ETSI EN 319 522-2 V1.1.1 (2018-09)

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

Reference

DEN/ESI-0019522-2

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 only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

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 European Standard (EN) has been produced by ETSI Technical Committee Electronic Signatures and Infrastructures (ESI).

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

National transposition dates	
Date of adoption of this EN:	23 August 2018
Date of latest announcement of this EN (doa):	30 November 2018
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	31 May 2019
Date of withdrawal of any conflicting National Standard (dow):	31 May 2019

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.

NOTE: Available at https://joinup.ec.europa.eu/solution/core-person-vocabulary.

[4] Registered Organizations Vocabulary v2.0.

NOTE: Available at https://joinup.ec.europa.eu/solution/registered-organization-vocabulary.

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] Directive 2012/17/EU of the European Parliament and of the Council of 13 June 2012 amending Council Directive 89/666/EEC and Directives 2005/56/EC and 2009/101/EC of the European Parliament and of the Council as regards the interconnection of central, commercial and companies registers. Text with EEA relevance.

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

[i.4] IETF RFC 5332: "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] CEF eIDAS Technical Sub-group: "eIDAS SAML Attribute profile", Version 1.1.2. October 2016.

[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 Definitions

For the purposes of the present document, the terms and definitions 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

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 four 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.

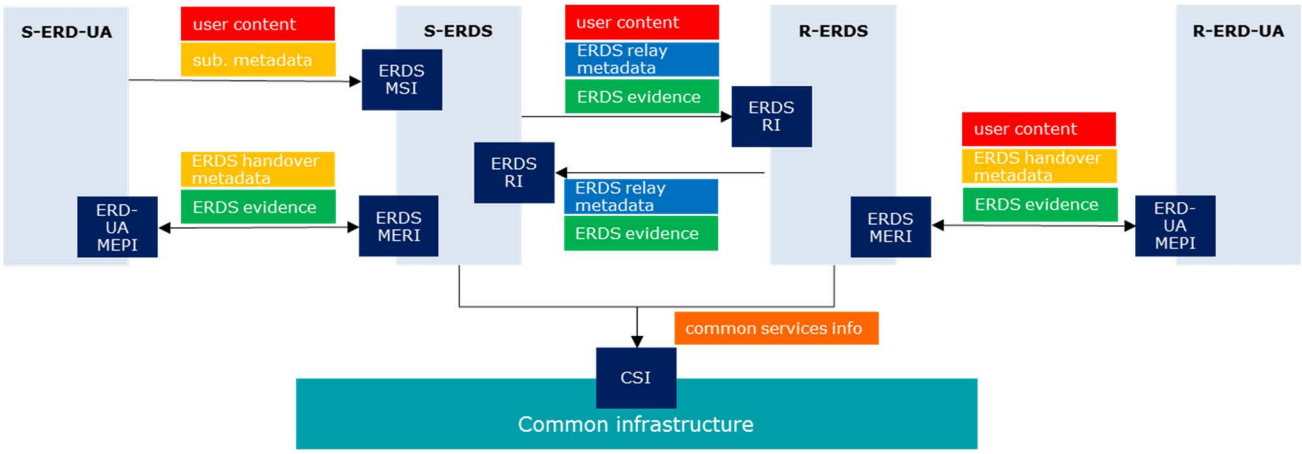

Figure 1: Data flowing through interfaces

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] [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

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).

The following clauses specify the semantics of the data which are transported through the interfaces; in particular:

- Clause 5 specifies the semantics of the components required for identifying the sender and the recipient.
- Clause 6 specifies the semantics of ERDS relay metadata.
- Clause 8 specifies the semantics of ERDS Evidence.
- Clause 9 specifies the semantics of information for Common Service Interface.

5 Identification of actors

5.1 Introduction

An ERDS needs to generate, exchange and validate attributes to support the identification and authentication of end entities like sender, recipient or a delegate.

5.2 Identifiers

An identifier shall have two components: an identifying scheme name and the identifier value, which shall be coherent with the identifying scheme name. The identifier shall be unique within the network of interoperating ERDSs.

5.3 Identity attributes

5.3.1 Introduction

All attributes in the present document related to identification and authentication are derived from the EU Vocabulary. For natural persons, the attributes defined by the Core Person Vocabulary [3] shall be used, for legal persons, the attributes defined by the Registered Organization Vocabulary [4] shall be used. The Registered Organization Vocabulary defines the core vocabulary for legal persons registered through a formal process, typically in a national or regional register.

For the sake of simplicity, the present document limits the supported attributes to the ones defined in the eIDAS attribute profile specification [i.10], which are also attributes derived from the ISA vocabulary.

5.3.2 Identity attributes of natural persons

For natural persons, a non empty subset of the following identity attributes shall be used.

Table 3: Natural person identity attributes

Attribute (Friendly) Name as defined by [i.10]	eIDAS minimum data set attribute	Core Vocabulary Equivalent
FamilyName	Current Family Name	cbc:FamilyName
FirstName	Current First Names	cvb:GivenName
DateOfBirth	Date of Birth	cvb:BirthDate
PersonIdentifier	Uniqueness Identifier	cva:Cvidentifier
BirthName	First Names at Birth	cvb:BirthName
BirthName	Family Name at Birth	cvb:BirthName
PlaceOfBirth	Place of Birth	cva:BirthPlaceCvlocation
CurrentAddress	Current Address	cva:Cvaddress
Gender	Gender	cvb:GenderCode

5.3.3 Identity attributes of legal person

For legal persons, a non empty subset of the following identity attributes shall be used.

Table 4: Legal person identity attributes

Attribute (Friendly) Name as defined by [i.10]	eIDAS minimum data set attribute	Core Vocabulary Equivalent
LegalName	Current Legal Name	cvb:LegalName
LegalPersonIdentifier	Uniquenes Identifier	cva:Cvidentifier
LegalAddress	Current Address	cva:Cvaddress
VATRegistration	VAT Registration Number	cva:CvbusinessCode
TaxReference	Tax Reference Number	cva:CvbusinessCode
BusinessCodes	Directive 2012/17/EU [i.2] Identifier	cva:CvbusinessCode
LEI	Legal Entity Identifier (LEI)	cva:CvbusinessCode
EORI	Economic Operator Registration and Identification (EORI)	cva:CvbusinessCode
SEED	System for Exchange of Excise Data (SEED)	cva:CvbusinessCode
SIC	Standard Industrial Classification (SIC)	cva:CvbusinessCode

5.3.4 Identity attributes of other entities

Identity attributes may also be provided for entities which do not correspond to natural or legal persons (e.g. applications, things). They are not specified in the current version of the present document.

5.4 Identity verification and authentication assurance levels information

This clause defines the information which is necessary to establish the level of assurance for the entities which take part in the electronic delivery process. This information shall include:

1) An attribute containing details of the registration and identity proofing and verification assurance level. This attribute:

   a) shall contain one identifier of the assurance level itself. This identifier shall have a URI as value;

   b) may also contain an identifier of the identification policy. This identifier shall have a URI as value;

   c) may also contain details on the identification policy;

   d) may also contain one or more URIs pointing to resources that contain details of the aforementioned policy provided in different languages.

2) An attribute containing details of the authentication means and mechanisms assurance level. This attribute:

   a) shall contain one identifier of the assurance level itself. This identifier shall have a URI as value;

   b) may also contain an identifier of the authentication policy. This identifier shall have a URI as value;

   c) may also contain details on the authentication policy;

   d) may also contain one or more URIs pointing to resources that contain details of the aforementioned policy provided in different languages.

Furthermore, the identity assurance information may include an attribute containing details of the performed authentication, either an assertion generated by an assertion provider or as a sequence of components, consisting of:

- the date and time when the authentication process was conducted;
- the identification of the authentication method used.