

1

ENTSOG AS4 Profile

2

Version 2 Revision 0 – 2015-06-17

3

Disclaimer

4 **This document only provides specific technical information given for indicative purposes**
5 **only and, as such, it is subject to further modifications. The information contained in the**
6 **document is non-exhaustive and non-contractual in nature and subject to the completion**
7 **of the applicable process foreseen for the approval of the EU Regulation embedding the**
8 **Network Code on Interoperability and Data Exchange.**

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

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

44	2.3.4	Security.....	20
45	2.3.4.1	Network Layer Security.....	20
46	2.3.4.2	Transport Layer Security.....	20
47	2.3.4.3	Message Layer Security.....	21
48	2.3.4.4	Certificates and Public Key Infrastructure.....	21
49	2.3.4.5	Certificate Profile.....	22
50	2.3.4.5.1	Key Size.....	22
51	2.3.4.5.2	Key Algorithm.....	22
52	2.3.4.5.3	Naming.....	23
53	2.3.4.5.4	Certificate Body.....	23
54	2.3.4.5.5	Extensions Signing and Encryption End Entities.....	24
55	2.3.4.5.6	Extended Key Usage.....	25
56	2.3.4.5.7	Certificate Lifetime.....	25
57	2.3.5	Message Payload and Flow Profile.....	26
58	2.3.6	Test Service.....	27
59	2.3.7	Environments.....	27
60	3	Example.....	28
61	4	Revision History.....	30
62	5	References.....	36
63			

64 **1 Introduction**

65 COMMISSION REGULATION (EU) 2015/703 of 30 April 2015 establishing a network code on
66 interoperability and data exchange rules published on 30 April 2015 by the European
67 Commission (EC) specifies that “*The following common data exchange solutions shall be used*
68 *[for the communication] protocol: AS4*” [CR2015/703]. This document defines an ENTSOG
69 AS4 Profile that aims to support cross-enterprise collaboration in the gas sector using secure
70 and reliable exchange of business documents based on the AS4 standard [AS4]. This is done
71 by providing an ENTSOG AS4 ebHandler profile and a usage profile for the AS4
72 communication protocol that allow actors in the gas sector to deploy AS4 communication
73 platforms in a consistent and interoperable way.

74 The ENTSOG AS4 Profile has been validated successfully during a Proof of Concept test that
75 took place from May to July 2014 between 7 parties. The outcome was presented on a
76 workshop in Brussels on September 9th 2014.

77 The main goals of this profile are to:

- 78 • Support exchange of EDIG@S XML documents and other payloads.
- 79 • Support business processes of Transmission System Operators for gas, such as
80 Capacity Allocation Mechanism [CAM] and Nomination [NOM], as well as future
81 business processes.
- 82 • Leverage experience gained with other B2B protocols in the gas sector, such as AS2
83 as described in the EASEE-gas implementation guide [EGMTP].
- 84 • Provide security guidance based on state-of-the-art best practices, following
85 recommendations for “near term” (defined as “at least ten years”) future system use
86 [ENISAAKSP].
- 87 • Provide suppliers of AS4-enabled B2B communication solutions with guidance
88 regarding the required AS4 functionality.

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

93 **2 AS4 Profile**

94 This specification defines the ENTSOG AS4 profile as the selection of a specific conformance
95 profile of the AS4 standard [AS4], which is profiled further for increased consistency and
96 ease of configuration, and an AS4 Usage Profile that defines how to use a compliant
97 implementation for gas industry document exchange. Section 2.1 describes the AS4
98 ebHandler Conformance Profile, of which this profile is an extended subset. Section 2.2
99 describes the feature set that conformant products are REQUIRED to support. Section 2.3 is
100 a usage guide that describes configuration and deployment options for conformant
101 products.

102 **2.1 AS4 and Conformance Profiles**

103 **2.1.1 AS4 Standard**

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

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

113 **2.1.2 AS4 ebHandler Conformance Profile**

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

121 **2.2 ENTSOG AS4 ebHandler Feature Set**

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

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

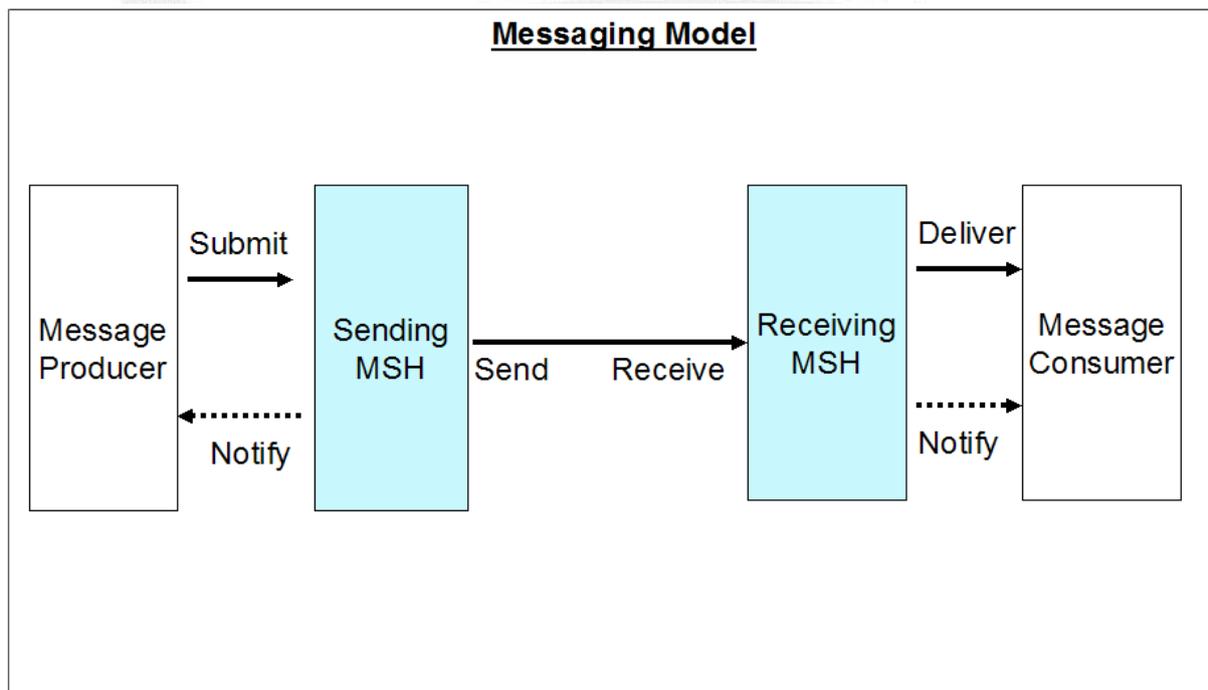
- 129 • There is an added recommendation to support the Two Way Message Exchange
130 Pattern (MEP) (cf. section 2.2.1).
- 131 • Transport Layer Security processing, if handled in the AS4 handler, is profiled (cf.
132 section 2.2.6.1).
- 133 • Algorithms specified for securing messages at the Message Layer are updated to
134 current guidelines (cf. section 2.2.6.2).

135 It also relaxes some requirements:

- 136 • Support for **Pull** mode in AS4 will only be REQUIRED when business processes
137 determine that **Pull** mode exchanges are necessary (cf. section 2.2.2).
- 138 • All payloads are exchanged in separate MIME parts (cf. section 2.2.3.2).
- 139 • Asynchronous reporting of receipts and errors is not REQUIRED (cf. sections 2.2.4,
140 2.2.5).
- 141 • WS-Security support is limited to the X.509 Token Profile (cf. section 2.2.6.2).

142 2.2.1 Messaging Model

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



147
148 **Figure 1 AS4 Messaging Model**

149 Business applications or middleware, acting as *Producer*, *Submit* message content and
150 metadata to the Sending MSH, which packages this content and sends it to the Receiving
151 MSH of the business partner, which in turn *Delivers* the message to another business
152 application that *Consumes* the message content and metadata. Subject to configuration,
153 Sending and Receiving MSH may *Notify Producer* or *Consumer* of particular events. Note that
154 there is a difference between *Sender* and *Initiator*. For **Push** exchanges, the Sending MSH
155 initiates the transmission of the message. For **Pull** exchanges, the transmission is initiated by
156 the Receiving MSH.

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

- 160 • *One Way / Push*

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

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

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

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

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

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

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

173 2.2.2 Message Pulling and Partitioning

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

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

181 This allows implementations of this profile to also support the following Message Exchange
182 Patterns:

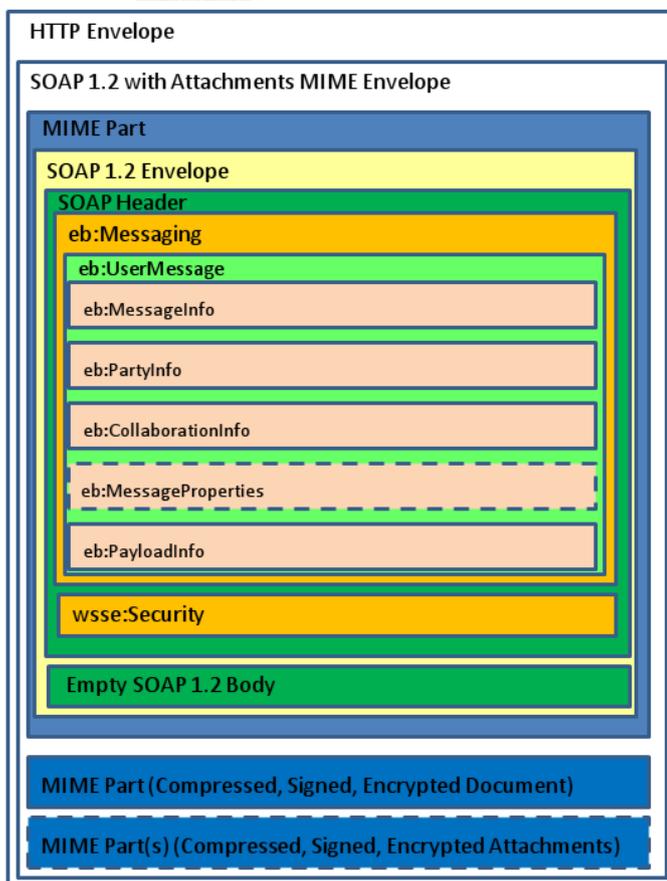
- 183 • *One Way / Pull*
- 184 • *Two Way / Push-and-Pull*

- 185 • *Two Way / Pull-and-Push*
- 186 • *Two Way / Pull-and-Pull*

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

190 2.2.3 Message Packaging

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



194
 195 **Figure 2 AS4 Message Structure**

196 2.2.3.1 UserMessage

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

202 A compliant product MUST allow the Producer, when submitting messages, to set a value for
203 **AgreementRef**, to select a particular PMode.

204 It MUST be able to send and receive messages in which the optional *pmode* attribute of
205 **AgreementRef** is not set.

206 The ebMS3 and AS4 specifications do not constrain the value of **MessageId** beyond
207 conformance to the Internet Message Format [RFC2822], which requires the value to be
208 unique. It is RECOMMENDED that the value be universally unique. Products can do this by
209 including a UUID string in the *id-left* part of the identifier set using randomly (or pseudo-
210 randomly) chosen values.

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

212 **2.2.3.2 Payloads**

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

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

221 **2.2.3.3 Message Compression**

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

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

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

230 **2.2.4 Error Handling**

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

- 233 • The parameter **PMode[1].ErrorHandling.Report.AsResponse** MUST be set to the
234 value *true*.
- 235 • The parameter **PMode[1].ErrorHandling.Report.ProcessErrorNotifyConsumer**
236 SHOULD be set to the value *true*.

237 2.2.5 Reliable Messaging and Reception Awareness

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

- 240 • The parameter **PMode[1].Security.SendReceipt.NonRepudiation** MUST be set to the
241 value *true*.
- 242 • The parameter **PMode[1].Security.SendReceipt.ReplyPattern** MUST be set to the
243 value *Response*.

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

- 247 • The parameter **PMode[1].ReceptionAwareness** MUST be set to *true*.
- 248 • The parameter **PMode[1].ReceptionAwareness.Retry** MUST be set to *true*.
- 249 • The parameter **PMode[1].ReceptionAwareness.DuplicateDetection** MUST be set to
250 *true*.

251 The parameters **PMode[1].ReceptionAwareness.Retry.Parameters** and related
252 **PMode[1].ReceptionAwareness.DuplicateDetection.Parameters** are sets of parameters
253 configuring retries and duplicate detection. These parameters are not fully specified in [AS4]
254 and implementation-dependent. Products MUST support configuration of parameters for
255 retries and duplicate detection.

256 Reception awareness errors generated by the Sender MUST be reported to the Submitting
257 application:

- 258 • The parameter **PMode[1].ErrorHandling.Report.MissingReceiptNotifyProducer**
259 MUST be set to *true*.
- 260 • The parameter **PMode[1].ErrorHandling.Report.SenderErrorsTo** MUST NOT be set.
261 There is no support for reporting sender errors to a third party.

262 2.2.6 Security

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

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

272 2.2.6.1 Transport Layer Security

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

- 276 • When a message is pushed, the Sender authenticates Recipient's server to which the
277 message is pushed
- 278 • When a message is pulled, the Receiver authenticates Sender's server from which the
279 message is pulled

280 Guidance on the use of Transport Layer Security is published in the ENISA Algorithms, Key
281 Sizes and Parameters Report 2013 [ENISAAKSP] and in a Mindest-standard of the Federal
282 Office for Information Security (BSI) [BSITLS]. If TLS is handled by the AS4 message handler
283 (and not offloaded to some infrastructure component), then:

- 284 • It MUST be possible to configure the accepted TLS version(s) in the AS4 message
285 handler. The ENISA and BSI reports state that TLS 1.0 and TLS 1.1 SHOULD NOT be
286 used in new applications. Older version such as SSL 2.0 [RFC6176] and SSL 3.0 MUST
287 NOT be used. Products compliant with this profile MUST therefore support TLS 1.2
288 [RFC5246].
- 289 • It MUST be possible to configure accepted TLS cipher suites in the AS4 message
290 handler. IANA publishes a list of TLS cipher suites [TLSSP], only a subset of which the
291 ENISA Report considers future-proof (see [ENISAAKSP], section 5.1.2). Products MUST
292 support cipher suites included in this subset. Vendors MUST add support for newer,
293 safer cipher suites, as and when such suites are published by IANA/IETF.
- 294 • Support for SSL 3.0 and for cipher suites that are not currently considered secure
295 SHOULD be disabled by default.
- 296 • Perfect Forward Secrecy, which is REQUIRED in [BSITLS], is supported by the
297 TLS_ECDHE_* and TLS_DHE_* cipher suites, which SHOULD be supported.

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

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

307 2.2.6.2 Message Layer Security

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

- 311 • Web Services Security SOAP Message Security [WSSSMS].
- 312 • Web Services Security X.509 Certificate Token Profile [WSSX509].
- 313 • Web Services Security SOAP Message with Attachments (SwA) Profile [WSSSWA].

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

319 AS4 message signing is based on the W3C XML Signature recommendation. AS4 can be
320 configured to use specific digest and signature algorithms based on identifiers defined in this
321 recommendation. At the time of publication of the AS4 standard [AS4], the current version
322 of W3C XML Signature was the June 2008, XML Signature, Second Edition specification
323 [XMLDSIG]. The current version is the April 2013, Version 1.1 specification [XMLDSIG1],
324 which defines important new algorithm identifiers, including identifiers for SHA2, and
325 deprecates SHA1, in line with guidance from ENISA [ENISAAKSP].

326 This ENTISO AS4 profile uses the following AS4 parameters and values:

- 327 • The **PMode[1].Security.X509.Sign** parameter MUST be set in accordance with section
328 5.1.4 and 5.1.5 of [AS4].
- 329 • The **PMode[1].Security.X509.Signature.HashFunction** parameter MUST be set to
330 *http://www.w3.org/2001/04/xmlenc#sha256*.
- 331 • The **PMode[1].Security.X509.Signature.Algorithm** parameter MUST be set to
332 *http://www.w3.org/2001/04/xmlsig-more#rsa-sha256*.

333 This anticipates an update to the AS4 specification to reference this newer specification that
334 has been identified as part of the OASIS AS4 maintenance work.

335 For encryption, WS-Security leverages the W3C XML Encryption recommendation. The
336 following AS4 configuration options configure this feature:

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

342 AS4 also references an older version of XML Encryption than the current one ([XMLENC]
343 instead of [XMLENC1]). However, the AES 128 algorithm [AES] was already referenced in that

344 earlier version. AES is fully consistent with current recommendations for “near term” future
345 system use [ENISAAKSP]. However, the newer W3C specification recommends AES GCM
346 strongly over any CBC block encryption algorithms.

347 Key Transport algorithms are public key encryption algorithms especially specified for
348 encrypting and decrypting keys, such as symmetric keys used for encryption of message
349 content. No parameter is defined to support configuration of key transport in [EBMS3].
350 Implementations are RECOMMENDED to support the following algorithms:

- 351 • For encryption method algorithm, <http://www.w3.org/2009/xmlenc11#rsa-oaep>.
352 This is the algorithm used as value for the *Algorithm* attribute of
353 *xenc:EncryptionMethod* on *xenc:EncryptedKey*.
- 354 • As mask generation function, <http://www.w3.org/2009/xmlenc11#mgf1sha256>. This
355 is the algorithm used as value for the *Algorithm* attribute of *xenc:MGF* in
356 *xenc:EncryptionMethod*.
- 357 • As digest generation function, <http://www.w3.org/2001/04/xmlenc#sha256>. This is
358 the algorithm used as value for the *Algorithm* attribute on *ds:DigestMethod* in
359 *xenc:EncryptionMethod*.

360 2.2.7 Networking

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

364 2.2.8 Configuration Management

365 ENTSOG has identified a requirement for automated exchange and management of AS4
366 configuration data in order to allow parties to negotiate and automate updates to AS4
367 configurations using the exchange of AS4 messages. The main initial requirement is the
368 automated exchange of X.509 certificates. As a prerequisite for an anticipated future
369 agreement update protocol specification for AS4, AS4 products MUST provide an Application
370 Programming Interface (API) to create, read, update and delete AS4 configuration data,
371 including Processing Mode definitions and X.509 certificates used for AS4 message
372 exchanges. In this version of this Usage Profile the API and associated data formats are not
373 required to follow any standard.

374 Based on the ENTSOG requirement, an XML schema for Agreement Updates [AU] has been
375 submitted to the OASIS ebCore Technical Committee for standardization. This proposal is
376 similar to, but different from, earlier work in the IETF defining a Certificate Exchange
377 Message for EDIINT [CEM]. The final outcome of standardisation is not yet available and the
378 XML schema in any future OASIS specification may differ in incompatible ways from the
379 submitted draft. In this version of this Usage Profile, AS4 products are therefore NOT
380 REQUIRED to implement the draft.

381 **2.3 Usage Profile**

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

390 **2.3.1 Message Packaging**

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

392 **2.3.1.1 Party Identification**

393 When exchanging messages in compliance with this profile, parties registered in the ENTSOG
394 Energy Identification Coding Scheme (EIC) for natural gas transmission MUST be identified
395 using the appropriate EIC Code [EIC]. Entities that do not have an EIC code and need to use
396 this profile MUST contact ENTSOG or their local issuing office (LIO) and request an EIC code.
397 This value MUST be used as the content for the **PMode.Initiator.Party** and
398 **PMode.Responder.Party** processing mode parameters, which AS4 message handlers use to
399 populate the **UserMessage/PartyInfo/{From|to}/PartyId** elements.

400 Note that AS4 party identifiers identify the communication partner. The communication
401 partner may be:

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

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

- 405 1. The communication partner may *impersonate* the business entity. In this case the
406 AS4 **Party** identifier is the identifier of the business entity.
- 407 2. The business entity may explicitly *delegate* message processing to the
408 communication partner. In this case the AS4 **Party** identifier is the identifier of the
409 communication partner. Note that, when used to exchange EDIG@S documents, in
410 this case the AS4 party identifier will differ from the value of the EDIG@S
411 *{issuer/recipient}_MarketParticipant.identification* elements, as the latter refer to the
412 business partner.

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

416 The AS4 processing layer will validate the identifiers of Sender and Receiver specified in the
417 ebMS3 headers against P-Mode configurations. This involves the validation of message
418 signatures against configured X.509 certificates. In case of delegation, the X.509 certificates

419 used at the AS4 level relate to the communication partners rather than to business partners
420 on whose behalf the messages are exchanged. The exchanged payloads (EDIG@S or other)
421 typically also reference sending and receiving business entities. The responsibility of
422 determining the validity of implied delegation relations between business document layer
423 entities and entities at the AS4 layer is not in scope for the AS4 message handler, but
424 SHOULD be addressed in business applications or integration middleware.

425 In AS4, it is possible to qualify the Party identifier value using a Party *type* attribute. EIC code
426 values are sufficiently distinct from other codes to not require disambiguation, and this
427 profile does not support other identifier types. Therefore, the *type* attribute MUST NOT be
428 used.

429 **2.3.1.2 Business Process Alignment**

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

432 **2.3.1.2.1 Service**

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

- 441 • For gas business processes, the value content of **Service** is specified in the ENTOSOG
442 AS4 Mapping Table (section 2.3.1.2.4) which MUST be used for AS4 messages
443 carrying specified messages. These values are taken from an EDIG@S process area
444 code list. As not all EDIG@S message exchanges concern TSOs, it may be that not all
445 **Service** values that are needed to fully cover the EDIG@S processes are in the table.
446 The values are constrained to be consistent with [EBMS3], section 5.2.2.8, which
447 requires the values to be a URI if no *type* attribute is present, but does not require
448 the value to be an absolute URI. The example message in section 3 uses the value
449 A06, which is an EDIG@S code representing Nomination and Matching Processes.
- 450 • For services not related to gas business processes, or not related to gas business
451 processes covered by EDIG@S, no convention is defined in or imposed by this Usage
452 Profile. For example, the pre-defined test service (see section 2.3.6) has an absolute
453 **Service** URI value defined in [EBMS3]. The ENTOSOG list (or future versions of it) MAY
454 specify other non-gas business services.
- 455 • For gas business processes, the optional type attribute of Service MUST NOT be used.
456 For other services, the use (or non-use) of the *type* attribute on **Service** is not
457 constrained by this Usage Profile.

458 **2.3.1.2.2 Action**

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

- 460 • For gas business processes in which EDIG@S XML documents are exchanged,
461 ENTSOG provides a value table listing actions (section 2.3.1.2.4). The value for **Action**
462 in that table for a particular exchange **MUST** be used in AS4 messages. The example
463 message in section 3 uses the *http://docs.oasis-open.org/ebxml-*
464 *msg/as4/200902/action* value, which is the default action defined in section 5.2.5 of
465 the AS4 standard [AS4]. As not all EDIG@S message exchanges concern TSOs, it may
466 be that not all **Action** values that are needed to fully cover the EDIG@S business
467 processes are in the service metadata table.
- 468 • For services not related to gas business processes, and for any (hypothetical future)
469 gas business processes not covered by EDIG@S, no convention is defined in or
470 imposed by this Usage Profile. For example, the pre-defined test service (see section
471 2.3.6) has an absolute **Action** URI value defined in [EBMS3].

472 **2.3.1.2.3 Role**

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

- 476 • For gas business processes covered by EDIG@S, the values **MUST** be set to values
477 specified in the ENTSOG AS4 Mapping Table (section 2.3.1.2.4). For gas business
478 processes, that table will relate to information in the EDIG@S document content. In
479 EDIG@S, the sender and receiver role are expressed as EDIG@S header elements. For
480 example, in an EDIG@S v5.1 Nomination document, these are called
481 *issuer_Marketparticipant_marketRole.code* of type *IssuerRoleType* and
482 *recipient_Marketparticipant_marketRole.code* of type *PartyType*.
- 483 • For services not related to gas business processes, or services not covered by
484 EDIG@S, no convention is defined in or imposed by this Usage Profile. For example,
485 the ebMS3 test service **MUST** use the default initiator and responder roles defined in
486 section 5.2.5 of [AS4].

487 **2.3.1.2.4 ENTSOG AS4 Mapping Table**

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

- 490 • EDIG@S process category (e.g. *A06 Nomination and Matching*).
- 491 • EDIG@S XML document schema (e.g. NOMINT).
- 492 • Document type element code for the **type** child element of the EDIG@S document
493 root element (e.g. *ANC*).

- 494 • Document type value defined for the document type element code in the EDIG@S
495 XML schema (e.g. *Forwarded single sided nomination*).
- 496 • **Service** value to use in an AS4 message carrying the EDIG@S document (configured
497 as the PMode[1].BusinessInfo.Service PMode parameter). For gas industry
498 exchanges, the values identify the gas business services that TSOs provide to each
499 other and to other communication partners.
- 500 • **Action** value to use in an AS4 message carrying the EDIG@S document (configured as
501 the PMode[1].BusinessInfo.Action PMode parameter). For exchanges that are
502 modelled in a service-oriented approach, the values identify the operations or
503 activities in a service. For exchanges that are not modelled in a service-oriented
504 approach, the default action [http://docs.oasis-open.org/ebxml-
msg/as4/200902/action](http://docs.oasis-open.org/ebxml-
505 msg/as4/200902/action) specified in the AS4 standard [AS4] will be used.
- 506 • **From/Role** to use in an AS4 message carrying the EDIG@S document (configured as
507 the AS4 PMode.Initiator.Role PMode parameter). This value matches the EDIG@S
508 *recipient_Marketparticipant_marketRole.code* (e.g. *ZSH*). Corresponding sender role
509 code value (e.g. *Shipper*)
- 510 • **To/Role** to use in an AS4 message carrying the EDIG@S document (configured as the
511 AS4 PMode.Responder PMode parameter). This value matches the EDIG@S
512 *issuer_Marketparticipant_marketRole.code* (e.g. *ZSO*). Corresponding receiver role
513 code value (e.g. *Transit System Operator*)

514 Implementations of this profile MUST use the **Service, Action, From/Role** and **To/Role**
515 values to use specified in this table.

516 AS4 Role values MUST indicate business roles. If a Service Provider sends or receives
517 messages on behalf of some other organisation (whether in a delegation or impersonation
518 mode), the AS4 role values used relates to the business role of that other organisation.
519 There is no separate role value for Service Providers.

520 2.3.1.3 Message Correlation

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

- 522 1. **UserMessage/MessageInfo/RefToMessageId** provides a way to express that a
523 message is a response to a single specific previous message. The **RefToMessageId**
524 element is used in response messages in Two Way message exchanges. Whether two
525 exchanges in a business process are modelled as a Two Way exchange or as two One
526 Way exchanges is a decision made in the Business Requirements Specification for the
527 business process. In this version of this Usage Profile, all exchanges are considered
528 One Way.
- 529 2. **UserMessage/CollaborationInfo/ConversationId** provides a more general way to
530 associate a message with an ongoing conversation, without requiring a message to
531 be a response to a single specific previous message, but allowing update messages to
532 existing conversations from both Sender and Receiver of the original message.

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

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

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

540 2.3.2 Agreements

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

- 542 • The element MUST be present in every AS4 message.
- 543 • Its value MUST be agreed between each pair of gas industry parties exchanging AS4
544 messages conforming to this profile.
- 545 • Its value MUST unambiguously identify Sender's X.509 signing certificate and
546 Receiver's X.509 encryption certificate. In other words, if two AS4 messages
547 compliant with this Usage Profile have the same value for this element, they are
548 signed using the same mutually known and agreed signing certificate and their
549 payloads are encrypted using the same mutually known and agreed encryption
550 certificate. This is a deployment constraint on PMode configurations.
- 551 • The attributes *pmode* and *type* MUST NOT be set.

552 Furthermore:

- 553 • It is REQUIRED that for every tuple of <**From/PartyId, From/Role, To/PartyId,**
554 **To/Role, Service, Action, AgreementRef**> values, a unique processing mode is
555 configured. This is another deployment constraint on PMode configurations.
- 556 • For a tuple of <**From/PartyId, From/Role, To/PartyId, To/Role, Service, Action**>
557 values, organisations MAY agree to configure multiple processing modes differing on
558 other PMode parameters such as certificates used, or the URL of endpoints, for
559 different values of **AgreementRef**. This includes the AS4 test service (see section
560 2.3.6), meaning two parties can verify that they have consistent and properly PMode
561 configurations and firewalls for a particular agreement by sending each other AS4
562 test service messages using the corresponding **AgreementRef**.
- 563 • Parties MAY also use different values for **AgreementRef** to target AS4 gateways in
564 different environments (see section 2.3.7), each having a different gateway endpoint
565 URLs.

566 Note that according to [EBMS3] the value of **AgreementRef** MUST be a URI because the type
567 attribute is not set. However, ebMS3 does not require the value to be an absolute URI.

568 2.3.3 MPC

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

- 572 • MAY be present in the AS4 UserMessage. If this is the case, it MUST be set to the
573 value *http://docs.oasis-open.org/ebxml-
574 msg/ebms/v3.0/ns/core/200704/defaultMPC*, which identifies the default MPC, and
575 therefore MUST NOT be set to some other value
- 576 • MAY be omitted from the AS4 UserMessage. This is equivalent to it being present
577 with the default MPC value

578 2.3.4 Security

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

580 2.3.4.1 Network Layer Security

581 This profile is intended to support exchange of AS4 messages using either the public Internet
582 or private data networks for communication. When using the public Internet, each
583 organisation is individually responsible to implement security measures to protect access to
584 its IT infrastructure. Data exchange may use IPv4 or IPv6.

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

- 588 • MUST use static IP addresses (or IP address ranges) for inbound and outbound AS4
589 HTTPS connections.
- 590 • MUST communicate all IP addresses (or IP address ranges) used for outgoing and
591 incoming connections to their trading partners, also covering addresses of any
592 passive nodes in active-passive clusters. Note that the address of the HTTPS endpoint
593 which an AS4 server is to push messages to or pull messages from MAY differ from
594 the address (or addresses) used for outbound connections.
- 595 • MUST notify their trading partners about any IP address changes sufficiently in
596 advance to allow firewall and other configuration changes to be applied.

597 2.3.4.2 Transport Layer Security

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

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

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

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

611 **2.3.4.3 Message Layer Security**

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

- 613 • The **PMode[1].Security.X509.Signature.Certificate** parameter MUST be set to a value
614 matching the requirements specified in section 2.3.4.4.
- 615 • The **PMode[1].Security.X509.Encryption.Certificate** parameter MUST be set to a
616 value matching the requirements specified in section 2.3.4.4.

617 **2.3.4.4 Certificates and Public Key Infrastructure**

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

- 620 • General requirements;
- 621 • Requirements for Transport Layer Security;
- 622 • Requirements for Message Layer Security.

623 The following general requirements apply to all certificates:

- 624 • A three year validity period for end entity certificates is RECOMMENDED.
- 625 • Guidance on size for RSA public keys for future system use indicates a key size of
626 2048 bits [BSIALG] or even 3072 bits [ENISAAKSP] is appropriate. Keys with size less
627 than 2048 bits MUST NOT be used.
- 628 • The signature algorithm used to sign public keys MUST be based on at least the SHA-
629 256 hashing algorithm.

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

- 631 • TLS server certificates for use in production environments MUST be issued by a
632 Certification Authority (CA). This CA SHOULD meet the requirements specified in [EN
633 319 411-1].
- 634 • No additional requirements are placed on TLS client certificates.

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

- 636 • The Message Layer Security certificates for use in production environments MUST be
637 issued by a Certification Authority (CA).

- 638
- Organisations MAY use certificates issued by EASEE-gas.
- 639
- Use of certificates issued by another Certification Authority is subject to review by
- 640
- 641
- 642
- 643
- 644
- The type of certificates MUST be certificates for organisations, for which proof of
- 645
- identity is required (often referred to as “Class 2” certificates).

646 B2B document exchange typically occurs in a community of known entities, where

647 communication between parties and counterparties is secured using pre-agreed certificates.

648 Such an environment is different from open environments, where certificates establish

649 identities for (possibly previously unknown) entities and Certification Authorities play an

650 essential role to establish trust. Entities MUST proactively notify all communication partners

651 of any updates to certificates used, and in turn MUST process any certificate updates from

652 their communication partners. This concerns both regular renewals of certificates at their

653 expiration dates and replacements for revoked certificates.

654 Organisations MAY also use Certificate Revocation Lists (CRL) or the Online Certificate Status

655 Protocol (OCSP). Individual companies should assess the potential impact on the availability

656 of the AS4 service when using such mechanisms, as their use may cause a certificate to be

657 revoked automatically and messages to be rejected.

658 2.3.4.5 Certificate Profile

659 This section defines a profile for X.509 certificates to secure AS4 communication. This profile

660 is consistent with the EASEE-gas certificate profile. For specific requirements, see

661 [ENISAAKSP] and [TS119312].

662 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.

663 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
--------------	-------------------------	-----------------------

664 **2.3.4.5.3 Naming**

665 The following example uses the ENTSOG name as CA. This is only provided as an illustration.
666 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

667 **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 usually 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	M	A unique CA generated number
subject.commonName	EIC code	M	Preferrably the EIC code. Depends on what the CA allows.
subjectPublicKeyInfo.Algorithm	RsaEncryption	M	The encryption algorithm, at least RSA.
subjectPublicKeyInfo.Subject			The public key of the subject.

	tPublicKey			
	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.

668

669 **2.3.4.5.5 Extensions Signing and Encryption 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; note that some CAs 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	M	
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	

Extension Name	Ref RFC 5280	Sign end entity	Encrypt end entity	TLS Client / Server end entity	Comments
otherName					TRUE if applicable.
otherName.type-id					OID = 1.3.6.1.4.1.311.20.2.3 Preferrably the subjectserialnumber followed by ENTSOG serialnumber
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	

670 **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

671 **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

672

673 2.3.5 Message Payload and Flow Profile

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

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

- 684 • In case the **Action** is set to the AS4 default action (see section 2.3.1.2.2) and the
685 exchanged business document is an EDIG@S XML document, for the business
686 document part a **Property** MUST be included in the **PartProperties** with a name
687 *EDIGASDocumentType* set to the same value as the top-level **type** element in the
688 EDIG@S XML document, which is of type *DocumentType*. The mapping from a pair of
689 **From/PartyId** element and *EDIGASDocumentType* property values to XSDs MUST be
690 agreed and unique, allowing Receivers to validate XML documents using a specific
691 (version of an) XML schema for a particular receiver and document type.
- 692 • The part property *EDIGASDocumentType* MUST NOT be used with payloads that are
693 not EDIG@S XML business documents.

694 In case the **Action** is not set to the AS4 default action, the mapping from **Service** and **Action**
695 value pairs to XSDs MUST be unique, allowing Receivers to validate XML documents using a
696 specific XML schema.

697 Some gas data exchanges are traditional batch-scheduled exchanges that can involve very
698 large payloads. The trend in the industry towards service-oriented and event-driven
699 exchanges is leading to more, and more frequent, exchanges, with smaller payloads per
700 exchange. It is expected that the vast majority of payloads will be less than 1 MB in size
701 (prior to compression), with rare exceptions up to 10 MB. The number of messages
702 exchanged over a period, their distribution over time and the peak load/average load ratio,
703 are dependent on business process and other factors. Parties MUST take peak message
704 volumes and maximum message size into account when initially deploying AS4. Parties
705 SHOULD also monitor trends in message traffic for existing processes and anticipate any new
706 business processes being deployed (and the expected increases in message and data
707 volumes), and adjust their deployments accordingly in a timely manner.

708 In practice, there are limitations on the maximum size of payloads that business partners can
709 accept. These limitations may be caused by capabilities of the AS4 message product, or by
710 constraints of the business application, internal middleware, storage or other software or
711 hardware. When designing business processes and document schemas, and when
712 generating content based on those schemas, these requirements SHOULD be taken into
713 account. In particular, business processes in which large amounts of data are exchanged and

714 the business applications supporting these processes SHOULD be designed such that data
715 can be exchanged as a series of related messages, the payload size of each of which does not
716 exceed 10 MB, rather than as a single message carrying a single large payload that could
717 potentially be much larger.

718 2.3.6 Test Service

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

- 721 • **UserMessage/CollaborationInfo/Service** set to *http://docs.oasis-open.org/ebxml-*
722 *msg/ebms/v3.0/ns/core/200704/service*
- 723 • **UserMessage/CollaborationInfo/Action** set to *http://docs.oasis-open.org/ebxml-*
724 *msg/ebms/v3.0/ns/core/200704/test*.

725 This feature MUST be supported so that business partners can perform a basic test of the
726 communication configuration (including security at network, transport and message layer,
727 and reliability) in any environment, including the production environment. This functionality
728 MAY be supported as a built-in feature of the AS4 product. If not, a PMode MUST be
729 configured with these values. The AS4 product MUST be configured so that messages with
730 these values are not delivered to any business application.

731 2.3.7 Environments

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

742

743 3 Example

744 The following non-normative example is included to illustrate the structure of an AS4
745 message conforming to this profile, for a hypothetical `http://docs.oasis-open.org/ebxml-`
746 `msg/as4/200902/action` action invoked by a hypothetical shipper 21X-EU-A-X0A0Y-Z on a
747 hypothetical service A06 exposed by a hypothetical transmission system operator 21X-EU-B-
748 P0Q0R-S. The detailed contents of the `wsse:Security` header is omitted.

```

749 POST /as4handler HTTP/1.1
750 Host: receiver.example.com:8893
751 User-Agent: Turia
752 Content-Type: multipart/related; start="<f8df1904-a6b9-422b-8239-6a971838503f@sender.example.com>";
753 boundary= "c5bae1842d1e"; type="application/soap+xml"
754 Content-Length: 472639
755
756 --c5bae1842d1e
757 Content-Id: <f8df1904-a6b9-422b-8239-6a971838503f@sender.example.com>
758 Content-Type: application/soap+xml; charset="UTF-8"
759
760 <S12:Envelope xmlns:S12="http://www.w3.org/2003/05/soap-envelope"
761 xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
762 xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
763 xmlns:eb3="http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/">
764   <S12:Header>
765     <eb3:Messaging wsu:Id="_18f85fc2-a956-431e-a80e-09a10364871b">
766       <eb3:UserMessage>
767         <eb3:MessageInfo>
768           <eb3:Timestamp>2016-04-03T14:49:28.886Z</eb3:Timestamp>
769           <eb3:MessageId>2016-92105209999001264.example.com</eb3:MessageId>
770         </eb3:MessageInfo>
771         <eb3:PartyInfo>
772           <eb3:From>
773             <eb3:PartyId>21X-EU-A-X0A0Y-Z</eb3:PartyId>
774             <eb3:Role>ZSH</eb3:Role>
775           </eb3:From>
776           <eb3:To>
777             <eb3:PartyId>21X-EU-B-P0Q0R-S</eb3:PartyId>
778             <eb3:Role>ZSO</eb3:Role>
779           </eb3:To>
780         </eb3:PartyInfo>
781         <eb3:CollaborationInfo>
782           <eb3:AgreementRef>2016-3</eb3:AgreementRef>
783           <eb3:Service>A06</eb3:Service>
784           <eb3:Action>http://docs.oasis-open.org/ebxml-msg/as4/200902/action</eb3:Action>
785           <eb3:ConversationId>2016-921</eb3:ConversationId>
786         </eb3:CollaborationInfo>
787         <eb3:PayloadInfo>
788           <eb3:PartInfo href="cid:0b960692-a3c6-4e85-80da-36009d3ae043@sender.example.com">
789             <eb3:PartProperties>
790               <eb3:Property name="MimeType">application/xml</eb3:Property>
791               <eb3:Property name="CharacterSet">utf-8</eb3:Property>
792               <eb3:Property name="CompressionType">application/gzip</eb3:Property>
793               <eb3:Property name="EDIGASDocumentType">01G</eb3:PartProperties>
794             </eb3:PartInfo>
795           </eb3:PayloadInfo>
796         </eb3:UserMessage>
797       </eb3:Messaging>
798     <wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-
799 secext-1.0.xsd"
800     xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-
801 1.0.xsd">
802       <!-- details omitted -->
803     </wsse:Security>
804   </S12:Header>
805   <S12:Body wsu:Id="_b656ef2c-516"/>
806 </S12:Envelope>
807
808 --c5bae1842d1e
809 Content-Id: <0b960692-a3c6-4e85-80da-36009d3ae043@sender.example.com>
810 Content-Type: application/octet-stream

```

811 Content-Transfer-Encoding: binary
812
813 BINARY CIPHER DATA
814 --c5bae1842d1e--



815 **4 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"> • Textual updates from discussions at F2F 2013-11-04. • 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. • Provided guidance for TLS based on ENISA and other guidelines (section 2.2.6.1). • Provided guidance on WS-Security based on ENISA guidelines, advice from XML Security experts (section 2.2.6.2). • Added test service (section 2.3.6). • Added support for CL3055 (section 2.3.1.1). • Guidance on correlation is now mentioned as an option only, leaving choice between document-oriented and service-oriented exchanges (section 2.3.1.3). • More guidance on certificates (section 2.3.4.4). • Added a section on environments (section 2.3.7). • Added an example message (section 3). • Values to be confirmed: five minutes for retries (section 2.2.5), 10 MB total payload size (section 2.3.5)
V0r3	2013-11-29	PvdE	<ul style="list-style-type: none"> • Textual updates from F2F on 2013-11-21. • Added messaging model diagram (section 2.2.1). • Add note that Pull is not required to summary (section 2.2) • Added a diagram of AS4 message structure (section 2.2.3). • All payloads are carried in separate MIME parts;

			<p>no support for external payloads; renamed from “attachments” to “payloads” (section 2.2.3.2).</p> <ul style="list-style-type: none"> • The reference to TLS cipher suites is more general (section 2.2.6.1). • Simplified party identifiers, only EIC codes are allowed (section 2.3.1.1). • ENTSOG will publish Service/Action info (section 2.3.1.2). • Guidance on correlation is left to business processes (section 2.3.1.3). • Client authentication not recommended (section 2.3.4.2). • No preferred CA; state the 3072 is for future applications (section 2.3.4.4). • The test service is now in the Usage Profile as it can be provided via configuration (section 2.3.6). • The section on separating environments is simplified (section 2.3.7). • The usage profile on reliable messaging is removed. • Fixed reference to BSI TLS document (section 5).
V0r4	2013-12-04		<ul style="list-style-type: none"> • Updates based on discussions at F2F, 2013-12-03 • Disclaimer added. • In 2.2.1, explained Sender-Receiver concepts are orthogonal to Initiator-Responder. • Updated guidance on payload size. • Added RFC 6176 reference. • Improved wording on environments. • Anonymous EIC codes in example.
V0r5	2013-12-06	PvdE	<ul style="list-style-type: none"> • Draft finalized in team teleconference.
V0r6	2014-02-14	PvdE, EJvN	<ul style="list-style-type: none"> • Updates based on team teleconference • Generalized title of 2.3.4.4 and updated content to reflect the new appendix on certificate

			<p>requirements.</p> <ul style="list-style-type: none"> • Added reference to [BSIALG]. • Added discussion on key transport algorithms. • Updated AES encryption from to http://www.w3.org/2001/04/xmlenc#aes128-cbc to http://www.w3.org/2001/04/xmlenc#aes128-gcm following [XMLENC1].
V0r7	2014-04-22	PvdE	<p>ENISA comments:</p> <ul style="list-style-type: none"> • In 2.3.4.1, change use of firewalls from MAY to SHOULD. • New section 2.2.7 which recommends IPv6.
V0r8	2014-07-28	PvdE	<ul style="list-style-type: none"> • The AES-GCM encryption URI is identified using http://www.w3.org/2009/xmlenc11#aes128-gcm. • Moved the certificate profile into the Usage Profile section. • Minor editorial changes.
V0r9	2014-07-30	PvdE	<ul style="list-style-type: none"> • Fixed header dates. Accepted all changes to fix Microsoft Word change track formatting errors.
V1r0	2014-09-22	JDK	<ul style="list-style-type: none"> • Remove “draft” and “not for implementation”. Add reference to PoC in introduction.
V1r1	2015-03-05	PvdE	<ul style="list-style-type: none"> • New draft V1r1 incorporating first updates for 2015: <ul style="list-style-type: none"> ○ Updates on Role, Service, Action based on meeting of 2015-02-17 (section 2.3.1.2). ○ Message identifiers to be universally unique (2.2.3.1). • Updated the example in section 3 accordingly. • New profiling for AgreementRef, in support of certificate rollover (section 2.2.3.1 and 2.3.2). • No need to be able to set MessageId, RefToMessageId and ConversationId as we’re not using them (section 2.2.3.1).

V1r2	2015-03-09	JM, PvdE	<ul style="list-style-type: none"> • Service and Action in example are changed to their coded values. • Corrected the current EDIG@S version to 5.1. • Various spelling corrections. • Profiling for MPC (another feature that is not used currently). • Added missing AgreementRef in message example. • Changed year in timestamps in example to 2016. • 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.
V1r3	2015-03-18	PvdE	<ul style="list-style-type: none"> • Accepted all changes up to and including v1r2 for ease of review. • Added more clarification on Communication vs Business partners. • Changed language on mapping table to not preclude that a future version of the table may be maintained somewhere else/by someone else. • Removed the BRS reference from the mapping table column list. • Added some comments on the relation (degree of overlap) between EDIG@S process categories and ENTSOG Service/Action values. • 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.
V1r4	2015-03-24	PvdE	<ul style="list-style-type: none"> • In Service example, add a prefix http://entsog.eu/services/EDIG@S/ to indicate

			that a Service is based on an EDIG@S service category.
V1r5	2015-04-02	PvdE	<ul style="list-style-type: none"> Accepted all changes up to v1r4 for readability. <p>Updates based on conference call of 2015-04-01</p> <ul style="list-style-type: none"> In section 2.3.5, introduced the <i>EDIGASDocumentType</i> property and added further profiling of the PartInfo element. Renamed the Service Metadata Mapping Table to ENTISOG AS4 Mapping Table. Introduced the AS4 default action. Changed the example in section 3 to use agreed values. Clarified that roles are business roles in 2.3.1.2.4. In 2.3.5, allowed XSDs to be agreed not just per Service/Action, but also for a partner.
V1r6	17/04/15	JM	<ul style="list-style-type: none"> Accepted some formatting changes and corrected some small editorial errors.
V1r7	20/04/15	JM	<ul style="list-style-type: none"> Accepted all changes
V1r8	19/05/15	PvdE	<ul style="list-style-type: none"> New section 2.2.8 on configuration management.
V1r9	26/5/15	PvdE	<ul style="list-style-type: none"> Update on certificate requirements
V1r10	2/6/15	PvdE	<ul style="list-style-type: none"> The part property "<i>EDIGASDocumentType</i>" was replaced by an incorrect value in the message example in section 3.
V1r11	09/06/15	JM	<ul style="list-style-type: none"> Updated Service Field in message example with EDIG@S Code
V1r12	15/06/15	PvDE/JM	<ul style="list-style-type: none"> Improved discussion of Entso^g AS4 Mapping Table Editorial clean up Updated reference to Network Code to the Commission Regulation 2015/703. Removed a reference to an unpublished

			<p>overview of certificate standards and requirements.</p> <ul style="list-style-type: none"> Updated Agreement Update reference to ebCore Working Draft.
V2r0	17/06/15	JM	<ul style="list-style-type: none"> Revised to Version number to 2 for publication

816 **5 References**

817

- 818 [AES] Advanced Encryption Standard. FIPS 197. NIST, November 2001.
819 <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>
- 820 [AS4] AS4 Profile of ebMS 3.0 Version 1.0. OASIS Standard, 23 January 2013.
821 <http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/profiles/AS4-profile/v1.0/>
- 822 [AU] ebCore Agreement Update Schema. OASIS ebCore Technical Committee
823 Working Draft. [https://www.oasis-](https://www.oasis-open.org/committees/document.php?document_id=55825)
824 [open.org/committees/document.php?document_id=55825](https://www.oasis-open.org/committees/document.php?document_id=55825)
- 825 [BSIALG] Entwurf Algorithmenkatalog 2014. Bundesamt für Sicherheit in der
826 Informationstechnik (BSI). Bonn, 11 Oktober 2013.
827 [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)
828 [hmenkatalog Entwurf 2013.pdf?__blob=publicationFile.](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ElekSignatur/Algorithmenkatalog_Entwurf_2013.pdf?__blob=publicationFile)
- 829 [BSITLS] Mindeststandard des BSI nach § 8 Abs. 1 Satz 1 BSI für den Einsatz des
830 SSL/TLS-Protokolls in der Bundesverwaltung. Bundesamt für Sicherheit in der
831 Informationstechnik (BSI). Bonn, 08 Oktober 2013.
832 [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)
833 [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)
- 834 [CAM] Business Requirements Specification for the Capacity Allocation Mechanism
835 (CAM) Network Code. Draft Version 0 Revision 05 – 2012-10-05.
- 836 [CEM] Certificate Exchange Messaging for EDIINT. Expired Internet-Draft.
837 [https://tools.ietf.org/html/draft-meadors-certificate-exchange-14.](https://tools.ietf.org/html/draft-meadors-certificate-exchange-14)
- 838 [CR2015/703] COMMISSION REGULATION (EU) 2015/703 of 30 April 2015 establishing a
839 network code on interoperability and data exchange rules.
840 [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)
841 [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)
- 842 [EBMS3] OASIS ebXML Messaging Services Version 3.0: Part 1, Core Features. OASIS
843 Standard. 1 October 2007. [http://docs.oasis-open.org/ebxml-](http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/core/os/)
844 [msg/ebms/v3.0/core/os/](http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/core/os/)
- 845 [EDIG@S] EASEE-gas EDIG@S. Version 5.1. <http://www.EDIG@S.org/version-5/>
- 846 [EGCDN] Common Data Network. EASEE-gas Common Business Practice 2007-002/01.
847 http://easee-gas.eu/docs/cbp/approved/CBP2007-002-01_DataNetwork.pdf
- 848 [EGMTP] Message Transmission Protocol. EASEE-gas Common Business Practice 2007-
849 001/01. [http://easee-gas.eu/docs/cbp/approved/CBP2007-001-](http://easee-gas.eu/docs/cbp/approved/CBP2007-001-01_MessageTransmissionProtocol.pdf)
850 [01_MessageTransmissionProtocol.pdf](http://easee-gas.eu/docs/cbp/approved/CBP2007-001-01_MessageTransmissionProtocol.pdf)
- 851 [EIC] ENTSOG. Energy Identification Coding Scheme (EIC) for natural gas
852 transmission. Party Codes. <http://www.entsog.eu/eic-codes/eic-party-codes-x>

- 853 [EN 319 411-1] Draft European Standard. Electronic Signatures and Infrastructures (ESI);
854 Policy and security requirements for Trust Service Providers issuing certificates;
855 Part 1: Policy requirements for Certification Authorities issuing web site
856 certificates, v0.0.4, 2013-11.
857 [http://docbox.etsi.org/esi/Open/Latest_Drafts/prEN-319411-1v004-Policy-req-
for-CA-issuing-website-cert-STABLE-DRAFT.pdf](http://docbox.etsi.org/esi/Open/Latest_Drafts/prEN-319411-1v004-Policy-req-
858 for-CA-issuing-website-cert-STABLE-DRAFT.pdf)
- 859 [EN 319 411-3] European Standard. Electronic Signatures and Infrastructures (ESI); Policy
860 and security requirements for Trust Service Providers issuing certificates; Part
861 3: Policy requirements for Certification Authorities issuing public key
862 certificates, v1.1.1, 2013-01. (Formerly [ETSI TS 102 042])
863 [http://www.etsi.org/deliver/etsi_EN/319400_319499/31941103/01.01.01_60/
EN_31941103v010101p.pdf](http://www.etsi.org/deliver/etsi_EN/319400_319499/31941103/01.01.01_60/
864 EN_31941103v010101p.pdf)
- 865 [ENISAAKSP] Algorithms, Key Sizes and Parameters Report 2013 recommendations version
866 1.0 – October 2013. ENISA. [http://www.enisa.europa.eu/activities/identity-
and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report](http://www.enisa.europa.eu/activities/identity-
867 and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report)
- 868 [NOM] Business Requirements Specification for the Nomination (NOM) Network Code.
869 Draft Version 0 Revision 9 – 2013-06-04.
- 870 [OSSLTLS] OpenSSL TLS 1.2 Cipher Suites.
871 http://www.openssl.org/docs/apps/ciphers.html#TLS_v1_2_cipher_suites.
- 872 [RFC2119] A. Ramos. Key words for use in RFCs to Indicate Requirement Levels. IETF RFC
873 2119. January 1998. <http://www.ietf.org/rfc/rfc2119.txt>
- 874 [RFC2822] P. Resnick. Internet Message Format <https://tools.ietf.org/html/rfc2822>
- 875 [RFC5246] T. Dierks et al. The Transport Layer Security (TLS) Protocol Version 1.2. IETF RFC
876 5246. August 2008. <http://tools.ietf.org/html/rfc5246>
- 877 [RFC6176] S. Turner et al. Prohibiting Secure Sockets Layer (SSL) Version 2.0. RFC 6176.
878 March 2011. <http://tools.ietf.org/html/rfc6176>
- 879 [RFC6555] D. Wing et al. Happy Eyeballs: Success with Dual-Stack Hosts.
880 <http://tools.ietf.org/html/rfc6555>
- 881 [TLSSP] Transport Layer Security (TLS) Parameters. Last Updated 2013-10-03.
882 [http://www.iana.org/assignments/tls-parameters/tls-parameters.xml#tls-
parameters-4](http://www.iana.org/assignments/tls-parameters/tls-parameters.xml#tls-
883 parameters-4)
- 884 [TS119312] ETSI TS 119 312 V1.1.1 Electronic Signatures and Infrastructures (ESI);
885 Cryptographic Suites.
886 [http://www.etsi.org/deliver/etsi_ts/119300_119399/119312/01.01.01_60/ts
119312v010101p.pdf](http://www.etsi.org/deliver/etsi_ts/119300_119399/119312/01.01.01_60/ts
887 119312v010101p.pdf)
- 888 [WSSSMS] OASIS Web Services Security: SOAP Message Security Version 1.1.1. OASIS
889 Standard, May 2012. [http://docs.oasis-open.org/wss-m/wss/v1.1.1/wss-
SOAPMessageSecurity-v1.1.1.doc](http://docs.oasis-open.org/wss-m/wss/v1.1.1/wss-
890 SOAPMessageSecurity-v1.1.1.doc)

- 891 [WSSSWA] OASIS Web Services Security: Web Services Security SOAP Message with
892 Attachments (SwA) Profile Version 1.1.1. OASIS Standard, May 2012.
893 <http://docs.oasis-open.org/wss-m/wss/v1.1.1/wss-SwAProfile-v1.1.1.doc>
- 894 [WSSX509] OASIS Web Services Security: Web Services Security X.509 Certificate Token
895 Profile Version 1.1.1. OASIS Standard, May 2012.
896 [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)
897 [v1.1.1.doc](http://docs.oasis-open.org/wss-m/wss/v1.1.1/wss-x509TokenProfile-v1.1.1.doc)
- 898 [XMLDSIG] XML Signature Syntax and Processing (Second Edition). W3C Recommendation
899 10 June 2008. <http://www.w3.org/TR/2008/REC-xmlsig-core-20080610>
- 900 [XMLDSIG1] XML Signature Syntax and Processing Version 1.1. W3C Recommendation 11
901 April 2013. <http://www.w3.org/TR/xmlsig-core1/>
- 902 [XDSIGBP] XML Signature Best Practices. W3C Working Group Note 11 April 2013.
903 <http://www.w3.org/TR/2013/NOTE-xmlsig-bestpractices-20130411/>
- 904 [XMLENC] XML Encryption Syntax and Processing. W3C Recommendation 10 December
905 2002. <http://www.w3.org/TR/xmlenc-core/>
- 906 [XMLENC1] XML Encryption Syntax and Processing Version 1.1. W3C Recommendation 11
907 April 2013. <http://www.w3.org/TR/xmlenc-core1/>
- 908