ETSI TR 119 530 V1.1.1 (2019-02)

Electronic Signatures and Infrastructures (ESI);
Registered Electronic Mail (REM);
Feasibility study: Interoperability profile between
ETSI EN 319 532-based REM systems
and PReM-based systems

Reference
DTR/ESI-0019530

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

ETSI

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

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

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

Contents

Intellectual Property Rights

Essential patents

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

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

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Electronic Signatures and Infrastructures (ESI).

The present document is a standalone document and it is closely tied to ETSI EN 319 522 [i.21] and ETSI EN 319 532 [i.22].

Modal verbs terminology

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

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

Introduction

Registered Electronic Mail (REM) Service is a particular type of an "Electronic Registered Delivery Service" (ERDS). Standard email, used as backbone, makes interoperability smooth and increases usability. At the same time, the application of additional security mechanisms ensures integrity, confidentiality and non-repudiation (of submission, consignment, handover, etc.), and protects against risk of loss, theft, damage and any illegitimate modification of user content. ETSI EN 319 532 [i.22] gives technical specification for REM Service.

Postal Registered Electronic Mail (PReM) is an electronic version of the conventional postal registered mail service. It can be provided to the customers by entities called "designated operators" that are part of a program called "Secure electronic Postal Services (SePS)". It provides strong authentication, confidentiality and integrity protecting the message, and non-repudiation attributes to evidence, events and operations. UPU S52-2 [i.25] provides functional specification for PReM.

The currently existing PReM specifications were built based on ETSI TS 102 640 [i.23], which is a historical technical specification for REM, originally published in 2008 and last updated in 2011. The latest REM technical specification is ETSI EN 319 532 [i.22], published in 2018, which builds on the more general specification of Electronic Registered Delivery Service (ERDS) defined in ETSI EN 319 522 [i.21]. The new ETSI EN 319 532 [i.22] is an evolution of the older ETSI TS 102 640 [i.23]. The new REM standard was created based on ETSI TS 102 640 [i.23], but it is restructured to align with the ERDS standard, and contains a number of necessary changes and updates. The changes of Evidence (especially in formats) in ERDS (ETSI EN 319 522 [i.21]) did not allow the definition of a new ERDS/PReM interoperability profile like that defined in ETSI TS 102 640 [i.23]. Such interoperability profile was based on the PReM S52-1 [i.24] specification at the time. Since its publication the UPU S52-1 [i.24] has also been updated in UPU S52-2 [i.25], introducing changes in the workflows, messages and evidences.

The present document aims to provide a feasibility study that will pave the way for the update of UPU S52-2 / CEN/TS 16326 [i.25] and eventually the production of the interoperability profile between systems based on ETSI EN 319 522 [i.21] and ETSI EN 319 532 [i.22], and systems based on PReM [i.25] properly updated as recommended in the present document.

1 Scope

The present document represents a feasibility study for an interoperability profile between systems based on ETSI EN 319 522 [i.21] / ETSI EN 319 532 [i.22] ERDS/REMS specification and UPU S52-2 PReM specification [i.25].

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

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

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

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

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

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

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

[i.4] ETSI EN 319 522-1: "Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 1: Framework and architecture".

[i.5] ETSI EN 319 522-2: "Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 2: Semantic contents".

[i.6] ETSI EN 319 522-3: "Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 3: Formats".

[i.7] ETSI EN 319 521: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Electronic Registered Delivery Service Providers".

[i.8] ETSI EN 319 531: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Registered Electronic Mail Service Providers".

[i.9] ETSI TS 102 640-1: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 1: Architecture".

[i.10] ETSI TS 102 640-2: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 2: Data requirements, Formats and Signatures for REM".

[i.11] ETSI TS 102 640-6-1: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 6: Interoperability Profiles; Sub-part 1: REM-MD UPU PReM Interoperability Profile".

[i.12] ETSI EN 319 132-1: "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures".

[i.13] ETSI TS 101 903: "Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signatures (XAdES)".

[i.14] ETSI TS 103 171 (V2.1.1): "Electronic Signatures and Infrastructures (ESI); XAdES Baseline Profile".

[i.15] IETF RFC 7522: "Security Assertion Markup Language (SAML) 2.0 Profile for OAuth 2.0 Client Authentication and Authorization Grants".

[i.16] ETSI TS 102 176-1: "Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms".

[i.17] ETSI TS 102 231: "Electronic Signatures and Infrastructures (ESI); Provision of harmonized Trust-service status information".

[i.18] ETSI TS 119 312: "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites".

[i.19] ETSI TS 119 612: "Electronic Signatures and Infrastructures (ESI); Trusted Lists".

[i.20] IETF RFC 2046: "Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types".

[i.21] ETSI EN 319 522 (all parts): "Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services".

[i.22] ETSI EN 319 532 (all parts): "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) Services".

[i.23] ETSI TS 102 640 (all parts): "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM)".

[i.24] UPU S52-1: "Functional specification for postal registered electronic mail".

NOTE: This is version 1 of the UPU S52 specification; date of adoption is 30 October 2008.

[i.25] UPU S52-2 / CEN/TS 16326: "Functional specification for postal registered electronic mail".

NOTE: This is version 2 of the UPU S52 specification; date of adoption is 9 April 2013.

[i.26] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[i.27] ETSI TS 101 862: "Qualified Certificate profile".

[i.28] ETSI EN 319 412 (all parts): "Electronic Signatures and Infrastructures (ESI); Certificate Profiles".

[i.29] IETF RFC 5322: "Internet Message Format".

[i.30] IETF RFC 3851: "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification".

[i.31] IETF RFC 5751: "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification".

[i.32] ETSI EN 319 132 (all parts): "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures".

[i.33] IETF RFC 8446: "The Transport Layer Security (TLS) Protocol Version 1.3".

[i.34] ETSI TS 102 640-5: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 5: REM-MD Interoperability Profiles".

[i.35] IETF RFC 2822: "Internet Message Format".

[i.36] CWA 14169: "Secure signature-creation devices "EAL 4+"".

[i.37] CEN EN 419211 (parts 1 to 6): "Protection profiles for secure signature creation device".

[i.38] ETSI TS 102 640 (V1.1.1) (parts 1 to 3): "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Architecture, Formats and Policies".

3 Definition of terms, symbols, abbreviations and terminology

3.1 Terms

For the purposes of the present document, the terms given in ETSI EN 319 522 [i.21], ETSI EN 319 532 [i.22], ETSI TS 102 640-6-1 [i.11], UPU PReM S52-1 [i.24] and UPU S52-2 / CEN/TS 16326 [i.25] apply.

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI EN 319 522 [i.21], ETSI EN 319 532 [i.22], ETSI TS 102 640-6-1 [i.11], UPU PReM S52-1 [i.24] and UPU S52-2 / CEN/TS 16326 [i.25] apply.

3.4 Terminology

For the purposes of the present document, the terminology given in ETSI EN 319 522 [i.21], ETSI EN 319 532 [i.22], ETSI TS 102 640-6-1 [i.11], UPU PReM S52-1 [i.24] and UPU S52-2 / CEN/TS 16326 [i.25] apply.

4 Goals and approaches

This feasibility study includes:

- A gap analysis between the new ETSI EN 319 522 [i.21] / ETSI EN 319 532 [i.22] and the historical ETSI TS 102 640 [i.23] regarding those aspects covered within UPU S52-2 / CEN/TS 16326 [i.25].
- A gap analysis between the latest UPU S52-2 [i.25] and the obsolete UPU S52-1 [i.24] regarding those aspects affecting the interoperability with ETSI REM-based systems.
- Recommendations for updating UPU S52-2 / CEN/TS 16326 [i.25] specifications in the light of the gap analysis aforementioned. This would speed up the update of the UPU S52-2 / CEN/TS 16326 [i.25] specifications as the members of the UPU and CEN TC 331 could start their work based on these recommendations.
- Recommendations for the production of the interoperability profile between the new UPU S52-2 / CEN/TS 16326 [i.25] and the ETSI EN 319 532 [i.22], which would speed up the production of such profile once the updated UPU S52-2 / CEN/TS 16326 [i.25] is published.

5 Gap analysis

5.1 REM - ETSI TS 102 640 vs ETSI EN 319 532

5.1.1 Introduction

ETSI EN 319 522 [i.21] and ETSI EN 319 532 [i.22] include relevant modifications to certain aspects defined in ETSI TS 102 640 [i.23] (among which, for instance, change in schema for evidence, definition of new evidence, changes in the contents of the messages, etc.), resultant of comments arrived from stakeholders and findings of an ESI team that worked before the start of the STF, in the identification of fixes required by the aforementioned ETSI TS.

The following clauses from 5.1.2 to 5.1.6 outline, in a structured way, all these aspects.

The tables contained in the aforementioned clauses summarize the semantics and syntactical differences between the definitions specified in ETSI EN 319 532-1 [i.1] and the definitions specified in ETSI TS 102 640-1 [i.9].

Only the definitions that are relevant for the present gap analysis appear in the tables. All the terms used but undefined in the tables may be found in the respective specification of provenance.

5.1.2 Changes on terms and boundary roles

Table 1 and Table 2 summarize similarities and differences between definitions, components and roles of ETSI EN 319 532-1 [i.1] and ETSI TS 102 640-1 [i.9].

Table 1: Definitions defined in ETSI EN 319 532-1 [i.1] and ETSI TS 102 640-1 [i.9], similarities and differences

#	Terms as per ETSI EN 319 532-1 [i.1] Terms as per ETSI TS 102 640-1 [i.9]	Definitions as per ETSI TS 102 640-1 [i.9]	Definitions as per ETSI EN 319 532-1 [i.1]
1	Consignment N/A		Act of making the user content available to the recipient within the boundaries of the electronic registered delivery service
2	ERDS evidence REM-MD evidence	Signed data created within a REM-MD, which proves that a certain event has occurred at a certain time	Data generated by the electronic registered delivery service, which aims to prove that a certain event has occurred at a certain time
3	Handover N/A		Act of having the user content successfully cross the border of the recipient's electronic registered delivery service towards the recipient's ERD user agent/application
4	original message original message	e-mail message generated by the Sender's User Agent or under the Sender's technical/legal responsibility (i.e. outside of the REM-MD), which may be signed by the Sender	Data including user content and submission metadata
5	Registered Electronic Mail Service (REMS) REM Management Domain (REM-MD)	Set of technical and physical components, personnel, policies and processes that provide REM services	Electronic registered delivery service which builds on the formats, protocols and mechanisms used in ordinary e-mail messaging
6	Registered Electronic Mail Service Provider (REMSP) N/A	See note.	Entity which provides registered electronic mail service
7	REM dispatch REM dispatch	REM-MD Envelope containing the Original Message and related REM-MD Evidence	Data composed of a user content, some ERDS relay metadata and ERDS evidence, in the form of a REM envelope
8	REM envelope REM-MD envelope	Signed structure generated by the REM-MD which envelopes an Original message and/or REM-MD Evidence	Signed data structure generated by the registered electronic mail service which contains any of the user content, ERDS relay metadata and/or ERDS evidence
9	REM message REM-MD Message	Message generated by the REM MD under the REM MD sole technical/legal responsibility (i.e. inside of the REM MD)	Data composed of an optional user content, ERDS relay metadata and zero or more ERDS evidence, in the form of a REM envelope
10	REM payload 		REM message which contains the user content and some ERDS relay metadata
11	REM interoperability domain REM Policy Domain	Any domain where a common set of rules (e.g. legal, company policy or agreement) is enforced for the provision of REM services	Homogeneous operational space consisting of a set of REMSPs able to properly interoperate among themselves
12	REM interoperability domain rules REM Policy	Set of rules (e.g. legal, company policy or agreement) enforced for the provision of REM Services	Set of rules defining a REM interoperability domain
13	REMS notification N/A		Data composed of ERDS relay metadata and zero or more ERDS evidence, in the form of a REM envelope, which includes a reference to the user content to be delivered
14	REMS receipt N/A		Data composed of ERDS relay metadata and ERDS evidence, in the form of a REM envelope
15	user content N/A		Original data produced by the sender which has to be delivered to the recipient
16	N/A REM Object	Message object handled by a REM-MD. This is a REM-MD Message, REM-Dispatch or Original message	

NOTE: In some form and in some case, REMSP is mapped to REM-MD.

Table 2: Components/roles defined in ETSI EN 319 532-1 [i.1] and ETSI TS 102 640-1 [i.9], similarities and differences

#	Components as per ETSI EN 319 532-1 [i.1] Roles as per ETSI TS 102 640-1 [i.9]	Description of roles as per ETSI TS 102 640-1 [i.9]	Description of components as per ETSI EN 319 532-1 [i.1]
1	REMS message delivery agent REM-MD Message Transfer Agent	Role that supports the transfer of REM Objects to REM Recipient's and REM Sender's REM Message Store either directly or via the REM Object Relay Interface into another REM-MD or via a REM-MD Message Gateway.	REMS message delivery agent is equivalent to the component "ERDS Message delivery system" (defined in ETSI EN 319 522-1 [i.4]): this component grants that the user content submitted by the sender is made available to the intended recipient. Note that this does not necessarily imply a transfer of the data (e.g. the delivery can consist in making existing data available to the recipient).
2	REMS evidence provider REM-MD Evidence Provider	Role that issues REM-MD Evidence.	REM-MD Evidence Provider is equivalent to the component "ERDS Evidence provider" (defined in ETSI EN 319 522-1 [i.4]): this component produces the ERDS evidence upon completion of specific delivery events.
3	REMS evidence repository REMS message store REM-MD repository message archive REM Message Store	REM-MD repository: Role that supports the storage of REM Objects, REM-MD Evidence and any other, which will be accessed by reference. message archive: optional role that supports storage of REM Objects and REM-MD Evidence, as required for later use for evidential or any other legally admitted purposes, at the relevant REM-MD for an indefinite or definite time period, to be accessed once or many times by one or more entities. REM Message Store: role that supports the storage of REM Objects. In other words the set of mailboxes of the users.	REMS evidence repository is equivalent to the component "ERDS Evidence repository" (defined in ETSI EN 319 522-1 [i.4]): this component grants the persistence of ERDS evidence for a period of time which depends on the specific policies of the service. Storing of the ERDS evidence can be performed by a third party service, outside the ERDS. In addition to the general ERDS components, a REMS also provides a REMS message store component. A REMS message store is allocated to the senders and recipients, and is securely accessible by senders and recipients respectively to retrieve REM messages addressed to them.
4	REMS user directory REM-MD repository	In interoperability profile ETSI TS 102 640-6-1 [i.11] the PReM Directory Service was mapped inside the REM-MD repository role.	REMS user directory is equivalent to the component "ERDS User directory" (defined in ETSI EN 319 522-1 [i.4]): this component is used to translate the unique identification of a recipient, possibly augmented by further metadata, into a delivery endpoint. The same recipient can correspond to more delivery endpoints, depending on metadata (e.g. user content and evidence, or even different types of user content, can be directed to different endpoints).
5	REMS REM-MD Evidence Verifier	Role that supports the verification of REM-MD Evidence.	This task is performed generally by REMS.
6	Registered Electronic Mail Service Provider (REMSP) REM-MD Message Gateway	Role that supports the transfer of REM objects to conventional e-mail (e.g. Internet) services and physical postal delivery services.	Entity which provides registered electronic mail service. In the most general case a service provider acting as a REMSP could also be able to communicate using other formats and protocols which are different from REM, and thus provide interconnection with other types of ERDSs. An intermediate ERDS could also provide such protocol conversion, thereby acting as a gateway between a REM and a non-REM ERDS.

#	Components as per ETSI EN 319 532-1 [i.1] Roles as per ETSI TS 102 640-1 [i.9]	Description of roles as per ETSI TS 102 640-1 [i.9]	Description of components as per ETSI EN 319 532-1 [i.1]
7	ERD User Agent/Application (ERD-UA) REM User Agent (REM-UA)	Entity by which REM Senders, REM Recipients participate in the exchange of REM Objects and Third Parties may access REM Objects.	System consisting of software and/or hardware components by which senders and recipients participate in the exchange of data with electronic registered delivery service providers.
8	recipient REM Recipient	Physical or legal entity legally responsible for the mailbox to which the original message is addressed.	Natural or legal person to which the user content is addressed.
9	sender REM Sender	Physical or legal entity legally responsible for the mailbox from which the original message has been sent.	Natural or legal person that has submitted the user content.
10	N/A REM Third Party	Party authorized to access REM Objects and REM-MD Evidence for specific purposes.	

5.1.3 Changes on event and evidence types

Table 3 and Table 4 summarize similarities and differences between events, flows and interfaces of ETSI EN 319 532-1 [i.1] and ETSI TS 102 640-1 [i.9].

These events are mentioned in clause 7 of ETSI TS 102 640-6-1 [i.11] on both the following directions of the flow:

1) Table 4 [i.11]: GAP Analysis - Transmission/Relay/Delivery - REM-MD → DO
2) Table 5 [i.11]: GAP Analysis - Transmission/Relay/Delivery - DO → REM-MD
3) Table 6 [i.11]: GAP Analysis - Retrieval - REM-MD → DO
4) Table 7 [i.11]: GAP Analysis - Retrieval - DO → REM-MD

In fact, the meaning that the events assume at gateway level has to be considered, respectively, in accordance and in the order in which they appear in the flows described in Table 4, Table 5, Table 6 and Table 7 of ETSI TS 102 640-6-1 [i.11].

Table 3: Events on flows interfaces in ETSI EN 319 532-1 [i.1] and ETSI TS 102 640-1 [i.9], similarities and differences

#	Events as per ETSI EN 319 532-1 [i.1] Events as per ETSI TS 102 640-1 [i.9]	Description of events as per ETSI TS 102 640-1 [i.9]	Description of events as per ETSI EN 319 532-1 [i.1]
1	6.2.2 B. Events related to the relay between REMSs - Table 4 - B.1 RelayAcceptance 6.2.2 Event B.1 - R-REM-MD Acceptance	One REM Object sent by the REM Sender's REM-MD and successfully received by the REM Recipient's REM-MD, was accepted by the latter	*"The receiving REMS has accepted the relayed REM message containing user content, and the REMSP takes responsibility for handling it according to the requirements in the present document and the policy rules."*
2	6.2.2 B. Events related to the relay between REMSs - Table 4 - B.2 RelayRejection 6.2.2 Event B.2 - R-REM-MD Rejection	One REM Object sent by the REM Sender's REM-MD and successfully received by the REM Recipient's REM-MD, was rejected by the latter due to policy, formal or technical reasons	*"The receiving REMS has rejected the relayed REM message containing user content. The receiving REMS shall inform the sending REMS about the reason(s) for the rejection."*
3	6.2.2 B. Events related to the relay between REMSs - Table 4 - B.3 RelayFailure 6.2.2 Event B.3 - Expiration of time to deliver to R-REM-MD	It was impossible to deliver within a given time period a REM Object to the REM Recipient's REM-MD due to technical errors and/or other problems	*"The sending REMS was unable to relay the REM message containing user content to the receiving REMS within a given time period, or the receiving REMS did not return ERDS evidence about the acceptance or rejection of the REM message within that time period."*
4	6.2.4 D. Events related to the consignment - Table 6 - D.1 ContentConsignment 6.2.3 Event C.1 - Message Delivery	REM Object was delivered to the REM Recipient's mailbox at a specific time	*"R-REMS has made the user content available to the recipient".*
5	6.2.4 D. Events related to the consignment - Table 6 - D.2. ContentConsignmentFailure 6.2.3 Event C.2 - Expiration of time to deliver message	REM Object could not be delivered to the REM Recipient's mailbox within a given time period due to technical errors and/or other reasons; Furthermore, no prove of delivery within a given period exists	*"The REMS could not make the user content available to the recipient within a given time period, or the REMS did not receive ERDS evidence within a given time period about the successful or unsuccessful consignment of the user content from the other REMS to which it had relayed the user content."*
6	6.2.5 E. Events related to the handover to the recipient - Table 7 - E.1. ContentHandover 6.2.3 Event F.1 (mailbox) -Retrieval	REM Object present in the REM Recipient's mailbox was retrieved by the REM Recipient	*"The user content has successfully passed through the REM MRI from the REMS to the client under the responsibility of the recipient."*
7	6.2.5 E. Events related to the handover to the recipient - Table 7 - E.2. ContentHandoverFailure 6.2.3 Event F.2 (mailbox) - Expiration of time for Retrieval	REM Object present in the REM Recipient's mailbox was not retrieved by the REM Recipient's mail client within a given period	*"The user content did not pass through the REM MRI within a given time".*

In ERDS/REMS specification there is not a specific name definition for any evidence generated in the flowing of the information. Rather, any evidence is fully identified by the event causing it.

Table 4 outlines the differences and mapping with the evidence set, concerning the restricted scope of the interoperability profile, defined in ETSI TS 102 640-2 [i.10]. ERDS has to be interpreted as a synonym of REMS.

Table 4: Evidence on flows interfaces defined in ETSI EN 319 532-1 [i.1] and ETSI TS 102 640-2 [i.10], similarities and differences

#	Relevant evidence as per ETSI EN 319 522-1 [i.4] Relevant evidence as per ETSI TS 102 640-2 [i.10]	Description of evidence as per ETSI TS 102 640-2 [i.10]	Description of evidence as per ETSI EN 319 522-1 [i.4]
1	Evidence for: 6.2.2 B. Events related to the relay between REMSs - Table 4 - B.1 RelayAcceptance 6.2.2 B. Events related to the relay between REMSs - Table 4 - B.2 RelayRejection 5.1.2 Evidence RelayToREMMDAcceptanceRejection	Evidence to prove that one REM-MD Message/REM Dispatch sent by the sender's REM-MD was successfully received by the recipient's REM-MD that accepted/rejected it.	The related evidence attests that, in situations where several ERDSs are co-operating (as in 4-corner model and extended model above), an intermediate or the recipient's ERDS has accepted (B.1)/rejected (B.2) one ERD message sent by the previous ERDS in the aforementioned chain.
2	Evidence for: 6.2.2 B. Events related to the relay between REMSs - Table 4 - B.3 RelayFailure 5.1.3 Evidence RelayToREMMDFailure	Evidence to prove that it was impossible to deliver a REM-MD Message/REM Dispatch within a given time period to the recipient's REM-MD due to technical errors and/or other problems.	The related evidence attests that, at the time specified in the evidence, it was impossible (or it is clear that it will be impossible) to deliver an ERD message within a given time period to either an intermediate ERDS provider or to the recipient's ERDS provider due to technical errors and/or other problems.
3	Evidence for: 6.2.4 D. Events related to the consignment - Table 6 - D.1 ContentConsignment 6.2.4 D. Events related to the consignment - Table 6 - D.2. ContentConsignmentFailure 5.1.4 Evidence DeliveryNonDeliveryToRecipient	Evidence to prove that the REM-MD Message/REM Dispatch was delivered to the recipient's mailbox or, OPTIONALLY, to a delegate's mailbox at a specific time or that it was not possible to deliver it within a given time period: 1) The recipient's REM-MD successfully deposited/was not able to deposit within a given time period a REM-MD Message/REM Dispatch into the recipient's or, OPTIONALLY, a delegate's REM mailbox. 2) The sender's REM-MD did not receive within a given time period from the recipient's REM-MD a REM-MD Evidence of successful/unsuccessful delivery.	The related evidence attests that: 1) (D.1) the user content, at a specific time indicated by the evidence, was made available for the recipient - through proper identification and authentication - within the boundaries of the ERDS; 2) (D.2) the user content could not be made available to the recipient within a given time period. • The recipient's ERDS was not able to consign the user content to the recipient. In this case the evidence is produced by the R-ERDS. • A relaying ERDS did not receive within a given time period from the relayed ERDS an evidence of successful or unsuccessful consignment. In this case it is the relaying ERDS that creates the evidence with the suitable reason code.
4	Evidence for: 6.2.5 E. Events related to the handover to the recipient - Table 7 - E.1. ContentHandover 6.2.5 E. Events related to the handover to the recipient - Table 7 - E.2. ContentHandoverFailure 5.1.6 Evidence RetrievalNonRetrievalByRecipient	Evidence to prove that the REM-MD Message/REM Dispatch present in the recipient's mailbox was retrieved/non retrieved within a given period - by the recipient or, OPTIONALLY, by a recipient's delegate.	The related evidence attests that: 1) (E.1) the user content at a specific time indicated by the evidence crossed the R-ERDS border and was handed to the recipient UA/Application upon proper authentication. 2) (E.2) the user content could not cross the R-ERDS border toward the recipient's ERD-UA after a certain number of attempts or a timeout as specified by the applicable policies.

5.1.4 Changes on messages

5.1.4.1 Introduction

The following clauses summarize the semantics and syntactical differences between the REM Messages components specified in ETSI EN 319 532-3 [i.3] and the REM Messages components specified in ETSI TS 102 640-2 [i.10].

All the aforementioned tables have the same format, explained in the following paragraphs.

Cells in first column (**#**) numerate the rows so that from one cell of the table a reference can be made to a certain row.

Cells in second column are split in two rows. The first row (**<Component to be compared> as per ETSI EN 319 532-3 [**i.3]) identifies the component under analysis and specified [i.3]. The second row (**<Component to be compared> as per ETSI TS 102 640-2 [**i.10**]**) identifies the component under analysis and specified [i.10].

Cells in third column (**In <Component to be compared> as per ETSI TS 102 640-2 [**i.10**]**) shows details of the component as specified in ETSI TS 102 640-2 [i.10]. These details can include simple values of the components, or the content model (sub-components).

Cells in fourth column (**In <Component to be compared> as per ETSI EN 319 532-3 [**i.3**]**) shows details of the component as specified in ETSI EN 319 522-3 [i.6]. In addition to these details, cells in this column include, most of the times, rationales and/or highlights of specific differences between this component in the REM Message analysed in the table and the corresponding component in the corresponding REM Message as specified in ETSI TS 102 640-2 [i.10].

5.1.4.2 Metadata implemented as optional extension headers in REM messages

Table 5 compares metadata:

- whose semantics and syntax have been defined in ETSI TS 102 640-2 [i.10] with metadata;
- whose incorporation, as optional extension headers to REM messages, has been specified in ETSI EN 319 532-3 [i.3], and which are based on;
- the semantics that has been defined in ETSI EN 319 522-2 [i.5]; and
- the formats that have been defined in ETSI EN 319 522-3 [i.6].

Table 5: Optional extension header fields defined in ETSI EN 319 532-3 [i.3] and ETSI TS 102 640-2 [i.10], similarities and differences

#	**Optional extension header fields as per ETSI EN 319 532-3 [i.3]** **Optional extension header fields as per ETSI TS 102 640-2 [i.10]**	**In Outermost MIME header as per ETSI TS 102 640-2 [i.10]**	**In Outermost MIME header as per ETSI EN 319 532-3 [i.3]**
1	REM-Message-Type X-REM-Msg-Type: <value>	ETSI TS 102 640-2 [i.10] allows the existence of these optional Extension header fields, for including information on whether the message is a REM Dispatch or another type of REM message.	ETSI EN 319 532-3 [i.3] requires the usage of the new REM-Message-Type header field, set to an URI value that identifies the type of REM message as defined in clause 4.3.5 of ETSI EN 319 522-3 [i.6] and clause 6.1 of ETSI EN 319 532-3 [i.3] itself.
2	REM-MessageDigest X-REM-hashValue	ETSI TS 102 640-2 [i.10] allows the existence of X-REM-hashValue optional Extension header field for including digest value of the message submitted by the sender.	ETSI EN 319 532-3 [i.3] defines the new REM-MessageDigest for the same purpose.
3	REM-DigestAlgorithm X-REM-hashAlgorithm	ETSI TS 102 640-2 [i.10] allows the existence of this X-REM-hashAlgorithm optional Extension header field for including the identifier of the digest algorithm used for computing the digest value of the message submitted by the sender.	ETSI EN 319 532-3 [i.3] defines the new REM-DigestAlgorithm for the same purpose.
4	REM-UAMessageIdentifier X-REM-UAMessageIdentifier	ETSI TS 102 640-2 [i.10] allows the existence of this X-REM-UAMessageIdentifier optional Extension header field for including the unique identifier of the original message as generated by S-REMS.	ETSI EN 319 532-3 [i.3] defines this new REM-UAMessageIdentifier optional Extension header field for carrying the same information.

#	Optional extension header fields as per ETSI EN 319 532-3 [i.3] Optional extension header fields as per ETSI TS 102 640-2 [i.10]	In Outermost MIME header as per ETSI TS 102 640-2 [i.10]	In Outermost MIME header as per ETSI EN 319 532-3 [i.3]
5	NA Other X-REM-<component> optional extension header fields	ETSI TS 102 640-2 [i.10] allows the existence of other optional Extension header fields for including additional information.	ETSI EN 319 532-3 [i.3] defines new additional optional Extension header fields as shown in rows below. All of them come from mapping metadata contents whose semantics is specified in ETSI EN 319 522-2, and whose syntax is defined in 319 522-3 [i.5], to MIME structures, as specified in clause 6.1 of ETSI EN 319 532-3 [i.3].
6	REM-MetadataVersion NA	ETSI TS 102 640-2 [i.10] does not define this optional Extension header field.	ETSI EN 319 532-3 [i.3] defines this new optional Extension header field for carrying the identifier of the version of the metadata set.
7	REM-RelayDate NA	ETSI TS 102 640-2 [i.10] does not define this optional Extension header field.	ETSI EN 319 532-3 [i.3] defines this new optional Extension header field for carrying the date and time when an ERDS relays the ERD message to the next ERDS in the delivery chain.
8	REM-ExpirationDate NA	ETSI TS 102 640-2 [i.10] does not define this optional Extension header field.	ETSI EN 319 532-3 [i.3] defines this new optional Extension header field for carrying the date-time by which the consignment or handover to recipient is required to be completed.
9	REM-RecipientAssuranceLevel NA	ETSI TS 102 640-2 [i.10] does not define this optional Extension header field.	ETSI EN 319 532-3 [i.3] defines this new optional Extension header field for carrying the level of assurance of the process of verification of the identity of the recipient that the sender requires.
10	REM-ApplicablePolicy NA	ETSI TS 102 640-2 [i.10] does not define this optional Extension header field.	ETSI EN 319 532-3 [i.3] defines this new optional Extension header field for carrying the identifier of the policy that the S-ERDS requires to be applied to the management of the ERD message by the subsequent ERDSs in the delivery chain.
11	REM-ModeOfConsignment NA	ETSI TS 102 640-2 [i.10] does not define this optional Extension header field.	ETSI EN 319 532-3 [i.3] defines this new optional Extension header field for carrying the identifier of the requested mode of consignment of the user content to the recipient chosen among the following options: basic, consented, consented signed, or other (not specified in [i.3]).
12	REM-ScheduledDelivery NA	ETSI TS 102 640-2 [i.10] does not define this optional Extension header field.	ETSI EN 319 532-3 [i.3] defines this new optional Extension header field for carrying the time instant after which the user content can be consigned/handed over.
13	REM-EventIdentifier NA	ETSI TS 102 640-2 [i.10] does not define this optional Extension header field (see note).	ETSI EN 319 532-3 [i.3] defines this new optional Extension header field for carrying the identifier of the event that has triggered the issuance of the evidence.
NOTE: Actually the ETSI TS 102 640-5 [i.34] (REM-MD Interoperability profiles) defines some more header fields including: X-REM-EvidenceType and X-REM-EventCode - the combination of these two old headers is the counterpart of the new REM-EventIdentifier header.			

5.1.4.3 Differences in the outermost MIME section header of a REM message

Table 6 compares the components of the outermost MIME header as specified in ETSI EN 319 522-3 [i.6], with the outermost MIME header as specified in ETSI TS 102 640-2 [i.10].

Table 6: Differences in the outermost MIME section headers as per ETSI EN 319 532-3 [i.3] and the outermost MIME section header as per ETSI TS 102 640-2 [i.10]

#	Outermost MIME section header component as per Table 3 of ETSI EN 319 532-3 [i.3] Outermost MIME section header component as per clause 4.1 of ETSI TS 102 640-2 [i.10]	In Outermost MIME section header as per ETSI TS 102 640-2 [i.10]	In Outermost MIME section header as per ETSI EN 319 532-3 [i.3]
1	Content-Type	Value: "multipart/signed". 'protocol' parameter value: application/pkcs7-signature". Recommended 'micalg' parameter value be conformant to ETSI TS 102 176-1 [i.16].	Value: "multipart/signed". 'protocol' parameter value: application/pkcs7-signature". Recommended 'micalg' parameter value be conformant to ETSI TS 119 312 [i.18]. Recommended 'boundary' parameter value be conformant to IETF RFC 2046 [i.20], section 5.1.1.
2	To	Its value is always equal to the value of the 'To' header field in the original message.	If the message carries evidence for the sender, this field can match the value of the 'From' header field in the original message. If the message is a REM dispatch or REM payload, then its value is always equal to the value of the 'To' header field in the original message.
3	Reply-To	Its value always matches the value of the 'From' header field in the original message.	If the message carries evidence for the sender ETSI EN 319 532-3 [i.3] recommends that this header is not present, and if it is present, then it recommends that its value is the REM service address. If the message is a REM dispatch or REM payload, then its value is always equal to the value of the 'From' header field in the original message.
4	Cc	ETSI TS 102 640-2 [i.10] does not specify any requirement for this header field.	See in clause 6.2.1 of ETSI EN 319 532-3 [i.3] the requirements for this header field.
5	Subject	Its recommended value is transformed from the Subject of the original sender's message, e.g.: "REM Dispatch: subject_of_original_message" or "REM Delivery Receipt: subject_of_original_message".	Its recommended value is transformed from the Subject of the original sender's message: REM <event identifier>: <original subject> (E.g.: "REM `ContentConsignment`: subject_of_original_message").
6	Return-Path	ETSI TS 102 640-2 [i.10] does not specify any requirement for this header field.	See in clause 6.2.1 of ETSI EN 319 532-3 [i.3] the requirements for this header field.
7	Received	ETSI TS 102 640-2 [i.10] does not specify any requirement for this header field.	See in clause 6.2.1 of ETSI EN 319 532-3 [i.3] the requirements for this header field.
8	In-Reply-To	ETSI TS 102 640-2 [i.10] does not specify any requirement for this header field.	See in clause 6.2.1 of ETSI EN 319 532-3 [i.3] the requirements for this header field.

5.1.4.4 Differences in the signed data MIME section header of a REM message

Table 7 compares the components of the signed data MIME section header as specified in ETSI EN 319 522-3 [i.6], with the signed data MIME section header as specified in ETSI TS 102 640-2 [i.10].

Table 7: Differences in the signed data MIME section header as per ETSI EN 319 532-3 [i.3] and the signed data MIME section header as per ETSI TS 102 640-2 [i.10]

#	Signed data MIME section header component as per Table 4 of ETSI EN 319 532-3 [i.3] / Signed data MIME section header component as per clause 4.2 of ETSI TS 102 640-2 [i.10]	In signed data MIME section header as per ETSI TS 102 640-2 [i.10]	In signed data MIME section header as per ETSI EN 319 532-3 [i.3]
1	Content-Type	Value: "multipart/mixed".	Value: "multipart/mixed". Recommended 'boundary' parameter value be conformant to IETF RFC 2046 [i.20], section 5.1.1.

5.1.4.5 Differences in the Introduction MIME section header of a REM message

Table 8, Table 9 and Table 10 compare the components of the introduction MIME section header as specified in ETSI EN 319 522-3 [i.6], with the introduction MIME section header as specified in ETSI TS 102 640-2 [i.10].

Table 8: Differences in the introduction MIME section header as per ETSI EN 319 532-3 [i.3] and the introduction MIME section header as per ETSI TS 102 640-2 [i.10]

#	Introduction MIME section header component as per Table 5 of ETSI EN 319 532-3 [i.3] / Introduction MIME section header component as per clause 4.4 of ETSI TS 102 640-2 [i.10]	In introduction MIME section header as per ETSI TS 102 640-2 [i.10]	In introduction MIME section header as per ETSI EN 319 532-3 [i.3]
1	Content-Type	Value: "multipart/alternative".	Value: "multipart/alternative". Recommended 'boundary' parameter value be conformant to IETF RFC 2046 [i.20], section 5.1.1.
2	REM-Section-Type X-REM-Section-Type	Value for X-REM-Section-Type header field: "rem_message/introduction".	Value for REM-Section-Type header field: "rem_message/introduction".

Table 9: Differences in the FREE-TEXT introduction MIME section header fields body as per ETSI EN 319 532-3 [i.3] and the introduction MIME section header constraints as per ETSI TS 102 640-2 [i.10]

#	Introduction MIME section header component as per Table 6 of ETSI EN 319 532-3 [i.3] Introduction MIME section header component as per clause 4.4.1 of ETSI TS 102 640-2 [i.10]	In introduction MIME section header as per ETSI TS 102 640-2 [i.10]	In introduction MIME section header as per ETSI EN 319 532-3 [i.3]
1	Content-Type	Value: "text/plain". Recommended 'charset' parameter value be conformant to UTF-8.	Value: "text/plain". Recommended 'charset' parameter value be conformant to UTF-8.
2	Content-Disposition	Value: "inline".	Value: "inline".
3	Content-Transfer-Encoding	Value: 7bit.	Value: "7bit, 8bit or quoted-printable".

Table 10: Differences in the HTML introduction MIME section header fields body as per ETSI EN 319 532-3 [i.3] and the Html MIME section header constraints as per ETSI TS 102 640-2 [i.10]

#	Introduction MIME section header component as per Table 7 of ETSI EN 319 532-3 [i.3] Introduction MIME section header component as per clause 4.4.2 of ETSI TS 102 640-2 [i.10]	In introduction MIME section header as per ETSI TS 102 640-2 [i.10]	In introduction MIME section header as per ETSI EN 319 532-3 [i.3]
1	Content-Type	Value: "text/html". Recommended 'charset' parameter value be conformant to UTF-8.	Value: "text/html". Recommended 'charset' parameter value be conformant to UTF-8.
2	Content-Transfer-Encoding	Value: 7bit or quoted-printable.	Value: "7bit, 8bit or quoted-printable".

5.1.4.6 Differences in the original message MIME section header of a REM message

Table 11 compares the components of the original message MIME header as specified in ETSI EN 319 522-3 [i.6], with the Original message MIME header as specified in ETSI TS 102 640-2 [i.10].

Table 11: Differences in the original message MIME section header fields as per ETSI EN 319 532-3 [i.3] and the Original message MIME section header constraints as per ETSI TS 102 640-2 [i.10]

#	Original message MIME section header component as per Table 8 of ETSI EN 319 532-3 [i.3] Original message MIME section header component as per clause 4.5 of ETSI TS 102 640-2 [i.10]	In original message MIME section header as per ETSI TS 102 640-2 [i.10]	In original Message MIME section header as per ETSI EN 319 532-3 [i.3]
1	Content-Type	Value: "message/rfc822". 'name' parameter value: AttachedMimeMessage.	Value: "message/rfc822". 'name' parameter value: "AttachedMimeMessage".
2	Content-Disposition	Value: "attachment". filename=AttachedMimeMessage.	Value: "attachment". 'filename' parameter: same value of the 'name' parameter of the Content-Type: header field.
3	Content-Transfer-Encoding	Value: 7bit.	Value: "binary".
4	Content-Description	<not specified>	Value: a brief text description.
5	REM-Section-Type X-REM-Section-Type	Value for X-REM-Section-Type header field: "rem_message/original".	Value for REM-Section-Type header field: "rem_message/original".

5.1.4.7 Differences in the extensions MIME section header of a REM message

Table 12 compares the components of the extensions MIME header as specified in ETSI EN 319 522-3 [i.6], with the Extensions MIME header as specified in ETSI TS 102 640-2 [i.10].

Table 12: Differences in the extensions MIME section header fields as per ETSI EN 319 532-3 [i.3] and the Extension MIME section header constraints as per ETSI TS 102 640-2 [i.10]

#	Extensions MIME section header component as per Table 9 of ETSI EN 319 532-3 [i.3] Extensions MIME section header component as per clause 4.6 of ETSI TS 102 640-2 [i.10]	In extensions MIME section header as per ETSI TS 102 640-2 [i.10]	In extensions MIME section header as per ETSI EN 319 532-3 [i.3]
1	Content-Type	Value: "application/xml". 'name' parameter value: "REMExtension.xml". 'charset' parameter value: "URF-8".	Value: "application/xml" or "application/octet-stream". 'name' parameter value: <REM_EXTENSION_NAME>. Recommended 'charset' parameter value be conformant to UTF-8 for XML attachments.
2	Content-Disposition	Value: "attachment". 'filename' parameter: same value of the 'name' parameter of the Content-Type header.	Value: "attachment". 'filename' parameter: same value of the 'name' parameter of the Content-Type: header field.
3	Content-Transfer-Encoding	Value: "quoted-printable".	Value: "quoted-printable", "base64" or "binary".
4	Content-Description	<not specified>.	Value: a brief text description.
5	REM-Section-Type X-REM-Section-Type	Value for X-REM-Section-Type header field: "rem_message/extension".	Value for REM-Section-Type header field: "rem_message/extension".
6	REM-Extension-Namespace-URI	<not specified>.	Value: the namespace URI relevant to the extension.
7	REM-Extension-Code X-REM-Extension-Code	Value: in accordance with the type of the attachment, a unique code identifying the type of extension in order to allow automatic processing.	Value: in accordance with the type of the attachment, a unique code identifying the type of extension in order to allow automatic processing.

5.1.4.8 Differences in the evidence MIME section header of a REM message

Table 13 and Table 14 compare the components of the evidence set MIME header as specified in ETSI EN 319 522-3 [i.6], with the Evidence MIME header as specified in ETSI TS 102 640-2 [i.10].

Table 13: Differences in the XML ERDS evidence MIME section header fields as per ETSI EN 319 532-3 [i.3] and the XML REM-MD Evidence MIME section header constraints as per ETSI TS 102 640-2 [i.10]

#	XML ERDS evidence MIME section header component as per Table 10 of ETSI EN 319 532-3 [i.3] XML REM-MD Evidence MIME section header component as per clause 4.7.2 of ETSI TS 102 640-2 [i.10]	In XML REM-MD evidence MIME section header as per ETSI TS 102 640-2 [i.10]	In XML ERDS Evidence MIME section header as per ETSI EN 319 532-3 [i.3]
1	Content-Type	Value: "application/xml". 'name' parameter value: "<REM_EVIDENCE_NAME>.xml". 'charset' parameter value: "URF-8".	Value: "application/xml". 'name' parameter value: "<REM_EVIDENCE_NAME>.xml". 'charset' parameter value be conformant to UTF-8.
2	Content-Disposition	Value: "attachment". 'filename' parameter: same value of the 'name' parameter of the Content-Type header.	Value: "attachment". 'filename' parameter: same value of the 'name' parameter of the Content-Type: header field.
3	Content-Transfer-Encoding	Value: "quoted-printable".	Value: "quoted-printable", "base64" or "binary".
4	Content-Description	<not specified>.	Value: a brief text description.
5	REM-Section-Type	<not specified>.	Value for REM-Section-Type header field: "rem_message/xml_evidence".

Table 14: Differences in the PDF ERDS evidence MIME section header fields as per ETSI EN 319 532-3 [i.3] and the PDF REM-MD Evidence MIME section header constraints as per ETSI TS 102 640-2 [i.10]

#	PDF ERDS evidence MIME section header component as per Table 10 of ETSI EN 319 532-3 [i.3] PDF REM-MD Evidence MIME section header component as per clause 4.7.3 of ETSI TS 102 640-2 [i.10]	In PDF REM-MD evidence MIME section header as per ETSI TS 102 640-2 [i.10]	In PDF ERDS Evidence MIME section header as per ETSI EN 319 532-3 [i.3]
1	Content-Type	Value: "application/pdf". 'name' parameter value: "<REM_EVIDENCE_NAME>.pdf".	Value: "application/pdf". 'name' parameter value: "<REM_EVIDENCE_NAME>.pdf".
2	Content-Disposition	Value: "attachment". 'filename' parameter: same value of the 'name' parameter of the Content-Type header.	Value: "attachment". 'filename' parameter: same value of the 'name' parameter of the Content-Type: header field.
3	Content-Transfer-Encoding	Value: "base64".	Value: "base64" or "binary".
4	Content-Description	<not specified>.	Value: a brief text description.
5	REM-Section-Type	<not specified>.	Value for REM-Section-Type header field: "rem_message/pdf_evidence".

NOTE: Another difference at "evidence" level between and ETSI EN 319 532 [i.22] and ETSI TS 102 640 [i.23] is that the new REM standard no longer specifies evidence in ASN.1 formats. ERDS evidence set, used in REMS, is based on XML format. PDF evidence may be also provided, but the relevant format is out of scope of REMS standard.

5.1.4.9 Differences in the signature MIME section header of a REM message

Table 15 compares the components of the signature MIME header as specified in ETSI EN 319 522-3 [i.6], with the Signature MIME header as specified in ETSI TS 102 640-2 [i.10].

Table 15: Differences in the REMS signature MIME section header fields as per ETSI EN 319 532-3 [i.3] and the REM-MD Signature MIME section header constraints as per ETSI TS 102 640-2 [i.10]

#	REMS signature MIME section header component as per Table 12 of ETSI EN 319 532-3 [i.3] REM-MD Signature MIME section header component as per clause 4.3 of ETSI TS 102 640-2 [i.10]	In REM-MD signature MIME section header as per ETSI TS 102 640-2 [i.10]	In REMS Signature MIME section header as per ETSI EN 319 532-3 [i.3]
1	Content-Type	Value: "application/pkcs7-signature". 'name' parameter value: "smime.p7s".	Value: "application/pkcs7-signature". 'name' parameter value: "smime.p7s".
2	Content-Disposition	Value: "attachment". 'filename' parameter recommended value: "smime.p7s".	Value: "attachment". 'filename' parameter recommended value: "smime.p7s".
3	Content-Transfer-Encoding	Value: "base64".	Value: "base64".
4	Content-Description	The value for this header field may be: "S/MIME Cryptographic Signature".	The value for this header field may be: "S/MIME Cryptographic Signature".

NOTE: All header fields have the same requirements here, so actually there is no difference between ETSI TS 102 640 [i.23] and ETSI EN 319 532 [i.22] in the signature MIME section headers.

5.1.5 Changes on evidence structure and semantic

The present clause summarizes the differences between the ERDS Evidence specified in ETSI EN 319 522-3 [i.6] and the REM Evidence specified in ETSI TS 102 640-2 [i.10].

Table 16 shows the differences between ERDS Evidence as specified by ETSI EN 319 522-3 [i.6] and REM Evidence as specified by ETSI TS 102 640-2 [i.10].

Cells in first column (**#**) numerate the rows so that from one cell of the table a reference can be made to a certain row.

Cells in second column are split in two rows. The first row (**ERDS Evidence Component as per ETSI EN 319 522-3 [**i.6**]**) identifies the ERDS Evidence component under analysis. The second row (**ERDS Evidence Component as per ETSI TS 102 640-2 [**i.10**]**) identifies the corresponding (whenever such a component existed) REM Evidence component.

Cells in third column (**In REM Evidence as per ETSI TS 102 640-2 [**i.10**]**) shows details of the component as specified in ETSI TS 102 640-2 [i.10]. These details can include simple values of the components (like in the case of attribute `version`), or the content model (sub-components) (as in the case of `EvidenceIssuerDetails`).

Cells in fourth column (**In ERDS Evidence as per ETSI EN 319 522-3 [**i.6**]**) shows details of the component as specified in ETSI EN 319 522-3 [i.6]. In addition to these details, cells in this column include, most of the times, rationales and/or highlights of specific differences between the component in ERDS Evidence and the corresponding component in REM Evidence.

Table 16: Differences between ERDS Evidence as per ETSI EN 319 522-3 [i.6] and REM Evidence as per ETSI TS 102 640-2 [i.10]

#	ERDS Evidence Component as per ETSI EN 319 522-3 [i.6] REM Evidence Component as per ETSI TS 102 640-2 [i.10]	In REM Evidence as per ETSI TS 102 640-2 [i.10]	In ERDS Evidence as per ETSI EN 319 522-3 [i.6]
1	Target namespace	Its value is: http://uri.etsi.org/02640/v1#	Its value is: http://uri.etsi.org/19522/v1#
2	Attribute `version` of root element	Its value is `"1.2.1"`	Its value is "`EN319522v1.1.1`".

3	`Evidence/ERDSEventId`
	XML elements of type rem:REMEvidenceType for each type of REM Evidence, namely:
	`SubmissionAcceptanceRejection`
	`RelayREMMDAcceptanceRejection`
	`RelayREMMDFailure`
	`DeliveryNonDeliveryToRecipient`
	`DownloadNonDownloadByRecipient`
	`RetrievalNonRetrievalByRecipient`
	`AcceptanceRejectionByRecipient`
	`RelayToNonREMSystem`
	`ReceivedFromNonREMSystem`
		There is one XML element of type REMEvidenceType was associated to one or two different REM Evidence objects. For instance, the XML element `rem:SubmissionAcceptanceRejection` could be an evidence for the event of submission accepted, or for the event of submission rejection.	There is only ONE ERDS Evidence XML element: `Evidence` of type `EvidenceType`.
			
			Its component `ERDSEventId` identifies the event the evidence is associated to. Table 2 in clause 5.2.2.5 of [i.6] list the values of this child element and the event each value is associated to.

4	`Evidence/ERDSEventId` `REMEvidenceType instance/EventCode`	In ETSI TS 102 640-2 [i.10] those XML REM Evidences that could be associated to more than one event, needed this element for identifying the event the evidence was associated to.	In ETSI EN 319 522-3 [i.6] the aforementioned `Evidence/ERDSEventId` element contains an identifier of the event that the evidence is associated to.
5	`Evidence/EventReasons` `REMEvidenceType instance/EventResasons`	Annex D of ETSI TS 102 640-2 [i.10] defines a set of codes associated to certain reasons for the occurrence of events.	Clause 5.2.2.7 of ETSI EN 319 522-3 [i.6] changes the codes defined in annex D of ETSI TS 102 640-2 [i.10] for certain reasons, and define new reasons for the occurrence of the event associated to the evidence.
6	`Evidence/ EvidenceIssuerDetails` `REMEvidenceType instance/ EvidenceIssuerDetails`	In ETSI TS 102 640-2 [i.10] this element was an instance of `rem:EntityDetailsType`. Instances of this type have the following content: - `rem:NamesPostalAddresses`: an OPTIONAL sequence of components including one legal name and one postal address. - An OPTIONAL sequence of elements each one being EITHER `tsl:ElectronicAddress`, an electronic address as the ones used as electronic addresses for TSPs in Trusted Lists, OR `rem:AttributedElectronicAddress`, an attributed URI, where the attribute indicated the scheme where the address had been generated. - `rem:CertificateDetails`: an	In ETSI EN 319 522-3 [i.6] this element is an instance of `EntityDetailsType`. Instances of this type have the following content: - `Identity`: a MANDATORY component with one or more `Attribute` elements defined in SAML 2. - `CertificateDetails`: an OPTIONAL container of details of the certificate issued to the entity. This type is identical to the type present in `REMEvidenceType instance/EvidenceIssuerDetails/CertificateDetails` except that it uses instances of `CertIDTypeV2` instead of instances of `xades:CertIDType` (see ETSI EN 319 132-1 [i.12] and ETSI 101 903 [i.13] v1.4.2 for differences between them) - OPTIONALY some other content. The `CertID` element of `CertificateDetails` is an instance of `CertIDTypeV2`.

#	ERDS Evidence Component as per ETSI EN 319 522-3 [i.6] REM Evidence Component as per ETSI TS 102 640-2 [i.10]	In REM Evidence as per ETSI TS 102 640-2 [i.10]	In ERDS Evidence as per ETSI EN 319 522-3 [i.6]
		OPTIONAL container of details of the certificate issued to the entity. - OPTIONALY some other content. The `CertID` element of `rem:CertificateDetails` is an instance of `xades:CertIDType`.	The `rem:AttributedElectronicAddress` was discarded as the URIs may include schema information in their values. The `Attribute` element specified in SAML 2 has emerged as a more general component than the `rem:NamesPostalAddresses` element.

7	`Evidence/SenderDetails`
	
	`REMEvidenceType instance/SenderDetails`
		In ETSI TS 102 640-2 [i.10] this element was an instance of `rem:EntityDetailsType`.	In ETSI EN 319 522-3 [i.6] this element is an instance of `UserDetailsType`. Instances of this type have the following content:
			- `Identity`: a MANDATORY component with one or more `Attribute` elements defined in SAML 2.
			- `Identifier`: a MANDATORY complex component of type `EntityIdentifierType`, whose value is a string, and that has a mandatory attribute identifying the scheme where the user identifier has been issued.
			- `AssuranceLevelsDetails`: a MANDATORY complex component that contains the details of the assurance levels achieved during the process of the validation of the identification of the user (sender in this case), and during the authentication process carried out with the user (sender in this case).
			
			Note that for users ETSI EN 319 522-3 [i.6]:
			- Uses the more general Attribute element specified in SAML 2 instead the `rem:NamesPostalAddresses`.
			- DROPS `rem:CertificateDetails` containing details of certificates issued to users.
			- DROPS the choice between electronic address as the ones used in Trusted Lists, and the attribute URI.
			- Uses an identifier (String) issued under a certain scheme (whose identifier appears as an XML attribute of the component) to the user.
			- Adds information of the level of assurance achieved for the validation of user identification process, and the level of assurance achieved during the authentication of the user (See a deeper analysis in row showing details of `rem:SenderAuthenticationDetails` below in the present table).

8	`Evidence/RecipientDetails` `REMEvidenceType instance/RecipientsDetails`	In ETSI TS 102 640-2 [i.10] this element was a sequence of instances of `rem:EntityDetailsType`.	In ETSI EN 319 522-3 [i.6] the `Evidence` root element contains one or more `RecipientDetails` children, each one being one instance of `UserDetailsType`.

#	ERDS Evidence Component as per ETSI EN 319 522-3 [i.6] REM Evidence Component as per ETSI TS 102 640-2 [i.10]	In REM Evidence as per ETSI TS 102 640-2 [i.10]	In ERDS Evidence as per ETSI EN 319 522-3 [i.6]
			The differences between one of these instances and the instances of `rem:EntityDetailsType` will be as in the previous row of the table.
9	`Evidence/RecipientsDelegateDetails` `REMEvidenceType instance/RecipientsDelegatesDetails`	In ETSI TS 102 640-2 [i.10] `rem:RecipientsDelegatesDetails` was a sequence of instances of `rem:RecipientsDelegateType`. Each instance of this type has the following content: - `remDelegateDetails`: a MANDATORY component instance of `rem:EntityDetailsType` reviewed before. - `rem:DelegatingRecipients`: an optional list of integers, each one identifying one of the recipients of the message the delegate acts on behalf of.	In ETSI EN 319 522-3 [i.6] the `Evidence` root element contains one or more `RecipientsDelegateDetails` children, each one being one instance of `RecipientsDelegatesDetailsType`. This type EXTENDS the UserDetailsType incorporating in its contents the mandatory `DelegatingRecipients` component, a list of integers, each one identifying one of the recipients of the message the delegate acts on behalf of. Consequently, ERDS evidence replaces the content of `rem:EntityDetailsType` with the content of the new `UserDetailsType` content (which includes information on assurance levels for validation of identification and for authentication) to the `RecipientsDelegateDetails` component.
10	`Evidence/SenderDelegateDetails` NA	REM Evidence specified by ETSI TS 102 640-2 [i.10] did not incorporate a component for including details of users that could act as delegates of the actual sender of the message.	ETSI EN 319 522-3 [i.6] includes within the ERDS Evidence the OPTIONAL component `SenderDelegateDetails`, which is an instance of `DelegateDetailsType`, whose contents are the same as the contents of instances of `UserDetailsType`. This component does not need any list of integers as for each message there is only one sender.
11	`Evidence/MessageIdentifier` `REMEvidenceType instance/SenderMessageDetails /MessageIdentiferByREMMD`	In ETSI TS 102 640-2 [i.10] the identifier assigned by the REMS to the message submitted by the sender is present as value of the `MessageIdentiferByREMMD` child of the `SenderMessageDetails` element.	In ETSI EN 319 522-3 [i.6] `MessageIdentifier`, which is a string generated by the S-ERDS, is an OPTIONAL child element of the `Evidence` root element.

12	`Evidence/UserContentInfo`
	`REMEvidenceType instance/SenderMessageDetails /DigestValue`
	`REMEvidenceType instance/SenderMessageDetails /DigestMethod`
		In ETSI TS 102 640-2 [i.10], the `rem:SenderMessageDetails` OPTIONAL element has these two OPTIONAL children for carrying the digest value of the sender's message and the identifier of the digest algorithm used for computing it.
		
		A more detailed analysis of `REMEvidenceType instance/SenderMessageDetails` is shown in row #19.
			In ETSI EN 319 522-3 [i.6] `UserContentInfo` is an OPTIONAL child element of the `Evidence` root element. Its contents are the following ones:
			- `AppLayerIdentifier`: OPTIONAL component identifying the application layer that has generated the content (if this content was generated by such application layer).
			- `ComposingParts`: an OPTIONAL integer indicating the number of parts of the user content.
			- `PartsInfo`: a MANDATORY component, whose contents are:
			o `Identifer`: a MANDATORY component whose

#	ERDS Evidence Component as per ETSI EN 319 522-3 [i.6] REM Evidence Component as per ETSI TS 102 640-2 [i.10]	In REM Evidence as per ETSI TS 102 640-2 [i.10]	In ERDS Evidence as per ETSI EN 319 522-3 [i.6]
			value is the identifier of the part, o `ContentType`: a MANDATORY component, whose value identifies the type of the content, o `ds:DigestMethod`: an OPTIONAL component containing the digest value of the part, o `ds:DigestMethod`: an OPTIONAL component whose value is the identifier of the algorithm used for computing the digest value of the part.
13	`Evidence/ExternalERDSDetails` NA	No component with information of another REMS appeared in the specification `rem:REMEvidenceType` as per ETSI TS 102 640-2 [i.10].	In ETSI EN 319 522-3 [i.6] `ExternalERDSDetails` is an OPTIONAL child element of the `Evidence` root element. It is an instance of `EntityDetailsType`. Its contents will be the same as the contents of `EvidenceIssuerDetails`.
14	`Evidence/ExternalSystem` `REMEvidenceType instance/ForwardedToExternalSystem`	In ETSI TS 102 640-2 [i.10], the usage of `rem:ForwardedToExternalSystem` OPTIONAL element can be used in situations where the REMS forwards the message to one non REMS system. Its value provided means for identifying this non REMS system. Its name, and the specification in clause 5.2.2.4.5 of ETSI TS 102 640-2 [i.10], seems to indicate that it is not used in situations where a message has been received FROM a non REMS system.	In ETSI EN 319 522-3 [i.6] the usage of `ExternalSystem` OPTIONAL element is explicitly allowed for situations where: - A message has been successfully forwarded to a non ERDS/REMS system. - The forwarding of a message to a non ERDS/REMS system has failed. - A message has been successfully received from a non ERDS/REMS system. As in the `rem:ForwardedToExternalSystem` its value provided means for identifying this non REMS system.
15	`Evidence/ds:Signature` `REMEvidenceType instance/ds:Signature`	The ds:Signature element in in ETSI TS 102 640-2 [i.10] is a XAdES signature compliant with ETSI TS 103 171 [i.14].	The ds:Signature element in in ETSI EN 319 522-3 [i.6] is a XAdES signature compliant with ETSI EN 319 132-1 [i.12].
16	`SenderDetails/AssuranceLevelsDetails/ AuthenticationAssuranceLevel` `REMEvidenceType instance/SenderAuthenticationDetails`	In ETSI TS 102 640-2 [i.10], this element contains information on the authentication conducted by the sender for submitting the message. It is an instance of `rem:AuthenticationDetailsType` type, whose contents are: • A CHOICE between. – A sequence of `rem:AuthenticationTime` (the time when the authentication process took place), and the `rem:AuthenticationMethod` (an identifier of the authentication method used) AND – A SAML 2 `Assertion` element. • `rem:AdditionalDetails`. OPTIONAL component.	As mentioned before, in ETSI EN 319 522-3 [i.6] the information on the authentication processes carried on the sender, recipients, and delegates appear in of - `SenderDetails/AssuranceLevelsDetails/ AuthenticationAssuranceLevel`. - `SenderDelegateDetails/AssuranceLevelsDetails/ AuthenticationAssuranceLevel`. - `RecipientDetails/AssuranceLevelsDetails/ AuthenticationAssuranceLevel`. - `RecipientsDelegateDetails/AssuranceLevelsDetails/ AuthenticationAssuranceLevel`. Moreover, the contents of these components are: - `AssuranceLevel`, a MANDATORY component providing details of the assurance level achieved for the authentication process, namely: o A MANDATORY component whose value is an

#	ERDS Evidence Component as per ETSI EN 319 522-3 [i.6] REM Evidence Component as per ETSI TS 102 640-2 [i.10]	In REM Evidence as per ETSI TS 102 640-2 [i.10]	In ERDS Evidence as per ETSI EN 319 522-3 [i.6]
			URI identifying the assurance level o An OPTIONAL component identifying the policy where this assurance level was defined o An OPTIONAL component providing details of the aforementioned policy. o An OPTIONAL component providing a list of URIS where the details of the policy can be found. - `AuthenticationDetails`, a MANDATORY component whose contents are a CHOICE between: o A sequence of `AuthenticationTime` (the time when the authentication process took place), and the `AuthenticationMethod` (an identifier of the authentication method used), o A SAML 2 `Assertion` element. o An OAuth 2.0 token as specified in [i.15]. ETSI EN 319 522-3 [i.6]: - requires mandatory elements providing explicit information related with the achieved assurance level of the authentication process, while this information was not required in ETSI TS 102 640-2 [i.10]. - Includes management of OAuth 2.0 tokens, not present in ETSI TS 102 640-2 [i.10]. - Allows to include this type of information also for the delegates of the recipients and the delegate of the sender. ETSI TS 102 640-2 [i.10] did not provide it for the delegates of the recipients (the role of delegate of the sender was not present in ETSI TS 102 640-2 [i.10]).
17	`RecipientDetails/AssuranceLevelsDetails/ AuthenticationAssuranceLevel` `REMEvidenceType instance/RecipientAuthenticationDetails`	Same considerations as in previous row apply.	Same considerations as in previous row apply.
18	NA `REMEvidenceType instance/ReplyToAddress`	In ETSI TS 102 640-2 [i.10], this optional component contains the electronic address indicated in the Reply-To MIME header present in the original message.	ETSI EN 319 522-3 [i.6] has dropped this component from the ERDS evidence, and has left it only as a component of the meta-data components set of the message.
19	`Evidence/UserContentInfo` `REMEvidenceType instance/SenderMessageDetails`	In ETSI TS 102 640-2 [i.10], this optional component is an instance of type `rem:MessageDetailsType`, whose contents are: - `rem:MessageSubject`: an OPTIONAL component whose value was the Subject of the original message. - `rem:UAMessageIdentifier`: an	`Evidence/UserContentInfo` specified in ETSI EN 319 522-3 [i.6] and analysed in row #12, keeps part of the information in `REMEvidenceType instance/SenderMessageDetails` and adds other contents.

#	ERDS Evidence Component as per ETSI EN 319 522-3 [i.6] REM Evidence Component as per ETSI TS 102 640-2 [i.10]	In REM Evidence as per ETSI TS 102 640-2 [i.10]	In ERDS Evidence as per ETSI EN 319 522-3 [i.6]
		OPTIONAL component whose value was the identifier generated by the UA for the original message. - `rem: MessageIdentifierByREMMD`: an OPTIONAL component whose value was the identifier generated by the REMS for the original message. - `ds:DigestValue` and `ds:DigestMethod` an OPTIONAL pair of components containing the digest of the original method and the identifier of the digest algorithm used for computing it.	

5.1.6 Changes on trusting

Table 17 compares the provisions of ETSI TS 102 640-1 [i.9] with ETSI EN 319 532-2 [i.2] as regards trust establishment between REM services.

The approach is similar in the two documents, the basis of which is the definition of a domain (REM Policy Domain in the TS, trust domain in the EN) in which REM services can participate under implicit or explicit domain regulation. The REM Policy Domain also implies common policy rules for the members of the domain, while the trust domain does not make such an assumption, therefore the EN is more flexible in this respect.

Both the TS and the EN mention the Trust-service Status Lists (TSL) aka. Trusted Lists (TL) as a method for publishing and checking membership of a REMS within a trust domain. A notable difference is that the EN refers to Trusted List (TL) as defined in the latest version of ETSI TS 119 612 [i.19], which is an evolution of the older Trust-service Status List (TSL) as defined in the historical ETSI TS 102 231 [i.17]. Both documents recommend the use of TSL/TL, although the language of the EN is a bit more explicit about this. This is due to the fact that since the publication of the TS the eIDAS Regulation [i.26] (and related implementing acts) have adopted the Trusted Lists as the mandatory method for publishing information about qualified trust services within the EU. While the ETSI EN 319 532-2 [i.2] allows various methods for REM trust establishment (and the referenced ETSI EN 319 522-2 [i.5] lists several examples), it includes a note that the EU Trusted Lists can be used for this purpose.

ETSI TS 102 640-1 [i.9] specifies three possible scenarios for trust establishment based on REM Policy Domains (REM-PD) using TSL as the method for publishing trust information: Closed REM-PD, Interoperable REM-PDs without Root TSL, Interoperable REM-PDs with Root TSL. It makes use of the "Pointers to other TSLs" feature to link the different TSLs to each other. On the other hand, ETSI EN 319 532-2 [i.2] does not specify the interconnection of different trust domains in such detail, and does not contain any provisions on pointers between different TSLs. It merely references the general recommendations of ETSI EN 319 522-2 [i.5], which leaves the governance of trust domains more open, to be determined by the specific implementations.

Table 18 compares the provisions of ETSI TS 102 640-2 [i.10] with ETSI EN 319 532-3 [i.3] as regards the provision of REMS trust information when using Trusted List.

The approach of the two documents is identical, with only a few changes in the requirements.

The notable difference here is again the version of the referenced TSL/TL specification: the TS refers to the historical ETSI TS 102 231 [i.17], while the EN refers to the latest ETSI TS 119 612 [i.19]. As a consequence the required Service type identifier URI is different (the newer version acknowledges that REMS is a specific type of ERDS, and defines separate URIs for the qualified and non-qualified service). Another minor difference is that the ETSI EN 319 532-3 [i.3] allows the Service digital identity field to contain a CA certificate used for issuing the REMS digital signature certificates (as an alternative to containing the REMS digital signature certificate itself).

Table 17: Trust building between REM services in ETSI EN 319 532-2 [i.2] and ETSI TS 102 640-1 [i.9], Similarities and differences

#	Clause of ETSI EN 319 532-2 [i.2] Clause of ETSI TS 102 640-1 [i.9]	Provisions as per ETSI TS 102 640-1 [i.9]	Provisions as per ETSI EN 319 532-2 [i.2]
1	9.3 REM trust establishment and governance 4.4 REM Administrative Viewpoint	*"As defined in clause 3.1, a REM policy domain is any domain where a common set of rules (e.g. legal, company policy or agreement) is enforced for the provision of REM services. […] REM-MDs that exchange REM-MD Envelopes (be they actually REM Dispatches or REM-MD Messages) trust each other by definition if they belong to the same REM-PD, especially if such REM-PD is governed by an Authority that ensures that all REM-MDs abide by common rules.* *[…]* *It is therefore recommended that:* *1) a REM-PD-internal mechanism to provide authorized entities with information on the REM-MDs governed by the Authority of the involved REM-PD, likely the same REM-PD these entities belong to; this mechanism may be freely chosen by each REM-PD if it is used only within the REM-PD at issue; access to the information may even be restrict to a limited number of entities, requiring their authentication;* *2) a cross-REM-PD mechanism to allow the information in the item above to be accessed from one REM-PD to another; this mechanism, differently from the previous one, shall allow all the REM-MDs, that are supposed to reliably exchange REM-MD Envelopes, to ascertain the status of their counterparts in the relative pertaining REM-PDs.* *While the present document gives no indication on the mechanism as in previous item 1, although it proposes the TSL as in TS 102 231, it recommends adoption of the said TS 102 231 at least as a mechanism as in item 2."*	*"The requirements and explanations given in clause 9.3 of ETSI EN 319 522-2 shall apply to REM, with the following amendments.* *[BEGIN referenced text of ETSI EN 319 522-2]* *[…] Trust is defined as the existence of a trust domain within which co-operation between participating ERDSs is regulated. The specific conditions (policies) for a trust domain may vary; the present document has no requirements on how a trust domain is established or governed. […]* *Information about ERDSs participating in specific trust domains may be found by the following means:* *1) Locally configured by exchange of information, including certificates, between the involved ERDSs.* *2) Maintaining a trust domain Trust Status List (TSL), typically a responsibility of an actor co-ordinating the trust domain, termed the "scheme operator" by ETSI TS 119 612. An X.509 certificate represents the "service digital identity" of the ERDS in the TSL.* *3) As a special case of TSL, the European Trust List system will list ERDSs which are qualified in the sense of eIDAS Regulation; and the trust domain may be defined as "all qualified ERDSs".* *4) The trust domain may be defined by a domain PKI issuing X.509 certificates to all participating ERDSs.* *5) Metadata on capabilities of an ERDS may be extended to contain trust domain information; this is out of scope of the present document.* *[END of referenced text of ETSI EN 319 522-2 [i.5]* *The REMS should use Trusted List (TL) to establish trust with other REMSs.* *NOTE: This TL can be e.g. the European Trusted List system established pursuant to the Regulation (EU) No 910/2014, or it can be a different TL set up specifically for a trust domain of REM services.* *The REMS should ensure publication of information about itself in a TL to facilitate trust establishment by other REMSs."*

#	Clause of ETSI EN 319 532-2 [i.2] Clause of ETSI TS 102 640-1 [i.9]	Provisions as per ETSI TS 102 640-1 [i.9]	Provisions as per ETSI EN 319 532-2 [i.2]
2	9.3 REM trust establishment and governance 7 REM Trust Building	*"[…] it is indispensible, in order to achieve the desired reliability, that all the interested entities (i.e. Relying Parties) have access to the information on the abidance of the involved REM-MDs by the respective REM-PD rules. This access is required to be possible independently from what REM-PD the enquiring Relying Parties belong to.* *[…]* *The recommended common mechanism is the Trust-service Status List (TSL) specified in the ETSI TS 102 231."*	*"The requirements and explanations given in clause 9.3 of ETSI EN 319 522-2 shall apply to REM, with the following amendments."* [BEGIN referenced text of ETSI EN 319 522-2 [i.5] *"[…] A trust domain shall have governance, at least for the policy regarding conditions for an ERDS to join. […] Participation in a trust domain should be assessed by an X.509 certificate representing an ERDS in the trust domain. By use of this certificate, or certificates derived from it, ERDSs can be authenticated towards one another, and ERD messages and evidences can be signed and encrypted between ERDSs.* *Information about ERDSs participating in specific trust domains may be found by the following means:"* [see above] [END of referenced text of ETSI EN 319 522-2 [i.5]
3	9.3 REM trust establishment and governance 7.1 Closed REM-PD	"*In one closed REM-PD, i.e. that envisages no interaction with other REM-PDs, any mechanism may be implemented to provide REM-PD wide accessibility to the REM-MD status information.* *Where the TSL is used to this purpose it would list the related REM-MD, specifying, as indicated in ETSI TS 102 231 [*i.17*], both their current status and, optionally, their status history. Any entity belonging to the same REM-PD would access the TSL and verify its authenticity as provided for by the REM-PD rules. In this TSL, the signing public key of each REM-MD, or preferably its corresponding certificates, would be published so that any relying party would be able to use it to verify their signature on each REM-MD Envelope they issue. […] The following provisions apply.* *a) […]* *b) […]* *c) […]* *d) […]* *e) […]* "	*"The requirements and explanations given in clause 9.3 of ETSI EN 319 522-2 [*i.5*] shall apply to REM, with the following amendments."* [BEGIN referenced text of ETSI EN 319 522-2 [i.5] *"A trust domain may be established bilaterally between two or more ERDSs; in this case the governance should be through explicit or implicit agreements.* *A trust domain may require specific policy, security, and technical conditions to be met by all participating ERDSs."* [END of referenced text of ETSI EN 319 522-2 [i.5]
4	9.3 REM trust establishment and governance	*"If a REM-PD authority makes use of TSL to point to other TSLs issued by different*	[No corresponding provisions.]

#	**Clause of ETSI EN 319 532-2 [i.2]** **Clause of ETSI TS 102 640-1 [i.9]**	**Provisions as per ETSI TS 102 640-1 [i.9]**	**Provisions as per ETSI EN 319 532-2 [i.2]**
	7.2 Interoperable REM-PDs TSL - No Root TSL	*Authorities, each TSL issuer shall implement what is specified in clause 7.1 where, to ensure interoperability, in provisions a), b), d), the "should" keyword is to be changed in "shall". Additionally what is hereinafter specified also applies. […]"*	
5	9.3 REM trust establishment and governance	*"What is specified in clause 7.1 applies. To ensure interoperability in provisions a), b), d), the "should" keyword is to be changed to "shall". Additionally what is hereinafter specified also applies. […]"*	[No corresponding provisions.]
	7.3 Interoperable REM-PDs TSL - Root TSL		

Table 18: REMS information in Trusted Lists in ETSI EN 319 532-3 [i.3] and ETSI TS 102 640-2 [i.10], Similarities and differences

#	TL field in ETSI EN 319 532-3 [i.3] TL field in ETSI TS 102 640-2 [i.10]	Provisions as per ETSI TS 102 640-2 [i.10]	Provisions as per ETSI EN 319 532-3 [i.3]
1	Service type identifier (as per clause 5.5.1 of ETSI TS 119 612 [i.19]) Service type identifier	*"Set to http://uri.etsi.org/TrstSvc/Svctype/REM."*	*"This element shall be one of the following:* • *http://uri.etsi.org/TrstSvc/Svctype/EDS/REM.* • *http://uri.etsi.org/TrstSvc/Svctype/EDS/REM/Q."*
2	Service digital identity (as per clause 5.5.3 of ETSI TS 119 612 [i.19]) Service digital identity	*"the TSP X.509 certificate associated to the key used to sign the REM-MD Evidences and optionally the corresponding X509SKI element."*	*"This element shall contain an X.509 certificate, which shall be one of the following:* • *A single certificate used by the REMS for digital signing of all REM messages and ERDS evidence.* • *A single CA certificate that is used solely for the purpose of issuing certificates to components of the REMS for digital signing of REM messages and/or ERDS evidence.* *This element may contain optionally the corresponding X509SKI element."*
3	Service supply point (as per clause 5.5.7 of ETSI TS 119 612 [i.19]) Service Supply Point	*"This element provides information for access to the MD-RI (REM-MD Message and Evidence Relay Interface) defined in ETSI TS 102 640-1 [*i.9*].* *Depending on the implemented protocol, the element shall provide a pointer to a web service or to a smtp server.* *Via appropriate conventions, a file containing service metadata information may be reachable based on this pointer."*	*"This element should provide one or more URIs to access the REM RI (Relay Interface) defined in clause 5 of ETSI EN 319 532-1 [*i.1*].* *Depending on the implemented transport protocol, this element may provide a pointer e.g. to an SMTP server, to a web service, etc. If the Relay Interface is provided using SMTP then this URI should be an smtp: URI."*
4	TSP service definition URI (as per clause 5.5.8 of ETSI TS 119 612 [i.19]) TSP service definition URI	*"If present, this URI shall point to published general information relevant to the users like public certificates, addresses, etc."*	*"If present, this URI may point to published general information relevant to the users like public certificates, addresses, etc."*
5	Service information extensions (as per clause 5.5.9 of ETSI TS 119 612 [i.19]) Service information extensions	*"If present, extensions shall not be set as critical (see note).* *NOTE: Use of extension is discouraged as they can create barriers to interoperability."*	*"If present, extensions shall not be set as critical."*

5.2 PReM - UPU S.52 2008 vs UPU S.52 CEN/TS 16326 (2013)

5.2.1 Introduction

The next clauses from 5.2.2 to 5.2.6 contain some gap between PReM S52-1 [i.24] (used for the definition of interoperability profile ETSI TS 102 640-6-1 [i.11]) and UPU S52-2 / CEN/TS 16326 [i.25]. In this analysis are considered only the parts that could result critical for the implementation of the interoperability profile between REM/PReM.

5.2.2 Changes on flows

In UPU S52-2 / CEN/TS 16326 [i.25] the flows have changed a little bit compared to PReM S52-1 [i.24] used at the time for the interoperability profile defined in ETSI TS 102 640-6-1 [i.11].

The operation is now a bit more symmetrical. This also reflected on the verbs (as abstract operations) that describe the interchange flows.

The following differences outlined in Table 19 deserve particular mention.

Table 19: Differences between flows in PReM S52-1 [i.24] and UPU S52-2 / CEN/TS 16326 [i.25]

#	Flow elements from UPU S52-2 / CEN/TS 16326 [i.25] and PReM S52-1 [i.24]	Flow properties as per PReM S52-1 [i.24]	Flow properties as per S52-2 / CEN/TS 16326 [i.25]
1	SePS operational verbs number Operational Verbs mapping	# Six: CheckIntegrity LogEvent Postmark RetrieveResults Sign Verify	# Three: CheckIntegrity none Postmark none none Verify
2	Additional server-side operational verbs number Operational Verbs mapping	# Five: SendMessageToDestination SubscribeNotification UnsubscribeNotification none RejectMessage ReceiveNotification	# Four: SendMessageToDestination none none RetrieveMessage RejectMessage ReceiveNotification
3	Interaction	Web based Standard email client	Web-based client interface Extension to existing email client SW

Figure 1 and Figure 2 of both documents S52-1 [i.24] and UPU S52-2 / CEN/TS 16326 [i.25] describe how the flows are changed in the last S52-2 specification, also to fully accomplish the behaviours behind the new operational verbs.

Other than the specific flows described in clause "5.1 conceptual model" and "5.2 Operation Scenarios" of UPU PReM S52-1 [i.24] there are new flows defined in the new UPU S52-2 / CEN/TS 16326 [i.25]. These are outlined in "Figure 3 - State diagram of PReM message exchange between DOO and DOD" of [i.25] and in the relevant explanations of the further sequence actions diagram, describing how the main flows of send message/receive notifications are interleaved with the interactions with the yellow page role from DOO and/or DOD.

Furthermore the following "Figure 4 - Operation work flow" in [i.25], clause 5.2 has been completely reviewed according with the new verbs and operation flows.

The operations that are relevant for interoperability between REM/PReM are summarized, for the first interoperability profile, in Figure 3 of ETSI TS 102 640-6-1 [i.11]. The new UPU S52-2 / CEN/TS 16326 [i.25] has changed the workflow. The impact on the interoperability profile is summarized in the mapping of the following Table 20.

Table 20: Differences between workflows diagram in PReM S52-1 [i.24] and UPU S52-2 / CEN/TS 16326 [i.25]

#	**WorkFlow functions from clause 5.2.1 and Figure 4 of UPU S52-2 / CEN/TS 16326 [i.25]** **WorkFlow functions from clause 5.2.1 and Figure 3 of UPU PReM S52-1 [i.24]**	**Flow properties as per clause 5.2.1 and Figure 3 of PReM S52-1 [i.24] and Figure 3 of ETSI TS 102 640-6-1 [i.11]**	**Flow properties as per clause 5.2.1 and Figure 4 of S52-2 / CEN/TS 16326 [i.25]**
1	4.4 3.7	4.4 Invoke DO of Destination **SendMessageToDestination** to forward PReM Dispatch	3.7 Invoke **SendMessageToDestination** of DOD
2	5.1 5.1	5.1 Receive/NotReceive PReM Dispatch using **SendMessageToDestination**	5.1 Invoke **SendMessageToDestination** receive PReM Dispatch
3	5.8/10.4 5.2/5.3 negative case	5.8 Notify with Evidence of Acceptance/Rejection 10.4 Notify with Evidence of Delivery or Expiration or Reject	5.2 Check Parameters (negative case) 5.3 VerifyRequesterSignature (negative case) InvokeReceiveNotification (positive case)
4	6.1/11.1 3.8 positive case 3.10 negative case 7.1, 7.2, 7.3, 7.4, 7.5, 10.1, 15.1, 15.2	6.1 Receive Evidence of Acceptance/Rejection 11.1 Receive Evidence of Delivery	3.8 Store EFW-DSP-DOO 3.10 Store EFF-UNR-DOO 7.1, 7.2, 7.3, 7.4, 7.5, 10.1, 15.1, 15.2 Save forwarded evidence and send notification

Table 21: Differences between workflows definition in PReM S52-1 [i.24] and UPU S52-2 / CEN/TS 16326 [i.25]

#	WorkFlow functions from table in clause 5.2.2 of UPU S52-2 / CEN/TS 16326 [i.25] WorkFlow functions from table in clause 5.2.2 of UPU PReM S52-1 [i.24]	Flow properties as per table in clause 5.2.2 of PReM S52-1 [i.24] and Table 4 of ETSI TS 102 640-6-1 [i.11]	Flow properties as per table in clause 5.2.2 of S52-2 / CEN/TS 16326 [i.25]
1	1.4 None	None	Convert message into PReMObject(s) (in MIME format)
2	1.5 None	None	Sign RequesterSignature of SendMessageToDestination
3	1.6 None	None	Invoke SendMessageToDestination at DOO to upload Object to DOO
4	2.1 None	None	Use SendMessageToDestination to accept Mailer's PReM Object
5	2.2 b) None	None	*"Mailer address format must be in IETF RFC 2822 format"*
6	2.9 None	None	If PReM message was accepted, DOO generates Evidence of Sent-PReM MessageAcceptance-DOO
7	2.10.1 2.10.2 2.10.3 None	None	(1) DOO generates Evidence of Sent-PReM MessageRejection-DOO (2) DOO generates Evidence of Successful Notification (3) DOO generates Evidence of Failed Notification
8	3.1 None	None	Prepare PReM Message which includes the following contents (refer to section 8.2.2): i) Introduction Section ii) PReM Object iii) Postmark of PReM Object to proof the acceptance date and time iv) Electronic signature for the above three items
9	3.3 None	None	3.3 Prepare PReM Dispatch which includes the following contents (refer to section 8.2.3): i) Introduction Section ii) PReM Message iii) Evidence Group iv) Postmark the above items (message forwarding date and time) v) Electronic Signature of all the above items
10	3.5 None	None	Generate Evidence of Sign-PReM Dispatch-DOO (ESG-DSP-DOO)
11	6.1 None	None	Decompose PReM Dispatch
12	6.3 None	None	Extract PReM Message from PReM Dispatch; extract PReM Object and Postmark from PReM Message

Furthermore the aforementioned differences, implementing a new interoperability profile the statement and considerations of clause "5.2.4 Interoperation between PReM System and non-PReM System" of UPU S52-2 / CEN/TS 16326 [i.25] need to be considered.

5.2.3 Changes on messages

In UPU S52-2 / CEN/TS 16326 [i.25] the formats have been specified more in detail compared to PReM S52-1 [i.24] used at the time for the interoperability profile defined in ETSI TS 102 640-6-1 [i.11]. These changes need to be assessed during the drafting of a new interoperability profile. Table 22 summarize the differences detected in the present study.

See point #1 and #5 of Table 21.

Table 22: Changes on messages

#	Type of change or new specification	References	Notes
1	Format	See point #1 and #5 of Table 21 of the present document	These specifications promote the interoperability.
2	Format	See point #8 and #9 of Table 21 of the present document	These steps of the flow reveal a particular deep structure of the objects manipulated by PReM. The structure is different from that managed in REM. This specification does not facilitate the interoperability.
3	Format	Clause 8.1 and point 2.6 of Table in clause 5.2.2 of UPU S52-2 / CEN/TS 16326 [i.25]	The message identifier requirement can be addressed at Gateway Level with a double id, if PReM cannot use the format used in REM.
4	Format	8.2 UPU S52-2 / CEN/TS 16326 [i.25] Point 2.4 of Table in clause 5.2.2 regarding PostMark application.	As already mentioned at point 2 above, the "Figures 5, and 7 PReM dispatch" and "Figure 6 PReM message" confirms that the enveloping deep and structure of PReM is different from that of REM. To facilitate the interoperability it is recommended to have at least one structure level of PReM that is comparable to REM dispatch structure. E.g. for this purpose, perhaps the PReM Message structure (except the PostMark object, that may be mapped to a REM dispatch extension), could be maintained fully aligned with REM dispatch object. So, at gateway level, the task is simplified and consists of properly "prepare" (from REM to PReM side, enveloping again REM dispatch into a PReM dispatch) and "decompose" (from PReM to REM side, extracting a REM dispatch structure) PReM dispatch according to the flow direction.

5.2.4 Changes on evidence structure and semantic

Table 23: Changes on evidence

#	Type of change or new specification	References	Notes
1	Semantic flow	See points #6, #7 and #10 of Table 21 of the present document	This section and all the other regarding the evidence need to be assessed in depth to find a way for allowing the interoperability.
2	Semantic flow	8.3 and Table 1 of UPU S52-2 / CEN/TS 16326 [i.25]	This section contains the list of all PReM evidence.
3	Format	8.4 and Figure 8 UPU S52-2 / CEN/TS 16326 [i.25]	This section contains the format of PReM evidence.

The questions to address in order to allow interoperability are at least:

1) Format of the evidence
2) Format of enveloping
3) Type of evidence
4) Flow of evidence

When these evidence objects regard to the flow between the boundary REM/PReM roles, the four aforementioned questions are to be managed at Gateway level.REM and PReM gateway sides have to generate the type of evidence mutually needed by the reciprocal side.

To facilitate interoperability it is fundamental to have at least the format of evidence, (question 1 above), fully aligned in both REM and PReM. Questions 2, 3 and 4 can instead be addressed at Gateway Level.

From PReM to REM evidence flow, all the needed/mandatory evidence objects can be generated at Gateway level with the correct format and the correct content.

5.2.5 Changes on signature

Table 24: Changes on signature

#	Type of change or new specification	References	Notes
1	Format	8.6, Figure 9 and Figure 10 of UPU S52-2 / CEN/TS 16326 [i.25]	This section contains the format of signatures applied to PReM message and PReM dispatch.

The questions to address in order to allow interoperability are at least:

1) Format of the signature

2) Type of signature

3) Objects where apply the signature

When these signatures regard objects like messages and/or evidence, to facilitate interoperability, it is fundamental to have at least the format and type of signature, (questions 1 and 2 above), fully aligned in both REM and PReM. Questions 3 can instead be addressed at Gateway Level if it is not already accomplished at service side.

5.2.6 Changes on trusting

Table 25: Changes on trust

#	Type of change or new specification	References	Notes
1	Semantic flow	Flow properties of point 2.7 of table in clause 5.2.2 of S52-2 / CEN/TS 16326 [i.25]	Check if DOD is in the designated operator Trust List.
2	Format		To help communication between Designed Operators and localization of DO Service Points a central Yellow Page repository is now implemented.

The questions to address in order to allow interoperability are at least:

1) Mapping between REM trusting and location and PReM Yellow Page service.

2) Type of information stored in central repository.

When these practices regard lookup processes about boundary activities between REM/PReM, to facilitate interoperability, it is fundamental to have the location mechanism and type of information, (questions 1 and 2 above), redundant and mutually compatible in both REM and PReM environments. E.g. through an agreement each side of the gateway should be able to lookup on the own environment the required information (e.g. for routing and/or locate) starting from the key information coming from the other side.

6 Recommendation for follow-up activities

6.1 Overview

The historical ETSI TS 102 640-6-1 [i.11] specified requirements for achieving interoperability between legacy REM systems (based on the ETSI TS 102 640 [i.23] series) and legacy PReM systems (based on the UPU S52-1 [i.24] version), in order to support the forwarding and delivery of messages and related evidence between REM service providers (REM-MD as defined in ETSI TS 102 640 [i.23]) and Designated Operators (DO) as defined in UPU S52-1 [i.24]. The chosen approach for this interoperability was the definition of a REM/PReM Gateway, which was to be part of both the REM and the PReM network, thereby establishing the interconnection of the two networks and providing a mapping and translation between the specificities of the two networks. The operation of such a REM/PReM Gateway was highly dependent on the fact that the UPU S52-1 [i.24] specification defined the PReM message formats and PReM evidence formats by reference to the ETSI TS 102 640-2 [i.10] REM message and evidence formats.

As detailed in clause 5 of the present document, both the ETSI REM specification and the UPU PReM specification have evolved since the creation of the original ETSI TS 102 640-6-1 [i.11] interoperability profile. In order to achieve a similar interoperability between state-of-the-art REM systems (based on the ETSI EN 319 532 [i.22] series) and state-of-the-art PReM systems (based on the UPU S52-2 [i.25] or later version) the developments in the REM and PReM standards as well as other developments of internet technologies and security techniques should be considered and integrated into the technical specifications.

Clause 6.2 provides recommendations for UPU to consider in the future versions of S52-2 [i.25], in order to provide input to speed up the update of the specification. The following clauses present the issues to consider which can facilitate the interoperability between PReM and REM systems.

Clause 6.3 provides recommendations for ETSI to consider in the creation of an interoperability profile, which specifies requirements for achieving interoperability between state-of-the-art REM systems (based on the latest ETSI EN 319 532 [i.22] version) and state-of-the-art PReM systems (based on the latest UPU S52-2 [i.25] version).

6.2 UPU-side activities

6.2.1 Update of references

The current S52-2 [i.25] references a number of documents which have become obsolete since its publication, and of which newer versions exist. The following Table 26 provides recommendations to update the references.

Table 26: Recommendation for updating references

Existing reference in S52-2 [i.25]	Up-to-date version to be referenced
ETSI TS 102 640 [i.38]: "Registered Electronic Mail (REM): Architecture, Formats, and ISM Policies".	ETSI EN 319 532 (parts 1 to 4) [i.22]: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) Services".
ETSI TS 101 862 [i.27] (V1.3.3), January 2006: "Qualified Certificate Profile".	ETSI EN 319 412 (parts 1 to 5) [i.28]: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles".
CWA 14169 [i.36: "Secure signature-creation devices "EAL 4+".	CEN EN 419211 (parts 1 to 6) [i.37]: "Protection profiles for secure signature creation device".
Directive 1999/93/EC [i.26] of the European Parliament and of the Council on a Community framework for electronic signatures.	Regulation (EU) No 910/2014 [i.26] of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.
IETF RFC 2822 [i.35]: "Internet Message Format" (April 2001) P. Resnick.	IETF RFC 5322 [i.29]: "Internet Message Format".
IETF RFC 3851 [i.30]: "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification".	IETF RFC 5751 [i.31]: "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification".
ETSI TS 101 903 [i.13] (V1.3.2), March 2006: "XML Advanced Electronic Signatures (XAdES)".	ETSI EN 319 132 (parts 1 and 2) [i.32]: "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures".

6.2.2 Update of security techniques

UPU S52-2 [i.25] prescribes the use of SSL (Secure Sockets Layer) and refers to SSL in multiple sections. SSL is obsolete and no versions of this protocol are considered secure any more. The evolution of SSL is TLS (Transport Layer Security), whose current version at the time of writing the present document is version 1.3, see IETF RFC 8446 [i.33]: The Transport Layer Security (TLS) Protocol Version 1.3.

UPU S52-2 [i.25] normatively refers to UPU S43 Secured electronic postal services (SePS), which still recommends and at some points requires MD5 and SHA1 digest algorithms. Since the S43 publication MD5 and SHA1 algorithms have been compromised, they are considered insecure and their use is strongly discouraged. At the time of writing the present document the SHA2 and SHA3 families represent recommended digest algorithms. For more information on recommended cryptographic suites, see ETSI TS 119 312 [i.18].

6.2.3 Adaptation of flows

ETSI EN 319 522-1 [i.4] defines the logical model of an Electronic Registered Delivery Service (ERDS) and the set of relevant events the ERDS should provide evidence about, which also apply to REMS since REMS is defined as a specific type of ERDS. Systems based on the UPU PReM specification can be considered as full-fledged ERDS and thus achieve interoperability with REMS (or other types of ERDS for that matter) provided that the basic workflow and the relevant events can be mapped.

For this purpose the following concepts should be possible to be mapped to PReM implementations:

- **user content:** original data produced by the sender which has to be delivered to the recipient;
- **submission:** transaction in which the user content, coming from the outside, passes through the boundary of the ERDS;
- **relay:** transaction in which the user content is passed from one ERDS to another ERDS;
- **consignment:** act of making the user content available to the recipient, within the boundaries of the electronic registered delivery service;
- **handover:** act of having the user content successfully cross the border of the recipient's electronic registered delivery service towards the recipient's ERD user agent/application;
- **notification for acceptance:** notification sent by the ERDS to the recipient about an incoming message, to which the recipient needs to respond by acceptance or rejection of delivery of the message, otherwise it will expire in a predefined time period;
- **notification of consignment:** notification sent by the ERDS to the recipient about the availability of a consigned message, to which the recipient does not need to respond.

Not all of the above mentioned features are required to be supported. For example, either consignment or handover is required for an ERDS, and if the ERDS provides one of them then the other is optional. Relay, notification for acceptance and notification of consignment are optional features.

In order to achieve interoperability with REMS (and possibly other ERDS) systems, the PReM workflow should be adapted so that the above mentioned concepts are identifiable, which would make it possible to define the necessary mapping between the workflows.

6.2.4 Adaptation of message formats

As mentioned earlier, the original interoperability profile between legacy REM and legacy PReM systems relied on the fact that the UPU S52-1 [i.24] defined the PReM message formats by reference to the ETSI TS 102 640-2 [i.10] REM message formats, and only specified an enveloping mechanism for the transport of those REM-based messages. UPU S52-2 [i.25] defines a new PReM message format, which is based on REM, but introduces a number of different requirements in the message structure, as detailed in clause 5.2.3. As a consequence, the mere enveloping and forwarding, as defined in clause 11 of ETSI TS 102 640-6-1 [i.11], will not be suitable to interconnect the PReM and REM networks.

There are two alternatives to enable the forwarding of messages:

1) The PReM message structure is adapted to align with the latest REM message structure, so that the implementations can handle PReM and REM messages alike. This update can be performed based on the information provided in clause 5.1.4.

2) The REM/PReM Gateway approach is used in the interoperability profile, and the REM/PReM Gateway is required to parse and process both REM and PReM message formats, always extract all objects (user content/PReM Object, evidences, PostMarks, etc.) and perform a re-enveloping according to the other message structure before forwarding.

Considering that the re-enveloping mechanism tremendously increases the complexity of both the specification and the implementation of the REM/PReM Gateway, alternative 1) is recommended from the options above.

6.2.5 Adaptation of evidence format

As mentioned earlier, the original interoperability profile between legacy REM and legacy PReM systems relied on the fact that the UPU S52-1 [i.24] defined the PReM evidence formats by reference to the ETSI TS 102 640-2 [i.10] REM evidence formats.

As the provision of evidence is an essential function of PReM and REM services, and the evidences need to be interpreted and accepted by all relying parties, a common standard evidence format is crucial to the adoption of these services. Since evidence is protected by the digital signature of the issuing service, transformation of the evidence data into a different format would break the integrity of the signed data, thereby making the digital signature impossible to validate, which would also prevent the authentication of evidence origin. Therefore, format transformation of signed evidence is impractical.

For these reasons it is recommended that the PReM evidence format is adapted to completely align with the ERDS evidence format defined in ETSI EN 319 522-3 [i.6]. The information provided in clause 5.1.5 aims to support this update in order to avoid more complicated mechanisms consisting in re-enveloping techniques of original formats, side by side, at gateway level.

6.2.6 Update of policy considerations

UPU S52-2 [i.25] specifies some policy considerations for the provision of the service across borders. These stipulations should be updated taking into account the following information:

- Regulation (EU) No 910/2014 (eIDAS) [i.26] has repealed Directive 1999/93/EC, so all references to the Directive should be revised and the appropriate concepts from the eIDAS Regulation [i.26] should be applied.

- ETSI EN 319 521 [i.7] and ETSI EN 319 531 [i.8] define policy and security requirements for ERDS and REMS (respectively), which can be used by service providers aiming to implement and demonstrate conformance to the eIDAS Regulation [i.26] requirements.

- eID (electronic identification means as defined by Chapter II of eIDAS [i.26]) should be added as an option for identification management and authentication model.

- Advanced Electronic Signatures and Qualified Electronic Signatures are redefined by eIDAS and can continue to be used. The eIDAS Regulation [i.26] also provides detailed requirements on the issuance of Qualified Certificates, which can also be relied upon.

- The eIDAS Regulation [i.26] defines electronic seals ("signatures" created by legal persons) and also recognizes remote (server-based) signature and validation services, which may be considered in relation to the Sign and Verify operations defined in the S43 Secured Electronic Postal Services specification.

6.3 ETSI-side activities

The approach to the interoperability profile in the historical ETSI TS 102 640-6-1 [i.11] was based on the definition of a REM/PReM Gateway, which acts as a REM-MD in the REM network and as a Designated Operator in the PReM network. The same gateway approach can be used to enable the interconnection of the delivery systems based on the latest ETSI EN 319 532 [i.22] series and the latest UPU S52-2 [i.25] specification. In order to specify the requirements for the REM/PReM Gateway a gap analysis needs to be performed between the relevant standards and mappings need to be defined for functions, events, evidence, operations and messages. This includes the following tasks:

- The PReM events and evidence types should be mapped to ERD event types, taking into account the changes in PReM evidence types in UPU S52-2 [i.25] and the few changes in event types between ETSI TS 102 640 [i.23] and ETSI EN 319 522 [i.21].
- The PReM operations (verbs) should be mapped to the REM message sequences, taking into account that SubscribeNotification, UnsubscribeNotification, LogEvent, RetrieveResults and Sign operations are not used any more, while RetrieveMessage is defined as a new operation in the current version of the PReM specification [i.25].
- The functional gap analysis should be recreated to identify the main similarities and differences between the functional aspects of REM and PReM, taking into account the changes in the PReM operation workflows and the REM logical model.
- Transformation rules should be defined between PReM message structures and REM message structures. The complexity of this task heavily depends on whether the alignment between REM and PReM message formats can be improved by future versions of the standards, as described in clause 6.2.4. If the message formats are fully aligned then no transformation is needed apart from the enveloping for transport in the SOAP structure. If the message formats are divergent then a complete field-to-field mapping and a re-enveloping mechanism need to be defined.
- The mapping of protocol elements should be recreated for operations SendMessageToDestination, ReceiveNotification.
- The mutual recognition system between REM and PReM networks should be redefined, taking into account the changes in trust establishment as described in clause 5.1.6 and clause 5.2.6.

The findings and specifications of ETSI TS 102 640-6-1 [i.11] can be used as input in the creation of the new REM-PReM interoperability profile, although its parts outlined in Table 27 need to be reviewed and updated.

Table 27: Notes for interoperability profile specification starting from ETSI TS 102 640-6-1 [i.11]

Clauses of ETSI TS 102 640-6-1 [i.11]	Notes for updating tasks
5. Mapping of terms and definition	New terms and new meanings have been defined in ETSI REM (see clause 5.1.2).
6. Mapping of boundary roles	Name of roles has been updated in ETSI REM (see clause 5.1.2)
7. Functional GAP analysis between REM and PReM	The format of the exchanged messages and evidence structure is changed in ETSI REM (see clauses 5.1.4 and 5.1.5) The events and the relevant evidence semantics have been updated in ETSI REM (see clause 5.1.5). Functional description of the service flow (Operation scenarios and workflow) has been updated in ETSI REM (see clause 5.1.3). Functional description of the service flow (Operation scenarios and workflow) is changed in UPU PReM (see clause 5.2.2). Event/evidence set, associated each to a specific function in REM/PReM, and so the defined mapping is changed in both ETSI REM and UPU PReM.
8. High level definition of the inter-communication flows between REM and PReM	New terms and new meanings have been defined in ETSI REM about network elements and class aggregations (see clause 5.1.2).
8.2. Operational scenario	The names and formats of the exchanged objects has been updated in ETSI REM.

Clauses of ETSI TS 102 640-6-1 [i.11]	Notes for updating tasks
9. Mapping of exchanged formats	The formats, nomenclature, semantic and reference standards relevant to: • attachments • signatures • evidence have been updated in both ETSI REM and UPU PReM. Changes in the message formats are described in clause 5.1.4 and clause 5.2.3. The content of the present clause needs to be updated according to the decisions to: • maintain, in UPU PReM, an explicit normative reference to the ETSI REM specifications regarding the new formats of messages, evidence set structure, but also digital signatures. • maintain the format of the messages/evidence/digital signature exchanged between REM/PReM **exactly the same** of that defined in ETSI REM specification [i.22]; or • leave some extra work at Gateway level which cares some additional enveloping activity capable of rebuild the formats and structures required by each side. This extra work could involve, as an example, re-enveloping, re-sign and any other business necessary to cover the gap.
10. Mapping of evidence names and semantics	The types of evidence and their usage has been updated in ETSI REM and in UPU PReM. Changes in evidence structure and semantics are described in clause 5.1.5 and clause 5.2.4. Anyway, the attention for the purpose of interoperability is only for the type of evidence that flows between REMS and PReM Designed Operators (and vice versa according to the flow direction of electronic communication).
11. Mapping of protocol elements	The package of information conveyed among Designated Operators has been updated. A deep analysis on the changes required at REM-PReM Gateway level is required in this clause. Similarly as has been outlined in the row "9. Mapping of exchanged formats", the content of the present clause needs to be updated according to the decisions that will be taken at UPU level. These should regard the full/partial maintenance of references to the new formats and way to operate defined in ETSI ERDS and REM. Particular attention merits the "**Data**" section. Even in this mapping the aforementioned decisions will influence if the work inside the REM-PReM Gateway will be "simple" (← same formats) or there will be some extra work (←different formats between REM-PReM). In this latter case, some extra work at Gateway level which cares all the countermeasures capable of smooth out the delta by techniques re-enveloping, re-sign, etc. Deep changes in ETSI REM and UPU PReM involves both the following clauses: • 11.1 Enveloping REM Dispatch in PReM Web Service business payload →Changes will be necessary in this clause in terms, enveloping, formats, semantics, behavior, etc. • 11.2 PReM Designated Operators - relay Web Service Interface →Changes will be necessary in this clause in terms, semantics, flows, verbs, mappings, etc.
12. Definition of mutual recognition system based on ETSI-TSL and UPU-Designated Operator Trusted List	The systems for implementing the trust among the service elements have been updated on both ETSI REM and UPU PReM. ETSI REM evolved towards TL and/or SML/SMP. Whereas UPU PReM introduced the concept of Yellow Page inside the role of Trusted List distribution point. Changes in trust establishment are described in clause 5.1.6 and clause 5.2.6. The update of the present clause should take in account all these changes in order to define an effective cross recognition/trusting system.

7 Conclusions

The historical REM-PReM interoperability profile in ETSI TS 102 640-6-1 [i.11] was defined relying on the fact that the then-current UPU S52-1 [i.24] PReM specification normatively referred to the then-current ETSI TS 102 640 [i.23] REM specification with respect to the format of messages and evidences. This effectively allowed relaying of messages and evidences between REM and PReM systems without format conversion. Since then both the REM and PReM standards have evolved, and the message and evidence formats have drifted apart. Moreover, UPU considered updating its UPU S52-2 [i.25] standard again to take into account the Regulation EU No 910/2014 (eIDAS) [i.26], which created a common legal framework for trust services including electronic registered delivery services in the European Union.

Clause 5 of the present document analyses the gaps and changes between the latest REM/PReM standards and the historical standards on which the original ETSI TS 102 640-6-1 [i.11] interoperability profile was based on. Clause 6 of the present document provides recommendation for follow-up standardisation activities on both the UPU and the ETSI side that could lead to the production of a new REM-PReM interoperability profile, which would specify the requirements to achieve interoperability between systems based on the latest REM and the latest PReM specifications.

For the new REM-PReM interoperability profile the present document recommends to apply the approach of defining a REM/PReM Gateway, similarly to the one defined by the original ETSI TS 102 640-6-1 [i.11]. This gateway would assume the role of a REM Service in the network of interconnected REM services as defined in ETSI EN 319 532-1 [i.1], and would assume the role of a Designated Operator in the network of PReM services as defined in UPU S52-2 [i.25] or any later version thereof. The gateway would implement and comply with both the REM and the PReM specifications, performing relay, mapping, translation and other processing activities as necessary to interconnect the two networks of services.

In order to specify the operation of the REM/PReM Gateway, further study and standardisation work needs to be done, as described in clause 6. Updating the UPU S52-2 [i.25] standard as recommended in clause 6 to re-establish the alignment in message and evidence formats would greatly facilitate the creation of the new REM-PReM interoperability profile between the latest REM and PReM specifications, and it would also make it easier to implement the Gateway.

More specifically, in the future version of the UPU PReM S52 ([i.24] and [i.25]) standard it is recommended to ensure the alignment with ETSI EN 319 532 [i.22] in the following aspects:

1) Format of evidence set.

2) Format of messages.

3) Format of digital signatures.

4) Deep structure of messages/enveloping.

5) Compatibility of other mechanisms (e.g. PostMark) using the extensions mechanisms defined in REM dispatch and/or REM message.

Otherwise, any interoperability between REM/PReM will require new enveloping and translation mechanisms to be implemented in the REM/PReM Gateway, to ensure format compatibility between the two services.

It is obvious that if there is no evident necessity to maintain distinct formats, the interoperability between REM/PReM would not only be possible but also simple to realize.

History

Document history		
V1.1.1	February 2019	Publication