

1

ENTSOG Configuration Management Approach

2

Version ~~0-0~~ Revision ~~0-31~~ – ~~2017~~~~2020-12XX-12YY~~



3

Disclaimer

4 **This document only provides specific technical information given for indicative purposes**
5 **only and, as such, it is subject to further modifications. The information contained in the**
6 **document is non-exhaustive and non-contractual in nature.**

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

11

12

13

Table of contents

14		
15	1 Introduction.....	54
16	2 Required Features	65
17	3 Data Exchange Parameters	87
18	3.1 Party Parameters.....	98
19	3.2 (Sub) Profile Parameters	98
20	3.3 Network and Network Security Parameters	1140
21	3.4 Certificate Sets	1244
22	3.5 Business Process Relations.....	1342
23	3.6 Agreement Parameters	1342
24	3.7 Delegation	1443
25	4 Structured Export	1544
26	4.1 CPPA3 Profile.....	1645
27	4.2 Profile Export.....	1645
28	4.3 Agreement Export	1645
29	4.4 Delegation Export.....	1745
30	4.5 Network and Network Security Export	1746
31	5 CPPA3 Usage Profile.....	1746
32	5.1 CPP and CPA	1846
33	5.2 Party Information	1847
34	5.3 Service Specification.....	1948
35	5.4 PayloadProfile	2049
36	5.5 ebMS3Channel	2049
37	5.6 HTTPTransport.....	2120
38	5.7 Delegation	2221
39	6 EASEE-Connect	2321
40	7 Revision History.....	2423
41	8 References.....	2524
42	1 Introduction.....	4

Formatted: Default Paragraph Font, English (United Kingdom), Check spelling and grammar

43	2	Required Features	5
44	3	Data Exchange Parameters	7
45	3.1	Party Parameters	8
46	3.2	(Sub) Profile Parameters	8
47	3.3	Network and Network Security Parameters	10
48	3.4	Certificate Sets	11
49	3.5	Business Process Relations	12
50	3.6	Agreement Parameters	12
51	3.7	Delegation	13
52	4	Structured Export	14
53	4.1	CPPA3 Profile	15
54	4.2	Profile Export	15
55	4.3	Agreement Export	15
56	4.4	Delegation Export	15
57	4.5	Network and Network Security Export	16
58	5	CPPA3 Usage Profile	16
59	5.1	CPP and CPA	16
60	5.2	Party Information	17
61	5.3	Service Specification	18
62	5.4	PayloadProfile	19
63	5.5	ebMS3Channel	19
64	5.6	HTTPTransport	20
65	5.7	Delegation	21
66	6	Revision History	22
67	7	References	23
68			

Formatted: Default Paragraph Font, English (United Kingdom), Check spelling and grammar

Formatted: Default Paragraph Font, English (United Kingdom), Check spelling and grammar

Formatted: Default Paragraph Font, English (United Kingdom), Check spelling and grammar

Formatted: Default Paragraph Font, English (United Kingdom), Check spelling and grammar

Formatted: Default Paragraph Font, English (United Kingdom), Check spelling and grammar

Formatted: Default Paragraph Font, English (United Kingdom), Check spelling and grammar

Formatted: Default Paragraph Font, English (United Kingdom), Check spelling and grammar

Formatted: Default Paragraph Font, English (United Kingdom), Check spelling and grammar

Formatted: Default Paragraph Font, English (United Kingdom), Check spelling and grammar

Formatted: Default Paragraph Font, Check spelling and grammar

Formatted: Default Paragraph Font, Check spelling and grammar

Formatted: Default Paragraph Font, English (United Kingdom), Check spelling and grammar

Formatted: Default Paragraph Font, English (United Kingdom), Check spelling and grammar

Formatted: Default Paragraph Font, English (United Kingdom), Check spelling and grammar

Formatted: Default Paragraph Font, English (United Kingdom), Check spelling and grammar

Formatted: Default Paragraph Font, Check spelling and grammar

Formatted ...

Formatted ...

69 **1 Introduction**

70 ENTSOG has produced a number of usage profiles [[AS4UPAS4UPAS4UP](#), WSUP, INTUP] to
71 support the implementation of the common data exchange solutions defined in the Network
72 Code on Interoperability and Data Exchange [CR2015/703]. AS4, which is used for
73 document-based data exchange, and SOAP/HTTPS, which is used for integrated exchange,
74 support machine-to-machine exchange of structured information. To use these solutions
75 successfully, TSOs and their counterparties need to configure various communication
76 parameters in their communication products. Many of these parameters are pre-defined in
77 the ENTSOG specifications and can be inferred by referencing the applicable specification
78 version, but others are unique to specific parties and counterparties, and therefore need to
79 be exchanged and configured between parties.

80 While it is possible to exchange communication configuration parameters bilaterally, this is
81 inefficient and, if manual effort is involved, error-prone. Stakeholders in the gas sector have
82 identified the need for a secure collaboration platform that allows parties to share and agree
83 on such parameters, and to retrieve parameter sets in a structured format that can be
84 imported or applied (semi-)automatically. The main identified benefits of the platform relate
85 to setting up configurations for new parties and/or new services, where many parameters
86 need to be set. The platform would therefore complement and serve a purpose different
87 from the ebCore Agreement Update feature, which supports updates of existing
88 configurations.

89 This document provides the following:

- 90 • An overview of requirements and key features that a central configuration portal
91 should address. This is done in section 2. The exchange platform should allow parties
92 to securely self-manage their parameter values, to selectively share these values with
93 counterparties and to link profiles to agreements.
- 94 • A specification of a set of data elements for data exchange configuration parameters.
95 This is discussed in section 3, which groups and defines the various parameters.
- 96 • A specification of functionality to export partner profiles and agreements. The
97 exchange platform should allow parties to download parameters in structured
98 formats. Vendors or systems integrators may use this functionality to (semi-
99)automatically configure communication. This is discussed in section 4.
- 100 • A specification of a Usage Profile of an [OASIS ~~draft~~](#) standard, ebCore CPPA3, that can
101 be used in the export function. This is done in section 5.
- 102 • [A short description of EASEE-Connect, a service from EASEE-gas that implements the
103 concepts described in this document. This is provided in section 6.](#)

104 ENTSOG does not currently intend to develop or host this platform, but encourages its
105 stakeholders, and stakeholder communities [such as EASEE gas](#), to develop and operate such
106 a platform.

107 **2 Required Features**

108 The collaboration platform is to allow gas sector parties to maintain, exchange and agree on
109 communication configuration data securely. Since TSOs exchange data among themselves,
110 but also with other market participants, the platform should be open to all relevant parties
111 in the gas business. The platform is useful if its users can serve as “one stop shop” to
112 configure configuration with all or the vast majority of their counterparties.

113 The collaboration platform needs a formal identification system for parties and therefore
114 identifies parties using their EIC code [\[EIC\]](#), as issued by ENTSOG and other issuing agencies.
115 EIC codes are unambiguous and used as party identifier header values in AS4 messaging.

116 The collaboration platform should allow parties to provide and maintain their configuration
117 parameters themselves. A self-service model avoids unnecessary delays, puts those
118 responsible for data and data quality in charge of managing that data, and minimizes the
119 operational costs of the platform.

120 The collaboration platform should allow sharing data where needed, but limit unnecessary
121 sharing where possible. Parties exchange data in support of business processes with
122 counterparties. The platform should allow parties to specify who their counterparties are,
123 i.e. who they send messages to and who they receive messages from. This information can
124 then be used to control the visibility of the data in the platform: configuration data is only
125 shared among parties who are each other’s counterparties, but otherwise confidential, and
126 agreements can only be formed among counterparties.

127 By analogy to human-to-human communication, the collaboration platform is more like a
128 social network (in which people can share selectively, self-organize in private groups) than to
129 email (which offers ad hoc any-to-any data sharing but no controls on visibility and sharing,
130 and no concept of a communication agreement). Market communication is based on
131 party/counterparty relations. These relations are typically stable rather than ad hoc, but not
132 fully static, as players still enter or leave the market [and add or drop business partners](#), and
133 companies may reorganize.

134 The collaboration platform is most useful if it allows all relevant parameters to be
135 maintained. This includes parameters specific to the party, the communication protocol
136 profile parameters, network and network security configuration, certificate sets, business
137 process relations, agreement parameters and delegation information. A full overview and
138 categorization of data exchange parameters is provided in section 3.

139 The platform should be able to support the full lifecycle or data communication. Companies
140 periodically update their communication services and configuration parameters change
141 accordingly. They may take on new roles, and outsource others. Companies also have other
142 environments than their production systems, and need counterparty data to configure each
143 of them, and need to be able to indicate in which intervals environments and configuration
144 sets are valid.

145 The data that is managed in the collaboration platform is used in communication and
146 networking systems. Since the data is structured and even minor errors can cause
147 communication failures, it is important that the data can be exported (or downloaded) in a (or
148 in a selection of) structured electronic format(s). This is further addressed in section 4.

149 The platform can only be trusted if its operation is secure, all access to and use of its services
150 is authenticated and authorized and all operations are logged and monitored. Each company
151 registered to the platform should be able to manage which employees can use the platform
152 on its behalf, and which operations they can perform.

153 **3 Data Exchange Parameters**

154 The ENTSOG data exchange specifications describe the use of data exchange solutions for
155 various types of exchanges. These solutions are parameterized, meaning they need to be
156 provided with configuration parameters to function appropriately. This section provides an
157 overview and basic set of configuration data elements. The elements are grouped to support
158 common reuse patterns:

- 159
- Party parameters
 - (Sub) Profile parameters
 - Networking and Network security parameters.
 - Certificate sets.
- 162

163 The grouping provides support and flexibility for real-life data exchange situations and
164 covers all parameters needed for the ENTSOG document-based and integrated exchanges.

165 Examples of some supported situations, not exclusive of others, are:

- 166
- A party has a “test” and a “production” environment for document-based exchange.
167 This is handled as two (sub) profiles, with different endpoints hosted on different
168 servers with different IP addresses and possibly different certificate sets.
 - A party has two “production” environments for document-based exchange that are
169 the same except that the first expires a month after the second is activated and that
170 ~~the~~ they are linked to different certificate sets. This can occur during a certificate
171 switch period.
 - A party has a “production” environment for document-based AS4 exchange and
172 another “production” environment for integrated data exchange profile B.
 - A party has two (sub) profiles that are both for the “test” environment. One is the
173 regular test environment; the other is being used to test a new vendor product that
174 the party will migrate to.
- 177

178 Parameters that have fixed values defined in the ENTSOG specifications are not covered in
179 this overview. Instead, each (sub) profile is labelled with the type and version of applied data
180 exchange solution. When configuring a generic, off-the-shelf communication system (i.e. not
181 an ad hoc solution for an ENTSOG profile), users therefore need to combine the data
182 elements specified in this section and the preconfigured values.

183 Note that a secure configuration exchange platform will need to manage other data, for
184 example administrative data and authorizations, to support its own operation and use. This
185 section only covers the data elements to be used to configure exchanges following the
186 ENTSOG data exchange specifications.

187 This version of this document is focussed on document-based exchange. In principle, the
188 approach could be extended to integrated and interactive exchange, though details and
189 technologies used would be different.

190 3.1 Party Parameters

191 Party parameters provide information about a TSO or other company that is independent of
192 data exchange solution.

193 This group also includes contact information which obviously is not directly used in a
194 communication system, but can be useful in case of trouble-shooting.

Parameter	Description	Cardinality
Party Name	Name of the party	1
Party Identifier	EIC code of the party	1
Party Contact	A list of contacts for the party. Each contact has a type (e.g. "business contact", "technical contact") and one or multiple communication addresses. Each communication address has a type (e.g. email address, telephone number) and value.	1..n
Party Role	The role the party may perform, encoded as an EDIG@S role code value.	1..n
Counter Party Identifier	A list of EIC codes of the counterparties of the party	1..n

195 3.2 (Sub) Profile Parameters

196 For each party, multiple party (sub) profiles may be defined. A (sub) profile is valid in an
197 environment, uses a (version of a) data exchange solution on a URI, is valid in a certain
198 interval, involves a set of certificates and has a network (security) configuration.

Parameter	Description	Cardinality
Sub Profile Identifier	An identifier for the sub-profile (only needed internally for cross references from agreements)	1

Parameter	Description	Cardinality
Party Reference	Reference to party for which this is a sub-profile	1
Party Role	<p>The role of the party for which this is a sub-profile. Must be one of the roles party may perform.</p> <p>If none specified, the sub profile applies to all roles that party may perform</p>	0..n
Environment	The environment for which the sub profile provides values, e.g. "acceptance" versus "production"	1
Activation Date	Date and time from which the sub parameter set is valid	1
Expiration Date	Date and time until which the sub parameter set is valid	1
Data Exchange Solution	<p>Indication which data exchange solution is used. Possible values are ENTSOG AS4, ENTSOG Integrated Data Exchange Profile A, B or C.</p> <p>Other values can be used for other solutions (e.g. legacy solutions, or solutions with NRA approval), such as EASEE-gas AS2.</p>	1
Data Exchange Solution version	<p>Optional protocol version, useful in case future incompatible changes are made.</p> <p>CurrentThe current version for ENTSOG AS4 is 3.56.</p>	0..1
Data Exchange Product	<p>Vendor name and name and version of the product the solution is deployed on.</p> <p>Note: this element is for information only and parties are not required to disclose it. It may be useful for trouble shooting.</p>	0..1

Parameter	Description	Cardinality
Endpoint URI	HTTP or HTTPS URI for the endpoint. The domain name must be resolvable using DNS records ("A" for IPv4, "AAAA" for IPv6).	1
Network Security Parameter Set ID	Cross reference to a network Security Parameter Set	0..1
Certificate Set ID	Cross reference to a Certificate Set. Presence/absence dependent on data exchange solution used: not needed for interactive exchange. Referenced certificates must be valid in the validity interval of the profile.	0..1

199 **3.3 Network and Network Security Parameters**

200 A sub profile may be constrained to be used with a set of network parameters and network
201 security parameters.

Parameter	Description	Cardinality
Network Security Parameter Set ID	Internal identifier for cross-referencing the network security parameter set	1
IPv4 supported	Boolean indicator that expresses if IPv4 may be used for communication	1
Client IP v4	IPv4 address or address range from which the endpoint initiates HTTP(S) connections Requires the IPv4 supported parameter to be true.	0..n
Server IP v4	IPv4 address or address range at which the endpoint accepts HTTP(S) connections Requires the IPv4 supported parameter to be true. A DNS "A" record MUST exist for the	0..n

Parameter	Description	Cardinality
	domain name used in the Endpoint and must resolve to an address in this range.	
IPv6 supported	Boolean indicator that expresses if IPv6 may be used for communication	1
Client IP v6	IPv6 address or address range from which the endpoint initiates HTTP(S) connections Requires the IPv6 supported parameter to be true.	0..n
Server IP v6	IPv6 address or address range at which the endpoint accepts HTTP(S) connections Requires the IPv6 supported parameter to be true. A DNS "AAAA" record MUST exist for the domain name used in the Endpoint and must resolve to an address in this range.	0..n

202 3.4 Certificate Sets

203 A reusable set of certificates, to be used in conjunction with one or multiple (sub) profiles.

Parameter	Description	Cardinality
Certificate Set ID	Internal identifier for cross-referencing the certificate set	1
Signing Certificate (Chain)	An ordered list containing the leaf signing certificate, any intermediate certificates and the Certification Authority certificate.	1
Encryption Certificate (Chain)	An ordered list containing the leaf encryption certificate, any intermediate certificates and the Certification Authority certificate.	1
Server Certificate (Chain)	An ordered list containing the TLS leaf	0..1

Parameter	Description	Cardinality
	server authentication certificate, any intermediate certificates and the Certification Authority certificate.	
Client Certificate (Chain)	An ordered list containing the TLS leaf client authentication certificate, any intermediate certificates and the Certification Authority certificate. Note: TLS client authentication is allowed, but not recommended in ENTSOG data exchange solutions.	0..1

204 3.5 Business Process Relations

205 Business process information is provided in the ENTSOG Service Action table
206 [\[AS4MAPAS4MAPAS4MAP\]](#), which lists, for each pair of roles, the types of EDIG@S or other
207 documents that can be exchanged between them. [The table includes service area codes](#)
208 [which are linked to EDIG@S versions \(4, 5, 6\) and can therefore be used to indicate which](#)
209 [EDIG@S version\(s\) a party supports.](#) From that table, in combination with the information on
210 roles performed by parties, the relevant AS4 parameters (Service, Action, From Role, To
211 Role) and the EDIG@S Document Type can be inferred. By listing roles for parties, and listing
212 counterparties for parties, all potential exchanges between parties can be computed.
213 [A potential future enhancement could be to allow parties to more precisely indicate which](#)
214 [versions of which business processes they support, and the relevant \(versions of\) document](#)
215 [types exchanged in these processes.](#)

216 3.6 Agreement Parameters

217 ENTSOG AS4 uses the AS4 agreement concept and requires the AS4 agreement reference
218 header to be present in AS4 messages. This allows its users to handle certificate switches in a
219 much more flexible way than the previous AS4 practice. As both involved parties may have
220 multiple different (sub) profiles, linking to distinct certificate sets, an agreement is a relation
221 at the sub-profile layer rather than the party layer.

Parameter	Description	Cardinality
Party Sub Profile Reference	A reference to a sub-profile of a party	1
Counterparty Sub Profile	A reference to a sub-profile of another	1

Parameter	Description	Cardinality
Reference	party	
An agreement sequence number	An integer that indicates a version of an agreement.	1
Activation Date	Date and time from which the delegation is valid. Must be compatible with the activation dates of the parties involved.	1
Expiration Date	Date and time until which the delegation is valid. Must be compatible with the expiration dates of the parties involved.	1

222 Note that the referenced (sub) profiles must be of the same type. A “test” agreement must
 223 be between two “test” (sub) profiles and a “production” agreement between two
 224 “production” (sub) profiles. It is not possible to have an agreement involving a “test” party
 225 profile and a “production” counterparty profile.

226 3.7 Delegation

227 Where normally organizations operate a messaging gateway to send and receive messages
 228 to their counterparties, sometimes organizations do not create or receive messages
 229 themselves, but use third party service providers that send and receive messages on behalf
 230 of and for them. Two situations can be distinguished:

- 231 1. Impersonation: in this situation, the third party sends and receives messages to the
 232 counterparties of the customer using the identity of its customer. For configuration
 233 and the configuration exchange platform, this is not different from the usual
 234 situation. The profile configuration is still registered with the EIC code of the
 235 customer.
- 236 2. Delegation: in this situation there are no messaging profiles for the customer in the
 237 portal, but there are for their service providers. To allow counterparties to know that
 238 a party uses a service provider, so that they can configure messaging with that
 239 service provider, an explicit delegation table can be used.

240 The delegation relation has the following properties:

Parameter	Description	Cardinality
-----------	-------------	-------------

Parameter	Description	Cardinality
Delegating Party Profile	Reference to a registered party	1
Delegating Party Role	The role for which the party delegates communication	0..n
Delegated Party Profile	Reference to a registered party	1
Activation Date	Date and time from which the delegation is valid	0..1
Expiration Date	Date and time until which the delegation is valid	0..1

241 Note that the model makes it possible for parties to delegate processing for some roles but
242 not for others. Also note that using multiple records with different activation/expiration
243 dates, it is possible to describe a switch from one service provider to another, or to describe
244 a outsourcing switch from an in-house solution to a service provider.

245 Delegation information is not messaging configuration information. Rather, it defines
246 constraints on relations between sender and receiver identifiers at message layer and at
247 business document layer, which can be validated in middleware or in business systems. All
248 configuration data for the actual exchange with the delegated party is not included in the
249 table. That data is instead provided as a (sub) profile of the delegated party. So, if party A
250 wants to exchange data with a party B that delegate to a service provider X, A must
251 configure an agreement with X. If A also outsources its data exchange to a service provider Y,
252 then X and Y must have an agreement.

253 **4 Structured Export**

254 A collaboration platform in which parties can self-manage their configuration parameters
255 and their relations with counter-parties is already a very useful first step. A next step is to
256 allow configuration data to be exported into a structured XML format, which can be
257 imported into communication software to set parameter sets efficiently. This eliminates
258 manual data entry and avoids the associated potential data entry errors.

259 The OASIS ebCore ~~draft CPPA3~~ [standard \[CPPA3SPEC\]](#) and its associated ~~XML~~ [XML schema](#)
260 [\[CPPA3XSD\]](#) ~~[CPPA3SPEC]~~ and ~~specification [CPPA3XSD]~~ provide a standard mechanism to
261 encode partner profile and agreement information for multiple communication protocols,
262 including AS2 and AS4. It can be used as a vendor-independent intermediate format to
263 export data managed in a secure configuration sharing environment into proprietary formats
264 and interfaces of communication products.

265 In addition to exporting to a (draft) standard format, the secure central platform may also
266 offer direct exports to proprietary formats.

267 **4.1 CPPA3 Profile**

268 The OASIS ebCore ~~draft~~ CPPA3 ~~XML schemastandard [CPPA3SPEC] and its associated XML~~
269 ~~schema [CPPA3XSD] [CPPA3SPEC] and specification [CPPA3XSD]~~ provide a structured XML
270 format for party profile and party agreement configuration. As is common with standard
271 formats that are intended to be used in very different contexts, it offers many options and
272 typically benefits from being profiled. Such profiling may cover both functionality to be
273 implemented in products and conventions to be adopted by users.

274 For the secure gas configuration data exchange platform, a usage profile is provided in
275 section 5. A proof-of-concept that illustrates the use of ebCore CPPA3 and that implements
276 this usage profile is published as open source, under the MIT license, on the public Internet
277 [AS4CPOC]. It includes sample code to generate CPP and CPA documents for parties.

278 **4.2 Profile Export**

279 A (Sub) Party parameter set, as described in section 3.2, can be exported together with
280 referenced party information (see section 3.1), network and network security information
281 (see section 3.3) and security sets (see section 3.4) as an ebCore CPPA3 CPP document.

282 ~~A CPP can capture all relevant information for AS2 exchanges, and could therefore be used~~
283 ~~to configure EASEE gas AS2 exchanges. However, for~~ ENTISOG AS4 the export ~~as the a~~ CPP
284 structure is ~~in itself not~~ insufficient ~~for communicate as because~~ it does not include
285 ~~information about the counterparty and agreement-related information.~~

286 **4.3 Agreement Export**

287 For ENTISOG AS4, which uses the AS4 concept of “agreements”, the configuration for a
288 partner is to be derived from an Agreement parameter set, as described in section 3.6, along
289 with data from referenced profiles (see section 3.2), party information (section 3.1), network
290 and network security information (see section 3.3) and security sets (see section 3.4).

291 ~~The main difference to configuration based on party profiles is that with agreements,~~
292 ~~multiple~~ agreements can be active at the same time. Each of them relates to certificates
293 specified in the certificate sets of the associated profiles. Furthermore, an agreement has an
294 identifier that is included in the AS4 message as the value of an AS4 header. This allows
295 receivers of AS4 messages to select the agreement that applies to the message, and process
296 it accordingly.

297 **4.4 Delegation Export**

298 The draft CPPA3 schema has a concept called “delegation channels” that delegation
299 information can be mapped to. This concept can be used in CPA documents in which one or
300 both parties P1 and or P2 use at least one service provider S. The CPA XML structure then
301 has P1 as the agreement Party and P2 as the agreement counterparty. For the party P that
302 delegates messaging to S, there will be a channel that simply expresses that any of P’s
303 actions bound to send will use S as the sender or receiver. Whether that communication
304 uses AS2 or AS4 or other aspects of the configuration are determined by P’s configuration
305 for S.

306 The users of this delegation information are not the AS2 or AS4 messaging gateways, but
307 business applications or middleware applications.

- 308 • A sender party P1 can use the information to determine that a EDIG@S message to
309 P2 is to be sent to S instead of to P2 and therefore must use a messaging
310 configuration for use with S. In this case, the messaging receiver (*AS2-To* in AS2 or
311 *To/PartyID* in AS4) is different from the EDIG@S XML recipient.
- 312 • A receiver party P2 can use the information to determine that a EDIG@S message
313 from S may (from a business point of view) be from a business party P1. This means
314 that the messaging sender (*AS2-From* in AS2 or *From/PartyID* in AS4) identity is
315 different from the EDIG@S XML recipient identity.

316 Alternatively, the delegation information can be exported in CSV or another tabular format
317 that is simpler than the CPPA3 the XML format.

318 **4.5 Network and Network Security Export**

319 The network and network security parameters are typically not used by the AS2 or AS4
320 endpoints directly. Instead, they are used in rules on the company’s firewall and configured
321 by the company’s network administrators, which are typically a different people team than
322 from the AS4 system administrators. Although the CPP and CPA formats include the relevant
323 information, a simpler and separate export format could be used. For example, for Linux one
324 could generate a shell script that invokes the *iptables* command with the relevant options, or
325 a simple file in CSV or another tabular format. These simpler exports could be handed over
326 to network management for review and deployment.

327 **5 CPPA3 Usage Profile**

328 As ENTSOG AS4 is a highly constrained profile, which has fixed values for many features, a
329 CPPA3 Usage Profile can be used that simplifies its use. The following implementation
330 guidelines are provided:

331 **5.1 CPP and CPA**

332 CPPA3 defines two document types. CPP is an XML format for a party profile. CPA is a
 333 similar format for party agreements. They have similar structures and the latter can be
 334 formed automatically by unifying (merging) the content of two of the former.

335 A CPP has a ProfileIdentifier. This identifier serves the purpose of the (Sub) Profile
 336 Identifier specified in section 3.2. Its value is not used in AS4.

337 A CPA has an AgreementIdentifier. This identifier is used in AS4 and has an
 338 important role in ENTSOG AS4. Its content can be derived from the agreement sequence
 339 number (see section 3.6) and the party identifiers (see section 3.2).

340 A CPP MAY have an allowed attribute that points to a list of party identifiers. This list can
 341 be populated from the list of counter party identifiers (see section 3.1).

342 CPP and CPA have ActivationDate and ExpirationDate elements set based on
 343 values defined in 3.2 and 3.6.

344 **5.2 Party Information**

345 The CPPA3 PartyInfo element, which provides party information, is profiled as follows:

- 346 • The PartyId value for a party MUST be to the EIC Code for the party.
- 347 • The PartyId/@type attribute MUST be set to the fixed value
 348 http://www.entsoe.eu/eic-codes/eic-party-codes-x.
- 349 • The PartyName MUST be set to party's Party Name.

350 As an example, the following screenshot was taken from the ENTSOG approved EIC code
 351 section on ENTSOG's Website [EIC].

352

353



EIC PARTY CODES (X)			Last update on 2017-09-15	
EIC Code	Party Name	Display Name		
21X000000010012	APX Gas NL BV	APX-GAS-NL		
21X000000010020	APX Gas Zeebrugge BV	APX-GAS-ZEEBRUGG		
21X000000010012	APX Gas NL BV	APX-GAS-NL	Balance Responsible Party	
21X000000010020	APX Gas Zeebrugge BV	APX-GAS-ZEEBRUGG	Balance Responsible Party	

354 The first entry on this line can therefore be represented in CPPA3 as the following
 355 PartyInfo content:

```
356 <cppa:PartyName xml:lang="en">APX Gas NL BV</cppa:PartyName>
357 <cppa:PartyId type="http://www.entsoe.eu/eic-codes/eic-party-codes-x">21X000000010012</cppa:PartyId>
```

358 Certificates used for message layer signing and encryption MUST be provided as
 359 Certificate elements containing XML Signature KeyInfo elements. Within the
 360 KeyInfo, the full certificate chain MUST be provided, in order, from the leaf certificate to
 361 the issuing Certification Authority's root certificate, as X509Certificate elements.

362 Furthermore, a `CertificateDefaults` element MUST be included which MUST include
363 a `SigningCertificateRef` and an `EncryptionCertificateRef` element, which
364 reference a `Certificate`.

365 Note that in CPPA3, definition and use of certificates are separate. So, if a single certificate is
366 used for both signing and encryption, only one definition must be provided, to which there
367 are two references.

368 In a CPP, there is only a `PartyInfo` element. In a CPA, there is also a
369 `CounterPartyInfo` element. It relates to the other party in the agreement. It has the
370 same structure as the `PartyInfo` element.

371 5.3 Service Specification

372 All companies engaged in gas sector business can participate in one or more roles. The
373 ENTSOG AS4 Mapping Table [[AS4MAPAS4MAPAS4MAP](#)] provides a tabular definition of all
374 data exchanges specified in all ENTSOG Business Requirements Specification (BRS)
375 document. Therefore, it is possible to compute the full set of potential exchanges of any gas
376 company by selecting the exchanges in which the sending party role or the receiving party
377 role is one of the roles the company may perform.

378 The following example specifies the exchanges from the company in the ZSO role, where the
379 counterparty is a ZTZ. According to the mapping table, one of the services among these
380 roles is the A08 role. For this service, many action bindings are to be specified. Apart from
381 the binding for A08, other service bindings may follow. (Both further discussed after this
382 example).

```
383 <cppa:ServiceSpecification>
384   <cppa:PartyRole name="ZSO"/>
385   <cppa:CounterPartyRole name="ZTZ"/>
386   <cppa:ServiceBinding>
387     <cppa:Service type="http://edigas.org/service">A08</cppa:Service>
388     <!-- a number of action bindings, see below -->
389   </cppa:ServiceBinding>
390   <!-- other service binding definitions follow -->
391 </cppa:ServiceSpecification>
```

392 Within a service, separate `ActionBinding` elements MUST be provided for each message
393 exchange specified in the AS4 mapping table for the pair of roles. The following example
394 shows the content for the A08 service in the above example.

```
395 <cppa:ActionBinding sendOrReceive="send"
396   action="http://docs.oasis-open.org/ebxml-msg/as4/200902/action" id="ab_1_1">
397   <cppa:ChannelId>ch_send</cppa:ChannelId>
398   <cppa:PayloadProfileId>pp_ALW</cppa:PayloadProfileId>
399 </cppa:ActionBinding>
400 <cppa:ActionBinding sendOrReceive="receive"
401   action="http://docs.oasis-open.org/ebxml-msg/as4/200902/action" id="ab_1_3">
402   <cppa:ChannelId>ch_receive</cppa:ChannelId>
403   <cppa:PayloadProfileId>pp_ALU</cppa:PayloadProfileId>
404 </cppa:ActionBinding>
```

405 A party acting in a role may be either the sender or the recipient in the exchange. This is
406 reflected in the `sendOrReceive` attribute value. In the example, there is one exchange
407 from the party to the counterparty and one in the reverse direction.

408 In the ENTSOG AS4 profile [[AS4UPAS4UPAS4UP](#)], it is specified that the `action` is fixed to
409 be the AS4 default action. There may be multiple bindings for this action in the service,
410 which are only differentiated by the type of document exchanged. In a CPPA3 document
411 there are therefore multiple bindings for the action. In theory, multiple action bindings MAY
412 involve the same document. For this reason, CPPA3 does not include its payload
413 specification as child content of the `ActionBinding` element but instead has a
414 `PayloadProfileId` element whose content is an XML IDREF to a separate reusable
415 definition. The value of the identifier can be any XML ID, such as `pp_ALW` and `pp_ALU` in
416 the example below.

417 Similarly, there is a cross-referencing `ChannelId` element that specifies the
418 communication channel to be used for the exchange (see section 5.5).

419 5.4 *PayloadProfile*

420 In CPPA3, payload definitions can be specified in a `PayloadProfile` element. This
421 element has a mandatory `id` attribute that is the target of the `PayloadProfileId`
422 element. To support protocols like AS4 that may include multiple payloads, in CPPA3 the
423 `PayloadProfile` element includes as many `PayloadPart` elements as are needed. For
424 each part, the minimum and maximum cardinality is specified using attributes. For ENTSOG
425 AS4, where the payload is always a single EDIGAS document, the `PayloadPart` element
426 MUST contain a single `PayloadPart` element in which the `PartName` element has the
427 fixed content "businessdocument". It also MUST contain and a fixed
428 `MIMEContentType` element with fixed content "application/xml" and a fixed single
429 `Property` element with fixed name "EDIGASDocumentType", minimum and maximum
430 occurrence of "1" and a `value` attribute.

```
431 <cppa:PayloadProfile id="pp_ALU">  
432   <cppa:PayloadPart maxOccurs="1" minOccurs="1">  
433     <cppa:PartName>businessdocument</cppa:PartName>  
434     <cppa:MIMEContentType>application/xml</cppa:MIMEContentType>  
435     <cppa:Property maxOccurs="1" minOccurs="1" name="EDIGASDocumentType" value="ALU"/>  
436   </cppa:PayloadPart>  
437 </cppa:PayloadProfile>
```

438 The value of the `value` attribute MUST be set to the EDIG@S Document Type Code
439 specified for the exchange in the AS4 Mapping Table.

440 5.5 *ebMS3Channel*

441 For document based exchange, EU regulations [CR2009/715] specify that the common
442 solution is AS4. Therefore, all exchanges use the AS4 protocol. To configure AS4, which is a

443 profile of ebMS3, CPPA3 provides the ebMS3Channel element. This element provides
 444 configurability for all ebMS3 features using sub-elements, including reliable messaging, WS-
 445 Security, error handling etc. However, the ENTSOG AS4 Usage Profile [\[AS4UPAS4UPAS4UP\]](#)
 446 provides fixed values for these features.

447 To support usage profiles, and to obviate the need of entering predictable and repetitive
 448 values, CPPA3 provides a ChannelProfile element, the content of which is a mutually
 449 understood identifier of a usage profile.

450 These implementation guidelines require that the ChannelProfile element MUST occur
 451 and that its content MUST be set to "http://www.entsog.eu/AS4-USAGE-
 452 PROFILE/v3/UserMessageChannel". This value is a URI identifier, which is used for
 453 identification only. It does not resolve to a page on the ENTSOG site. The identifier identifies
 454 the use of version 3 of the ENTSOG AS4 Usage Profile. Apart from this element, other child
 455 elements MUST NOT be used.

456 Using the transport attribute, an ebMS3Channel references a transport. For AS4, this is
 457 always an HTTPTransport. Since there are different transports for incoming and outgoing
 458 messages, a CPPA3 document MUST include two ebMS3Channel elements, one for
 459 incoming and one for outgoing messages. They have different id attribute values (so they
 460 can be referenced unambiguously) and different transport attribute values (since they
 461 reference distinct transports). Otherwise, there are no differences between the two
 462 definitions.

```

463 <cppa:ebMS3Channel id="ch_send" transport="tr_send">
464   <cppa:ChannelProfile
465     >http://www.entsog.eu/AS4-USAGE-PROFILE/v3/UserMessageChannel</cppa:ChannelProfile>
466   </cppa:ebMS3Channel>
467 <cppa:ebMS3Channel id="ch_receive" transport="tr_receive">
468   <cppa:ChannelProfile
469     >http://www.entsog.eu/AS4-USAGE-PROFILE/v3/UserMessageChannel</cppa:ChannelProfile>
470   </cppa:ebMS3Channel>
471
  
```

472 Note that there also exist implicit other channels, in addition to these two. AS4 errors and
 473 receipts use different channels, viz. the HTTP backchannel. These channels are considered
 474 implied by the reference of the ENTSOG AS4 Usage profile using the ChannelProfile
 475 element. For use in AS4 products these implicit channels, and the configuration of all
 476 channels, may need to be made explicit. One way of doing that is to extend the CPPA3
 477 document by adding the implied content, under the control of the ChannelProfile
 478 value. The AS4-CPPA3 proof-of-concept [\[AS4CPOC\]](#) shows how this could be done in CPPA3,
 479 using an open source CPPA3 library module.

480 **5.6 HTTPTransport**

481 These implementation guidelines REQUIRE that each CPPA3 document has two
 482 HTTPTransport elements.

483 The first covers exchanges where the party specified in the `PartyInfo` element sends the
 484 AS4 message, and is therefore using HTTP in client capacity. In a CPP, it MUST contain a
 485 `ClientIPv4` and/or `ClientIPv6` child element that specifies the client IP addresses (or
 486 address ranges) from which the transport will be initiated.

487 The second transport covers the case where it receives the AS4 message, and is therefore
 488 using HTTP in server capacity. In a CPA, it MUST contain an `Endpoint` child element that
 489 specifies the URL at which the message handler accepts incoming connections. It MAY
 490 contain `ServerIPv4` and/or `ServerIPv6` child elements.

491 In a CPA, both `HTTPTransport` elements contain elements from both the party and the
 492 counterparty, in either direction. They therefore MUST contain `ClientIPv4` and/or
 493 `ClientIPv6` children elements and an `Endpoint` child element.

494 For example, in a CPP, these two `HTTPTransport` elements could look as follows:

```

495 <cppa:HTTPTransport id="tr_send">
496   <cppa:ClientIPv4>5.2.3.4</cppa:ClientIPv4>
497 </cppa:HTTPTransport>
498 <cppa:HTTPTransport id="tr_receive">
499   <cppa:Endpoint>https://tso5.eu/as4</cppa:Endpoint>
500 </cppa:HTTPTransport>
  
```

501 In a corresponding CPA example, these two `HTTPTransport` elements could look as
 502 follows:

```

503 <cppa:HTTPTransport id="tr_send">
504   <cppa:ClientIPv4>5.2.3.4</cppa:ClientIPv4>
505   <cppa:Endpoint>https://tso1.eu/as4</cppa:Endpoint>
506 </cppa:HTTPTransport>
507 <cppa:HTTPTransport id="tr_receive">
508   <cppa:ClientIPv4>1.2.3.4</cppa:ClientIPv4>
509   <cppa:Endpoint>https://tso5.eu/as4</cppa:Endpoint>
510 </cppa:HTTPTransport>
  
```

511 Just as there was a lot of implicit information in an `ebMS3Channel` element, there is
 512 information implicit in transport definitions. An example is that TLS is to be used in version
 513 1.2.

514 5.7 Delegation

515 In principle, CPPA3 can represent delegation information using its `DelegationChannel`
 516 element. A single CPP or CPA document can mix action bindings to `ebMS3Channel` and
 517 action bindings using `DelegationChannel`. However, as noted in section 4.4, simpler
 518 tabular formats may be of more practical use.

519

520 **6 EASEE-connect**

521 EASEE-connect [EASEE-CON] is a solution for the management and secure exchange of digital
522 parameters and identifiers prerequisite for engaging in an AS4/AS2 communication with
523 business partners in the European gas market. It can be viewed as an implementation of the
524 concepts presented in this document for the EASEE-gas community.

525 EASEE-connect is a digital platform developed by EASEE-gas whereby gas market participants
526 can create and manage their AS4 and AS2 company profiles and portfolio of business
527 connections in a simple and secure way. The platform provides a single repository of
528 technical information, contact details and AS4/AS2 settings that gas market participants
529 need to exchange with each other in order to establish a secure communication channel. By
530 accessing only one platform, gas companies can both manage their data and pull the data of
531 their partners.

532 EASEE-connect replaces the mail preparation and handling associated with traditional
533 business communication and the poorly updated and incomplete spreadsheets currently
534 used in the sector to manage this type of data. Furthermore, EASEE-connect meets
535 demanding security requirements.

536 By using EASEE-connect, gas companies have access to an automated profile management
537 system that helps them increase efficiency and quality of information, save time and money,
538 and avoid mistakes and security risks.

Formatted: Heading 1

539 **67** Revision History

Revision	Date	Editor	Changes Made
v0r1wd1	2017-09-14	PvdE	First Draft for discussion
v0r2wd2	2017-10-05	PvdE	Intermediate version for internal review
v0r3wd3	2017-10-10	PvdE, JM	Editorial fixes added back in
Version 0 Rev_0	2017-12-12	JM	Created version for publication
wd4	2020-09-29	PvdE	Draft for ITC KG; updates: <ul style="list-style-type: none"> • CPPA3 is standardized; • EASEE-Connect is in operation; • links updated.
Version 0 Rev_1	2020-XX-YY		

Formatted Table

Formatted: Font: (Default) +Body (Calibri)

Formatted: List Paragraph, Bulleted + Level: 1 + Aligned at: 0.63 cm + Indent at: 1.27 cm

540 **78 References**

- 541 [AS4] AS4 Profile of ebMS 3.0 Version 1.0. OASIS Standard, 23 January 2013.
542 <http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/profiles/AS4-profile/v1.0/>
- 543 [AS4AGR] ENTSOG AS4 Agreements and Agreement Updates. Revision 1. 2017-01-09.
544 [https://entsog.eu/interoperability-and-data-exchange-nc#as4-supporting-](https://entsog.eu/interoperability-and-data-exchange-nc#as4-supporting-documents)
545 [documents - https://entsog.eu/publications/common-data-exchange-](https://entsog.eu/publications/common-data-exchange-solutions#ENTSOG-AS4-AGREEMENTS-AND-AGREEMENT-UPDATES)
546 [solutions#ENTSOG-AS4-AGREEMENTS-AND-AGREEMENT-UPDATES](https://entsog.eu/publications/common-data-exchange-solutions#ENTSOG-AS4-AGREEMENTS-AND-AGREEMENT-UPDATES)
- 547 [AS4CPOC] ENTSOG AS4 Automated Configuration Proof of Concept.
548 https://bitbucket.org/ebcore/as4_mgmt_poc
- 549 [AS4UP] ENTSOG AS4 Profile. Current Version 3 Revision 56, 20162019-0305-2806.
550 [https://entsog.eu/interoperability-and-data-exchange-nc#as4-documents-for-](https://entsog.eu/interoperability-and-data-exchange-nc#as4-documents-for-implementation)
551 [implementation https://entsog.eu/publications/common-data-exchange-](https://entsog.eu/publications/common-data-exchange-solutions#AS4-USAGE-PROFILE)
552 [solutions#AS4-USAGE-PROFILE](https://entsog.eu/publications/common-data-exchange-solutions#AS4-USAGE-PROFILE)
- 553 [AS4MAP] ENTSOG Service/Action table [https://entsog.eu/interoperability-and-data-](https://entsog.eu/interoperability-and-data-exchange-nc#as4-documents-for-implementation)
554 [exchange-nc#as4-documents-for-implementation](https://entsog.eu/interoperability-and-data-exchange-nc#as4-documents-for-implementation)
555 [https://www.entsog.eu/publications/common-data-exchange-](https://www.entsog.eu/publications/common-data-exchange-solutions#ENTSOG-AS4-MAPPING-TABLE)
556 [solutions#ENTSOG-AS4-MAPPING-](https://www.entsog.eu/publications/common-data-exchange-solutions#ENTSOG-AS4-MAPPING-TABLE)
557 [TABLEhttps://www.entsog.eu/publications/common-data-exchange-solutions.](https://www.entsog.eu/publications/common-data-exchange-solutions)
- 558 [CPPA3SPEC] Collaboration Protocol Profile and Agreement Version 3.0. [Specification](https://www.oasis-open.org/committees/documents.php?wg-abbrev=ebcore)
559 [Working Draft](https://www.oasis-open.org/committees/documents.php?wg-abbrev=ebcore)OASIS Committee Specification. [https://www.oasis-](https://www.oasis-open.org/committees/documents.php?wg-abbrev=ebcore)
560 [open.org/committees/documents.php?wg-abbrev=ebcore](https://www.oasis-open.org/committees/documents.php?wg-abbrev=ebcore) [https://docs.oasis-](https://docs.oasis-open.org/ebcore/cppa/v3.0/)
561 [open.org/ebcore/cppa/v3.0/](https://docs.oasis-open.org/ebcore/cppa/v3.0/)
- 562 [CPPA3XSD] Collaboration Protocol Profile and Agreement Version 3.0. [OASIS Committee](https://docs.oasis-open.org/ebcore/cppa/v3.0/cs01/schema/)
563 [Specification. XML Schema](https://docs.oasis-open.org/ebcore/cppa/v3.0/cs01/schema/) [Working Draft.](https://www.oasis-open.org/committees/documents.php?wg-abbrev=ebcore) [https://docs.oasis-](https://docs.oasis-open.org/ebcore/cppa/v3.0/cs01/schema/)
564 [open.org/ebcore/cppa/v3.0/cs01/schema/](https://www.oasis-open.org/committees/documents.php?wg-abbrev=ebcore) [https://www.oasis-](https://www.oasis-open.org/committees/documents.php?wg-abbrev=ebcore)
565 [open.org/committees/documents.php?wg-abbrev=ebcore](https://www.oasis-open.org/committees/documents.php?wg-abbrev=ebcore)
- 566 [CR2009/715]] REGULATION (EC) No 715/2009 OF THE EUROPEAN PARLIAMENT AND OF THE
567 COUNCIL of 13 July 2009 on conditions for access to the natural gas
568 transmission networks and repealing Regulation (EC) No 1775/2005.
569 <http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32009R0715>
- 570 [CR2015/703] COMMISSION REGULATION (EU) 2015/703 of 30 April 2015 establishing a
571 network code on interoperability and data exchange rules.
572 <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015R0703>
- 573 [EASEE-CON] EASEE-Connect <https://easee-gas.eu/easee-connect>

Field Code Changed

Field Code Changed

- 574 [EDIG@S] EASEE-gas EDIG@S. Version 5.1. <https://www.edigas.org/version-5/>
575 <http://www.EDIG@S.org/version-5/>
- 576 [EIC] ENTSOG Approved EIC Party Codes.
577 <https://www.entsog.eu/eic-codes/eic-party-codes-x>
578 <https://www.entsog.eu/approved-codes#all-approved-eic-codes>
- 579 [HOWTO] Setting up an AS4 System. Version 23. 20162019-1105-1615.
580 [https://www.entsog.eu/interoperability-and-data-exchange-nc#as4-](https://www.entsog.eu/interoperability-and-data-exchange-nc#as4-supporting-documents)
581 [supporting-documents](https://www.entsog.eu/interoperability-and-data-exchange-nc#as4-supporting-documents)
582 [https://entsog.eu/publications/common-data-exchange-solutions#AS4-HOW-](https://entsog.eu/publications/common-data-exchange-solutions#AS4-HOW-TO-SET-UP-A-SYSTEM-DOCUMENT)
583 [TO-SET-UP-A-SYSTEM-DOCUMENT](https://entsog.eu/publications/common-data-exchange-solutions#AS4-HOW-TO-SET-UP-A-SYSTEM-DOCUMENT)
- 584 [WSUP] ENTSOG Integrated Data Exchange Usage Profile. Current Version 0 Revision 0.
585 2017-03-28. [https://www.entsog.eu/interoperability-and-data-exchange-](https://www.entsog.eu/interoperability-and-data-exchange-nc#integrated-data-exchange-usage-profile)
586 [nc#integrated-data-exchange-usage-profile](https://www.entsog.eu/interoperability-and-data-exchange-nc#integrated-data-exchange-usage-profile)
587 [https://entsog.eu/publications/common-data-exchange-](https://entsog.eu/publications/common-data-exchange-solutions#INTEGRATED-DATA-EXCHANGE-USAGE-PROFILE)
588 [solutions#INTEGRATED-DATA-EXCHANGE-USAGE-PROFILE](https://entsog.eu/publications/common-data-exchange-solutions#INTEGRATED-DATA-EXCHANGE-USAGE-PROFILE)
- 589 [INTUP] ENTSOG Interactive Profile. Current Version 0 Revision 0.
590 [https://www.entsog.eu/interoperability-and-data-exchange-nc#interactive-](https://www.entsog.eu/interoperability-and-data-exchange-nc#interactive-data-exchange-usage-profile)
591 [data-exchange-usage-profile](https://www.entsog.eu/interoperability-and-data-exchange-nc#interactive-data-exchange-usage-profile) [https://entsog.eu/publications/common-data-](https://entsog.eu/publications/common-data-exchange-solutions#INTERACTIVE-DATA-EXCHANGE-USAGE-PROFILE)
592 [exchange-solutions#INTERACTIVE-DATA-EXCHANGE-USAGE-PROFILE](https://entsog.eu/publications/common-data-exchange-solutions#INTERACTIVE-DATA-EXCHANGE-USAGE-PROFILE)
- 593 [CDEST] ENTSOG Common Data Exchange Solution Table.
594 [https://www.entsog.eu/interoperability-and-data-exchange-nc#common-](https://www.entsog.eu/interoperability-and-data-exchange-nc#common-network-operation-tools)
595 [network-operation-tools](https://www.entsog.eu/interoperability-and-data-exchange-nc#common-network-operation-tools)
596 [https://entsog.eu/publications/common-data-exchange-solution-](https://entsog.eu/publications/common-data-exchange-solution-table#COMMON-DATA-EXCHANGE-SOLUTION-TABLE)
597 [table#COMMON-DATA-EXCHANGE-SOLUTION-TABLE](https://entsog.eu/publications/common-data-exchange-solution-table#COMMON-DATA-EXCHANGE-SOLUTION-TABLE)

Field Code Changed