AS4 Usage Profile Questions and Answers

Versions of the Usage Profile:

> **What versions of the Usage Profile are there?**
- At any point in time there is a single current approved version of the Usage Profile, published at the ENTSOG Web site: http://www.entsog.eu/publications/as4#AS4-USAGE-PROFILE.
- In addition to the current approved Usage Profile, ENTSOG may publish unapproved draft future versions of the usage profile. These drafts may fix errors or omissions in the profile, changes based on implementation experience, or functional enhancements.

> **Which version of the Usage Profile should I use?**
- There is only one approved version and in principle that version is the version to implement.
- However, the draft version may correct errors or omissions in the current approved version, and may include solutions to issues you may encounter in your AS4 implementation. Do keep in mind that there is no 100% guarantee that the draft version is not changed before publication.

> **What should I do if ENTSOG publishes a draft version?**
- It is recommended that you review drafts for any changes that may affect you, positively or negatively, as these changes are likely to be mandatory in a future approved version. If you have any feedback to any of the changes under consideration, please contact ENTSOG as soon as possible.
- If you have (an) issue(s) with the current approved profile, you may check the unapproved draft. Your issue may be a known issue for which the draft already provides a fix.

AS4 Header:

> **Is support required for message properties?**
- Yes, as stated in section 2.2.3.1 of the Usage Profile and according to AS4, any ebHandler compliant product supports this requirement.
- Having said this, the current version of the Usage Profile does not define any message properties. (It does define a part property, *EDIGASDocumentType*).

Agreements:

> **What information is included in an agreement?**
  - An agreement denotes a set of Pmodes. In the Usage Profile, all Pmodes in an agreement have the same signing and encryption certificates.

> **What naming convention applies to agreement identifiers?**
  - None is defined in the current usage profile.
  - A draft update of the usage profile provides a convention for the value of *AgreementRef* that combines the party identifiers and a version number.

> **How many agreements exist between two partners?**
  - At least one and two overlapping agreements during renewal period.

> **What happens upon certificate renewal?**
  - A new agreement is created that is identical to the old one, except for the certificates used.

> **Are there constraints on combinations of Party Identifiers, Agreements and Certificates?**
  - Agreement identifiers are unique per pair of parties.
  - Per agreement there is one pair of signing/encryption certificates per partner. So for each message from P1 to P2, the agreement determines the certificate of P1 that P1 uses to sign the message, the certificate of P2 that P1 encrypts the message with, and the certificate of P2 that P2 will use to sign the AS4 receipt for the message.

> **Which certificate is used in case of impersonation?**
  - The one configured for the agreement and associated Pmodes.

Agreement Update:

> Is support for Agreement Update required?
  - Not yet, but it is likely to be required in a future version of the profile.

> What is the impact of AU on the AS4 component?
  - No direct impact, it can be handled outside the AS4 component.
  - AU can be handled automatically or manually.

AS4 Error Handling:

> Which Error codes are to be used in the Entsog Usage Profile?
  - The regular ebMS3 / AS4 error codes are used. No additional codes are defined in the Usage Profile.

> Do AS4 errors have to be signed?
  - They should be, but they can't always be.

Duplicate Elimination:

> **Why is it needed?**
  - To handle the "lost receipt" situation, prevent messages from being delivered more than once.

> **What is the detection window?**
  - At least as long as the retry interval.
  - In ENTSOG, a maximum of an hour suffices, after which the message is in error.

Encryption:

> **Why is there a reference to symmetric keys for key transport?**
  - The partner's encryption certificate is used to encrypt a symmetric key that is used to encrypt the data.

> **Is there a recommendation for key transport algorithms?**
  - Yes, but they are recommended, not mandatory.

> **Are the algorithms from the AS4 Usage Profile supported in all products?**
  - No, some products on the market do not implement all mandatory algorithms.
  - Therefore, in your agreements with suppliers, make sure that the supplier does not just provide an AS4 solution, but a solution that conforms to the ENTSOG AS4 solution.

> **What is the MIME type of an encrypted compressed payload?**
  - Application/octet-stream.

> **Are receipts and errors encrypted?**
  - No, it is superfluous and may cause interop issues

> **Is the empty SOAP Body to be encrypted?**
  - No, but it is to be signed.

Networking:

> **Is support for IPv6 required?**
  - A product must be able to serve as a dual-stack networking client, i.e. to connect to a counterparty AS4 gateway that is only accessible on IPv6, only on IPv4, or on IPv4 and IPv6.
  - Parties can deploy their AS4 gateway as IPv4 and/or IPv6 servers.
  - If all of your current counterparties use IPv4, you may postpone implementing IPv6 until your first new IPv6 only partner.

Payload Processing:

> **Is a Gateway required to do schema validation?**
  - No, the gateway may just pass on the content to a business application that does the validation.
  - To be able to validate the schema, message metadata including sender and receiver party ID and EDIGASDocumentType must be passed on along with the payload.

> **What does the PayloadInfo element look like?**
  - It contains an *href* to a MIME attachment.
  - It has two properties related to AS4 compression and one to encode the EDIGAS document type.
  - The following is an example for a DELORD.

```
<eb3:PayloadInfo
  xmlns:eb3="http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/">
  <eb3:PartInfo>          href="cid:a1d7fdf5-d67e-403a-ad92-3b9deff25d43@tso.eu"
      <eb3:PartProperties>
    <eb3:Property       name="CompressionType">application/gzip</eb3:Property>
    <eb3:Property            name="MimeType">application/xml</eb3:Property>
    <eb3:Property          name="EDIGASDocumentType">ANC</eb3:Property>
   </eb3:PartProperties>
  </eb3:PartInfo>
</eb3:PayloadInfo>
```

Token References:

> **Which token reference mechanism in WS-Security is to be used?**

- There are three options and Usage Profile currently allows all of them.
- BinarySecurityToken is the most interoperable option; future versions may mandate support for this by all products.

Transport Layer Security:

> **Does the profile require support for client authentication?**

- Some organisations require client authentication for inbound communication and therefore the product should support this feature. In other situations it is not recommended as the profile supports authentication based on X.509 message signing.
- No support is required for the AS4 alternative pull authorisation feature.

> **Which cipher suites are to be used?**

- The ENTSOG profile (section 2.2.6) refers to the 2013 ENISA report, section 5.1.2 of which specifies a number of cipher suites.
- Section 2.2.6 of the ENTSOG profiles states that "Products MUST support cipher suites included in this subset."
- This results in the following list:

  *_WITH_Camellia_128_GCM_SHA256
  *_WITH_AES_128_GCM_SHA256
  *_WITH_Camellia_256_GCM_SHA384
  *_WITH_AES_256_GCM_SHA384
  *_WITH_AES_128_CCM
  *_WITH_AES_128_CCM_8
  *_WITH_AES_256_CCM
  *_WITH_AES_256_CCM_8

  Where * denotes the underlying key exchange primitive.
- TSOs using TLS software limited to AES-CBC-based encryption MUST add support to the safer AES-GCM algorithm as soon as possible.

AS4 Deployment Issues and Future Profile Updates:

> **For Sender and Receiver, is a *type* attribute used on PartyId?**

- The current version of the ENTSOG AS4 usage profile is explicit in requiring the *type* attribute to be absent.
- However, due to recently encountered interoperability issues, the published draft update to the Usage Profile mandates the presence of the type attribute, with a fixed value http://www.entsoe.eu/eic-codes/eic-party-codes-x.
- Parties that encounter this interoperability issue with certain communication partners are recommended to implement this change now in anticipation of an upcoming update of the profile.
- For communication with partners for whom this issue does not arise, you may configure your communication as currently specified in the profile, or change to comply with the anticipated future profile.

> **Which algorithm is to be used for XML Encryption?**

- The algorithm to be used according to the Usage Profile is *http://www.w3.org/2009/xmlenc11#aes128-gcm*.
- This value was re-confirmed by ENISA and therefore no change is currently foreseen for this.
- Parties using (or wanting to use) products not supporting this algorithm are recommended to encourage the vendor to adapt its product to be compliant with the profile.
- Parties needing to communicate with a partner using a product not supporting this algorithm are recommended to encourage that partner to adopt a compliant solution.
- In situations in which a (or both) communication partner(s) is not currently able to deploy an AS4 solution compliant with the ENTSOG AS4 profile, parties may be able to use http://www.w3.org/2001/04/xmlenc#aes128-cbc, which is AES with CBC instead of GCM. This is not recommended for future use, but allows parties to start using AS4 without delay.

> **Is the value of AgreementRef value tied to a direction of message flows?**
  - In ebXML an agreement is between two parties in a particular interval, not to a particular direction message flows. Therefore the current version of the ENTSOG AS4 is incorrectly worded. This is fixed in the published draft update of the usage profile.

> **Is a *type* attribute used on Service?**
  - The current version of the ENTSOG AS4 usage profile is explicit in requiring the *type* attribute to be absent. Section 2.3.1.2.1 explains that this is consistent with an interpretation of the EDIGAS codes as relative URIs.
  - However, due to recently encountered interoperability issues with products that require the value to be an absolute (and not a relative) URI in the absence of a type attribute, the draft update the Usage Profile mandates the presence of the type attribute, with a fixed value http://edigas.org/service.
  - Parties that encounter this interoperability issue with certain communication partners are recommended to implement this change now in anticipation of an upcoming update of the profile.
  - For communication with partners for whom this issue does not arise, you may configure your communication as currently specified in the profile, or change to comply with the anticipated future profile.
  - While the proposed URI currently references the EDIGAS site, in AS4 messages it is an identifier only that is not retrieved during AS4 messaging.