



1

## ENTSOG AS4 Profile

2

**Draft Version 3.6 – 2018-03-27**

3

### **Disclaimer**

4 **This document provides only specific technical information given for indicative purposes**  
5 **and, as such, it can be subject to further modifications. The information contained in the**  
6 **document is non-exhaustive as well as non-contractual in nature and closely connected**  
7 **with the completion of the applicable process foreseen by the relevant provisions of**  
8 **Commission Regulation (EU) 2015/703 of 30 April 2015 establishing a network code on**  
9 **interoperability and data exchange rules.**

10 **No warranty is given by ENTSOG in respect of any information so provided, including its**  
11 **further modifications. ENTSOG shall not be liable for any costs, damages and/or other**  
12 **losses that are suffered or incurred by any third party in consequence of any use of -or**  
13 **reliance on- the information hereby provided.**

<b>Table of contents</b>	
14	
15	1 Introduction..... 5
16	2 AS4 Profile ..... 6
17	2.1 AS4 and Conformance Profiles..... 6
18	2.1.1 AS4 Standard ..... 6
19	2.1.2 AS4 ebHandler Conformance Profile ..... 6
20	2.2 ENTSOG AS4 ebHandler Feature Set..... 6
21	2.2.1 Messaging Model ..... 7
22	2.2.2 Message Pulling and Partitioning..... 8
23	2.2.3 Message Packaging ..... 9
24	2.2.3.1 UserMessage..... 10
25	2.2.3.2 Payloads ..... 10
26	2.2.3.3 Message Compression ..... 10
27	2.2.4 Error Handling ..... 10
28	2.2.5 Reliable Messaging and Reception Awareness ..... 11
29	2.2.6 Security..... 11
30	2.2.6.1 Transport Layer Security ..... 12
31	2.2.6.2 Message Layer Security..... 13
32	2.2.7 Networking..... 14
33	2.2.8 Configuration Management ..... 15
34	2.3 Usage Profile ..... 15
35	2.3.1 Message Packaging ..... 15
36	2.3.1.1 Party Identification ..... 15
37	2.3.1.2 Business Process Alignment..... 16
38	2.3.1.2.1 Service ..... 16
39	2.3.1.2.2 Action..... 17
40	2.3.1.2.3 Role ..... 18
41	2.3.1.2.4 ENTSOG AS4 Mapping Table ..... 19
42	2.3.1.3 Message Correlation ..... 19
43	2.3.2 Agreements ..... 20
44	2.3.3 MPC ..... 21

45	2.3.4	Security.....	21
46	2.3.4.1	Network Layer Security.....	21
47	2.3.4.2	Transport Layer Security.....	22
48	2.3.4.3	Message Layer Security.....	22
49	2.3.4.4	Certificates and Public Key Infrastructure.....	22
50	2.3.4.5	Certificate Profile.....	24
51	2.3.4.5.1	Key Size.....	24
52	2.3.4.5.2	Key Algorithm.....	24
53	2.3.4.5.3	Naming.....	24
54	2.3.4.5.4	Certificate Body.....	25
55	2.3.4.5.5	Extensions for Signing, Encryption and TLS End Entities.....	26
56	2.3.4.5.6	Extended Key Usage.....	27
57	2.3.4.5.7	Certificate Lifetime.....	27
58	2.3.5	Networking.....	27
59	2.3.6	Message Payload and Flow Profile.....	28
60	2.3.7	Test Service.....	29
61	2.3.8	Environments.....	29
62	2.4	ebCore Agreement Update.....	30
63	2.4.1	Mandatory Support.....	30
64	2.4.2	Implementation Guidelines.....	30
65	3	Examples.....	31
66	3.1	Message with EDIG@S Payload.....	31
67	3.2	Alternative Using Defaults.....	33
68	4	Processing Modes.....	33
69	5	Revision History.....	38
70	6	References.....	48
71			

## 72 **1 Introduction**

73 COMMISSION REGULATION (EU) 2015/703 of 30 April 2015 establishing a network code on  
74 interoperability and data exchange rules published on 30 April 2015 by the European  
75 Commission (EC) specifies that *“The following common data exchange solutions shall be used*  
76 *[for the communication] protocol: AS4”* [CR2015/703] for document-based exchanges. This  
77 document defines an ENTSOG AS4 Profile that aims to support cross-enterprise collaboration  
78 in the gas sector using secure and reliable exchange of business documents based on the  
79 AS4 standard [AS4]. This is done by providing an ENTSOG AS4 ebHandler profile and a usage  
80 profile for the AS4 communication protocol that allow actors in the gas sector to deploy AS4  
81 communication platforms in a consistent and interoperable way. This document also  
82 specifies a mechanism to manage certificate exchanges and updates for AS4 using ebCore  
83 Agreement Update [AU].

84 The main goals of this profile are to:

- 85 • Support exchange of EDIG@S XML documents and other payloads.
- 86 • Support business processes of Transmission System Operators for gas, such as  
87 Capacity Allocation Mechanism [CAM] and Nomination [NOM], as well as future  
88 business processes.
- 89 • Leverage experience gained with other B2B protocols in the gas sector, such as AS2  
90 as described in the EASEE-gas implementation guide [EGMTP].
- 91 • Provide security guidance based on state-of-the-art best practices, following  
92 recommendations for “near term” (defined as “at least ten years”) future system use  
93 [ENISA13,ENISA14].
- 94 • Provide suppliers of AS4-enabled B2B communication solutions with guidance  
95 regarding the required AS4 functionality.
- 96 • Facilitate management and exchange of certificates for AS4 by users deploying the  
97 profile.

98 This profile adopts document conventions common in technical specifications for Internet  
99 protocols and data formats. The key words "MUST", "MUST NOT", "REQUIRED", "SHALL",  
100 "SHALL", "NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in  
101 this document are to be interpreted as described in [RFC2119].

## 102 **2 AS4 Profile**

103 This specification defines the ENTSOG AS4 profile as the selection of a specific conformance  
104 profile of the AS4 standard [AS4], which is profiled further for increased consistency and  
105 ease of configuration, and an AS4 Usage Profile that defines how to use a compliant  
106 implementation for gas industry document exchange. Section 2.1 describes the AS4  
107 ebHandler Conformance Profile, of which this profile is an extended subset. Section 2.2  
108 describes the feature set that conformant products are REQUIRED to support. Section 2.3 is  
109 a usage guide that describes configuration and deployment options for conformant  
110 products. Section 2.4 describes how certificates for use with AS4 configurations for this  
111 profile can be exchanged and managed using ebCore Agreement Update [AU].

### 112 **2.1 AS4 and Conformance Profiles**

#### 113 **2.1.1 AS4 Standard**

114 This ENTSOG AS4 profile is based on the AS4 Profile of ebMS 3.0 Version 1.0. OASIS Standard  
115 [AS4]. AS4 itself is based on other standards, in particular on OASIS ebXML Messaging  
116 Services Version 3.0: Part 1, Core Features OASIS Standard [EBMS3], which in turn is based  
117 on various Web Services specifications.

118 The OASIS Technical Committee responsible for maintaining the AS4, ebMS 3.0 Core and  
119 other related specifications is tracking and resolving issues in the specifications, which it  
120 intends to publish as a consolidated Specification Errata. Implementations of the ENTSOG  
121 AS4 Profile SHOULD track and implement resolutions at [https://tools.oasis-](https://tools.oasis-open.org/issues/browse/EBXMLMSG)  
122 [open.org/issues/browse/EBXMLMSG](https://tools.oasis-open.org/issues/browse/EBXMLMSG).

#### 123 **2.1.2 AS4 ebHandler Conformance Profile**

124 The AS4 standard [AS4] defines multiple conformance profiles, which define specific  
125 functional subsets of the version 3.0 ebXML Messaging, Core Specification [EBMS3]. A  
126 conformance profile corresponds to a class of compliant applications. This version of the  
127 ENTSOG AS4 Profile is based on an extended subset of the **AS4 ebHandler Conformance**  
128 **Profile** and a Usage Profile. It aims to support business processes such as Capacity Allocation  
129 Mechanism [CAM] and Nomination [NOM], in which documents are to be transmitted  
130 securely and reliably to Receivers with a minimal delay.

### 131 **2.2 ENTSOG AS4 ebHandler Feature Set**

132 The ENTSOG AS4 feature set is, with some exceptions, a subset of the feature set of the AS4  
133 ebHandler Conformance Profile. This section selects specific options in situations where the  
134 AS4 ebHandler provides more than one option. This section is addressed to providers of AS4  
135 products and can be used as a checklist of features to be provided in AS4 products. The  
136 structure of this chapter mirrors the structure of the ebMS3 Core Specification [EBMS3].

137 Compared to the AS4 ebHandler Conformance Profile, this profile adds, or updates, some  
138 functionality:

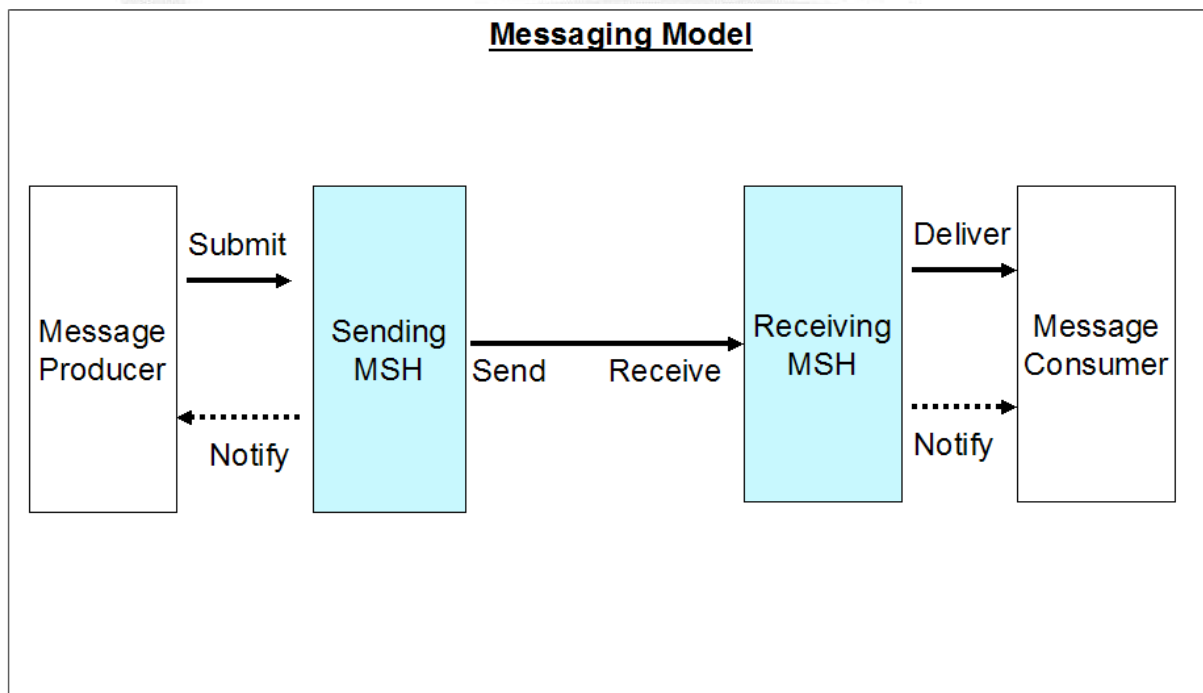
- 139 • There is an added recommendation to support the Two Way Message Exchange  
140 Pattern (MEP) (cf. section 2.2.1).
- 141 • Transport Layer Security processing, if handled in the AS4 handler, is profiled (cf.  
142 section 2.2.6.1).
- 143 • Algorithms specified for securing messages at the Message Layer are updated to  
144 current guidelines (cf. section 2.2.6.2).

145 It also relaxes some requirements:

- 146 • Support for **Pull** mode in AS4 will only be REQUIRED when business processes  
147 determine that **Pull** mode exchanges are necessary (cf. section 2.2.2).
- 148 • All payloads are exchanged in separate MIME parts (cf. section 2.2.3.2).
- 149 • Asynchronous reporting of receipts and errors is not REQUIRED (cf. sections 2.2.4,  
150 2.2.5).
- 151 • WS-Security support is limited to the X.509 Token Profile (cf. section 2.2.6.2).

## 152 2.2.1 Messaging Model

153 This profile constrains the channel bindings of message exchanges between two AS4  
154 Message Service Handlers (MSHs), one of which acts as Sending MSH and the other as the  
155 Receiving MSH. The following diagram (from [EBMS3]) shows the various actors and  
156 operations in message exchange:



157  
158 **Figure 1 AS4 Messaging Model**

159 Business applications or middleware, acting as *Producer*, *Submit* message content and  
160 metadata to the Sending MSH, which packages this content and sends it to the Receiving  
161 MSH of the business partner, which in turn *Delivers* the message to another business  
162 application that *Consumes* the message content and metadata. Subject to configuration,  
163 Sending and Receiving MSH may *Notify Producer* or *Consumer* of particular events. Note that  
164 there is a difference between *Sender* and *Initiator*. For **Push** exchanges, the Sending MSH  
165 initiates the transmission of the message. For **Pull** exchanges, the transmission is initiated by  
166 the Receiving MSH.

167 The AS4 ebHandler Conformance Profile is the AS4 conformance profile that provides  
168 support for Sending and Receiving roles using **Push** channel bindings. Support is REQUIRED  
169 for the following Message Exchange Pattern:

- 170 • *One Way / Push*

171 For **PMode.MEP**, support is therefore REQUIRED for the following values:

- 172 • <http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/oneWay>

173 While the AS4 ebHandler does not require support for the Two-Way MEP, support for this  
174 MEP may be added in future versions of this ENTSSOG AS4 profile (see section 2.3.1.3). A  
175 message handler that supports Two Way MEPs allows the Producer submitting a message  
176 unit to set the optional *RefToMessageId* element in the *MessageInfo* section in support of  
177 request-response exchanges. For **PMode.MEP**, support is therefore RECOMMENDED for the  
178 following value:

- 179 • <http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/twoWay>

180 For **PMode.MEPbinding**, support is REQUIRED for:

- 181 • <http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/push>

182 Note that these values are identifiers only and do not resolve to content on the OASIS site.

## 183 2.2.2 Message Pulling and Partitioning

184 Business processes currently under consideration for this version of this profile are time-  
185 critical and considered only supported by the **Push** channel binding, because it allows the  
186 *Sender* to control the timing of transmission of the message. Future versions of this profile  
187 MAY also support business processes with less time-critical timing requirements. These  
188 future uses could benefit from the ebMS3 **Pull** feature. For **PMode.MEPbinding**, applications  
189 SHOULD therefore also support:

- 190 • <http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/pull>

191 This allows implementations of this profile to also support the following Message Exchange  
192 Patterns:

- 193 • *One Way / Pull*
- 194 • *Two Way / Push-and-Pull*

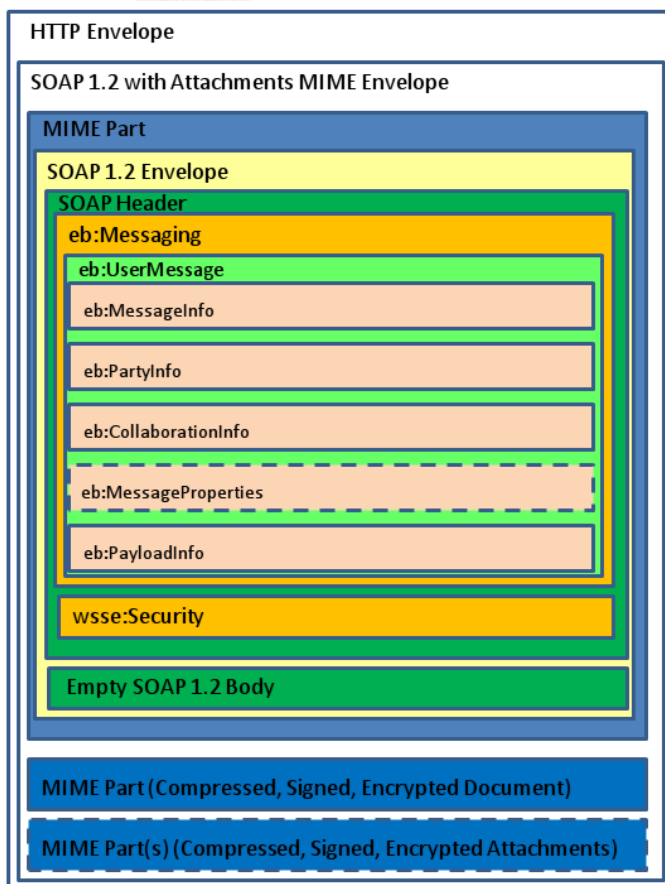


- 195 • *Two Way / Pull-and-Push*
- 196 • *Two Way / Pull-and-Pull*

197 Note that any compliant AS4 ebHandler is REQUIRED to support the first of these options.  
198 That requirement is relaxed in this profile. The other three options combine Two Way  
199 exchanges (see section 2.2.1) with the **Pull** feature.

### 200 2.2.3 Message Packaging

201 The AS4 message structure (see Figure 2) provides a standard message header that  
202 addresses B2B requirements and offers a flexible packaging mechanism based on SOAP and  
203 MIME enveloping. Dashed line style is used for optional message components.



204  
205 **Figure 2 AS4 Message Structure**

206 The SOAP envelope SHOULD be encoded as UTF-8 (see [EBMS3], section 5.1.2.5). If the SOAP  
207 envelope is correctly encoded in UTF-8 and the character set header is set to UTF-8,  
208 receivers MUST support the presence of the Unicode Byte Order Mark (BOM; see [BP20],  
209 section 3.1.2).

### 210 2.2.3.1 UserMessage

211 AS4 defines the ebMS3 **Messaging** SOAP header, which envelopes **UserMessage** XML  
212 structures, which provide business metadata to exchanged payloads. In AS4, ebMS3  
213 messages other than receipts or errors carry a single **UserMessage**. The ENTSOG AS4 profile  
214 follows the AS4 ebHandler Conformance Profile in requiring full configurability for “General”  
215 and “BusinessInfo” P-Mode parameters as per sections 2.1.3.1 and 2.1.3.3 of [AS4].

216 A compliant product MUST allow the Producer, when submitting messages, to set a value for  
217 **AgreementRef**, to select a particular P-Mode. A compliant product, acting as Receiver, MUST  
218 take the value of the AS4 **AgreementRef** header into account when selecting the applicable  
219 P-Mode. It MUST be able to send and receive messages in which the optional *pmode*  
220 attribute of **AgreementRef** is not set.

221 The ebMS3 and AS4 specifications do not constrain the value of **MessageId** beyond  
222 conformance to the Internet Message Format [RFC2822], which requires the value to be  
223 unique. Products can do this by including a UUID string in the *id-left* part of the identifier set  
224 using randomly (or pseudo-randomly) chosen values.

225 As in the AS4 ebHandler profile, support for **MessageProperties** is REQUIRED in this profile.

### 226 2.2.3.2 Payloads

227 Section 5.1.1 of the ebMS3 Core Specification [EBMS3] requires implementations to process  
228 both non-multipart (simple SOAP) messages and multipart (SOAP-with-attachments)  
229 messages, and this is a requirement for the AS4 ebHandler Conformance Profile. Due to the  
230 mandatory use of the AS4 compression feature in this profile (see section 2.2.3.3), XML  
231 payloads MAY be converted to binary data, which is carried in separate MIME parts and not  
232 in the SOAP Body. AS4 messages based on this profile always have an empty SOAP Body.

233 The ebMS3 mechanism of supporting “external” payloads via hyperlink references (as  
234 mentioned in section 5.2.2.12 of [EBMS3]) MUST NOT be used.

### 235 2.2.3.3 Message Compression

236 The AS4 specification defines payload compression as one of its additional features. Payload  
237 compression is a useful feature for many content types, including XML content.

- 238 • The parameter **PMode[1].PayloadService.CompressionType** MUST be set to the  
239 value *application/gzip*. (Note that GZIP is the only compression type currently  
240 supported in AS4).

241 Mandatory use of the AS4 compression feature is consistent with current practices for gas  
242 B2B data exchange, such as the EASEE-gas AS2 profile [EGMTP]. Compressed payloads are in  
243 separate MIME parts.

### 244 2.2.4 Error Handling

245 This profile specifies that errors MUST be reported and transmitted synchronously to the  
246 Sender and SHOULD be reported to the Consumer.

- 247
- The parameter **PMode[1].ErrorHandling.Report.AsResponse** MUST be set to the value *true*.
- 248
- 249
- The parameter **PMode[1].ErrorHandling.Report.ProcessErrorNotifyConsumer**
- 250
- SHOULD be set to the value *true*.

## 251 2.2.5 Reliable Messaging and Reception Awareness

252 This profile specifies that non-repudiation receipts MUST be sent synchronously for each  
253 message type.

- 254
- The parameter **PMode[1].Security.SendReceipt.NonRepudiation** MUST be set to the value *true*.
- 255
- 256
- The parameter **PMode[1].Security.SendReceipt.ReplyPattern** MUST be set to the value *Response*.
- 257

258 This profile requires the use of the AS4 Reception Awareness feature. This feature provides a  
259 built-in *Retry* mechanism that can help overcome temporary network or other issues and  
260 detection of message duplicates.

- 261
- The parameter **PMode[1].ReceptionAwareness** MUST be set to *true*.
- 262
- The parameter **PMode[1].ReceptionAwareness.Retry** MUST be set to *true*.
- 263
- The parameter **PMode[1].ReceptionAwareness.DuplicateDetection** MUST be set to
- 264
- true*.

265 The parameters **PMode[1].ReceptionAwareness.Retry.Parameters** and related  
266 **PMode[1].ReceptionAwareness.DuplicateDetection.Parameters** are sets of parameters  
267 configuring retries and duplicate detection. These parameters are not fully specified in [AS4]  
268 and implementation-dependent. Products MUST support configuration of parameters for  
269 retries and duplicate detection.

270 Reception awareness errors generated by the Sender MUST be reported to the Submitting  
271 application:

- 272
- The parameter **PMode[1].ErrorHandling.Report.MissingReceiptNotifyProducer**
- 273
- MUST be set to *true*.
- 274
- The parameter **PMode[1].ErrorHandling.Report.SenderErrorsTo** MUST NOT be set.
- 275
- There is no support for reporting sender errors to a third party.

## 276 2.2.6 Security

277 AS4 message exchanges can be secured at multiple communication layers: the network  
278 layer, the transport layer, the message layer and the payload layer. The first and last of these  
279 are not normally handled by B2B communication software and therefore out of scope for  
280 this section. Transport layer security is addressed, even though its functionality MAY be  
281 offloaded to another infrastructure component.

282 This section provides parameter settings based on multiple published sets of best practices.  
283 It is noted that after publication of this document, vulnerabilities may be discovered in the  
284 security algorithms, formats and exchange protocols specified in this section. Such  
285 discoveries SHOULD lead to revisions to this specification.

#### 286 2.2.6.1 Transport Layer Security

287 When using AS4, Transport Layer Security (TLS) is an option to provide message  
288 confidentiality and authentication. Server authentication, using a server certificate, allows  
289 the client to make sure the HTTPS connection is set up with the right server.

- 290 • When a message is pushed, the Sender authenticates Recipient's server to which the  
291 message is pushed
- 292 • When a message is pulled, the Receiver authenticates Sender's server from which the  
293 message is pulled

294 Guidance on the use of Transport Layer Security is published in the ENISA Algorithms, Key  
295 Sizes and Parameters Reports [ENISA13,ENISA14] and in a Mindest-standard of the Federal  
296 Office for Information Security (BSI) in Germany [BSITLS]. If TLS is handled by the AS4  
297 message handler (and not offloaded to some infrastructure component), then:

- 298 • TLS server authentication is REQUIRED.
- 299 • It MUST be possible to configure the accepted TLS version(s) in the AS4 message  
300 handler. The ENISA and BSI reports state that TLS 1.0 and TLS 1.1 SHOULD NOT be  
301 used in new applications. Older versions such as SSL 2.0 [RFC6176] and SSL 3.0 MUST  
302 NOT be used. Products compliant with this profile MUST therefore at least support  
303 TLS 1.2 [RFC5246].
- 304 • It MUST be possible to configure accepted TLS cipher suites in the AS4 message  
305 handler. IANA publishes a list of TLS cipher suites [TLSSP], only a subset of which the  
306 ENISA Report considers future-proof (see [ENISA13], section 5.1.2). Products MUST  
307 support cipher suites included in this subset. Vendors MUST add support for newer,  
308 safer cipher suites, as and when such suites are published by IANA/IETF.
- 309 • Support for SSL 3.0 and for cipher suites that are not currently considered secure  
310 SHOULD be disabled by default.
- 311 • Perfect Forward Secrecy, which is REQUIRED in [BSITLS], is supported by the  
312 TLS\_ECDHE\_\* and TLS\_DHE\_\* cipher suites, which SHOULD be supported.
- 313 • Publicly known vulnerabilities and attacks against TLS MUST be prevented and  
314 publicly known recommended countermeasures MUST be applied. Organisations  
315 MUST follow web security developments and MUST continually upgrade security  
316 measures as new general vulnerabilities become known.

317 If TLS is not handled by the AS4 message handler, but by another component, these  
318 requirements are to be addressed by that component (see section 2.3.4.2).

319 Transport Layer client authentication authenticates the Sender (when used with the Push  
320 MEP binding) or Receiver (when used with Pull). Since this profile uses WS-Security for  
321 message authentication (see section 2.2.6.2), the use of client authentication at the  
322 Transport Layer can be considered redundant. Whether or not client authentication is to be  
323 used depends on the deployment environment (see section 2.3.4.2). To support  
324 deployments that do require client authentication, products MUST allow Transport Layer  
325 client authentication to be configured for an AS4 HTTPS endpoint.

### 326 2.2.6.2 Message Layer Security

327 To provide message layer protection for AS4 messages, this profile REQUIRES the use of the  
328 following Web Services Security version 1.1.1 OASIS Standards, profiled in ebMS3.0 [EBMS3]  
329 and AS4 [AS4]:

- 330 • Web Services Security SOAP Message Security [WSSMS].
- 331 • Web Services Security X.509 Certificate Token Profile [WSSX509].
- 332 • Web Services Security SOAP Message with Attachments (SwA) Profile [WSSSWA].

333 The X.509 Certificate Token Profile supports signing and encryption of AS4 messages. This  
334 profile REQUIRES the use of X.509 tokens for message signing and encryption, for all AS4  
335 exchanges. This is consistent with current practice in the gas sector, as specified in the  
336 EASEE-gas AS2 profile [EGMTP]. The AS4 option of using Username Tokens, which is  
337 supported in the AS4 ebHandler Conformance Profile, MUST NOT be used.

338 AS4 message signing is based on the W3C XML Signature recommendation. AS4 can be  
339 configured to use specific digest and signature algorithms based on identifiers defined in this  
340 recommendation. At the time of publication of the AS4 standard [AS4], the current version  
341 of W3C XML Signature was the June 2008, XML Signature, Second Edition specification  
342 [XMLDSIG]. The current version is the April 2013, Version 1.1 specification [XMLDSIG1],  
343 which defines important new algorithm identifiers, including identifiers for SHA2, and  
344 deprecates SHA1, in line with guidance from ENISA [ENISA13,ENISA14].

345 This ENTSOG AS4 profile uses the following AS4 parameters and values:

- 346 • The **PMode[1].Security.X509.Sign** parameter MUST be set in accordance with section  
347 5.1.4 and 5.1.5 of [AS4].
- 348 • The **PMode[1].Security.X509.Signature.HashFunction** parameter MUST be set to  
349 *http://www.w3.org/2001/04/xmenc#sha256*.
- 350 • The **PMode[1].Security.X509.Signature.Algorithm** parameter MUST be set to  
351 *http://www.w3.org/2001/04/xmldsig-more#rsa-sha256*.

352 This anticipates an update to the AS4 specification to reference this newer specification that  
353 has been identified as part of the OASIS AS4 maintenance work. For encryption, WS-Security  
354 leverages the W3C XML Encryption recommendation. The following AS4 configuration  
355 options configure this feature:

- 356 • The **PMode[1].Security.X509.Encryption.Encrypt** parameter MUST be set in  
357 accordance with section 5.1.6 and 5.1.7 of [AS4].
- 358 • The parameter **PMode[1].Security.X509.Encryption.Algorithm** MUST be set to  
359 <http://www.w3.org/2009/xmlenc11#aes128-gcm>. This is the algorithm used as value  
360 for the *Algorithm* attribute of *xenc:EncryptionMethod* on *xenc:EncryptedData*.

361 AS4 also references an older version of XML Encryption than the current one ([XMLENC]  
362 instead of [XMLENC1]). However, the AES 128 algorithm [AES] was already referenced in that  
363 earlier version. AES is fully consistent with current recommendations for “near term” future  
364 system use [ENISA13,ENISA14]. However, the newer W3C specification recommends AES  
365 GCM strongly over any CBC block encryption algorithms.

366 In WS-Security, there are three mechanisms to reference a security token (see section 3.2 in  
367 [WSSX509]). The ebMS3 and AS4 specifications do not constrain this, neither do they  
368 provide a P-Mode parameter to select a specific option. For interoperability, products  
369 SHOULD therefore implement all three options. It is RECOMMENDED that products allow  
370 configuration of security token reference type, so that a compatible type can be selected for  
371 a communication partner (see section 2.3.4.3). Note that as *BinarySecurityToken* is the most  
372 widely implemented option for security token references in AS4 products, products MUST  
373 implement this option.

374 Key Transport algorithms are public key encryption algorithms especially specified for  
375 encrypting and decrypting keys, such as symmetric keys used for encryption of message  
376 content. No parameter is defined to support configuration of key transport in [EBMS3].  
377 Implementations MUST use the following algorithms on outbound messages and MUST  
378 accept them on inbound messages:

- 379 • For encryption method algorithm, <http://www.w3.org/2009/xmlenc11#rsa-oaep>.  
380 This is the algorithm used as value for the *Algorithm* attribute of  
381 *xenc:EncryptionMethod* on *xenc:EncryptedKey*.
- 382 • As mask generation function, <http://www.w3.org/2009/xmlenc11#mgf1sha256>. This  
383 is the algorithm used as value for the *Algorithm* attribute of *xenc:MGF* in  
384 *xenc:EncryptionMethod*.
- 385 • As digest generation function, <http://www.w3.org/2001/04/xmlenc#sha256>. This is  
386 the algorithm used as value for the *Algorithm* attribute on *ds:DigestMethod* in  
387 *xenc:EncryptionMethod*.

388 For backwards compatibility with versions of ENTSOG AS4 profile prior to version 3.6,  
389 implementations MAY also accept, on incoming messages, the use of other key transport  
390 algorithm options specified in section 5.5 of [XMLENC1].

## 391 2.2.7 Networking

392 AS4 communication products compliant with this profile MUST support both IPv4 and IPv6  
393 and MUST be able to connect using either IP4 or IPv6. To support transition from IPv4 to  
394 IPv6, products SHOULD support the “happy eyeballs” requirements defined in [RFC6555].

## 395 **2.2.8 Configuration Management**

396 ENTSOG has identified a requirement for automated or semi-automated exchange and  
397 management of AS4 configuration data in order to allow parties to negotiate and automate  
398 updates to AS4 configurations using the exchange of AS4 messages. The main initial  
399 requirement is the automated exchange of X.509 certificates.

400 AS4 products compliant with this specification MUST provide an Application Programming  
401 Interface (API) to manage (i.e. create, read, update and delete) AS4 configuration data,  
402 including Processing Mode definitions and X.509 certificates used for AS4 message  
403 exchanges. This API MUST provide all functionality required to create and process ebCore  
404 Agreement Update messages (see section 2.4).

## 405 **2.3 Usage Profile**

406 This section contains implementation guidelines that specify how products that comply with  
407 the requirements of the ENTSOG AS4 ebHandler (section 2.2) SHOULD be configured and  
408 deployed. This is similar to the concept of Usage Agreements in section 5 of [AS4] as it does  
409 not constrain how AS4 products are implemented, but rather how they are configured and  
410 used. The audience for this section are operators/administrators of AS4 products and B2B  
411 integration project teams. The structure of this chapter also partly mirrors the structure of  
412 [EBMS3], and furthermore covers some aspects outside core pure B2B messaging  
413 functionality.

### 414 **2.3.1 Message Packaging**

415 This usage profile constrains values for several elements in the AS4 message header.

#### 416 **2.3.1.1 Party Identification**

417 When exchanging messages in compliance with this profile, parties registered in the ENTSOG  
418 Energy Identification Coding Scheme (EIC) for natural gas transmission MUST be identified  
419 using the appropriate EIC Code [EIC]. Entities that do not have an EIC code and need to use  
420 this profile MUST contact ENTSOG or their Local Issuing Office (LIO) and request an EIC code.  
421 This value MUST be used as the content for the **PMode.Initiator.Party** and  
422 **PMode.Responder.Party** processing mode parameters, which AS4 message handlers use to  
423 populate the **UserMessage/PartyInfo/{From|to}/PartyId** elements.

424 The *type* attribute on the **PartyId** element MUST be present and set to the fixed value  
425 <http://www.entsoe.eu/eic-codes/eic-party-codes-x> which indicates that the value of the  
426 element is to be interpreted as an EIC code. This value is a URI used as an identifier only. It is  
427 not a URL that resolves to content on the ENTSOE web site. Note that AS4 party identifiers  
428 identify the communication partner. The communication partner may be:

- 429 1. The entity involved in the business transaction
- 430 2. A third party providing B2B communication services for other entities

431 In the second case, there are two options for setting the P-Mode parameters:

- 432 1. The communication partner may *impersonate* the business entity. In this case the  
433 AS4 **Party** identifier is the identifier of the business entity.
- 434 2. The business entity may explicitly *delegate* message processing to the  
435 communication partner. In this case the AS4 **Party** identifier is the identifier of the  
436 communication partner. Note that, when used to exchange EDIG@S documents, in  
437 this case the AS4 party identifier will differ from the value of the EDIG@S  
438 *{issuer/recipient}\_MarketParticipant.identification* elements, as the latter refer to the  
439 business partner.

440 Parties MAY use third party communication providers for AS4 communication. Such  
441 providers MAY use either the impersonation or delegation model, subject to approval by the  
442 business transaction partner.

443 The AS4 processing layer will validate the identifiers of Sender and Receiver specified in the  
444 ebMS3 headers against P-Mode configurations. This involves the validation of message  
445 signatures against configured X.509 certificates. In case of delegation, the X.509 certificates  
446 used at the AS4 level relate to the communication partners rather than to business partners  
447 on whose behalf the messages are exchanged. The exchanged payloads (EDIG@S or other)  
448 typically also reference sending and receiving business entities. The responsibility of  
449 determining the validity of implied delegation relations between business document layer  
450 entities and entities at the AS4 layer is not in scope for the AS4 message handler, but MUST  
451 be addressed in business applications or integration middleware.

### 452 2.3.1.2 Business Process Alignment

453 Several mandatory headers in AS4 serve to carry metadata to align a message exchange to a  
454 business process or to a technical service.

#### 455 2.3.1.2.1 Service

456 The **Service** and **Action** header elements in the **UserMessage/ CollaborationInfo** group  
457 relate a message to the business process the message relates to and the roles that sender  
458 and receiver perform, or to a technical service. This Usage Profile is intended to be used with  
459 business processes that are currently being modelled by ENTSOG and EASEE-gas as well as  
460 future, possibly not yet identified, business processes. For current and future gas business  
461 processes, ENTSOG maintains and publishes, on its public Web site, a link to a table of  
462 **Service** and **Action** values to be used in AS4 messages compliant to this Usage Profile (see  
463 section 2.3.1.2.4).

464 The value of the **Service** element content MUST set as follows:

- 465 • For gas business processes covered by EDIG@S, the value content of **Service** is  
466 specified in the ENTSOG AS4 Mapping Table (section 2.3.1.2.4) which MUST be used  
467 for AS4 messages carrying specified messages. These values are taken from an  
468 EDIG@S process area code list. As not all EDIG@S message exchanges concern TSOs,  
469 it may be that not all **Service** values that are needed to fully cover the EDIG@S



470 processes are in the table. The example message in section 3.1 uses the value *A06*,  
471 which is an EDIG@S code representing Nomination and Matching Processes.

472 • For the pre-defined test service (see section 2.3.7), the absolute **Service** URI value  
473 *http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/service* defined in  
474 [EBMS3] MUST be used. This value is a URI used as an identifier only. It does not  
475 resolve to content on the OASIS web site.

476 • For ebCore Agreement Update messages used for certificate exchange (see section  
477 2.4), the absolute **Service** URI value *http://docs.oasis-*  
478 *open.org/ebcore/ns/CertificateUpdate/v1.0* defined in [AU], section 4.1, MUST be  
479 used. This value is a URI used as an identifier only. It is not a URL that resolves to  
480 content on the OASIS web site.

481 • For other services not related to gas business processes, or not related to gas  
482 business processes covered by EDIG@S, no convention is defined in or imposed by  
483 this Usage Profile. The ENTSOG list (or future versions of it) MAY specify other non-  
484 gas business services.

485 The value of the *type* attribute of the **Service** element MUST comply with the following:

486 • For gas business processes covered by EDIG@S, the value MUST be the fixed value  
487 *http://edigas.org/service*. This value is a URI used as an identifier only. It does not  
488 resolve to a URL on the EDIGAS web sites

489 • For other services, the use (or non-use) of the *type* attribute on **Service** is not  
490 constrained by this Usage Profile.

491 In situations where the data exchange has not been classified, the service value  
492 *http://docs.oasis-open.org/ebxml-msg/as4/200902/service* MAY be used. This is the default  
493 P-Mode value for this parameter specified in section 5.2.5 of [AS4]. With this value, the *type*  
494 attribute MUST NOT be used. The non-normative example in section 3.1 uses the value  
495 “A06” for the **Service** header element, which is an EDIG@S service code. The other non-  
496 normative example in section 3.2 uses the AS4 default P-Mode parameter value.

#### 497 **2.3.1.2.2 Action**

498 The **Action** header identifies an operation or activity in a **Service**.

499 • For gas business processes covered by EDIG@S in which EDIG@S XML documents are  
500 exchanged, ENTSOG provides a value table listing actions (section 2.3.1.2.4). The  
501 value for **Action** in that table for a particular exchange MUST be used in AS4  
502 messages. The example messages in section 3.1 use the *http://docs.oasis-*  
503 *open.org/ebxml-msg/as4/200902/action* value, which is the default action defined in  
504 section 5.2.5 of the AS4 standard [AS4]. As not all EDIG@S message exchanges  
505 concern TSOs, it may be that not all **Action** values that are needed to fully cover the  
506 EDIG@S business processes are in the service metadata table.

- 507
- 508
- 509
- 510
- For the pre-defined test service (see section 2.3.7) the absolute **Action** URI value *http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/test* defined in [EBMS3] **MUST** be used. This value is a URI used as an identifier only. It is not a URL that resolves to content on the OASIS web site.
- 511
- For ebCore Agreement Update messages used for certificate exchange, the **Action** values *UpdateCertificate*, *ConfirmCertificateUpdate* and *RejectCertificateUpdate* defined in [AU], section 4.1, **MUST** be used.
- 514
- For other services not related to gas business processes, and for any (hypothetical future) gas business processes not covered by EDIG@S, no convention is defined in or imposed by this Usage Profile.
- 515
- 516

### 517 **2.3.1.2.3 Role**

518 The mandatory AS4 headers **UserMessage/PartyInfo/ {From|To}/Role** elements define the  
519 role of the entities sending and receiving the AS4 message for the specified **Service** and  
520 **Action**.

- 521
- For gas business processes covered by EDIG@S, the values **MUST** be set to values specified in the ENTSOG AS4 Mapping Table (section 2.3.1.2.4). For gas business processes, that table will relate to information in the EDIG@S document content. In EDIG@S, the sender and receiver role are expressed as EDIG@S header elements. For example, in an EDIG@S v5.1 Nomination document, these are called *issuer\_Marketparticipant\_marketRole.code* of type *IssuerRoleType* and *recipient\_Marketparticipant\_marketRole.code* of type *PartyType*.
- 522
- 523
- 524
- 525
- 526
- 527
- For the ebMS3 test service and for ebCore Agreement Update, the default initiator and responder roles *http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/initiator* and *http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/responder* defined in section 5.2.5 of [AS4] **MUST** be used. These URI values are used as identifiers only. They are not URLs that resolve to content on the OASIS web site.
- 528
- 529
- 530
- 531
- 532
- 533
- For services not related to gas business processes, or services not covered by EDIG@S, no convention is defined in or imposed by this Usage Profile.
- 534
- 535

536 In situations where the data exchange has not been classified, the role values  
537 *http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/initiator* **MAY** be used for  
538 the initiator role and *http://docs.oasis-open.org/ebxml-*  
539 *msg/ebms/v3.0/ns/core/200704/responder* for the responder role. These are the default P-  
540 Mode values for this parameter specified in section 5.2.5 of [AS4].

541 The non-normative example in section 3.1 uses the value “ZSH” for the initiating role header  
542 element (EDIG@S code for Shipper) and “ZSO” (EDIG@S code for Transmission System  
543 Operator) for the responding role header element. The other non-normative example in  
544 section 3.2 uses the AS4 default P-Mode parameter values.

#### 545 **2.3.1.2.4 ENTSOG AS4 Mapping Table**

546 ENTSOG maintains and publishes, in a machine-processable format, in collaboration with  
 547 EASEE-gas, the ENTSOG AS4 Mapping Table containing columns for the following values:

- 548 • EDIG@S process category (e.g. *A06 Nomination and Matching*).
- 549 • EDIG@S XML document schema (e.g. *NOMINT*).
- 550 • Document type element code for the **type** child element of the EDIG@S document  
 551 root element (e.g. *ANC*).
- 552 • Document type value defined for the document type element code in the EDIG@S  
 553 XML schema (e.g. *Forwarded single sided nomination*).
- 554 • **Service** value to use in an AS4 message carrying the EDIG@S document (configured  
 555 as the **PMode[1].BusinessInfo.Service** P-Mode parameter). For gas industry  
 556 exchanges, the values identify the gas business services that TSOs provide to each  
 557 other and to other communication partners.
- 558 • **Action** value to use in an AS4 message carrying the EDIG@S document (configured as  
 559 the **PMode[1].BusinessInfo.Action** P-Mode parameter). For exchanges that are  
 560 modelled in a service-oriented approach, the values identify the operations or  
 561 activities in a service. For exchanges that are not modelled in a service-oriented  
 562 approach, the default action *http://docs.oasis-open.org/ebxml-  
 563 msg/as4/200902/action* specified in the AS4 standard [AS4] will be used.
- 564 • **From/Role** to use in an AS4 message carrying the EDIG@S document (configured as  
 565 the AS4 **PMode.Initiator.Role** P-Mode parameter). This value matches the EDIG@S  
 566 *recipient\_Marketparticipant\_marketRole.code* (e.g. *ZSH*). Corresponding sender role  
 567 code value (e.g. *Shipper*).
- 568 • **To/Role** to use in an AS4 message carrying the EDIG@S document (configured as the  
 569 AS4 **PMode.Responder.Role** P-Mode parameter). This value matches the EDIG@S  
 570 *issuer\_Marketparticipant\_marketRole.code* (e.g. *ZSO*). Corresponding receiver role  
 571 code value (e.g. *Transit System Operator*).

572 Implementations of this profile MUST use the **Service**, **Action**, **From/Role** and **To/Role**  
 573 values to use specified in this table for the data exchanges covered by the table.

574 For business services, AS4 **Role** values MUST indicate business roles. If a Service Provider  
 575 sends or receives messages on behalf of some other organisation (whether in a delegation or  
 576 impersonation mode), the AS4 role values used relates to the business role of that other  
 577 organisation. There is no separate role value for Service Providers.

#### 578 **2.3.1.3 Message Correlation**

579 AS4 provides multiple mechanisms to correlate messages within a particular flow.

- 580 1. **UserMessage/MessageInfo/RefToMessageId** provides a way to express that a  
 581 message is a response to a single specific previous message. The **RefToMessageId**

582 element is used in response messages in Two Way message exchanges. Whether two  
583 exchanges in a business process are modelled as a Two Way exchange or as two One  
584 Way exchanges is a decision made in the Business Requirements Specification for the  
585 business process. In this version of this Usage Profile, all exchanges are considered  
586 One Way.

587 2. **UserMessage/CollaborationInfo/ConversationId** provides a more general way to  
588 associate a message with an ongoing conversation, without requiring a message to  
589 be a response to a single specific previous message, but allowing update messages to  
590 existing conversations from both Sender and Receiver of the original message.

591 In this version of this Usage Profile, the following rules shall apply:

- 592 1. **UserMessage/MessageInfo/RefToMessageId** MUST NOT be used. The default  
593 exchange is the One Way exchange.
- 594 2. **UserMessage/CollaborationInfo/ ConversationId** MUST be included in any AS4  
595 message (as it is a mandatory element) with as content the empty string.

596 The **RefToMessageId** and **ConversationId** elements may be used in future versions of this  
597 Usage Profile, for example to support request-response interactions.

### 598 2.3.2 Agreements

599 The **AgreementRef** element is profiled as follows:

- 600 • The element MUST be present in every AS4 message.
- 601 • Its value MUST be agreed between each pair of gas industry parties exchanging AS4  
602 messages conforming to this profile.
- 603 • In ebMS3, in principle, any value will do as long as, between two parties, the selected  
604 identifier is unique and therefore distinguishes messaging using one agreement from  
605 messages using another. For consistency, it is RECOMMENDED to use the following  
606 URI naming convention:  
607 *http://entsog.eu/communication/agreements/<EIC\_CODE\_Party\_A>/<EIC\_CODE\_Par*  
608 *ty\_B>/<version>*  
609 where **EIC\_CODE\_Party\_A** is the EIC code of the party that alphabetically precedes  
610 **EIC\_CODE\_Party\_B** of the other party, the version number is initially 1 and  
611 increments for any update.
- 612 • Its value MUST unambiguously identify each party's X.509 signing certificate and  
613 X.509 encryption certificate. In other words, if two AS4 messages from P1 to P2  
614 compliant with this Usage Profile have the same value for this element, they are  
615 signed using the same mutually known and agreed signing certificate (for P1) and  
616 their payloads are encrypted using the same mutually known and agreed encryption  
617 certificate (for P2). This is a deployment constraint on P-Mode configurations, in  
618 support of the introduction of the ebCore Agreement Update protocol [AU].
- 619 • The attributes *pmode* and *type* MUST NOT be set.

620 Furthermore:

- 621 • It is REQUIRED that for every tuple of <**From/PartyId, From/Role, To/PartyId,**  
622 **To/Role, Service, Action, AgreementRef**> values, a unique processing mode is  
623 configured. This is another deployment constraint on P-Mode configurations.
- 624 • For a tuple of <**From/PartyId, From/Role, To/PartyId, To/Role, Service, Action**>  
625 values, organisations MAY agree to configure multiple processing modes differing on  
626 other P-Mode parameters such as certificates used, or the URL of endpoints, for  
627 different values of **AgreementRef**. This includes the AS4 test service (see section  
628 2.3.7), meaning two parties can verify that they have consistent and properly  
629 configured P-Modes and firewalls for a particular agreement by sending each other  
630 AS4 test service messages using the corresponding **AgreementRef**.
- 631 • Parties MAY also use different values for **AgreementRef** to target AS4 gateways in  
632 different environments (see section 2.3.8), each having a different gateway endpoint  
633 URL and possibly certificates.

### 634 2.3.3 MPC

635 The ebMS3 optional attribute *mpc* on UserMessage is mainly used to support the Pull  
636 feature, which is not used in the current value of this Usage Profile. Therefore, the use of  
637 *mpc* is profiled. The attribute:

- 638 • MAY be present in the AS4 UserMessage. If this is the case, it MUST be set to the  
639 value [http://docs.oasis-open.org/ebxml-](http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/defaultMPC)  
640 [msg/ebms/v3.0/ns/core/200704/defaultMPC](http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/defaultMPC), which identifies the default MPC, and  
641 therefore MUST NOT be set to some other value
- 642 • MAY be omitted from the AS4 UserMessage. This is equivalent to it being present  
643 with the default MPC value

### 644 2.3.4 Security

645 This section describes configuration and deployment considerations in the area of security.

#### 646 2.3.4.1 Network Layer Security

647 Commission Regulation 2015/703 states that the Internet shall be used to exchange AS4  
648 messages [CR2015/703]. When using the public Internet, each organisation is individually  
649 responsible to implement security measures to protect access to its IT infrastructure.

650 Organisations use firewalls to restrict incoming or outgoing message flows to specific IP  
651 addresses, or address ranges. This prevents unauthorised hosts from connecting to the AS4  
652 communication server. Organisations therefore:

- 653 • MUST use static IP addresses (or IP address ranges) for inbound and outbound AS4  
654 HTTPS connections.

- 655
- 656
- 657
- 658
- 659
- MUST communicate all IP addresses (or IP address ranges) used for outgoing and incoming connections to their trading partners, also covering addresses of any passive nodes in active-passive clusters. Note that the address of the HTTPS endpoint which an AS4 server is to push messages to or pull messages from MAY differ from the address (or addresses) used for outbound connections.
- 660
- MUST notify their trading partners about any IP address changes sufficiently in advance to allow firewall and other configuration changes to be applied.
- 661

#### 662 **2.3.4.2 Transport Layer Security**

663 The Transport Layer Security settings defined in section 2.2.6.1 MAY be implemented in the  
664 AS4 communication server but TLS MAY also be offloaded to a separate infrastructure  
665 component (such as a firewall, proxy server or router). In that case, the recommendations  
666 on TLS version and cipher suites of 2.2.6.1 MUST be addressed by that component.

667 The X.509 certificate used by such a separate component MAY follow the requirements of  
668 section 2.3.4.4, but this is NOT REQUIRED.

669 The TLS cipher suites recommended in section 2.2.6.1 are supported in recent versions of  
670 TLS toolkits and which therefore are available for use. Support for these suites is  
671 RECOMMENDED. Whether or not less secure cipher suites (which are only recommended for  
672 legacy applications) are allowed is a local policy decision.

673 This profile does NOT REQUIRE the use of client authentication. Client authentication MAY  
674 be a requirement in the networking policy of individual organisations that the AS4  
675 deployment needs to meet, but is NOT RECOMMENDED.

#### 676 **2.3.4.3 Message Layer Security**

677 The following parameters control configuration of security at the message layer:

- 678
- The **PMode[1].Security.X509.Signature.Certificate** parameter MUST be set to a value matching the requirements specified in section 2.3.4.4.
- 679
- The **PMode[1].Security.X509.Encryption.Certificate** parameter MUST be set to a value matching the requirements specified in section 2.3.4.4.
- 680
- If a product allows selection of the type of security token reference, it MUST be set to a type supported by the counterparty.
- 681
- 682
- 683

#### 684 **2.3.4.4 Certificates and Public Key Infrastructure**

685 In this Usage Profile, X.509 certificates are used to secure both Transport Layer and Message  
686 Layer communication. Requirements on certificates can be sub-divided into three groups:

- 687
- General requirements;
- 688
- Requirements for Transport Layer Security;
- 689
- Requirements for Message Layer Security.

690 The following general requirements apply to all certificates:

- 691 • A three year validity period for end entity certificates is RECOMMENDED.
- 692 • Guidance on size for RSA public keys for future system use indicates a key size of  
693 2048 bits [BSIALG] or even 3072 bits [ENISA13,ENISA14] is appropriate. Keys with size  
694 less than 2048 bits MUST NOT be used.
- 695 • The signature algorithm used to sign public keys MUST be based on at least the SHA-  
696 256 hashing algorithm.
- 697 • A certificate for use in a production environment MUST be issued by a Certification  
698 Authority (CA).
- 699 • The choice of Certification Authority issuing the certificate is left to implementations  
700 but is subject to review by ENTSOG.
- 701 • The issuing CA SHOULD, at a minimum, meet the Normalised Certificate Policy (NCP)  
702 requirements specified in [EN 319 411-1].

703 The following additional requirements apply for certificates for Transport Layer Security:

- 704 • A TLS server certificate SHOULD comply with the certificate profile defined in [EN 319  
705 412-4]. At a minimum, the CA Browser forum baseline requirements SHOULD be met  
706 [CABFBRCP]. Extended Validation Certificates MAY be used [CABFEVV].
- 707 • If a single TLS server certificate is needed to secure host names on different base  
708 domains, or to host multiple virtual HTTPS servers using a single IP address, it is  
709 RECOMMENDED to use a Multi-Domain (Subject Alternative Name) certificate.  
710 Alternatively, wild card certificates MAY be used.
- 711 • No additional requirements are placed on TLS client certificates.

712 The following additional requirements apply for certificates for Message Layer Security:

- 713 • Organisations MAY use a certificate issued by EASEE-gas.
- 714 • The type of certificate MUST be certificates for organisations, for which proof of  
715 identity is required.
- 716 • The issued certificate SHOULD comply with the certificate profile defined in [EN 319  
717 412-3].

718 A sample certificate profile is provided in section 2.3.4.5. For certificates used for Message  
719 Layer Security it follows the EASEE-gas convention of including the party EIC code (see  
720 section 2.3.1.1) as recommended value for the Common Name. Alternatively, the EIC code  
721 MAY be used as the Subject SerialNumber of as the Subject OrganisationIdentifier.

722 B2B document exchange typically occurs in a community of known entities, where  
723 communication between parties and counterparties is secured using pre-agreed certificates.  
724 Such an environment is different from open environments, where certificates establish  
725 identities for (possibly previously unknown) entities and Certification Authorities play an  
726 essential role to establish trust. Entities MUST proactively notify all communication partners

727 of any updates to certificates used, and in turn MUST process any certificate updates from  
 728 their communication partners. This concerns both regular renewals of certificates at their  
 729 expiration dates and replacements for revoked certificates. See section 2.4 for a description  
 730 of the use of ebCore Agreement Update to exchange certificates.

731 Organisations MAY also use Certificate Revocation Lists (CRL) or the Online Certificate Status  
 732 Protocol (OCSP). Individual companies should assess the potential impact on the availability  
 733 of the AS4 service when using such mechanisms, as their use may cause a certificate to be  
 734 revoked automatically and messages to be rejected.

### 735 2.3.4.5 Certificate Profile

736 This section defines a profile for X.509 certificates to secure AS4 communication. This profile  
 737 is consistent with the EASEE-gas certificate profile. For specific requirements, see [ENISA13,  
 738 ENISA14, EN 319 411-1 , EN 319 412-3, EN 319 412-4] and [TS119312].

#### 739 2.3.4.5.1 Key Size

Entity	Algorithm	Keylength
Root-CA	RSA	Dependent on maximum lifetime of certificate: For 3 years: minimum of 2048 bits For 6 years: minimum of 3072 bits For 10 years: minimum of 4096 bits
Sub-CA	RSA	
End-Entities	RSA	Minimum of 2048 bits, assuming a maximum lifetime of 3 years for end entity certificates.

#### 740 2.3.4.5.2 Key Algorithm

Entity	Signing Algorithm	O.I.D.
Root-CA	sha256WithRSAEncryption	1.2.840.113549.1.1.11
Sub-CA	sha256WithRSAEncryption	1.2.840.113549.1.1.11
End-Entities	sha256WithRSAEncryption	1.2.840.113549.1.1.11

#### 741 2.3.4.5.3 Naming

742 The following example uses the ENTSOG name as CA. This is only provided as an illustration.  
 743 ENTSOG does not currently intend to become a Certification Authority.

Entiteit	Example Value	Comments
Root-CA	C=BE	ISO country code (ISO 3166)
	O=ENTSOG	Name of the Organisation
	CN=ENTSOG CA	Name of the CA
Sub-CA	C=	ISO country code (ISO 3166)
	O=	Name of the Organisation
	OU=	Name of the organisational unit



	CN=	Name of the sub-CA
--	-----	--------------------

744 **2.3.4.5.4 Certificate Body**

Certificate Component	Example Value	Presence	Comments
Certificate		M	
TBSCertificate		M	
Version	v3	M	X.509 version 3 is required.
serialNumber	Unique number	M	A unique CA generated number
Signature		M	The calculated signature (for instance the sha2 value encrypted with RSA key with length 4096)
validity.notBefore	Date	M	The start date of the certificate
validity.notAfter	Date	M	The end date of the certificate, at most 3 years after the start date (for end-entities).
issuer.countryName	BE	M	The country code of the country where the CA resides (ISO 3166)
issuer.organisationName	ENTSOG	M	Example, if ENTSOG is the CA
issuer.commonName	ENTSOG CA	M	Example, if ENTSOG is the CA
subject.countryName	BE	M	ISO country code (ISO 3166)
subject.organisationName	Fluxys	M	Name of member organisation
subject.organisationUnit			Not applicable
subject.serialNumber	Unique number		A unique CA generated number. May be used to encode the EIC code, as alternative to using the Common Name.
subject.commonName	EIC code*	M	Preferably the EIC code, following EASEE-gas convention, but some CAs do not support using the EIC in certificate fields.
subject.organizationIdentifier	EIC code*		Recommended in [EN 319 412-3]. May be used to encode the EIC code, as alternative to using the Common Name.
subjectPublicKeyInfo.Algorithm	RsaEncryption	M	The encryption algorithm, at least RSA.
subjectPublicKeyInfo.SubjectPublicKey			The public key of the subject.
Extensions		M	
signatureAlgorithm	sha2WithRSAEncryption	M	At least SHA-2 is required. SHA-1 is not allowed.
signatureValue	Signature of ENTSOG CA	M	The digital signature value.

745

746 **2.3.4.5.5 Extensions for Signing, Encryption and TLS End Entities**

Extension Name	Ref RFC 5280	Sign end entity	Encrypt end entity	TLS Client / Server end entity	Comments
AuthorityKeyIdentifier	4.2.1.1	M	M	M	
keyIdentifier		X	x	X	
authorityCertIssuer		M	M	M	
authorityCertSerialNumber		M	M	M	
SubjectKeyIdentifier	4.2.1.2	M	M	M	
subjectKeyIdentifier		M	M	M	
KeyUsage	4.2.1.3	MC	MC	MC	
<i>digitalSignature</i>		M	x	M	
nonRepudiation		M*	x	X	* Recommended; Some CAs do not support this for organisations and limit this extension to qualified certificates for natural persons.
<i>keyEncipherment</i>		X	M	M	In WS-Security the certificate is used to encrypt a symmetric encryption key; it is not used directly to encrypt message data.
<i>dataEncipherment</i>		X	x	X	
<i>keyAgreement</i>		X	x	x	
keyCertSign		X	x	X	Only for CA root and sub-CA certificates.
cRLSign		X	x	X	Only for CA CRL publishing.
encipherOnly		X	x	X	
decipherOnly		X	x	X	
CertificatePolicies	4.2.1.4	X	x	X	
PolicyMappings	4.2.1.5	X	x	X	
SubjectAltName	4.2.1.6	X	x	X	
otherName					TRUE if applicable.
otherName.type-id					OID = 1.3.6.1.4.1.311.20.2.3 Preferably the subjectserialnumber followed by ENTSOG serialnumber

Extension Name	Ref RFC 5280	Sign end entity	Encrypt end entity	TLS Client / Server end entity	Comments
IssuerAltName	4.2.1.7	X	x	X	
SubjectDirectoryAttributes	4.2.1.8	X	x	X	
BasicConstraints	4.2.1.9	M	M	M	
CA		False	False	False	Only TRUE in case of a CA root or sub-CA certificate.
PathLenConstraint		X	x	X	
NameConstraints	4.2.1.10	X	x	X	
AuthorityInfoAccess		M	M	M	The URL of the OCSP responder.
PolicyConstraints	4.2.1.11	X	x	X	
ExtKeyUsage	4.2.1.12	X	x	M	See next table.
CRLDistributionPoints	4.2.1.13	X	x	X	The URL of the CRL.
InhibitAnyPolicy	4.2.1.14	X	x	X	
FreshestCRL	4.2.1.15	X	x	X	
privateInternetExtensions	4.2.2	X	x	X	

747 **2.3.4.5.6 Extended Key Usage**

Extended Key Usage OID	Ref RFC 5280	TLS Client / Server end entity
id-kp-clientAuth	4.2.1.12	M
id-kp-serverAuth	4.2.1.12	M

748 **2.3.4.5.7 Certificate Lifetime**

Entity	Maximum Period	Start Refresh
Root-CA	15 years	2 years before
Sub-CA	10 years	1 year before
End Entities	3 years	6 months before

749 **2.3.5 Networking**

750 Data exchange MUST use IPv4 or IPv6. It is RECOMMENDED that AS4 gateway deployments  
751 support both IPv4 and IPv6 for the exchange of AS4 messages. This allows these gateways to  
752 support both communication partners that are still restricted to using IPv4 and other  
753 communication partners that have already deployed IPv6.

754 Due to IPv4 address exhaustion and the increased roll-out of IPv6, some future deployments  
755 of gateways using ENTISO AS4 MAY be IPv6 only. A future version of this profile will  
756 therefore REQUIRE support for IPv6.

### 757 2.3.6 Message Payload and Flow Profile

758 A single AS4 UserMessage MUST reference, via the *PayloadInfo* header, a single structured  
759 business document and MAY reference one or more other (structured or unstructured)  
760 payload parts. The business document is considered the “leading” payload part for business  
761 processing. Any payload parts other than the business document are not to be processed in  
762 isolation but only as adjuncts to the business document. Business document, attachments  
763 and metadata MUST be submitted and delivered as a logical unit. The format of the business  
764 document SHOULD be XML, but other datatypes MAY be supported in specific business  
765 processes or contexts.

766 For each business process, the Business Requirement Specification specifies the XML schema  
767 definition (XSD) that the business document is expected to conform to.

- 768 • For gas business processes covered by EDIG@S, in which the value content of **Service**  
769 is specified in the ENTSOG AS4 Mapping Table, the **Action** is set to the default action  
770 and the exchanged business document is an EDIG@S XML document (section  
771 2.3.1.2.4), for the business document part a **Property** SHOULD be included in the  
772 **PartProperties** with a name *EDIGASDocumentType* set to the same value as the top-  
773 level **type** element in the EDIG@S XML document, which is of type *DocumentType*.  
774 The mapping from a combination of **From/PartyId** element, **To/PartyId** and  
775 *EDIGASDocumentType* property values to XSDs MUST be agreed and unique, allowing  
776 Receivers to validate XML documents using a specific (version of an) XML schema for  
777 a particular sender, receiver and document type.
- 778 • The part property *EDIGASDocumentType* MUST NOT be used with payloads that are  
779 not EDIG@S XML business documents.
- 780 • When using the ebMS3 test service (see section 2.3.7), no XML schema constraints  
781 apply to any of the included payloads.
- 782 • For certificate exchange (see section 2.4), the XML schemas specified in the ebCore  
783 Agreement Update [AU] specification for certificate update request, update  
784 acceptance and update exception MUST be used with, respectively, the  
785 *UpdateCertificate*, *ConfirmCertificateUpdate* and *RejectCertificateUpdate* values for  
786 **Action**.
- 787 • For other services, in case the **Action** is not set to the AS4 default action, the  
788 mapping from **Service** and **Action** value pairs to XSDs MUST be unique, allowing  
789 Receivers to validate XML documents using a specific XML schema.

790 Some gas data exchanges are traditional batch-scheduled exchanges that can involve very  
791 large payloads. The trend in the industry towards service-oriented and event-driven  
792 exchanges is leading to more, and more frequent, exchanges, with smaller payloads per  
793 exchange. It is expected that the vast majority of payloads will be less than 1 MB in size  
794 (prior to compression), with rare exceptions up to 10 MB. The number of messages  
795 exchanged over a period, their distribution over time and the peak load/average load ratio,  
796 are dependent on business process and other factors. Parties MUST take peak message

797 volumes and maximum message size into account when initially deploying AS4. Parties  
798 SHOULD also monitor trends in message traffic for existing processes and anticipate any new  
799 business processes being deployed (and the expected increases in message and data  
800 volumes), and adjust their deployments accordingly in a timely manner.

801 In practice, there are limitations on the maximum size of payloads that business partners can  
802 accept. These limitations may be caused by capabilities of the AS4 message product, or by  
803 constraints of the business application, internal middleware, storage or other software or  
804 hardware. When designing business processes and document schemas, and when  
805 generating content based on those schemas, these requirements SHOULD be taken into  
806 account. In particular, business processes in which large amounts of data are exchanged and  
807 the business applications supporting these processes SHOULD be designed such that data  
808 can be exchanged as a series of related messages, the payload size of each of which does not  
809 exceed 10 MB, rather than as a single message carrying a single large payload that could  
810 potentially be much larger.

### 811 2.3.7 Test Service

812 Section 5.2.2 of [EBMS3] defines a server test feature that allows an organisation to “Ping” a  
813 communication partner. The feature is based on messages with the values of:

- 814 • **UserMessage/CollaborationInfo/Service** set to *http://docs.oasis-open.org/ebxml-*  
815 *msg/ebms/v3.0/ns/core/200704/service*
- 816 • **UserMessage/CollaborationInfo/Action** set to *http://docs.oasis-open.org/ebxml-*  
817 *msg/ebms/v3.0/ns/core/200704/test*.

818 This feature MUST be supported so that parties can perform a basic test of the  
819 communication configuration (including security at network, transport and message layer,  
820 and reliability) in any environment, including the production environment, with any of their  
821 communication partners. This functionality MAY be supported as a built-in feature of the  
822 AS4 product. If not, a P-Mode MUST be configured with these values. The AS4 product MUST  
823 be configured so that messages with these values are not delivered to any business  
824 application.

### 825 2.3.8 Environments

826 B2B data exchange solutions are part of the overall IT service lifecycle, in which different  
827 environments are operated (typically in parallel) for development, test, pre-production (in  
828 some companies referred to as “acceptance environments” or “QA environments”) and  
829 production. Development and test are typically internal environments in which trading  
830 partners are simulated using stubs. When exchanging messages between organisations (in  
831 either pre-production or production environments), they must target the appropriate  
832 environment. In order to prevent a configuration error from causing non-production  
833 messages to be delivered to production environments or vice versa, organisations SHOULD  
834 configure processing modes at message handlers so that messages from one type of  
835 environment cannot be accepted inadvertently in a different type of environment.

## 836 **2.4 ebCore Agreement Update**

837 Based on ENTSOG and other community requirements, an XML schema and exchange  
838 protocol for Agreement Updates [AU] was developed in the OASIS ebCore Technical  
839 Committee. This specification is currently an OASIS Committee Specification (CS). A  
840 Committee Specification is an OASIS Standards Final Deliverable that is stable and suited for  
841 implementation. The Agreement Update specification is similar to, but not to be confused  
842 with, earlier work in the IETF defining a Certificate Exchange Message for EDIINT [CEM].

### 843 **2.4.1 Mandatory Support**

844 As from 01.07.2017, implementers of the ENTSOG AS4 Usage Profile **MUST** be able to  
845 support ebCore Agreement Update for Certificate Exchange with their communication  
846 partners. Prior to that date, partners **MAY** use the mechanism, subject to bilateral  
847 agreement.

848 Support for ebCore Agreement Update requirement entails the following:

- 849 • AS4 products **MUST** be able to exchange ebCore Agreement Update AS4 messages.  
850 As AS4 is payload-agnostic, this imposes no special requirements on products. The  
851 only requirement on implementers deploying AS4 products is that these messages  
852 **MUST** use the **Service** and **Action** values specified in sections 2.3.1.2.1 and 2.3.1.2.2,  
853 respectively.
- 854 • Mechanisms to create an ebCore AU document; use it to submit an update to an AS4  
855 configuration; convert the success/failure of such an update to a positive/negative  
856 ebCore response document; provide an interface to the AS4 MSH for submission and  
857 delivery of ebCore documents exchanged with communication partners.

858 The AS4 configuration management API (see section 2.2.8) **MUST** provide all functionality to  
859 implement ebCore Agreement Update. However, direct integration of any functionality to  
860 process ebCore Agreement Update within the AS4 gateway is **NOT REQUIRED**. The  
861 functionality **MAY** be implemented in some add-on component or in an application that both  
862 uses the AS4 gateway for partner communication and is able to manipulate its configuration.

863 It is **NOT REQUIRED** to implement a fully automated process to process certificate updates.  
864 Organizations **MAY** implement a process that involves approval or other manual steps to  
865 process certificate updates.

### 866 **2.4.2 Implementation Guidelines**

867 When using Agreement Update for Certificate Update, the following guidelines apply:

- 868 • A party **MUST** obtain the new certificate that it intends to replace an existing  
869 certificate with significantly in advance of the expiration date of the certificate to be  
870 replaced.
- 871 • Once a party has obtained the new certificate, parties **MUST** determine the  
872 communication partners and agreements that are using the old certificate. To each of

873 these partners, and for all agreements, the party SHOULD send a Certificate Update  
874 Request as soon as possible.

875 • The **ActivateBy** value in the update requests MUST be set such that the period in  
876 which the request is to be processed is sufficiently long. The definition of “sufficiently  
877 long” is partner-dependent, but should take into account that the process on the  
878 partner side may be a (partly) manual process. Therefore, time for validation of the  
879 request, including validation of the certificate and the issuing Certification Authority;  
880 time to create and perform a change request within the partner organization  
881 SHOULD be taken into account.

882 • The specific **ActivateBy** value MUST be set to a date and time acceptable to the  
883 receiving organization. This MAY depend on working hours and staff availability,  
884 release schedules etc.

885 • When an updated agreement has been created and agreed, it MUST first be tested  
886 using the test service, as described in section 2.3.7 of this document and section 3.5  
887 of [AU]. These tests MUST cover test messages in both directions.

888 • The **ActivateBy** value SHOULD be set to a date and time sufficiently in advance to the  
889 expiration data and time of the old agreement, such that a fall-back to the old  
890 agreement, and any necessary troubleshooting, is possible in case any blocking issue  
891 occurs during tests.

892 • If the updated agreement has been tested successfully, the regular message flow that  
893 used the old agreement SHOULD be re-deployed to the new agreement. The old  
894 agreement SHOULD NOT be used any more for new exchanges.

895 • The ebCore Agreement also provides an explicit Agreement Termination feature. Use  
896 of this feature is NOT REQUIRED, but may be agreed bilaterally.

897 • Even in case of successful deployment of the new agreement, the old agreement  
898 SHOULD NOT be deactivated immediately. This is to allow any in-process messages  
899 that use to old agreement to still be processed. For example, a message that was not  
900 successfully sent and is being retransmitted due to AS4 reliable messaging may be  
901 received at a time when the new agreement has already been deployed. In this case,  
902 the configuration for the old agreement SHOULD still be available to successfully  
903 receive, acknowledge and deliver the message.

### 904 **3 Examples**

#### 905 **3.1 Message with EDIG@S Payload**

906 The following non-normative example is included to illustrate the structure of an AS4  
907 message conforming to this profile, for a hypothetical [http://docs.oasis-open.org/ebxml-](http://docs.oasis-open.org/ebxml-msg/as4/200902/action)  
908 [msg/as4/200902/action](http://docs.oasis-open.org/ebxml-msg/as4/200902/action) action invoked by a hypothetical shipper 21X-EU-A-X0A0Y-Z on a  
909 hypothetical service A06 exposed by a hypothetical transmission system operator 21X-EU-B-  
910 PQ0QR-S. The detailed contents of the *wsse:Security* header is omitted.

```

911 POST /as4handler HTTP/1.1
912 Host: receiver.example.com:8893
913 User-Agent: Turia
914 Content-Type: multipart/related; start="<f8df1904-a6b9-422b-8239-6a971838503f@sender.example.com>";
915 boundary= "c5bae1842d1e"; type="application/soap+xml"
916 Content-Length: 472639
917
918 --c5bae1842d1e
919 Content-Id: <f8df1904-a6b9-422b-8239-6a971838503f@sender.example.com>
920 Content-Type: application/soap+xml; charset="UTF-8"
921
922 <S12:Envelope xmlns:S12="http://www.w3.org/2003/05/soap-envelope"
923 xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
924 xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
925 xmlns:eb3="http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/">
926 <S12:Header>
927 <eb3:Messaging wsu:Id="_18f85fc2-a956-431e-a80e-09a10364871b">
928 <eb3:UserMessage>
929 <eb3:MessageInfo>
930 <eb3:Timestamp>2016-04-03T14:49:28.886Z</eb3:Timestamp>
931 <eb3:MessageId>2016-92105209999001264@example.com</eb3:MessageId>
932 </eb3:MessageInfo>
933 <eb3:PartyInfo>
934 <eb3:From>
935 <eb3:PartyId
936 type="http://www.entsoe.eu/eic-codes/eic-party-codes-x">21X-EU-A-X0A0Y-Z</eb3:PartyId>
937 <eb3:Role>ZSH</eb3:Role>
938 </eb3:From>
939 <eb3:To>
940 <eb3:PartyId
941 type="http://www.entsoe.eu/eic-codes/eic-party-codes-x">21X-EU-B-P0Q0R-S</eb3:PartyId>
942 <eb3:Role>ZSO</eb3:Role>
943 </eb3:To>
944 </eb3:PartyInfo>
945 <eb3:CollaborationInfo>
946 <eb3:AgreementRef
947 >http://entsog.eu/communication/agreements/21X-EU-A-X0A0Y-Z/21X-EU-B-P0Q0R-S/3</eb3:AgreementRef>
948 <eb3:Service type="http://edigas.org/service">A06</eb3:Service>
949 <eb3:Action> http://docs.oasis-open.org/ebxml-msg/as4/200902/action</eb3:Action>
950 <eb3:ConversationId></eb3:ConversationId>
951 </eb3:CollaborationInfo>
952 <eb3:PayloadInfo>
953 <eb3:PartInfo href="cid:0b960692-a3c6-4e85-80da-36009d3ae043@sender.example.com">
954 <eb3:PartProperties>
955 <eb3:Property name="MimeType">application/xml</eb3:Property>
956 <eb3:Property name="CharacterSet">utf-8</eb3:Property>
957 <eb3:Property name="CompressionType">application/gzip</eb3:Property>
958 <eb3:Property name="EDIGASDocumentType">01G</eb3:Property>
959 </eb3:PartProperties>
960 </eb3:PartInfo>
961 </eb3:PayloadInfo>
962 </eb3:UserMessage>
963 </eb3:Messaging>
964 <wsse:Security xmlns:wss="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-
965 secext-1.0.xsd"
966 xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-
967 1.0.xsd">
968 <!-- details omitted -->
969 </wsse:Security>
970 </S12:Header>
971 <S12:Body wsu:Id="_b656ef2c-516"/>
972 </S12:Envelope>
973
974 --c5bae1842d1e
975 Content-Id: <0b960692-a3c6-4e85-80da-36009d3ae043@sender.example.com>
976 Content-Type: application/octet-stream
977 Content-Transfer-Encoding: binary
978
979 BINARY CIPHER DATA
980
981 --c5bae1842d1e--

```



981 **3.2 Alternative Using Defaults**

982 The following example fragment is a variant of the sample message shown in section **Error!**  
983 **Reference source not found.**, for a data exchange that has not been classified using EDIG@S  
984 code values for **Service** and **Role**. Instead of an EDIG@S service code, it uses the default  
985 service value, as described in section 2.3.1.2.1. Instead of EDIG@S role codes, it uses the  
986 default initiator and responder roles, as described in section 2.3.1.2.3.

```

987 ...
988 <eb3:PartyInfo>
989   <eb3:From>
990     <eb3:PartyId
991       type="http://www.entsoe.eu/eic-codes/eic-party-codes-x">21X-EU-A-X0A0Y-Z</eb3:PartyId>
992     <eb3:Role>http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/initiator</eb3:Role>
993   </eb3:From>
994   <eb3:To>
995     <eb3:PartyId
996       type="http://www.entsoe.eu/eic-codes/eic-party-codes-x">21X-EU-B-P0Q0R-S</eb3:PartyId>
997     <eb3:Role>http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/responder</eb3:Role>
998   </eb3:To>
999 </eb3:PartyInfo>
1000 <eb3:CollaborationInfo>
1001   <eb3:AgreementRef
1002     >http://entsog.eu/communication/agreements/21X-EU-A-X0A0Y-Z/21X-EU-B-P0Q0R-S/3</eb3:AgreementRef>
1003   <eb3:Service> http://docs.oasis-open.org/ebxml-msg/as4/200902/service</eb3:Service>
1004   <eb3:Action> http://docs.oasis-open.org/ebxml-msg/as4/200902/action</eb3:Action>
1005   <eb3:ConversationId></eb3:ConversationId>
1006 </eb3:CollaborationInfo>
1007 ...

```

1008 **4 Processing Modes**

1009

P-Mode Parameter	Profile Value
PMode.ID	Not used
PMode.Agreement	http://entsog.eu/communication/agreements/<EIC_CODE_Party_A>/<EIC_CODE_Party_B>/<version>  @pmode and @type attributes not used.
PMode.MEP	http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/oneWay http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/twoWay
PMode.MEPBinding	http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/push http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/pushAndPush
PMode.Initiator.Party	Value is an EIC code.  The @type attribute is required with fixed value http://www.entsoe.eu/eic-codes/eic-party-codes-x

P-Mode Parameter	Profile Value
PMode.Initiator.Role	Set in accordance with ENTSOG AS4 Mapping Table or to AS4 default for test and AU.
PMode.Initiator.Authorisation.username	Not used
PMode.Initiator.Authorisation.password	Not used
PMode.Responder.Party	Value is an EIC code. @type attribute required with value <a href="http://www.entsoe.eu/eic-codes/eic-party-codes-x">http://www.entsoe.eu/eic-codes/eic-party-codes-x</a>
PMode.Responder.Role	Set in accordance with ENTSOG AS4 Mapping Table for business services.
PMode.Responder.Authorisation.username	Not used
PMode.Responder.Authorisation.password	Not used
PMode[1].Protocol.Address	Required, HTTPS URL of the receiver.
PMode[1].Protocol.SOAPVersion	1.2
PMode[1].BusinessInfo.Service	Set in accordance with ENTSOG AS4 Mapping Table, for business services. Default service for test; ebCore AU service for certificate update.
PMode[1].BusinessInfo.Action	Default values from AS4, <a href="http://docs.oasis-open.org/ebxml-msg/as4/200902/action">http://docs.oasis-open.org/ebxml-msg/as4/200902/action</a> , for business services. Test action for test. The ebCore AU values for AU.
PMode[1].BusinessInfo.Properties	Optional
PMode[1].BusinessInfo.MPC	Either not used or (equivalently) set to the ebMS3 default MPC.
PMode[1].Errorhandling.Report.SenderErrorsTo	Not used
PMode[1].Errorhandling.Report.ReceiverErrorsTo	Not used

P-Mode Parameter	Profile Value
PMode[1].Errorhandling.Report.AsResponse	True
PMode[1].Errorhandling.Report.ProcessErrorNotifyConsumer	True (Recommended)
PMode[1].Errorhandling.DeliveryFailuresNotifyProducter	True (Recommended)
PMode[1].Reliability	Not used
PMode[1].Security.WSSversion	1.1.1
PMode[1].Security.X509.Sign	True
PMode[1].Security.X509.Signature.Certificate	Signing Certificate of the Sender
PMode[1].Security.X509.Signature.HashFunction	<a href="http://www.w3.org/2001/04/xmlenc#sha256">http://www.w3.org/2001/04/xmlenc#sha256</a>
PMode[1].Security.X509.Signature.Algorithm	<a href="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256">http://www.w3.org/2001/04/xmldsig-more#rsa-sha256</a>
PMode[1].Security.X509.Encryption.Encrypt	True
PMode[1].Security.X509.Encryption.Certificate	Encryption Certificate of the Receiver
PMode[1].Security.X509.Encryption.Algorithm	<a href="http://www.w3.org/2009/xmlenc11#aes128-gcm">http://www.w3.org/2009/xmlenc11#aes128-gcm</a>
PMode[1].Security.X509.Encryption.MinimalStrength	128
PMode[1].Security.UsernameToken.username	Not used

P-Mode Parameter	Profile Value
PMode[1].Security. UsernameToken. password	Not used
PMode[1].Security. UsernameToken.Digest	Not used
PMode[1].Security. UsernameToken.Nonce	Not used
PMode[1].Security. UsernameToken.Created	Not used
PMode[1].Security. PModeAuthorise	False
PMode[1].Security.SendReceipt	True
PMode[1].Security.SendReceipt. NonRepudiation	True
PMode[1].Security.SendReceipt. ReplyPattern	Response
PMode[1].PayloadService. CompressionType	application/gzip
PMode[1].ReceptionAwareness	True
PMode[1].ReceptionAwareness. Retry	True
PMode[1].ReceptionAwareness. Retry.Parameters	Not profiled
PMode[1].ReceptionAwareness. DuplicateDetection	True
PMode[1].ReceptionAwareness. DetectDuplicates.Parameters	Not profiled

P-Mode Parameter	Profile Value
PMode[1].BusinessInfo. subMPCext	Not used

1010



1011 **5 Revision History**

Revision	Date	Editor	Changes Made
v0r1	2013-10-29	PvdE	First Draft for discussion
V0r2	2013-11-18	PvdE	<ul style="list-style-type: none"> <li>• Textual updates from discussions at F2F 2013-11-04.</li> <li>• Improved separation of the AS4 feature set (chapter 2.2) and the usage profile (2.3). For the feature set the audience are vendors and for the usage profile users/implementers.</li> <li>• Provided guidance for TLS based on ENISA and other guidelines (section 2.2.6.1).</li> <li>• Provided guidance on WS-Security based on ENISA guidelines, advice from XML Security experts (section 2.2.6.2).</li> <li>• Added test service (section 2.3.7).</li> <li>• Added support for CL3055 (section 2.3.1.1).</li> <li>• Guidance on correlation is now mentioned as an option only, leaving choice between document-oriented and service-oriented exchanges (section 2.3.1.3).</li> <li>• More guidance on certificates (section 2.3.4.4).</li> <li>• Added a section on environments (section 2.3.8).</li> <li>• Added an example message (section 3.1).</li> <li>• Values to be confirmed: five minutes for retries (section 2.2.5), 10 MB total payload size (section 2.3.6)</li> </ul>
V0r3	2013-11-29	PvdE	<ul style="list-style-type: none"> <li>• Textual updates from F2F on 2013-11-21.</li> <li>• Added messaging model diagram (section 2.2.1).</li> <li>• Add note that Pull is not required to summary (section 2.2)</li> <li>• Added a diagram of AS4 message structure (section 2.2.3).</li> <li>• All payloads are carried in separate MIME parts;</li> </ul>

			<p>no support for external payloads; renamed from “attachments” to “payloads” (section 2.2.3.2).</p> <ul style="list-style-type: none"> <li>• The reference to TLS cipher suites is more general (section 2.2.6.1).</li> <li>• Simplified party identifiers, only EIC codes are allowed (section 2.3.1.1).</li> <li>• ENTSOG will publish Service/Action info (section 2.3.1.2).</li> <li>• Guidance on correlation is left to business processes (section 2.3.1.3).</li> <li>• Client authentication not recommended (section 2.3.4.2).</li> <li>• No preferred CA; state the 3072 is for future applications (section 2.3.4.4).</li> <li>• The test service is now in the Usage Profile as it can be provided via configuration (section 2.3.7).</li> <li>• The section on separating environments is simplified (section 2.3.8).</li> <li>• The usage profile on reliable messaging is removed.</li> <li>• Fixed reference to BSI TLS document (section 6).</li> </ul>
V0r4	2013-12-04		<ul style="list-style-type: none"> <li>• Updates based on discussions at F2F, 2013-12-03</li> <li>• Disclaimer added.</li> <li>• In 2.2.1, explained Sender-Receiver concepts are orthogonal to Initiator-Responder.</li> <li>• Updated guidance on payload size.</li> <li>• Added RFC 6176 reference.</li> <li>• Improved wording on environments.</li> <li>• Anonymous EIC codes in example.</li> </ul>
V0r5	2013-12-06	PvdE	<ul style="list-style-type: none"> <li>• Draft finalized in team teleconference.</li> </ul>
V0r6	2014-02-14	PvdE, EJvN	<ul style="list-style-type: none"> <li>• Updates based on team teleconference</li> <li>• Generalized title of 2.3.4.4 and updated content to reflect the new appendix on certificate</li> </ul>

			<p>requirements.</p> <ul style="list-style-type: none"> <li>• Added reference to [BSIALG].</li> <li>• Added discussion on key transport algorithms.</li> <li>• Updated AES encryption from to <a href="http://www.w3.org/2001/04/xmlenc#aes128-cbc">http://www.w3.org/2001/04/xmlenc#aes128-cbc</a> to <a href="http://www.w3.org/2001/04/xmlenc#aes128-gcm">http://www.w3.org/2001/04/xmlenc#aes128-gcm</a> following [XMLENC1].</li> </ul>
V0r7	2014-04-22	PvdE	<p>ENISA comments:</p> <ul style="list-style-type: none"> <li>• In 2.3.4.1, change use of firewalls from MAY to SHOULD.</li> <li>• New section 2.2.7 which recommends IPv6.</li> </ul>
V0r8	2014-07-28	PvdE	<ul style="list-style-type: none"> <li>• The AES-GCM encryption URI is identified using <a href="http://www.w3.org/2009/xmlenc11#aes128-gcm">http://www.w3.org/2009/xmlenc11#aes128-gcm</a>.</li> <li>• Moved the certificate profile into the Usage Profile section.</li> <li>• Minor editorial changes.</li> </ul>
V0r9	2014-07-30	PvdE	<ul style="list-style-type: none"> <li>• Fixed header dates. Accepted all changes to fix Microsoft Word change track formatting errors.</li> </ul>
V1r0	2014-09-22	JDK	<ul style="list-style-type: none"> <li>• Remove “draft” and “not for implementation”. Add reference to PoC in introduction.</li> </ul>
V1r1	2015-03-05	PvdE	<ul style="list-style-type: none"> <li>• New draft V1r1 incorporating first updates for 2015: <ul style="list-style-type: none"> <li>○ Updates on Role, Service, Action based on meeting of 2015-02-17 (section 2.3.1.2).</li> <li>○ Message identifiers to be universally unique (2.2.3.1).</li> </ul> </li> <li>• Updated the example in section 3.1 accordingly.</li> <li>• New profiling for <b>AgreementRef</b>, in support of certificate rollover (section 2.2.3.1 and 2.3.2).</li> <li>• No need to be able to set MessageId, RefToMessageId and ConversationId as we’re not using them (section 2.2.3.1).</li> </ul>



V1r2	2015-03-09	JM, PvdE	<ul style="list-style-type: none"> <li>• Service and Action in example are changed to their coded values.</li> <li>• Corrected the current EDIG@S version to 5.1.</li> <li>• Various spelling corrections.</li> <li>• Profiling for MPC (another feature that is not used currently).</li> <li>• Added missing AgreementRef in message example.</li> <li>• Changed year in timestamps in example to 2016.</li> <li>• In section 2.2.1, the requirement to support Two Way MEPs no longer makes sense as it is inconsistent with the profiling of 2.3.1.3, which says that <i>RefToMessageId is not used</i>. Added a note that it may be added in the future.</li> </ul>
V1r3	2015-03-18	PvdE	<ul style="list-style-type: none"> <li>• Accepted all changes up to and including v1r2 for ease of review.</li> <li>• Added more clarification on Communication vs Business partners.</li> <li>• Changed language on mapping table to not preclude that a future version of the table may be maintained somewhere else/by someone else.</li> <li>• Removed the BRS reference from the mapping table column list.</li> <li>• Added some comments on the relation (degree of overlap) between EDIG@S process categories and ENTSOG Service/Action values.</li> <li>• Added some text for a change (to be confirmed) from using EDIG@S process category names instead of category numbers, and from using Document Type names instead of Document Type code, and of Role names instead of Role codes. These are marked as comments and to be processed before finalizing the document.</li> </ul>
V1r4	2015-03-24	PvdE	<ul style="list-style-type: none"> <li>• In Service example, add a prefix <a href="http://entsog.eu/services/EDIG@S/">http://entsog.eu/services/EDIG@S/</a> to indicate</li> </ul>

			that a Service is based on an EDIG@S service category.
V1r5	2015-04-02	PvdE	<ul style="list-style-type: none"> <li>Accepted all changes up to v1r4 for readability.</li> </ul> <p>Updates based on conference call of 2015-04-01</p> <ul style="list-style-type: none"> <li>In section 2.3.6, introduced the <i>EDIGASDocumentType</i> property and added further profiling of the PartInfo element.</li> <li>Renamed the Service Metadata Mapping Table to ENTSOG AS4 Mapping Table.</li> <li>Introduced the AS4 default action.</li> <li>Changed the example in section 3.1 to use agreed values.</li> <li>Clarified that roles are business roles in 2.3.1.2.4.</li> <li>In 2.3.6, allowed XSDs to be agreed not just per Service/Action, but also for a partner.</li> </ul>
V1r6	17/04/15	JM	<ul style="list-style-type: none"> <li>Accepted some formatting changes and corrected some small editorial errors.</li> </ul>
V1r7	20/04/15	JM	<ul style="list-style-type: none"> <li>Accepted all changes</li> </ul>
V1r8	19/05/15	PvdE	<ul style="list-style-type: none"> <li>New section 2.2.8 on configuration management.</li> </ul>
V1r9	26/5/15	PvdE	<ul style="list-style-type: none"> <li>Update on certificate requirements</li> </ul>
V1r10	2/6/15	PvdE	<ul style="list-style-type: none"> <li>The part property "<i>EDIGASDocumentType</i>" was replaced by an incorrect value in the message example in section 3.1.</li> </ul>
V1r11	09/06/15	JM	<ul style="list-style-type: none"> <li>Updated Service Field in message example with EDIG@S Code</li> </ul>
V1r12	15/06/15	PvDE/JM	<ul style="list-style-type: none"> <li>Improved discussion of ENTSOG AS4 Mapping Table</li> <li>Editorial clean up</li> <li>Updated reference to Network Code to the Commission Regulation 2015/703.</li> <li>Removed a reference to an unpublished</li> </ul>

			<p>overview of certificate standards and requirements.</p> <ul style="list-style-type: none"> <li>Updated Agreement Update reference to ebCore Working Draft.</li> </ul>
V2r0	17/06/15	JM	<ul style="list-style-type: none"> <li>Revised to Version number to 2 for publication</li> </ul>
V2r1	05/01/16	JM	<ul style="list-style-type: none"> <li>Added in confirmation of algorithm requirements</li> </ul>
V2r2	09/06/16	PvdE	<ul style="list-style-type: none"> <li>Type attribute on PartyId in section 2.3.1.1 added.</li> <li>Type attribute on Service in section 2.3.1.2.1 added.</li> <li>In section 2.3.2, provided a URI-based naming conventions for agreements.</li> <li>In section 2.3.6, the schema is fixed for sender and document type for each receiver.</li> <li>In section 2.3.6, added that EDIG@S XML documents are encoded in UTF-8.</li> <li>Updated example in section 3.1.</li> <li>New section 4, PMode table.</li> <li>Updated reference to ebCore AU to current version.</li> </ul>
V2r3	30/06/16	PvdE	<ul style="list-style-type: none"> <li>Removed statement on UTF-8 encoding of EDIG@S</li> <li>Added UTF-8 and BOM clarification to SOAP envelope encoding.</li> <li>In the example in section 3.1, added a missing closing tag <code>&lt;/eb3:Property&gt;</code> and made ConversationId an empty element as per section 2.3.1.3.</li> <li>Added BP20 reference to bibliography.</li> <li>Removed an obsolete duplicate comment on type attribute on PartyId.</li> <li>Added discussion of security token</li> </ul>

			<p>references and indicated a preference for BST in 2.2.6.2.</p> <ul style="list-style-type: none"> <li>• In 2.3.4.3, indicated that parties must select a compatible option for security token references.</li> </ul>
V2r4	19/07/16	ICT KG	<ul style="list-style-type: none"> <li>• Reviewed at ITC KG meeting</li> </ul>
V2r5	22/08/16	JM	<ul style="list-style-type: none"> <li>• Updated Legal Disclaimer</li> </ul>
V2r6	4/10/16	PvdE	<ul style="list-style-type: none"> <li>• Updated status of ebCore Agreement Update, due its approval as Committee Specification in the OASIS ebCore TC</li> <li>• Updated Configuration Management API discussion in section 2.2.8</li> <li>• New section 2.4 on Agreement Update.</li> <li>• Updated discussion of <b>Service</b> and <b>Action</b> also for ebCore messages.</li> <li>• Fixed a typo in section 3.1, message ID was not RFC 2822 compliant.</li> <li>• Many editorial changes, a.o. redundant white space.</li> </ul>
V2.7	18/10/16		<ul style="list-style-type: none"> <li>• Accepted all changes</li> <li>• In 2.2.3.2, changed to reflect that compression is not guaranteed to take place when the compression P-Mode is set.</li> <li>• In 2.2.6.1 changed “support TLS 1.2” to “at least support TLS 1.2”.</li> <li>• In 2.3.1.2.4, added “For business services,”.</li> <li>• In 2.3.1.3, rephrased as “as content the empty string”.</li> <li>• Fixed the wording in the first bullet in 2.3.6.</li> <li>• In section, improved definition of PMode[1].BusinessInfo.Service, Action and Role to include test and AU.</li> </ul>
V2.8	24/10/16	JM	<ul style="list-style-type: none"> <li>• Reviewed and corrected grammatical errors</li> </ul>

			<ul style="list-style-type: none"> <li>Created Rev 3 for publication following ITC KG &amp; INT WG approval</li> </ul>
V2.9	2/11/16	PvdE	<ul style="list-style-type: none"> <li>Minor editorial</li> <li>In section 2.2.3.1, add requirement that a Receiving MSH <b>MUST</b> use AgreementRef to select the P-Mode to use for a message: <i>"A compliant product, acting as Receiver, MUST take the value of the AS4 AgreementRef header into account when selecting the applicable P-Mode."</i> This is needed so that the right certificates are selected.</li> <li>In section 2.3.1.2.4, added the underlined eight words to the sentence <i>"Implementations of this profile MUST use the Service, Action, From/Role and To/Role values to use specified in this table <u>for the data exchanges covered by the table</u>"</i> to explain that for other exchanges, the profile does not apply. This is intended to help users that also want to use AS4 for other exchanges.</li> <li>In section 2.3.4.5, removed "Class 2" terminology for requirements, as the term creates confusion. Some CAs have different categories and/or constraints. The reference to NCP is now the only constraint.</li> <li>Renamed title of section 2.3.4.5.5 to include TLS as well.</li> <li>In 2.3.4.5.4, clarified that many CAs do not support the use of EIC codes as CN in certificates, and that therefore this is not mandatory.</li> <li>In section 2.3.4.5.5, KeyAgreement requirement dropped.</li> <li>In the References section, upgraded to references to the ENISA report from the 2013 to the (most recent) 2014 version.</li> </ul>

V3.0	PvdE		<ul style="list-style-type: none"> <li>• Added back in the 2013 ENISA reference as requested by ITC KG</li> <li>• Approved as v3.0 by ITC KG</li> </ul>
V3r1	PvdE		<ul style="list-style-type: none"> <li>• Updated the references of ETSI ESI European Norms to the current versions.</li> <li>• Some re-structuring of requirements on certificates, making it clear the review process applies to all certificates and CAs.</li> <li>• Harmonized “CA” as abbreviation for <b>Certification</b> Authority.</li> <li>• Mention that EV certificates may be used.</li> <li>• Mentioned options for EIC code in certificate.</li> </ul>
V3r2	PvdE	2016-12-23	<ul style="list-style-type: none"> <li>• Incorporated improvements in the sections on Certificates, TLS and IP networking from the Interactive and Integrated profiles, to create a common base and consistency with the other documents.</li> <li>• New minor section “Networking” in Usage Profile to cover IPv4/IPv6.</li> <li>• Removed reference to private networks, as the network code states that the Internet is to be used and for consistency with other profiles.</li> </ul>
V3.3	PvdE	2017-02-13	<ul style="list-style-type: none"> <li>• Specified the use of the AS4 P-Mode values for <i>Service</i> and <i>Role</i> for situations where the data exchange is not classified. (For <i>Action</i>, the default value was already specified).</li> </ul>
V3.4	PvdE	2017-02-24	<ul style="list-style-type: none"> <li>• Added an example of unclassified exchanges using default Service and Role values in section 3.2. The other example is now in the subsection 3.1.</li> </ul>
V3.5	PvdE	2017-02-24	<ul style="list-style-type: none"> <li>• In section 2.3.6, changed the requirement on presence of the <b>EDIGASDocumentType</b> part property from MUST to SHOULD.</li> </ul>

V3.6	PvdE	2018-03-27	<p>After feedback from implementators, ITC kernel group reviewed all “recommendations” (e.g. SHOULD instead of MUST) and checked whether they could be tightened. This version incorporates the decisions of the ITC KG.</p> <ul style="list-style-type: none"> <li>• Section 2.2.3.1, UUID in MessageId.</li> <li>• Section 2.2.6.2, BinarySecurityToken.</li> <li>• Section 2.2.6.2, Key Transport Algorithms.</li> <li>• Section 2.3.1.1, checking delegation relations.</li> <li>• Section 2.3.4.1, use of firewalls.</li> </ul>
------	------	------------	--

## 1012 **6 References**

- 1013 [AES] Advanced Encryption Standard. FIPS 197. NIST, November 2001.  
1014 <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>
- 1015 [AS4] AS4 Profile of ebMS 3.0 Version 1.0. OASIS Standard, 23 January 2013.  
1016 <http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/profiles/AS4-profile/v1.0/>
- 1017 [AU] ebCore Agreement Update Specification Version 1.0. OASIS Committee  
1018 Specification. 19 September 2016. [http://docs.oasis-open.org/ebcore/ebcore-](http://docs.oasis-open.org/ebcore/ebcore-au/v1.0/)  
1019 [au/v1.0/](http://docs.oasis-open.org/ebcore/ebcore-au/v1.0/)
- 1020 [BP20] Basic Profile Version 2.0. OASIS Committee Specification.  
1021 <http://docs.oasis-open.org/ws-brsp/BasicProfile/v2.0/BasicProfile-v2.0.pdf>
- 1022 [BSIALG] Entwurf Algorithmenkatalog 2014. Bundesamt für Sicherheit in der  
1023 Informationstechnik (BSI). Bonn, 11 Oktober 2013.  
1024 [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ElekSignatur/Algorit-](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ElekSignatur/Algorithmenkatalog_Entwurf_2013.pdf?__blob=publicationFile)  
1025 [menkatalog\\_Entwurf\\_2013.pdf?\\_\\_blob=publicationFile.](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ElekSignatur/Algorithmenkatalog_Entwurf_2013.pdf?__blob=publicationFile)
- 1026 [BSITLS] Mindeststandard des BSI nach § 8 Abs. 1 Satz 1 BSIg für den Einsatz des  
1027 SSL/TLS-Protokolls in der Bundesverwaltung. Bundesamt für Sicherheit in der  
1028 Informationstechnik (BSI). Bonn, 08 Oktober 2013.  
1029 [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_BSI_TLS_1_2_Version_1_0.pdf)  
1030 [Mindeststandard\\_BSI\\_TLS\\_1\\_2\\_Version\\_1\\_0.pdf](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_BSI_TLS_1_2_Version_1_0.pdf)
- 1031 [CABFBRCP] CA Browser Forum: " Baseline Requirements Certificate Policy for the Issuance  
1032 and Management of Publicly-Trusted Certificates ". Latest Version 1.4.1,  
1033 September 2016.  
1034 <https://cabforum.org/baseline-requirements-documents/>
- 1035 [CABFEVV] CA Browser Forum. "Guidelines For The Issuance And Management Of  
1036 Extended Validation Certificates". Latest Version 1.6.0. July 2016.  
1037 <https://cabforum.org/extended-validation/>
- 1038 [CAM] Business Requirements Specification for the Capacity Allocation Mechanism  
1039 (CAM) Network Code. Draft Version 0 Revision 05 – 2012-10-05.
- 1040 [CEM] Certificate Exchange Messaging for EDIINT. Expired Internet-Draft.  
1041 <https://tools.ietf.org/html/draft-meadors-certificate-exchange-14>.
- 1042 [CR2015/703] COMMISSION REGULATION (EU) 2015/703 of 30 April 2015 establishing a  
1043 network code on interoperability and data exchange rules.  
1044 [http://eur-lex.europa.eu/legal-](http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2015.113.01.0013.01.ENG)  
1045 [content/EN/TXT/?uri=uriserv:OJ.L\\_.2015.113.01.0013.01.ENG](http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2015.113.01.0013.01.ENG)
- 1046 [EBMS3] OASIS ebXML Messaging Services Version 3.0: Part 1, Core Features. OASIS  
1047 Standard. 1 October 2007. [http://docs.oasis-open.org/ebxml-](http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/core/os/)  
1048 [msg/ebms/v3.0/core/os/](http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/core/os/)
- 1049 [EDIG@S] EASEE-gas EDIG@S. Version 5.1. <http://www.EDIG@S.org/version-5/>



- 1050 [EGCDN] Common Data Network. EASEE-gas Common Business Practice 2007-002/01.  
1051 [http://easee-gas.eu/docs/cbp/approved/CBP2007-002-01\\_DataNetwork.pdf](http://easee-gas.eu/docs/cbp/approved/CBP2007-002-01_DataNetwork.pdf)
- 1052 [EGMTP] Message Transmission Protocol. EASEE-gas Common Business Practice 2007-  
1053 001/01. [http://easee-gas.eu/docs/cbp/approved/CBP2007-001-](http://easee-gas.eu/docs/cbp/approved/CBP2007-001-01_MessageTransmissionProtocol.pdf)  
1054 [01\\_MessageTransmissionProtocol.pdf](http://easee-gas.eu/docs/cbp/approved/CBP2007-001-01_MessageTransmissionProtocol.pdf)
- 1055 [EIC] ENTSOG. Energy Identification Coding Scheme (EIC) for natural gas  
1056 transmission. Party Codes. <http://www.entsog.eu/eic-codes/eic-party-codes-x>
- 1057 [EN 319 411-1] European Standard. Electronic Signatures and Infrastructures (ESI); Policy  
1058 and security requirements for Trust Service Providers issuing certificates; Part  
1059 1: General requirements, v1.1.1, 2016-02. (Formerly [ETSI EN 319 411-3])  
1060 [http://www.etsi.org/deliver/etsi\\_en/319400\\_319499/31941101/01.01.01\\_60/](http://www.etsi.org/deliver/etsi_en/319400_319499/31941101/01.01.01_60/en_31941101v010101p.pdf)  
1061 [en\\_31941101v010101p.pdf](http://www.etsi.org/deliver/etsi_en/319400_319499/31941101/01.01.01_60/en_31941101v010101p.pdf)
- 1062 [EN 319 412-3] Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3:  
1063 Certificate profile for certificates issued to legal persons.  
1064 [http://www.etsi.org/deliver/etsi\\_en/319400\\_319499/31941203/01.01.01\\_60/](http://www.etsi.org/deliver/etsi_en/319400_319499/31941203/01.01.01_60/en_31941203v010101p.pdf)  
1065 [en\\_31941203v010101p.pdf](http://www.etsi.org/deliver/etsi_en/319400_319499/31941203/01.01.01_60/en_31941203v010101p.pdf)
- 1066 [EN 319 412-4] Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4:  
1067 Certificate profile for web site certificates.  
1068 [http://www.etsi.org/deliver/etsi\\_en/319400\\_319499/31941204/01.01.01\\_60/](http://www.etsi.org/deliver/etsi_en/319400_319499/31941204/01.01.01_60/en_31941204v010101p.pdf)  
1069 [en\\_31941204v010101p.pdf](http://www.etsi.org/deliver/etsi_en/319400_319499/31941204/01.01.01_60/en_31941204v010101p.pdf)
- 1070 [ENISA13] Algorithms, Key Sizes and Parameters Report 2013 recommendations version  
1071 1.0 – October 2013. ENISA. [http://www.enisa.europa.eu/activities/identity-](http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report)  
1072 [and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report](http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report)
- 1073 [ENISA14] Algorithms, Key Size and Parameters Report 2014. November 2014. ENISA.  
1074 [http://www.enisa.europa.eu/activities/identity-and-](http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report)  
1075 [trust/library/deliverables/algorithms-key-sizes-and-parameters-report](http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report)
- 1076 [NOM] Business Requirements Specification for the Nomination (NOM) Network Code.  
1077 Draft Version 0 Revision 9 – 2013-06-04.
- 1078 [OSSLTLS] OpenSSL TLS 1.2 Cipher Suites.  
1079 [http://www.openssl.org/docs/apps/ciphers.html#TLS\\_v1\\_2\\_cipher\\_suites](http://www.openssl.org/docs/apps/ciphers.html#TLS_v1_2_cipher_suites).
- 1080 [RFC2119] A. Ramos. Key words for use in RFCs to Indicate Requirement Levels. IETF RFC  
1081 2119. January 1998. <http://www.ietf.org/rfc/rfc2119.txt>
- 1082 [RFC2822] P. Resnick. Internet Message Format <https://tools.ietf.org/html/rfc2822>
- 1083 [RFC5246] T. Dierks et al. The Transport Layer Security (TLS) Protocol Version 1.2. IETF RFC  
1084 5246. August 2008. <http://tools.ietf.org/html/rfc5246>
- 1085 [RFC6176] S. Turner et al. Prohibiting Secure Sockets Layer (SSL) Version 2.0. RFC 6176.  
1086 March 2011. <http://tools.ietf.org/html/rfc6176>

- 1087 [RFC6555] D. Wing et al. Happy Eyeballs: Success with Dual-Stack Hosts.  
1088 <http://tools.ietf.org/html/rfc6555>
- 1089 [TLSSP] Transport Layer Security (TLS) Parameters. Last Updated 2013-10-03.  
1090 [http://www.iana.org/assignments/tls-parameters/tls-parameters.xml#tls-](http://www.iana.org/assignments/tls-parameters/tls-parameters.xml#tls-parameters-4)  
1091 [parameters-4](http://www.iana.org/assignments/tls-parameters/tls-parameters.xml#tls-parameters-4)
- 1092 [TS119312] ETSI TS 119 312 V1.1.1 Electronic Signatures and Infrastructures (ESI);  
1093 Cryptographic Suites.  
1094 [http://www.etsi.org/deliver/etsi\\_ts/119300\\_119399/119312/01.01.01\\_60/ts\\_](http://www.etsi.org/deliver/etsi_ts/119300_119399/119312/01.01.01_60/ts_119312v010101p.pdf)  
1095 [119312v010101p.pdf](http://www.etsi.org/deliver/etsi_ts/119300_119399/119312/01.01.01_60/ts_119312v010101p.pdf)
- 1096 [WSSSMS] OASIS Web Services Security: SOAP Message Security Version 1.1.1. OASIS  
1097 Standard, May 2012. [http://docs.oasis-open.org/wss-m/wss/v1.1.1/wss-](http://docs.oasis-open.org/wss-m/wss/v1.1.1/wss-SOAPMessageSecurity-v1.1.1.doc)  
1098 [SOAPMessageSecurity-v1.1.1.doc](http://docs.oasis-open.org/wss-m/wss/v1.1.1/wss-SOAPMessageSecurity-v1.1.1.doc)
- 1099 [WSSSWA] OASIS Web Services Security: Web Services Security SOAP Message with  
1100 Attachments (SwA) Profile Version 1.1.1. OASIS Standard, May 2012.  
1101 <http://docs.oasis-open.org/wss-m/wss/v1.1.1/wss-SwAProfile-v1.1.1.doc>
- 1102 [WSSX509] OASIS Web Services Security: Web Services Security X.509 Certificate Token  
1103 Profile Version 1.1.1. OASIS Standard, May 2012.  
1104 [http://docs.oasis-open.org/wss-m/wss/v1.1.1/wss-x509TokenProfile-](http://docs.oasis-open.org/wss-m/wss/v1.1.1/wss-x509TokenProfile-v1.1.1.doc)  
1105 [v1.1.1.doc](http://docs.oasis-open.org/wss-m/wss/v1.1.1/wss-x509TokenProfile-v1.1.1.doc)
- 1106 [XMLDSIG] XML Signature Syntax and Processing (Second Edition). W3C Recommendation  
1107 10 June 2008. <http://www.w3.org/TR/2008/REC-xmlsig-core-20080610>
- 1108 [XMLDSIG1] XML Signature Syntax and Processing Version 1.1. W3C Recommendation 11  
1109 April 2013. <http://www.w3.org/TR/xmlsig-core1/>
- 1110 [XDSIGBP] XML Signature Best Practices. W3C Working Group Note 11 April 2013.  
1111 <http://www.w3.org/TR/2013/NOTE-xmlsig-bestpractices-20130411/>
- 1112 [XMLENC] XML Encryption Syntax and Processing. W3C Recommendation 10 December  
1113 2002. <http://www.w3.org/TR/xmlenc-core/>
- 1114 [XMLENC1] XML Encryption Syntax and Processing Version 1.1. W3C Recommendation 11  
1115 April 2013. <http://www.w3.org/TR/xmlenc-core1/>