ETSI EN 319 522-4-3 V1.1.1 (2018-09)

Electronic Signatures and Infrastructures (ESI);
Electronic Registered Delivery Services;
Part 4: Bindings;
Sub-part 3: Capability/requirements bindings

Reference
DEN/ESI-0019522-4-3

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

Contents

Intellectual Property Rights 4
Foreword 4
Modal verbs terminology 4
1 Scope 5
2 References 5
2.1 Normative references 5
2.2 Informative references 5
3 Definitions and abbreviations 6
3.1 Definitions 6
3.2 Abbreviations 6
4 Common Service Interface bindings - general concepts 6
5 Capability metadata location, BDXL binding 6
6 Capability metadata publishing, SMP binding 7
7 Trust information bindings 7
7.1 Introduction 7
7.2 EU Trusted List 8
7.3 Domain Trusted List 9
7.4 Domain PKI 9
7.5 Bilateral trust and other trust models 10
History 11

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 4, sub-part 3 of a multi-part deliverable. Full details of the entire series can be found in part 1 [i.2].

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 provides the binding of the Common Service Interface information, whose semantics is defined in ETSI EN 319 522-2 [1] and whose format is defined in ETSI EN 319 522-3 [2] to the specific services provided by OASIS Business Metadata Service Location [3] and the OASIS Service Metadata Publishing [4]. Furthermore, the present document specifies how to establish trust between ERDSs by use of a Trusted List [5], including the EU Trusted List system used for qualified trust services under the Regulation (EU) No 910/2014 [i.1] using the Trusted List format defined by the corresponding Commission implementing decision (EU) 2015/1505 [i.3], and by means of a domain PKI.

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

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

[3] OASIS: "Business Document Metadata Service Location Version 1.0", OASIS standard, August 2017.

[4] OASIS: "Service Metadata Publishing (SMP) Version 1.0", OASIS standard, August 2017.

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

[6] W3C Recommendation (11 April 2013): "XML Signature Syntax and Processing Version 1.1".

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

[i.3] Commission Implementing Decision (EU) 2015/1505 of 8th September 2015 laying down technical specifications and formats relating to trusted lists pursuant to Article 22(5) of Regulation (EU) No 910/2014.

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in ETSI EN 319 522-1 [i.2] apply.

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI EN 319 522-1 [i.2] apply.

4 Common Service Interface bindings - general concepts

This part specifies the binding for the common services to specific protocols. Semantics for common services shall be as defined in ETSI EN 319 522-2 [1] and formats shall be as defined in ETSI EN 319 522-3 [2].

Specifically:

- receiver identification service is bound to OASIS Business Document Metadata Service Location [3];
- capability discovery service is bound to OASIS Service Metadata Publisher [4];
- ERDS trust evaluation is bound to Trusted List [5] or to use of a domain PKI.

5 Capability metadata location, BDXL binding

When metadata is used, the first step is to obtain the address where the sought metadata is located. This goes for both recipient metadata and metadata about ERDS capabilities, relevant for both the R-ERDS and intermediate ERDSs. This clause describes use of the OASIS Business Document Metadata Service Location Version 1.0 [3] (BDXL), commonly used with the OASIS Service Metadata Publishing (SMP) Version 1.0 [4] described in the next clause.

BDXL is based on DNS (Domain Name Service), which is a common infrastructure for the Internet. From unique identification of an actor - the participant identifier in BDXL terms - for which metadata shall be accessed, a query string is constructed for DNS, returning a URI to the SMP publishing metadata for the identified actor.

In the scope of the present document, the actor identified by the participant identifier is either a recipient or an ERDS, meaning the identified SMP publishes either recipient metadata or ERDS capability metadata as defined by ETSI EN 319 522-2 [1]. ERDS metadata is defined as an extension to SMP metadata, meaning that ERDS metadata is also stored in SMP.

Registration in DNS and forming of query strings shall be done as specified by OASIS BDXL [3]. The identity of an ERDS should be registered in BDXL, i.e. in DNS, by a domain name.

BDXL [3] requires a participant identifier to be registered in BDXL with one and only one URI to an SMP, i.e. one identity shall resolve to one SMP. When a recipient subscribes to more than one ERDS using more than one SMP, either:

- the BDXL registration for the recipient shall resolve to one and the same SMP, which in turn may include pointers (SMP redirection) to other SMPs holding information about the recipient; or

- the recipient identification shall be coupled with a domain, which may be the ERDS name or other information, thereby creating multiple participant identifiers that in BDXL may resolve to URIs for different SMPs.

6 Capability metadata publishing, SMP binding

The URI returned from BDXL points to a metadata repository that shall be in accordance with OASIS Service Metadata Publishing (SMP) Version 1.0 [4].

As stated by SMP [4], clause 4, for core conformance to SMP, SMP service implementations and client lookup implementations (usually from S-ERDS) shall comply with the SMP specification, in particular:

1) The XML schema, refer Appendix B of the SMP specification [4].

2) Use of signatures for signing and verifications as defined in SMP [4], clause 3.6.2.

3) Process execution as defined in SMP [4], clause 2.1.

4) The syntax and semantics defined in the normative parts of SMP [4], clause 3.

5) The SMP REST binding as defined in clauses 3.2, 3.3, 3.4 and 3.5 of SMP [4].

SMP [4], clause 3.6.2 prescribes use of a specific mode of enveloped XML DSIG [6] for digital signatures.

In addition to the REST binding defined by SMP [4], further protocol bindings are possible, but the present document does not specify any other bindings.

SMP [4], clause 2.4 defines participant identifier, document identifier, and process identifier. Each type of identifier should be represented by its scheme and value. Document identifier and process identifier are application protocol information that shall be supplied as sender metadata if this information is necessary for selection of the R-ERDS or ERDS RI to which the ERD message shall be forwarded.

If more than one ServiceMetadata resource exists, as allowed by SMP [4], clause 3.4, selection shall be based on document identifier and/or process identifier.

A service in the SMP data model is a URL, which in the context of the present document is the ERDS RI to which the ERD message shall be routed. The capabilities of this ERDS RI are described by the ServiceMetadata.

The SMP specification [4] allows extensions. The use of extensions shall not contradict nor cause non-conformance with the SMP specification [4]. Metadata for the capabilities of an ERDS is defined in ETSI EN 319 522-3 [2] as an extension to SMP. The capabilities described by the metadata are common to all ERDS RIs exposed by the ERDS. By defining this as an extension to SMP, the existing SMP ServiceMetadata definition does not need to be changed.

7 Trust information bindings

7.1 Introduction

Trust is defined as the existence of a trust domain within which co-operation between participating ERDSs is regulated.

Trust may be established bilaterally between two or more ERDSs, meaning that the trust domain consists of the ERDSs that have entered into bilateral, mutually recognized agreements. Trust may even be established unilaterally, meaning an ERDS trusts another ERDS but not the other way around; this is not considered further in the present document.

As bilateral trust establishment has challenges in scaling to larger numbers of ERDSs, trust infrastructures may be used to establish trust. In this case, the trust infrastructure, i.e. the trust domain, shall have governance, at least for policy regarding conditions for an ERDS to join.

Trust domain policies and governance are out of scope of the present document. However, it is noted that a trust domain policy may specify policy, security, and technical requirement that each ERDS is obliged to fulfil; hence technical interoperability between the ERDSs may be ensured. In other cases, the trust domain may only provide mutual recognition of other ERDSs, while verification of the capabilities of another ERDS (e.g. by use of ERDS metadata) is necessary to determine whether an ERD message can be forwarded to the other ERDS.

The present document provides requirements for establishment of trust domains by use of the EU Trusted List system, by use of a domain specific trusted list, and by a domain specific PKI.

For the trust information bindings specified in clauses 7.2 to 7.3, the information retrieved from the ServiceEndpoint shall be used by verifying that either:

- the certificate is the service digital identity of an ERDS included in a relevant TSL; or
- the certificate has a path to a CA certificate that is the service digital identity of an ERDS in a relevant TSL.

For the trust information bindings specified in clauses 7.4, verify that the certificate has a path to the root-CA of the domain PKI.

7.2 EU Trusted List

An ERDS that has been granted status as a qualified trust service according to Regulation (EU) No 910/2014 [i.1], i.e. the service is a QERDS, shall be listed in the EU Trusted List system established in accordance with article 22 of Regulation (EU) No 910/2014 [i.1]. The Commission implementing decision (EU) 2015/1505 [i.3] specifies the format of the national Trusted Lists based on ETSI TS 119 612 [5].

The following service type identifiers (`tsl:ServiceTypeIdentifier`) URLs are supported for a (Q)ERDS according to ETSI TS 119 612 [5]:

- http://uri.etsi.org/TrstSvc/Svctype/EDS/Q - A qualified electronic registered delivery service providing qualified registered electronic deliveries in accordance with the applicable national legislation in the territory identified by the TL Scheme territory or with Regulation (EU) No 910/2014 whichever is in force at the time of provision.
- http://uri.etsi.org/TrstSvc/Svctype/EDS/REM/Q - A qualified electronic registered mail delivery service providing qualified electronic registered mail deliveries in accordance with the applicable national legislation in the territory identified by the TL Scheme territory or with Regulation (EU) No 910/2014 [i.1] whichever is in force at the time of provision.
- http://uri.etsi.org/TrstSvc/Svctype/EDS - An electronic registered delivery service, not qualified.
- http://uri.etsi.org/TrstSvc/Svctype/EDS/REM - A Registered Electronic Mail delivery service, not qualified.

Where Regulation (EU) No 910/2014 [i.1] is in force, the following trust domains may be established:

- All QERDSs shall be trusted, meaning all services registered according to the two first bullet points above.
- All non-REM QERDSs shall be trusted, meaning all services registered according to the first bullet point in the previous list.
- All qualified REM services shall be trusted, meaning all services registered according to the second bullet point in the previous list.
- To any of the trust domains in the previous bullet points, add non-qualified ERDSs and/or non-qualified REM services listed in the EU Trusted List system that shall be trusted.

NOTE 1: The intention of Regulation (EU) No 910/2014 is that all qualified trust services are trusted. A different question is to what extent the Regulation requires QERDS providers to trust one another for ERD message relaying. It may be argued that a trust domain consisting of all QERDSs (the first bullet point above) is reasonable, and that the technology dependent trust domains of qualified non-REM or REM services (second and third bullet points) are not relevant since these are restrictions that are a matter of capabilities of the QERDSs rather than lack of trust.

The service digital identity element (`tsl:ServiceDigitalIdentity/tsl:DigitalId`) of a (Q)ERDS in the EU Trusted List system shall be one of the following:

1) A single certificate used by the ERDS for digital signing of all ERD messages and ERD evidences.

2) A single CA certificate that shall be used solely for the purpose of issuing certificates to components of the ERDS for digital signing of ERD messages and/or ERD evidences.

Use of a single signing certificate as service digital identity is only applicable where the ERDS is a centralized service, or where it is feasible to replicate the private key corresponding to the certificate to all components of the ERDS where digital signing will take place.

When a CA certificate is used as service digital identity, this may be a root CA or subordinate CA certificate, and there may be a hierarchy of subordinate CAs underneath the CA. An ERD message or ERD evidence digitally signed using a subject certificate that has a path to the CA certificate used as service digital identity shall be regarded as being digitally signed by the ERDS. I.e. all subject certificates issued under this CA are authorized to sign ERD messages and ERD evidences on behalf of the ERDS.

NOTE 2: If the ERDS uses Trusted Lists to publish trust information about itself, the ERDS capability metadata can be accessible in any of the following ways:

- Downloadable from the URI pointed by the TSP service definition URI, as per clause 5.5.8 of ETSI TS 119 612 [5].
- Downloadable from a URI pointed by the additionalServiceInformation field of Service information extensions, as per clause 5.5.9.4 of ETSI TS 119 612 [5].
- Embedded within the additionalServiceInformation field of Service information extensions, as per clause 5.5.9.4 of ETSI TS 119 612 [5].

To establish trust in an ERDS based on information in a TL, an actor, which may be another ERDS, shall validate the ERDS's digital signature on an ERD message or ERD evidence, verify that the signing certificate can be linked to the service digital identity in the TL, verify that the service current status is "granted", and verify that the service type identifier is set according to the requirements of the applicable trust domain. If this process is applied to evaluate trust at a time in the past, the process shall use the information (signature validity and service information in the TL) that was valid at that point in time.

7.3 Domain Trusted List

Trusted Lists may be used in other contexts than that governed by Regulation (EU) No 910/2014 [i.1]. A domain TL providing information on ERDSPs/ERDSs shall adhere to the specifications of clause 7.2 above except for the following amended requirements.

The TL shall be formatted according to ETSI TS 119 612 [5].

A Trusted List scheme shall define the conditions that have to me met in order for a trust service provider and its services to be listed. The Trusted List scheme shall be published as required by ETSI TS 119 612 [5], clause 5.3.
A scheme limiting the TL to only contain ERDSPs/ERDSs may be used, or a scheme where ERDSPs/ERDSs are listed along with other types of services.

A Trusted List Scheme Operator shall be assigned and identified as required by ETSI TS 119 612 [5], clause 5.3.

Service type identifiers shall be as specified in clause 7.2, but the Trusted List scheme may restrict allowed service type identifiers to be a subset of those defined. If a service type identifier indicates a qualified ERDS or REM service, then the Trusted List scheme shall unambiguously identify the legislation that the qualified status refers to.

7.4 Domain PKI

In this model, all participating ERDSs will receive X.509 certificates issued within a PKI established as part of the governance of the trust domain. The certificate policy for this PKI should specify the requirements that an ERDS shall fulfil to obtain a certificate and become member of the trust domain.

To establish trust in another ERDS, an ERDS shall verify that the other ERDS has a valid certificate issued within the domain PKI and is in possession of the corresponding private key.

The present document has no further provisions on use of a domain PKI for trust establishment.

7.5 Bilateral trust and other trust models

Trust between ERDSs may be established bilaterally by two or more ERDSs entering into an agreement for exchange of ERD messages and evidences. Such trust establishment is not subject to standardization by the present document.

Bilateral trust establishment will usually involve manual exchange of X.509 certificates between the ERDSs, to ensure that digital signatures on ERD messages and evidence can be validated across ERDSs. Exchange of certificates may also enable encryption of ERD messages and evidence between ERDSs.

It may be possible to extend ERDS metadata published in SMP or otherwise by trust domain information, including publishing of the X.509 certificate representing the ERDS. The present document makes no provisions for standardization for this alternative.

History

Document history			
V1.0.0	May 2018	EN Approval Procedure	AP 20180823: 2018-05-25 to 2018-08-23
V1.1.1	September 2018	Publication	