



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

iTeh Standards
(<https://standards.iteh.ai>)

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

[oSIST prEN 319 522-2 V1.2.0:2023](https://standards.iteh.ai/catalog/standards/sist/c69f5791-4160-4412-a7c8-4f5594e805fd/osist-pren-319-522-2-v1-2-0-2023)

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**

**(<https://standards.iteh.ai>)
Document Preview**

[oSIST prEN 319 522-2 V1.2.0:2023](https://standards.iteh.ai/catalog/standards/sist/c69f5791-4160-4412-a7c8-4f5594e805fd/osist-pren-319-522-2-v1-2-0-2023)

<https://standards.iteh.ai/catalog/standards/sist/c69f5791-4160-4412-a7c8-4f5594e805fd/osist-pren-319-522-2-v1-2-0-2023>

Reference

REN/ESI-0019522-2v121

Keywordse-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/CommitteeSupportStaff.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.

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.

The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2023.
All rights reserved.

Contents

Intellectual Property Rights	5
Foreword.....	5
Modal verbs terminology.....	5
1 Scope	6
2 References	6
2.1 Normative references	6
2.2 Informative references.....	6
3 Definition of terms, symbols and abbreviations.....	7
3.1 Terms.....	7
3.2 Symbols.....	7
3.3 Abbreviations	7
4 Overview	7
5 Identification of actors.....	10
5.1 Introduction	10
5.2 Identifiers	10
5.3 Identity attributes.....	10
5.3.1 Introduction.....	10
5.3.2 Identity attributes of natural persons.....	10
5.3.3 Identity attributes of legal person	10
5.3.4 Identity attributes of other entities	10
5.4 Identity verification and authentication assurance levels information	11
6 ERDS relay metadata	11
6.1 Introduction	11
6.2 Metadata components.....	12
6.2.1 MD01 - Metadata version	12
6.2.2 MD02 - Relay date and time.....	12
6.2.3 MD03 - Expiry date and time	12
6.2.4 MD04 - Recipient required level of assurance.....	12
6.2.5 MD05 - Applicable policy	13
6.2.6 MD06 - Mode of consignment.....	13
6.2.7 MD07 - Scheduled delivery	13
6.2.8 MD08 - Sender's identifier.....	14
6.2.9 MD09 - Reply-to.....	14
6.2.10 MD10 - Recipient's identifier	14
6.2.11 MD11 - Message identifier	14
6.2.12 MD12 - In reply to.....	14
6.2.13 MD13 - Message type.....	14
6.2.14 MD14 - User content information.....	15
6.2.15 MD15 - Other metadata	15
7 Digital signatures in ERDS provisioning	15
7.1 Objects and actors for digital signatures.....	15
7.2 Common requirements for digital signatures	15
8 ERDS evidence set and components	16
8.1 Introduction	16
8.2 Evidence components.....	17
8.2.1 G01 - Evidence identifier.....	17
8.2.2 G02 - Evidence version.....	17
8.2.3 G03 - Event identifier	17
8.2.4 G04 - Reason identifier.....	18
8.2.5 G05 - Event time.....	18
8.2.6 G06 - Transaction log information	18
8.2.7 R01 - Evidence issuer policy identifier.....	18

8.2.8	R02 - Evidence issuer details.....	18
8.2.9	R03 - Signature by issuing ERDS.....	19
8.2.10	I01 - Sender's identity attributes	19
8.2.11	I02 - Sender's identifier.....	19
8.2.12	I03 - Sender's delegate identity attributes	19
8.2.13	I04 - Sender's delegate identifier.....	20
8.2.14	I05 - Recipient's identity attributes	20
8.2.15	I06 - Recipient's identifier.....	20
8.2.16	I07 - Recipient's delegate identity attributes	20
8.2.17	I08 - Recipient's delegate identifier	21
8.2.18	I09 - Recipient referred to by the Evidence	21
8.2.19	I10 - Sender's identity assurance level details.....	21
8.2.20	I11 - Sender's delegate identity assurance level details	21
8.2.21	I12 - Recipient's identity assurance level details	22
8.2.22	I13 - Recipient's delegate identity assurance level details	22
8.2.23	M01 - Message identifier.....	22
8.2.24	M02 - User content information	22
8.2.25	M03 - Submission date and time	22
8.2.26	M04 - External system.....	23
8.2.27	M05 - External ERDS.....	23
8.2.28	E01 - Extensions	23
8.3	Evidence components values.....	23
8.3.1	Free text	23
8.3.2	Events	23
8.3.3	Reasons	24
8.3.3.1	Reasons related to Events A.x (Sender's submission).....	24
8.3.3.2	Reasons related to the Events B.x (Relay between ERDSs)	25
8.3.3.3	Reasons related to events C.x (Acceptance/rejection by the recipient).....	25
8.3.3.4	Reasons related to events D.x (Consignment to the recipient).....	27
8.3.3.5	Reasons related to events E.x (Handover to the recipient).....	27
8.3.3.6	Reasons related to events F.x (Connection to non ERDS).....	28
8.4	Additional requirements for components of evidence.....	29
9	Common Services Interface content.....	31
9.1	Introduction	31
9.2	ERD message routing.....	31
9.3	ERDS trust establishment and governance.....	31
9.4	Capability management.....	32
9.4.1	Introduction.....	32
9.4.2	Resolving recipient identification to ERDS identification.....	32
9.4.3	Recipient metadata.....	33
9.4.4	ERDS capability metadata.....	33
Annex A (informative): Change History		35
History		36

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.

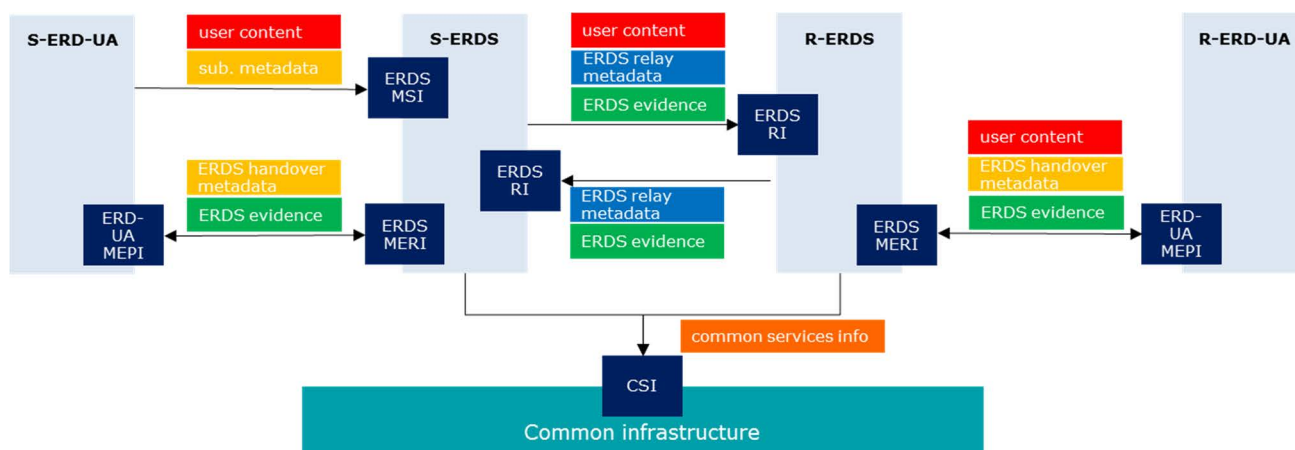


Figure 1: Data flowing through interfaces

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
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 RetrieveMessage API, 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 into 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).