SLOVENSKI STANDARD
oSIST prEN 319 522-2 V1.2.0:2023

01-december-2023

Elektronski podpisi in infrastruktura (ESI) - Storitve elektronske priporočene dostave - 2. del: Semantične vsebine

Electronic Signatures and Infrastructures (ESI) - Electronic Registered Delivery Services - Part 2: Semantic contents

Ta slovenski standard je istoveten z: **ETSI EN 319 522-2 V1.2.0 (2023-10)**

ICS:

35.040.01	Kodiranje informacij na splošno	Information coding in general

oSIST prEN 319 522-2 V1.2.0:2023 **en**

Draft ETSI EN 319 522-2 V1.2.0 (2023-10)

Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 2: Semantic contents

Reference

REN/ESI-0019522-2v121

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

Contents

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 2 of a multi-part deliverable. Full details of the entire series can be found in part 1 [1].

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.

1 Scope

The present document specifies the semantic content that flows across the interfaces of ERD services which are specified in ETSI EN 319 522-1 [1], clause 5.

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] IETF RFC 3061: "A URN Namespace of Object Identifiers".

[3] Core Person Vocabulary v2.0.

[4] Registered Organizations Vocabulary v2.0.

[5] CEF eIDAS Technical Sub-group: "eIDAS SAML Attribute profile", Version 1.2. 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] Void.

[i.3] IETF RFC 4122: "A Universally Unique IDentifier (UUID) URN Namespace".

[i.4] IETF RFC 5322: "Internet Message Format".

[i.5] ETSI TS 119 312: "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites".

[i.6] ETSI TS 119 612: "Electronic Signatures and Infrastructures (ESI); Trusted Lists".

[i.7] ETSI EN 319 522-3: "Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 3: Formats".

[i.8] ETSI EN 319 522-4-1: "Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 4: Bindings; Sub-part 1: Message delivery bindings".

[i.9] ETSI EN 319 522-4-2: "Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 4: Bindings; Sub-part 2: evidence and identification bindings".

[i.10] Void.

[i.11] ETSI EN 319 122-1: "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures".

[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 EN 319 142-1: "Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in ETSI EN 319 522-1 [1] and the following apply:

ERD dispatch: ERD message which contains the user content, some ERDS relay metadata and ERDS evidence

ERD payload: ERD message which contains the user content and some ERDS relay metadata

ERDS receipt: ERD message which contains ERDS evidence and some ERDS relay metadata

ERDS serviceinfo: ERD message which contains some ERDS relay metadata

3.2 Symbols

Void.

3.3 Abbreviations

Void.

4 Overview

The present document specifies the semantic content that flows across the interfaces which have been identified in ETSI EN 319 522-1 [1]. No requirements are introduced on the specific formats for the content; formats are specified in ETSI EN 319 522-3 [i.7].

Figure 1 outlines how data flows through the interfaces in the 4-corner model. User content shall not be changed by ERDSs. Data flowing between systems is always encrypted, as specified by the applicable binding. As detailed below, not all objects are always required.

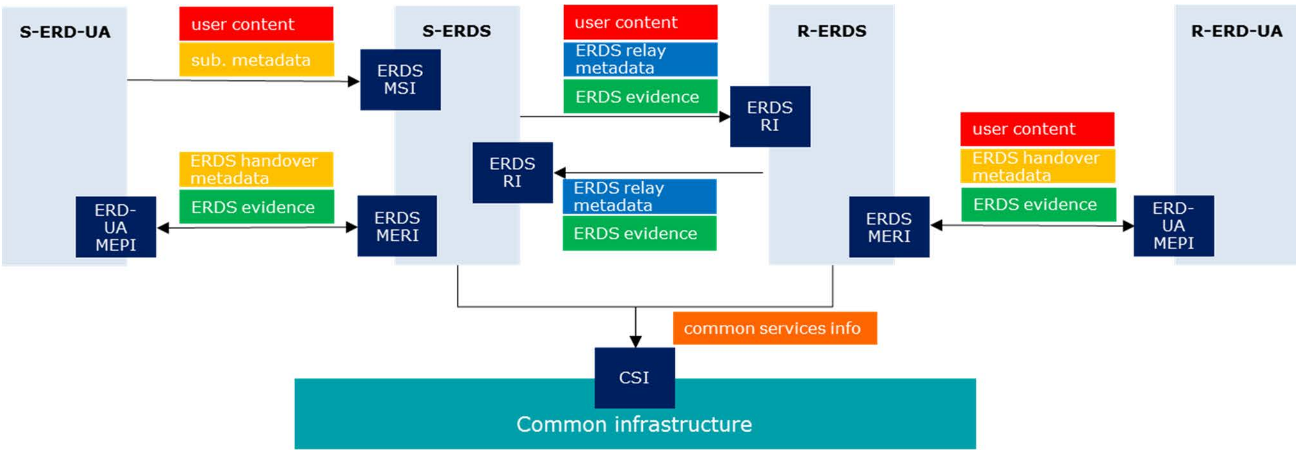

Figure 1: Data flowing through interfaces

For convenience, the present document defines (table 1) some aggregate constructs (ERD dispatch, ERDS receipt, ERDS serviceInfo, ERD payload, original message) which package the basic objects (user content, ERDS relay metadata, ERDS evidence, submission metadata) in different modes. Constructs define the semantic information flowing between parties, so they ease the definition of bindings [3] and [4], even if, specific bindings may split the construct in its basic objects for transport.

The naming convention used in the present document is that constructs whose content is completely generated by the ERDS are prefixed with "ERDS", while constructs whose content includes user generated data is prefixed with "ERD". Table 1 specifies the composition of constructs as a collection of basic objects.

Table 1: Composition of constructs

Construct \ Basic object		user content	ERDS relay metadata	ERDS evidence	submission metadata
ERD message	ERD dispatch	1	1	1..n	0
	ERDS receipt	0	1	1..n	0
	ERDS serviceInfo	0	1	0	0
	ERD payload	1	1	0	0
	original message	1	0	0	0..1

NOTE: ERDS receipt (which contains ERDS relay metadata and also ERDS evidence) and ERDS serviceInfo (which only contains ERDS relay metadata) may play the role of notifications in those cases where this feature is required, and in such cases the recipient can be informed of this role by some metadata or other element.

Table 2 provides an abstract specification of the functions provided by the ERDS APIs as defined in ETSI EN 319 522-1 [1].

Table 2: Abstract interfaces

Interface	Provided function	Description	Arguments and output
ERDS MSI	out := SubmitMessage(og)	The method is used for posting an original message to the S-ERDS. In order to use the SubmitMessage API, the UA/Application has to prove that the sender is the owner of the sender's identifier (via an authentication token, a challenge response, etc.).	og: original message, composed of user content and (optional) submission metadata. out: the outcome of the method. There is no specification on the outcome, which may be a simple success/error indication, or may include a message identifier or a larger set of information.
ERDS MERI	out :=RetrieveMessage (mi)	The method is used for retrieving a user content from the R-ERDS. Alternatively, a push of the user content to the recipient UA/application can be used through the ERD-UA MEPI interface In order to use the RetrieveMessageAPI, the UA/Application has to prove that the recipient is the owner of the recipient's identifier (via an authentication token, a challenge response, etc.).	mi: this is a set of parameters which is used for the identification and retrieval of the requested user content. out: this is the outcome of the method, which, in case of success, includes the user content and possibly handover metadata and ERDS evidence. In case of failure the outcome will include error information.
	e := GetEvidences(ei)	The method is used for retrieving one or more evidences associated to a user content which has previously been managed by the ERDS. Note that this is not the only way to obtain evidence, since an evidence can be transmitted in different ways (e.g. as an output of the SubmitMessage or the RetrieveMessage).	ei: this is a set of parameters which is used for the identification and retrieval of the requested evidence. e: the requested evidences.
ERD-UA MEPI	out := HandoverObjects(o)	The method is used for handing over user content, ERDS evidence, handover metadata to the ERD-UA.	o: a combination of user content [0..1], ERDS evidence [0..n], handover metadata [0..1], excluding void. out: this is the outcome of the method, which is a success/failure indication plus error information in case of failure.
ERDS RI	out := Relay(em)	The method is used for relaying an ERD message to a different ERDS. Relaying is used when S-ERDS has not the capability to deliver to the recipient itself. Metadata and evidences may be transmitted with the user content or independently from the user content through this method.	em: ERD message. out: this is the outcome of the method, which is a success/failure indication plus error information in case of failure. It may also include an evidence and ERDS relay metadata.
CSI	re:= LookupERDS(ri)	This method is used to identify the ERDS which has the capability to deliver to a defined recipient. The method may return more than one ERDS.	ri: unique identification of the recipient, which may be one identifier or a set of attributes that together provides unique identification (e.g. id, domain, application protocol, etc.). re: one or more endpoints of the ERDS(s) which has(have) the capability to deliver to the recipient identified by ri.
	out := ValidateERDS(ei, p)	This method may be used to validate the inclusion of an ERDS intro a trust circle. The method may receive some parameters for the validation (e.g. date and time of validity, specific trust circle, etc.).	ei: a unique identifier for the ERDS. p: a set of parameters for the validation out: the outcome of the check, which may include a set of information about the ERDS from a trust perspective.
	em := GetERDSMetadata (ei)	This method is used to retrieve operational metadata about a specific ERDS.	ei: a unique identifier for the ERDS. em: a set of information about the ERDS from an operational perspective (capabilities, requirements, endpoints).