1 # ENTSOG Configuration Management Approach

2 **Version 0 Revision 3 – 2020-XX-YY**

## ***Disclaimer***

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

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

## Table of contents

# 1 Introduction

ENTSOG has produced a number of usage profiles [AS4UP, WSUP, INTUP] to support the implementation of the common data exchange solutions defined in the Network Code on Interoperability and Data Exchange [CR2015/703]. AS4, which is used for document-based data exchange, and SOAP/HTTPS, which is used for integrated exchange, support machine-to-machine exchange of structured information. To use these solutions successfully, TSOs and their counterparties need to configure various communication parameters in their communication products. Many of these parameters are pre-defined in the ENTSOG specifications and can be inferred by referencing the applicable specification version, but others are unique to specific parties and counterparties, and therefore need to be exchanged and configured between parties.

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

This document provides the following:

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

ENTSOG does not currently intend to develop or host this platform, but encourages its stakeholders, and stakeholder communities to develop and operate such a platform.

## 2 Required Features

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

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

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

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

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

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

The platform should be able to support the full lifecycle or data communication. Companies periodically update their communication services and configuration parameters change

accordingly. They may take on new roles, and outsource others. Companies also have other environments than their production systems, and need counterparty data to configure each of them, and need to be able to indicate in which intervals environments and configuration sets are valid.

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

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

# 3 Data Exchange Parameters

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

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

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

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

- A party has a “test” and a “production” environment for document-based exchange. This is handled as two (sub) profiles, with different endpoints hosted on different servers with different IP addresses and possibly different certificate sets.
- A party has two “production” environments for document-based exchange that are the same except that the first expires a month after the second is activated and that they are linked to different certificate sets. This can occur during a certificate switch period.
- A party has a “production” environment for document-based AS4 exchange and 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 regular test environment; the other is being used to test a new vendor product that the party will migrate to.

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

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

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

## 3.1 Party Parameters

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

This group also includes contact information which obviously is not directly used in a 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 |

## 3.2 (Sub) Profile Parameters

For each party, multiple party (sub) profiles may be defined. A (sub) profile is valid in an environment, uses a (version of a) data exchange solution on a URI, is valid in a certain 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 | The role of the party for which this is a sub-profile. Must be one of the roles party may perform.<br>If none specified, the sub profile applies to all roles that party may perform | 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 | Indication which data exchange solution is used. Possible values are ENTSOG AS4, ENTSOG Integrated Data Exchange Profile A, B or C.<br>Other values can be used for other solutions (e.g. legacy solutions, or solutions with NRA approval), such as EASEE-gas AS2. | 1 |
| Data Exchange Solution version | Optional protocol version, useful in case future incompatible changes are made. The current version for ENTSOG AS4 is 3.6. | 0..1 |
| Data Exchange Product | Vendor name and name and version of the product the solution is deployed on.<br>Note: this element is for information only and parties are not required to disclose it. It may be useful for trouble shooting. | 0..1 |

| Parameter | Description | Cardinality |
|---|---|---|
| Endpoint URI | HTTP or HTTPS URI for the endpoint.<br>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.<br>Presence/absence dependent on data exchange solution used: not needed for interactive exchange.<br>Referenced certificates must be valid in the validity interval of the profile. | 0..1 |

## *3.3 Network and Network Security Parameters*

A sub profile may be constrained to be used with a set of network parameters and network 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<br>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<br>Requires the IPv4 supported parameter to be true.<br>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<br>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<br>Requires the IPv6 supported parameter to be true.<br>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 |

## *3.4 Certificate Sets*

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.<br>Note: TLS client authentication is allowed, but not recommended in ENTSOG data exchange solutions. | 0..1 |

## 3.5 Business Process Relations

Business process information is provided in the ENTSOG Service Action table [AS4MAP], which lists, for each pair of roles, the types of EDIG@S or other documents that can be exchanged between them. The table includes service area codes which are linked to EDIG@S versions (4, 5, 6) and can therefore be used to indicate which EDIG@S version(s) a party supports. From that table, in combination with the information on roles performed by parties, the relevant AS4 parameters (Service, Action, From Role, To Role) and the EDIG@S Document Type can be inferred. By listing roles for parties, and listing counterparties for parties, all potential exchanges between parties can be computed.

## 3.6 Agreement Parameters

ENTSOG AS4 uses the AS4 agreement concept and requires the AS4 agreement reference header to be present in AS4 messages. This allows its users to handle certificate switches in a much more flexible way than the previous AS4 practice. As both involved parties may have multiple different (sub) profiles, linking to distinct certificate sets, an agreement is a relation 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 Reference | A reference to a sub-profile of another party | 1 |
| An agreement sequence | An integer that indicates a version of an | 1 |

| Parameter | Description | Cardinality |
|---|---|---|
| number | agreement. | |
| 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 |

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

## *3.7 Delegation*

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

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

The delegation relation has the following properties:

| Parameter | Description | Cardinality |
|---|---|---|
| Delegating Party Profile | Reference to a registered party | 1 |
| Delegating Party Role | The role for which the party delegates | 0..n |

| Parameter | Description | Cardinality |
|---|---|---|
| | communication | |
| 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 |

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

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

# 4 Structured Export

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

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

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

## 4.1 CPPA3 Profile

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

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

## 4.2 Profile Export

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

For ENTSOG AS4 the export as a CPP structure is in itself not sufficient for communicate because it does not include information about the counterparty and agreement-related information.

## 4.3 Agreement Export

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

Multiple agreements can be active at the same time. Each of them relates to certificates specified in the certificate sets of the associated profiles. Furthermore, an agreement has an identifier that is included in the AS4 message as the value of an AS4 header. This allows receivers of AS4 messages to select the agreement that applies to the message, and process it accordingly.

## 4.4 Delegation Export

The draft CPPA3 schema has a concept called “delegation channels” that delegation information can be mapped to. This concept can be used in CPA documents in which one or both parties P1 and or P2 use at least one service provider S. The CPA XML structure then has P1 as the agreement Party and P2 as the agreement counterparty. For the party P that delegates messaging to S, there will be a channel that simply expresses that any of P’s actions bound to send will use S as the sender or receiver. Whether that communication

uses AS2 or AS4 or other aspects of the configuration are determined by P's configuration for S.

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

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

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

### *4.5 Network and Network Security Export*

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

## *5 CPPA3 Usage Profile*

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

### *5.1 CPP and CPA*

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

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

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

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

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

## *5.2 Party Information*

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

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

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

| | | | |
|---|---|---|---|
| 21X0000000010012 | APX Gas NL BV | APX-GAS-NL | Balance Responsible Party |
| 21X0000000010020 | APX Gas Zeebrugge BV | APX-GAS-ZEEBRUGG | Balance Responsible Party |

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

```
<cppa:PartyName xml:lang="en">APX Gas NL BV</cppa:PartyName>
<cppa:PartyId type="http://www.entsoe.eu/eic-codes/eic-party-codes-x">21X0000000010012</cppa:PartyId>
```

Certificates used for message layer signing and encryption MUST be provided as `Certificate` elements containing XML Signature `KeyInfo` elements. Within the `KeyInfo`, the full certificate chain MUST be provided, in order, from the leaf certificate to the issuing Certification Authority's root certificate, as `X509Certificate` elements. Furthermore, a `CertificateDefaults` element MUST be included which MUST include a `SigningCertificateRef` and an `EncryptionCertificateRef` element, which reference a `Certificate`.

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

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

## 5.3 Service Specification

All companies engaged in gas sector business can participate in one or more roles. The ENTSOG AS4 Mapping Table [AS4MAP] provides a tabular definition of all data exchanges specified in all ENTSOG Business Requirements Specification (BRS) document. Therefore, it is possible to compute the full set of potential exchanges of any gas company by selecting the exchanges in which the sending party role or the receiving party role is one of the roles the company may perform.

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

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

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

```
<cppa:ActionBinding sendOrReceive="send"
    action="http://docs.oasis-open.org/ebxml-msg/as4/200902/action" id="ab_1_1">
        <cppa:ChannelId>ch_send</cppa:ChannelId>
        <cppa:PayloadProfileId>pp_ALW</cppa:PayloadProfileId>
      </cppa:ActionBinding>
      <cppa:ActionBinding sendOrReceive="receive"
    action="http://docs.oasis-open.org/ebxml-msg/as4/200902/action" id="ab_1_3">
        <cppa:ChannelId>ch_receive</cppa:ChannelId>
        <cppa:PayloadProfileId>pp_ALU</cppa:PayloadProfileId>
</cppa:ActionBinding>
```

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

In the ENTSOG AS4 profile [AS4UP], it is specified that the `action` is fixed to be the AS4 default action. There may be multiple bindings for this action in the service, which are only differentiated by the type of document exchanged. In a CPPA3 document there are therefore multiple bindings for the action. In theory, multiple action bindings MAY involve the same document. For this reason, CPPA3 does not include its payload specification as child content of the `ActionBinding` element but instead has a `PayloadProfileId`

element whose content is an XML IDREF to a separate reusable definition. The value of the identifier can be any XML ID, such as `pp_ALW` and `pp_ALU` in the example below.

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

## *5.4 PayloadProfile*

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

```
<cppa:PayloadProfile id="pp_ALU">
    <cppa:PayloadPart maxOccurs="1" minOccurs="1">
      <cppa:PartName>businessdocument</cppa:PartName>
      <cppa:MIMEContentType>application/xml</cppa:MIMEContentType>
      <cppa:Property maxOccurs="1" minOccurs="1" name="EDIGASDocumentType" value="ALU"/>
    </cppa:PayloadPart>
</cppa:PayloadProfile>
```

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

## *5.5 ebMS3Channel*

For document based exchange, EU regulations [CR2009/715] specify that the common solution is AS4. Therefore, all exchanges use the AS4 protocol. To configure AS4, which is a profile of ebMS3, CPPA3 provides the `ebMS3Channel` element. This element provides configurability for all ebMS3 features using sub-elements, including reliable messaging, WS-Security, error handling etc. However, the ENTSOG AS4 Usage Profile [AS4UP] provides fixed values for these features.

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

These implementation guidelines require that the `ChannelProfile` element MUST occur and that its content MUST be set to "`http://www.entsog.eu/AS4-USAGE-PROFILE/v3/UserMessageChannel`". This value is a URI identifier, which is used for

identification only. It does not resolve to a page on the ENTSOG site. The identifier identifies the use of version 3 of the ENTSOG AS4 Usage Profile. Apart from this element, other child elements MUST NOT be used.

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

```
<cppa:ebMS3Channel id="ch_send" transport="tr_send">
  <cppa:ChannelProfile
        >http://www.entsog.eu/AS4-USAGE-PROFILE/v3/UserMessageChannel</cppa:ChannelProfile>
</cppa:ebMS3Channel>
<cppa:ebMS3Channel id="ch_receive" transport="tr_receive">
   <cppa:ChannelProfile
        >http://www.entsog.eu/AS4-USAGE-PROFILE/v3/UserMessageChannel</cppa:ChannelProfile>
</cppa:ebMS3Channel>
```

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

## *5.6 HTTPTransport*

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

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

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

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

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

```
<cppa:HTTPTransport id="tr_send">
    <cppa:ClientIPv4>5.2.3.4</cppa:ClientIPv4>
</cppa:HTTPTransport>
<cppa:HTTPTransport id="tr_receive">
    <cppa:Endpoint>https://tso5.eu/as4</cppa:Endpoint>
</cppa:HTTPTransport>
```

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

```
<cppa:HTTPTransport id="tr_send">
    <cppa:ClientIPv4>5.2.3.4</cppa:ClientIPv4>
    <cppa:Endpoint>https://tso1.eu/as4</cppa:Endpoint>
</cppa:HTTPTransport>
<cppa:HTTPTransport id="tr_receive">
    <cppa:ClientIPv4>1.2.3.4</cppa:ClientIPv4>
    <cppa:Endpoint>https://tso5.eu/as4</cppa:Endpoint>
</cppa:HTTPTransport>
```

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

### *5.7 Delegation*

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

## *6 EASEE-connect*

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

EASEE-connect is a digital platform developed by EASEE-gas whereby gas market participants can create and manage their AS4 and AS2 company profiles and portfolio of business connections in a simple and secure way. The platform provides a single repository of technical information, contact details and AS4/AS2 settings that gas market participants need to exchange with each other in order to establish a secure communication channel. By

accessing only one platform, gas companies can both manage their data and pull the data of their partners.

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

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

# 7 Revision History

| Revision | Date | Editor | Changes Made |
|---|---|---|---|
| wd1 | 2017-09-14 | PvdE | First Draft for discussion |
| wd2 | 2017-10-05 | PvdE | Intermediate version for internal review |
| wd3 | 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:<br>• CPPA3 is standardized;<br>• EASEE-Connect is in operation;<br>• links updated. |
| Version 0 Rev_1 | 2020-XX-YY | | |

# 8 References

[AS4] AS4 Profile of ebMS 3.0 Version 1.0. OASIS Standard, 23 January 2013. http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/profiles/AS4-profile/v1.0/

[AS4AGR] ENTSOG AS4 Agreements and Agreement Updates. Revision 1. 2017-01-09. https://entsog.eu/interoperability-and-data-exchange-nc#as4-supporting-documents

[AS4CPOC] ENTSOG AS4 Automated Configuration Proof of Concept. https://bitbucket.org/ebcore/as4_mgmt_poc

[AS4UP] ENTSOG AS4 Profile. Current Version 3 Revision 6, 2019-05-06. https://entsog.eu/interoperability-and-data-exchange-nc#as4-documents-for-implementation

[AS4MAP] ENTSOG Service/Action table https://entsog.eu/interoperability-and-data-exchange-nc#as4-documents-for-implementationhttps://www.entsog.eu/publications/common-data-exchange-solutions .

[CPPA3SPEC] Collaboration Protocol Profile and Agreement Version 3.0. OASIS Committee Specification. https://docs.oasis-open.org/ebcore/cppa/v3.0/

[CPPA3XSD] Collaboration Protocol Profile and Agreement Version 3.0. OASIS Committee Specification. XML Schema. https://docs.oasis-open.org/ebcore/cppa/v3.0/cs01/schema/

[CR2009/715]] REGULATION (EC) No 715/2009 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 July 2009 on conditions for access to the natural gas transmission networks and repealing Regulation (EC) No 1775/2005. http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32009R0715

[CR2015/703] COMMISSION REGULATION (EU) 2015/703 of 30 April 2015 establishing a network code on interoperability and data exchange rules. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015R0703

[EASEE-CON] EASEE-Connect https://easee-gas.eu/easee-connect

[EDIG@S] EASEE-gas EDIG@S. Version 5.1. https://www.edigas.org/version-5/

[EIC] ENTSOG Approved EIC Party Codes. https://www.entsog.eu/approved-codes#all-approved-eic-codes

[HOWTO] Setting up an AS4 System. Version 3. 2019-05-15. https://www.entsog.eu/interoperability-and-data-exchange-nc#as4-supporting-documents

[WSUP] ENTSOG Integrated Data Exchange Usage Profile. Current Version 0 Revision 0. 2017-03-28. https://www.entsog.eu/interoperability-and-data-exchange-nc#integrated-data-exchange-usage-profile

[INTUP] ENTSOG Interactive Profile. Current Version 0 Revision 0. https://www.entsog.eu/interoperability-and-data-exchange-nc#interactive-data-exchange-usage-profile

[CDEST] ENTSOG Common Data Exchange Solution Table. https://www.entsog.eu/interoperability-and-data-exchange-nc#common-network-operation-tools