Public Review: resolution of public comments on Draft ETSI EN 319 411-1 V0.0.10 (2015-01)

Electronic Signatures and Infrastructures (ESI);

Policy and security requirements for Trust Service Providers issuing certificates;

Part 1: General requirements

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted
a	7.3.6 a)		General	The wording of the subclause is too complicated. The meaning of the requirement is unclear and invokes speculations about what is actualy required.	Simplify subclause text.	OK. I´d change the ".. limited to that compatible.." for "compatible" And also ".. in the generating .." for ".. for generating .."
a	7.5.11 i)		General/Editorial	7.5.11 i) seems to duplicate 7.5.11 a)	Delete 7.5.11 i)	Agreed. Delete i)
B	2	2.1	General	The requirements of this document should be aligned with the RFC 3647 template to enable TSPs to ensure full compliance and to facilitate trust mapping across TSPs.	Include the RFC Clause/Subclause/Paragraph number in parentheses next to each Clause/Subclause/Paragraph in this document. Where this document introduces new requirements that do not appear in RFC 3647, note that fact as well. At the very least each Clause and Subclause should display the relevant RFC 3647 Clause/Subclause number.	Agreed Document to be aligned with RFC 3647
C			General	The standard only states general requirements to TSPs issuing certificates and do not distinguish between issuing CAs and root CAs.	The standard should distinguish between issuing CAs and root CAs and or the 319 411-x serie should be extended with regards general requirements for root CAs.	Rejected. This document is to review the whole TSP operational processes. Where appropriate requirements specific to

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted
						root CAs are already included.
C	**4.5**	**“c) To request a certificate for a device or system …”**	**Technical**	**The sentence on page 14 “The subject can be: […] d) a device or system operated by on on behalf of a natural person or legal person” refers to both a natural person and a legal person whereas the paragraph only refers to subcribers as legal persons.**	**Inclusion of a paragraph iii. under c) with subscriber being a natural person.**	**Agreed. Updated accordingly.**
C	**6.2**	**“following compromise, the use of the subject's private key is immediately and permanently discontinued;”**	**Technical**	**In keyUsage profile D and F in ETSI 319 412-2 clause 5.4.3. keys can be used for Key Encipherment and Key Agreement (Bit 2 or 4).**	**Subjects should still have the opportunity to decrypt data using a compromised private key if the keyUsage profile D or F is used.** **The phrase “except for key decipherment” should added.**	**Agreed.**
C	**7.2**	**c)**	**Technical**	**It is required that “The TSP shall publicly disclose its Certification Practice Statement …”** **The CSP may include both public and confidential information. E.g. Disaster Recovery Plans and Business Continuity Plans.**	**Proposed change: “The TSP shall publicly disclose the public part of its Certification Practice Statement …”**	**Agreed with changes: Reword for not including sensitive information** **The TSP is not obliged to disclose any aspects that express sensitive information in its CPS** **Note added.**

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted
C	**7.3.8**		**General**	**This clause addresses centrally generated keys deployed in a cryptographic device distributed to the subject.**	**There should be similar explicit requirements to setups where subjects keys are stored and used centrally which should be possible according to [i.16] Annex II litra 3 and 4**	**Reworded**
C	**7.4.6**	**g)**	**Technical**	**The paragraph require at least daily publication. This may be impractical and unnecessary for root certification authorities if the root CA system is located in an air-gapped extra secured environment. It may even introduce a higher risk.**	**The requirement should only apply to issuing CAs.** **Root CAs should be allowed longer CRL publication cycles.**	**Agree with changes. Clarify that 7.4.6 g applies to end user certificates.** **CA revocation lists covered in 7.4.6 i)**
C	**7.6**	**a)**	**General**	**There might be issue setting up controls for “staff [being] free from any commercial, financial and other pressures which might adversely influence trust” due to employees economical privacy unless a signed employee statement is enough.**		**Agree added** NOTE: The TSP may need to take into account privacy requirements.
C	**7.7.1**		**General**	**Production CAs should not issue test certificates.**	**A note stating that “Test certificates shall not be issued by production CA” should be added to the clause.**	**Agree with changes: Test certificates may need to be issued by production but they should be clearly indicated as such.**
D			**General**	**Requirements and options for SSL-certificates make this**	**Describe all specific requirements for SSL-certificates in a separate document and only describe the**	**The scope of the document is for general requirements for certificates, including**

Organization name	**Clause/ Subclause**	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change**	**RESOLUTION** on each comment submitted
				document incomprehensible for the use for other certificates like qualified certificates.	**general requirements for certificates in 319411-1.**	**SSL** **Rejected – restructuring the document is considered to add more complexities**
E	**7.4.6 Certificate revocation and suspension**	**Revocation status - letter n)**	**Technical**	**Letter n) in the part of Revocation status requires consistency of information about status of certificates in case that a TSP supports a multiple methods for providing revocation status. For eIDAS's stakeholders (mainly QTSP, supervisory bodies and conformity assessment bodies) would be very helpful to include examples how to fulfil the requirement of consistency of information.** **The requirement is of course a logical, but solution of it is not a trivial question.**	**Please add to the annex of norm examples, how TSP can fulfil the requirement of consistency of information about certificate's revocation status, OR modify the text of the letter n) to clarify the consistency requirements.**	**This document is not aimed to providing guidance on technical solutions, is about indicating policy requirements. It´s up to the CA to provide that consistency.**
F	**7.5.9**	**b**	**Technical**	**It is necessary to have more detailed requirements regarding handling of revocation status for unexpired certificates. In particular, how new TSP should handle revocation status for unexpired certificates**	**More detailed procedures or at least example/note would be very much appreciated. Clear and unified requirements would make this process more similar and allow avoiding possible trust problems when validating such certificates.**	**To be addressed as part of future work plan.**

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted
				and provide revocation status information (OSCP responses/CRLs) to relaying parties after transfer of obligations (i.e. whose keys should be used to sign CRLs and OCSP responses and how to avoid trust problems).		
G	7.4.6 a) vii)		Technical	It is required to document "the maximum delay between the confirmation of the revocation of a certificate to become effective and the actual change of the revocation status information of this certificate being made available to relying parties", but it is not clear whether the requirement applies to certificate suspensions as well, or not, because in other clauses suspensions are discussed separately from revocations (e.g. in iv)).	Since the relying parties must be aware of certificate suspensions as well, the proposal is to include them explicitly in the requirement: "the maximum delay between the confirmation of the revocation of a certificate, or its suspension, to become effective and (…)".	Agreed proposed change and included in some other bullets
G	7.4.6 f)		Technical	If a suspended certificate becomes valid again (i.e. if the revocation is not confirmed), it is not clear whether the period of time it was suspended should be taken into account (e.g. when	The proposal is to specify: "Once a suspended certificate becomes valid again, it is reinstated so that the period of time it remained suspended need not to be taken into account".	This issue is related to signature validation not a certificate policy. Rejected

Organization name	**Clause/ Subclause**	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change**	**RESOLUTION** on each comment submitted
				validating signatures created after the suspension), or not.		
G	**7.4.6 m)**		**Technical**	**It is not clear whether OCSP shall be supported and follow the requirements of RFC 6960, or it shall follow the requirements of RFC 6960 in case it is supported (i.e. whether the OCSP is mandatory or not).**	**The proposal is to clarify: "OCSP shall be supported, and shall follow the requirements of RFC 6960 [12], meanwhile CRL may be supported, and it shall follow the ITU-T Recommendation X.509 [7]".**	**Agreed.**
G	**7.4.6**		**Technical**	**The accuracy of revocation time included in the revocation status information distributed via OCSP and/or CRL, as well as the accuracy of other time values included in OCSP responses or CRLs, is not clear.** **Without knowing the accuracy of the clock the TSP operates it is impossible to make reliable conclusions based on the revocation status information obtained.**	**At a minimum, the TSP shall be required to document the maximum drift from UTC of all the times included in the revocation status information, with the maximum limit set (for example, to 1 second). This can be done by adding a new requirement in 7.4.6 a).** **Another option is to add a more general requirement for the maximum drift of TSP's clock from UTC, as the requirement is relevant for other operations, namely, the certificate generation (the "not before" and "not after" dates included in a certificate), as well.**	**Agreed. Added proposal on 7.4.6 a) and included UTC in definitions.**
H	**4.2**	**4th**	**Editorial**	**"Where a TSP includes a hierarchy of subordinate CAs up to a root CA the TSP is responsible for**	**"subordinate-CA complies" or "subordinate-CAs comply"**	**Agree.**

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted
				ensuring the subordinate-CAs complies with the applicable policy requirements” ➔ CAs = plural & complies = singular		
H	7.3.6	c)	General	Unclear what is meant here, an example could help		Agreed. Refer to X.509 for the definition of the key usages
H	7.3.8	e)	Editorial	First sentence is not complete, starts with “If a copy …” but ends with a full stop without explaining what if.		Agreed. Removed sentence
H	7.4.3	f)	General	No definition of “entity” in document. For certificate issued to legal person, is the legal person the “entity” and can a new certificate on the same DN be issued to that entity? What if the legal person structure changed, e.g. through merger/acquisition?		Rejected, this is a legal issue and is not in scope of this document
H	7.4.3	k)	Technical	For certificates issued to legal persons, is it correct that the subject identifier must indicate the natural person?		Agreed. Modified in document adding a conditional

Organization name	**Clause/ Subclause**	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change**	**RESOLUTION** on each comment submitted
I	**7.2 d**		**G**	**Why not to structure CPS according to relevant ETSI standards (319 411-1) structure? It would be easier to follow and align practices with requirements. Also in the case if Trust Service Provider provides different trust services, it would be possible to build up similarly with ETSI standards (concerning trust service provision) hierarchy of practice statements with more or less coherent structure and cross-references. The part “TSP management and operation” will be in case of different trust services in the great extent the same.**	**The structure of CPS could follow the structure of ETSI EN 319 411-1.**	**Rejected. The RFC is more widely accepted and valid for CPS and CP.**
I	**7.5**		**G**		**Clause 7.5 Trust Service Provider management and operation could be structured and aligned according to ETSI EN 319 401 clause 7 (same content), which has intuitively better structure (excluding cryptographic controls, which have a better structure and place in this standard). Would be easier to follow and align requirements. Business continuity and incident handling clause could be in separate clauses like in respective parts of ETSI EN 319**	**It is considered more appropriate to follow the RFC 3647 structure.**

Organization name	**Clause/ Subclause**	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change**	**RESOLUTION** on each comment submitted
					401.	