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

Important notice

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

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

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

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

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].