ITC-KG AS4
Proof of Concept
16 January 2014
Draft
INT0487-140108

Proof of concept AS4

Version 1 Revision 02 – 2014-01-08

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 and subject to the completion of the applicable process foreseen for the approval of the EU Regulation embedding the Network Code on Interoperability and Data Exchange.

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:

The network code Interoperability and Data Exchange specifies that for document based data exchanges the AS4 communication standard based on ebMS is to be used as a common protocol. The technical configuration parameters are defined by the ITC kernel group of ENTSOG together with a communication expert.

2. Purpose of "Proof of concept":

In order to validate the defined parameters and to detect in an early phase any potential issue related to the implementation of the communication system based on the defined usage profiles and security rules, a proof of concept (PoC) is set-up between a limited group of TSOs that use different software solutions. During the proof of concept the participating TSOs shall configure the communication interface according to the rules and settings defined for AS4 communications.

The proof of concept will allow ENTSOG to validate and fine tune the configuration parameters on one hand and to test on the other hand the interoperability of different AS4 products on the market. The experience acquired during the PoC will be used to update the configuration rules and will be integrated in a supporting document that will be published by ENTSOG. It will deliver guidance to all market participants for the implementation of an AS4 communication system for the European gas market.

3. Vendor involvement:

Vendors can be involved during the PoC through the products delivered or in use by the participating parties. Their input and technical support is mandatory during the PoC to validate the usage profiles and if necessary to adapt the product to make it compatible to the standard and with products of other vendors.

4. Participating parties for PoC:

TSOs (Entsog members) and volunteering counterparties (capacity booking platforms) are invited to participate for the AS4 prototyping phase in Q1/2014. They shall make the necessary resources available and liaise with their solution provider directly for all technical and commercial arrangements. Counterparties shall be selected based on a criteria list defined by ENTSOG. The number of parties involved in the PoC tests is preferably between minimum 4 and maximum 6, preferably using different software products.

Criteria for participants:

- Experience in data exchange and intent to proof an AS4 solution
- Meet the expected time frame for the PoC
- Participants will provide as soon as possible, X.509 certificates (a TLS server certificate, a WS-Security signing certificate and a WS-Security encryption certificate) for use in the tests. These certificates must not be self-signed certificates but must be test certificates issued by a Certificate Authority. Test certificates issued by EASEE-gasmay be used by participants.

- Once participants have deployed their test systems, they shall communicate endpoint configuration information (server URL, server IP address, client IP address or addresses) to ENTSOG. Test systems shall be deployed in debug mode, so that as much logging information as possible is generated.
- Make the necessary resources available and bear own cost for PoC. Configuring and performing the tests will require participation from both application management and network infrastructure management units within the participant's organization and possibly from the supplier of AS4 software and/or third party service providers.
- Contribute to the summary report for AS4 set up.

5. Deliverables:

The outcome of the PoC is to validate the AS4 Usage Profile and to make a list of FAQ, based on the experiences acquired during the interoperability tests. The results will be part of the supporting documents for the AS4 configuration and implementation.

During the PoC period, a communication system shall be configured and test files will be exchanged between the participating parties. Timing and impact of file sizes will be evaluated as well as security related settings.

ENTSOG will provide AS4 processing mode configurations for all participants for all tests. These configurations include test EIC codes for the participants (different from the production EIC codes) and values for other parameters, such as values that control the Service and Action AS4 message headers, and certificate and endpoint information as provided by participants.

ENTSOG can provide sample payloads to be used in testing, both of expected average and expected maximum size. These payloads will be valid formatted and realistic EDIG@S-XML messages, but will not include any production data.

During the PoC a number of test scenarios will be performed. Some general remarks on the tests:

- All tests will involve "Push" exchanges only. "Pull" exchanges will not be considered.
- Tests 5.1 and 5.2 involve communication using HTTPS. All other tests will be performed using HTTP (i.e. not transport layer security, only message layer security), in order to be able to be able to more easily capture on-the-wire message exchanges.
- All tests will use certificates meeting the requirements mentioned above in section 4.

5.1. TLS test, positive scenario

- Precondition: the AS4 handler and an HTTPS client test programme are configured to support the TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 cipher suite.
- The HTTPS client attempt to connect to the AS4 hander using this cipher suite.

- Expected result: a secure connection is established.

5.2. TLS test, fault scenario

- Precondition: the AS4 handler is configured to support TLS version 1.2 and the TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 cipher suite. An HTTPS client test programme is configured to support SSL 3.0 (or an even older version).
- The TLS client attempts to connect to the AS4 hander using SSL 3.0.
- Expected result: no connection is established as SSL 3.0 is not a supported version of transport layer security for the ENTSOG AS4 profile.

5.3. AS4 reliable messaging, basic functionality:

- Precondition: Sending and Receiving MSH are configured to exchange a particular message type using reliable messaging.
- Sending MSH sends a signed AS4 message of this type.
- Expected result: Receiving MSH returns a synchronous AS4 non-repudiation receipt. The content of the NonRepudiationInformation element in the returned receipt MUST match the Signature of the received message. (This can be determined using message logs, message trackers and/or TCP monitoring tools; the latter requires the test to not use TLS).

5.4. AS4 reliable messaging, fault scenario:

- Precondition: Sending and Receiving MSH are configured to exchange a particular message type using reliable messaging. Network connectivity between Sender and Receiver is blocked.
- Sending MSH attempts to send a signed AS4 message of this type (this fails).
- Expected result: the Sending MSH (which will enter retry mode) notifies the Producer that an error occurred after message retries are exhausted.

5.5. AS4 reliable messaging, retry feature:

- Precondition: Sending and Receiving MSH are configured to exchange a particular message type using reliable messaging. Network connectivity between Sender and Receiver is blocked.
- Sending MSH attempts to send a signed AS4 message of this type (this fails).
- Network connectivity is restored before the last scheduled Retry.
- Expected result: the Sending MSH successfully sends the message at the next Retry and receives an AS4 receipt. Retry mode ends now.

5.6. Compression test:

- Precondition: Sending and Receiving MSH are configured to exchange a particular message type using payload compression. The payload used is a 10MB EDIGAS XML payload. To be able to inspect the wire format of the message, no WS-Security is specified. A GZIP'ed data file from the XML for comparison using a GZIP tool for comparison. It is expected to be significantly smaller, likely less than 1MB.

- Sending MSH sends an AS4 message of this type.
- Expected result: receiving MSH delivers the uncompressed payload to the Consumer. On the wire, the content of the attached payload should match the GZIP'ed data file. Verify the size reduction (HTTP Content-Length).

5.7. Signing test, positive:

- Precondition: Sending and Receiving MSH are configured to exchange a particular message type using message signing using a certificate. The payload used is an EDIGAS XML payload.
- Sending MSH sends an AS4 message of this type.
- Expected result: receiving MSH delivers the payload to the Consumer and returns an AS4 receipt. On the wire, a WS-Security header with an XML Signature covering payload, headers and body is present.

5.8. Signing test, negative:

- Precondition: as in the positive case, except that the receiving MSH is configured for a different certificate than the sending MSH.
- Sending MSH sends an AS4 message of this type.
- Expected result: receiving MSH rejects the message.

5.9. Encryption test, positive:

- Precondition: Sending and Receiving MSH are configured to exchange a particular message type using message encryption using a particular certificate. The payload used is an EDIGAS XML payload.
- Sending MSH sends an AS4 message of this type.
- Expected result: receiving MSH delivers the payload in uncompressed form. On the wire, the message will show the MIME part containing the payload with binary data.

5.10. Encryption test, negative:

- Precondition: Sending and Receiving MSH are configured to exchange a particular message type using encryption but there is a configuration mismatch for the certificate. The payload used is an EDIGAS XML payload.
- Sending MSH sends an AS4 message of this type.
- Expected result: receiving MSH rejects the message.

5.11. Combined scenario: this is a combination of compression, signing and encryption as specified in the AS4 profile.

6. Planning:

The current planning is to make the PoC in the period between February and April 2014.

The results of the IOP testing will be published on the workshop organised by ENTSOG for all interested stakeholders (planned for May 2014).