



## **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](https://docbox.etsi.org/ESI/Open/Latest%20Drafts/Template-for-comments.doc)**

**Send comments ONLY to [E-SIGNATURES\\_COMMENTS@list.etsi.org](mailto:E-SIGNATURES_COMMENTS@list.etsi.org)**

**CAUTION: This DRAFT document is provided for information and is for future development work within the ETSI Technical Committee ESI only. ETSI and its Members accept no liability for any further use/implementation of this Specification.**

**Approved and published specifications and reports shall be obtained exclusively via the ETSI Documentation Service at**

**<http://www.etsi.org/standards-search>**

0  
1

---

**Reference**

DEN/ESI-0019522-4-1

---

**Keywords**

&lt;keywords&gt;

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

---

**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>

---

**Copyright Notification**

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.  
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2017.  
All rights reserved.

**DECT™**, **PLUGTESTS™**, **UMTS™** and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.  
**3GPP™** and **LTE™** are Trade Marks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.  
**GSM®** and the GSM logo are Trade Marks registered and owned by the GSM Association.

3  
4  
5  
6

Reproduction is only permitted for the purpose of standardization work undertaken within ETSI.  
The copyright and the foregoing restriction extend to reproduction in all media.

---

7	<b>Contents</b>	
8	.	
9	Intellectual Property Rights .....	5
10	Foreword.....	5
11	Modal verbs terminology .....	5
12	1 Scope .....	6
13	2 References .....	6
14	2.1 Normative references .....	6
15	3 Definitions and abbreviations.....	6
16	4 Message delivery bindings – general concepts .....	7
17	5 AS4 binding .....	7
18	5.1 Introduction.....	7
19	5.2 Generic requirements .....	7
20	5.3 Signing and encryption of the AS4 message .....	8
21	5.4 Binding of ERD dispatch .....	9
22	5.5 Binding of ERDS receipt .....	9
23	5.6 Binding of ERDS serviceInfo .....	9
24	5.7 Binding of ERD payload.....	9
25	6 RFC 5322 binding .....	9
26	History .....	10
27		
28		

29

30

---

## 31 Intellectual Property Rights

### 32 Essential patents

33 IPRs essential or potentially essential to the present document may have been declared to ETSI. The information  
 34 pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found  
 35 in ETSI SR 000 314: "*Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in*  
 36 *respect of ETSI standards*", which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web  
 37 server (<https://ipr.etsi.org>).

38 Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee  
 39 can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web  
 40 server) which are, or may be, or may become, essential to the present document.

### 41 Trademarks

42 The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners.  
 43 ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no  
 44 right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does  
 45 not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

---

## 46 Foreword

47 This draft European Standard (EN) has been produced by ETSI Technical Committee ESI and is now submitted for  
 48 public review before approval by TC ESI and submission for the combined Public Enquiry and Vote phase of the ETSI  
 49 standards EN Approval Procedure.

50 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

51

---

## 52 Modal verbs terminology

53 In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and  
 54 "**cannot**" are to be interpreted as described in clause 3.2 of the [ETSI Drafting Rules](#) (Verbal forms for the expression of  
 55 provisions).

56 "**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

57

---

## 58 1 Scope

59 The present document provides the binding of the ERD messages, whose semantics is defined in [2] and whose format  
60 is defined in [3], to specific transmission protocols.

---

## 61 2 References

### 62 2.1 Normative references

63 References are either specific (identified by date of publication and/or edition number or version number) or  
64 non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the  
65 referenced document (including any amendments) applies.

66 Referenced documents which are not found to be publicly available in the expected location might be found at  
67 <https://docbox.etsi.org/Reference/>.

68 NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee  
69 their long term validity.

70 The following referenced documents are necessary for the application of the present document.

- 71 [1] ETSI EN 319 522-1: " Electronic Signatures and Infrastructures (ESI); Electronic Registered  
72 Delivery Services; Part 1: Framework and Architecture".
- 73 [2] ETSI EN 319 522-2: " Electronic Signatures and Infrastructures (ESI); Electronic Registered  
74 Delivery Services; Part 2: Semantic Contents".
- 75 [3] ETSI EN 319 522-3: " Electronic Signatures and Infrastructures (ESI); Electronic Registered  
76 Delivery Services; Part 3: Formats".
- 77 [4] ETSI TS 119 312 Electronic Signatures and Infrastructures (ESI); Cryptographic Suites

78

79

---

## 80 3 Definitions and abbreviations

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

82

83

84

85

---

## 86 4 Message delivery bindings – general concepts

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

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

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

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

92

---

## 93 5 AS4 binding

### 94 5.1 Introduction

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

99 The configuration of an ebMS V3/AS4 message exchange is done using P-Modes, short for processing modes. A P-  
100 Mode, described in section 4 of the ebMS version 3 Core Specification, is a set of parameters each specifying a specific  
101 detail of the message exchange, e.g. the identifiers of the sender and receiver and the signing algorithm. When parties  
102 are going to set up a message exchange they need to agree on the P-Mode(s) to use.

103 To facilitate P-Mode creation and improve interoperability between parties, *profiles* can be created to predefine a set of  
104 values for certain P-Mode parameters. AS4 itself is already such a profile of the ebMS V3 Core Specification. The next  
105 clauses set further constraints on the values of certain P-Mode parameters to ensure interoperability of the message  
106 exchange between ERDS and to fulfil requirements put on the relay operation. Together with the meta-data mapping  
107 provided in part 3 this creates an “ERDS profile” of AS4.

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

109

### 110 5.2 Generic requirements

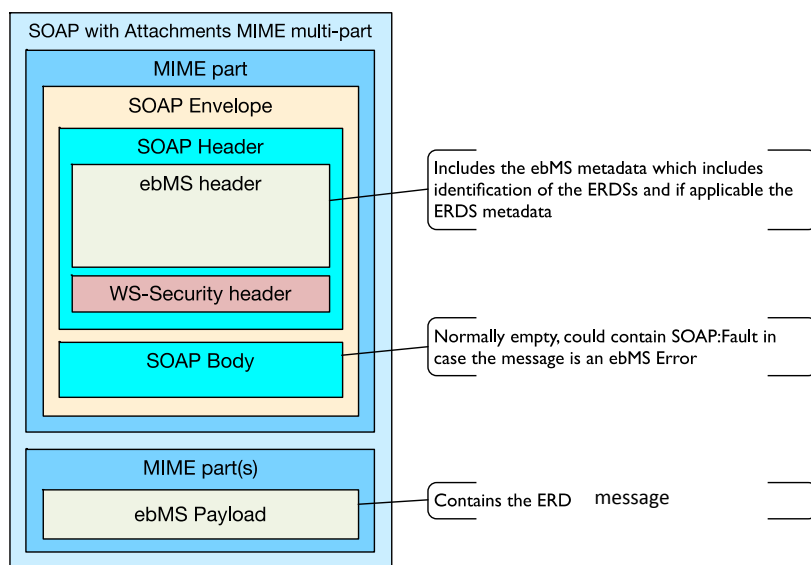
111 The AS4 specification defines several conformance clauses that define which features a compliant implementation must  
112 support. When using AS4 for the implementation of the relay operation ERDS SHALL conform to the *AS4 ebHandler*  
113 *Conformance Clause* and all related features as defined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

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

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

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

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



129

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

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

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

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

### 144 5.3 Signing and encryption of the AS4 message

145 The AS4 message shall be signed and encrypted by the sending ERDS. The following table shows the settings to be  
 146 used for signing and encryption of the AS4 message. As the P-Mode parameters use the algorithms identifiers from  
 147 XML Signature Syntax and Processing and XML Encryption Syntax and Processing specifications these are also  
 148 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 <i>Binary Security Token reference</i> .  If the <i>Binary Security Token reference</i> is used it shall reference a security token of type <i>X509v3</i> (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]

149

## 150 5.4 Binding of ERD dispatch

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

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

## 155 5.5 Binding of ERDS receipt

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

## 158 5.6 Binding of ERDS serviceInfo

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

161 The message shall not contain any payloads.

## 162 5.7 Binding of ERD payload

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

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

166

---

## 167 6 RFC 5322 binding

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

169

170

171

172

173

174

175

176  
177  
178

179

---

## History

<b>Document history</b>		
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

180