



1

ENTSOG AS4 Profile

2

Draft Version 3.5 – ~~2016-02-24~~ – 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.

14		Table of contents	
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	11
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.....	<u>1514</u>
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.....	<u>4847</u>
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:

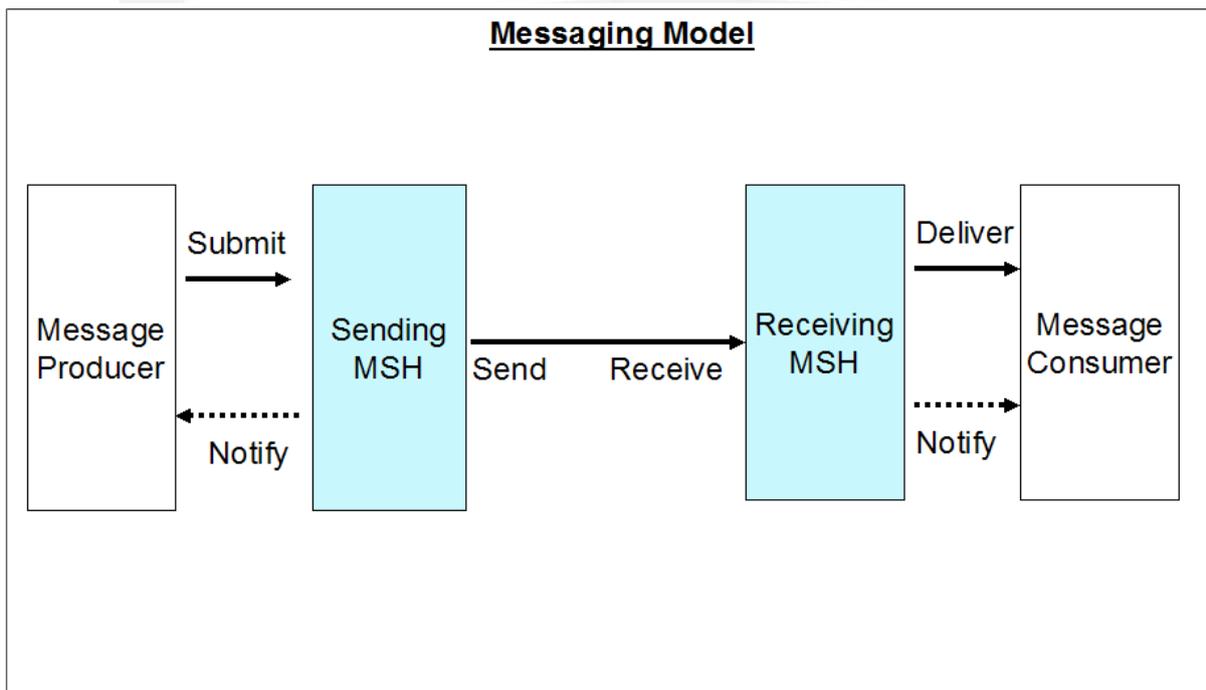
- 139 • There is an added recommendation to support the Two Way Message Exchange
- 140 Pattern (MEP) (cf. section 2.2.1).
- 141 • Transport Layer Security processing, if handled in the AS4 handler, is profiled (cf.
- 142 section 02-2-6-1).
- 143 • Algorithms specified for securing messages at the Message 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 ENTSOG 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

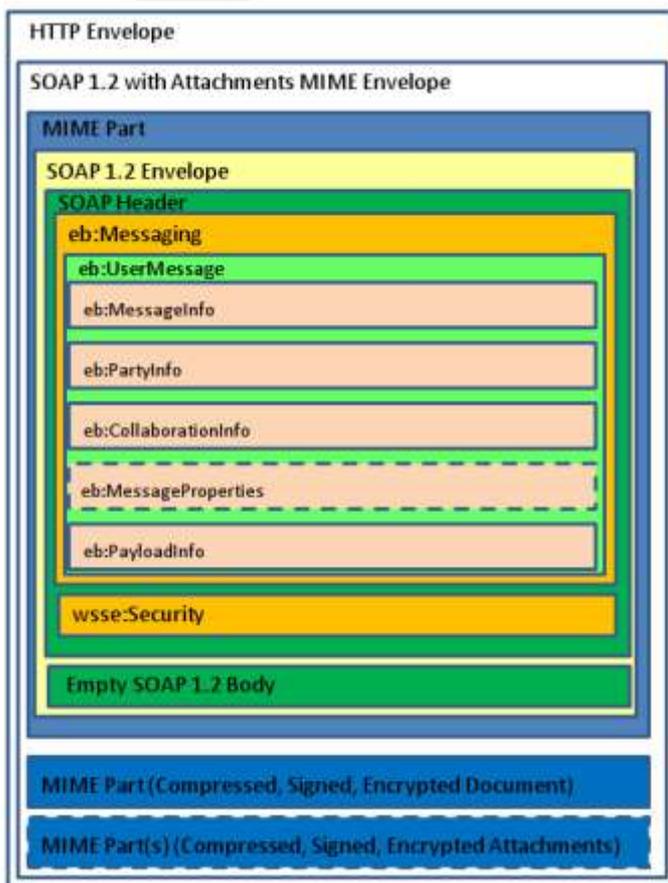
199 exchanges (see section 2.2.1) with the Pull feature.

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. ~~It is RECOMMENDED that the value be universally unique.~~ Products can do this by
224 including a UUID string in the id-left part of the identifier set using randomly (or pseudo-
225 randomly) chosen values.

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

227 2.2.3.2 Payloads

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

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

236 2.2.3.3 Message Compression

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

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

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

245 2.2.4 Error Handling

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

248 • The parameter PMode[1].ErrorHandling.Report.AsResponse MUST be set to the
249 value true.

250 • The parameter PMode[1].ErrorHandling.Report.ProcessErrorNotifyConsumer
251 SHOULD be set to the value true.

252 2.2.5 Reliable Messaging and Reception Awareness

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

255 • The parameter PMode[1].Security.SendReceipt.NonRepudiation MUST be set to the
256 value true.

257 • The parameter PMode[1].Security.SendReceipt.ReplyPattern MUST be set to the
258 value Response.

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

262 • The parameter PMode[1].ReceptionAwareness MUST be set to true.

263 • The parameter PMode[1].ReceptionAwareness.Retry MUST be set to true.

264 • The parameter PMode[1].ReceptionAwareness.DuplicateDetection MUST be set to
265 true.

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

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

273 • The parameter PMode[1].ErrorHandling.Report.MissingReceiptNotifyProducer
274 MUST be set to true.

275 • The parameter PMode[1].ErrorHandling.Report.SenderErrorsTo MUST NOT be set.
276 There is no support for reporting sender errors to a third party.

277 2.2.6 Security

278 AS4 message exchanges can be secured at multiple communication layers: the network
279 layer, the transport layer, the message layer and the payload layer. The first and last of these
280 are not normally handled by B2B communication software and therefore out of scope for

281 this section. Transport layer security is addressed, even though its functionality MAY be
282 offloaded to another infrastructure component.

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

287 ~~N.B. Following consultation with ENISA – The algorithm requirements will change from~~
288 ~~recommended to mandatory in a future approved version of the profile.~~

289 2.2.6.1 Transport Layer Security

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

- 293 • When a message is pushed, the Sender authenticates **Recipient's** server to which the
294 message is pushed
- 295 • When a message is pulled, the Receiver authenticates **Sender's** server from which the
296 message is pulled

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

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

318 MUST follow web security developments and MUST continually upgrade security
319 measures as new general vulnerabilities become known.

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

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

329 2.2.6.2 Message Layer Security

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

- 333 • Web Services Security SOAP Message Security [WSSSMS].
- 334 • Web Services Security X.509 Certificate Token Profile [WSSX509].
- 335 • Web Services Security SOAP Message with Attachments (SwA) Profile [WSSSWA].

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

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

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

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

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

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

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

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

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

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

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

394 2.2.7 Networking

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

398 2.2.8 Configuration Management

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

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

408 2.3 Usage Profile

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

417 2.3.1 Message Packaging

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

419 2.3.1.1 Party Identification

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

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

432 1. The entity involved in the business transaction

433 2. A third party providing B2B communication services for other entities

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

435 1. The communication partner may impersonate the business entity. In this case the
436 AS4 Party identifier is the identifier of the business entity.

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

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

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

455 2.3.1.2 Business Process Alignment

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

458 2.3.1.2.1 Service

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

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

- 468 • For gas business processes covered by EDIG@S, the value content of Service is
469 specified in the ENTSOG AS4 Mapping Table (section 2.3.1.2.4) which MUST be used

470 for AS4 messages carrying specified messages. These values are taken from an
471 EDIG@S process area code list. As not all EDIG@S message exchanges concern TSOs,
472 it may be that not all Service values that are needed to fully cover the EDIG@S
473 processes are in the table. The example message in section 3.1 uses the value A06,
474 which is an EDIG@S code representing Nomination and Matching Processes.

- 475 • For the pre-defined test service (see section [2.3.7.2-3.6](#)), the absolute Service URI
476 value <http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/service>
477 defined in [EBMS3] MUST be used. This value is a URI used as an identifier only. It
478 does not resolve to content on the OASIS web site.
- 479 • For ebCore Agreement Update messages used for certificate exchange (see section
480 2.4), the absolute Service URI value [http://docs.oasis-](http://docs.oasis-open.org/ebcore/ns/CertificateUpdate/v1.0)
481 [open.org/ebcore/ns/CertificateUpdate/v1.0](http://docs.oasis-open.org/ebcore/ns/CertificateUpdate/v1.0) defined in [AU], section 4.1, MUST be
482 used. This value is a URI used as an identifier only. It is not a URL that resolves to
483 content on the OASIS web site.
- 484 • For other services not related to gas business processes, or not related to gas
485 business processes covered by EDIG@S, no convention is defined in or imposed by
486 this Usage Profile. The ENTSOG list (or future versions of it) MAY specify other non-
487 gas business services.

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

- 489 • For gas business processes covered by EDIG@S, the value MUST be the fixed value
490 <http://edigas.org/service>. This value is a URI used as an identifier only. It does not
491 resolve to a URL on the EDIGAS web sites
- 492 • For other services, the use (or non-use) of the type attribute on Service is not
493 constrained by this Usage Profile.

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

500 2.3.1.2.2 Action

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

- 502 • For gas business processes covered by EDIG@S in which EDIG@S XML documents are
503 exchanged, ENTSOG provides a value table listing actions (section 2.3.1.2.4). The
504 value for Action in that table for a particular exchange MUST be used in AS4
505 messages. The example messages in section [3.13](#) use the [http://docs.oasis-](http://docs.oasis-open.org/ebxml-msg/as4/200902/action)
506 [open.org/ebxml-msg/as4/200902/action](http://docs.oasis-open.org/ebxml-msg/as4/200902/action) value, which is the default action defined in
507 section 5.2.5 of the AS4 standard [AS4]. As not all EDIG@S message exchanges

508 concern TSOs, it may be that not all Action values that are needed to fully cover the
509 EDIG@S business processes are in the service metadata table.

- 510 • For the pre-defined test service (see section 2.3.72-3-6) the absolute Action URI value
511 <http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/test> defined in
512 [EBMS3] MUST be used. This value is a URI used as an identifier only. It is not a URL
513 that resolves to content on the OASIS web site.
- 514 • For ebCore Agreement Update messages used for certificate exchange, the Action
515 values UpdateCertificate, ConfirmCertificateUpdate and RejectCertificateUpdate
516 defined in [AU], section 4.1, MUST be used.
- 517 • For other services not related to gas business processes, and for any (hypothetical
518 future) gas business processes not covered by EDIG@S, no convention is defined in
519 or imposed by this Usage Profile.

520 2.3.1.2.3 Role

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

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

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

544 The non-normative example in section 3.1 uses the value “ZSH” for the initiating role header
545 element (EDIG@S code for Shipper) and “ZSO” (EDIG@S code for Transmission System

546 Operator) for the responding role header element. The other non-normative example in
547 section 3.2 uses the AS4 default P-Mode parameter values.

548 2.3.1.2.4 ENTSOG AS4 Mapping Table

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

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

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

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

581 2.3.1.3 Message Correlation

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

583 1. UserMessage/MessageInfo/RefToMessageId provides a way to express that a
584 message is a response to a single specific previous message. The RefToMessageId
585 element is used in response messages in Two Way message exchanges. Whether two
586 exchanges in a business process are modelled as a Two Way exchange or as two One
587 Way exchanges is a decision made in the Business Requirements Specification for the
588 business process. In this version of this Usage Profile, all exchanges are considered
589 One Way.

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

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

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

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

601 2.3.2 Agreements

602 The AgreementRef element is profiled as follows:

- 603 • The element MUST be present in every AS4 message.
- 604 • Its value MUST be agreed between each pair of gas industry parties exchanging AS4
605 messages conforming to this profile.
- 606 • In ebMS3, in principle, any value will do as long as, between two parties, the selected
607 identifier is unique and therefore distinguishes messaging using one agreement from
608 messages using another. For consistency, it is RECOMMENDED to use the following
609 URI naming convention:
610 `http://entsog.eu/communication/agreements/<EIC_CODE_Party_A>/<EIC_CODE_Par`
611 `ty_B>/<version>`
612 where EIC_CODE_Party_A is the EIC code of the party that alphabetically precedes
613 EIC_CODE_Party_B of the other party, the version number is initially 1 and
614 increments for any update.
- 615 • Its value MUST unambiguously identify each party's X.509 signing certificate and
616 X.509 encryption certificate. In other words, if two AS4 messages from P1 to P2
617 compliant with this Usage Profile have the same value for this element, they are
618 signed using the same mutually known and agreed signing certificate (for P1) and
619 their payloads are encrypted using the same mutually known and agreed encryption
620 certificate (for P2). This is a deployment constraint on P-Mode configurations, in
621 support of the introduction of the ebCore Agreement Update protocol [AU].

- 622
- The attributes pmode and type MUST NOT be set.

623 Furthermore:

- 624
- It is REQUIRED that for every tuple of <From/PartyId, From/Role, To/PartyId, To/Role, Service, Action, AgreementRef> values, a unique processing mode is configured. This is another deployment constraint on P-Mode configurations.
- 625
- For a tuple of <From/PartyId, From/Role, To/PartyId, To/Role, Service, Action>
- 626
- For a tuple of <From/PartyId, From/Role, To/PartyId, To/Role, Service, Action> values, organisations MAY agree to configure multiple processing modes differing on other P-Mode parameters such as certificates used, or the URL of endpoints, for different values of AgreementRef. This includes the AS4 test service (see section [2.3.72-3.6](#)), meaning two parties can verify that they have consistent and properly configured P-Modes and firewalls for a particular agreement by sending each other AS4 test service messages using the corresponding AgreementRef.
- 627
- Parties MAY also use different values for AgreementRef to target AS4 gateways in different environments (see section [2.3.82-3.7](#)), each having a different gateway endpoint URL and possibly certificates.
- 628
- 629
- 630
- 631
- 632
- 633
- 634
- 635
- 636

637 2.3.3 MPC

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

- 641
- MAY be present in the AS4 UserMessage. If this is the case, it MUST be set to the value <http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/defaultMPC>, which identifies the default MPC, and therefore MUST NOT be set to some other value
- 642
- MAY be omitted from the AS4 UserMessage. This is equivalent to it being present with the default MPC value
- 643
- 644
- 645
- 646

647 2.3.4 Security

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

649 2.3.4.1 Network Layer Security

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

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

- 656
- MUST use static IP addresses (or IP address ranges) for inbound and outbound AS4
657 HTTPS connections.

- 658
- 659
- 660
- 661
- 662
- 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.
- 663
- MUST notify their trading partners about any IP address changes sufficiently in advance to allow firewall and other configuration changes to be applied.
- 664

665 2.3.4.2 Transport Layer Security

666 | The Transport Layer Security settings defined in section 02-2-6-1 MAY be implemented in the
667 AS4 communication server but TLS MAY also be offloaded to a separate infrastructure
668 component (such as a firewall, proxy server or router). In that case, the recommendations
669 | on TLS version and cipher suites of 02-2-6-1 MUST be addressed by that component.

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

672 | The TLS cipher suites recommended in section 02-2-6-1 are supported in recent versions of
673 TLS toolkits and which therefore are available for use. Support for these suites is
674 RECOMMENDED. Whether or not less secure cipher suites (which are only recommended for
675 legacy applications) are allowed is a local policy decision.

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

679 2.3.4.3 Message Layer Security

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

- 681
- The PMode[1].Security.X509.Signature.Certificate parameter MUST be set to a value matching the requirements specified in section 2.3.4.4.
- 682
- 683
- The PMode[1].Security.X509.Encryption.Certificate parameter MUST be set to a value matching the requirements specified in section 2.3.4.4.
- 684
- If a product allows selection of the type of security token reference, it MUST be set to a type supported by the counterparty.
- 685
- 686

687 2.3.4.4 Certificates and Public Key Infrastructure

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

- 690
- General requirements;
- 691
- Requirements for Transport Layer Security;
- 692
- Requirements for Message Layer Security.

693 The following general requirements apply to all certificates:

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

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

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

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

- 716 • Organisations MAY use a certificate issued by EASEE-gas.
- 717 • The type of certificate MUST be certificates for organisations, for which proof of
718 identity is required.
- 719 • The issued certificate SHOULD comply with the certificate profile defined in [EN 319
720 412-3].

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

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

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

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

738 2.3.4.5 Certificate Profile

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

742 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.

743 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

744 2.3.4.5.3 Naming

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

Entiteit	Example Value	Comments
Root-CA	C=BE	ISO country code (ISO 3166)
	O=ENTSGOG	Name of the Organisation
	CN=ENTSGOG 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
--	-----	--------------------

747 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 319 412-3EN 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.

748

749 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	
digitalSignature		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.
keyEncipherment		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.
dataEncipherment		X	x	X	
keyAgreement		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

Extension Name	Ref RFC 5280	Sign end entity	Encrypt end entity	TLS Client / Server end entity	Comments
					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	

750 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

751 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

752 2.3.5 Networking

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

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

760 2.3.6 Message Payload and Flow Profile

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

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

- 771 • For gas business processes covered by EDIG@S, in which the value content of Service
772 is specified in the ENTSOG AS4 Mapping Table, the Action is set to the default action
773 and the exchanged business document is an EDIG@S XML document (section
774 2.3.1.2.4), for the business document part a Property SHOULD be included in the
775 PartProperties with a name EDIGASDocumentType set to the same value as the top-
776 level type element in the EDIG@S XML document, which is of type DocumentType.
777 The mapping from a combination of From/PartyId element, To/PartyId and
778 EDIGASDocumentType property values to XSDs MUST be agreed and unique, allowing
779 Receivers to validate XML documents using a specific (version of an) XML schema for
780 a particular sender, receiver and document type.
- 781 • The part property EDIGASDocumentType MUST NOT be used with payloads that are
782 not EDIG@S XML business documents.
- 783 • When using the ebMS3 test service (see section ~~2.3.72-3.6~~), no XML schema
784 constraints apply to any of the included payloads.
- 785 • For certificate exchange (see section 2.4), the XML schemas specified in the ebCore
786 Agreement Update [AU] specification for certificate update request, update
787 acceptance and update exception MUST be used with, respectively, the
788 UpdateCertificate, ConfirmCertificateUpdate and RejectCertificateUpdate values for
789 Action.
- 790 • For other services, in case the Action is not set to the AS4 default action, the
791 mapping from Service and Action value pairs to XSDs MUST be unique, allowing
792 Receivers to validate XML documents using a specific XML schema.

793 Some gas data exchanges are traditional batch-scheduled exchanges that can involve very
794 large payloads. The trend in the industry towards service-oriented and event-driven
795 exchanges is leading to more, and more frequent, exchanges, with smaller payloads per

796 exchange. It is expected that the vast majority of payloads will be less than 1 MB in size
797 (prior to compression), with rare exceptions up to 10 MB. The number of messages
798 exchanged over a period, their distribution over time and the peak load/average load ratio,
799 are dependent on business process and other factors. Parties MUST take peak message
800 volumes and maximum message size into account when initially deploying AS4. Parties
801 SHOULD also monitor trends in message traffic for existing processes and anticipate any new
802 business processes being deployed (and the expected increases in message and data
803 volumes), and adjust their deployments accordingly in a timely manner.

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

814 2.3.7 Test Service

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

- 817 • UserMessage/CollaborationInfo/Service set to <http://docs.oasis-open.org/ebxml->
818 [msg/ebms/v3.0/ns/core/200704/service](http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/service)
- 819 • UserMessage/CollaborationInfo/Action set to <http://docs.oasis-open.org/ebxml->
820 [msg/ebms/v3.0/ns/core/200704/test](http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/test).

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

828 2.3.8 Environments

829 B2B data exchange solutions are part of the overall IT service lifecycle, in which different
830 environments are operated (typically in parallel) for development, test, pre-production (in
831 some companies referred to as “acceptance environments” or “QA environments”) and
832 production. Development and test are typically internal environments in which trading
833 partners are simulated using stubs. When exchanging messages between organisations (in
834 either pre-production or production environments), they must target the appropriate
835 environment. In order to prevent a configuration error from causing non-production

836 messages to be delivered to production environments or vice versa, organisations SHOULD
837 configure processing modes at message handlers so that messages from one type of
838 environment cannot be accepted inadvertently in a different type of environment.

839 2.4 ebCore Agreement Update

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

846 2.4.1 Mandatory Support

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

851 Support for ebCore Agreement Update requirement entails the following:

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

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

866 It is NOT REQUIRED to implement a fully automated process to process certificate updates.
867 Organizations MAY implement a process that involves approval or other manual steps to
868 process certificate updates.

869 2.4.2 Implementation Guidelines

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

- 871 • A party MUST obtain the new certificate that it intends to replace an existing
872 certificate with significantly in advance of the expiration date of the certificate to be
873 replaced.

- 874
- 875
- 876
- 877
- Once a party has obtained the new certificate, parties MUST determine the communication partners and agreements that are using the old certificate. To each of these partners, and for all agreements, the party SHOULD send a Certificate Update Request as soon as possible.
- 878
- 879
- 880
- 881
- 882
- 883
- 884
- The ActivateBy value in the update requests MUST be set such that the period in which the request is to be processed is sufficiently long. The definition of “sufficiently long” is partner-dependent, but should take into account that the process on the partner side may be a (partly) manual process. Therefore, time for validation of the request, including validation of the certificate and the issuing Certification Authority; time to create and perform a change request within the partner organization SHOULD be taken into account.
- 885
- 886
- 887
- The specific ActivateBy value MUST be set to a date and time acceptable to the receiving organization. This MAY depend on working hours and staff availability, release schedules etc.
- 888
- 889
- 890
- When an updated agreement has been created and agreed, it MUST first be tested using the test service, as described in section ~~2.3.72-3.6~~ of this document and section 3.5 of [AU]. These tests MUST cover test messages in both directions.
- 891
- 892
- 893
- 894
- The ActivateBy value SHOULD be set to a date and time sufficiently in advance to the expiration data and time of the old agreement, such that a fall-back to the old agreement, and any necessary troubleshooting, is possible in case any blocking issue occurs during tests.
- 895
- 896
- 897
- If the updated agreement has been tested successfully, the regular message flow that used the old agreement SHOULD be re-deployed to the new agreement. The old agreement SHOULD NOT be used any more for new exchanges.
- 898
- 899
- The ebCore Agreement also provides an explicit Agreement Termination feature. Use of this feature is NOT REQUIRED, but may be agreed bilaterally.
- 900
- 901
- 902
- 903
- 904
- 905
- 906
- Even in case of successful deployment of the new agreement, the old agreement SHOULD NOT be deactivated immediately. This is to allow any in-process messages that use to old agreement to still be processed. For example, a message that was not successfully sent and is being retransmitted due to AS4 reliable messaging may be received at a time when the new agreement has already been deployed. In this case, the configuration for the old agreement SHOULD still be available to successfully receive, acknowledge and deliver the message.

907 **3 Examples**

908 3.1 Message with EDIG@S Payload

909 The following non-normative example is included to illustrate the structure of an AS4
910 message conforming to this profile, for a hypothetical `http://docs.oasis-open.org/ebxml-
911 msg/as4/200902/action` action invoked by a hypothetical shipper 21X-EU-A-X0A0Y-Z on a

912 hypothetical service A06 exposed by a hypothetical transmission system operator 21X-EU-B-
 913 P0Q0R-S. The detailed contents of the wsse:Security header is omitted.

914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982

```

POST /as4handler HTTP/1.1
Host: receiver.example.com:8893
User-Agent: Turia
Content-Type: multipart/related; start="<f8df1904-a6b9-422b-8239-6a971838503f@sender.example.com>";
boundary= "c5bae1842d1e"; type="application/soap+xml"
Content-Length: 472639

--c5bae1842d1e
Content-Id: <f8df1904-a6b9-422b-8239-6a971838503f@sender.example.com>
Content-Type: application/soap+xml; charset="UTF-8"

<S12:Envelope xmlns:S12="http://www.w3.org/2003/05/soap-envelope"
xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
xmlns:eb3="http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/" >
  <S12:Header>
    <eb3:Messaging wsu:Id="_18f85fc2-a956-431e-a80e-09a10364871b">
      <eb3:UserMessage>
        <eb3:MessageInfo>
          <eb3:Timestamp>2016-04-03T14:49:28.886Z</eb3:Timestamp>
          <eb3:MessageId>2016-921@5209999001264@example.com</eb3:MessageId>
        </eb3:MessageInfo>
        <eb3:PartyInfo>
          <eb3:From>
            <eb3:PartyId
              type="http://www.entsoe.eu/eic-codes/eic-party-codes-x">21X-EU-A-X0A0Y-Z</eb3:PartyId>
            <eb3:Role>ZSH</eb3:Role>
          </eb3:From>
          <eb3:To>
            <eb3:PartyId
              type="http://www.entsoe.eu/eic-codes/eic-party-codes-x">21X-EU-B-P0Q0R-S</eb3:PartyId>
            <eb3:Role>ZS0</eb3:Role>
          </eb3:To>
        </eb3:PartyInfo>
        <eb3:CollaborationInfo>
          <eb3:AgreementRef
            >http://entsog.eu/communication/agreements/21X-EU-A-X0A0Y-Z/21X-EU-B-P0Q0R-S/3</eb3:AgreementRef>
          <eb3:Service type="http://edigas.org/service">A06</eb3:Service>
          <eb3:Action> http://docs.oasis-open.org/ebxml-msg/as4/200902/action</eb3:Action>
          <eb3:ConversationId></eb3:ConversationId>
        </eb3:CollaborationInfo>
        <eb3:PayloadInfo>
          <eb3:PartInfo href="cid:0b960692-a3c6-4e85-80da-36009d3ae043@sender.example.com">
            <eb3:PartProperties>
              <eb3:Property name="MimeType">application/xml</eb3:Property>
              <eb3:Property name="CharacterSet">utf-8</eb3:Property>
              <eb3:Property name="CompressionType">application/gzip</eb3:Property>
              <eb3:Property name="EDIGASDocumentType">01G</eb3:Property>
            </eb3:PartProperties>
          </eb3:PartInfo>
        </eb3:PayloadInfo>
      </eb3:UserMessage>
    </eb3:Messaging>
    <wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
      xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
      <!-- details omitted -->
    </wsse:Security>
  </S12:Header>
  <S12:Body wsu:Id="_b656ef2c-516"/>
</S12:Envelope>

--c5bae1842d1e
Content-Id: <0b960692-a3c6-4e85-80da-36009d3ae043@sender.example.com>
Content-Type: application/octet-stream
Content-Transfer-Encoding: binary

BINARY CIPHER DATA
  
```

983 --c5bae1842d1e-

984 3.2 Alternative Using Defaults

985 The following example fragment is a variant of the sample message shown in section [Error!](#)
 986 [Reference source not found.3-1](#), for a data exchange that has not been classified using
 987 EDIG@S code values for Service and Role. Instead of an EDIG@S service code, it uses the
 988 default service value, as described in section 2.3.1.2.1. Instead of EDIG@S role codes, it uses
 989 the default initiator and responder roles, as described in section 2.3.1.2.3.

```

990 ...
991 <eb3:PartyInfo>
992   <eb3:From>
993     <eb3:PartyId
994       type="http://www.entsoe.eu/eic-codes/eic-party-codes-x">21X-EU-A-X0A0Y-Z</eb3:PartyId>
995     <eb3:Role>http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/initiator</eb3:Role>
996   </eb3:From>
997   <eb3:To>
998     <eb3:PartyId
999       type="http://www.entsoe.eu/eic-codes/eic-party-codes-x">21X-EU-B-P0Q0R-S</eb3:PartyId>
1000     <eb3:Role>http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/responder</eb3:Role>
1001   </eb3:To>
1002 </eb3:PartyInfo>
1003 <eb3:CollaborationInfo>
1004   <eb3:AgreementRef
1005     >http://entsog.eu/communication/agreements/21X-EU-A-X0A0Y-Z/21X-EU-B-P0Q0R-S/3</eb3:AgreementRef>
1006   <eb3:Service> http://docs.oasis-open.org/ebxml-msg/as4/200902/service</eb3:Service>
1007   <eb3:Action> http://docs.oasis-open.org/ebxml-msg/as4/200902/action</eb3:Action>
1008   <eb3:ConversationId></eb3:ConversationId>
1009 </eb3:CollaborationInfo>
1010 ...
  
```

 1011 **4 Processing Modes**

1012

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-

P-Mode Parameter	Profile Value
	party-codes-x
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 http://www.entsoe.eu/eic-codes/eic-party-codes-x
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, http://docs.oasis-open.org/ebxml-msg/as4/200902/action , 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

P-Mode Parameter	Profile Value
PMoDe[1].Errorhandling.Report.ReceiverErrorsTo	Not used
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	http://www.w3.org/2001/04/xmlenc#sha256
PMoDe[1].Security.X509.Signature.Algorithm	http://www.w3.org/2001/04/xmldsig-more#rsa-sha256
PMoDe[1].Security.X509.Encryption.Encrypt	True
PMoDe[1].Security.X509.Encryption.Certificate	Encryption Certificate of the Receiver
PMoDe[1].Security.X509.Encryption.Algorithm	http://www.w3.org/2009/xmlenc11#aes128-gcm
PMoDe[1].Security.X509.Encryption.MinimalStrength	128
PMoDe[1].Security.	Not used

P-Mode Parameter	Profile Value
UsernameToken. username	
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

P-Mode Parameter	Profile Value
PMode[1].ReceptionAwareness. DetectDuplicates.Parameters	Not profiled
PMode[1].BusinessInfo. subMPCext	Not used

1013

1014 **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"> • 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 02.2.6.1). • Provided guidance on WS-Security based on ENISA guidelines, advice from XML Security experts (section 2.2.6.2). • Added test service (section 2.3.72-3.6). • 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 2.3.82-3.7). • Added an example message (section 3.13). • Values to be confirmed: five minutes for retries (section 2.2.5), 10 MB total payload size (section 2.3.62-3.5)
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).

			<ul style="list-style-type: none"> • All payloads are carried in separate MIME parts; no support for external payloads; renamed from “attachments” to “payloads” (section 2.2.3.2). • The reference to TLS cipher suites is more general (section 02.2.6.1). • 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 2.3.7.2-3.6). • The section on separating environments is simplified (section 2.3.8.2-3.7). • The usage profile on reliable messaging is removed. • Fixed reference to BSI TLS document (section 6).
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,	<ul style="list-style-type: none"> • Updates based on team teleconference

		EJvN	<ul style="list-style-type: none"> Generalized title of 2.3.4.4 and updated content to reflect the new appendix on certificate requirements. 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 <u>3.13</u> 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 RefToMessageId is not used. 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. Updates based on conference call of 2015-04-01 In section 2.3.62-3.5, introduced the EDIGASDocumentType property and added further profiling of the PartInfo element. Renamed the Service Metadata Mapping Table to ENTSOG AS4 Mapping Table. Introduced the AS4 default action. Changed the example in section 3.13 to use agreed values. Clarified that roles are business roles in 2.3.1.2.4. In 2.3.62-3.5, 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 3.13.
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 ENTSOG AS4 Mapping Table Editorial clean up Updated reference to Network Code to the

			<p>Commission Regulation 2015/703.</p> <ul style="list-style-type: none"> Removed a reference to an unpublished overview of certificate standards and requirements. 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
V2r1	05/01/16	JM	<ul style="list-style-type: none"> Added in confirmation of algorithm requirements
V2r2	09/06/16	PvdE	<ul style="list-style-type: none"> Type attribute on PartyId in section 2.3.1.1 added. Type attribute on Service in section 2.3.1.2.1 added. In section 2.3.2, provided a URI-based naming conventions for agreements. In section 2.3.62-3.5, the schema is fixed for sender and document type for each receiver. In section 2.3.62-3.5, added that EDIG@S XML documents are encoded in UTF-8. Updated example in section 3.13. New section 4, PMode table. Updated reference to ebCore AU to current version.
V2r3	30/06/16	PvdE	<ul style="list-style-type: none"> Removed statement on UTF-8 encoding of EDIG@S Added UTF-8 and BOM clarification to SOAP envelope encoding. In the example in section 3.13, added a missing closing tag <code></eb3:Property></code> and made ConversationId an empty element as per section 2.3.1.3. Added BP20 reference to bibliography. Removed an obsolete duplicate comment on

			<p>type attribute on PartyId.</p> <ul style="list-style-type: none"> Added discussion of security token references and indicated a preference for BST in 2.2.6.2. In 2.3.4.3, indicated that parties must select a compatible option for security token references.
V2r4	19/07/16	ICT KG	<ul style="list-style-type: none"> Reviewed at ITC KG meeting
V2r5	22/08/16	JM	<ul style="list-style-type: none"> Updated Legal Disclaimer
V2r6	4/10/16	PvdE	<ul style="list-style-type: none"> Updated status of ebCore Agreement Update, due its approval as Committee Specification in the OASIS ebCore TC Updated Configuration Management API discussion in section 2.2.8 New section 2.4 on Agreement Update. Updated discussion of Service and Action also for ebCore messages. Fixed a typo in section <u>3.13</u>, message ID was not RFC 2822 compliant. Many editorial changes, a.o. redundant white space.
V2.7	18/10/16		<ul style="list-style-type: none"> Accepted all changes In 2.2.3.2, changed to reflect that compression is not guaranteed to take place when the compression P-Mode is set. In <u>02-2-6-1</u> changed “support TLS 1.2” to “at least support TLS 1.2”. In 2.3.1.2.4, added “For business services,”. In 2.3.1.3, rephrased as “as content the empty string”. Fixed the wording in the first bullet in <u>2.3.62-3-5</u>. In section, improved definition of PMode[1].BusinessInfo.Service, Action and

			Role to include test and AU.
V2.8	24/10/16	JM	<ul style="list-style-type: none"> Reviewed and corrected grammatical errors Created Rev 3 for publication following ITC KG & INT WG approval
V2.9	2/11/16	PvdE	<ul style="list-style-type: none"> Minor editorial In section 2.2.3.1, add requirement that a Receiving MSH MUST use AgreementRef to select the P-Mode to use for a message: "A compliant product, acting as Receiver, MUST take the value of the AS4 AgreementRef header into account when selecting the applicable P-Mode." This is needed so that the right certificates are selected. In section 2.3.1.2.4, added the underlined eight words to the sentence "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>" 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. 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. Renamed title of section 2.3.4.5.5 to include TLS as well. 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. In section 2.3.4.5.5, KeyAgreement requirement dropped. In the References section, upgraded to

			references to the ENISA report from the 2013 to the (most recent) 2014 version.
V3.0	PvdE		<ul style="list-style-type: none"> • Added back in the 2013 ENISA reference as requested by ITC KG • Approved as v3.0 by ITC KG
V3r1	PvdE		<ul style="list-style-type: none"> • Updated the references of ETSI ESI European Norms to the current versions. • Some re-structuring of requirements on certificates, making it clear the review process applies to all certificates and CAs. • Harmonized “CA” as abbreviation for Certification Authority. • Mention that EV certificates may be used. • Mentioned options for EIC code in certificate.
V3r2	PvdE	2016-12-23	<ul style="list-style-type: none"> • 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. • New minor section “Networking” in Usage Profile to cover IPv4/IPv6. • Removed reference to private networks, as the network code states that the Internet is to be used and for consistency with other profiles.
V3.3	PvdE	2017-02-13	<ul style="list-style-type: none"> • Specified the use of the AS4 P-Mode values for Service and Role for situations where the data exchange is not classified. (For Action, the default value was already specified).
V3.4	PvdE	2017-02-24	<ul style="list-style-type: none"> • 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.
V3.5	PvdE	2017-02-24	<ul style="list-style-type: none"> • In section 2.3.6, changed the requirement on presence of the EDIGASDocumentType part

			property from MUST to SHOULD.
<u>V3.6</u>	<u>PvdE</u>	<u>2018-03-27</u>	<p><u>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.</u></p> <ul style="list-style-type: none"> • <u>Section 2.2.3.1, UUID in MessageId.</u> • <u>Section 2.2.6.2, BinarySecurityToken.</u> • <u>Section 2.2.6.2, Key Transport Algorithms.</u> • <u>Section 2.3.1.1, checking delegation relations.</u> • <u>Section 2.3.4.1, use of firewalls.</u>

1015 **6 References**

- 1016 [AES] Advanced Encryption Standard. FIPS 197. NIST, November 2001.
1017 <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>
- 1018 [AS4] AS4 Profile of ebMS 3.0 Version 1.0. OASIS Standard, 23 January 2013.
1019 <http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/profiles/AS4-profile/v1.0/>
- 1020 [AU] ebCore Agreement Update Specification Version 1.0. OASIS Committee
1021 Specification. 19 September 2016. [http://docs.oasis-open.org/ebcore/ebcore-](http://docs.oasis-open.org/ebcore/ebcore-au/v1.0/)
1022 [au/v1.0/](http://docs.oasis-open.org/ebcore/ebcore-au/v1.0/)
- 1023 [BP20] Basic Profile Version 2.0. OASIS Committee Specification.
1024 <http://docs.oasis-open.org/ws-brsp/BasicProfile/v2.0/BasicProfile-v2.0.pdf>
- 1025 [BSIALG] Entwurf Algorithmenkatalog 2014. Bundesamt für Sicherheit in der
1026 Informationstechnik (BSI). Bonn, 11 Oktober 2013.
1027 [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)
1028 [menkatalog_Entwurf_2013.pdf?__blob=publicationFile.](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ElekSignatur/Algorithmenkatalog_Entwurf_2013.pdf?__blob=publicationFile)
- 1029 [BSITLS] Mindeststandard des BSI nach § 8 Abs. 1 Satz 1 BSI für den Einsatz des
1030 SSL/TLS-Protokolls in der Bundesverwaltung. Bundesamt für Sicherheit in der
1031 Informationstechnik (BSI). Bonn, 08 Oktober 2013.
1032 [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)
1033 [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)
- 1034 [CABFBRCP] CA Browser Forum: " Baseline Requirements Certificate Policy for the Issuance
1035 and Management of Publicly-Trusted Certificates ". Latest Version 1.4.1,
1036 September 2016.
1037 <https://cabforum.org/baseline-requirements-documents/>
- 1038 [CABFEVV] CA Browser Forum. "Guidelines For The Issuance And Management Of
1039 Extended Validation Certificates". Latest Version 1.6.0. July 2016.
1040 <https://cabforum.org/extended-validation/>
- 1041 [CAM] Business Requirements Specification for the Capacity Allocation Mechanism
1042 (CAM) Network Code. Draft Version 0 Revision 05 – 2012-10-05.
- 1043 [CEM] Certificate Exchange Messaging for EDIINT. Expired Internet-Draft.
1044 [https://tools.ietf.org/html/draft-meadors-certificate-exchange-14.](https://tools.ietf.org/html/draft-meadors-certificate-exchange-14)
- 1045 [CR2015/703] COMMISSION REGULATION (EU) 2015/703 of 30 April 2015 establishing a
1046 network code on interoperability and data exchange rules.
1047 [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)
1048 [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)
- 1049 [EBMS3] OASIS ebXML Messaging Services Version 3.0: Part 1, Core Features. OASIS
1050 Standard. 1 October 2007. [http://docs.oasis-open.org/ebxml-](http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/core/os/)
1051 [msg/ebms/v3.0/core/os/](http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/core/os/)
- 1052 [EDIG@S] EASEE-gas EDIG@S. Version 5.1. <http://www.EDIG@S.org/version-5/>

- 1053 [EGCDN] Common Data Network. EASEE-gas Common Business Practice 2007-002/01.
1054 http://easee-gas.eu/docs/cbp/approved/CBP2007-002-01_DataNetwork.pdf
- 1055 [EGMTP] Message Transmission Protocol. EASEE-gas Common Business Practice 2007-
1056 001/01. [http://easee-gas.eu/docs/cbp/approved/CBP2007-001-](http://easee-gas.eu/docs/cbp/approved/CBP2007-001-01_MessageTransmissionProtocol.pdf)
1057 [01_MessageTransmissionProtocol.pdf](http://easee-gas.eu/docs/cbp/approved/CBP2007-001-01_MessageTransmissionProtocol.pdf)
- 1058 [EIC] ENTSOG. Energy Identification Coding Scheme (EIC) for natural gas
1059 transmission. Party Codes. <http://www.entsog.eu/eic-codes/eic-party-codes-x>
- 1060 [EN 319 411-1] European Standard. Electronic Signatures and Infrastructures (ESI); Policy
1061 and security requirements for Trust Service Providers issuing certificates; Part
1062 1: General requirements, v1.1.1, 2016-02. (Formerly [ETSI EN 319 411-3])
1063 [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)
1064 [en_31941101v010101p.pdf](http://www.etsi.org/deliver/etsi_en/319400_319499/31941101/01.01.01_60/en_31941101v010101p.pdf)
- 1065 [EN 319 412-3] Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3:
1066 Certificate profile for certificates issued to legal persons.
1067 [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)
1068 [en_31941203v010101p.pdf](http://www.etsi.org/deliver/etsi_en/319400_319499/31941203/01.01.01_60/en_31941203v010101p.pdf)
- 1069 [EN 319 412-4] Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4:
1070 Certificate profile for web site certificates.
1071 [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)
1072 [en_31941204v010101p.pdf](http://www.etsi.org/deliver/etsi_en/319400_319499/31941204/01.01.01_60/en_31941204v010101p.pdf)
- 1073 [ENISA13] Algorithms, Key Sizes and Parameters Report 2013 recommendations version
1074 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)
1075 [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)
- 1076 [ENISA14] Algorithms, Key Size and Parameters Report 2014. November 2014. ENISA.
1077 [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)
1078 [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)
- 1079 [NOM] Business Requirements Specification for the Nomination (NOM) Network Code.
1080 Draft Version 0 Revision 9 – 2013-06-04.
- 1081 [OSSTLS] OpenSSL TLS 1.2 Cipher Suites.
1082 http://www.openssl.org/docs/apps/ciphers.html#TLS_v1_2_cipher_suites.
- 1083 [RFC2119] A. Ramos. Key words for use in RFCs to Indicate Requirement Levels. IETF RFC
1084 2119. January 1998. <http://www.ietf.org/rfc/rfc2119.txt>
- 1085 [RFC2822] P. Resnick. Internet Message Format <https://tools.ietf.org/html/rfc2822>
- 1086 [RFC5246] T. Dierks et al. The Transport Layer Security (TLS) Protocol Version 1.2. IETF RFC
1087 5246. August 2008. <http://tools.ietf.org/html/rfc5246>
- 1088 [RFC6176] S. Turner et al. Prohibiting Secure Sockets Layer (SSL) Version 2.0. RFC 6176.
1089 March 2011. <http://tools.ietf.org/html/rfc6176>

- 1090 [RFC6555] D. Wing et al. Happy Eyeballs: Success with Dual-Stack Hosts.
1091 <http://tools.ietf.org/html/rfc6555>
- 1092 [TLSSP] Transport Layer Security (TLS) Parameters. Last Updated 2013-10-03.
1093 [http://www.iana.org/assignments/tls-parameters/tls-parameters.xml#tls-](http://www.iana.org/assignments/tls-parameters/tls-parameters.xml#tls-parameters-4)
1094 [parameters-4](http://www.iana.org/assignments/tls-parameters/tls-parameters.xml#tls-parameters-4)
- 1095 [TS119312] ETSI TS 119 312 V1.1.1 Electronic Signatures and Infrastructures (ESI);
1096 Cryptographic Suites.
1097 http://www.etsi.org/deliver/etsi_ts/119300_119399/119312/01.01.01_60/ts
1098 [119312v010101p.pdf](http://www.etsi.org/deliver/etsi_ts/119300_119399/119312/01.01.01_60/ts)
- 1099 [WSSSMS] OASIS Web Services Security: SOAP Message Security Version 1.1.1. OASIS
1100 Standard, May 2012. <http://docs.oasis-open.org/wss-m/wss/v1.1.1/wss->
1101 [SOAPMessageSecurity-v1.1.1.doc](http://docs.oasis-open.org/wss-m/wss/v1.1.1/wss-)
- 1102 [WSSSWA] OASIS Web Services Security: Web Services Security SOAP Message with
1103 Attachments (SwA) Profile Version 1.1.1. OASIS Standard, May 2012.
1104 <http://docs.oasis-open.org/wss-m/wss/v1.1.1/wss-SwAProfile-v1.1.1.doc>
- 1105 [WSSX509] OASIS Web Services Security: Web Services Security X.509 Certificate Token
1106 Profile Version 1.1.1. OASIS Standard, May 2012.
1107 <http://docs.oasis-open.org/wss-m/wss/v1.1.1/wss-x509TokenProfile->
1108 [v1.1.1.doc](http://docs.oasis-open.org/wss-m/wss/v1.1.1/wss-x509TokenProfile-)
- 1109 [XMLDSIG] XML Signature Syntax and Processing (Second Edition). W3C Recommendation
1110 10 June 2008. <http://www.w3.org/TR/2008/REC-xmlsig-core-20080610>
- 1111 [XMLDSIG1] XML Signature Syntax and Processing Version 1.1. W3C Recommendation 11
1112 April 2013. <http://www.w3.org/TR/xmlsig-core1/>
- 1113 [XDSIGBP] XML Signature Best Practices. W3C Working Group Note 11 April 2013.
1114 <http://www.w3.org/TR/2013/NOTE-xmlsig-bestpractices-20130411/>
- 1115 [XMLENC] XML Encryption Syntax and Processing. W3C Recommendation 10 December
1116 2002. <http://www.w3.org/TR/xmlenc-core/>
- 1117 [XMLENC1] XML Encryption Syntax and Processing Version 1.1. W3C Recommendation 11
1118 April 2013. <http://www.w3.org/TR/xmlenc-core1/>