Draft ETSI EN 319 522-4-1 V0.0.4 (2017-10)

Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services Part 4-1: Message delivery 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-0019522-4-1

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 5
Foreword 5
Modal verbs terminology 5
1 Scope 6
2 References 6
2.1 Normative references 6
3 Definitions and abbreviations 6
4 Message delivery bindings – general concepts 7
5 AS4 binding 7
5.1 Introduction 7
5.2 Generic requirements 7
5.3 Signing and encryption of the AS4 message 8
5.4 Binding of ERD dispatch 9
5.5 Binding of ERDS receipt 9
5.6 Binding of ERDS serviceInfo 9
5.7 Binding of ERD payload 9
6 RFC 5322 binding 9
History 10

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 4-1 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] ETSI TS 119 312 Electronic Signatures and Infrastructures (ESI); Cryptographic Suites

3 Definitions and abbreviations

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

4 Message delivery bindings – general concepts

The present document specifies the bindings of the interface ERDS-RI to specific protocols.

As defined in [319 522-2], the ERDS-RI interface allows for the exchange of ERD messages (ERD dispatch, ERD payload, ERDS receipt, ERDS serviceInfo). Specific formats for these objects are defined in EN319 522-3 [3].

The protocol bindings define the packaging of ERD messages into protocol specific constructs.

The following clauses will define the mapping of the abstract constructs to AS4 and RFC5322.

5 AS4 binding

5.1 Introduction

This clause provides a specification for the exchange of an **ERD message** between two ERDS, i.e. the implementation of the relay operation as defined in part 2, using the AS4 message exchange protocol. This binding specification consists of four clauses for each of the defined constructs in part 2, clause 4 and one clause describing the generic requirements that apply to all bindings.

The configuration of an ebMS V3/AS4 message exchange is done using P-Modes, short for processing modes. A P-Mode, described in section 4 of the ebMS version 3 Core Specification, is a set of parameters each specifying a specific detail of the message exchange, e.g. the identifiers of the sender and receiver and the signing algorithm. When parties are going to set up a message exchange they need to agree on the P-Mode(s) to use.
To facilitate P-Mode creation and improve interoperability between parties, *profiles* can be created to predefine a set of values for certain P-Mode parameters. AS4 itself is already such a profile of the ebMS V3 Core Specification. The next clauses set further constraints on the values of certain P-Mode parameters to ensure interoperability of the message exchange between ERDS and to fulfil requirements put on the relay operation. Together with the meta-data mapping provided in part 3 this creates an “ERDS profile” of AS4.

EDITOR NOTE: dynamic P-Mode support is foreseen. It will be included before final release

5.2 Generic requirements

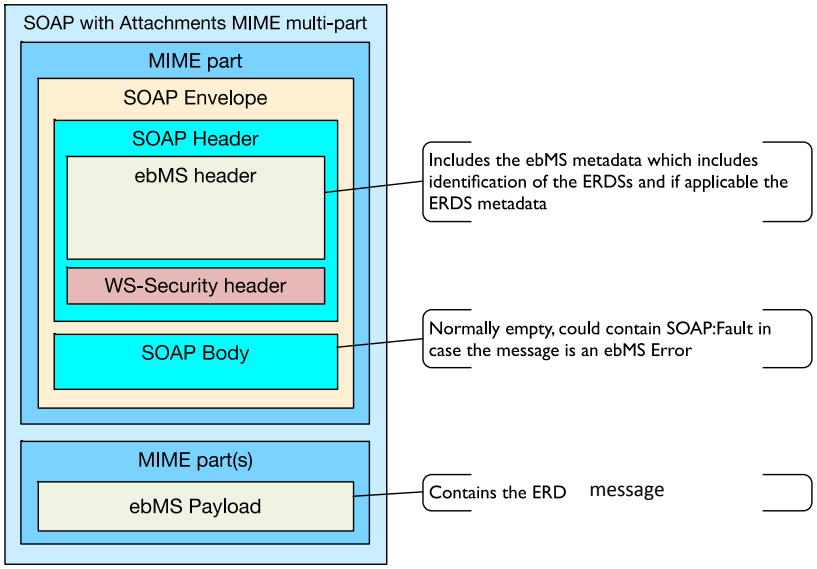
The AS4 specification defines several conformance clauses that define which features a compliant implementation must support. When using AS4 for the implementation of the relay operation ERDS SHALL conform to the *AS4 ebHandler Conformance Clause* and all related features as defined in section 6.1 of AS4. Additionally the following requirements as described in the next paragraphs and clauses apply.

Although the AS4 ebHandler Conformance Clause (that ERDS must support) allows the use of two message exchange patterns, push and pull, for the relay of an **ERD message** ERDS SHALL only use the push message exchange pattern.

The ebMS V3 specification defines two types of messages: User and Signal. The User Messages are used to transport the business data between systems and Signal Messages are to inform systems about events that happen in the message processing. Therefore, **ERD messages** are packaged in User Messages.

AS4 User Messages use a message format based on SOAP with Attachments with a specific SOAP header which contains metadata specific to the AS4 protocol and the. the business data either directly in the SOAP Body or in separate attachments (“ebMS payload”, in the picture). The ebMS header contains references to all ebMS payloads and can also include meta-data on each ebMS payload. The ebMS payloads can be encrypted and the complete AS4 message, i.e. the ebMS header and ebMS payloads can be signed using WS-Security.

ERD messages, with exception of the **ERDS serviceInfo** which are mapped to ebMS *Message Properties* as specified in part 3, shall be included as ebMS payloads that are packaged as SOAP attachments, i.e. the SOAP Body shall not be used. The AS4 Compression Feature as defined in section 3.1 of the AS4 Profile and which offers the option to compress payloads packaged in the SOAP attachments shall not be used by the ERDS.



The PMode.Initiator and PMode.Responder parameters shall include the identifiers of the sending respectively receiving ERDS. Both the PMode.Initiator.Role and PMode.Responder.Role shall contain the value http://uri.etsi.org/19522/as4binding/v1#Role#ERDS.

PMode[1].BusinessInfo.Service shall be set to http://uri.etsi.org/19522/as4binding/v1#Relay. The Service type shall not be used.

Receipts shall be used to indicate the AS4 message was successfully be sent by the receiving ERDS and the ERD Dispatch is ready for further processing. Note that this only indicates that the exchange of the ERD Dispatch was successful but provides no information on the actual delivery of the ERD payload and/or evidence to the final recipient. Both the Receipt and Error Signal messages shall be sent back synchronously to the sending ERDS.

It is recommended that the AS4 Reception Awareness Feature as specified in section 3.2 of the AS4 specification is used. ERDS should use the duplicate elimination function to prevent redundant delivery of the same message to the user application. Note however that using duplicate elimination on the AS4 exchange does not guarantee that the same ERD Message is only delivered once to the user application as the same message may be submitted multiple times by the sending user application (resulting in multiple AS4 messages).

5.3 Signing and encryption of the AS4 message

The AS4 message shall be signed and encrypted by the sending ERDS. The following table shows the settings to be used for signing and encryption of the AS4 message. As the P-Mode parameters use the algorithms identifiers from XML Signature Syntax and Processing and XML Encryption Syntax and Processing specifications these are also provided.

Function	P-Mode parameter(s)	Algorithm specification
Signing and encryption key hash function	PMode[1].Security.Signature.HashFunction PMode[1].Security.Encryption.KeyTransportAlgorithmParameters	Hash function as specified in ETSI TS 119 312 [4]
Certificate reference method	PMode[1].Security.Signature.X509TokenReferenceType PMode[1].Security.Encryption.X509TokenReferenceType	It is recommended to use the *Binary Security Token reference*. If the *Binary Security Token reference* is used it shall reference a security token of type *X509v3* (i.e. include only the certificate and no chain).

Signing algorithm	PMode[1].Security.Signature.Algorithm	Security signature algorithm as specified in ETSI TS 119 312 [4]
Encryption algorithm	PMode[1].Security.Encryption.Algorithm	Security encryption algorithm as specified in ETSI TS 119 312 [4]
Encryption key transport algorithm	PMode[1].Security.Encryption. KeyTransportAlgorithmParameters	as specified in ETSI TS 119 312 [4]
Encryption key mask algorithm	PMode[1].Security.Encryption. KeyMaskAlgorithmParameters	as specified in ETSI TS 119 312 [4]

5.4 Binding of ERD dispatch

When relaying an ERD dispatch using AS4 the sending ERDS shall use to *http://uri.etsi.org/19522/as4binding/v1#Actions/ERDdispatch* as value for PMode[1].Action.

The message shall include one or more payloads containing the user content including possible attachments and one or more containing the ERDS evidence(s).

5.5 Binding of ERDS receipt

The specific case where evidence and identification information (ERDS receipt) flow independently is taken into account in [319 522-4-2], clause 5.3.

5.6 Binding of ERDS serviceInfo

When relaying an ERDS serviceInfo using AS4 the sending ERDS shall use to *http://uri.etsi.org/19522/as4binding/v1#Actions/ERDserviceInfo* as value for PMode[1].Action.

The message shall not contain any payloads.

5.7 Binding of ERD payload

When relaying an ERD payload using AS4 the sending ERDS shall use to *http://uri.etsi.org/19522/as4binding/v1#Actions/ERDpayload* as value for PMode[1].Action.

The message shall include one or more payloads containing the user content including possible attachments.

6 RFC 5322 binding

This binding is provided in EN 319 532-3 [3].

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