ENTSOG AS4 Proof-of-Concept

Final Report

Final version – 2014-08-01

Disclaimer

This document relates to the draft ENTSOG AS4 usage profile that contains specific technical information that is given for indicative purposes only and, as such, is subject to further modifications. The information contained in this document, like the information in the draft ENTSOG AS4 usage profile, is non-exhaustive and non-contractual in nature and subject to the completion -and subsequent outcomes- of the applicable process foreseen for the approval of the EU Regulation embedding the Network Code on Interoperability and Data Exchange.

This report was finalized on its publication date and describes the testing of Proof-of-Concept scenarios. The information contained in this document represents a snapshot of the capabilities of the presented AS4 software implementations and their deployments at the organizations participating in the Proof-of-Concept at this specific date. These results may not relate to capabilities of past or future deployments of these AS4 software implementations and/or deployments of these implementations, or of past or future versions of these implementations and/or deployments.

The information provided in this document is provided AS-IS and does not represent any endorsement by ENTSOG and/or any of its participating partners of the mentioned software implementations and/or their vendors.

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 is a European organization set up to promote the completion and functioning of the internal market and cross-border trade for gas and to ensure the optimal management, coordinated operation and sound technical evolution of the European natural gas transmission network. Its legal basis is the EU Gas Regulation 715/2009 [EC715-2009]. The lack of harmonisation in technical, operational and communication areas might create barriers to the free flow of gas in the European Union, thus hampering market integration. European interoperability and data exchange rules allow the necessary harmonisation in those areas, therefore leading to effective market integration.

1.1 Network Code on Interoperability and Data Exchange Rules

As part of ENTSOG's work in the area of interoperability, it developed a Network Code on Interoperability and Data Exchange Rules [DNCIDX], which was submitted to the European Commission in January 2014. This network code states that "*AS4 shall be used as common data exchange protocol for document based data exchanges*". AS4 is a modern open standard for B2B data exchange [AS4]. It is a profile of ebMS3 [EBMS3], a more general open standard, based on Web Services technology. The selection of AS4 was based on a comparison of multiple transport communications.

1.2 ENTSOG AS4 Profile

To use a communication protocol, in practice simply referencing a particular standard (whether AS4 or some other standard) is not sufficient. Communication protocols can often be implemented in many different ways, as they are aimed to support a wide range of applications and have optional features and variants. As a result, different implementations may not be interoperable. Past experience in the gas sector with older protocols like AS2 and in other sectors shows that additional implementation guidelines are needed to enable consistent and interoperable implementations of transport protocols. When applied to AS4, such guidelines can provide suppliers of AS4-enabled B2B communication solutions with essential guidance regarding the required AS4 functionality. Implementation guidelines also standardize aspects that relate to how the standard is used in a particular community, rather than to features of the standard itself.

ENTSOG therefore set up a team to define a usage profile for AS4. This work was done in the months following the formal submission of the Network Code on Interoperability and Data Exchange Rules. A draft version of the Usage Profile was published in January 2014, and presented on February 2014 in Brussel at a workshop on Interoperability Network Code Data Exchange requirements. Some key features of this profile are:

- The profile is based on AS4 [AS4], a state-of-the-art protocol that simplifies and standardizes the use of Web Services for B2B data exchange and avoids many known complexities and interoperability issues in these technologies.

- While the AS4 **pull** feature may be useful in the future, it is considered that the immediate requirements of the gas sector can be achieved using **push** exchanges. This simplifies the initial envisaged use of AS4 in the gas sector.
- The profile leverages experience gained in the past with other B2B protocols in the gas sector, such as AS2 as described in the EASEE-gas implementation guide [EGMTP]. Accordingly, the AS4 profile uses message layer signing, encryption and compression. In addition to message layer security, the AS4 profile specifies and profiles use of transport layer security.
- The profile follows state-of-the-art best practice in security, following recommendations for "near term" (defined as "at least ten years") future system use by the European Union Agency for Network and Information Security (ENISA) agency [ENISAAKSP].
- The profile uses AS4 reliable messaging, and applies retransmission and duplicate elimination to provide once-and-only-once reliable messaging. This increases the overall robustness of document exchange.

The ENTSOG AS4 profile differs from some other AS4 profiles deployed in other business sectors and geographies, such as the profiles developed for the Australian Superannuation initiative [SUPERAS4]. The ENTSOG profile requires encryption and is more specific in the use of security algorithms. Unlike the SuperAnnuation profiles, it does not currently use the AS4 pull feature.

At the workshop in February 2014, the usage profile was presented to stakeholders. The discussions did not result in changes to the profile. The usage profile was then submitted to the ENISA agency, which kindly accepted a request to review the document and provided their feedback in June 2014.

2 Proof-of-concept

In order to validate the defined parameters and to detect in an early phase any potential issues related to the implementation of the communication system based on the defined usage profiles and security rules, ENTSOG proposed a proof-of-concept (PoC) between a limited group of organizations that use different software solutions. This proposal was also presented at the February 2014 workshop [AS4PoC]. The document explains that during the proof-of-concept a number of participating parties will configure the communication interface according to the rules and settings defined for AS4 communications. The proof-of-concept, as described in that document, has been carried out as planned and was completed by the end of July 2014. This document is the final report of that proof-of-concept.

2.1 Objectives and Scope

The goal of the proof-of-concept was to allow ENTSOG and its members to validate and fine tune the configuration parameters on one hand and to test on the other hand the functionality of different AS4 products on the market and their interoperability. The goal was to use the experience acquired during the PoC to consolidate the usage profile. The

validated and improved implementation guidelines will deliver guidance to all market participants for the implementation of an AS4 communication system for the European gas market.

The proof-of-concept was not a formal conformance or interoperability test. In the tests, the defined scenarios were tested but products have not been tested exhaustively and only key features were validated. To cover all interoperability aspects, participating vendors could (and are encouraged to) engage in independent interoperability testing programmes where more issues, including corner cases, can be covered. The PoC also did not address functional or non-functional features that are not related to the AS4 protocol, and that may be important differentiators for specific messaging product implementations and their practical deployment.

The AS4 solutions tested in the proof-of-concept involved both commercial solutions (in all cases released launched fairly recently) as well as prototypes that, at the time of writing, were not yet commercially available, were still under active development and/or had not yet been subjected to interoperability testing with other AS4 products.

Furthermore, the signing, encryption and compression features in the ENTSOG profile are fairly high-end and are known to have caused configuration or interoperability issues with other protocols and other uses of WS-Security in the past. Therefore issues with these features were considered likely. As a result of all these factors, the proof-of-concept was not expecting all scenarios to be processed successfully for all combinations of partners for all products.

2.2 Participants

ENTSOG invited its member Transmission System Operators (TSOs) and their counterparties to participate in the proof-of-concept. The invitation was specifically addressed to TSOs rather than to software vendors or other solution providers. In the proof-of-concept, five TSOs and two other organizations participated on a voluntary basis. In alphabetical order, these are:

ENAGAS (Madrid, Spain, http://enagas.es/portal/site/enagas) is the Spanish Transmission System Operator and the main carrier of natural gas in Spain. Its main mission is to ensure competition and security of the Gas System in Spain. It has nearly 10,000 km of pipelines throughout the Spanish territory. The company participated using AS4 software provided by Tibco.

ENI (Milan, Italy, http://www.eni.com/en_IT/home.html) is a major international integrated energy company. ENI operates in the oil and gas, electricity generation and sale, petrochemicals, oilfield services construction and engineering industries. In the proof-of-concept, the company participated using AS4 software also provided by Tibco.

Gassco (Karmøy, Norway, http://www.gassco.no/en/) is Transmission System Operator in Norway. Gassco is responsible for the safe and efficient gas transport from the Norwegian continental shelf and intends to be a leading gas transporter in Europe. In the proof-of-concept, the company participated using AS4 software provided by Axway. Gassco joined the

proof-of-concept at the end of the project only. Therefore, it only participated in a limited number of tests.

Gas Connect Austria (GCA, Vienna, Austria, http://www.gasconnect.at/en) is Transmission System Operator in Austria. The company is Europe's gas transportation partner in Austria. With a 2,000 km high-pressure pipeline network, Gas Connect Austria operates an infrastructure that acts as a central hub in the European natural gas grid. In the proof-of-concept, the company participated using AS4 software provided by ADES.

Gaz-System (Warsaw, Poland, http://en.gaz-system.pl/) is a Transmission System Operator in Poland. Gaz-System's key task is the transport of gas via the transmission network throughout Poland to supply with gas the distribution networks and final customers connected to the transmission system. In the proof-of-concept, the company participated using AS4 software provided by Software AG.

SNAM Rete Gas (Milan, Italy, http://www.snamretegas.it/en/index.html) is a Transmission System Operator in in Italy. The company is active in Italy in the transport and dispatching of natural gas. For many years it has been planning, building and managing a network which today reaches round 32,306 km and extends across most of Italy. In the proof-of-concept, the company participated using AS4 software provided by Tibco.

Westnetz (Dortmund, Germany, www.westnetz.de/) is active in the western part of Germany and operates a gas network of 26,000 km. It also provides data communication services to Thyssengas (Dortmund, Germany, http://www.thyssengas.com/), an independent Transmission System Operator operating a gas network of 4,200 km. In the proof-of-concept, Westnetz participated using AS4 software provided by Seeburger.

The companies participated on a voluntary basis and funded their participation in the project themselves.

Four other TSO participants participated in the early stages of the proof-of-concept. Two of them withdrew because their solution provider could not provide an AS4 solution in the expected timeframe. Two other companies had access to AS4 solutions (from their solution providers) but had to withdraw due to internal resource issues and priorities within their companies.

ENTSOG performed project management for the proof-of-concept. The project was supported by Sonnenglanz Consulting, an external consulting company with expertise in AS4.

Rather than developing in-house AS4 solutions, all seven participants in the proof-of-concept partnered with third party solution providers to deploy AS4. The selection of these solution providers was done by the participating parties and in all cases reflected an established business relation. ENTSOG had no involvement in the selection of solution providers and their participation in the proof-of-concept does not represent any endorsement by ENTSOG of the particular solution provider or its product. The participating solution providers are, in alphabetical order:

ADES (Vienna, Austria, http://www.ades.at/) is a provider of IT software and services. In the proof-of-concept, ADES provided an AS4 solution to Gas Connect Austria.

Axway (Phoenix, AZ, USA and Paris, France, http://www.axway.com/) is a global software and service company with a track record in B2B integration solutions. In the proof-of-concept, Axway supplied software to Gassco, Norway. This was a patched version of a product that includes AS4 functionality under development for a future release of this product.

Seeburger (Bretten, Germany, http://www.seeburger.com/home.html) is a software company providing solutions for business-to-business integration. In the proof-of-concept, Seeburger supplied AS4 software to its partner Westnetz for its customer Thyssengas (both Germany).

Software AG (Darmstadt, Germany, www.softwareag.com/) is an international software company. In the proof-of-concept, Software AG provided AS4 software to Gaz-System, Poland.

Tibco Software Inc. (Palo Alto, CA, USA, www.tibco.com/) is a company providing infrastructure and business intelligence software. In the proof-of-concept, Tibco provided AS4 software to ENAGAS (Spain), ENI and SNAM Rete Gas (both Italy).

2.3 Scenarios

The scenarios that were tested in the proof-of-concept are documented in the proof-of-concept documentation [AS4PoC]. For convenience, these scenarios are summarized in Table 1 AS4 Proof-of-Concept Scenarios.

Scenario	Description
1	TLS Test, Positive Scenario
2	TLS Test, Negative Scenario
3	Minimal AS4 Message Exchange
4	AS4 reliable messaging, basic functionality
5	AS4 reliable messaging, fault scenario
6	AS4 reliable messaging, retry scenario
7	AS4 compression feature
8	Signing test, positive
9	Signing test, negative
10	Encryption test, positive
11	Encryption test, negative
12	Signing and Compression

13	Signing, Encryption and Compression

Table 1 AS4 Proof-of-Concept Scenarios

The scenarios can be summarized and grouped as follows:

- Scenarios 1-3 are concerned with transport layer security. These only concern the secure connection and not AS4, so they can be tested using TLS test tools.
- Scenarios 4-6 address reliable messaging. This concerned the retry, duplicate elimination and error reporting features of AS4.
- Scenarios 7-13 address signing, encryption and compression. Scenario 13 is the scenario that complies with the AS4 usage profile. However, as this profile combines many features, each of which could fail independently, and to test failure cases, the additional scenarios 7-12 were added, which progressively add features and complexity.

A supplementary document was created to define values for mandatory AS4 header fields like *From/PartyID*, *To/PartyID, Service* and *Action.* Furthermore, ENTSOG centrally maintained and distributed an electronic "*address book*" containing information on communication endpoints, such as server URL and IP numbers, and administrative information like contact information. Each participant used this information to configure the various scenarios and associated "*processing mode parameters*" in their AS4 communication software, using the native configuration facilities of their products.

The project team met via Web conference every one or two weeks, in which results of the preceding period were reviewed and the tests for the following period were planned. Not all pairs of participants performed all tests. The pairs that were formed, were formed for various reasons, such as organizational and technical readiness, business relevance, or to test more combinations of different products.

3 Proof-of-Concept Results

In this section we will summarize the results of the various tests among participants in the proof-of-concept.

3.1 ENAGAS, SNAM and ENI

As ENAGAS, ENI and SNAM were all using software from Tibco, no interoperability issues were expected among the three partners and none occurred. However, some issues were found in the Tibco implementation of AS4 and in its support for TLS, as required for the ENTSOG profile.

- In AS4, it is possible to qualify the *PartyId* element with an optional *type* attribute. In the ENTSOG profile, only one party type is used, the IEC code type. This *type* attribute is used in other AS4 usage profiles, but not in the ENTSOG profile. However, the Tibco product currently requires this attribute. As a temporary workaround, a dummy value was provided to this attribute in order to be able to complete the tests.

- The ENTSOG AS4 usage profile mandates the use of version 1.2 of TLS [RFC5246]. The Tibco AS4 product does not currently support TLS 1.2. Instead, ENAGAS and SNAM offloaded TLS at a network component, which is an option the usage profile explicitly supports.
- The ENTSOG AS4 profile states that products must reject connections using the unsecure SSL 3.0 and TLS 1.0 protocols. Tibco does not currently support restricting inbound secure connections to specific protocol versions.

Support issues have been raised with Tibco for all three cases. With the workarounds applied, all positive and negative scenarios were completed successfully.

3.2 ENAGAS and Westnetz/Thyssengas

These exchanges involved independent AS4 implementations, from Tibco and Seeburger. All tests were completed successfully, except for scenario 13, in which case an issue was found relating to the order of signing, encryption and compression. Seeburger fixed this functionality, but due to lack of resources on the side of ENAGAS it could not be re-tested during the proof-of-concept. However, the same issue occurred in the tests of Westnetz and GCA (see section 3.5, below) and was successfully resolved.

3.3 Gassco and ENI

Gassco joined the proof-of-concept close to its end and had only a short period to do tests. It therefore only tested the positive scenarios with ENI. These exchanges involved independent AS4 implementations, from Axway and Tibco. Most of the tested scenarios were completed successfully, including the ones involving signing and compression. An issue in the Axway implementation was found with the scenarios involving encryption (10 and 13). A temporary workaround was suggested by Axway and the company states that a permanent fix has already been developed by its engineering team. Unfortunately none of these could be tested due to the end of the proof-of-concept. The functionality will be provided in Axway's upcoming supported AS4 products.

3.4 Gaz-System and Westnetz/Thyssengas

These exchanges involved independent AS4 implementations, from Software AG and Seeburger. The scenarios 2 up to and including 12 were successfully completed. Scenario 1 could not be tested due to configuration issues.

In scenario 3, while the message was successfully transmitted, there was a different interpretation of HTTP response codes. The Software AG product expects code 200, whereas the Seeburger software provides the value 204. A request for clarification was issued to the OASIS Technical Committee responsible for maintaining AS4 and ebMS3. Basically, any response in the 2** range indicates successful transmission.

In scenario 8, the Software AG product expected a WS-Security Timestamp, as it is used for duplicate elimination. Seeburger solved the issue by adding the timestamp. However, AS4

and the ENTSOG profiles do not mandate this element. The issue has been reported to Software AG.

In scenario 10, Software AG product incorrectly expects receipts for encrypted messages to be encrypted. The vendor is aware of this issue and will fix it.

In configuring scenario 13, Gaz-System found that there are technical problems with using separate certificates for signing and encryption. They have reported this to Software AG. The issue is being worked on but could not be fixed in the course of the proof-of-concept.

3.5 GCA and Westnetz/Thyssengas

These exchanges involved independent AS4 implementations, from ADES and Seeburger. In their testing, the teams experienced some issues with encryption, one of which related to the order of the security headers, already mentioned in section 3.2 above. Others involved problems that were more specific to the encryption mechanisms. Some of them were caused by the Seeburger software, others were caused by the ADES implementation.

One issue concerned the use of Diffie-Hellman primes during the setup of the HTTPS connection between the systems. Whereas the Seeburger system is implemented in Java, the ADES system is not. Due to a bug in the Java core (http://bugs.java.com/bugdatabase/view_bug.do?bug_id=6521495), only primes with a length between 512 and 1024 bit which are a multiple of 64 can be used. The teams found that, for example, newer versions of Apache will set the length according to the certificate key length (which however has no direct connection to the length of the Diffie-Hellman modulus (which are those primes) in the protocol itself), which would lead to 2048 bit long ciphers in the case of the ENTSOG usage profile, rendering the connection unable to be established with Java based systems. This behavior of Apache can be disabled, in which case messages can be exchanged successfully.

Another issue concerned the use of the *http://www.w3.org/2009/xmlenc11#aes128-gcm* encryption algorithm, which the usage profile recommends, in accordance with the W3C 1.1 XML Encryption version 1.1 recommendation [XMLENC1]. This algorithm is supported in the WSS4J security library, which is used (directly or indirectly, via other frameworks) by the Seeburger product and many other products, but some interoperability issues were found during tests. The WSS4J library also does not support the *http://www.w3.org/2009/xmlenc11#rsa-oaep* algorithm, which can be combined with a SHA2-based mask generation function. It does support the *http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p* algorithm. This is an option that is allowed in the usage profile.

The teams spent an extended time analyzing, solving and testing these issues in their products. The end result is that GCA and Westnetz successfully completed all tests in both directions.

3.6 GCA and SNAM

GCA and SNAM started testing near the end of the proof-of-concept project, with GCA using AS4 software from ADES and SNAM using AS4 software from Tibco. All tests were completed successfully, except for scenarios 11 and 13 which involve encryption. Analysis of these scenarios was still ongoing at the end of the proof-of-concept.

4 Summary and Conclusion

As is common in this type of tests, some time was needed in most organizations for basic operations such as obtaining a test system, obtain resources to deploy software, configuring firewall rules, configuring partners. This is independent of any technology and protocols like AS4. Some additional time was needed by each participant to configure their AS4 systems for specific test partners and for the various scenarios. Again, this would be the case for any communication protocol. Given that the various scenarios are all different in subtle but important ways, that the products were new to many and the AS4 protocol to all, and that AS4 (for good reasons) has more configuration options than some other protocols, it was a positive outcome that most participants were able to complete the full test scenario for a specific partner in a relatively short amount of time.

The AS4 interoperability tests involved products from five vendors, three of which have been tested with three other products and two of which have been tested with one other product. The tests have successfully confirmed interoperability for all scenarios involving AS4 reliable messaging, compression, signing and encryption.

While not technically part of AS4, the ENTSOG profile mandates TLS 1.2, support for which is not available in all products. This issue does not arise when using a separate component for TLS processing, as is explicitly allowed by the AS4 usage profile and as will be quite common in production environments of many TSOs. Therefore an acceptable alternative solution is available today.

The proof-of-concept has not uncovered any issues with the usage profile, but has found potential issues dependent on specific programming languages and/or frameworks. As noted in section 3.5 above, a core Java bug impacts the use of an underlying security algorithm used in TLS that can cause interoperability issues with non-Java products. Since this is a problem in Java itself, such problems could have a major impact as many B2B communication products are written in Java. Implementers should be aware of this issue. Furthermore, the current version of widely used WSS4J framework does not support the *http://www.w3.org/2009/xmlenc11#rsa-oaep* algorithm identifier, though it does support *http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p*, which combines this algorithm with a SHA1-based mask function.

All participants found the profile to be sufficiently clear and to provide them with sufficient guidance to configure their products. For AS4, the usage profile has highlighted the need to clarify expected HTTP response codes (see section 3.4). The OASIS TC has created an issue to clarify this (https://issues.oasis-open.org/browse/EBXMLMSG-57). There may also be a need

to clarify use of WS-Security timestamps (https://issues.oasis-open.org/browse/EBXMLMSG-58).

The ENISA review resulted in some comments. The profile had already taken into account the results of the ENISA review of security algorithms, key sizes and parameters. The ENISA review did not concern any of the profile sections in which these were used. The ENISA comments have been reviewed and have been incorporated, along with other minor editorial improvements and one correction, in an updated v0.9 draft of the Usage Profile, that will be delivered with this report.

Overall, the proof-of-concept clearly validates the decision to select AS4 as an advanced and capable solution for document-based exchange. ENTSOG thanks all participating parties in the proof-of-concept for their voluntary contribution to the successful completion of the test scenarios in the AS4 proof-of-concept and for making available all resources to make the tight deadlines of the project.

5 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/

[AS4PoC] ENTSOG Proof-of-concept AS4. INT0487-140108. http://www.entsog.eu/public/uploads/files/publications/INT%20Network%20Code/2014/INT0487-140108%20proofofconcept%20as4-v1.2%20clean.pdf

[AS4UP] ENTSOG. AS4 Usage Profile. Version 0.5, January 2014. http://www.entsog.eu/public/uploads/files/publications/INT%20Network%20Code/2014/INT0488%20140108%20AS4%20usage%20profile%20v0r5.pdf.

[CAM] Business Requirements Specification for the Capacity Allocation Mechanism (CAM) Network Code. Draft Version 0 Revision 05 – 2012-10-05.

[DNCIDX] ENTSOG Draft Network Code on Interoperability and Data Exchange Rules. http://www.entsog.eu/public/uploads/files/publications/INT%20Network%20Code/2013/ACERSubmission/INT0352-130910%20Network%20Code%20on%20Interoperability%20and%20Data%20Exchange%20Rules_Final.pdf

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

[EC715-2009] 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/LexUriServ/LexUriServ.do?uri=OJ:L:2009:211:0036:0054:EN:PDF

[EGMTP] Message Transmission Protocol. EASEE-gas Common Business Practice 2007-001/01. http://easee-gas.eu/docs/cbp/approved/CBP2007-001-01_MessageTransmissionProtocol.pdf

[EIC] ENTSOG. Energy Identification Coding Scheme (EIC) for natural gas transmission. Party Codes. http://www.entsog.eu/eic-codes/eic-party-codes-x

[ENISAAKSP] Algorithms, Key Sizes and Parameters Report 2013 recommendations version 1.0 – October 2013. ENISA. http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report

[NOM] Business Requirements Specification for the Nomination (NOM) Network Code. Draft Version 0 Revision 9 – 2013-06-04.

[RFC5246] T. Dierks et al. The Transport Layer Security (TLS) Protocol Version 1.2. IETF RFC 5246. August 2008. http://tools.ietf.org/html/rfc5246

[SUPERAS4] Australian Taxation Office. DATA AND PAYMENT STANDARDS – MESSAGE ORCHESTRATION AND PROFILES.

https://www.ato.gov.au/uploadedFiles/Content/SPR/downloads/spr00335171_Message_Orchestration.pdf

[XMLENC1] XML Encryption Syntax and Processing Version 1.1. W3C Recommendation 11 April 2013. http://www.w3.org/TR/xmlenc-core1/