ENTSOG Integrated Data Exchange Profile

Version 0 Revision 0 – 2017-03-28

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

1.1 Integrated Data Exchange

COMMISSION REGULATION (EU) 2015/703 of 30 April 2015 establishing a network code on interoperability and data exchange rules published on 30 April 2015 by the European Commission (EC) specifies that:

"The following common data exchange solutions shall be used [for] the integrated data exchange:

> *(i) protocol: HTTP/S-SOAP;*
>
> *(ii) data format: Edig@s-XML, or an equivalent data format ensuring identical degree of interoperability. Entsog shall publish such an equivalent data format."* [CR2015/703].

For interoperability and consistency, additional guidelines are required to specify how the identified protocol is to be used. This document is a technical specification that provides such additional guidelines.

This specification provides a technical profiling of the use of Web Services specifications for Integrated Data Exchange. It does not define, and is independent of, any specific services and is business content-agnostic.

1.2 Use Cases

A number of different use cases have been identified that can be supported by Integrated Data Exchange. As these use cases have different requirements, it is not possible to specify a single profile covering all use cases. For this reason, this technical specification is divided in multiple parts:

- Common profiling of Web Services specifications. This profiling applies to all uses of Web Services for Integrated Data Exchange. This is covered in section 2.
- Profiling specific to public information services not requiring any user registration or authentication. This is covered in section 3 ("*Profile A*").
- Profiling specific to public information services requiring users to register and authenticate. This is covered in section 4 ("*Profile B*").
- Profiling specific to services provided to specific users and involving the exchange of private information of those users. This is covered in section 5 ("*Profile C*").

1.3 Goals

The main goals of this profile are to:

- Support public, private, anonymous and authenticated access to services.
- Focus, for public information services, on ease-of-use and, for private information services, on advanced security.
- Support exchange of EDIG@S-XML or other XML payloads, for integrated, non-document-based exchanges.
- Increase interoperability and consistency and facilitate implementations by selecting and profiling Web Services standards.
- Provide security guidance based on state-of-the-art best practices, following recommendations for “near term” (defined as “at least ten years”) future system use [ENISA13, ENISA14]
- Support anonymous service consumers, as defined in [BP20] as:
  A CONSUMER or INSTANCE is deemed "non-addressable" when, for whatever reason, it is either unwilling or unable to provide a network endpoint that is capable of accepting connections. This means that the CONSUMER or INSTANCE cannot service incoming HTTP connections and can only transmit HTTP Request messages and receive HTTP Response messages.

"SHALL", "NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

2 Common Profiling

This section specifies profiling of Web Services common to all Integrated Data Exchange types.

2.1 Network Layer

Integrated Data Exchange MUST use the public Internet [EGCDN] for communication [CR2015/703]. Each organisation is individually responsible for implementing security measures to protect access to its IT infrastructure.

Web Services products compliant with this profile MUST support both IPv4 and IPv6 and MUST be able to connect using either IPv4 or IPv6. To support transition from IPv4 to IPv6, products SHOULD support the “happy eyeballs” requirements defined in [RFC6555].

It is RECOMMENDED that deployments of Integrated Data Exchange support both IPv4 and IPv6 for the exchange of data. This allows them to support both communication partners that are still restricted to using IPv4 and other communication partners that have already deployed IPv6.

Due to IPv4 address exhaustion and the increased roll-out of IPv6, some future deployments of Integrated Data Exchange MAY be IPv6 only. A future version of this profile will therefore REQUIRE support for IPv6.

2.2 Transport Layer

Integrated Data Exchange MUST use HTTP over TLS, providing confidentiality of all exchanges. The minimum version of HTTP to use is 1.1. HTTP/2 MAY be used.

The Web Application MUST support HTTP compression. Clients MUST support HTTP compression and MUST signal support for compression by setting the Accept-Encoding HTTP header.

Guidance on the use of Transport Layer Security is published in the ENISA Algorithms, Key Sizes and Parameters Reports [ENISA13, ENISA14] and in a Mindest-standard of the Federal Office for Information Security (BSI) in Germany [BSITLS]:

- TLS server authentication is REQUIRED and MUST use an x.509 certificate meeting the requirements stated in section 2.7.
- It MUST be possible to configure the accepted TLS version(s) in the Integrated Data Exchange server. The ENISA and BSI reports state that TLS 1.0 and TLS 1.1 SHOULD NOT be used in new applications. Older versions such as SSL 2.0 [RFC6176] and SSL 3.0 MUST NOT be used. Products compliant with this profile SHOULD therefore support TLS 1.2 [RFC5246].
- It MUST be possible to configure accepted TLS cipher suites in the Web Application. IANA publishes a list of TLS cipher suites [TLSSP], only a subset of which the ENISA Report considers future-proof (see [ENISA13], section 5.1.2). Products MUST support cipher suites included in this subset. Vendors MUST add support for newer, safer cipher suites, as and when such suites are published by IANA/IETF.
- Support for SSL 3.0 and for cipher suites that are not currently considered secure SHOULD be disabled by default.
- Perfect Forward Secrecy, which is REQUIRED in [BSITLS], is supported by the TLS_ECDHE_* and TLS_DHE_* cipher suites, which SHOULD be supported.
- Publicly known vulnerabilities and attacks against TLS MUST be prevented and publicly known recommended countermeasures MUST be applied. Organisations MUST follow web security developments and MUST continually upgrade security measures as new general vulnerabilities become known.

2.3 Messaging

2.3.1 Message Exchange Pattern

All integrated data exchanges follow the SOAP Request-Response pattern using the SOAP 1.2 HTTP Binding [S12A], where the request message is posted by the SOAP client to the Web Service server and the response or fault is returned synchronously on the HTTP back channel.

Asynchronous communication is not supported in this profile.

2.3.2 SOAP Version

All messages MUST be valid SOAP 1.2 messages as specified in [S12s].

2.3.3 Packaging

SOAP messages compliant with this specifications are simple SOAP 1.2 envelopes. This version of this profile is limited to simple SOAP envelopes.

Request, response and fault content MUST be in XML format and MUST be contained as the single child element of the **Body** of the SOAP 1.2 envelope.

Note: the use of MIME wrapping as specified in the SOAP-with-attachments or MTOM [SWA, S12MTOM] specifications is under consideration for a future version of this profile.

The SOAP **Header**, if present, MUST but be empty and therefore MUST NOT include any headers. This constraint also applies to Web Services Addressing [WSADDR], i.e. there MUST NOT be any WS-Addressing headers in the SOAP header.

For this specification, any business-level headers are considered part of the payload content and MUST therefore be included in the XML payload content element in the SOAP Body. The SOAP **Header** MUST NOT include any custom business header elements.

2.3.4 Reliable Messaging

The Web Services Reliable Messaging protocol [WSRM] MUST NOT be used.

2.3.5 Interoperability Options

The use of SOAP MUST conform to the section 3 of OASIS Basic Profile version 2.0 [BP20], with the exception of section 3.7, as that section is about WS-Addressing, which is not used in the profile.

2.4 Service Description

2.4.1 WSDL

Web Services SHOULD be described using Web Services Description Language (WSDL) version 1.1 [WSDL11]. Schema definitions for requests, responses or faults MUST be included in, or referenced from, WSDL documents for specific services.

As specified in the Network Code, payload content MUST be EDIG@S-XML, or an equivalent data format defined and published by ENTSOG, ensuring identical degree of interoperability.

The schema definitions for payload content are out of scope for this specification. EDIG@S--XML and other XML payload schemas define standardised business headers. For this specification, any such business headers are simply part of the SOAP message payload content and not processed differently from other content.

The XML schemas MUST provide the ability to transport binary data in BASE64 encoded form [RFC4648], if binary content is to be exchanged in the server.

A WSDL compliant with this specification MAY define separate WSDL ports for different services. This allows a service provider to optimise its services by directing messages targeting specific services to specific endpoints, without requiring any processing of the XML request content.

2.4.2 Interoperability Options

The use of WSDL MUST conform to section 4 of OASIS Basic Profile version 2.0 [BP20].

2.5 Service Discovery

Use of Universal Description, Discovery, and Integration (UDDI) [UDDI] for service discovery is NOT REQUIRED.

2.6 Security and Availability

Each organisation is individually responsible for implementing security measures to protect access to its IT infrastructure. Appropriate security measures are to be undertaken as required by Article 22 of [CR2015/703]. This includes measures for Disaster Recovery and Business Continuity. The measures deployed MUST adhere to each organisation’s policies and standards for security.

Organisations MUST comply with applicable national and European regulation including the General Data Protection Regulation and Directive [D2016/680, R2016/679] and the Directive on Security of Network and Information Systems [D2016/1148].

Security options and policies appropriate to specific classes of use cases are further discussed in section 3

2.7 Certificates and Certificate Profile

2.7.1 Certificates and Public Key Infrastructure

In this Usage Profile, X.509 certificates are used to secure both Transport Layer and SOAP Message communication. Requirements on certificates can be sub-divided into three groups:

- General requirements;
- Requirements for Transport Layer Security;
- Requirements for SOAP Message Security.

The following general requirements apply to all certificates:

- A three year validity period for end entity certificates is RECOMMENDED.
- Guidance on size for RSA public keys for future system use indicates a key size of 2048 bits [BSIALG] or even 3072 bits [ENISA13, is appropriate. Keys with size less than 2048 bits MUST NOT be used.
- The signature algorithm used to sign public keys MUST be based on at least the SHA-256 hashing algorithm.
- A certificate for use in a production environment MUST be issued by a Certification Authority (CA).
- The choice of Certification Authority issuing the certificate is left to implementations but is subject to review by ENTSOG.
- The issuing CA SHOULD, at a minimum, meet the Normalised Certificate Policy (NCP) requirements specified in [EN 319 411-1].

The following additional requirements apply for certificates for Transport Layer Security:

- A TLS server certificate SHOULD comply with the certificate profile defined in [EN 319 412-4]. At a minimum, the CA Browser forum baseline requirements SHOULD be met [CABFBRCP]. Extended Validation Certificates MAY be used [CABFEVV].
- If a single TLS server certificate is needed to secure host names on different base domains, or to host multiple virtual HTTPS servers using a single IP address, it is RECOMMENDED to use a Multi-Domain (Subject Alternative Name) certificate. Alternatively, wild card certificates MAY be used.
- No additional requirements are placed on TLS client certificates.

The following additional requirements apply for certificates for SOAP Message Security:

- Organisations MAY use a certificate issued by EASEE-gas.

- The type of certificate MUST be certificates for organisations, for which proof of identity is required.
- The issued certificate SHOULD comply with the certificate profile defined in [EN 319 412-3].

A sample certificate profile is provided in section 2.7.2. For certificates used for Message Layer Security it follows the EASEE-gas convention of including the party EIC code as recommended value for the Common Name. Alternatively, the EIC code MAY be used as the Subject SerialNumber or as the Subject OrganisationIdentifier.

Organisations MAY also use Certificate Revocation Lists (CRL) or the Online Certificate Status Protocol (OCSP). Individual companies should assess the potential impact on the availability of the Integrated Date Exchange service when using such mechanisms, as their use may cause a certificate to be revoked automatically and messages to be rejected.

2.7.2 Certificate Profile

This section defines a profile for X.509 certificates to secure Integrated Data Exchange. This profile is consistent with the EASEE-gas certificate profile. For specific requirements, see [ENISA13, , EN 319 411-1 , EN 319 412-3, EN 319 412-4] and [TS119312].

2.7.2.1 Key Size

Entity	Algorithm	Keylength
Root-CA	RSA	Dependent on maximum lifetime of certificate: For 3 years: minimum of 2048 bits For 6 years: minimum of 3072 bits For 10 years: minimum of 4096 bits
Sub-CA	RSA	
End-Entities	RSA	Minimum of 2048 bits, assuming a maximum lifetime of 3 years for end entity certificates.

2.7.2.2 Key Algorithm

Entity	Signing Algorithm	O.I.D.
Root-CA	sha256WithRSAEncryption	1.2.840.113549.1.1.11
Sub-CA	sha256WithRSAEncryption	1.2.840.113549.1.1.11
End-Entities	sha256WithRSAEncryption	1.2.840.113549.1.1.11

2.7.2.3 Naming

The following example uses the ENTSOG name as CA. This is only provided as an illustration. ENTSOG does not currently intend to become a Certification Authority.

Entiteit	Example Value	Comments
Root-CA	C=BE	ISO country code (ISO 3166)
	O=ENTSOG	Name of the Organisation
	CN=ENTSOG CA	Name of the CA
Sub-CA	C=	ISO country code (ISO 3166)
	O=	Name of the Organisation
	OU=	Name of the organisational unit
	CN=	Name of the sub-CA

2.7.2.4 Certificate Body

Certificate Component	Example Value	Presence	Comments
Certificate		M	
TBSCertificate		M	
Version	v3	M	X.509 version 3 is required.
serialNumber	Unique number	M	A unique CA generated number
Signature		M	The calculated signature (for instance the sha2 value encrypted with RSA key with length 4096)
validity.notBefore	Date	M	The start date of the certificate
validity.notAfter	Date	M	The end date of the certificate, at most 3 years after the start date (for end-entities).
issuer.countryName	BE	M	The country code of the country where the CA resides (ISO 3166)
issuer.organisationName	ENTSOG	M	Example, if ENTSOG is the CA
issuer.commonName	ENTSOG CA	M	Example, if ENTSOG is the CA
subject.countryName	BE	M	ISO country code (ISO 3166)
subject.organisationName	Fluxys	M	Name of member organisation
subject.organisationUnit			Not applicable
subject.serialNumber	Unique number		A unique CA generated number. May be used to encode the EIC code, as alternative to using the Common Name.
subject.commonName	EIC code*	M	Preferably the EIC code, following EASEE-gas convention, but some CAs do not support using the EIC in certificate fields.
subject. organizationIdentifier	EIC code*		Recommended in [**EN 319 412-3**]. May be used to encode the

					EIC code, as alternative to using the Common Name.
		subjectPublicKeyInfo.Algorithm	RsaEncryption	M	The encryption algorithm, at least RSA.
		subjectPublicKeyInfo.SubjectPublicKey			The public key of the subject.
		Extensions		M	
	signatureAlgorithm		sha2WithRSAEncryption	M	At least SHA-2 is required. SHA-1 is not allowed.
	signatureValue		Signature of ENTSOG CA	M	The digital signature value.

2.7.2.5 Extensions for Signing, Encryption and TLS End Entities

Extension Name		Ref RFC 5280	Sign end entity	Encrypt end entity	TLS Client / Server end entity	Comments
AuthorityKeyIdentifier		4.2.1.1	M	M	M	
	keyIdentifier		X	x	X	
	authorityCertIssuer		M	M	M	
	authorityCertSerialNumber		M	M	M	
SubjectKeyIdentifier		4.2.1.2	M	M	M	
	subjectKeyIdentifier		M	M	M	
KeyUsage		4.2.1.3	MC	MC	MC	
	digitalSignature		M	x	M	
	nonRepudiation		M*	x	X	* Recommended; Some CAs do not support this for organisations and limit this extension to qualified certificates for natural persons.
	keyEncipherment		X	M	M	In WS-Security the certificate is used to encrypt a symmtric encryption key; it is not used directly to encrypt message data.
	dataEncipherment		X	x	X	

Extension Name	Ref RFC 5280	Sign end entity	Encrypt end entity	TLS Client / Server end entity	Comments
keyAgreement		X	x	x	
keyCertSign		X	x	X	Only for CA root and sub-CA certificates.
cRLSign		X	x	X	Only for CA CRL publishing.
encipherOnly		X	x	X	
decipherOnly		X	x	X	
CertificatePolicies	4.2.1.4	X	x	X	
PolicyMappings	4.2.1.5	X	x	X	
SubjectAltName	4.2.1.6	X	x	X	
otherName					TRUE if applicable.
otherName.type-id					OID = 1.3.6.1.4.1.311.20.2.3 Preferably the subjectserialnumber followed by ENTSOG serialnumber
IssuerAltName	4.2.1.7	X	x	X	
SubjectDirectoryAttributes	4.2.1.8	X	x	X	
BasicConstraints	4.2.1.9	M	M	M	
CA		False	False	False	Only TRUE in case of a CA root or sub-CA certificate.
PathLenConstraint		X	x	X	
NameConstraints	4.2.1.10	X	x	X	
AuthorityInfoAccess		M	M	M	The URL of the OCSP responder.
PolicyConstraints	4.2.1.11	X	x	X	
ExtKeyUsage	4.2.1.12	X	x	M	See next table.
CRLDistributionPoints	4.2.1.13	X	x	X	The URL of the CRL.
InhibitAnyPolicy	4.2.1.14	X	x	X	
FreshestCRL	4.2.1.15	X	x	X	
privateInternetExtensions	4.2.2	X	x	X	

2.7.2.6 Extended Key Usage

Extended Key Usage OID	Ref RFC 5280	TLS Client / Server end entity
id-kp-clientAuth	4.2.1.12	M
id-kp-serverAuth	4.2.1.12	M

2.7.2.7 Certificate Lifetime

Entity	Maximum Period	Start Refresh
Root-CA	15 years	2 years before
Sub-CA	10 years	1 year before
End Entities	3 years	6 months before

3 Profile A: Anonymous Access to Public Information

3.1 Introduction

This section describes profile A, which supports anonymous access to public information and profiles Web Services for use with it. Transmission System Operators are required [CR2011/1227] to provide certain types of information to the general public. By using Integrated Data Exchange to allow parties to request this information, the requested information can be provided in a structured format and can support access to the information from applications or using other automated mechanisms.

Transmission System Operators MAY offer these information services on a “fair use policy” basis, and MAY implement mechanisms to block service abuse.

3.2 Network Layer

Unlike profile C, no IP address-based protection measures (such as whitelisting of IP addresses or IP address ranges used with communication partner) specific to the Integrated Data Exchange are required.

3.3 Transport Layer

While version 1.2 is the RECOMMENDED version for TLS, TLS 1.1 MAY be used if TLS 1.2 is not supported by the client, the security risk is deemed acceptable for the information exchanged and industry recommendations are implemented [TLS1.1-NIST].

4 Profile B: Authenticated Access to Public Information

4.1 Introduction

This section describes profile B, which supports authenticated access to public information and profiles Web Services for use with it. This profile is very similar to profile A, except for its registration and authentication requirements. Service Consumers are assumed to have registered to the Service Provider and obtained a username and password allowing their Web Service clients to authenticate themselves to the Web Service server.

The mechanism for such registration and for the management and distribution of usernames and passwords is out of scope for this document.

The information requested and provided in the Web Service MUST be public information.

4.2 Network Layer

The Network Layer profiling specified in section 3.2 for profile A also applies to this profile B.

4.3 Transport Layer

While version 1.2 is the RECOMMENDED version for TLS, TLS 1.1 MAY be used if TLS 1.2 is not supported by the client, the security risk is deemed acceptable for the information exchanged and industry recommendations are implemented [TLS1.1-NIST].

4.4 Messaging

4.4.1 WS-Security

In this version of this profile, Profile B SOAP request messages MUST be secured using WS-Security [WSSSMS], using a Username Token [WSSUNT]. This token authenticates the requester using a username and password and authorises its access to the Web Service. The use of WS-Security in Profile B is limited to authentication.

Note: a potential requirement has been identified to support, as an alternative, the use of SAML tokens for authentication. This requirement is currently under consideration. A future version of this profile may add a requirement to secure SOAP messages using the Web Services Security SAML Token Profile [WSSSAML].

4.4.2 Interoperability Options

Use of WS-Security MUST conform to the OASIS Basic Security Profile [BSP11], section 12 of which covers the Username token.

5 Profile C: Authenticated Access to Private Information

5.1 Introduction

This section describes profile C, which supports authenticated access to private information and profiles Web Services for use with it. The information requested and provided in the Web Service is assumed to be private, potentially commercially sensitive, information. For this reason additional message layer security measures are taken, in addition to the use of transport layer security.

5.2 Network Layer

Commission Regulation 2015/703 states that the Internet shall be used to exchange data [CR2015/703]. When using the public Internet, each organisation is individually responsible to implement security measures to protect access to its IT infrastructure.

Organisations SHOULD use firewalls to restrict incoming or outgoing message flows to specific IP addresses, or address ranges. This prevents unauthorised hosts from connecting to the Web Services server. Organisations therefore:

- MUST use static IP addresses (or IP address ranges) for inbound and outbound SOAP/HTTPS connections.
- MUST communicate all IP addresses (or IP address ranges) used for outgoing and incoming connections to their communication partners, also covering addresses of any passive nodes in active-passive clusters. Note that the address of the HTTPS server endpoint MAY differ from the address (or addresses) used for outbound connections.
- MUST notify their communication partners about any IP address changes sufficiently in advance to allow firewall and other configuration changes to be applied.

5.3 Transport Layer

Organisations MUST secure the transport layer. The minimum REQUIRED TLS version is 1.2.

5.4 Messaging

5.4.1 WS-Security

Profile C SOAP request, response and fault messages MUST be secured using WS-Security [WSSSMS], using the X.509 Certificate Token Profile [WSSX509], protecting the message using signing and encryption.

Service Providers and Consumers MUST exchange X.509 signing and encryption certificates prior to using the service. The mechanism for sharing certificates is out of scope for this specification.

Messaging is secured using WS-Security:

- Web Services Security SOAP Message Security [WSSSMS].
- Web Services Security X.509 Certificate Token Profile [WSSX509].

The X.509 Certificate Token Profile supports signing and encryption of SOAP messages. This profile REQUIRES the use of X.509 tokens for message signing and encryption.

WS-Security message signing is based on the W3C XML Signature recommendation. The following algorithms MUST be used:

- As message digest algorithm, *http://www.w3.org/2001/04/xmlenc#sha256*.
- As signature algorithm, *http://www.w3.org/2001/04/xmldsig-more#rsa-sha256*.
- As encryption algorithm, *http://www.w3.org/2009/xmlenc11#aes128-gcm*.

In WS-Security, there are three mechanisms to reference a security token (see section 3.2 in [WSSX509]). For interoperability, products SHOULD therefore implement all three options. Note that as *BinarySecurityToken* is the most widely implemented option for security token references in WS-Security-based products, products SHOULD implement this option.

Key Transport algorithms are public key encryption algorithms especially specified for encrypting and decrypting keys, such as symmetric keys used for encryption of message content. The following algorithm MUST be used:

- For encryption method algorithm, *http://www.w3.org/2009/xmlenc11#rsa-oaep*. This is the algorithm used as value for the *Algorithm* attribute of *xenc:EncryptionMethod* on *xenc:EncryptedKey*.
- As mask generation function, *http://www.w3.org/2009/xmlenc11#mgf1sha256*. This is the algorithm used as value for the *Algorithm* attribute of *xenc:MGF* in *xenc:EncryptionMethod*.
- As digest generation function, *http://www.w3.org/2001/04/xmlenc#sha256*. This is the algorithm used as value for the *Algorithm* attribute on *ds:DigestMethod* in *xenc:EncryptionMethod*.

5.4.2 Interoperability Options

Use of WS-Security MUST conform to the OASIS Basic Security Profile [BSP11], section 9 of which covers XML Signature, section 10 of which covers XML Encryption and section 13 of which covers the X.509 token profile.

386 ## *6 Revision History*

Revision	Date	Editor	Changes Made
v0r1	2016-03-18	PvdE	First Draft for discussion
V0r2	2016-06-08	PvdE	Feedback from April and May Workshops processed.
V0r3	2016-06-22	PvdE	Feedback from June ICT KG WG processed. • Fixed some bibliographic references. • ENTSOG approval for any non-EDIG@S XML. • Editorial.
V0r4	2016-09-05	ITC KG, PvdE	Feedback from August ICT KG WG. • Comments by reviewers, resolution by the ITC KG members. • Faults • Business content (incl. headers) versus technical content • Mention potential use of attachments for the future. • Mention potential use of SAML for Profile B for the future. • Suggest using different WSDL ports for different services to optimize routing. • Misc. Editorial. • In 3.2, remove reference to AS4 profile.
Rev_0.5	2016.09.20	ITC KG	Feedback from September ITC KG meeting.
Rev_0.6	2016.10.05	PvdE	Review comments from Andrew McManus processed.

			Review comments from JD processed. Some more comments from ITC KG processed. Added IETF RFC reference for BASE64.
Rev_0.7	2016.12.23	ITC KG, PvdE	Comments from ONTRAS, GTS. TLS and networking aligned with other profiles. HTTP compression recommended for large data sets. Included the certificate, certificate profile, WS-Security sections from the AS4 profile to make this document self-contained.
Rev_0.8	2017.02.07	JM	Accepted all tracked changes following ITC KG Meeting on 24 January 2017
Rev_0.9	2017.12.24	PvdE	Fixed copy-paste errors from AS4 profile. Explicitly stated that Profile B only uses WS-Security for authentication.
Rev_0	2017-03-28	JM	Created Rev_0 with final corrections for publication

7 References

[BSIALG] Entwurf Algorithmenkatalog 2014. Bundesamt für Sicherheit in der Informationstechnik (BSI). Bonn, 11 Oktober 2013. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ElekSignatur/Algorithmenkatalog_Entwurf_2013.pdf?__blob=publicationFile.

[BSITLS] Mindeststandard des BSI nach § 8 Abs. 1 Satz 1 BSIG für den Einsatz des SSL/TLS-Protokolls in der Bundesverwaltung. Bundesamt für Sicherheit in der Informationstechnik (BSI). Bonn, 08 Oktober 2013. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_BSI_TLS_1_2_Version_1_0.pdf

[BP20] Basic Profile Version 2.0. OASIS Committee Specification. http://docs.oasis-open.org/ws-brsp/BasicProfile/v2.0/BasicProfile-v2.0.html

[BSP11] Basic Security Profile Version 1.1. OASIS Committee Specification 01. 22 October 2014. http://docs.oasis-open.org/ws-brsp/BasicSecurityProfile/v1.1/BasicSecurityProfile-v1.1.pdf

[CABFBRCP] CA Browser Forum: " Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates ". Latest Version 1.4.1, September 2016. https://cabforum.org/baseline-requirements-documents/

[CABFEVV] CA Browser Forum. “Guidelines For The Issuance And Management Of Extended Validation Certificates”. Latest Version 1.6.0. July 2016. https://cabforum.org/extended-validation/

[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=uriserv:OJ.L_.2015.113.01.0013.01.ENG

[CR2011/1227] REGULATION (EU) No 1227/2011 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 October 2011 on wholesale energy market integrity and transparency http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32011R1227.

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

[EGCDN] Common Data Network. EASEE-gas Common Business Practice 2007-002/01. http://easee-gas.eu/docs/cbp/approved/CBP2007-002-01_DataNetwork.pdf

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

[EN 319 411-1] European Standard. Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements, v1.1.1, 2016-02. (Formerly [ETSI EN 319 411-3]) http://www.etsi.org/deliver/etsi_en/319400_319499/31941101/01.01.01_60/en_31941101v010101p.pdf

[EN 319 412-3] Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons. http://www.etsi.org/deliver/etsi_en/319400_319499/31941203/01.01.01_60/en_31941203v010101p.pdf

[EN 319 412-4] Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates. http://www.etsi.org/deliver/etsi_en/319400_319499/31941204/01.01.01_60/en_31941204v010101p.pdf

[ENISA13] 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

[ENISA14] Algorithms, Key Size and Parameters Report 2014. November 2014. ENISA. http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report

[ENTSOGAS4] ENTSOG AS4 Profile. Version 2 Revision 0, 2015-06-17. http://www.entsog.eu/public/uploads/files/publications/INT%20Network%20Code/2015/int0488%20131206%20as4%20usage%20profile%20v2r0.pdf

[RFC2119] A. Ramos. Key words for use in RFCs to Indicate Requirement Levels. IETF RFC 2119. January 1998. http://www.ietf.org/rfc/rfc2119.txt

[RFC4648] S. Josefsson. The Base16, Base32, and Base64 Data Encodings. IETF RFC 4648. October 2006. https://tools.ietf.org/html/rfc4648

[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

[RFC6176] S. Turner et al.Prohibiting Secure Sockets Layer (SSL) Version 2.0. RFC 6176. March 2011. http://tools.ietf.org/html/rfc6176

[RFC6555] D. Wing et al. Happy Eyeballs: Success with Dual-Stack Hosts. http://tools.ietf.org/html/rfc6555

[SWA] SOAP Message Transmission Optimization Mechanism , M. Gudgin, N. Mendelsohn, M. Nottingham, H. Ruellan, Editors, W3C Recommendation, 25 January 2005. http://www.w3.org/TR/2005/REC-soap12-mtom-20050125/

[S12] SOAP Version 1.2 Part 1: Messaging Framework. W3C Recommendation. 27 April 2007. http://www.w3.org/TR/soap12-part1/

[S12A] SOAP Version 1.2 Part 2: Adjuncts (Second Edition) https://www.w3.org/TR/soap12-part2/

[S12MTOM] SOAP Message Transmission Optimization Mechanism. M. Gudgin, N. Mendelsohn, M. Nottingham, H. Ruellan, Editors, W3C Recommendation, 25 January 2005,. http://www.w3.org/TR/2005/REC-soap12-mtom-20050125/

[TLSSP] Transport Layer Security (TLS) Parameters. Last Updated 2013-10-03. http://www.iana.org/assignments/tls-parameters/tls-parameters.xml#tls-parameters-4

[TLS1.1-NIST] Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, April 2014. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r1.pdf

[TS119312] ETSI TS 119 312 V1.1.1 Electronic Signatures and Infrastructures (ESI); Cryptographic Suites. http://www.etsi.org/deliver/etsi_ts/119300_119399/119312/01.01.01_60/ts_119312v010101p.pdf

[UDDI] OASIS UDDI TC. UDDI Version 3.02. OASIS Standard. https://www.oasis-open.org/committees/uddi-spec/doc/spec/v3/

[WSADDR] Web Services Addressing 1.0 – Core. W3C Recommendation. 9 May 2006. http://www.w3.org/TR/2006/REC-ws-addr-core-20060509/

[WSDL11] Web Services Description Language (WSDL) 1.1. W3C Note, 15 March 2001. http://www.w3.org/TR/2001/NOTE-wsdl-20010315

[WSRM] Web Services Reliable Messaging (WS-ReliableMessaging) Version 1.2. OASIS Standard, 2 February 2009. http://docs.oasis-open.org/ws-rx/wsrm/v1.2/

[WSSSAML] Web Services Security SAML Token Profile Version 1.1.1. OASIS Standard, 18 May 2012. http://docs.oasis-open.org/wss-m/wss/v1.1.1/os/wss-SAMLTokenProfile-v1.1.1-os.html

[WSSSMS] OASIS Web Services Security: SOAP Message Security Version 1.1.1. OASIS Standard, May 2012. http://docs.oasis-open.org/wss-m/wss/v1.1.1/wss-SOAPMessageSecurity-v1.1.1.doc

[WSSUNT] OASIS Web Services Security Username Token Profile Version 1.1.1. OASIS Standard, May 2012.

http://docs.oasis-open.org/wss-m/wss/v1.1.1/wss-UsernameTokenProfile-v1.1.1.pdf

[WSSX509] OASIS Web Services Security: Web Services Security X.509 Certificate Token Profile Version 1.1.1. OASIS Standard, May 2012. http://docs.oasis-open.org/wss-m/wss/v1.1.1/wss-x509TokenProfile-v1.1.1.doc