1   **ENTSOG AS4 Agreements and Agreement Updates**

2   **Version Rev_1 – 2017-01-09**

3 **Table of contents**

14

1   *Introduction*

The current version Rev_3 of the ENTSOG AS4 profile [AS4TSO] introduces the concept of agreements and agreement updates to the ENTSOG AS4 profile. The agreement concept is an established ebXML concept for (versions of) messaging technical configurations that is applied to AS4 [AS4]. In ENTSOG AS4, it is used for certificate updates. Agreement Update, a generalisation of peer-to-peer online certificate exchange, is standardised at OASIS in the separate ebCore Agreement Update specification [AU]. Together, agreements and agreement updates enable a flexible mechanism for exchanging certificates and for managing and updating security configurations for signing and encryption of ENTSOG AS4 messages.

Software vendors should note that as AS4 products for use with the ENTSOG profile will be required to support these new features from 1 July 2017, to make it possible to implement these features in production. This document explains some of the consequences of the use of these concepts with AS4 and the impact and requirements on AS4 implementations and their deployments, in order to allow solution providers to determine if their products need any enhancements or adjustments to support this features and to make any adjustments in time for use by their users.

The audience for this document are providers of solutions supporting the AS4 Usage Profile for TSO [AS4TSO] and implementers of those solutions within the gas industry. This document is informative only. It is only intended to help implementers, but does not replace or overrule the functionality specified in the ENTSOG AS4 profile and the underlying AS4 and ebCore Agreement Update specifications. This document complements the "Setting Up and AS4 System" document [AS4SETUP].

2   Agreements

2.1   Agreements and P-Modes

In ebMS3, **AgreementRef** is one of the fields in the **Messaging** header. The content of the **AgreementRef** header is configured using the **PMode.Agreement** processing mode parameter ([EBMS3], section 5.2.2.7). In ebMS3, **AgreementRef** is optional. However, in the ENTSOG AS4 profile, its use is mandatory and the P-Mode parameter must therefore be set.

Depending on how the P-Modes (processing modes) are configured, in ebMS3 there may be, for a given combination of the parameters **Pmode.Initiator.Party** (controlling the **From** header value), **Pmode.Responder.Party** (the **To** header), **Pmode[1].BusinessInfo.Service** (the **Service** header) and **Pmode[1].BusinessInfo.Action** (the **Action** header), multiple P-Modes with distinct values for **Pmode.Agreement** (which controls the **AgreementRef** header). This functionality is used in the ENTSOG AS4 profile and must be supported by AS4 products used to exchange ENTSOG AS4 messages.

In this document we will discuss implementation aspects of agreements and P-Mode selection for incoming and outgoing messages. For these cases we will look at configurations and updates to configurations.

2.2   Certificates and P-Modes

P-Modes and P-Modes for ENTSOG AS4 in particular specify the certificates used to secure the AS4 message. The **Pmode[1].Security.X509.Signature.Certificate** specifies the signing certificate and **Pmode[1].Security.X509.Encryption.Certificate** the encryption certificate.

Different P-Modes for the same communication partner may therefore use different certificates. In the ENTSOG AS4 profile, certificates are associated with agreements. It is not sufficient for a product to allow certificates to be specified for communication partners. Instead, certificates are specified for P-Modes and linked not only to the communication partner but also to the **Pmode.Agreement** parameter, reflecting one configuration with that partner.

P-Modes that specify use of certificates have a validity interval that is dependent on the validity interval of those certificates. The ENTSOG AS4 profile is designed to support certificate rollover by having overlapping validity intervals for certificates and for the P-Modes that use them. AS4 products for use with ENTSOG AS4 must support this feature.

2.3   Incoming Messages

The expected handling of agreements in incoming messages has an impact on the way an AS4 MSH implements the **Receive** operation (see Figure 1 in section 2.1.1, Messaging Model, of ebMS3 Core [EBMS3]).
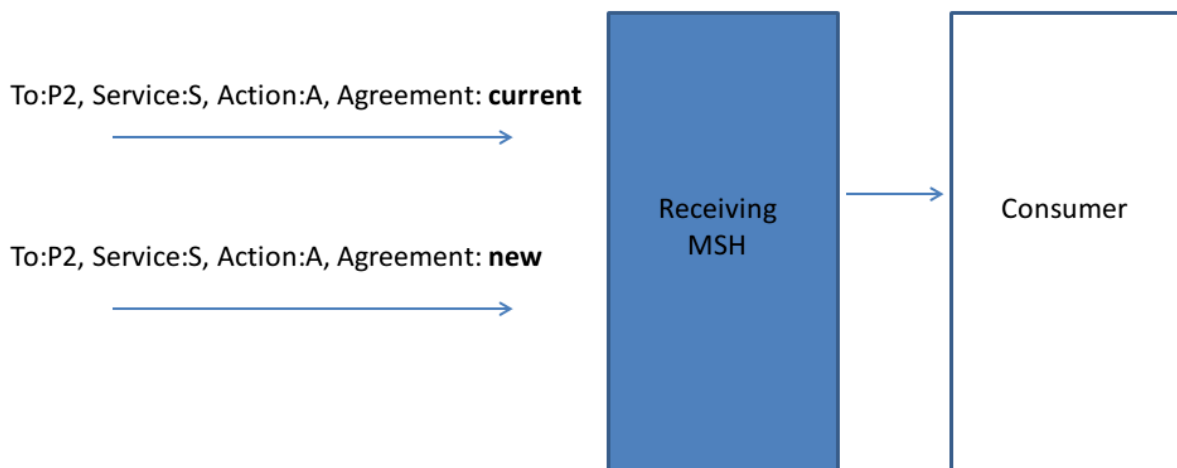
Messaging Model
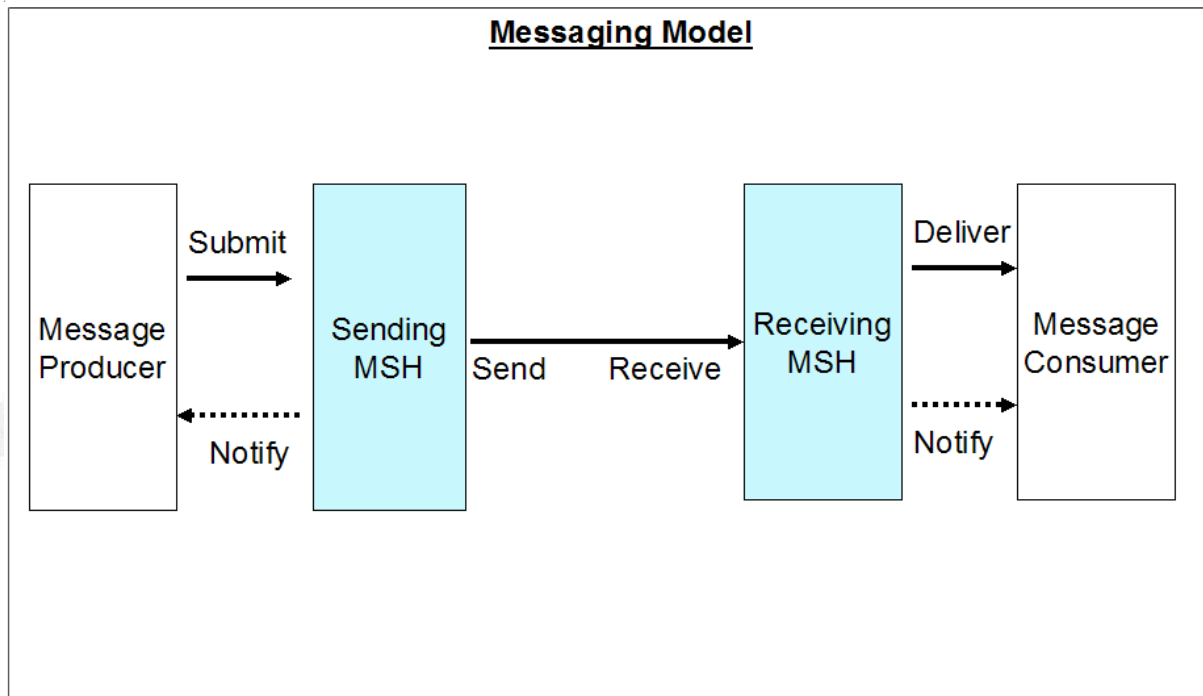
72

73 The ENTSOG AS4 profile requires AS4 products to be able to set the **AgreementRef** header
74 value and requires products to include the **AgreementRef** header value when looking up the
75 P-Mode that controls the processing of an incoming message ([AS4TSO], section 2.2.3.1).
76 This is a constraint on implementations, as the ebMS3 and AS4 specifications are
77 underspecified as to how P-Mode are determined and this behaviour is therefore
78 implementation-specific (see https://issues.oasis-open.org/browse/EBXMLMSG-48). Not all
79 currently available AS4 products support these requirements. Vendors looking to provide
80 solutions to the gas industry for the ENTSOG AS4 profile are strongly encouraged to verify
81 that their products support these requirements.

82 The ENTSOG AS4 Usage Profile ([AS4TSO], section 2.3.2) also specifies that, for a specific
83 value for **Pmode.Agreement**, it must be possible to unambiguously determine the signing
84 and encryption certificates of the parties involved. For two messages with the same values
85 for all ebMS3 headers except for **AgreementRef**, different P-Modes are expected to have
86 been configured and are to be inferred from incoming messages. It also means that if one or
87 both parties change(s) one or more certificates, a new P-Mode is expected to be created and
88 agreed by the parties with a distinct agreement identifier. Taken together, these constraints
89 imply that, for any incoming AS4 message, a compliant AS4 MSH is expected to be able to
90 infer unambiguously the certificates that are expected to be used.

91 The following diagram illustrates P-Mode inference for the ENTSOG AS4 profile. It assumes
92 that P-Modes for a current agreement and a new agreement are deployed at the same time
93 and that there are two P-Modes deployed that have the same values P2, S, A for To PartyId,
94 Service and Action, respectively, but differ in the values for Agreement (**current** or **new**). The
95 P-Mode configuration to use with the incoming messages can be found by the receiving MSH
96 by using the **AgreementRef** header as one of the keys to find the P-Mode that has this value

97   for the **Pmode.Agreement** parameter.

Incoming Messages

To:P2, Service:S, Action:A, Agreement: **current**

To:P2, Service:S, Action:A, Agreement: **new**

Receiving MSH

Consumer

98

99   If an incoming message uses (a) different certificate(s) than is specified for the Agreement
100   (and therefore the P-Mode), the message must be rejected using an **EBMS:0003** error,
101   because it is inconsistent with the processing mode of the MSH.

102   When deploying a new agreement, for incoming messages there is no need to immediately
103   deactivate all P-Modes related to the current agreement. To the contrary, it can be useful,
104   for incoming messages, to deploy the new P-Mode set in parallel to the current set. Any
105   messages still using the current agreement (including any delayed retries of previously
106   unsuccessful transmission) can then still be processed successfully. This is a deployment
107   decision, not a product requirement, but it is an option that the product must enable.

108   *2.4   Outgoing Messages*

109   The expected handling of agreements in outgoing messages relates to the way an AS4 MSH
110   implements the **Submit** operation (see Figure 1 in section 2.1.1, Messaging Model, of ebMS3
111   Core [EBMS3]). The **Submit** operation in ebMS3 is an abstract operation, the implementation
112   of which is left to implementations. This is intentional, as ebMS3 is about B2B messaging
113   whereas the backend interfaces are specific to enterprises, middleware, frameworks
114   programming languages etc. all of which are out of scope for ebMS3 as a standard. Likewise,
115   ENTSOG AS4 also does not provide a specification for this operation.

116 Agreements in ENTSOG AS4 are aspects of the configuration of the ebMS3 MSH and do not
117 relate to any business functionality or semantics and are therefore not relevant to the
118 message **Producer** or **Consumer**. This means that the **Agreement** is not a parameter that
119 business applications or middleware should have to specify when, in the role of a messaging
120 **Producer**, they **Submit** metadata and a payload to be sent to a communication partner to
121 the MSH. Products must support this and should only require the **Producer** to provide
122 enough metadata to allow the MSH to infer the P-Mode to be used for sending. This
123 metadata is left to implementations, but is likely to include at the minimum the destination
124 **PartyID** and party type, **Service** and **Action**.

125 In principle, in situations where there are multiple deployed P-Modes with different
126 **Agreement** identifiers for different sets of certificates, the metadata provided with the
127 **Submit** call is not sufficiently unambiguous to allow the sending MSH to determine which P-
128 Mode to use. In these situations, the logic to select one of multiple candidate P-Modes is left
129 to implementations.

Outgoing Messages
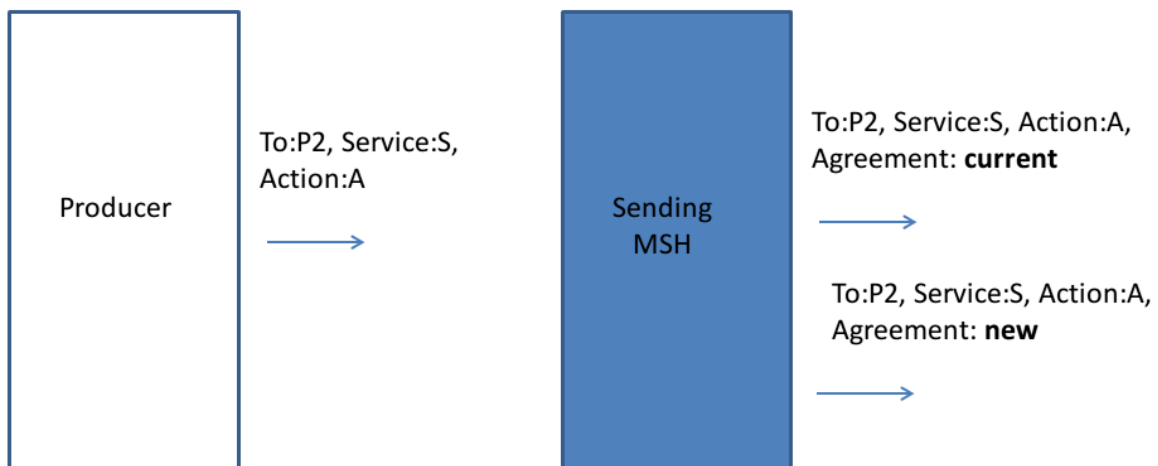
130

131 If the MSH is configured as described in section 3.4 of ENTSOG's "How to Set Up an AS4
132 System" [AS4SETUP], there actually need not be more than one applicable agreement. That
133 document recommends that, before using the agreement for business messages, it should
134 be used with the ebMS3 test service, as profiled in the ENTSOG AS4 profile. The test
135 message validates the correct configuration of the AS4 MSH and the environment in which it

136 is deployed, including properly configured certificates and properly configured firewalls. If
137 there is a new agreement, for outgoing messages, initially only the outgoing "test" message
138 needs to be deployed. Business messages (with business values for **Service** and **Action**) at
139 this point can still use the old agreement. Once use of the test service has successfully
140 validated the new agreement, the other P-Modes for the new agreement, covering outgoing
141 business messages, can be deployed and the P-Modes for outgoing messages for the
142 previous agreement deactivated. This is a deployment decision, not a product requirement.

143 The timeline in the following diagram illustrates this.
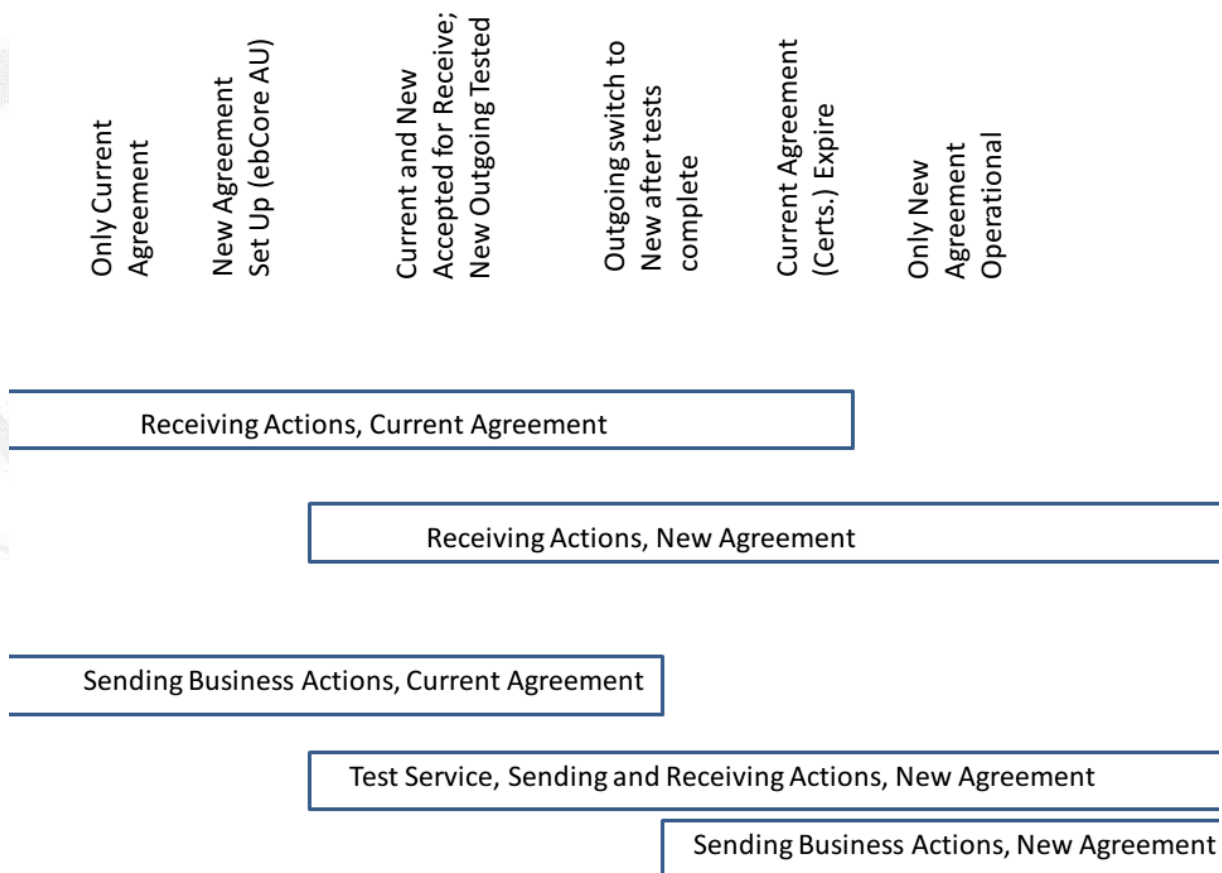
144
145 Initially, only one agreement is deployed, the current agreement. Its P-Modes are used for
146 both incoming and outgoing messages.

147 Then, a new agreement is formed, using ebCore Agreement Update. The AU protocol
148 guarantees an agreed activation date for the agreement, so that parties can prepare the
149 deployment of the relevant P-Modes.

150 Parties must be able to receive messages using the new agreement P-Modes from the
151 agreed activation date and time.

152 In principle, they can also use P-Modes for outgoing messages from that in time. However,
153 the diagram illustrates that, to be sure there are no issues with the new certificates, it is

154   recommendable to start with the test service. Once the test is successful, the new P-Modes
155   for outgoing business messages are safe to be used.

3   *Agreement Updates*

156

3.1   *ebCore Agreement Update*

157

158 The v2r0 version of the ENTSOG AS4 profile mandates AS4 implementations to provide an
159 API to manage AS4 configuration, but does not mandate a specific API. The new v3r0 version
160 more specifically requires the API to provide all functionality to implement the OASIS ebCore
161 Agreement Update specification [AU]. The latest version of the ENTSOG AS4 profile
162 mandates support for Agreement Update from 01.07.2017, and uses the protocol to update
163 certificates.

164 Sections 4.1 and 4.4 of the Agreement Update specification provide information on the use
165 of ebCore Agreement Update with ebMS3 and AS4. In essence, support for agreement
166 update for certificate updates requires a product to be able to configure a new set of P-
167 Modes using a set of currently deployed P-Modes as input, copying all parameter-value
168 settings except for those parameters that reference a certificate that is replaced. How the P-
169 Mode configuration is represented in the product (as database tables, XML files etc.) is left
170 to the product.

171 Agreement Update in ENTSOG AS4 uses AS4 itself to communicate the configuration
172 updates. For the MSH, these messages are just payloads targeting a specific pre-identified
173 service. The XML structures defined in Agreement Update can be processed within or
174 outside of the AS4 product, as long as any updates to the MSH configuration can be done
175 using the product's configuration API.

4   *References*

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

179 [AS4SETUP]   Setting up an AS4 System. ENTSOG INT0697-161115_Rev_2
180   http://www.entsog.eu/public/uploads/files/publications/INT%20Network%20C
181   ode/2015/INT0697_150625_Setting%20up%20an%20AS4%20System%20v1r0.
182   pdf

183 [AU]   OASIS ebCore Agreement Update Specification Version 1.0. OASIS Committee
184   Specification.
185   http://docs.oasis-open.org/ebcore/ebcore-au/v1.0/

186 [AS4MT]   ENTSOG AS4 Mapping Table.
187   http://www.entsog.eu/publications/as4#ENTSOG-AS4-MAPPING-TABLE

188 [AS4TSO]   ENTSOG AS4 Usage Profile for TSOs. ENTSOG INT 0488-161511_Rev_3
189   http://www.entsog.eu/publications/as4#AS4-USAGE-PROFILE

190 [EBMS3]   OASIS ebXML Messaging Services Version 3.0: Part 1, Core Features. OASIS
191   Standard. 1 October 2007. http://docs.oasis-open.org/ebxml-
192   msg/ebms/v3.0/core/os/

193 **5 _Revision History_**

Revision	Date	Editor	Changes Made
v0r1	2016-11-07	PvdE	First Draft for discussion
V0r2	2016-12-05	PvdE	Feedback from November ITC KG meeting; diagrams from the presentation included.
Rev_0	2016-12-13	ITC KG	For Approval by INT WG
Rev_1	2017-01-09	ITC KG	For Approval by INT WG

194