ENTSOG Interactive 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 Interactive 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) defines *interactive data exchange*: as a mechanism in which "*the data is exchanged interactively through a web application via a browser.*" It specifies that:

"*The common data exchange solutions shall comprise the protocol, the data format and the network. [..] For the interactive data exchange, the protocol shall be HTTP/S.*"

Additional guidelines are useful to specify how the identified protocol is to be used. This document is a technical specification that provides such additional guidelines. These guidelines are mostly about consistency and usability than about technical conformance, because the exchange involves humans and is not completely automated. For this reason, the issue of technical interoperability applies less, because data exchange is site-to-user or user-to-site, but not site-to-site. It does apply to upload and download functionality (see section 2.10), in which structured data formats are used.

In this profile, the term "Web Application" is used as it is the term using in [CR2015/703]. The term relates to aspects such as presentation, interaction, format and content and does not prescribe any particular application technology to be used to implement the Web Application on a Web server.

1.2 Use Cases

A number of different use cases have been identified that can be supported by Interactive Data Exchange. These include:

- Anonymous access to public information.
- Authenticated access to public information.
- Authenticated access to private information.
- Authenticated transactions involving private information.

As these use cases have different requirements, it is not possible to specify a single profile covering all use cases. For this reason, the technical specification is divided in multiple parts:

- Common guidelines for Interactive Data Exchange. This profiling applies to all uses of Interactive Data Exchange. This is covered in section 2.
- Additional Guidelines relating to security. A number of options are covered in section 3.

1.3 Goals

The main goals of this profile are to:

- Support public, private, anonymous and authenticated access to services.

- Support both information access and transactions.
- Increase consistency and usability and facilitate implementations.
- 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].

1.4 Terminology

This profile adopts document conventions common in technical specifications for Internet protocols and data formats. The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

2 Common Guidelines for Interactive Data Exchange

2.1 Introduction

This section provides common guidelines for interactive data exchange.

2.2 Network Layer

Interactive 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.

Data exchange MUST use 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 Interactive 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 Interactive Data Exchange MAY be IPv6 only. A future version of this profile will therefore REQUIRE support for IPv6.

2.3 Transport Layer

Interactive Data Exchange MUST use HTTP over TLS, providing confidentiality of all exchanges. The minimum version of HTTP to use is 1.1. HTTP/2 [RFC7540] MAY be used. Servers 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**Error! Reference source not found.**] and in 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 2.5.
- It MUST be possible to configure the accepted TLS version(s) in the Web Application. 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.

If TLS 1.2 is not supported by the client, the server MAY use TLS 1.1 if the security risk is deemed acceptable for the information exchanged, provided that industry recommendations on securing TLS 1.1 are implemented [TLS1.1-NIST].

2.4 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.

2.5 Certificates and Public Key Infrastructure

In this Usage Profile, X.509 certificates are used to secure the Transport Layer. Requirements on certificates can be sub-divided into two groups:

- General requirements;
- Requirements for Transport Layer 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:

- At a minimum, the CA Browser forum baseline requirements SHOULD be met [CABFBRCP]. Extended Validation Certificates MAY be used [CABFEVV].
- For server certificates, the Certification Authority SHOULD be trusted by commonly used Web Browsers and/or Operating Systems (see section 2.7).
- 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.

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.

2.6 Content

The Web Application SHOULD comply with HTML5, which in this profile is used as a buzzword to refer to modern Web technologies, many of which (though by no means all) are developed at the Web Hypertext Application Technology Working Group [WHATWG]. As the WHATWG develops HTML5 as a “living standard” that is continuously updated and hence a moving target, it is RECOMMENDED that implementers of Web Applications align, at a minimum, with the W3C HTML 5 recommendation [HTML5].

Organisations SHOULD validate their content using the W3C Markup Validation Service, https://validator.w3.org/, or an equivalent validation service.

The use of plug-ins and/or proprietary formats is NOT RECOMMENDED.

For business data, the Web Application MUST align with the specification of information elements provided in the ENTSOG Business Requirements Specifications (BRS) in terms of:

- Naming and semantics.
- Cardinality (minimum/maximum occurrence).
- Data types and units.
- Grouping of elements (or of groups).

2.7 Client Independence

The Web Application SHOULD not be tied to a particular client application or device. The Web Application is RECOMMENDED to implement Responsive Web Design enabling adaptive scaling for different screen resolutions and usability on mobile devices.

The Web Application MUST NOT require a particular operating system or browser. Recent versions of commonly used Web Browsers MUST be supported. The Web Application SHOULD NOT depend on features that are only available in the very latest (versions of) Web browsers, except if required for security purposes.

2.8 Accessibility

The Web Application MUST be accessible to people with disabilities. At a minimum, the Application MUST comply with the W3C Web Content Accessibility Guidelines [WCAG10].

2.9 Language

To allow the Web Application to be used by users in the various EU Member States, natural language content of the Web Application SHOULD be available in multiple languages. At a minimum, one official language (or more, if required by national legislation) of the Member State in which the company is based and English SHOULD be supported.

This also applies for input methods for text. English (Latin subset) input and company local input MUST be supported. Support for other alphabets are OPTIONAL. The Web Application MUST make provisions for text input in different (unsupported) writing systems (e.g. graceful rejection, automatic transliteration) and MUST make provisions to prevent script spoofing / homograph attacks.

2.10 Upload / Download Function

If the Web Application provides functionality for bulk uploading and/or downloading of data, it MUST support uploading and/or downloading data in CSV, XML and/or other machine-processable formats, to allow subsequent analysis or otherwise processing of the data.

Use of standardized structured data formats and schemas is RECOMMENDED. The specific data formats and schemas to be used depend on the type of data that is exchanged interactively and out of scope for this profile.

To download (or upload) large data sets efficiently, the Web Application SHOULD allow users to download (or upload) data in a compressed format.

Apart from machine-processable formats, the Web Application MAY in addition support other (including presentation-oriented) formats.

3 Security Options for Interactive Data Exchange

3.1 Introduction

Whereas the guidelines of section 2 apply to all Interactive Data Exchanges, this section specifies a number of alternative security options. The use cases described in section 1.2 vary in the security options appropriate to them. This section provides an overview of options available to providers offering Interactive Data Exchange.

3.2 No Authentication

The use case “anonymous access to public information” MUST NOT require any authentication of the user when accessing the Web Application.

To prevent abuse by automated data collection tools, the Web Site MAY use CAPTCHA (“Completely Automated Public Turing test to tell Computers and Humans Apart”) or other challenge/response mechanisms to determine whether or not the user is human.

3.3 Username / Password Authentication

If the Web Application provides “registered access to public information”, the user MUST be authenticated using a Username and a Password.

The registration process, the management and the issuance of usernames and passwords is left to implementations.

3.4 Two Factor Authentication

Two Factor Authentication is a method of confirming a user's claimed identity by utilising a combination of two different components, typically a combination of knowledge (something the user knows, such as a passcode or PIN) and possession (something they have, such as a USB token or). For services provided to specific users and involving the exchange of private information of those users, or the execution of business transactions involving the companies on whose behalf the authenticated users act, or access to non-public data from those companies, Two Factor Authentication MUST be used. In this scenario, the user has access to the site upon successful authentication until the user session expires.

Two Factor Authentication MAY be provided by a personal certificate distributed using a PIN protected USB token. However, the specific technology used for Two Factor Authentication is left to implementations. Furthermore, the registration process, the management and the issuance of authentication tokens is left to implementations.

Note that due to the risk that SMS messages or voice calls may be intercepted or redirected, implementers of new systems SHOULD carefully consider alternative authenticators.

Note that there is currently no requirement for users to be able to use a single authentication component (such as a particular USB token) to access services of distinct services.

3.5 Token-Based Authorisation

Depending on business requirements and/or risk assessment, an additional layer MAY be added to the Two Factor Authentication option described in section 3.4 to provide authorisation and non-repudiation. This layer requires the user to use a token not only for authentication, but also to explicitly commit to specific transactions. For example, the Web Application could request the user to enter a transaction identifier to confirm the transaction.

4 Revision History

Revision	Date	Editor	Changes Made
Rev0.1	2016-05-09	PvdE	First Draft for discussion
Rev_0.2	2016-06-08	PvdE	Updates based on feedback at May 2016 workshop.
Rev_0.3	2016-06-22	PvdE	Updated based on feedback at June 2016 workshop.
Rev_0.4	2016-09-05	ITC KG, PvdE	Updated based on feedback at August 2016 workshop. • Define term Two Factor. • Clarification of difference between interactive exchange and the other types of exchange: more about usability/consistency than about standardization/interoperability. • Misc. Editorial.
Rev_0.5	2016-09-20	ITC KG	Updates from September meeting; review
Rev_0.6	2016-10-04	PvdE	Further comments from September meeting, JD and JM processed. Comments from Andrew McManus
Rev_0.7	2016-12-15	ITC KG	Comments from Gaz System, ONTRAS, GTS, reviewed and updated in ITC KG meeting. Review from ENTSOG Legal on section 2.9. Comments on “Web Application” term. Network Layer and TLS aligned with other profiles. Certificate information included rather than AS4 reference.
Rev_0.8	2017-02-07	JM	Accepted all tracked changes following ITC KG Meeting on 24 January 2017
Rev_0	2017-03-28	JM	Created Rev_0 for publication

5 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

[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

[D2016/680] DIRECTIVE (EU) 2016/680 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016L0680

[D2016/1148] DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L1148

[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

[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

[HTML5] I. Hickson et al. HTML5. A vocabulary and associated APIs for HTML and XHTML. W3C Recommendation 28 October 2014. https://www.w3.org/TR/html5/

[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 [R2016/679] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679

[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

[RFC7540] M. Belshe et al. Hypertext Transfer Protocol Version 2 (HTTP/2). RFC 7540, May 2015. https://tools.ietf.org/html/rfc7540

[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

[WCAG10] W. Chrisholm, G. Vanderheiden and I. Jacobs. Web Content Accessibility Guidelines 1.0. W3C Recommendation 5-May-1999. https://www.w3.org/TR/1999/WAI-WEBCONTENT-19990505/ [WHATWG] Web Hypertext Application Technology Working Group (WHATWG). HTML Living Standard. https://html.spec.whatwg.org/multipage/index.html