Draft ETSI EN 319 532-4 V1.3.0 (2023-10)

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

Reference

REN/ESI-0019532-4v131

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 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Important notice

The present document can be downloaded from:
https://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

If you find a security vulnerability in the present document, please report it through our Coordinated Vulnerability Disclosure Program:
https://www.etsi.org/standards/coordinated-vulnerability-disclosure

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.
No recommendation as to products and services or vendors is made or should be implied.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Contents

Intellectual Property Rights 6
Foreword 6
Modal verbs terminology 6
Introduction 7
1 Scope 8
2 References 8
2.1 Normative references 8
2.2 Informative references 9
3 Definition of terms, symbols, abbreviations and terminology 10
3.1 Terms 10
3.2 Symbols 10
3.3 Abbreviations 10
3.4 Terminology 11
4 General requirements 11
4.1 Introduction 11
4.2 Compliance requirements 11
5 SMTP interoperability profile 12
5.1 General requirements 12
5.2 Style of operation 12
5.3 REMS - interfaces constraints 12
5.3.1 Introduction 12
5.3.2 REM MSI: Message Submission Interface 13
5.3.3 REM MRI-ERI: Message and Evidence Retrieval Interface 13
5.3.4 REM RI: Relay Interface 13
5.3.5 CSI: Common Service Interface 14
5.4 REM message constraints 14
5.4.1 REMS relay metadata MIME Header Fields constraints 14
5.4.2 signed data MIME Header Fields constraints 15
5.4.3 REMS introduction MIME Header Fields-Body constraints 15
5.4.3.1 General Requirements 15
5.4.3.2 multipart/alternative: free text subsection Header Fields constraints 15
5.4.3.3 multipart/alternative: HTML subsection Header Fields constraints 15
5.4.4 original message MIME Header Fields constraints 15
5.4.5 REMS extensions MIME Header Fields constraints 16
5.4.6 ERDS evidence MIME Header Fields constraints 16
5.4.7 REMS signature MIME Header Fields-Body constraints 16
5.5 REMS - evidence set constraints 17
5.5.1 ERDS evidence types constraints 17
5.5.1.1 Mandatory evidence - all styles of operation 17
5.5.1.2 Mandatory evidence - S&N style of operation 17
5.5.1.3 Conditional evidence - all styles of operation 18
5.5.2 ERDS evidence components constraints 19
5.5.2.1 General requirements 19
5.5.2.2 SubmissionAcceptance - SubmissionRejection 19
5.5.2.3 ContentConsignment - ContentConsignmentFailure 20
5.5.2.4 ContentHandover - ContentHandoverFailure 20
5.5.2.5 RelayAcceptance - RelayRejection 21
5.5.2.6 RelayFailure 21
Annex A (informative): REM best practices 22
Annex B (informative): REM baseline rationales 23
B.1 Introduction 23

B.2 Common Service Interface (CSI) 23
B.2.1 Overview 23
B.2.2 Derived rationales 25
B.2.2.1 General 25
B.2.2.2 Message Routing 25
B.2.2.3 Trust establishment 25
B.2.2.4 Capability discovery and management 35
B.2.2.5 Governance support 38
B.3 Digital signatures and time-stamp 39
B.3.1 Overview 39
B.3.2 Submission event 41
B.3.3 Relay event 42
B.3.4 Consignment event 44
Annex C (normative): REM baseline requirements 45
C.1 General requirements 45
C.2 Common Service Interface (CSI) 45
C.2.1 Overview 45
C.2.2 General provisions 45
C.2.3 Basic handshake 46
C.2.3.1 Introduction 46
C.2.3.2 Message Routing 46
C.2.3.3 Trust establishment 46
C.2.3.3.1 Trust - Trusted List general requirements 46
C.2.3.3.2 Trust - Trusted List service element restrictions 47
C.2.3.3.3 Trust - Validation steps 49
C.2.3.4 Capability discovery and management 50
C.2.3.4.1 Capabilities - Trusted List general requirements 50
C.2.3.4.2 Capability metadata - Trusted List referencing of REMS metadata 54
C.2.3.4.3 Capability metadata - Consistency and validation steps 57
C.2.3.4.4 Capability-based security - Trusted List referencing of security tokens 58
C.2.3.4.5 Capability-based security - Consistency and validation steps 59
C.2.3.4.6 Capability - Discovery interface 60
C.2.3.5 Governance support 60
C.3 ERDS evidence - composition 65
C.3.1 General requirements 65
C.3.2 New ERDS evidence extensions 66
C.3.2.1 GeneralEvidenceInfo extension 66
C.3.2.2 RelayEvidenceInfo extension 67
C.3.3 Composition requirements 68
C.3.4 Detail requirements 70
C.4 Digital signatures and time-stamp 76
C.4.1 Overview 76
C.4.2 REM messages - digital signature provisions 77
C.4.3 ERDS evidence - digital signature provisions 77
C.4.4 ERDS evidence - time-stamp provisions 78
C.4.5 Specific applications 78
C.4.5.1 Submission event 78
C.4.5.2 Relay event 80
C.4.5.3 ContentConsignment event 84
C.4.5.4 Summary tables 87
Annex D (informative): REM baseline best practices 92
D.1 Global governance practices 92
D.1.1 General 92
D.1.2 Links with national laws 92
D.1.3 REMID policy elements 92

D.2 Registration and setup practices 93
D.2.1 General 93
D.2.2 Certificate and signature properties 93
D.2.2.1 Certificate significant elements 93
D.2.2.2 Certificate issuing path 93
D.2.2.3 Digital signature - signature-policy-identifier 94
D.2.3 TL fulfilment 95
D.2.4 Flow elements 95
D.3 Periodical practices 95
D.4 Run-time practices 95
D.4.1 General 95
D.4.2 Basic handshake 95
D.4.3 Content checks 96
D.4.4 Events checks 96
D.4.5 Complete set of examples 97
Annex E (normative): XML schema files 98
E.1 XML Schema file location for namespace http://uri.etsi.org/19532/v1# 98
Annex F (informative): Change History 99
History 101

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are 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 Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, 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.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This draft European Standard (EN) has been produced by ETSI Technical Committee Electronic Signatures and Infrastructures (ESI), and is now submitted for the combined Public Enquiry and Vote phase of the ETSI standards EN Approval Procedure.

The present document is part 4 of a multi-part deliverable. Full details of the entire series can be found in part 1 [4].

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

Modal verbs terminology

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

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

Introduction

Registered Electronic Mail (REM) is a particular instance of an Electronic Registered Delivery Service (ERDS). Standard email, used as a 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.). It protects against the risk of loss, theft, damage and any illegitimate modification.
The present document covers the common and worldwide-recognized requirements to address electronic registered delivery securely and reliably. Particular attention is paid to the Regulation (EU) No 910/2014 [i.1]. However, the legal effects are outside the scope of the present document.

1 Scope

The present document specifies the interoperability profiles of the Registered Electronic Mail (REM) messages according to the formats defined in ETSI EN 319 532-3 [6] and the concepts and semantics defined in ETSI EN 319 532-1 [4] and ETSI EN 319 532-2 [5]. It deals with issues relating to authentication, authenticity and integrity of the information, with the purpose to address the achievement of interoperability across REM service providers, implemented according to the aforementioned specifications.

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

More specifically, the present document:

a) Defines generalities on profiling.

b) Defines constraints for SMTP profile.

The present document also specifies a REM baseline supporting the technical interoperability amongst service providers in different regulatory frameworks.

NOTE: Specifically but not exclusively, REM baseline specified in the present document aims at supporting implementations of interoperable REM services by use of Trusted List Frameworks to constitute Trusted domains and qualified REM services (instances of electronic registered delivery services) by use of EU Trusted List system as per Regulation (EU) No 910/2014 [i.1].

2 References

2.1 Normative references

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

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

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

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

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

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

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

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

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

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

[7] IETF RFC 5321: "Simple Mail Transfer Protocol".

[8] IETF RFC 5322: "Internet Message Format".

[9] IETF RFC 2045: "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies".

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

[11] ETSI EN 319 522-4-3: "Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 4: Bindings; Sub-part 3: Capability/requirements bindings".

[12] ETSI TS 119 612 (V2.2.1): "Electronic Signatures and Infrastructures (ESI); Trusted Lists".

[13] ETSI EN 319 122-1: "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures".

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

[15] eIDAS Technical Specifications: "SAML Attribute Profile" - Version 1.2", 31 August 2019.

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] 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.2] ISO/IEC TR 10000:1998: "Information technology - Framework and taxonomy of International Standardized Profiles".

[i.3] IETF RFC 6698: "The DNS-Based Authentication of Named Entities (DANE), Transport Layer Security (TLS) Protocol: TLSA".

[i.4] IETF RFC 7208: "Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1".

[i.5] IETF RFC 6376: "DomainKeys Identified Mail (DKIM) Signatures".

[i.6] NIST Special Publication 800-177: "Trustworthy Email".

[i.7] NIST Special Publication 800-45: "Guidelines on Electronic Mail Security, Version 2".

[i.8] IPJ - The Internet Protocol Journal - November 2016, Volume 19, Number 3: "Comprehensive Internet E-Mail Security: Review of email vulnerabilities and security threats".

[i.9] IETF RFC 4035: "Protocol Modifications for the DNS Security Extensions".

[i.10] IETF RFC 7489: "Domain-based Message Authentication, Reporting, and Conformance (DMARC)".

[i.11] IETF RFC 8551: "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 4.0 Message Specification".

[i.12] ETSI EN 319 521: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Electronic Registered Delivery Service Providers".

[i.13] IETF RFC 7817: "Updated Transport Layer Security (TLS) Server Identity Check Procedure for Email-Related Protocols".

[i.14] IETF RFC 2046: "Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types".

[i.15] ETSI TR 119 001 (V1.2.1): "Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures; Definitions and abbreviations".

[i.16] IETF RFC 8550: "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 4.0 Certificate Handling".

3 Definition of terms, symbols, abbreviations and terminology

3.1 Terms

For the purposes of the present document, the terms given in ETSI EN 319 532-1 [4] and the following apply:

REMID authority: entity entitled to govern the REMID

NOTE: A REMID authority governs the REMID by the management of the REMID policy and through processes of supervision and monitoring, ensuring the adherence to the REMID policy and the requirements specified in the present document.

REMID policy: set of organizational, security and technical requirements that each adherent REMSP is obliged to fulfil to achieve interoperability

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI EN 319 532-1 [4], ETSI TR 119 001 [i.15] and the following apply:

CC Country Code

NOTE: As defined in ETSI TS 119 612 [12], clause 3.2.

DNS Domain Name System
EML Electronic Mail Format

NOTE: As per Internet Message Format syntax defined in IETF RFC 5322 [8].

MS Member State

NOTE: As defined in ETSI TS 119 612 [12], clause 3.2.

QERDS Qualified Electronic Registered Delivery Service

NOTE: As per the definition in ETSI EN 319 522-4-3 [11], clause 7.2.

QREMS Qualified Registered Electronic Mail Service
SAN Subject Alternative Name (or SubjectAltName) X509v3 digital certificate extension

NOTE: As per extension defined in IETF RFC 8550 [i.16], clause 4.4.3.

TSL Trust Status List

NOTE: As per the definition in ETSI EN 319 522-2 [2], clause 9.3.

3.4 Terminology

Since Registered Electronic Email Services are specific types of Electronic Registered Delivery Services, the present document uses the terms and definitions from ETSI EN 319 521 [i.12] and ETSI EN 319 522 (Parts 1 to 3) [1], [2] and [3].

ETSI EN 319 532-2 [5], clause 4.1 specifies the usage of prefixes ERD versus REM or ERDS versus REMS for naming concepts and structures.

The naming convention used in the present document is that constructs whose content is completely generated by the REMS are prefixed with "ERDS" or "REMS". In contrast, constructs whose content includes user-generated data is prefixed with "ERD" or "REM".

4 General requirements

4.1 Introduction

The present document provides one profile as intended in ISO/IEC TR 10000 [i.2]: *"the identification of chosen classes, conforming subsets, options and parameters of base standards, or International Standardized Profiles necessary to accomplish a particular function"*. In the present document the concept of profile embraces references like architectural, protocol detail, semantic and implementation aspects, and technical standard and service interoperability aspects.

More specifically, the present document specifies a REM service profile that uses the same formats (S/MIME based) and the same transport protocols (SMTP). Annex B and Annex C specify the baseline set of requirements for the implementation and configuration of interoperable REM services.

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

4.2 Compliance requirements

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

Table 1: Requirements categories

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

All the requirements shall be defined in tabular form.

Table 2: Requirements template

Nº	Service/Protocol element	EN reference	Requirement	Implementation guidance	Notes

Column **N**º shall identify a unique number for the requirements. This number shall start from 1 in each clause. The eventual references to it would also include the clause number to avoid any ambiguity.

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

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

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

Column **Implementation guidance** shall contain numbers referencing notes and letters referencing additional requirements. It is intended either to explain how the requirement is implemented or to include any other information not mandatory.

Column **Notes** shall contain additional notes to the requirement.

NOTE: Within a REMID, a provision different from the ones specified in the present document is viable if and only if such REMID does not envisage to interoperate with other REMIDs.

5 SMTP interoperability profile

5.1 General requirements

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

In particular, the concepts defined in IETF RFC 5321 [7], clause 2.3.1 regarding envelope and content of the Mail Objects, and the concepts defined in IETF RFC 5322 [8], clause 2.2 and IETF RFC 2045 [9] regarding the collection of header fields, structure, formats and message representation shall apply.

5.2 Style of operation

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

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

Then, all the REMS operating under the Store-And-Notify style of operation also need a REMS operating under Store-And-Forward style of operation that represents a common layer between the two styles of operation.

Differences only arise in the set of mandatory evidence, which is specified within the two styles of operations, as described in clause 5.5.

5.3 REMS - interfaces constraints

5.3.1 Introduction

The next clauses profile the interfaces specified in ETSI EN 319 522-1 [1] and ETSI EN 319 532-1 [4], clause 5.

5.3.2 REM MSI: Message Submission Interface

Table 3: REM message submission interface

Nº	Service/Protocol element	ETSI EN 319 532-1 [4] reference	Requirement	Implementation guidance	Notes
1	Any protocol, provided that it is secured	Clause 5	M	a)	

Implementation guidance:

a) The Message Submission Interface shall be implemented with a protocol that shall secure the communication from the originating mail User Agent to the SMTP server. More specifically, this protocol shall ensure proper identification and authentication of the user, confidentiality of the communication, authenticity and integrity of the submitted data. For example, SMTP on TLS according to IETF RFC 7817 [i.13] or SSL plus a check of credential over SMTP-AUTH may be used.

5.3.3 REM MRI-ERI: Message and Evidence Retrieval Interface

Table 4: REM message and evidence retrieval interface

Nº	Service/Protocol element	ETSI EN 319 532-1 [4] reference	Requirement	Implementation guidance	Notes
1	Any protocol, provided that it is secured	Clause 5	M	a)	

Implementation guidance:

a) The Message and Evidence Retrieval Interface shall be implemented with a protocol that shall secure the communication from the sender/recipient mail User Agent to the REMSP server. More specifically, this protocol shall ensure proper identification and authentication of the user, confidentiality of the communication, authenticity and integrity of the retrieved data. For example, IMAP or POP or HTTP on TLS according to IETF RFC 7817 [i.13] or SSL may be used.

5.3.4 REM RI: Relay Interface

Table 5: REM relay interface

Nº	Service/Protocol element	ETSI EN 319 532-1 [4] reference	Requirement	Implementation guidance	Notes
1	SMTP on TLS	Clause 5	M	a)	see note
NOTE: This is a profile for SMTP relay protocol among REMSPs, and it is reflected in this requirement.					

Implementation guidance:

a) The Relay Interface shall be implemented using SMTP protocol securing the communication from the sender REMSP server to the recipient REMSP server using TLS according to IETF RFC 3207 [10].

NOTE: Particular attention has to be paid to preserving confidentiality, authenticity, integrity, identification and authentication. TLS and the best practices recommended in Annex A give the necessary provision to accomplish these requirements. Further IETF work about MTA-to-MTA (TLS everywhere) dialogue is actually under a draft status and not added as a reference in the present document. However, it is a desirable practice in addition to opportunistic STARTTLS/DANE (see NIST Special Publication 800-177 [i.6] for more details).

5.3.5 CSI: Common Service Interface

The services used throughout this interface are not necessarily provided by a REMS (see note 1) and, for the present profile, the following three main elements shall be considered:

1) Routing

2) Trusting

3) Capability discovery and management

NOTE 1: For this reason, the prefix REM is omitted before the definition of the interface.

ETSI EN 319 532-2 [5], clause 9 shall identify the semantic requirements that apply to CSI.

Table 6: Common service interface

Nº	Service/Protocol element	ETSI EN 319 532-3 [6] reference	Requirement	Implementation guidance	Notes
1	DNS	Clause 9.2	M	a)	Routing interface
2	TL	Clause 9.3	R	b)	Trusting interface
3	TL/SMP	Clause 9.4	O	c)	Discovery/management interface

Implementation guidance:

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

NOTE 2: The best practices recommended in Annex A give further indications to accomplish security requirements about routing.

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

c) The Discovery/management Interface, part of CSI, may be implemented using both or either TL or SMP protocols.

5.4 REM message constraints

5.4.1 REMS relay metadata MIME Header Fields constraints

Table 7: REM message header fields constraints

Nº	Service/Protocol element	ETSI EN 319 532-3 [6] reference	Requirement	Implementation guidance	Notes
1	REM-MessageType	Clause 6.1	M	a)	
2	REM-EventIdentifier	Clause 6.1	M	b)	
3	REM-Evidence-ID	Clause 6.2.1	M	c)	
4	REM-ReasonIdentifier	Clause 6.2.1	R	d)	

Implementation guidance:

a) Its value shall be one of the 4 strings defined in table 2 of ETSI EN 319 532-3 [6], clause 6.1, related to the MD13 component.

b) Its value shall be the G03 component, as defined in table 2 of ETSI EN 319 532-3 [6], clause 6.1. It shall be composed by the URI in column 1, table 3 of ETSI EN 319 522-3 [3], clause 5.2.2.5.

c) Its value shall be the G01 component corresponding to the evidence specified inside the "EvidenceIdentifier" ERDS evidence element defined in ETSI EN 319 522-3 [3], clause 5.2.2.3.