Ecma/TC39/2015/034
Ecma/GA/2015/065

ICT/MSP (2015) 322
29/04/2015

European Multi-Stakeholder Platform on ICT Standardization

Meeting: **11 June 2015**

Draft Evaluation Report of IETF protocols for websites: FTP, HTTPS, HTTP, URI, URL, URN and UTF-8.

Document for:

Information	
Decision	✓
Discussion	✓

Email: ec-ict-std-platform@ec.europa.eu

Identification of ICT technical specifications

IETF protocols for websites: FTP, HTTPS, HTTP, URI, URL, URN and UTF-8.

Draft Evaluation Report

Version 03 – 16/04/2015

Management summary

This report contains the evaluation report as well as the proposed advice of the European Multi-stakeholder Platform on ICT Standardisation on the submission of 7 specifications: File Transfer Protocol (FTP); Hypertext Transfer Protocol (HTTP) 1.1; Hypertext Transfer Protocol Secure (HTTPS); Uniform Resource Identifier (URI); Uniform Resource Locator (URL); Uniform Resource Name (URN) and UCS Transformation Format 8-bit (UTF-8). to be identified in accordance with Article 13 and Annex II (based on the WTO[1] standardisation principles) of Regulation (EU) No. 1025 /2012[2].

When the evaluation started, also JavaScript Object Notation (JSON) was part of the evaluation. Several issues arose concerning the coherence between JSON and ECMA-404 and effects on interoperability. End of March ECMA and IETF started to work on synchronization of the two specifications. For this reason The Netherlands, who submitted JSON to the MSP procedure, decided to postpone the submission. Expectation is that in the autumn of 2015 the issues will be solved and the evaluation process can be continued. The results and discussions on JSON so far, are recorded in Annex 1 of this report.

The report covers mainly the following structure:

1) Assessment of the compliance with the "market acceptance" and "coherence" criteria set by Annex II.1 & 2; providing information on the proposed ICT technical specification against the background of the formal European standardisation system and existing and/or on-going standardization activities in the relevant domain

[1] World Trade Organisation

[2] Regulation (EU) No. 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European Standardisation. OJ L 316/12 of 14.11.2012

2) Assessment of the characteristics of the organisation and its technical specification developing procedures in accordance with Annex II.3.

3) Assessment of the compliance against the requirements for the identification of ICT technical specification, set by Annex II.4.

Further to the assessments above, it is proposed that the European Multi-stakeholder Platform on ICT Standardisation comes to the following conclusion: **a "positive" advice should be given on the identification of the submitted ICT technical specifications FTP, HTTPS, HTTP, URI, URL, URN and UTF-8.**

Evaluation Group

FTP, HTTPS, HTTP, URI, URL, URN and UTF-8

Report to the Platform

1 Objective for the report

1.1 Background

Economic growth and responsiveness to citizens' expectations in a digital world requires interoperability between services, applications and products. Achieving interoperability requires standards and technical specifications[3]. Public authorities should make use of the full range of standards and technical specifications when procuring hardware, software and information technology services; this will allow them to efficiently fulfil their tasks. The Pillar II of the Digital Agenda for Europe recognised the need of sound standards and common technical specifications to promote interoperability, and advocates public authorities to make use of available standards and common technical specifications when commissioning hardware, software and IT services from suppliers.

To that objective the Regulation (EU) No. 1025/2012 on European standardisation ("the Regulation") lays down in its Chapter IV a procedure for the identification of ICT technical specifications which are not issued by European, international or national standardisation organisations but that still could be referenced in public procurement acts by public authorities, provided that these ICT specifications, proposed by the Commission or by Member States, comply with the requirements set by Annex II of the Regulation.

These requirements cover the coherence of the proposed ICT specification with the formal European and international standardisation environment, the qualities of the standardisation process implemented in the standards setting organisation that issued the proposed ICT specification and some aspects of the proposed specification itself. Compliance with these requirements guarantees the public authorities that the proposed ICT specification is set in accordance with the founding principles recognised by the World Trade organisation (WTO) in the field of standardisation.

The objective of this report is to allow the European Multi-stakeholder Platform on ICT Standardisation ("the Platform") to evaluate the compliance of the proposed ICT specifications with the requirements set in Annex II of the Regulation. The Platform is subsequently expected to provide its advice to the Commission on the potential "identification" of the submitted ICT specifications.

[3] The definition of standards and technical specifications is given in Article 2 of Regulation (EU) No 1025/2012.

The Platform is an expert group set up by the Commission Decision of 28th November 2011. It is composed of representatives of Member States, Industry, societal organisations, formal standards organisations and fora & consortia. The Article 2.f of this Decision states that one of the tasks of the Platform is "*to advise the Commission on the identification of the technical specifications in the field of ICT which are not national, European of international standards*". The Platform agreed on a process for such identification (doc. ICT/MSP (2012) 057), in accordance with Article 13 of the Regulation.

1.2 The process

- On 04/12/2014 the Standardisation Forum Office of the Ministry of the Interior of the Netherlands submitted 28 ICT technical specifications, to the evaluation process in view of its identification by the Commission as ICT technical specifications eligible for referencing in public procurement, in accordance with Article 13 of the Regulation. The identified ICT technical specifications resulting from this process, in accordance with Article 14 of the Regulation, shall constitute a "common technical specification" referred to in Directives 2004/17/EC and 2004/18/EC and 2009/81/EC, and therefore shall become eligible for direct referencing in public procurement. The secretariat of the Platform has verified whether the information on the seven evaluation submission forms is complete. The submission forms have subsequently been forwarded to the members of the Platform for discussion and for the establishment of an Evaluation Group to assess this information with respect to the requirements set by the Annex II of the Regulation.

- The Platform noted the submission of the 28 technical specifications at its meeting of 04/12/2014. The Platform decided to establish an ad hoc Evaluation Group to carefully analyse the data provided in the submission form; to seek, if necessary, further information from the submitter and the specification originating organisation; and to consolidate the information in an evaluation report addressed to the Platform, which will allow the Platform to prepare its advice on the identification of the proposed ICT technical specification to the Commission. The Platform decided to cluster the evaluations in five reports, in each of which several related technical specifications are evaluated. In this report the following technical specifications are discussed: File Transfer Protocol (FTP); Hypertext Transfer Protocol (HTTP) 1.1; Hypertext Transfer Protocol Secure (HTTPS); Uniform Resource Identifier (URI); Uniform Resource Locator (URL); Uniform Resource Name (URN) and UCS Transformation Format 8-bit (UTF-8). The submission of and JavaScript Object Notation (JSON) was postponed. All these specifications are aimed at “setting-up a website”. The Platform will discuss the report and the draft advice to the Commission at its meeting of 11/06/2015.

- Should the Platform deliver a favourable opinion, the Commission will launch a consultation of sectoral experts.

- After consulting the MSP and the sectoral experts, the Commission may adopt the implementing Decision to identify File Transfer Protocol (FTP); Hypertext Transfer Protocol (HTTP) 1.1; Hypertext Transfer Protocol Secure (HTTPS); Uniform Resource Identifier (URI); Uniform Resource Locator (URL); Uniform Resource Name (URN) and UCS Transformation Format 8-bit (UTF-8) for referencing in public procurement.

1.3 Evaluation group

Following its decision of 04/12/2014, the Platform agreed to create an Evaluation Group made by volunteers members of the Platform, to assess whether FTP, HTTPS, HTTP, URI, URL, URN, UTF-8 and JSON comply with the requirements set by Annex II of the Regulation. A representative of Internet Engineering Taskforce (IETF), as specification setting organisation, participated on an advisory basis, while the secretariat of the group was assured by the Commission.

The Evaluation Group was composed of representatives from the following Platform members:

1. Netherlands (chair)
2. W3C (co-chair)
3. European Commission (secretary)
4. IETF (advisor)
5. Austria
6. Belgium
7. Switzerland
8. United Kingdom
9. DIGITALEUROPE
10. ECMA
11. IEEE
12. ETSI
13. W3C

The Evaluation Group has performed its tasks by electronic means, including a call conference. The group delivered its preliminary report to the Platform secretariat on 30/04/2015, to be presented to the Platform on its meeting of 11/06/2015.

1.4 Subject of the evaluation

This evaluation report covers eight technical specifications: FTP, HTTPS, HTTP, URI, URL, URN and , UTF-8. These specifications form a cluster of specifications targeted towards “setting-up a website”. Each of these specifications in the cluster is briefly described below in relation to the other specifications in the cluster.

The File Transfer Protocol (FTP) is specified in the Internet Standard RFC0959 and is a standard network protocol used to transfer computer files from one host to another host over a TCP-based network, such as the Internet. The objectives of FTP are 1) to promote sharing of files (computer programs and/or data), 2) to encourage indirect or implicit (via programs) use of remote computers, 3) to shield a user from variations in file storage systems among hosts, and 4) to transfer data reliably and efficiently. FTP, though usable directly by a user at a terminal, is designed mainly for use by programs. FTP is built on a client-server architecture and uses separate control and data connections between the client and the server. FTP users may authenticate themselves using a clear-text sign-in protocol, normally in the form of a username and password, but can connect anonymously if the server is configured to allow it. For secure transmission that protects the username and password, and encrypts the content, FTP is often secured with SSL/TLS (FTPS). SSH File Transfer Protocol (SFTP) is sometimes also used instead, but is technologically different.

The first version of the Hypertext Transfer Protocol (HTTP) is specified in the Proposed Standard RFC2616. The current version 1.1 is specified in RFCs 7230 to 7235. HTTP is an application-level protocol for distributed, collaborative, hypermedia information systems. It is a generic, stateless, protocol that can be used for many tasks beyond its use for hypertext, such as name servers and distributed object management systems, through extension of its request methods, error codes and headers. A feature of HTTP is the typing and negotiation of data representation, allowing systems to be built independently of the data being transferred. HTTP has been in use by the World-Wide Web global information initiative since 1990. HTTP/1.1 is a revision of the original HTTP (HTTP/1.0). In HTTP/1.0 a separate connection to the same server is made for every resource request. HTTP/1.1 can reuse a connection multiple times to download images, scripts, stylesheets, etc. after the page has been delivered. HTTP/1.1 communications therefore experience less latency as the establishment of TCP connections presents considerable overhead.

Hypertext Transfer Protocol Secure (HTTPS) is specified in the Proposed Standard RFC2817 and is a communications protocol for secure communication over a computer network, with especially wide deployment on the Internet. Technically, it is not a protocol in and of itself; rather, it is the result of simply layering the Hypertext Transfer Protocol (HTTP) on top of the SSL/TLS protocol, thus adding the security capabilities of SSL/TLS to standard HTTP communications. The security of HTTPS is therefore that of the underlying TLS, which uses long-term public and secret keys to exchange a short term session key to encrypt the data flow between client and server.

In computing, a Uniform Resource Identifier (URI) is specified in the Internet Standard RFC 3986 and is a string of characters used to identify a name of a resource. Such identification enables interaction with representations of the resource over a network, typically the World Wide Web, using specific protocols. Schemes specifying a concrete syntax and associated protocols define each URI. The most common form of URI is the uniform resource locator (URL), frequently referred to informally as a web address. More rarely seen in usage is the uniform resource name (URN), which was designed to complement URLs by providing a mechanism for the identification of resources in particular namespaces. The URN defines an item's identity, while the URL provides a method for finding it.

Uniform Resource Locator (URL) (also known as web address, particularly when used with HTTP) is specified in the Proposed Standard RFC4395 and is a specific character string that constitutes a reference to a resource. In most web browsers, the URL of a web page is displayed on top inside an address bar. An example of a typical URL would be "http://en.example.org/wiki/Main_Page". The address contains three elements: the type of protocol used to access the file (e.g., HTTP for a Web page, ftp for an FTP site); the domain name or IP address of the server where the file resides; and, optionally, the pathname to the file.

Uniform Resource Names (URNs) is specified in the Proposed Standard RFC 2141 and are intended to serve as persistent, location-independent, resource identifiers and are designed to make it easy to map other namespaces (which share the properties of URNs) into URN-space. Therefore, the URN syntax provides a means to encode character data in a form that can be sent in existing protocols, transcribed on most keyboards, etc.

UTF-8 (UCS Transformation Format—8-bit) is specified in the Internet Standard RFC3629 and is a variable-width encoding that can represent every character in the Unicode character set. It was designed for backward compatibility with ASCII and to avoid the complications of endianness and byte order marks in UTF-16 and UTF-32. UTF-8 has become the dominant character encoding for the World Wide Web, accounting for more than half of all Web pages. The Internet Mail Consortium (IMC) recommends that all e-mail programs be able to display and create mail using UTF-8. UTF-8 is also increasingly being used as the default character encoding in operating systems, programming languages, APIs, and software applications.

1.5 Possible links with other ICT technical specifications or standards

The previous section already describes the specifications in this cluster and possible links between them. In addition, the following links with other ICT technical specifications or standards can be identified.

FTP:

The main specification of FTP can be found in RFC 0959. However, there is a strong link with other IETF specifications, because the following specifications are necessary for basic implementations of the FTP protocol (see Annex 1 for a complete list):

- RFC 959: https://datatracker.ietf.org/doc/rfc959/
- RFC 2228: https://datatracker.ietf.org/doc/rfc2228/
- RFC 2640: https://datatracker.ietf.org/doc/rfc2640/
- RFC 3659: https://datatracker.ietf.org/doc/rfc3659/

HTTP:

The main specification of HTTP v1.1 can be found in RFC 2616. However, there is a strong link with other IETF specifications, because the following specifications are necessary for basic implementations of the HTTP protocol (see Annex 1 for a complete list):

- RFC 7230: https://datatracker.ietf.org/doc/rfc7230/
- RFC 7231: https://datatracker.ietf.org/doc/rfc7231/
- RFC 7232: https://datatracker.ietf.org/doc/rfc7232/
- RFC 7233: https://datatracker.ietf.org/doc/rfc7233/
- RFC 7234: https://datatracker.ietf.org/doc/rfc7234/
- RFC 7235: https://datatracker.ietf.org/doc/rfc7235/

HTTPS:

The main specification of HTTPS can be found in RFC 2817. However, there is a strong link with other IETF specifications, because the following specifications are necessary for basic implementations of the HTTPS protocol (see Annex 1 for a complete list):

- RFC 2817: http://datatracker.ietf.org/doc/rfc2817/
- RFC 4346: https://datatracker.ietf.org/doc/rfc4346/
- RFC 5246: https://datatracker.ietf.org/doc/rfc5246/
- RFC 7230: https://datatracker.ietf.org/doc/rfc7230/

URI/URL/URN:

The URI has become the standardized way to identify sources on the Internet. However, it should be noted that the DOI[4] System (recently acquired ISO status, ISO 26324[5]) is a character string (a "digital identifier") used to uniquely identify an object such as an electronic document. DOI implements the Uniform Resource Identifier (Uniform Resource Name) concept and adds to it a data model and social infrastructure. Organizations that meet the contractual obligations of the DOI system and are willing to pay to become a member of the system can assign DOIs. URL/URNs are mainly used for webpages or parts of webpages, while DOI is mainly used for books, documents or articles. URL/URNs and DOI make use of each other and can exist next to each other. Therefore, no interoperability issues will arise.

[4] http://www.doi.org/

[5] http://www.iso.org/iso/home/news_index/news_archive/news.htm?refid=Ref1561

UTF-8:

The RFC which is assessed in this report is RFC3629, which sets guidelines on the use of UTF-8 in Internet protocols and defines the rules for MIME types. UTF-8 has become the most common encoding for HTML files. ASCII (from the American National Standards Institute) was the most commonly used character encoding on the World Wide Web until December 2007, when it was surpassed by UTF-8, which includes ASCII as a subset. UTF-8 is designed for backward compatibility with ASCII and thus no interoperability issues will arise. The Universal Character Set (UCS), defined by the International Standard ISO/IEC 10646, is a standard set of characters upon which many character encodings are based. Currently, the dominant UCS encoding is UTF-8. The same set of characters is defined by the Unicode standard, which further defines additional character properties and other application details of great interest to implementers. ISO/IEC 10646 and Unicode define several encoding forms of their common repertoire: UTF-8, UCS-2, UTF-16, UCS-4 and UTF-32. ISO/IEC 10646 is equivalent to the specifications created by the Unicode consortium. UTF-8 is defined by Unicode and therefore an ISO standard. RFC3629 sets a few guidelines on the use of UTF-8 in Internet protocols and defines the rules for MIME types. UTF-8 is a profile for the use of ISO/IEC 10646 in Internet protocols and uses that specification as normative.

2 Evaluation of compliance with the general conditions

2.1 Market acceptance

The first thing that can be said about market acceptance of the ICT specifications under consideration is that they all have been accepted by the market and are widely in use. They are so-called common standards and specifications that are used in most IT systems within the government domain as well as other domains. For each of the specifications a few words are spent on the market and its usage. The European Commission maintains a list of the current state of play of recommended/mandatory ICT standards and specifications in the EU Member States[6]. For each of specifications, it is noted which countries is mentioning the standard. Most likely all computers of public authorities use the protocols and the specifications covered as no competitors to be interoperable with exist anymore nowadays.

Most common web browsers can retrieve files hosted on FTP servers. The first FTP client applications were command-line applications developed before operating systems had graphical user interfaces, and are still shipped with most Windows, Unix, and Linux operating systems. Many FTP clients and automation utilities have since been developed for desktops, servers, mobile devices, and hardware, and FTP has been incorporated into productivity applications, such as Web page editors. Well-known FTP-clients for Windows are CuteFTP, FileZilla, WinSCP and WS FTP. For Mac OS X is Cyberduck a well-known opensourceclient. A full-featured FTP client can be run within Firefox in the form of an extension called FireFTP. The EC list indicates that FTP is listed in The Netherlands, Estonia, France, Germany, Malta, Slovakia, and Switzerland.

All of the major web browsers support HTTP1.1. The European Commission list indicates that HTTP is listed in Belgium, the Netherlands, Estonia, Germany, France, Malta, Portugal, Spain, and Switzerland. Most popular websites have also a secure implementation of HTTPS. It is especially used for payment transactions on the internet, e-mail and for sensitive transactions. In the late 2000s and early 2010s, HTTPS began to see widespread use for protecting page authenticity on all types of websites, securing accounts and keeping user communications, identity and web browsing private. The European Commission list indicates that HTTPS is listed in the Netherlands, Malta and Portugal.

The Web makes use of a single global identification system: the URI (with URL's and URN's as types or URI's). They are a cornerstone of Web architecture and are necessary so that we can refer to things on the Web, access them, describe them, and share them. The Web relies on global agreement to follow the rules of URIs. There are no interoperability issues between URI/URL/URN and other existing European or International standards. URI has become the standardized way to identify sources on the Internet. The European Commission list indicates that URI is listed in the Netherlands, Finland, and Spain. URL and URN are listed in the Netherlands, and Spain.

As mentioned, the DOI System is another character string (a "digital identifier") used to uniquely identify an object such as an electronic document. URL/URNs are mainly used for webpages or parts

[6] https://joinup.ec.europa.eu/community/camss/og_page/list-standards

of webpages, while DOI is mainly used for books, documents or articles. URL/URNs and DOI make use of each other and can exist next to each other in the market.

UTF-8 has become the most common encoding for HTML files. ASCII (from the American National Standards Institute) was the most commonly used character encoding on the World Wide Web until December 2007, when it was surpassed by UTF-8, which includes ASCII as a subset. UTF-8 is designed for backward compatibility with ASCII and thus no interoperability issues will arise. The European Commission list indicates that UTF-8 is listed in Belgium, the Netherlands, Estonia, Finland, France, Malta, Portugal, Spain, Slovakia, and Switzerland. More than half of all Web pages are encoded in UTF-8. IETF requires all Internet protocols to identify the encoding used for character data, and the supported character encodings must include UTF-8. The Internet Mail Consortium (IMC) recommends that all e-mail programs be able to display and create mail using UTF-8. It is also increasingly being used as the default character encoding in operating systems, programming languages, APIs, and software applications.

2.2 Coherence with the formal European standardisation environment

2.2.1 The specification covers a domain where the adoption of a new European standard or standardisation deliverable is not foreseen within a reasonable period.

There is no adoption of new European Standards foreseen covering exactly the same area as all the specifications in this cluster. Below, a brief explanation is given per specification.

FTP covers the area of exchanging computer files. No other specifications in this area are being considered to become a European standard.

HTTP covers the area of exchanging and transferring hypertexts. It is the underlying protocol used by the World Wide Web. No other specifications in this area are being considered to become a European standard.

HTTPS covers the area of securing web communications. No other specifications that cover this area are considered to become a European standard. Secure HTTP (S-HTTP) is a little-used alternative to the HTTPS for encrypting web communications carried over http. It is defined in RFC 2660. HTTPS and S-HTTP were both defined in the mid-1990s. Netscape and Microsoft supported HTTPS rather than S-HTTP, leading to HTTPS becoming the *de facto* standard mechanism for securing web communications. S-HTTP is also not under consideration to become a European standard.

URI covers the area of identification of resources in the form of URLs or URNs. No other specifications cover this area that are under consideration to become a European standard. As mentioned DOI is an alternative that covers the area of books, documents and articles.

UTF-8 is defined by Unicode and therefore an ISO standard. RFC3629, assessed in this report, sets a few guidelines on the use of UTF-8 in Internet protocols and defines the rules for MIME types. UTF-8 is a profile for the use of ISO/IEC 10646 in Internet protocols and uses the ISO specification as

normative. Therefore, the RFC3629 and the area it covers is not being set by ISO, but builds on top of ISO standards.

The Universal Character Set (UCS), defined by the International Standard ISO/IEC 10646, is a standard set of characters upon which many character encodings are based. Currently, the dominant UCS encoding is UTF-8. The same set of characters is defined by the Unicode standard, which further defines additional character properties and other application details of great interest to implementers. ISO/IEC 10646 and Unicode define several encoding forms of their common repertoire: UTF-8, UCS-2, UTF-16, UCS-4 and UTF-32. ISO/IEC 10646 is equivalent to the specifications created by the Unicode consortium.

2.2.2 The current scope of the formal European standardisation organisations does not cover any similar domain

For all the specifications in this cluster there are no current activities in the formal European standardisation organisations that cover the same domain. Thus, no European standardisation organisation will produce a standard with the same scope as the specifications in this cluster.

2.2.3 Transposition of the proposed ICT technical specification into a European standard or standardisation deliverable is not foreseen within a reasonable period.

For all the specifications in this cluster there are no current activities in the IETF to transposition them into a European standard. It is the default policy of the IETF to maintain the specifications as separate IETF RFCs and not to engage a standardization trajectory towards European or International Standardization Organizations.

3 Evaluation of compliance with the attributes

3.1 The organisation developing the specification

Summary: the FTP, HTTPS, HTTP, URI, URL, URN and UTF-8 specifications are approved and will be maintained by a non for profit organisation. The development of the specifications is based on open and transparent processes, participation by all relevant stakeholders is possible, and decisions are taken on the basis of consensus.

The specifications have been developed and are maintained by the Internet Engineering Task Force (IETF). The IETF is the principal body engaged in the development of new Internet standard specifications.

What follows is an informal narrative, for a full overview of authoritative documents as they relate to the IETF standards process see http://www.ietf.org/about/process-docs.html

The IETF's aim is to make the Internet work better by producing high quality, relevant technical documents that influence the way people design, use, and manage the Internet.

Its mission includes the following (see RFC3935, http://www.ietf.org/rfc/rfc3935.txt, for more details):

1. Identifying, and proposing solutions to, pressing operational and technical problems in the Internet

2. Specifying the development or usage of protocols and the near-term architecture to solve such technical problems for the Internet

3. Making recommendations to the Internet Engineering Steering Group (IESG) regarding the standardization of protocols and protocol usage in the Internet

4. Facilitating technology transfer from the Internet Research Task Force (IRTF) to the wider Internet community

5. Providing a forum for the exchange of information within the Internet community between vendors, users, researchers, agency contractors, and network managers. The IETF meeting is not a conference, although there are technical presentations. The IETF is not a traditional standards organization, although many specifications that are produced become standards. The IETF is made up of volunteers, many of whom meet three times a year to fulfil the IETF mission.

Most of the work in the IETF is done by e-mail in various IETF mailing lists, and during IETF meetings, held three times a year. There is no membership in the IETF. Anyone may subscribe to a mailing list and participate, or register for a meeting and then attend.

Organizational home, financial and legal support for the IETF[7] are provided by the **I**nternet **Soc**iety (ISOC). ISOC maintains the books and is hired the IETF's directly employed administrative staff.

The Internet Society is an international not-for-profit organization concerned with the growth and evolution of the worldwide Internet and with the social, political, and technical issues that arise from its use. The ISOC is an organization with individual and organizational members. The ISOC is managed by a Board of Trustees elected by the worldwide individual membership.

The way in which the members of the ISOC Board of Trustees are selected, and other matters concerning the operation of the Internet Society, are described in the ISOC By Laws [C].

3.2 The development process

The Internet Standards Process is documented in RFC2026, as updated by RFC6410. Again, what follows is an informal narrative.

IETF has no specific membership rules; participation to IETF standardisation activities is open to all on the basis of direct participation. The decision process is based on achieving a rough consensus among the participants (see RFC7282 “On Consensus and Humming in the IETF”).

The Internet Standards Process is an **open, transparent, consensus based process**.

3.2.a IETF rules and procedures

3.2.a.1 Standardization process

IETF Best Current Practice (BCP) 9 called “The Internet Standards Process “ (which consists of RFC2026, RFC5657, RFC6410, RFC7100, RFC7127) specifies the process used by the Internet community for the standardization of protocols and procedures. It defines the stages in the standardization process, the requirements for moving a document between those stages and the types of documents used during this process. BCP78 “Rights Contributors Provide to the IETF Trust” (RFC5378) and BCP79 “Intellectual Property Rights in IETF Technology” (RFC 3979 and RFC5879) address copyright and intellectual property right issues associated with the standards process (see also 3.3.3 below).

IETF publishes the RFC series of documents structured as follows:

Main series	Document status
Standards track	
	Internet Standard (STD)

7 And the related and/or supporting organisations such as the Internet Architecture Board (IAB), the Internet Research Task Force (IRTF), the IETF Administrative Oversight Committee (IAOC), the Internet Engineering Steering Group (IESG), and the RFC Editor.

	Draft Standard
	Proposed Standard
Non-standards track	Informational – Best Current Practice
	Informational
	Experimental
	Historic

The document status Draft Standard has been abandoned by RFC6410 (October 2013) to motivate revisions of the standards specifications that clarify, modify, enhance, or remove features based on implementation and deployment experience.

Any specification that is currently at the abandoned Draft Standard maturity level will retain that classification, absent explicit actions

All standard track documents can be found via http://www.rfc-editor.org/search/standards.php

3.2.a.2 Standards track maturity levels

Specifications become Internet Standards through a set of two maturity levels known as the "Standards Track". These maturity levels are "Proposed Standard" and "Internet Standard".

“Internet Standard” maturity level is attributed to an RFC after confirmation of the following criteria (from RFC6410):

α) There are at least two independent interoperating implementations with widespread deployment and successful operational experience.
β) There are no errata against the specification that would cause an implementation to fail to interoperate with deployed ones.
χ) There are no unused features in the specification that greatly increase implementation complexity.
δ) If the technology required to implement the specification requires patented or otherwise controlled technology, then the set of implementations must demonstrate at least two independent, separate and successful uses of the licensing process.

The IETF Standards Process no longer requires a formal interoperability report, recognizing that deployment and use is sufficient to show interoperability.

"Proposed Standard" is the entry-level maturity for the standards track. A specific action by the IESG is required to move a specification onto the standards track at the "Proposed Standard" level.

Informational RFCs that are published as Best Current Practice (BCP) have a level of review and consensus similar to standard-track documents. These type of RFCs usually document technical operational practices or procedures but are also used for the publication of the IETF procedures.

3.2.a.3 Non-standards track maturity levels

Non-standards track specifications may be published as "Experimental" or "Informational" RFCs.

Their level of review depends on the RFC publication stream (IETF, IAB, IRTF, and independent). With the exception of Informational RFCs that are published as *Best Current Practice:* these informational and experimental RFCs have various levels of review or Internet community consensus. (See section 2 of RFC 5741 for details)

3.2.a.4 Proposed standards and Internet Standards

Proposed Standards are characterized as follows (from BCP9/RFC7127):

The entry-level maturity for the standards track is "Proposed Standard". A specific action by the IESG is required to move a specification onto the standards track at the "Proposed Standard" level.

A Proposed Standard specification is stable, has resolved known design choices, has received significant community review, and appears to enjoy enough community interest to be considered valuable.

Usually, neither implementation nor operational experience is required for the designation of a specification as a Proposed Standard. However, such experience is highly desirable and will usually represent a strong argument in favor of a Proposed Standard designation.

The IESG may require implementation and/or operational experience prior to granting Proposed Standard status to a specification that materially affects the core Internet protocols or that specifies behavior that may have significant operational impact on the Internet.

A Proposed Standard will have no known technical omissions with respect to the requirements placed upon it. Proposed Standards are of such quality that implementations can be deployed in the Internet.

However, as with all technical specifications, Proposed Standards may be revised if problems are found or better solutions are identified, when experiences with deploying implementations of such technologies at scale is gathered.

Internet standards are characterized by (also from BCP9/RFC7127):

A specification for which significant implementation and successful operational experience has been obtained may be elevated to the Internet Standard level. An Internet Standard (which may simply be referred to as a Standard) is characterized by a high degree of technical maturity and by a generally held belief that the specified protocol or service provides significant benefit to the Internet community.

A relatively small number of standard track documents are advanced to the Internet Standard level.

There can be two reasons why a document doesn’t advance in maturity on the standards track:

- The specification has not been submitted by the community for advancing its maturity on the standards track; or
- The advancement of the document has failed to reach consensus on the requirements for maturing (as mentioned in 3.2.a.2, also see RFC6410). Such failure would be documented through the IETF last call process.

FTP, URI and UTF-8 are Internet standards. For HTTPS, HTTP, URL and URN the documents at proposed standard track level have not been submitted for advancing their maturity on the standards track.

3.2.1. Openness

Open: interested parties can join mailing lists (with public archives) without charge and participate in the development of the specification and the development of the consensus. Face to face meetings are organized 3 times per year[8] and allow for remote participation.

3.2.2. Consensus

Consensus: IETF Standards are subject to IETF consensus as judged by the Internet Engineering Steering Group (IESG), a management body consisting of 12 members. The consensus determination includes a 2 or 4 week '*last call*' on the public IETF mailing list. Determination of consensus can be appealed through a well-defined 3 step appeal process (involving the IESG, the Internet Architecture Board –IAB-, and the ISOC Board of Trustees).

3.2.3. Transparency

Transparency: Public archives of the mailing lists are maintained, records of meetings are published in proceedings, and decisions by the IESG are minuted and made available publicly.

3.3 The specification

3.3.1. Maintenance

Updating of a specification is done through the publication of a new set of RFCs.

IETF exists since 1986 and has proven to be a stable organisation, which has been developing and maintaining standards over a long period. The various specifications are maintained in the different relevant working groups part of the IETF structure.

It should be pointed out that no review cycle is imposed on Standards Track documents at any maturity level. Updating of specifications is undertaken upon request from IETF participants.

3.3.2. Availability

8 Sometimes working groups organize interim-meetings.

All IETF specifications are available for free download from http://www.rfc-editor.org/

More specific, by adding the RFC number of the specification concerned in the following string: **http://tools.ietf.org/html/rfcXXXX.txt**

3.3.3. Intellectual Property rules

The IETF intellectual property rights rules are defined in RFC 3979 (http://www.rfc-editor.org/in-notes/rfc3979.txt), "Intellectual Property Rights in IETF Technology" (updated by RFC 4879 (http://www.rfc-editor.org/in-notes/rfc4879.txt), "Clarification of the Third Party Disclosure Procedure in RFC 3979").

The policy with respect to IPR (patents) can be summarized as followed:

> The IETF takes no position regarding the validity or scope of any intellectual property rights or other rights that might be claimed to pertain to the implementation or use of the technology described in any IETF documents or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights.
>
> Contributors to the IETF process are expected to disclose the existence of IPR in technology.
>
> The IETF Executive Director is expected to receive written assurance that a FRAND license (possibly royalty free) will be made available, or that no license will be required. In fact, while there is a preference for royalty-free licensing, the IETF working groups may opt to prefer technology that is known to have FRAND or even no known licensing terms.
>
> The absence of IPR disclosures is not the same thing as the knowledge that there will be no IPR claims in the future. The validity and enforceability of any IPR may be challenged for legitimate reasons, and the mere existence of an IPR disclosure should not automatically be taken to mean that the disclosed IPR is valid or enforceable. In fact IETF Working Groups will take into account on their own opinions of the validity, enforceability or applicability of IPR in their evaluation of alternative technologies.

The IETF's licensing policy is nuanced and in a summary it is not possible to describe in detail those nuances; the reader is advised to carefully read 3979 if there are any concerns.

Participants to the IETF process are being made aware of the IPR policies by means of the so called "NOTE WELL" that is shown at working group meetings, during registration, when subscribing to a mailing list, etc.

http://datatracker.ietf.org/ipr/ relate to the TLS specification needed to implement HTTPS.

RFC5246
http://datatracker.ietf.org/ipr/1154/
http://datatracker.ietf.org/ipr/1153/
http://datatracker.ietf.org/ipr/1004/
http://datatracker.ietf.org/ipr/975/

http://datatracker.ietf.org/ipr/974/

Our assessment is that all these disclosures are accompanied with FRAND licensing terms.

Copyright

In addition to IPR in the technology there is IPR on the 'words', or copyright.

Copyright procedures and copyright holders have changed over time (see http://trustee.ietf.org/docs/IETF-Copyright-FAQ.pdf for a good entry into copyright issues). The procedures describe how Contributors to the IETF process provide license to the IETF.

For recent documents (say 2006 onward) the copyright of RFCs is with the IETF Trust. (A Trust under the laws of the Virginia Commonwealth, the Trust members are IETF officials for details see http://trustee.ietf.org)

For documents written between April 1 1994 and 2006 specific right, and later full copyright, have been with ISOC.

For RFCs published between 1969 and 1994 information on rights and permissions must be sought directly from persons claiming rights therein.

In general everybody is licensed to copy, translate and redistribute RFCs in full. The IETF itself is licensed to copy and modify the contributions but 3rd parties will need to be licensed to develop derivative works. These terms allow the IETF to maintain a specification.

For more detail read RFC 5378 and the Trust Legal Provisions at http://trustee.ietf.org/license-info/

3.3.4. Relevance

Al the assessed specifications facilitate interoperability between public administration, more specific:
- FTP has become a standard network protocol used to transfer computer files from one host to another host, supported by all common web browsers.
e.g. FTP is one of the tools suggested in the EC “Information Providers Guide”:
http://ec.europa.eu/ipg/tools/wcm-portal/documentation/tips_factsheets/ftp/index_en.htm#section_2
- HTTP is the standard protocol used for data communication between web clients and web servers .
- HTTPS has widespread use for protecting page authenticity on all types of websites, securing accounts and keeping user communications, identity and web browsing private.
- URI/URL/URN are necessary to identify a name of a resource that enables interaction with representations of the resource over a network using specific protocols.
- More than half of all Web pages are encoded in UTF-8. IETF requires all Internet protocols to identify the encoding used for character data, and the supported character encodings must include UTF-8. The Internet Mail Consortium (IMC) recommends that all e-mail programs be able to display and create mail using UTF-8. It is also increasingly being used as the default character encoding in operating systems, programming languages, APIs, and software applications.

3.3.5. Neutrality and stability

The specifications can be used independently from specific vendor products. The specifications can be used on any operating system and hardware platform.

3.3.6. Quality

All the specifications are already widely implemented and used.

4 Summary and conclusion

The Evaluation Group has evaluated a cluster of 7 specifications used for setting up websites: File Transfer Protocol (FTP); Hypertext Transfer Protocol (HTTP) 1.1; Hypertext Transfer Protocol Secure (HTTPS); Uniform Resource Identifier (URI); Uniform Resource Locator (URL); Uniform Resource Name (URN) and UCS Transformation Format 8-bit (UTF-8).

Overall, the ICT technical specifications FTP, HTTPS, HTTP, URI, URL, URN and UTF-8 are acknowledged to be stable, accepted by the market and all widely in use. They are so-called common standards and specifications that are used in most IT systems within the government domain as well as other domains.

The Evaluation Group believes that as such, FTP, HTTPS, HTTP, URI, URL, URN and UTF-8 comply with the requirements for the identification of ICT technical specifications, set by Annex II of Regulation (EU) No. 1025/2012.

In particular FTP, HTTPS, HTTP, URI, URL, URN and UTF-8 fulfil the general conditions indicated in the Annex II, i.e., it has market acceptance, and is coherent with standards published by the formal European standardisation organisations. There is no duplication with existing standards or ongoing standardisation activities, and current plans for future standardisation in this sector contemplate harmonizing the available specifications. The proposed ICT specifications are complementary to existing European standards established by CEN, CENELEC and ETSI.

The organisation that develops the specifications, IETF, complies with the attributes referred in the Annex II, i.e., is an open, transparent, non-profit organisation with expertise in developing standards in the field of ICT. Participation to IETF standardisation activities is open to all interested parties. Decisions are based on consensus building within the technical committees. IETF is taking care of maintenance. IETF specifications are freely available for download, and no royalties are charged for the use or implementation of FTP, HTTPS, HTTP, URI, URL, URN and UTF-8. IETF does not impose IPR on its specifications. IETF favours that IPR are provided licence-free or licensed in a FRAND basis.

The IETF standards development process, as documented in RFC 2026 and RFC 6410 , provides various levels of quality assurance. INTERNET STANDARDS are assured to be neutral, stable, interoperable and to have passed formal quality assessment. PROPOSED STANDARDS are assured to be generally stable, to have resolved known design choices, to be believed to be well-understood, to have received significant community review, and to appear to enjoy enough community interest to be considered valuable.

Therefore FTP, HTTPS, HTTP, URI, URL, URN and UTF-8. are suitable for identification.

The Evaluation Group proposes to the Platform to give a positive advice to the identification of FTP, HTTPS, HTTP, URI, URL, URN and UTF-8. by the Commission so that it shall constitute a “common technical specification” in the sense of Article 14 of the Regulation (EU) No. 1025/2012.

Annex 1: Referenced RFCs for a proper implementation

For FTP, RFC0959:

RFC	TITLE
959	File Transfer Protocol
2228	FTP Security Extensions
2640	Internationalization of the File Transfer Protocol
2773	Encryption using KEA and SKIPJACK
3659	Extensions to FTP
7151	File Transfer Protocol HOST Command for Virtual Hosts

For HTTP, RFC2616:

RFC	TITLE
7230	Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing
7231	Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content
7232	Hypertext Transfer Protocol (HTTP/1.1): Conditional Requests
7233	Hypertext Transfer Protocol (HTTP/1.1): Range Requests
7234	Hypertext Transfer Protocol (HTTP/1.1): Caching
7235	Hypertext Transfer Protocol (HTTP/1.1): Authentication

For HTTPS, RFC2817:

RFC	TITLE
2817	Upgrading to TLS Within HTTP/1.1
2246	The TLS Protocol Version 1.0
4346	The Transport Layer Security (TLS) protocol version 1.1
5246	The Transport Layer Security (TLS) protocol version 1.2

7230	Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing
7231	Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content

634

635 For URI, RFC3986:

RFC	**TITLE**
3986	Uniform Resource Identifier (URI): Generic Syntax
6874	Representing IPv6 Zone Identifiers in Address Literals and Uniform Resource Identifiers
7320	URI Design and Ownership
1738	Uniform Resource Locators (URL)

636

637

Annex 1 to the MSP Evaluation Report of IETF website protocols _ information on JSON

When the evaluation of the cluster IETF protocols for websites started, also JavaScript Object Notation (JSON) was part of the evaluation. Several issues arose concerning the coherence between JSON and ECMA-404 and effects on interoperability. End of March ECMA and IETF started to work on synchronization of the two specifications. For this reason The Netherlands, who submitted JSON to the MSP procedure, decided to postpone the submission. Expectation is that in the autumn of 2015 the issues will be solved and the evaluation process can be continued. The results and discussions on JSON so far, are recorded in this Annex.

JSON specific lines in the Evaluation Report 16/04/2015

1.4 Subject of the evaluation

JavaScript Object Notation (JSON) is specified in the Proposed Standard RFC 7159. JSON is an open standard format that uses human-readable text to transmit data objects consisting of attribute value pairs. It is used primarily to transmit data between a server and web application, as an alternative to XML. Although originally derived from the JavaScript scripting language, JSON is a language-independent data format, and code for parsing and generating JSON data is readily available in a large variety of programming languages. JSON is also a formal international data processing standard: ECMA 404[9]. RFC 7159 adds to this specification of the MIME and clarification for interoperability purposes

2.1 Market acceptance

JSON is already widely applied and the most common web browsers support JSON, such as Internet Explorer, Safari, Opera, Firefox and Google. There are no interoperability issues for JSON and other existing European or international standards. JSON is a good alternative to XML, which has already been identified by the European Commission / MSP as a EU technical specification. However, they are not conflicting. The European Commission list indicates that JSON is listed in France.

2.2.1 Coherence

JSON is a good alternative to XML that covers more or less the same area. JSON is often compared to XML[10], but they are not conflicting. Both standards are commonly used. XML is standardized by W3C, which is not a formal European standardization organization. XML has been identified by the European Commission / MSP as an ICT technical specification.

3.3.4 Relevance

JSON is increasingly being used for “Internet of Things” / “Wireless Sensor Network” services, which is part of the Digital Agenda (http://ec.europa.eu/digital-agenda/en/internet-things)

[9] http://www.i-programmer.info/news/167-javascript/6484-json-is-now-an-ecma-standard.html

[10] http://www.json.org/xml.html

675 **Issues discussed on JSON March/ April 2015 by the Evaluation working Group**

676

677

678

Criteria	Comments on compliance to the criteria	Counter arguments
Coherence	SIP defines alternative solutions for existing formal standards, e.g. ITU-T H.323	The coherence principle refers explicit to European standards. H.323 is not an European standard but an international standard There are many implementations of SIP, implementations that do not hamper interoperability in a domain where EU standards have not gained market accepetance.
Market Acceptance	Neither SIP nor H.323 are modern techniques,	Lifetime of a specification is not relevant in the procedure. Nor are upcoming new specifications, especially when the exact functionality differs. The MSP procedure also provides the option to withdraw an identification later on, when circumstances have changed.
Market Acceptance	Web RTC might take over	WEBRTC is does not cover the exact same area, it is a technology to tunnel RTP traffic to a browser platform. The signaling technology is not part of that stack and in fact SIP may be used for the signaling methodology. (http://www.html5rocks.com/en/tutorials/webrtc/basics/#toc-signaling)
Market Acceptance.	The SIP specifications do not meet the following requirement in Annex 2/item 1: "Market acceptance can be demonstrated by operational examples of compliant implementations from different vendors"	' carriers such as BT, Verizon, Colt and KPN either use SIP (the old C7, but never H323). SIP trunking is dominant. The entire US phone system is an example of interoperable SIP'. 'Sip is 'over-deployed' already for many years in the Netherlands and beyond … there are thousands of different SIP implementations from hundreds of vendors worldwide' 'Interoperable SIP-trunking between different vendor equipment happens on nearly every long distance call by a major SP, or cable company, Skype to or from the pstn, and all WebEx calls'

Inter-operability	SIP is a generic protocol (like a toolbox), and vendors/service providers implement call set up procedures in proprietary ways, even though they follow the SIP specification. As a result, although SIP is used in many different implementations, they do not interoperate (by design). As a result, consumers purchasing e.g. a SIP phone may be misled to believe it will work with any given SIP voice provider. Listing it could mislead procurement agents in believing that a reference to SIP itself would provide guarantees of interoperability; this confusion should be avoided.	‘‘Sip as protocol certainly meets any interoperability criteria … saying that SIP is not interoperable because some end-points do not implement properly or are badly configured … is not a relevant or accurate observation’. ‘Every major commercial pbx supports sip trunk to Cisco equipment. The major pbx vendors (Cisco, Polycom, Microsoft,Avaya, Shoretel etc.) have all interoperable sip trunks between them’. ‘Initiatives like SIPit and SIPConnect contribute highly to vendor interoperability’.
Inter-operability	In practice nothing bad happens with a “not identification”. These standards are old standards (as said close to 20 years old) and in reality the industry and the operators know very well for many years how to deal with the existing incompatibilities. However, interoperability for SIP is a reasonable goal / expectation **only** when one speaks of specific profiles where SIP is used, for example in 3GPP IMS, where the SIP specifications are normatively referenced. This interoperability is to be expected *within* the same type of system by different vendors, and to be encouraged with *other systems* providing the same functionality that co-exist with them, e.g. "de jure" ITU-T H.323	We must regard the goal of the identification process: the identification of ICT technical specifications that could be referenced in public procurement. Identification of the RFC will still be necessary for procurers. If profiles are needed to attain interoperability, the identification of the specifications on which the profiles are based is needed. For procurement purposes that is necessary but not sufficient. Since 3GGP IMS is a profile that is used in a very specific use case and for applications like SIP trunking other non formal SDO endorsed profiles are used (mainly SIPConnect).

679
680

681