Electronic Signatures and Infrastructures (ESI);
Electronic Registered Delivery Services;
Part 4: Bindings;
Sub-part 1: Message delivery bindings
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 Message delivery bindings - general concepts.................................................................................6

5 AS4 binding.........................................................................................................................................6
5.1 Introduction ...................................................................................................................................6
5.2 Generic requirements ....................................................................................................................7
5.3 Signing and encryption of the AS4 message ....................................................................................7
5.4 Binding of ERD dispatch .............................................................................................................8
5.5 Binding of ERDS receipt ...............................................................................................................8
5.6 Binding of ERDS serviceInfo ....................................................................................................8
5.7 Binding of ERD payload ..............................................................................................................8

6 IETF RFC 5322 binding......................................................................................................................9

History..................................................................................................................................................10
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 1 of a multi-part deliverable. Full details of the entire series can be found in part 1 [i.3].

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

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 defines the binding of the ERD messages, 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 transmission protocol AS4 [4].

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] ETSI TS 119 312: "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites".
[6] 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".
[7] ETSI EN 319 532-3: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) Services; Part 3: Formats".

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] IETF RFC 5322: "Internet Message Format".
[i.3] ETSI EN 319 522-1: "Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 1: Framework and Architecture".
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.3] apply.

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI EN 319 522-1 [i.3] apply.

4 Message delivery bindings - general concepts

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

The bindings shall support the exchange of ERD messages (ERD dispatch, ERD payload, ERDS receipt, ERDS serviceInfo) through the ERDS-RI interface as defined in ETSI EN 319 522-2 [1]. Specific formats for these objects defined in ETSI EN 319 522-3 [2] shall be supported.

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

Clause 5 defines the mapping of the abstract constructs to AS4 [4]. Clause 6 points to a different document which defines the binding to IETF RFC 5322 [i.1].

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 ETSI EN 319 522-2 [1], using the AS4 message exchange protocol [4]. This binding specification consists of four clauses for each of the defined constructs in ETSI EN 319 522-2 [1], clause 4 and one clause describing the generic requirements that apply to all bindings.

The configuration of an ebMS V3/AS4 [4] 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 [i.4], 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 predefined a set of values for certain P-Mode parameters. The next clauses define such a profile by defining constraints on and defaults for the values of certain P-Mode parameters to ensure interoperability of the message exchange between ERDS and to fulfill requirements put on the relay operation. Together with the meta-data mapping provided in ETSI EN 319 522-3 [2] this creates an "ERDS profile" of AS4.

NOTE: The present document does not prescribe how the actual P-Modes used in an ERDS are created, this is left to the implementations. Depending on the environment, e.g. the number of ERDS in a network and the volatility of changes, either statically or dynamically configured P-Modes may be used. For dynamic configuration the capability lookup mechanism of CSI (e.g. may be used to find the target ERDS and get the relevant meta-data for setting the P-Mode parameters).
5.2 Generic requirements

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 [4]. Additionally the following requirements as described in the next paragraphs and clauses apply.

Although the AS4 ebHandler Conformance Clause 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.

ERD messages shall be packaged in User Messages. The user content, ERDS relay meta-data and ERDS evidence 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 [4] and which offers the option to compress payloads packaged in the SOAP attachments should not be used by the ERDS so the digest included in the signature of the AS4 message is calculated over the unmodified user content. If compression is needed ERDS may use the HTTP gzip transfer-encoding.

Each payload contained in the AS4 message shall have a part property, i.e. a //PartInfo/Property element shall be included in the message header that indicates the object type of the payload. The name of the property shall be http://uri.etsi.org/19522/v1#as4binding/PayloadType and the value shall be set according to table 1.

<table>
<thead>
<tr>
<th>Object type</th>
<th>Value for part property</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Content</td>
<td>UserContent</td>
</tr>
<tr>
<td>ERDS Relay metadata</td>
<td>ERDSRelayMetadata</td>
</tr>
<tr>
<td>ERDS Evidence</td>
<td>ERDSEvidence</td>
</tr>
</tbody>
</table>

Since the ERDS Relay metadata is always included the AS4 message shall always include at least one payload containing the XML representation of the metadata as specified in clause 4 of ETSI EN 319 522-3 [2].

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

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

Signed Receipts shall be used to indicate the AS4 message was successfully sent by the receiving ERDS and the ERD message is ready for further processing, i.e. both PMode[1].Security.SendReceipt shall PMode[1].Security.SendReceipt.NonRepudiation have value true.

NOTE 1: This only indicates that the exchange of the ERD message was successful but provides no information on the actual consignment/handover of the user content to the final recipient.

Both the Receipt and Error Signal messages shall be sent back synchronously to the sending ERDS, i.e. PMode[1].Security.SendReceipt.ReplyPattern and PMode[1].ErrorHandling.Report.AsResponse shall have value true.

The AS4 Reception Awareness Feature as specified in section 3.2 of the AS4 specification [4] should be used. ERDS should use the duplicate elimination function to prevent redundant delivery of the same message to the user application.

NOTE 2: 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

All AS4 messages exchanged between the ERDS shall be signed and encrypted by the sending ERDS. Table 2 shows the settings that shall be used for signing and encryption of the AS4 message. As AS4 uses XML Encryption Syntax and Processing [5] for message encryption the algorithms identifiers from this specification are used in table 2.
Table 2: Signing and encryption parameters

<table>
<thead>
<tr>
<th>Function</th>
<th>P-Mode parameter(s)</th>
<th>Algorithm specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate reference method</td>
<td>PMode[1].Security.Signature.X509TokenReferenceTypePMode[1].Security.Encryption.X509TokenReferenceType</td>
<td>The Binary Security Token reference as specified in the WS-Security X.509 Certificate Profile [i.2] should be used. If the Binary Security Token reference is used it shall reference a security token of type X509v3 (i.e. include only the certificate used for signing and no chain)</td>
</tr>
<tr>
<td>Encryption key mask algorithm</td>
<td>PMode[1].Security.Encryption.KeyMaskAlgorithmParameters</td>
<td>MGF1 with SHA256 shall be used: <a href="http://www.w3.org/2009/xmlenc11#mgf1sha256">http://www.w3.org/2009/xmlenc11#mgf1sha256</a></td>
</tr>
</tbody>
</table>

5.4 Binding of ERD dispatch

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

For each element //UserContentInfo//PartInfo in the ERDS relay metadata XML document there shall be a payload in the AS4 message. Beside the part property specified in clause 5.2 that indicates the object type there shall be a part property named http://uri.etsi.org/19522/v1/#as4binding/UserContentPartId and with value the identifier contained in the //UserContentInfo//PartInfo/Identifier element in the metadata.

Furthermore the message may include one or more payloads containing ERDS evidence(s). For each of these payloads the AS4 message header should contain a part property named http://uri.etsi.org/19522/v1/#as4binding/PayloadType with value ERDSEvidence.

5.5 Binding of ERDS receipt

The specific case where evidence and identification information (ERDS receipt) flow independently shall be as specified in ETSI EN 319 522-4-2 [6], clause 5.3.

5.6 Binding of ERDS serviceInfo

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

Beside the payload carrying the ERDS relay metadata the message shall not contain any further payloads.

5.7 Binding of ERD payload

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

For each element //UserContentInfo//PartInfo in the metadata XML document there shall be a payload in the AS4 message that has the two part properties: one named http://uri.etsi.org/19522/v1/#as4binding/PayloadType with value UserContentPart and one named http://uri.etsi.org/19522/v1/#as4binding/UserContentPartId and with value the identifier contained in the //UserContentInfo//PartInfo/Identifier element in the metadata.
Beside the payloads specified above and the one containing the ERDS Relay metadata there shall be no further payloads included in the message.

6 IETF RFC 5322 binding

This binding shall be implemented as defined in ETSI EN 319 532-3 [7].
### History

#### Document history

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Category</th>
<th>Date Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>V1.0.0</td>
<td>May 2018</td>
<td>EN Approval Procedure</td>
<td>AP 20180823: 2018-05-25 to 2018-08-23</td>
</tr>
<tr>
<td>V1.1.1</td>
<td>September 2018</td>
<td>Publication</td>
<td></td>
</tr>
</tbody>
</table>