM message - Headers constraints

Nº	Service/Protocol element	ETSI EN 319 532-3 [8] reference	Requirement	Implementation guidance	Notes
1	X-REM-Msg-Type	Clause 6.2.1	R	a	
2	X-REM-<component>	Clause 6.2.1	R	b	

371

372   Implementation guidance:

373   a)   The headers list **should** contain an "X-REM-Msg-Type:" header specifying the type of the actual message. Its
374   value shall be one of those defined in Clause 6.2.1 of ETSI EN 319 532-3 [8].

375   b)   The headers list **should** contain at least three "X-REM-<component>:" headers specifying the following
376   couples components/values:

377   -   X-REM-*EvidenceIdentifier*: <value1>:   (i.e. *G01 - Evidence identifier* defined in clause 8.2.1 of ETSI
378   EN 319 522-2 [4]).

379   -   X-REM-*EventIdentifier*: <value2>:   (i.e. *G03 - Event identifier* defined in clause 8.2.3 of
380   ETSI EN 319 522-2 [4]).

381   -   X-REM-*ReasonIdentifier*: <value3>:   (i.e. *G04 - Reason identifier* defined in clause 8.2.4 of
382   ETSI EN 319 522-2 [4]).

383   Where the values **shall** be filled respectively as:

384   ▪   <value1> *the value of the evidence identifier "Id"* defined inside the Evidence root element
385   structure in clause 5.2.2.3 of ETSI EN 319 522-2 [4].

386   ▪   <value2> one of the values of the signigficant part of the *ERDSEventId* defined in clause 5.2.2.4
387   of ETSI EN 319 522-2 [4] as outlined in the second column "Event Identifier" of Table 3 of the
388   same document (e.g. *SubmissionAcceptance*, *SubmissionRejection*, etc.).

389   ▪   <value3> the significant part of the "Code" element URI of `EventReason` structure defined in
390   clause 5.2.2.6 of ETSI EN 319 522-2 [4] (e.g. MessageAccepted, InvalidMessageFormat, etc.).

NOTE 1: A list of these strings is obtained by the most right part of the URI listed in Table 4 of ETSI EN 319 522-2 [4].

NOTE 2: Items Nº 1 and Nº 2 in the table, at the top of the present paragraph, facilitate achieving of interoperability that, however, may also be reached without them.

5.4.2 REMS - signature Headers constraints

Nº	Service/Protocol element	ETSI EN 319 532-3 [8] reference	Requirement	Implementation guidance	Notes
1	Content-Type	Clause 6.2.3	M	a	
2	Content-Disposition	Clause 6.2.3	M	b	

Implementation guidance:

a) The Content-Type header field **shall** be present. The value of the header **shall** be "**application/pkcs7-signature**". An additional "name" parameter **shall** be provided with value "**smime.p7s**".

b) The Content-Disposition field **shall** be present. The value of the header **shall** be "**attachment**". An additional "filename" parameter **shall** be provided with value "**smime.p7s**".

Every REM message generated by a REMSP **shall** include the field Content-Disposition and fill in the name/filename parameters. To maximize the level of interoperability the REMSPs **shall** be able to correctly interpret incoming messages without the presence of Content-Disposition and/or name/filename parameters.

5.4.3 REMS - introduction Headers-Body constraints

Nº	Service/Protocol element	ETSI EN 319 532-3 [8] reference	Requirement	Implementation guidance	Notes
1	X-REM-Section-Type	Clause 6.2.4.1	M	a	

Implementation guidance:

a) An **X-REM-Section-Type** header **shall** be provided with value "**rem_message/introduction**".

5.4.3.1 multipart/alternative: free text subsection Header constraints

Nº	Service/Protocol element	ETSI EN 319 532-3 [8] reference	Requirement	Implementation guidance	Notes
1	Content-Type	Clause 6.2.4.2	R	a	

Implementation guidance:

a) The value for this field **shall** be: "text/plain;". It also is recommended that this field assumes also the value charset="UTF-8".

5.4.3.2 multipart/alternative: HTML subsection Header constraints

Nº	Service/Protocol element	ETSI EN 319 532-3 [8] reference	Requirement	Implementation guidance	Notes
1	Content-Type	Clause 6.2.4.3	R	a	

Implementation guidance:

a) The value for this field **shall** be: "text/html;". It also is recommended that this field assumes also the value charset="UTF-8".

420

5.4.4 REMS - extensions MIME section Headers constraints

The present optional extension of the REM message contains a XML attachment. The following restrictions apply.

Nº	Service/Protocol element	ETSI EN 319 532-3 [8] reference	Requirement	Implementation guidance	Notes
1	X-REM-Section-Type	Clause 6.2.5	M	a	

423

Implementation guidance:

     a)   When present, a **X-REM-Section-Type** header **shall** be provided with value "**rem_message/extension**".

426

5.4.5 ERDS evidence - MIME section Headers constraints

Nº	Service/Protocol element	ETSI EN 319 532-3 [8] reference	Requirement	Implementation guidance	Notes
1	X-REM-Section-Type	Clause 6.2.6.2	M	a	

428

Implementation guidance:

     a)   An **X-REM-Section-Type** header **shall** be provided with value "**rem_message/evidence**".

431

Nº	Service/Protocol element	ETSI EN 319 532-3 [8] reference	Requirement	Implementation guidance	Notes
2	Content-Type	Clause 6.2.6.2	M	a	

432

Implementation guidance:

     a)   The value for this field **shall** be: "application/xml;" and name/charset fields **shall** assume the values specified in ETSI EN 319 532-3 [8] Clause 6.2.6.2.

The present profile requires that the evidence in XML format (defined in Clause 7.4 of ETSI EN 319 532-3 [8]**) is present in all REM messages**.

Optionally the PDF format, a defined in Clause 6.2.6.3 of ETSI EN 319 532-3 [8], **may** be present.

     NOTE: If the optional evidence in PDF format carries an embedded XML structure, it replicates the data in the mandatory XML evidence.

441

5.5 REMS - user content constraints

5.5.1 original message MIME section Headers constraints

Nº	Service/Protocol element	ETSI EN 319 532-3 [8] reference	Requirement	Implementation guidance	Notes
1	X-REM-Section-Type	Clause 6.3.2	M	a	

444

Implementation guidance:

     a)   An **X-REM-Section-Type** header **shall** be provided with value "**rem_message/original**".

447

5.6   REMS - evidence set and components constraints

5.6.1   ERDS evidence types constraints

5.6.1.1   Mandatory evidence - all styles of operation

The following evidence types specified in the indicated clauses of ETSI EN 319 522-1 [3] are always required.

Nº	Service/Protocol element	ETSI EN 319 522-1 [3] reference	Requirement	Implementation guidance	Notes
1	SubmissionAcceptance	Clause 6.2.1 A.1	M	a	see note 1
2	SubmissionRejection	Clause 6.2.1 A.2	M	b	see note 1
3	ContentConsignment	Clause 6.2.4 D.1	M	c	see note 2
4	ContentConsignmentFailure	Clause 6.2.4 D.2	M	c	see note 2
5	ConsignmentNotification	Clause 6.2.4 D.3	M	c	see note 3
6	ConsignmentNotificationFailure	Clause 6.2.4 D.4	M	c	see note 3
NOTE 1: Rationale: The sender **shall** be aware of the successful/unsuccessful outcome of his/her message submission.					
NOTE 2: Rationale: The sender **shall** have evidence on whether the recipient was/was not made available (within the boundaries of recipient's REMSP) of the user content he/she sent (where the sender's REMSP style of operation is "S&F").					
NOTE 3: Rationale: The sender **shall** have evidence on whether the recipient was/was not made available (within the boundaries of recipient's REMSP) of the notification the sender's REMSP generated in relation to the original message (where the sender's REMSP style of operation is "S&N").					

452

Implementation guidance:

a) The sender's REMSP **shall** include the SubmissionAcceptance (obviously related to a successful submission) in the REM dispatch(es) to be forwarded to the final recipient(s).

b) The sender's REMSP **shall** include the SubmissionRejection (obviously related to an unsuccessful submission) in the REMS receipt to be sent back to the sender.

c) The recipient's REMSP **shall** send back to the sender a REM receipt including the evidence relevant to the event of delivery of the REM dispatch or REMS notification or REM payload.

460

5.6.1.2   Mandatory evidence - S&N style of operation

The following evidence types specified in the indicated clause of ETSI EN 319 522-1 [3] are always required for messages conveyed to the recipient by reference.

Nº	Service/Protocol element	ETSI EN 319 522-1 [3] reference	Requirement	Implementation guidance	Notes
1	ContentHandover	Clause 6.2.5 E.1	M	a	see note
2	ContentHandoverFailure				
NOTE: Rationale: The sender needs to have evidence on whether the recipient downloaded/non downloaded within a predefined time period the user content referenced in the notification.					

464

Implementation guidance:

a) The recipient's REMSP **shall** send back to the sender one REMS receipts including the ContentHandover or the ContentHandoverFailure.

468

5.6.1.3   Conditional evidence - all styles of operation

To the following evidence types, specified in the indicated clauses of ETSI EN 319 522-1 [3], the below specified conditions apply.

Nº	Service/Protocol element	ETSI EN 319 522-1 [3] reference	Requirement	Implementation guidance	Notes
1	RelayAcceptance	Clause 6.2.2 B1	Conditional "M"	a, b, c	see note
2	RelayRejection	Clause 6.2.2 B2	Conditional "M"	a, b, c	see note
3	RelayFailure	Clause 6.2.2 B3	Conditional "M"	d, e	see note
NOTE:	Rationale for both evidence types: the sender needs to know if the sent message did not successfully reach, or was rejected by, the recipient's REMSP, to enact possible backup measures.				

Implementation guidance for 1. and 2.:

a) Mandatory if:

- no opposite provision is explicitly specified in the applicable REMID rules;

- no previous opposite agreement exists between the involved REMSPs.

Such agreement or interoperability provision **should** specify one of the following:

I) The sender's REMSP will assume that a REM dispatch or payload has been rejected by the recipient's REMSP if no contrary indication is received within a predefined time period.

II) The sender's REMSP will assume that a REM dispatch or payload has been accepted by the recipient's REMSP if no contrary indication is received within a predefined time period.

Alternative conditions **may** be specified in the above agreement provided that the issue is exhaustively dealt with b) or c):

b) If the evidence type under consideration is mandatory, the recipient's REMSP **shall** send back to the sender's REMSP a REM receipt including the RelayAcceptance or RelayRejection evidence.

c) In the cases addressed in the previous item I) and item II), the sender's REMSP **shall** build a REM receipt including respectively the RelayRejection or the RelayAcceptance evidence and **shall** send it to the sender.

Implementation guidance for 3.:

d) Mandatory if no opposite requirement within REMID exists.
Such interoperability requirement **should** specify that, if no contrary indication is received within a predefined time period, it is to be assumed that it was impossible to deliver a REM dispatch or payload within a given time period to the recipient's REMSP, due to any kind of problems.

Alternative conditions **may** be specified in the above interoperability requerement, provided that the issue is exhaustively dealt with e):

e) The sender's REMSP **shall** build a REM receipt, including the RelayFailure evidence and **shall** send it back to the sender.

5.6.2   ERDS evidence components constraints

In the following clauses, details on the Evidence components coming from ETSI EN 319 522-2 [4] Clause 8 are listed (in the third columns of each table) for each mandatory evidence type indicated in above clauses from 5.6.1.1 through 5.6.1.3. The modelling adopted in the tables defined in the following clauses differs from that used so far. More in detail, the following clauses list all Evidence components that are required to ensure interoperability, including those that in in Table 13 ETSI EN 319 522-2 [4] Clause 8.4 are already indicated as mandatory or whose absence implies a default value.

NOTE: This different approach has been adopted to give a more complete and comfortable view to the reader.

5.6.2.1   SubmissionAcceptance - SubmissionRejection

Nº	Evidence element	ETSI EN 319 522-2 [4] Clause 8 - reference	Requirement	Implementation guidance	Notes
1	Evidence identifier	G01	M		see note 1
2	Event identifier=SubmissionAcceptance or SubmissionRejection	G03	M		see note 1
3	Reason identifier	G04	M		
4	Reason code	G04	M (1..N)	a	
5	Evidence version	G02	M		see note 1
6	Event time	G05	M		see note 1
7	Evidence issuer policy identifier	R01	M (1..N)		see note 1
8	Evidence issuer details	R02	M		see note 1
9	Sender's identifier	I02	M		see note 1
10	Recipient's identifier	I04	M (1..N)		see note 1
11	Sender 's identity assurance details	I08	O	b	see note 1
12	user content information	M02	M		see note 1
13	Reply-to	MD09	M	c	
14	Submission date and time	M03	M	d	
NOTE 1: Readers are reminded that this requirement is present as mandatory in Table 13 ETSI EN 319 522-2 [4] Clause 8.4.					

509

510 Implementation guidance:

511 a) At least one Reason code **shall** be present, unless the applicable REMIDs explicitly require that when
512 submission is regularly accepted no Reason code is necessary. Multiple Reason code **may** be present
513 depending on the found exceptions.

514 b) If this field is not present it means that the class of authentication is Basic. In the other cases it specifies the
515 class of Authentication according to the semantic of ETSI EN 319 522-2 [4] Clause 5.5.

516 c) This field **shall** be present containing the email address of the original sender, unless the applicable REMIDs
517 explicitly require that no Reply-to is necessary.

518 d) This field **shall** be present.

519 ## 5.6.2.2 ContentConsignment - ContentConsignmentFailure

Nº	Evidence element	ETSI EN 319 522-2 [4] Clause 8 - reference	Requirement	Implementation guidance	Notes
1	Evidence identifier	G01	M		see note
2	Event identifier=ContentConsignment or ContentConsignmentFailure	G03	M		see note
3	Reason identifier	G04	M		
4	Reason code	G04	M (1..N)	a	
5	Evidence version	G02	M		see note
6	Event time	G05	M		see note
7	Evidence issuer policy identifier	R01	M (1..N)		see note
8	Evidence issuer details	R02	M		see note
9	Sender's identifier	I02	M		see note
10	Recipient's identifier	I04	M (1..N)		see note
11	Recipient referred to by the evidence	I07	M	b	
12	user content information	M02	M		see note
13	Message type	MD13	R	c	
NOTE: Readers are reminded that this requirement is present as mandatory in Table 13 ETSI EN 319 522-2 [4] Clause 8.4.					

520

521 Implementation guidance:

522 a) At least one Reason code **shall** be present, unless the applicable REMIDs explicitly require that when
523 consignment regularly occurred no Reason code is necessary. Multiple Reason code **may** be present depending
524 on the found exceptions:

525 b) This field **shall** be present.

526 c) This field **should** be present according to the semantic of ETSI EN 319 522-2 [4] Clause 6.2.13.

527

528 5.6.2.3   ContentHandover - ContentHandoverFailure

Nº	Evidence element	ETSI EN 319 522-2 [4] Clause 8 - reference	Requirement	Implementation guidance	Notes
1	Evidence identifier	G01	M		see note
2	Event identifier=ContentHandover or ContentHandoverFailure	G03	M		see note
3	Reason identifier	G04	M		
4	Reason code	G04	M (1..N)	a	
5	Evidence version	G02	M		see note
6	Event time	G05	M		see note
7	Evidence issuer policy identifier	R01	M (1..N)		see note
8	Evidence issuer details	R02	M		see note
9	Sender's identifier	I02	M		see note
10	Recipient's identifier	I04	M (1..N)		see note
11	Recipient referred to by the evidence	I07	M	b	
12	Recipient Authentication details	I05	O	c	
13	user content information	M02	M		see note
NOTE: Readers are reminded that this requirement is present as mandatory in Table 13 ETSI EN 319 522-2 [4] Clause 8.4.					

529

530 Implementation guidance:

531 a) At least one Reason code **shall** be present, unless the applicable REMIDs explicitly require that when
532   download regularly occurred no Reason code is necessary. Multiple Reason code **may** be present depending
533   on the found exceptions.

534 b) This field **shall** be present.

535 c) If this field is not present it means that the class of authentication is Basic. In the other cases, it specifies the
536   class of Authentication.

537 5.6.2.4   RelayAcceptance - RelayRejection

Nº	Evidence element	ETSI EN 319 522-2 [4] Clause 8 - reference	Requirement	Implementation guidance	Notes
1	Evidence identifier	G01	M		see note
2	Event identifier=RelayAcceptance or RelayRejection	G03	M		see note
3	Reason identifier	G04	M		
4	Reason code	G04	M (1..N)	a	
5	Evidence version	G02	M		see note
6	Event time	G05	M		see note
7	Evidence issuer policy identifier	R01	M (1..N)		see note
8	Evidence issuer details	R02	M		see note
10	Sender's identifier	I02	M		see note
11	Recipient's identifier	I04	M (1..N)		see note
12	Recipient referred to by the evidence	I07	M		see note
13	user content information	M02	M		see note
14	Message Type	MD13	R	b	
NOTE: Readers are reminded that this requirement is present as mandatory in Table 13 ETSI EN 319 522-2 [4] Clause 8.4.					

538

539 Implementation guidance:

540 a) At least one Reason code **shall** be present, unless the applicable REMIDs explicitly require that when the relay
541   to the recipient's REMSP regularly occurred no Reason code is necessary. Multiple Reason code **may** be
542   present depending on the found exceptions.

543 b) This field **should** be present according to the semantic of ETSI EN 319 522-2 [4] Clause 6.2.13.

544

5.6.2.5 RelayFailure

Nº	Evidence element	ETSI EN 319 522-2 [4] Clause 8 - reference	Requirement	Implementation guidance	Notes
1	Evidence identifier	G01	M		see note
2	Event identifier=RelayFailure	G03	M		see note
3	Reason identifier	G04	M		
4	Reason code	G04	M (1..N)	a	
5	Evidence version	G02	M		see note
6	Event time	G05	M		see note
7	Evidence issuer policy identifier	R01	M (1..N)		see note
8	Evidence issuer details	R02	M		see note
9	Sender's identifier	I02	M		see note
11	Recipient's identifier	I02	M (1..N)		see note
12	Recipient referred to by the evidence	I07	M		see note
13	user content information	M02	M		see note
14	Message Type	MD13	R	b	
NOTE: Readers are reminded that this requirement is present as mandatory in Table 13 ETSI EN 319 522-2 [4] Clause 8.4.					

546

547 Implementation guidance:

548   a)   At least one Reason code **shall** be present, unless the applicable REMIDs explicitly require that when relay to
549   the recipient's REMSP failed no Reason code is necessary.Multiple Reason code **may** be present depending on
550   the found exceptions.

551   b)   This field **should** be present according to the semantic of ETSI EN 319 522-2 [4] Clause 6.2.13.

552

6 REMS UPU interoperability profile

554 Editorial Note: The text of the present Clause 6 refers to the interoperability profile REM / PReM, and completely
555 comes from ETSI TS 102 640-6-1: "Registered Electronic Mail (REM); Part 6-1: REM-MD UPU PReM
556 Interoperability Profiles".
557 A set of first few changes were made to the text below for begin to adapt it to the new ETSI EN REM Specifications
558 (e.g. use of REMS instead of REM-MD). The original text from ETSI TS 102 640-6-1 defined an interoperability
559 profile based on UPU S52-1: "Functional specification for postal registered electronic mail (PReM)".
560 Since the UPU S52-1 PReM Technical Specification had the messages and evidence set formats inherited from ETSI
561 TS 102 640 REM specification, the old interoperability profile was facilitated by this close relationship.
562 Now, in new ETSI EN REM Specification both message and evidence formats have been updated to be adapted to the
563 new EU regulation requirements. As a consequence, the old aforementioned interoperability profile is no more
564 applicable as it is to the new ETSI EN REM.
565 The following remains an open item that ESI TB, UPU and CEN TC 331 are discussing:
566 - would an interoperability profile between the new ETSI EN REM and the currently available UPU S52-1 be useful?
567 - or should ESI TB wait for an update of UPU S52-1 before working on a new interoperability profile?
568 It is thus important to understand the direction and schedule of the evolution of UPU S52-1 PReM Technical
569 Specification to enable ESI TB to complete, in a comprehensive way, the interoperability profile, subject of the present
570 clause, between the new REM and the old or the new PReM (e.g. know if the new PReM aims to inherit the message
571 and evidence set formats of the new REM as for the past).
572 For making this process smoother, by increasing the operational and approval flexibility, the ESI TB is considering the
573 possibility of moving this section from the present EN document to a separate Technical Specification entirely
574 dedicated to this interoperability profile.
575 For all these evident issues, the content of the present section of the document needs to be further re-harmonized
576 according to the information that will be available about the PReM evolution and the relevant milestones.

577

6.1 Mapping of terms and definitions

579 In Table 1 a mapping among the main terms and definitions used in REM Technical specifications ETSI TS 102 640-1
580 [i.15], ETSI TS 102 640-2 [i.16], ETSI TS 102 640-3 [i.19], ETSI TS 102 640-4 [i.20], ETSI TS 102 640-5 [i.17] and
581 equivalent terms used in PReM UPU [11] specification is provided. An empty cell means that the corresponding
582 specification does not define an equivalent term of the one shown in the same row and defined in the other
583 specification.

584 **Table 1: Mapping of definitions**

ETSI REM definitions	UPU PReM definitions
certification authority	
information security policy	
Information Security Management System	
long term storage	
message archive	Message Store + Evidence Store
original message	PReM Object
REMS repository	Directory Server+Evidence Store+Message Store
Registered E-Mail	Postal Registered eMail
REM dispatch	PReM Message
REM Service Provider	Designated Operator
REMS envelope	Signed part of PReM Message
REMS evidence	Evidence
REMS Evidence Provider	Designated Operator
REMS Evidence Verifier	Designated Operator
REM message	PReM Message
REMS Message Gateway	Designated Operator
REMS Message Transfer Agent	
REMS Repository Retrieval Interface	
REMS Sender Message Submission Interface	
REMS Third Party Evidence Retrieval Interface	
REM Message Store	Message Store
REM Object	PReM Object or PReM Message or PReM Dispatch
REM Objects Relay Interface	
REM User Agent (REM-UA)	Web-browser/email client software
REM Policy	PReM policy
REM interoperability domain	UPU PReM group
REM interoperabilty domain Authority	UPU
REM Recipient	Addressee / Mailee
REM Sender	Mailer
REM Third Party	Authorized party
Signature Creation Server	
Time-Stamping Authority	
Time-Stamp Token	
	Notification
	Designated Operator Trust List

585

6.2 Mapping of boundary roles

587 For the purposes of the present document only the boundary elements of both systems **shall** be considered. In particular,
588 as outlined in Figure 1, the main roles involved in the interactions are: REMSPs, Designated Operators, Trusted Lists. A
589 new element is needed to cover the gap between the two systems: it is called REM/PReM Gateway.

590 The REM/PReM Gateway **shall** act with double role: it **shall** be considered as a generic REMSP when the
591 intercommunication is between REM network ←→ REM/PReM Gateway; in a similar way, the REM/PReM Gateway
592 **shall** be considered as one of the Designated Operators of the UPU/PReM network when the intercommunication is
593 between REM/PReM Gateway ←→ PReM network.

6.3 Functional GAP analysis between REM and PReM

595 The main differences between the functional aspects of ETSI REM and UPU PReM will be identified in this clause by
596 comparing, when possible, the similar aspects of the two systems under analysis.

597 The format of the exchanged messages in the REM model to which the present document refers is based on the MIME
598 standard (RFC 5751 [i.13]) enriched with a set of typical Headers of the SMTP (RFC 5321 [i.11]) messaging protocol.

599 Clause 6.1 of TS 102 640-1 [i.15] and clause 5.1 of TS 102 640-2 [**i**.16] define the "Events" and the corresponding
600 "Evidence" produced for each of these events.

601 Sections 5.2 and 7.2 of UPU PReM Technical Specification [11] define a functional description of the PReM service
602 flow.

603 Each event/evidence is associated to a function and a mapping between functions is identified in the following tables.
604 The attention is concentrated to the boundary functions that are involved in the gateway among REM and PReM
605 systems. Anyway, some other remarkable function is inserted in the table to provide a more general view when
606 significant for the interoperability.

607 The analysis is organized in a table with two columns where the first one **always** contains a list of the events and
608 relevant evidence of the flows of a **REM system**. The second column **always** contains a similar list with corresponding
609 functions of a PReM system. The order of the contents (cells of left/right) does not depend on the direction of the flow.
610 There is a correspondence between the two systems comparing, line by line, the left cell with right cell. When possible
611 the events/evidence/functions are grouped for analogy of meaning. Events or functions that are not present in one of the
612 two systems are identified in the comments. Internal events/functions that are not relevant for interoperability are
613 neglected in this analysis.

614 **Table 2: GAP Analysis - Transmission/Relay/Delivery - REMSP → DO**

Opr.	ETSI REM Events (TS 102 640-1 [i.15], clause 6.2) and Evidence (TS 102 640-2 [i.16], clause 5.1)	UPU PReM functions, events, and descriptions (UPU PReM Technical Specification [11], sections 5.2 and 8.3)
Transmission / Relay / Delivery (Orig. REMSP→Dest. DO)	*Function*: **Relay** This is the general operation (performed from a REMSP to a destination Designated Operator) to convey a REMS Message containing the Sender's message. To cover the gap among the two systems, the operation requires a gateway.	*Function/Method:* **SendMessageToDestination** This is the real function invoked from the REM/PReM Gateway that, **when executed at DO side**, allows PReM Message to be sent to DO of Destination.
	Function: **Relay** This is the general operation (performed from the Recipient's Designated Operator to Sender's REMSP) to convey a REMS Message containing an evidence relevant to a Sender's message. To cover the gap among the two systems, the operation requires a gateway.	*Function/Method*: **SubscribeNotification** This is the real function that allows the REM/PReM Gateway system to **subscribe** certain PReM events, and to be **notified** through a call to the ReceiveNotification function, when these events occur.
	Events: 6.2.2 Event B.1 - R-REMS Acceptance 6.2.2 Event B.2 - R-REMS Rejection This event occurs at Sender's REMSP side in consequence of the **result** of the relay operation.	*Events:* Events 5.1, in the Workflow Process of Figure 3, interpreted as result of the SendMessageToDestination execution (relay operation) for Receive/NotReceive the message conveyed from a Sender's REMSP to a Recipient's DO.

Opr.	ETSI REM Events (TS 102 640-1 [i.15], clause 6.2) and Evidence (TS 102 640-2 [i.16], clause 5.1)	UPU PReM functions, events, and descriptions (UPU PReM Technical Specification [11], sections 5.2 and 8.3)
	Evidence: 5.1.2 Evidence RelayToREMMDAcceptanceRejection The responsible for issuance of this recommended evidence should be the Recipient's DO but it is not present in the workflow of section 5.2.3 of PReM UPU [11] TS. The REM/PReM Gateway **shall** generate such evidence for the Sender, on behalf of the Recipient's DO, using as input the result of the SendMessageToDestination operation.	*Evidence:* EFW-DSP-ACC/REJDOD Evidence of Forward - Acceptance/Rejection - DOD #4 Table 4 section 8.3 of PReM UPU [11] TS. This evidence seems equivalent to the required RelayToREMMDAcceptanceRejection but it is not issued by a DO and it is only logged.
	Event: 6.2.2 Event B.3 - Expiration of time to deliver to R-REMS This event occurs at Sender's REMSP side when the attempts of relay within a fixed interval of time fail completely.	*Event:* This event makes sense at Sender's REMSP side, so it is not considered here.
	Evidence: 5.1.3 Evidence RelayToREMMDFailure The responsible for issuance of this evidence is the Sender's REMSP and the recipient of the evidence is the Sender.	*Evidence:* In the flow direction under analysis an evidence like that indicated in the left cell makes sense only at Sender's REMSP side and so it is not considered here.
	Events: 6.2.3 Event C.1 - Message Delivery	*Events:* Event 5.8 of the Workflow Process of section 5.2.3 of PReM UPU [11] TS (summarized in Figure 3 of the present document) for Acceptance/Non-Acceptance of the message conveyed from the Sender's REMSP to the Recipient's DO.
	Evidence: 5.1.4 Evidence DeliveryNonDeliveryToRecipient	*Evidence:* E-DSP-ACC/REJ-DOD Evidence of PReM Dispatch Acceptance/Rejection - DOD #27 Table 4 section 8.3. of PReM UPU [11] TS. The responsible for issuance of this evidence is the Recipient's DO. The 'DeliveryNonDeliveryToRecipient' evidence **shall** be notified to the Sender's REMSP, via the call-back function subscribed at REM/PReM Gateway level, by means of the ReceiveNotification. The function ReceiveNotification is invoked by the Recipient's DO and executed at REM/PReM Gateway level.
	Event: 6.2.3 Event C.2 - Expiration of time to deliver message This event occurs at Sender's REMSP side when no positive delivery evidence for a sent message is received in a fixed time.	*Event:* In this profile, this event makes sense only at Sender's REMSP side, so it is not considered here.

Opr.	ETSI REM Events (TS 102 640-1 [i.15], clause 6.2) and Evidence (TS 102 640-2 [i.16], clause 5.1)	UPU PReM functions, events, and descriptions (UPU PReM Technical Specification [11], sections 5.2 and 8.3)
	Evidence: 5.1.4 Evidence DeliveryNonDeliveryToRecipient The responsible for issuance of this evidence is the Sender's REMSP and the recipient of the evidence is the Sender.	*Evidence:* In this profile an evidence like that indicated in the left cell makes sense only at Sender's REMSP side and so it is not considered here.

615

616   **Table 3: GAP Analysis - Transmission/Relay/Delivery - DO → REMSP**

Opr	ETSI REM Events (TS 102 640-1 [i.15], clause 6.2) and Evidence (TS 102 640-2 [i.16], clause 5.1)	UPU PReM functions, events and descriptions (UPU PReM Technical Specification [11], sections 5.2 and 8.3)
Transmission / Relay / Delivery (Orig. DO → Dest. REMSP)	*Function:* **Relay** This is the general operation (performed from a Designated Operator to a destination REMSP) to convey a REMS Message containing the Sender's message. To cover the gap among the two systems, the operation requires a gateway.	*Function/Method:* **SendMessageToDestination** This is the real function invoked from the Sender's DO that, when executed at REM/PReM Gateway side, allows PReM Message to be sent to the REMSP of Destination.
	Function: **Relay** This is the general operation (performed from a REMSP to a Designated Operator) to convey a REMS Message containing an evidence relevant to a Sender's message. To cover the gap among the two systems, the operation requires a gateway.	*Function/Method:* **ReceiveNotification**: This is the real function subscribed from Sender's DO that, when invoked from Recipient's REM/PReM Gateway, allows REMSP system to notify certain REMS Events when these occur. The execution of the ReceiveNotification function happens at Sender's Designated Operator side.
	Events: 6.2.2 Event B.1 - R-REMS Acceptance 6.2.2 Event B.2 - R-REMS Rejection This event occurs at Recipient's REMSP side in consequence of the **execution** of the relay operation.	*Events:* Events 5.1 in the Workflow Process of section 5.2.3 of PReM UPU [11] TS (summarized in Figure 3 of the present document) interpreted as consequence of the execution of relay operation (at REM/PReM Gateway side) for Receive/NotReceive the message conveyed from the Sender's DO to the Recipient's REMSP. The event is the result of the SendMessageToDestination operation executed at REM/PReM Gateway level.
	Evidence: 5.1.2 Evidence RelayToREMMDAcceptanceRejection In REM network, the responsible for issuance of this recommended evidence is the Recipient's REMSP and the primary intended recipient is the Sender's REMSP (in this particular flow it is a Sender's DO). Since the workflow of section 5.2.3 of PReM UPU [11] TS does not have this evidence at Sender's DO side (this means that it is not expected nor recognized), it may be simply logged at REM/PReM Gateway side, and not sent back to the Sender's DO.	*Evidence:* EFW-DSP-ACC/REJDOD Evidence of Forward - Acceptance/Rejection - DOD #4 Table 4 section 8.3 of PReM UPU [11] TS. This evidence is substantial equivalent to the required RelayToREMMDAcceptanceRejection but, in the workflow of section 5.2.3 of PReM UPU [11] TS, it is only logged and not issued. This means that an evidence of this type, coming from a REM network through the REM/PReM Gateway, would not be recognized by the Sender's DO. So, even if it is generated in the REM network, it **shall** be only logged in the REM/PReM Gateway.

Opr	ETSI REM Events (TS 102 640-1 [i.15], clause 6.2) and Evidence (TS 102 640-2 [i.16], clause 5.1)	UPU PReM functions, events and descriptions (UPU PReM Technical Specification [11], sections 5.2 and 8.3)
	Event: 6.2.2 Event B.3 - Expiration of time to deliver to R-REMS This event makes sense when the Sender's operator is a REMSP.	*Event* This event makes sense when the Sender's operator is a REMSP.
	Evidence: 5.1.3 Evidence RelayToREMMDFailure This event makes sense when the Sender's operator is a REMSP.	*Evidence*: This evidence makes sense when the Sender's operator is a REMSP.
	Events: 6.2.3 Event C.1 - Message Delivery	*Events*: Event 6.1 of the Workflow Process of section 5.2.3 of PReM UPU [11] TS (summarized in Figure 3 of the present document) for Acceptance/Non-Acceptance of the message conveyed from the Sender's DO to the Recipient's REMSP.
	Evidence: 5.1.4 Evidence DeliveryNonDeliveryToRecipient The responsible for issuance of this evidence is the Recipient's REMSP. The 'DeliveryNonDeliveryToRecipient' evidence **shall** be **notified** to the Sender's DO, via the call-back function subscribed at Sender's DO level, by means of the ReceiveNotification. The function ReceiveNotification is invoked by the REM/PReM Gateway (when the event C.1 occurs at Recipient's REMSP) and executed at Sender's DO level.	*Evidence*: E-DSP-ACC/REJ-DOD Evidence of PReM Dispatch Acceptance/Rejection - DOD #27 Table 4 section 8.3 of PReM UPU [11] TS. The evidence 'DeliveryNonDeliveryToRecipient' **shall** be received by the Sender's DO executing the ReceiveNotification function invoked by the REM/PReM Gateway, as indicated in the left cell.
	Event: 6.2.3 Event C.2 - Expiration of time to deliver message This event makes sense when the Sender's operator is a REMSP.	*Event* In this profile, this event makes sense only at Sender's REMSP side.
	Evidence: 5.1.4 Evidence DeliveryNonDeliveryToRecipient This evidence makes sense when the Sender's operator is a REMSP.	*Evidence*: In this profile, this evidence makes sense only at Sender's REMSP side.

617

618   **Table 4: GAP Analysis - Retrieval - REMSP → DO**

Opr	ETSI REM Events (TS 102 640-1 [i.15], clause 6.2) and Evidence (TS 102 640-2 [i.16], clause 5.1)	UPU PReM functions, events and descriptions (UPU PReM Technical Specification [11], sections 5.2 and 8.3)
Retrieval (Orig. REMSP→Dest. DO)	*Function*: **Retrieval** The retrieval operation (performed at Designated Operator level) generates some evidence relevant to a Sender's message. To cover the gap among the two systems, the operation requires a gateway.	*Function/Method*: **SubscribeNotification** This is the real function that allows the REM/PReM Gateway system to **subscribe** certain PReM events, and to be **notified** through a call to the ReceiveNotification function, when these events occur.
	Function: **Retrieval** The retrieval operation (performed from a Designated Operator level) generates some evidence relevant to a Sender's message. To cover the gap among the two systems, the operation requires a gateway.	*Function/Method*: **RejectMessage** The Recipient **may** explicitly **Rejects** the message with **RejectMessage** function. This is the real function that allows PReM system to **notify** REM Senders, through a gateway, the Recipient's rejection of the message.
	Events: 6.2.3 Event F.1 (mailbox) - Retrieval	*Events*: Event 9.3 in the Workflow Process of section 5.2.3 of PReM UPU [11] TS for Retrieval of the message conveyed from the Sender's REMSP to the Recipient's DO. The Recipient explicitly **Rejects** the message with the invocation of the **RejectMessage** function. The RejectMessage function is translated in the proper evidence (Mailee **#31** Table 4 section 8.3 of PReM UPU [11] TS) notified by the Recipient's DO invoking the ReceiveNotification function. This event is mapped with the 'AcceptanceRejectionByRecipient' REMS Evidence. The Recipient **Accepts** the message and **Retrieves** it with **RetrieveResult** function: these two functions are available in REM system and they are related to the event F.1.

Opr	ETSI REM Events (TS 102 640-1 [i.15], clause 6.2) and Evidence (TS 102 640-2 [i.16], clause 5.1)	UPU PReM functions, events and descriptions (UPU PReM Technical Specification [11], sections 5.2 and 8.3)
	Evidence: 5.1.6 Evidence RetrievalNonRetrievalByRecipient	*Evidence*: E-MSG-ADRDLV/NDL-DOD Evidence of Delivery/Non-delivery - Addressee/Mailee **#29** Table 4 section 8.3 of PReM UPU [11] TS. E-MSG-ADR-REJDOD Evidence of Reject - Addressee/Mailee **#31** Table 4 section 8.3 of PReM UPU [11] TS. The responsible for issuance of "Retrieval" optional evidence is the Recipient's DO. The evidence **shall** be **notified** to the Sender's REMSP, via the call-back function subscribed at REM/PReM Gateway level, by means of the ReceiveNotification function invoked by the Recipient's DO (Event 10.4 in the Workflow Process of section 5.2.3 of PReM UPU [11] TS). The responsible for issuance of "Reject" optional evidence is the Recipient's DO. It **shall** be **notified** to the Sender's REMSP, via the call-back function subscribed at REM/PReM Gateway level, by means of the ReceiveNotification function invoked by the Recipient's DO (Event 10.4 in the Workflow Process of section 5.2.3 of PReM UPU [11] TS).
	Events: 6.2.3 Event F.2 (mailbox) - Expiration of time for Retrieval	*Events*: Event 9.3 in the Workflow Process of section 5.2.3 of PReM UPU [11] TS for Retrieval of the message conveyed from the Sender's REMSP to the Recipient's DO. The Recipient **Ignores** the message and it expires: This behaviour is available in REM system and it is related to the event F.2.
	Evidence: 5.1.6 Evidence RetrievalNonRetrievalByRecipient	*Evidence*: 30 E-MSG-ADR-EXPDOD Evidence of PReM Message Expiration - Addressee/Mailee. The responsible for issuance of "Expiration" optional evidence is the Recipient's DO. It **shall** be **notified** to the Sender's REMSP, via the call-back function subscribed at REM/PReM Gateway level, by means of the ReceiveNotification function invoked by the Recipient's DO.

619

620   **Table 5: GAP Analysis - Retrieval - DO →REMSP**

Opr	ETSI REM Events (TS 102 640-1 [i.15], clause 6.2) and Evidence (TS 102 640-2 [i.16], clause 5.1)	UPU PReM functions, events and descriptions (UPU PReM Technical Specification [11], sections 5.2 and 8.3)
Retrieval (Orig. DO → Dest. REMSP)	*Function*: **Retrieval** The retrieval operation (performed at REMSP level) generates some evidence relevant to a Sender's message. To cover the gap among the two systems, the operation requires a gateway.	*Function/Method*: **ReceiveNotification**: This is the real function subscribed from Sender's DO that, when invoked from Recipient's REM/PReM Gateway, allows REMSP system to notify certain REMS Events when these occur. The execution of the ReceiveNotification function happens at Sender's Designated Operator side.
	Events: 6.2.3 Event F.1 (mailbox) - Retrieval This event occurs at Recipient's REMSP side in consequence of the **execution** of the retrieval operation.	*Events*: Event 11.1 in the Workflow Process of section 5.2.3 of PReM UPU [11] TS (summarized in Figure 3 of the present document) to receive the notification of the message retrieved at Recipient's REMSP side.
	Evidence: 5.1.6 Evidence RetrievalNonRetrievalByRecipient In REM network, the responsible for issuance of this optional evidence is the Recipient's REMSP and the primary intended recipient is the Sender (in this particular flow it is a PReM sender). The RetrievalNonRetrievalByRecipient evidence, when issued, **shall** be **notified** to the Sender's DO (that after will notify this evidence to the intended PReM sender), via the call-back function subscribed at Sender's DO level, by means of the ReceiveNotification. The function ReceiveNotification is invoked by the REM/PReM Gateway (when the event F.1 occurs at Recipient's REMSP side) and executed at Sender's DO level.	*Evidence*: E-MSG-ADRDLV/NDL-DOD Evidence of Delivery/Non-delivery - Addressee/Mailee **#29** Table 4 section 8.3 of PReM UPU [11] TS. E-MSG-ADR-REJDOD Evidence of Reject - Addressee/Mailee **#31** Table 4 section 8.3 of PReM UPU [11] TS. The responsible for issuance of "Retrieval" optional evidence is the Recipient's REMSP. The RetrievalNonRetrievalByRecipient **shall** be mapped, at REM/PReM Gateway level, to one of the above PReM evidence types according to REM Evidence Event Code.
	Events: 6.2.3 Event F.2 (mailbox) - Expiration of time for Retrieval	*Events*: Event 9.3 in the Workflow Process of section 5.2.3 of PReM UPU [11] TS for Retrieval of the message conveyed from the Sender's REMSP to the Recipient's DO. The Recipient **ignores** the message and it expires: This behaviour is available in REM system and it is related to the event F.2.

Opr	ETSI REM Events (TS 102 640-1 [i.15], clause 6.2) and Evidence (TS 102 640-2 [i.16], clause 5.1)	UPU PReM functions, events and descriptions (UPU PReM Technical Specification [11], sections 5.2 and 8.3)
	Evidence: 5.1.6 Evidence RetrievalNonRetrievalByRecipient In REM network, the responsible for issuance of this optional evidence is the Recipient's REMSP and the primary intended recipient is the Sender (in this particular flow it is a PReM sender). The RetrievalNonRetrievalByRecipient evidence, when issued, **shall** be **notified** to the Sender's DO (that after will notify this evidence to the intended PReM sender), via the call-back function subscribed at Sender's DO level, by means of the ReceiveNotification. The function ReceiveNotification is invoked by the REM/PReM Gateway (when the event F.2 occurs at Recipient's REMSP side) and executed at Sender's DO level.	*Evidence*: 30 E-MSG-ADR-EXPDOD Evidence of PReM Message Expiration - Addressee/Mailee. The responsible for issuance of "Expiration" optional evidence is the Recipient's REMSP. It **shall** be notified to the Sender's DO, via the call-back function subscribed by Sender's DO, by means of the ReceiveNotification function invoked by the REM/PReM Gateway. The responsible for issuance of "Expiration" optional evidence is the Recipient's REMSP. The RetrievalNonRetrievalByRecipient **shall** be mapped, at REM/PReM Gateway level, to PReM evidence indicated above.

## 6.4 High level definition of the inter-communication flows between REM and PReM

6.4.1 Agreements

The interchange among a PReM system and a REM system is governed by an agreement among at least one REM Service Provider and one UPU Designated Operator. This agreement is part of a more high-level agreement among a UPU PReM Policy Domain and a REM interoperability domain (the REM terms are used in this context but the designated authorities are present behind these terms). The first Policy Domain, PReM-PD, represents the environment (common set of rules) of the universe PReM. The second interoperability domain, REMID, defines the space within which it has life the particular instance of REM to put in communication with the PReM. From the technical point of view, the agreement among the UPU PReM Policy Domain and a REM interoperability domain requires the application of the present technical specification that provides the support for the interoperability. Whereas, regarding the operational level, the agreement among REMSPs and DOs is concretised with a registration inside a special trusted index. These indexes **shall** be secured and trusted with an implementation like that defined in clause 6.8.
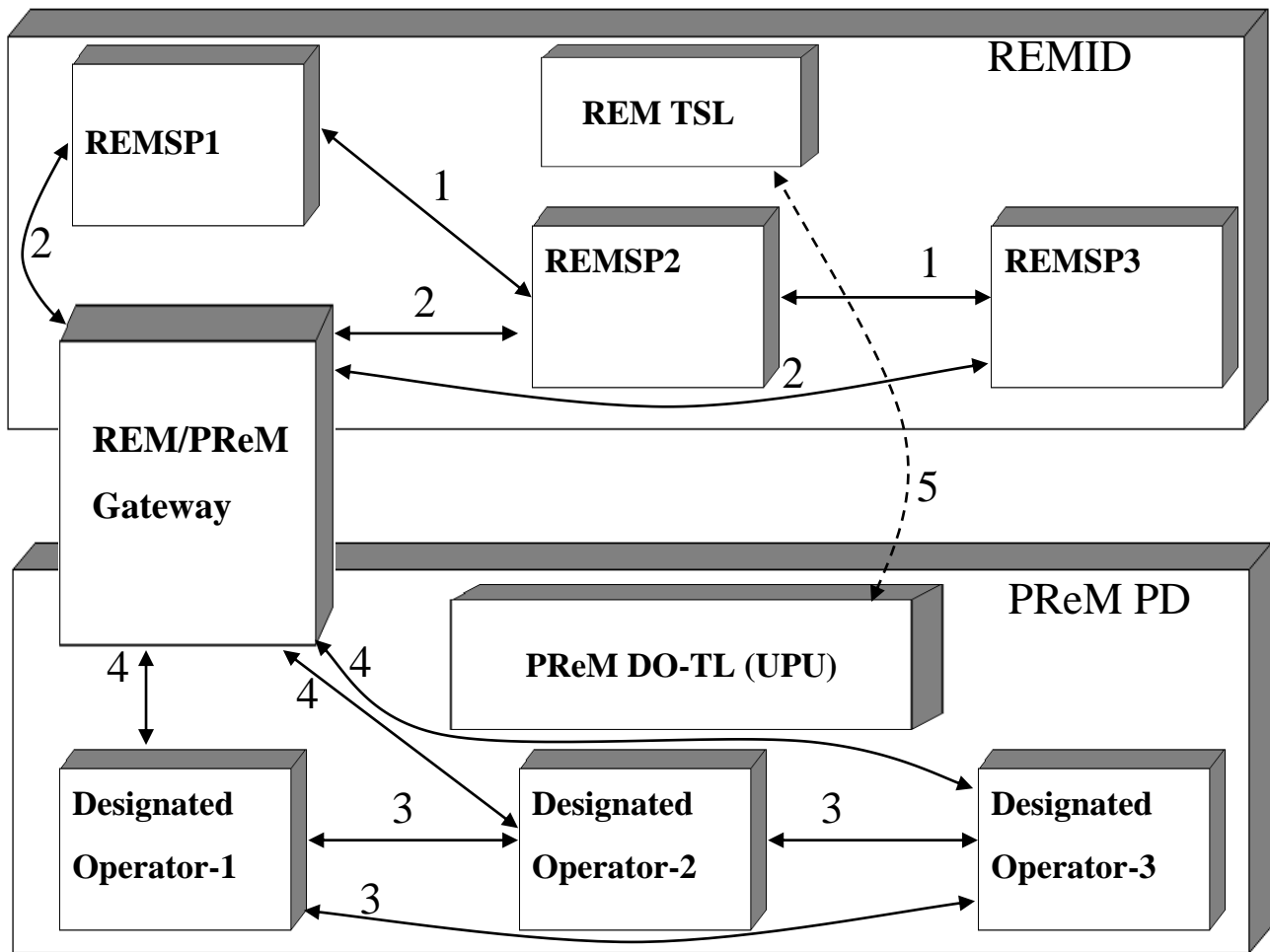
636

637   **Figure 1**

638   In Figure 1 a description of the main points of contact and interaction is represented.

639   The normal flows among REMSPs are represented with the label "1". In a similar way the normal flow among PReM
640   Designated Operators is indicated with the label "3".

641   The interaction from REM to PReM, identified by the labels "2" and "4", happens through a REM/PReM Gateway
642   implemented according to the profile defined in the present technical specification. From the point of view of any single
643   REMSP, the interaction through the Gateway ("2") is identical to that towards another generic REMSP of the same
644   system ("1"). The information, instead of arriving to a local REMSP, flows towards a remote Designated Operator of
645   the PReM system ("2" + "4") through the Gateway. The REM/PReM Gateway **may** be implemented to have a
646   behaviour like a normal REMSP or it **may** collapse in a particular role of an existing REMSP. In Figure 1 an explicit
647   separation is outlined for clarity reasons.

648   Conversely, the interaction from PReM to REM happens through a REM/PReM Gateway and it is identified by the
649   labels "4" + "2". Other than the role in REM network defined above, in the UPU/PReM network the REM/PReM
650   Gateway **shall** also be considered as one of the Designated Operators or to be collapsed in a particular role of an
651   existing DO.

652   The addressing bridging between these two systems is effected through a mutual acknowledgment by means of specific
653   indexes implemented for this purpose. The validation and trusting of these indexes **shall** be implemented through the
654   REM-TSL and PReM Designated Operators Trust List, identified by the label "5". Indexes implementation details are
655   out of the scope of the present document.

656 ## 6.4.2   Operational scenario

657 A typical operational scenario when a message flows from a REM system to a PReM system and vice versa is defined
658 in this clause.

659 The directions of the collateral informative flows on which the two main flows are based are:

660 - When a REM User is the initiator of a message for a PReM User:

661 - REM→PReM (REM send a dispatch to PReM),

662 - REM←PReM (REM receive the list of evidence from PReM).

663 - When a PReM User is the initiator of a message for a REM User:

664 - PReM→REM (PReM send a dispatch to REM),

665 - PReM←REM (PReM receive the list of evidence from REM).

666 The profile to use between the REM Sender and the REM/PReM Gateway (through the REMSP and the REM-UA)
667 **shall** be the "REMS Interoperability Profiles" defined in TS 102 640-5 [i.17] REM technical specification. To simplify
668 the description the terms REM Sender and REM Recipient **shall** be used in the present document without an explicit
669 mention of the REM-UA role that is always present in the middle to such type of interactions. Similarly REM "Senders"
670 and "Recipients" are generic terms that **shall** mean any entity like Process Applications, human users without any other
671 explicit mention.

672 # 6.5   Mapping of exchanged formats

673 The main aspects to consider during the interchanges between two messaging systems are those relevant to the structure
674 of the messages:

675 - attachments

676 - signatures

677 - evidence

678 An explicit normative reference to the REM ETSI TS [i.16] is reported in sections 2, 8.2, 8.4 and 8.5 of PReM UPU
679 [11] specification regarding the formats of the messages (and the formats of the types of evidence). So in a normal case,
680 when a PReM system interacts in a homogeneous way with another PReM system, it already uses the REM
681 specification for the formats of the PReM Messages and the formats of the evidence.

682 Under this light, in the case of interaction among REM and PReM systems, the format of the messages/evidence
683 exchanged is exactly the same defined in REM ETSI TS [i.16] specification and other additional requirement **shall not**
684 be needed. Figure 2 defines some detail of the format. Section 3.9 of UPU PReM Technical Specification [11] also
685 defines the formatting of attachments using a MIME structure and the signature of the external envelope using S/MIME
686 specification (as also defined in the normative reference to REM ETSI TS [i.16] specification).

687 Whereas the formats of the evidence are outwardly the same format of the messages, the list of types of evidence is
688 considered apart in clause 6.6.

6.6   Mapping of evidence names and semantics

For the UPU/PReM network, the types of evidence and their usage are defined in sections 8.2 and 5.2 of the PReM UPU [11] technical specification. In REM network all the evidence types are defined in TS 102 640-2 [i.16] clause 5.1.

According with the aforementioned definitions and with the GAP Analysis of clause 6.3, the list of the types of evidence **may** be classified in:

- Evidence internal to REMSP (or internal to the Designated Operator using the PReM UPU [11] terminology): these are the cases when both Sender and Recipients belong to the same REMSP (or the same Designated Operator). Even in this case, the evidence is produced, available for the users and logged locally to the Designated Operator.

- Evidence between the REMSP and the Sender/Recipient (or between a Designated Operator and a mailee/addressee using the PReM UPU [11] terminology): this is the direct evidence that flows from a REMSP (or Designated Operator) and the users registered to it.

- Evidence among REMSPs (or among the Designated Operators according to the PReM UPU [11] terminology): this is the evidence that flows between different REMSP (or different Designated Operators).

Only the third list of types of evidence is interesting for the purposes of interoperability, object of the present document. In fact, when two different systems REM/PReM need to interoperate, only the third type of evidence **shall** flow between the two types of systems and so between REMSP and DO (and vice versa according to the flow direction).

6.7   Mapping of protocol elements

In section 5.2.5 of the PReM UPU [11] specification it is recommended that the interchange of messages (Dispatches) among two Designated Operators (REMSP in REM terminology) is operated through Web Services.

The packages of information conveyed among Designated Operators are fully defined in the PReM UPU [11] specification as a XML schema and an associated WSDL.

A specific "**Data**" element is defined in the XML schema. It is a b64 binary element that **shall** host the REM Dispatch to be transmitted from a Designated Operator to another one. The same process **shall** be applied also in case of a REMS Message constituted by an evidence. The REM/PReM Gateway **shall** include the REM Dispatch or the REMS Message within a PReM WebService structure as specified in sections 7.1.7.2, 8.1 and 8.3 of the PReM UPU [11] specification.

6.7.1   Enveloping REM Dispatch in PReM Web Service business payload

Figure 2 illustrates how is implemented this mapping/embodying of REM Dispatch or REMS Messages to PReM Dispatch structure as WebService business payload.

719

720   ## PReM WebService Structure

721

722   ....
723   SendMessageToDestinationOptions
        TransactionKey
724   OriginalClaimedIdentity
        ClaimedIdentity
725   OrganizationID
        ClientApplication
726   ContentIdentifier
        Destination
727
728   **Data**

729   ContentMetadata
        …..

730

731

732
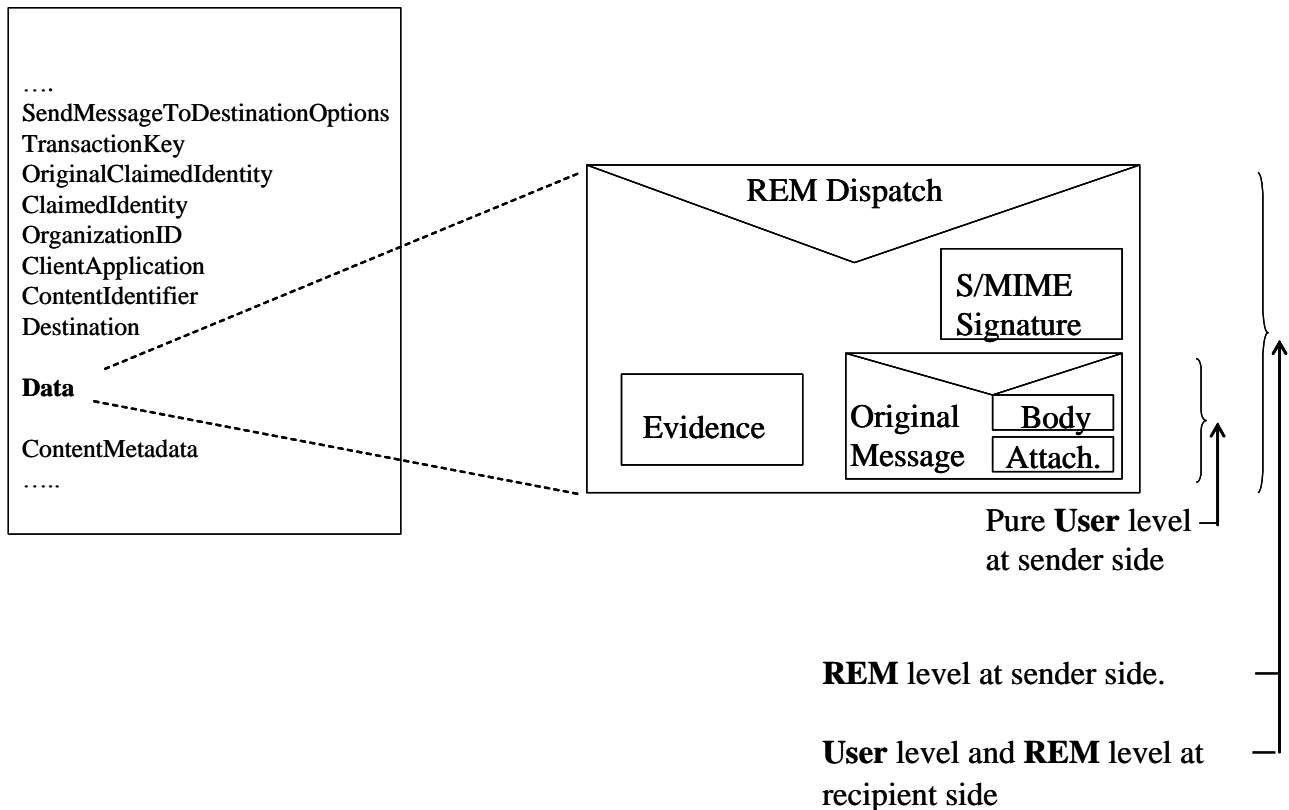
733

734

735

736   **Figure 2**

737   The envelope on the right part of Figure 2 represents the entire REM Dispatch according to the TS 102 640-1 [i.15],
738   TS 102 640-2 [i.16] and TS 102 640-5 [i.17] (equivalent to the PReM Message, in UPU Terminology).

739   The Sender's payload is the internal enveloped content indicated as "Original Message" in Figure 2.

740   The Recipient **shall** receive the entire content (indicated as "REM Dispatch" in Figure 2) containing the "untouched"
741   Sender's payload. Some variant to this schema **may** be possible according to the following rules:

742   •   The REM Dispatch/REMS Message **may** contain other attachments (for own purposes of UPU/PReM service),
743   but the basic structure with the mandatory elements defined in the TS 102 640-1 [i.15],
744   TS 102 640-2 [i.16] and TS 102 640-5 [i.17] **shall** be maintained unchanged.

745   •   The REMS Message representing an evidence (generally without a Sender's payload) **shall** be enveloped in the
746   PReM WebService Structure exactly as for the REM Dispatch (that contains the Original Message/Sender's
747   payload).

748   The mapping described in Figure 2 is implicitly performed when a UPU Designated Operator needs to interoperate with
749   another UPU Designated Operator according to the specification PReM UPU [11].

750   In consequence, a REM/PReM Gateway:

751   1) **shall** build up an appropriate PReM Web Service structure around the normal REM Dispatch, when the
752   direction is REM → PReM. This PReM Web Service structure **shall** be submitted to the UPU/PReM network
753   in order to be delivered to the intended PReM recipient;

754   2) **shall** extract the REMS Message, containing some evidence, from the "Data" element, when the direction of
755   the Sender's message is REM → PReM (and so the direction of the evidence messages is PReM → REM).
756   These evidence messages **shall** be submitted to the REM network in order to be delivered to the intended REM
757   recipient;

758   3)   **shall** extract the REM Dispatch contained in the "Data" element, when the direction is PReM → REM. This
759   REMS Message containing the Sender's payload **shall** be submitted to the REM network in order to be
760   delivered to the intended REM Recipient;

761   4)   **shall** build up an appropriate PReM Web Service structure around the normal REMS Message that contains an
762   evidence, when the direction of the Sender's message is PReM → REM (and so the direction of the evidence
763   messages is REM → PReM). These PReM Web Service structure **shall** be submitted to the UPU/PReM
764   network in order to be delivered to the intended PReM recipient.

765   Next clauses specify the processing to be implemented by the gateway.

6.7.2   PReM Designated Operators - relay Web Service Interface

767   The main purpose of the present document is directed to specify the requirements for a REM/PReM Gateway guarantor
768   of the interoperability among REMSP and PReM Designated Operators. The attention of this clause is concentrated to
769   analyse the Web Service operations (verbs in UPU PReM terminology) defined in PReM UPU [11] specification for the
770   interaction among homogenous PReM Designated Operators. The analysis of these verbs allows to define the interface
771   needed in the interoperability among REMSP and PReM Designated Operators.

772   The workflow among two general PReM Designated Operators is represented in Figure 3. This workflow is coherent
773   with the workflow defined in section 5.2.3 of PReM UPU [11] specification. It is purged of sub-flows not relevant for
774   interoperability purposes (that are represented by a cloud) and only the boundary functionalities are mentioned.
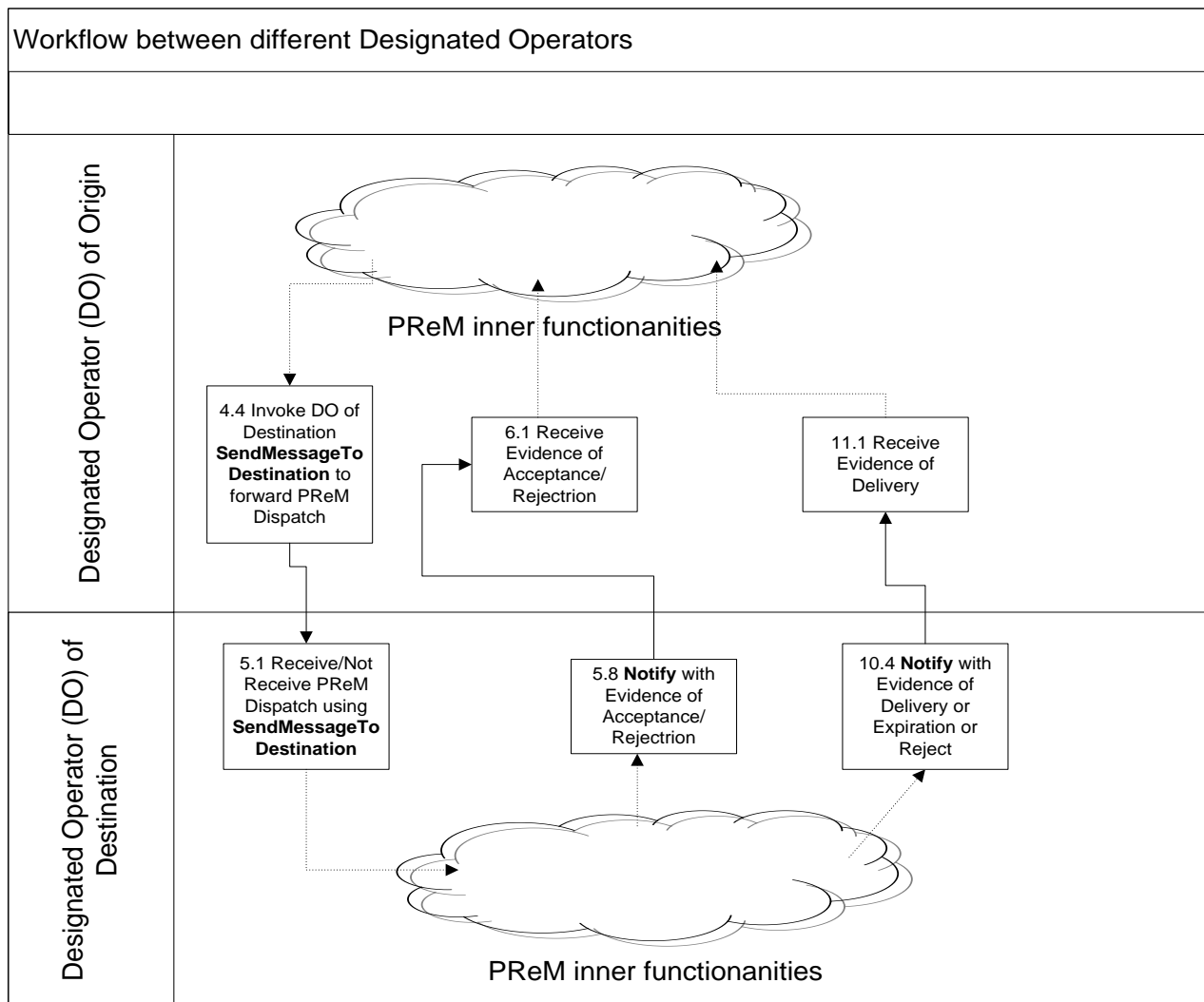
776   **Figure 3: Synthesis of section 5.2.3 of PReM UPU [11] TS**

777   The list of PReM verbs relevant for interoperability, that are mainly used in the functions represented in Figure 3, are:

778   • SendMessageToDestination;

779   • SubscribeNotification;

780   • UnsubscribeNotification;

781   • ReceiveNotification;

782   • RejectMessage.

783   As defined in clause 6 the REM/PReM Gateway **shall** act with double role: "a generic REMSP" plus "a Designated
784   Operators" according to the direction of the interaction. Under this light the typical usage of the previous functions is
785   the following:

786   • Case of REMSP that needs to relay a REMS Message to a PReM DO: REM→PReM:

787   - The REM/PReM Gateway **shall** register itself to receive notifications/evidence using the method
788   "**SubscribeNotification**" (this operation is done rarely, typically during the setup of the system).

789   - A REMSP **shall** relay a REM Dispatch or REMS Message and this, through the REM/PReM Gateway,
790   **shall** be sent to the correct PReM DO of destination by means of the **SendMessageToDestination**
791   method.

792   - The PReM DO of destination, **shall** deliver the incoming PReM Message to the Recipient
793   (Addressee/Mailee in PReM terminology) using the **SendMessageToDestination** method.

794   - The REM/PReM Gateway **shall** receive the evidence coming from the remote PReM DO of destination
795   using the **ReceiveNotification** method. The evidence **shall** be extracted and sent back to the originator
796   REMSP.

797   • Case of PReM DO that needs to relay a PReM Message to a REMSP: PReM→REM:

798   - The PReM DO of origin **shall** register itself to receive notifications/evidence using the method
799   "**SubscribeNotification**" (this operation is done rarely, typically during the setup of the system).

800   - The PReM DO of origin **shall** send a PReM Message to the REM/PReM Gateway by means of
801   **SendMessageToDestination** method and this, through the REM/PReM Gateway **shall** be sent to the
802   correct Recipient's REMSP.

803   - The Recipient's REMSP, **shall** deliver the REMS Message obtained by the incoming PReM Message
804   (the REM/PReM Gateway shall extract the REMS Message as payload of the PReM Message) to the
805   Recipient.

806   - The REM/PReM Gateway **shall** receive the evidence messages coming from the Recipient's REMSP and
807   **shall** notify them to the PReM DO of origin that, using the **ReceiveNotification** method **shall** receive all
808   the evidence messages.

809   A full description of the mapping for these functions is given in the next clauses.

810   6.7.2.1   SendMessageToDestination

811

812   The SendMessageToDestination method is used to send a PReM Message from a Designated Operator to another
813   Designated Operator. In the context of the present document, the role of one of the Designated Operators (Recipient's
814   DO or Sender's DO according to the direction of the flow) **shall** be covered by the REM/PReM Gateway.

815   The XML schema of such operation **may** be found in sections 7.1.7.1 and 7.1.7.2 of PReM UPU [11] specification.

816   6.7.2.1.1   Mapping of fields during a REM → PReM flow

817   The following table profiles the SendMessageToDestination operation in the use case of a REMSP sending REM
818   Dispatch to a PReM DO.

819 **Table 6: SendMessageToDestination XML elements**

Nº	Service / Protocol element	PReM UPU [11] reference	Requirement	Implementation guidance	Notes
1	EndLifeCycle	Clause 7.1.7.1	M	a	
2	ExtendLifeCycle	Clause 7.1.7.1	M	b	
3	IssuePostMarkedReceipt	Clause 7.1.7.1	M	c	
4	TransactionKey	Clause 7.1.7.1	M	d	
5	OriginalClaimedIdentity	Clause 7.1.7.1	M	e	
6	ClaimedIdentity	Clause 7.1.7.1	M	f	
7	OrganizationID	Clause 7.1.7.1	R	g	
8	ClientApplication	Clause 7.1.7.1	M	h	
9	ContentIdentifier	Clause 7.1.7.1	O	i	
10	Destination	Clause 7.1.7.1	M	l	
11	Timeout	Clause 7.1.7.1	M	m	
12	Data	Clause 7.1.7.1	M	n	
13	ContentMetadata	Clause 7.1.7.1	O	o	

820

821 Implementation guidance:

822 a) The SendMessageToDestination **shall** contain 'EndLifeCycle' element indicating if the current operation is at
823 the "end" of the business transaction lifecycle. Since in REM the concept of business transaction lifecycle is
824 not present, its value **shall** be set to true, where the meaning is that any interaction is always at the start/end of
825 the transaction lifecycle.

826 b) The SendMessageToDestination **shall** contain 'ExtendLifeCycle' element indicating if the current operation
827 extends the business transaction lifecycle. Its value **shall** be set to false.

828 c) The SendMessageToDestination **shall** contain 'IssuePostMarkedReceipt' element indicating if a specific
829 "PostMark" receipt (to attest that the REM Dispatch has been successfully received by the remote PReM
830 Designated Operator) is required. Its value **should** be false unless the Sender's REMSP is able to interpret such
831 receipt.

832 d) The SendMessageToDestination **shall** contain 'TransactionKey' element that is a complex type including a
833 unique transaction identifier. In order to have a unique identifier important for correlation of the exchanged
834 REM Dispatch and relevant evidence the value of its significant components **shall** be set as follows:

835 i) CountryCode: <two-bytes of the sender country according to the ISO 3166-1 [i.14] country code list>

836 ii) Version: <"1.0">

837 iii) Key: <the Message-ID value of the REMS Message envelope>

838 e) The SendMessageToDestination **shall** contain 'OriginalClaimedIdentity' element that is a complex type
839 specifying the original unique identification of the Sender. The value of its significant components **shall** be set
840 as follows:

841 i) NameQualifier: <the Internet Domain address of the Sender's e-mail address (the part on the right of the
842 '@' in the e-mail address according to the standard RFC 5322 [i.12])>

843 ii) Format: http://tools.ietf.org/html/rfc5322#section-3.4.1

844 iii) UserID: <the user part of Internet e-mail address of the Sender's e-mail address (the part on the left of the
845 '@' in the e-mail address according to the standard RFC 5322 [i.12])>

846 f) The SendMessageToDestination **shall** contain 'ClaimedIdentity' element that is a complex type specifying the
847 actual identification of the Sender. The value of its significant components **shall** be set to the same value of the
848 OriginalClaimedIdentity components (implementation guidance e).

849 g) The SendMessageToDestination **should** contain 'OrganizationID' element specifying the identifier of the
850 organization that provides the REM/PReM Gateway service. If present, its value **should** be set to the same
851 value of the TSP name present in Table 15 of Trusted Service Providers List for this organization.

852 h) The SendMessageToDestination **shall** contain 'ClientApplication' element that is a complex type specifying
853 the client application requesting the SendMessageToDestination. The value of its significant component **shall**
854 be set as follows:

855 i) NameAndVersion: "REM/PReM Gateway v1.0"

856 i) The SendMessageToDestination **may** contain 'ContentIdentifier' element specifying an identifier of the
857 content. If present, its value **shall** be set to "REMS Message".

858 j) The SendMessageToDestination **shall** contain 'Destination' element specifying the e-mail destination
859 addresses. Its value **shall** be set to a list of e-mail addresses (according to the syntax specified in
860 RFC 5322 [i.12]) relevant to a single remote PReM Designated Operator. If the REM Dispatch is directed to
861 many e-mail addresses belonging to different remote PReM Designated Operators, the same REM Dispatch
862 **shall** be sent many times, one per each remote Designated Operator. In each of these
863 SendMessageToDestination invocations the element "destination" **shall** be set to the exact list of addresses
864 relevant for each remote PReM Designated Operator. It is out of scope of the present document to specify the
865 routing aspects (e.g. how the messages are routed from any REMSP to the remote DO through the
866 REM/PReM Gateway).

867 k) The SendMessageToDestination **shall** contain 'Timeout' element specifying the period of time (in hours) that
868 the Recipient's DO should wait before considering a PReM Message as "not received" by the Recipient (if set
869 to 0 means that the timeout value is determined by the Recipient's DO). Its value **should** be set to the same
870 time period defined in laws/statutory requirements or local policies of REM network. In case no time period is
871 specified at REM level the value 0 **may** be used in Timeout element, indicating to use the Recipient's DO
872 default value (that in any case may override any specified value, as indicated in section 7.2.7.2 of PReM
873 UPU [11] specification).

874 l) The SendMessageToDestination **shall** contain 'Data' element that is a complex type specifying a binary
875 element (in b64 form) which embodies the entire REM Dispatch (or the REMS Message) to convey using the
876 SendMessageToDestination method. The value of its significant component **shall** be set as follows:

877 i) MimeType: "message/rfc822"

878 ii) base64Binary: <the base64 encoding of the entire REMS Message in MIME format>

879 m) The SendMessageToDestination **may** contain 'ContentMetadata' element that is a complex type specifying a
880 sequence of custom details regarding the REMS Message. If present its value **shall** be set as follows:

881 i) MetadataName: <name of the metadata>

882 ii) MetadataValue: <value of the metadata>

883 The REM/PReM Gateway **may** elaborate the answer of the SendMessageToDestination operation in order to produce
884 some new local Evidence to return back to the REM Sender, whenever this is not explicitly expected from the PReM
885 system.

886 6.7.2.1.2 Mapping of fields during a PReM → REM flow

887 The REM/PReM Gateway **shall** parse any PReM Dispatch coming from the PReM network and **shall** extract REM
888 Dispatch from the XML "Data" element. The REM Dispatch coming from the PReM network **shall** be auto consistent
889 in the sense that, according to the aspects considered in clause 6.5 of the present document, it **shall** have all the REM
890 fields correctly and coherently compiled to be interpreted by the destination REM system.

891 The REM/PReM Gateway **shall** decode any REM Dispatch (extracted as indicated above) from the base64 format and
892 **shall** submit it to the REM network. The submission operation requires to compile the "forward-path" and "reverse-
893 path" for the correct addressing to the proper REMSPs and to avoid loops and/or multiple submissions of the same
894 message. The two terms "forward" and "reverse" path are used in the present document like their usage in
895 RFC 5321 [i.11].

896 Below follows a non-normative example of how the "forward-path" and "reverse-path" are compiled:

897 This operation may be performed as follows:

   i) collect all the "To:" and "Cc:" MIME Headers from the REM Dispatch extracted from the 'Data' element;

   ii) select all the destination addresses that are belonging to the REM system. This may be done by a lookup to some specific trusted index (see clause 6.8 for trust building);

   iii) insert all the addresses selected in the previous point as "forward-path" for the correct routing of the REMS Message;

   iv) collect the "Reply-To:" MIME Headers from the REM Dispatch extracted from the 'Data' element and set it as "reverse-path" for the correct return path to use in case of exceptions.

905 It is out of scope of the present document to specify further these routing aspects.

6.7.2.2 SubscribeNotification

907 In the context of the present document, the SubscribeNotification method **shall** be used to cover the following
908 situations:

909 • Used by the REM/PReM Gateway for subscribing itself to the event notification service of the PReM system.
910 In this situation the SubscribeNotification is that usually implemented by any remote PReM DO.

911 • Used by any remote PReM Designated Operators to subscribe themselves to be notified on the relevant events
912 (called evidence in REM terminology) occurring at REM/PReM Gateway side. In this situation the
913 SubscribeNotification **shall** be implemented by the REM/PReM Gateway.

914 There is a direct correspondence among the PReM notifications and the evidence types in REM. It is required an
915 invocation of this function for each event type (and so evidence type) that needs to be notified to the REM/PReM
916 Gateway.

917 The REM/PReM Gateway **shall** subscribe itself, using the SubscribeNotification function, to each Designated Operator
918 of the PReM system that needs to use the gatewaying function with REM. Conversely, all these Designated Operators
919 of the PReM system that need to use the gatewaying function with REM **shall** subscribe themselves, using the
920 SubscribeNotification function to the REM/PReM Gateway.

921 This invocation is a "registration" of information (containing also a call-back URL), so it is performed rarely, and
922 typically at configuration time. Other means to register the required information **may** be possible under particular
923 agreements among the REM/PReM Gateway providers and PReM DO providers. Specification of alternative means is
924 out of scope of the present document.

925 The XML schema of such operation **may** be found in sections 7.1.9.1 and 7.1.9.2 of PReM UPU [11] specification.

6.7.2.2.1 Mapping of fields during a REM → PReM flow

927 Any DO **shall** implement the function SubscribeNotification. The REM/PReM Gateway **shall** subscribe itself to be
928 notified on events (evidence in REM terminology) occurring in any remote DO. Any event occurring at DO side means
929 a specific invocations to the ReceiveNotification (defined in clause 6.7.2.4.1) URL subscribed by the REM/PReM
930 Gateway with SubscribeNotification method.

931 Table 7 contains the mapping of the elements of SubscribeNotification, function invoked from the REM/PReM
932 Gateway and implemented in any remote DO.

933 **Table 7: SubscribeNotifications elements - REM → PReM**

Nº	Service / Protocol element	PReM UPU [11] reference	Requirement	Implementation guidance	Notes
1	EventType	Clause 7.1.9.1	M	a	
2	ClientApplication	Clause 7.1.9.1	M	b	
3	CallbackUrl	Clause 7.1.9.1	M	c	

935 Implementation guidance:

936 a) The SubscribeNotification **shall** contain 'EventType' element specifying the event to subscribe for which a
937   notification is required. This function **shall** be invoked, from the REM/PReM Gateway, for each of the
938   following events:

939   i)   "MessageDelivered"

940   ii)   "MessageUndelivered"

941   iii) "MessageReadByAddresee"

942 b) The SubscribeNotification **shall** contain 'ClientApplication' element that is a complex type specifying the
943   client application requesting the SubscribeNotification. The value of its significant component **shall** be set as
944   follows:

945   i)   NameAndVersion: "REM/PReM Gateway v1.0"

946 c) The SubscribeNotification **shall** contain 'CallbackUrl' element specifying the call-back URL function that it is
947   required to be invoked by any subscribed DO whenever the event denoted by EventType occurs. This URL
948   **shall** implement a function according to the interface defined for the "ReceiveNotification" method, as
949   described in clause 6.7.2.4.1 of the present document. The value of this element **shall** be set as follows:

950   i)   CallbackUrl: <URL of the WebService of the REM/PReM Gateway pointing to the ReceiveNotification
951   function>

952   Whenever some events occur at DO level, it **shall** invoke the specific ReceiveNotification call-back function
953   as defined in clause 6.7.2.4.1 of the present document.

954 6.7.2.2.2   Mapping of fields during a PReM → REM flow

955 The REM/PReM Gateway **shall** implement the function SubscribeNotification. The remote PReM Designated
956 Operators **shall** subscribe themselves to be notified on events (evidence in REM terminology) occurring in the
957 REM/PReM Gateway. The REMS Messages containing evidence information directed to PReM Designated Operators
958 **shall** be converted, by the REM/PReM Gateway, in specific invocations to the ReceiveNotification (defined in clause
959 6.7.2.4.2) URLs subscribed by any DO with SubscribeNotification method.

960 Table 8 contains the mapping of the elements of SubscribeNotification, function implemented in the REM/PReM
961 Gateway.

962   **Table 8: SubscribeNotifications elements - PReM → REM**

Nº	Service / Protocol element	PReM UPU [11] reference	Requirement	Implementation guidance	Notes
1	EventType	Clause 7.1.9.1	M	a	
2	ClientApplication	Clause 7.1.9.1	M	b	
3	CallbackUrl	Clause 7.1.9.1	M	c	

963

964 Implementation guidance:

965 a) The SubscribeNotification **shall** contain 'EventType' element specifying the event to subscribe for which a
966   notification is required. This function **shall** be invoked, by any remote DO, for each of the following events:

967   i)   "MessageDelivered"

968   ii)   "MessageUndelivered"

969   iii) "MessageReadByAddresee"

970 b) The SubscribeNotification **shall** contain 'ClientApplication' element that is a complex type specifying the
971   client application requesting the SubscribeNotification. The value of its significant component **may** be set as
972   follows:

973   i)   NameAndVersion: "Remote DO v1.0"
974   Other values **may** be used by the DOs for this element. It is out of scope of the present document to
975   provide further specification on this element since it is considered informative and not critical for the
976   interoperability.

977 c) The SubscribeNotification **shall** contain 'CallbackUrl' element specifying the call-back URL function that it is
978   required to be invoked by the REM/PReM Gateway whenever the event denoted by EventType occurs. This
979   URL **shall** implement a function according to the interface defined for the "ReceiveNotification" method, as
980   described in clause 6.7.2.4.2 of the present document. The value of this element **shall** be set as follows:

981   i) CallbackUrl: <URL of the WebService of the remote DO associated to the ReceiveNotification
982   function>

983   The REM/PReM Gateway **shall** maintain a configuration table with the following mapping.

984 **Table 9: SubscribeNotifications - Event mapping - PReM → REM**

PReM EventType	REM Event (TS 102 640-1 [i.15], clause 6.2)
MessageDelivered	6.2.3 Event C.1 - Message Delivery
MessageUndelivered	6.2.3 Event C.2 - Expiration of time to deliver message
MessageReadByAddresee	6.2.3 Event F.1 (mailbox) - Retrieval

985

986 Whenever a REMS Evidence, related to the specified REM Event, arrives to the REM/PReM Gateway, it **shall**
987   invoke the specific ReceiveNotification call-back function for all the subscribed PReM Designated Operators
988   as defined in clause 6.7.2.4.2 of the present document.

989 ## 6.7.2.3   UnsubscribeNotification

990 The UnsubscribeNotification method is useful to cancel a previous registration process performed by a
991 SubscribeNotification. It is out of scope of the present document to list all the possible reasons requiring to unsubscribe
992 a previous agreement. The full usage description of this method **may** be found in section 7.2.10 of PReM UPU [11]
993 specification

994 The REM/PReM Gateway requiring unsubscribing an agreement with some remote DO **shall** queue all the REMS
995 Evidence messages directed to such remote DO. The REMS Evidence messages queued, when any subscription
996 agreement with a remote DO is defined, **shall** subsequently be delivered as soon as a new subscription agreement will
997 be effected. Further details on the subscription agreements are out of scope of the present document.

998 ## 6.7.2.4   ReceiveNotification

999 The ReceiveNotification method is used to receive evidence information whenever some event, subscribed with the
1000 method SubscribeNotification, occurs.

1001 The XML schema of such operation **may** be found in section 7.1.11.1 of PReM UPU [11] specification.

1002 ### 6.7.2.4.1   Mapping of fields during a REM → PReM flow

1003 In this context the flow REM → PReM means that a REMS Message (or a REM Dispatch) has been sent to a remote
1004 PReM Designated Operator and the relevant evidence needs to be received from the REM/PReM Gateway by means of
1005 ReceiveNotification. The REM/PReM Gateway **shall** implement the ReceiveNotification function and it **shall** be
1006 available at the URL subscribed as indicated in clause 6.7.2.2.1 of the present document. The following table contains
1007 the mapping of the relevant elements.

1008 **Table 10: ReceiveNotifications elements - REM → PReM**

Nº	Service / Protocol element	PReM UPU [11] reference	Requirement	Implementation guidance	Notes
1	TransactionKey	Clause 7.1.11.1	M	a	
2	EventType	Clause 7.1.11.1	M	b	
3	EventDateTime	Clause 7.1.11.1	M	c	
4	EventData	Clause 7.1.11.1	M	d	

1009

1010 Implementation guidance:

1011 a) The ReceiveNotification **shall** contain 'TransactionKey' element specifying the TransactionKey returned back
1012   in the previous SubscribeNotification invocation. Even if the syntax of this element states that it is mandatory,
1013   its value **shall** be ignored, at REM/PReM Gateway side, during the implementation of ReceiveNotification.

1014   b)   The ReceiveNotification **shall** contain 'EventType' element specifying the event that has occurred on the
1015   remote PReM Designated Operator, the invoker of ReceiveNotification. The REM/PReM Gateway **shall**
1016   extract the evidence from the ReceiveNotification and **shall** submit it in the REM network as described in
1017   implementation guidance d) below. The evidence **shall** be fully formatted and enveloped in the EventData
1018   element by the remote PReM Designated Operator according to the following mapping table:

1019   **Table 11: ReceiveNotifications - Event mapping - REM → PReM**

PReM EventType	REMS Evidence (TS 102 640-1 [i.15], clause 5.1)
MessageDelivered	5.1.4 DeliveryNonDeliveryToRecipient
MessageUndelivered	5.1.4 DeliveryNonDeliveryToRecipient
MessageReadByAddresee	5.1.6 RetrievalNonRetrievalByRecipient

1020

1021   c)   The ReceiveNotification **shall** contain 'EventDateTime' element specifying the date/time reference of the event
1022   which has just occurred. Even if the syntax of this element states that it is mandatory, its value **shall** be
1023   ignored, at REM/PReM Gateway side, during the implementation of ReceiveNotification.

1024   d)   The ReceiveNotification **shall** contain 'EventData' element that is a complex type specifying a binary element
1025   (in b64 form) which embodies the entire REMS Message containing the REMS Evidence to convey using the
1026   ReceiveNotification method. The value of its significant component **shall** be set as follows:

1027   i)   MimeType: "message/rfc822"

1028   ii)   base64Binary: <the base64 encoding of the entire REMS Message containing the evidence>

1029   The REM/PReM Gateway, executing the invocation of ReceiveNotification, **shall** decode the REMS Message
1030   containing the evidence, extracted from the element indicated above, from the base64 format and **shall** submit it in the
1031   REM network. The submission operation requires to compile the "forward-path" and "reverse-path" for the correct
1032   addressing to the proper REMSPs and to avoid loops and/or multiple submissions of the same object. The two terms
1033   "forward" and "reverse" path are used in the present document like their usage in RFC 5321 [i.11].

1034   Below follows a non-normative example of how the "forward-path" and "reverse-path" are compiled:

1035   This operation may be performed as follows:

1036   i) collect all the "To:" MIME Headers from the REMS Message extracted from the 'EventData' element
1037   and set the "forward-path" with this value;

1038   ii) collect the "From:" MIME Headers from the REMS Message extracted from the 'EventData' element
1039   and set it as "reverse-path" (for the correct return path in case of exceptions).

1040   It is out of scope of the present document to specify further these routing aspects.

1041   6.7.2.4.2   Mapping of fields during a PReM → REM flow

1042   In this context the flow PReM → REM means that a PReM Message has been sent from a PReM Designated Operator
1043   of origin to a REMSP through the REM/PReM Gateway. The Gateway, receiving back the REMS Evidence from the
1044   Recipient's REMSP, **shall** notify this to the PReM Designated Operator of origin by means the invocation of
1045   ReceiveNotification. The ReceiveNotification function will be available at the URL subscribed in advance by the PReM
1046   Designated Operator as indicated in clause 6.7.2.2.2 of the present document.

1047   The REM/PReM Gateway **shall** invoke the proper URL notifying the correct PReM EventType according to the
1048   following table:

1049   **Table 12: ReceiveNotifications - Event mapping - PReM → REM**

REMS Evidence (TS 102 640-1 [i.15], clause 5.1)	PReM EventType
5.1.4 DeliveryNonDeliveryToRecipient - delivery case	MessageDelivered
5.1.4 DeliveryNonDeliveryToRecipient - expiration time to delivery case	MessageUndelivered
5.1.6 RetrievalNonRetrievalByRecipient - retrieval case	MessageReadByAddresee

1050

1051   Table 13 contains the mapping of all the relevant elements of the ReceiveNotification invocation.

1052 **Table 13: ReceiveNotifications elements - PReM → REM**

Nº	Service / Protocol element	PReM UPU [11] reference	Requirement	Implementation guidance	Notes
1	TransactionKey	Clause 7.1.11.1	M	a	
2	EventType	Clause 7.1.11.1	M	b	
3	EventDateTime	Clause 7.1.11.1	M	c	
4	EventData	Clause 7.1.11.1	M	d	

1053

1054 Implementation guidance:

1055 a) The ReceiveNotification **shall** contain 'TransactionKey' element specifying the TransactionKey returned back
1056 in the previous SubscribeNotification invocation.

1057 b) The ReceiveNotification **shall** contain 'EventType' element specifying the event to transmit to the Sender's
1058 PReM Designated Operator (the initiator of the messaging transaction) according with Table 12. The
1059 REM/PReM Gateway **shall** invoke the ReceiveNotification submitting the REMS Message containing an
1060 evidence to the Sender's DO as described in implementation guidance d) below.

1061 c) The ReceiveNotification **shall** contain 'EventDateTime' element specifying the date/time reference of the event
1062 which has just occurred. This time **should** be collected from the evidence.

1063 d) The ReceiveNotification **shall** contain 'EventData' element that is a complex type specifying a binary element
1064 (in b64 form) which embodies the entire REMS Message containing the REMS Evidence to be send back to
1065 the Sender's DO. The value of its significant component **shall** be set as follows:

1066 i) MimeType: "message/rfc822"

1067 ii) base64Binary: <the base64 encoding of the entire REMS Message containing the evidence>

1068 The REM/PReM Gateway, executing the invocation of ReceiveNotification, **shall** encode the REMS Message
1069 containing the evidence in base64 format and **shall** submit it to the Sender's DO.

1070 6.7.2.5 RejectMessage

1071 The RejectMessage method is useful to explicitly indicate the will of the Recipient to reject the message. It is out of
1072 scope of the present document to list all the possible reasons requiring this method. The full usage description of this
1073 method **may** be found in section 7.2.8 of PReM UPU [11] specification.

1074 Since the event associated with rejection is present in both technical specifications REM and UPU/PReM, it **may** be
1075 used in both directions.

1076 6.7.2.5.1 Mapping of evidence during a REM → PReM flow

1077 In this context the flow REM → PReM means that a REMS Message (or a REM Dispatch) has been sent to a remote
1078 PReM Designated Operator and the final Recipient rejects the incoming message with an explicit declaration. This act
1079 is translated in an invocation to the RejectMessage method.

1080 The REM/PReM Gateway **shall** implement the RejectMessage mapping this event to the
1081 '**AcceptanceRejectionByRecipient**' REMS Evidence (with EventCode='Rejection'). The new REMS Evidence message
1082 composed by the REM/PReM Gateway **shall** be sent back to the REM Sender of the original message. It is out of scope
1083 of the present document how the REM/PReM Gateway maintains the correlation among all the sent/received
1084 information needed to compose the 'AcceptanceRejectionByRecipient' REMS Evidence.

1085 6.7.2.5.2 Mapping of evidence during a PReM → REM flow

1086 In this context the flow PReM → REM means that a PReM Message has been sent to a REM Recipient and, in case of
1087 the optional reject mechanism is provided to the final user, this user rejects the incoming message with an explicit
1088 declaration. This declaration is translated, at Recipient's REMSP level, in a generation of a
1089 '**AcceptanceRejectionByRecipient**' REMS Evidence (with EventCode='Rejection').

1090 The REM/PReM Gateway **shall** invoke the RejectMessage implemented and executed, as usual in PReM environment,
1091 by the Sender's DO. It is out of scope of the present document how the REM/PReM Gateway maintains the correlation
1092 among all the sent/received information needed to invoke the RejectMessage method.

1093 # 6.8   Definition of mutual recognition system based on ETSI-TSL
1094 and UPU-Designated Operator Trusted List

1095 This clause contains the specifications that **should** be implemented for cross-trusting between ETSI/REM and
1096 UPU/PReM networks.

1097 A PReM Policy Domain, according to PReM UPU [11] specification, is a collection of PReM enabled Designated
1098 Operators operating which belong to a group that is managed according to rules and regulations agreed by the group.
1099 Each PReM Designated Operator grants trust to the PReM End Users abiding by the same Policy Domain rules and
1100 granting that each PReM Message properly submitted is managed, tracked and delivered under the common Policy
1101 Domain rules. Digital signatures applied by PReM Designated Operators to PReM Messages and PReM Evidence
1102 certify the respect of the Policy Domain rules. UPU is responsible for Policy Domain rules establishment and supervises
1103 Designated Operators operating under Policy Domain rules.

1104 A PReM Trust List is required to support PReM End User or interested party to:

1105 - verify that the signing certificate used for PReM Dispatch is valid and belongs to an authorized Designated
1106 Operator

1107 - verify if the PReM Designated Operator belongs to the expected PReM Policy Domain

1108 - verify if the PReM Designated Operator current status was in accord with PReM Policy Domain rules when a
1109 signature envelope was created

1110 TSL defined in TS 102 231 **[i.18]** addresses those requirements and is the recommended instrument for a seamless
1111 mutual recognition between a REM and PReM systems evidence. When a TSL is used to implement or complement a
1112 PReM Trust List, TS 102 640-1 [**i.15**] **shall** apply.

1113 In term of domain trust the following mapping among PReM, REM and TSL defined roles is applied:

1114 - entity responsible for Policy Domain rules (i.e. UPU) - REM interoperability domain (REMID) - TSL Schema
1115 Operator

1116 - PReM Designated Operator - REM Service Provider (REMSP) - TSLTrust Service Provider (TSP)

1117 - PReM Designated Operator signing service - REMS Evidence Provider - TSL Service

1118 A TSL contains trust information, in a hierarchical format. NOTE: The notations "[1]" and "[2]" above indicate the
1119 indexes of elements of the list.

1120

1121 Figure 4 shows the information contained in a TSL and how it is mapped to REM/PReM entities.
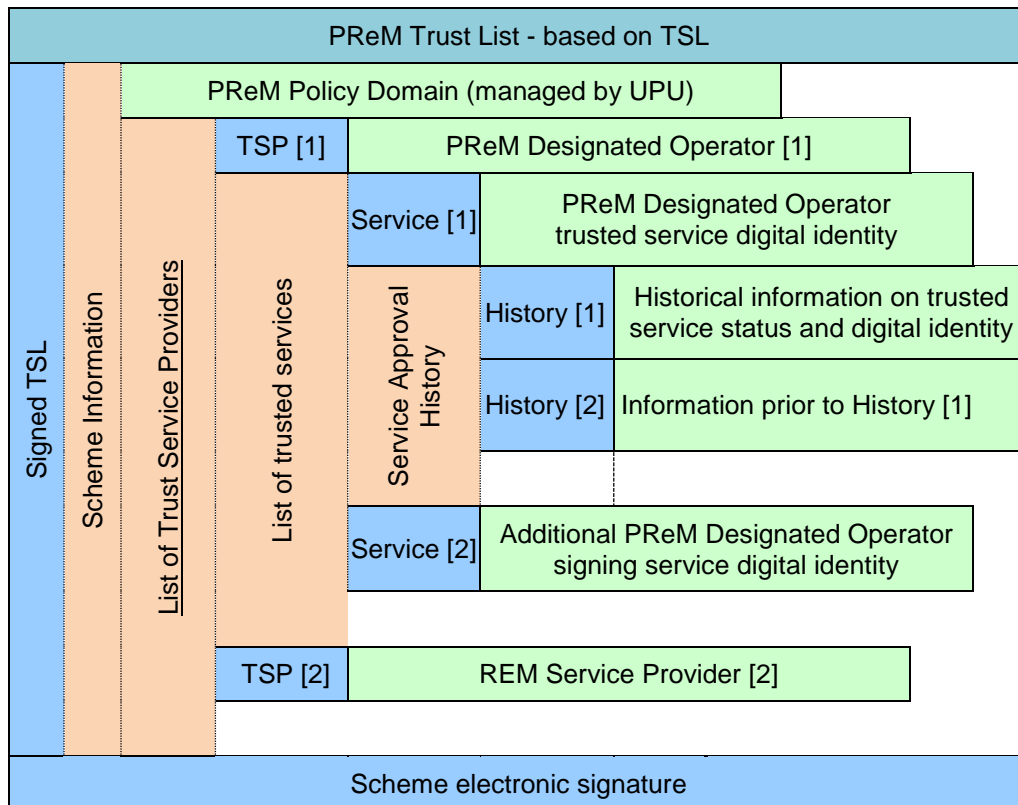
1122

1123   NOTE: The notations "[1]" and "[2]" above indicate the indexes of elements of the list.
1124
1125   **Figure 4: Mapping UPU Trust List to TSL (based on TS 102 231** [i.18]**)**

1126 When UPU, as responsible for PReM Policy Domain, issues a TSL, it acts as TSL schema operator and creates, signs
1127 and publishes the TSL.

1128 A TSL for PReM **shall** be of type Generic and all the Designated Operators **shall** be listed as TSP. Each of these **should**
1129 contain information related to REMS Evidence provider, current and historical information among which digital
1130 identity that can be used to verify the service signatures and status.

1131 It is assumed that each party that needs to verify a REMS Evidence **should** trust at least a Schema Operator.

1132 As non normative example, a REM User typically trusts TSLs issued by own REMID.

1133 A TSL issued for PReM **should** contain all the Designated Operators and the related certificated associated to the
1134 digital keys that they use to:

1135   i)   digital sign the PReM Messages

1136   ii)   verify integrity and trust of the PReM Messages (including the PReM Objects and Evidence)

1137 If a PReM Designated Operator certificate is no longer used (e.g. when approaching its expiration date) a new
1138 certificate is generated and associated to the service while the previous certificate is added to the service history. For
1139 each active signing digital key a Trusted Service element and its history **shall** be updated. No new Trusted Service entry
1140 **should** be added when a new signing key is generated and associated to a new certificate to renew an expiring one.

1141   ## 6.8.1   Scheme information section

1142   The scheme information section of a TSL issued by a PReM Policy Domain **should** be populated in conformance to
1143   Table 14.

1144   **Table 14: UPU PReM TSL Scheme Information**

TSL field name	Value
TSL type (M)	Set to "http://uri.etsi.org/TrstSvc/TSLType/generic"
Scheme operator name (M)	See TS 102 231 **[i.18]**
Scheme operator address (M)	
Scheme operator postal address (M)	
Scheme operator electronic address (M)	
Scheme name (M)	
Scheme information URI (M)	
Status determination approach (M)	Set to "Active"
Scheme type/community/rules (O)	Set to "supervision"
Scheme territory (O)	Not present
TSL policy/legal notice (M)	See TS 102 231 **[i.18]**
Historical information period (M)	
Pointers to other TSLs (O)	
Additional information field (O) Attribute of: Pointers to other TSLs	
List issue date and time (M)	
Next update (M)	
Distribution points (O)	
Scheme extensions (O)	Not present
List of Trust Service Providers (O) → sequence of elements in Table 15	List of Trust Service Providers as specified in clause 6.8.2

1145

1146   ## 6.8.2   List of Trust Service Providers section

1147   The List of Trust Service Providers section should be compiled according to Table 15.

1148   **Table 15: List of Trust Service Providers**

TSL field	Value
TSP name (M)	Set with the Designated Operator Name
TSP trade name (M)	See TS 102 231 **[i.18]**
TSP address (M)	
TSP postal address (M)	
TSP electronic address (M)	
TSP information URI (M)	An URI where general information relevant to the users like public certificates, addresses, etc. is published by the Designated Operator
TSP information extensions (O)	Not present
List of services (M)	Sequence of Trusted Service information elements as specified in clause 6.8.3

1149

6.8.3   Trusted Service information section

The List of Trust Service information section should be compiled according to Table 16.

Table 16: Trusted Service information

TSL field	Value
Service type identifier (M)	The value shall be one of the following. Case of UPU/PReM TSP: http://www.upu.int/PReMService Case of ETSI/REM TSP: http://uri.etsi.org/TrstSvc/Svctype/REM
Service name (M)	See TS 102 231 **[i.18]**
Service digital identity (M)	The Designated Operator Certificate X.509 certificate and optionally an X509 SKI element
Service current status (M)	Set to one of "In accord / Suspended / Revoked"
Current status starting date and time (M)	See TS 102 231 **[i.18]**
Scheme service definition URI (O)	
Service supply points (O)	
TSP service definition URI (O)	Optionally an URI for publishing general information relevant to the users like public certificates, addresses, etc.
Service information extensions (O)	Not present
Service approval history (O)	Sequence of service approval history elements as specified in clause 6.8.4

6.8.4   Trusted Service approval history section

The List of Trust Service approval history section should be compiled according to Table 17.

Table 17: Service approval History

TSL field	Value
Service type identifier	See Table 16
Service name	See Table 16
Service digital identity	See Table 16
Service previous status	See TS 102 231 **[i.18]**
Previous status starting date and time	
Service information extensions	Not present

7   Other interoperability profiles

Editorial Note: A "general purpose" mechanism allowing the coverage of other Transport Protocols (e.g already existing or more efficient protocols, suitable for REM, which might emerge in a future time) will be specified here, in the next developments of the present document. The guideline will consist in the specification of the minimum set of requirements, involving the fundamentals of a transport protocol, useful for REM - taking also into account provisions & structured formats from EN 319 532 Part-3.

History

Document history		
V0.0.1	March 2017	Version for ESI comments
V0.0.2	June 2017	Version for ESI comments
V0.0.2	September 2017	Version for ESI comments
V0.0.4	October 2017	Version for public review