Public Review: Resolution of Comments on Draft ETSI EN 319 422 V0.0.3 (2013-09) – 31 May 2014

Electronic Signatures and Infrastructures (ESI); Time stamping profile

Foreword: Please note that the following disposition of comments is provided to the light of the current context of the m460 mandate, in particular with regards to Directive 1999/93/EC. It should be noted that such disposition should be reviewed to the light of the eIDAS Regulation.

Clause/ Subclause	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change**	**Resolution** on each comment submitted
		General	All comments are important. However, this general comments highlights the most important comments which are marked in yellow below: [1] A TSA may have more than one TSU. There is a confusion between TSA and TSU in several places. [2] The response shall include at least the appropriate TSU certificate, otherwise the verification will be impossible since TSU certificates are usually not published. Therefore, the mandatory incorporation of the TSU certificate in the response should be mentioned. [3] One store and forward protocol is currently mandatory. Only the on-line protocol through HTTP or/and HTTPS should be supported.		See specific comment

Section 4.2.1		Technical	The text states: 4.2.1 Parameters to be supported The following requirement applies: no extension field shall be present. It does not make any harm to include any other non critical extension, since it may be ignored if it is not supported by the server.	Proposed replacement: 4.2.1 Parameters to be supported The following requirement applies: no critical extension field shall be present.	Agree
Section 4.3.1		Technical	The text states: NOTE: A TSA may not support ordering hence clients should not depend on the ordering of time-stamps. A TSA may have more than one TSU. In this specific case, it the a TSU instead of a TSA.[1] Change TSA into TSU.	Proposed replacement: NOTE: A TSU may not support ordering hence clients should not depend on the ordering of time-stamps.	Agree

Section 5.2.1		Technical	The current text focussed only on the parameters of the TSTInfo structure. It should be remembered that a TimeStampToken is contained in a CMS structure which encapsulates a signed data content type. RFC 2630 defines SignedData as: SignedData ::= SEQUENCE { version CMSVersion, digestAlgorithms DigestAlgorithmIdentifiers, encapContentInfo EncapsulatedContentInfo, certificates [0] IMPLICIT CertificateSet OPTIONAL, crls [1] IMPLICIT CertificateRevocationLists OPTIONAL, signerInfos SignerInfos } while "certificates is a collection of certificates. It is intended that the set of certificates be sufficient to contain chains from a recognized "root" or "top-level certification authority" to all of the signers in the signerInfos field. There may be more certificates than necessary, and there may be certificates sufficient to contain chains from two or more independent top-level certification authorities. There may also be fewer certificates than necessary, if it is expected that recipients have an alternate means of obtaining necessary certificates (e.g., from a previous set of certificates)". It is necessary to obtain the TSU certificate that will be used to verify the signature of the CMS structure. The response shall include at least the appropriate TSU certificate, otherwise the verification will be impossible since TSU certificates are usually not published. Therefore, the mandatory incorporation of the TSU certificate in the response should be mentioned.	Proposed replacement: 5.2.1 Parameters to be supported The following requirements apply to the content of the TSTInfo structure: • a genTime parameter limited to represent time with one second is required; • a minimum accuracy of one second is required; • an ordering parameter missing or set to false is required; • no extension is required to be generated; • no extension shall be marked critical. The following requirement applies to the content of the SignedData structure in which the TSTInfo structure is encapsulated: • the certificates parameter shall contain the TSU certificate which allows to verify the signature included in the signerInfos parameter.	Agree add The following requirement applies to the content of the SignedData structure in which the TSTInfo structure is encapsulated: • the certificates parameter shall contain the TSU certificate which allows to verify the signature included in the signerInfos parameter.

Section 5.2.2		Technical	It would be appropriate to recommend in a note the inclusion of the organizationIdentifier attribute.	Add a Note: Note: It is recommended to use an organizationIdentifier attribute.	Agree
Section 5.2.5		Technical	A TSU has a certificate, a TSA has no certificate since it can handle several TSUs.	Change: "5.2.5 TSA Certificates " into: "5.2.5 TSU Certificates"	Agree
Section 5.2.5		Technical	A TSU has a certificate, a TSA has no certificate since it can handle several TSUs.	Change: "It is recommended that certificates issued for TSA are as specified ..." into "It is recommended that certificates issued for TSU are as specified ..."	Agree
Section 5.2.5		Technical	The text is as follows: "5.2.5 TSA Certificates It is recommended that certificates issued for TSA are as specified in clauses A.9 and A.10 of TS 102 176-1 [5]". Clauses A.9 from TS 102 176-1 is called "TSU Certificates" rather than "TSA Certificates". The tile is ambiguous. the following title is more explicit: 5.2.5 Algorithms related to TSU Certificates The reference TS 102 176-1 is no more valid. The latest reference is : TR 119 312 V0.0.2 (2013-09)	Proposed change: "5.2.5 Algorithms related to TSU Certificates It is recommended that certificates issued for TSU certificates and for self-signed certificates for CAs issuing TSU certificates are as specified respectively in clauses A.9 and A.10 of TR 119 312 [5]". The reference [5] should be updated.	.Partially agree. Will reference new TS 119 312. Root CA certificate outside scope

Section 5.2.6		Technical	The text is as follows: 5.2.6 TSA Certificate Identifier The TSA certificate identifier must be present in the TSA signature as specified in RFC 3161 [1] (ESSCertID) or RFC 5816 [4] (ESSCertID or ESSCerIDv2). This text is misplaced since ESSCertID or ESSCerIDv2 are part of the parameters of the response. This section should be removed and the text should be moved with modifications into section 5.2.1.	An earlier proposed replacement was written as follows: "The following requirement applies to the content of the SignedData structure in which the TSTInfo structure is encapsulated: • the certificates parameter shall contain the TSU certificate which allows to verify the signature included in the signerInfos parameter." It is proposed to add after it : •the certificate identifier of the TSU certificate (ESSCertID as in RFC 3161 [1] or ESSCerIDv2 as in RFC 5816 [4]) MUST be included as a signerInfo attribute inside a SigningCertificate attribute.	Agree This is more precise
Section 6		Technical	The text is as follows: "6 Profiles for the transport protocols to be supported One on-line protocol and one store and forward protocol **must** be supported for every Time Stamping Authority (TSA). Among the four protocols that are defined in the RFC 3161 [1], the following protocol **should** be supported: • the Time Stamp Protocol via HTTP (section 3.4 from the RFC 3161 [1])." HTTP is an on-line protocol and not a store and forward protocol. Only the on-line protocol through HTTP or/and HTTPS should be supported [3]. The use of "must" and "should" above is not consistent.	Proposed change: "6 Profiles for the transport protocols to be supported One on-line protocol **must** be supported for every Time Stamping Unit (TSU). Among the four protocols that are defined in section 3 of RFC 3161 [1], the following on-line protocol **shall** be supported: • the Time Stamp Protocol via HTTP (section 3.4 from the RFC 3161 [1])."	Agree remove requirement for store and forward. HTTP or HTTPS shall be supported. Not recommend one over the other.

Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	OBSERVATIONS on each comment submitted
Intro.	**1**	**E**	**It is stated that "… electronic signatures *must* be time stamped during the life time of the … certificate".**	**Change *must* to *should*. In this context, "time stamped" will be understood as time stamping according to this document. There are other ways of capturing time, e.g. trusted archival, without this kind of time stamping.**	Agree Replace: To this respect, electronic signatures must be time stamped during the life time of the corresponding certificate. With: One method of assuring the signing time is to affix a digitally signed time-stamp bound to the signature as define RFC 3161.
2.2	**[i.2]**	**G**	**Is the reference to the old version needed? The referenced document will be outdated.**	**Delete reference – and delete reference from last sentence of Foreword.**	Disagree Practice for all ESI documents moving to EN.

5.2.2	**2**	**T**	**Structure of name for issuing TSP server should be same as for a CA, ref. draft EN 319 412-2, paragraph 5.2.4.1. Only legal person issuers should be allowed.**	**The issuer must be a legal person. The name of the issuer shall contain at least the following attributes:** **• countryName,** **• organizationName,** **• organizationIdentifier** **• commonName** **Additional attributes may be present.** **The countryName attribute shall specify the country in which the TSA is established.** **The organizationName attribute shall contain the full registered name of the TSA organization.** **Note: The organizationIdentifier attribute was added to X.520 in a technical corrigendum [16] having the object identifier 2.5.4.97 (id-at-organizationIdentifier OBJECT IDENTIFIER ::= {id-at 97}), defined as "An attribute of type organizationIdentifier holds an identification of an organization different from the organization name". See EN 319 412-1 [17] section 5 for further guidance on semantics for the organizationIdentifier attribute.** **Then add the two references X.520 corrigendum and EN 319 412-1 to normative references.**	**The subject identifier be a natural or legal persons as specified in 319 412-2 or 319 412-3 respecyively**
5.2.4	**1**	**T**	**Requirement for key length is too weak.**	**The key length for the selected signature algorithm** *shall* **be equal to or higher than the recommended value in clause 9.3 of TS 102 176-1.**	Disagree This should reference new TS 119 312. This is a recommendation This is not too weak. If necessary TS 119 312 should recommend minimums. If there is weaknesses in the advise given in 119 312 then this needs to be changed.

5.2.5	**1**	**T**	**Requirements for TSA certificates are too weak.**	**Reference to TS 102 176-1 only covers crypto only, and is only “recommended”.** **Certificates for CAs issuing TSA certificates should be specified as other CA certificates. There should be an indication that the CA issues TSA certificates (how?)** **Certificate for a TSA should refer to certificate profile for legal person (EN 319 412-3). There should be an indication in the subject name that this is a TSA (how?)**	See above
6	**1**	**T**	**Profiles for transport protocols should be explicit.**	**Select preferably one on-line protocol and one store and forward protocol to use. At present only one on-line protocol is specified as** *should* **be supported.**	**See comment from DP**
Annex B	**All**	**E**	**Delete Annex in final version.**	**Delete Annex in final version.**	**Delete all but directive**

Clause/ Subclause	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change**	**OBSERVATIONS** on each comment submitted
6		**Technical** **l**	**"One on-line protocol and one store and forward protocol must be supported for every Time Stamping Authority (TSA). Among the four protocols that are defined in the RFC 3161 [1], the following protocol should be supported:** **• the Time Stamp Protocol via HTTP (section 3.4 from the RFC 3161 [1])."** **Store and forward protocols are not really used and it is strange to oblige a TSA to support not only an on-line protocol, but also a store and forward protocol.** **In addition, the use of HTTP might even be made a "shall" since HTTP and HTTPS is really widely deployed.**	**for example the following text:** **Every Time Stamping Authority (TSA) shall support the following protocol:** **the Time Stamp Protocol via HTTP (section 3.4 from the RFC 3161 [1])** **It is recommended that the TSA supports HTTPS (<corresponding ref>).**	**Require HTTP or HTTPS** **Depending on policy may require to use HTTPS.**

whole document	**General**	**In some places TSA is used instead of TSU, for example the time-stamping certificates belongs to the TSU and not to the TSA**	**use TSU certificate instead of TSA certificate**	**Agree**

Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	OBSERVATIONS on each comment submitted
Informative reference	**2.2**	**Technical**	ETSI TS 101 861 is referenced here whereas TS 319 422 is supposed to be the new standard replacing ETSI TS 101 861. What is the point of referencing the old standard in the new one?	Obsolete standard ETSI TS 101 861 should not be referenced.	ESI practice to help know equivalence
Abbreviations	**3.3**	**Technical**	Typo : this section .3.3 should be 3.2		Agree Similar problem with clause 4.2.1 & 4.3

Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	OBSERVATIONS on each comment submitted
			Suggest title should be **Time stamping protocol and token**		**Agree**