Draft ETSI EN 319 522-4-3 V0.0.4 (2017-10)

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

STABLE DRAFT FOR PUBLIC REVIEW UNTIL 29 DECEMBER 2017

Download the template for comments:

https://docbox.etsi.org/ESI/Open/Latest_Drafts/Template-for-comments.doc

Send comments ONLY to E-SIGNATURES_COMMENTS@list.etsi.org

0

1

Reference
DEN/ESI-0019522-4-3

Keywords
<keywords>

2

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

Essential patents

IPRs essential or potentially essential to the present document 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 draft European Standard (EN) has been produced by ETSI Technical Committee| ESI and is now submitted for public review before approval by TC ESI and submission for the combined Public Enquiry and Vote phase of the ETSI standards EN Approval Procedure.

The present document is part 4-3 of a multi-part deliverable. Full details of the entire series can be found in [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 provides the binding of the ERD messages, whose semantics is defined in [2] and whose format is defined in [3], to specific transmission protocols.

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

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

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

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

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

3 Definitions and abbreviations

For the purposes of the present document, the definitions and abbreviations given in [1] apply.

4 Common Service Interface bindings – general concepts

This part specifies the binding for the common services to specific protocols. Semantics for common services is defined in EN 319 522 part 2 and formats are defined in EN 319 522 part 3.

Specifically,

- receiver identification service is bound to Service Metadata Locator [4};
- capability discovery service is bound to Service Metadata Publisher [5];
- ERDS trust evaluation is bound to TSL [6].

5 Capability metadata location, BDXSL 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 ERDS metadata. This clause describes use of the OASIS Business Document Metadata Service Location Version 1.0 [4] (BDXSL), commonly used with the OASIS Service Metadata Publishing (SMP) Version 1.0 described in the next clause.

BDXSL is based on DNS (Domain Name Service), which is a common infrastructure for the Internet. From unique identification of the actor, participant identifier in BDXSL 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.

Registration in DNS and forming of query strings shall be done as specified by OASIS BDXSL. This specification does not propose changes or additions to OASIS BDXSL.

BDXSL requires a participant identifier to be registered in BDXSL with one and only one URI to an SMP, i.e. one identity resolves to one SMP. When a recipient subscribes to the services of more than one ERDS using more than one SMP, either:

- The SML registration for the recipient resolves 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 must be amended by a domain, which may be the ERDS name or other information, thereby creating multiple participant identifiers that in BSXSL may resolve to URIs for different SMPs.

Metadata describing the service of an ERDS as described by part 2 of this specification may be located through SML by the same mechanism as recipient metadata. The identity of an ERDS or ERDSP should be registered in BDXSL, i.e. in DNS, by a domain name.

6 Capability metadata publishing, SMP binding

The URI returned from BDXSL points to a metadata repository that shall be in accordance with the specifications in the OASIS Service Metadata Publishing (SMP) Version 1.0 [5].

As stated by SMP [5] 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. XML schemas distributed with the SMP specification in the file bdx-smp-201605.xsd,
2. Use of signatures for signing and verifications as defined in SMP clause 3.6.2,
3. Process execution as defined in SMP clause 2.1,
4. The syntax and semantics defined in the normative portions of SMP clause 3,

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

The SMP specification allows extensions. The use of extensions shall not contradict nor cause non-conformance with the SMP specification. This specification extends SMP by defining ServiceMetadata for an ERDS as a service instance, as opposed to the currently defined SMP ServiceMetadata that maps to the capabilities of a specific ERDS RI, see below.

SMP clause 3.6.2 prescribes use of a specific mode of enveloped XML DSIG [7] for digital signatures.

NOTE: Transition to use of XAdES [8] is recommended but not included in this specification.

In addition to the REST binding defined by SMP, further protocol bindings are possible, but this specification does not specify any other bindings.

SMP 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.

The REST binding comprises two types of resources as defined in SMP clause 3.4:

- SignedServiceMetadata: Holds all of the metadata about a service, or a redirection URL to another SMP holding this information.
- Service group: From the participant identifier of the recipient, a list of references to individual ServiceMetadata resources associated with that participant identifier is returned. If more than one ServiceMetadata resource exists, 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 this specification is the ERD RI to which the ERD message shall be routed. The capabilities of this ERD EI are described by the ServiceMetadata.

This specification extends the SMP data model by metadata for the capabilities of an ERDS as defined in part 2 and 3 of this specification. The capabilities described by this 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.

The extension shall follow the pseudo-schema in clause 2.3.2.2 of SMP:

```
<Extension>
   <ExtensionID>xs:token</ExtensionID>?
   <ExtensionName>xs:string</ExtensionName>?
   <ExtensionAgencyID>xs:string</ExtensionAgencyID>?
   <ExtensionAgencyName>xs:string</ExtensionAgencyName>?
   <ExtensionAgencyURI>xs:anyURI</ExtensionAgencyURI>?
   <ExtensionVersionID>xs:normalizedString</ExtensionVersionID>?
   <ExtensionURI>xs:anyURI</ExtensionURI>?
   <ExtensionReasonCode>xs:token</ExtensionReasonCode>?
   <ExtensionReason>xs:string</ExtensionReason>?
   xs:any
</Extension>
```

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 recognised agreements. Trust may even be established unilaterally, meaning an ERDS trust another ERDS but not the other way around; this is not considered further in this specification.

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 this specification. However, it is noted that a policy may specify policy, security, and technical requirement that each ERDS must 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 the other ERDS (e.g. by use of ERDS metadata) is necessary to determine whether an ERD message can be forwarded to the ERDS.

This specification provides requirements for establishment of trust domains by use of the EU Trusted List system, by use of a domain specific trust status list, and by a domain specific PKI.

7.2 EU TL

One mechanism for establishing trust between two or more (Q)ERDS being compliant with Art. 43/44 of EU Regulation (EU) No 910/2014 is to rely on the EU TL mechanism. If the (Q)ERDS trust service status has been granted, the TSP Service can be listed in the national TL. The following service type identifiers (`tsl:ServiceTypeIdentifier`) URLs are supported for (Q)ERDSP according to TS 119 612:

- http://uri.etsi.org/TrstSvc/Svctype/EDS/Q - A qualified electronic delivery service providing qualified 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 whichever is in force at the time of provision.
- http://uri.etsi.org/TrstSvc/Svctype/EDS - An electronic delivery service, not qualified.
- http://uri.etsi.org/TrstSvc/Svctype/EDS/REM - A Registered Electronic Mail delivery service, not qualified.

A (Q)ERDSP must only use one single certificate for signing messages and evidences, which must be provided in the service digital identity element (`tsl:ServiceDigitalIdentity/tsl:DigitalId`).

Other certificates, e.g. the establishment of trusted communications between different (Q)ERDS, i.e. the relaying of messages and evidences through a ERDS RI interface, shall not be provided in the (Q)ERDS TSP Service part. QERDS shall rely on Qualified Website Authentication Certificates for this.

7.2 Domain TSL

EDITOR NOTE: this part still needs to be developed

7.3 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 must 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.

This specification has no further provisions on use of a domain PKI for trust establishment.

7.4 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 this specification.

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. This specification makes no provisions for standardization for this alternative.

History

Document history		
0.0.1	03/2017	V0.0.1 for ESI comments
0.0.2	06/2017	V0.0.2 for ESI comments
0.0.3	09/2017	V0.0.3 stable draft for ESI
0.0.4	10/2017	V0.0.4 for public review