Public Review: resolution of Comments on Draft ETSI EN 319 411-1 V0.0.4 (2013-11) – 31 May 2014

Policy and security requirements for Trust Service Providers issuing certificates; Part 1: Policy requirements for Certification Authorities issuing web site certificates

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	The term CA, present in the previous standard (TS 102 042) has been replaced with TSP which is a much vaguer term. CA should have been preserved for a better understanding.		In clause 3.2 is indicated that the more general term TSP is used in preference over CSP but the term CA is also used in the whole document. Also is indicated in 4.2 the way the different terminology is used. The term CA is used in clauses 4, 5 and 6. And in clauses and subclauses 7 has been used somewhere and not in all texts, only in 7.1 and 7.3.1 mentions TSP. In the mother document, the 319 401 the term TSP is the one used.
Subscriber and subject	4.5	Editorial	"In the present document to clarify the requirements which are applicable to the two different roles that may occur two different terms are used for the "subscriber" who contracts with the Certification Authority for the issuance of certificates and the "subject" to whom the certificate applies. "	In the present document, in order to clarify the requirements, we use two different terms for the role who contracts with the Certification Authority for the issuance of certificates and the role to whom the certificate applies. "Subscriber" is used for the role contracts with the CA and "Subject" applies to the role to whom the certificate is intended.	Agreed.

Overview	**5.1**	**Technical**	**“The CA shall develop, implement, enforce, and annually update a Certificate Policy and/or Certification Practice Statement that describes in detail how the CA implements the latest version of these Requirements.”** **This text suggests that can choose between a certificate Policy and a certificate Practice Statement.** **Furthermore, in section 7.1, the obligation to have a CPS has been removed from the standard.** **Could you confirm that the CPS has become optional?**		**This text is copied from the CAB Forum documents as it is, it can not be changed.** **Regarding 7.1 there´s no such indication. It is not optional. And checking the 401 there´s no such distinction.** **Anyway, that made me realize that this 7.1 title has to be change to a trust service practice statement and not using the certification term in this particular case. Will review the whole document.**
Certification Authority obligations and warranties	**6.1**	**Editorial**	**The CA warrants that has complied with the BRG [15] section 7.** **Typo identified**	**The CA warrants that <u>it</u> has complied with the BRG [15] section 7.**	**Agreed but not sure it´s a real typo.**
Certification Authority obligations and warranties	**6.1**	**Technical**	**How does the CA warrants that it has complied with the BRG?**		**By following the indications on the Baseline Requirements document in its section 7, which means, that you have complied with some requirements and these have been checked regularly**
Subject registration	**7.3.1**	**Technical**	**"The CA shall retain all documentation for at least seven years after any certificate based on that documentation ceases to be valid."** **What is the rationale behind the seven years?** **What happen if the registration documentation I kept 5 years instead of 7?**		**Because it´s indicated in the CABF documents, in the Baseline Requirements in section 15.3.2.** **If you don´t keep the information for 7 years you won´t pass the audit need for issuing baseline SSL certs.**

ETSI document	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	OBSERVATIONS on each comment submitted
411-1 **411-2** **411-3**	**2.2** **7.4.8**	**Item [i-7]** **Note 1**	**T** **E**	ISO/IEC 27002 was updated in 2012. Please check if changes may affect this document, e.g. in clause numbering reference.		Check out new ISO 27002:2012 provided by Nick
411-1 **411-2** **411-3**	**3.1**	**Definitions**	**T**	It would be correct to specify this definition comes from ISO/IEC 9594-8 or, if you prefer, ITU-T Recommendation X.509.		Yes, it´s true but this ways allows us to make changes than referring to a current spec. Check out ISO/IEC 9594-8 or ITU-T X.509 and refer accordingly
411-1 **411-2** **411-3**	**4.3**	**5th bulleted item**	**T**	"real time service" If this addressees OCSP, the term "real time" may be not correct, as explained few words later.	Please replace with "online service", thus recalling the meaning of "O" in OCSP.	Agreed, but online also can have multiple deviations. Check out the indication that OCSP is mandatory and CRL optional
411-1 **411-2** **411-3**	**7.2.1**	**Item f)**	**T**	Root key ceremony		See note on root key ceremony
411-1 **411-2** **411-3**	**7.2.1**	**Item g)**	**E**	Sub CA key ceremony		See note on root key ceremony
411-1 **411-2** **411-3**	**7.3.6**	**General**		ARLs		See note on ARLs generation

411-1	**7.3.6**	**Item e)**	**E**		"published at ***least*** every 24 hours." "published at ***most*** every 24 hours."	Partially agree. To be aligned with CABF and the new Regulation, "within 24 hours" should be used.
411-1 **411-2**	**7.3.6** **7.4.1**	**Item f) ii)**	**T**	"a new CRL may be published before the stated time of the next CRL issue;" Since CRLs are generally cached this practice is not to be recommended, especially if the interval between two CRLs is longer than 3 - 4 hours. When caching CRLs, a CRL issued much earlier than expected can create great disasters.	Please replace with: "ii) a new CRL **may** be published **shortly** before the stated time of the next CRL issue. NOTE: by "shortly" it is intended few minutes, to let the CA handle allow small inconveniences at CRL issue time."	**Rejected.** One shall not prevent a CA to issue a CRL at any time (e.g. after a new revocation). Modifying this requirement (present in 101 456 since many years) will impact existing CAs too much. In addition, trusting / caching a CRL is a matter of Relying Party policy. Agree – the policy states maximum's how a TSP implements this policy requirement is outside scope
411-1	**7.4.4**	**Item b)**	**T**	A Note here would be helpful to clarify that even authorized persons should not be left alone in these premises, lest readers may infer this requirement applies only to non-authorized persons		See Nick´s note "Every entry to the physically secure area shall be subject to independent oversight and non-authorised person shall be accompanied by an authorised person whilst in the secure area. Every entry and exit shall be logged."
411-1 **411-2** **411-3**	**7.4.6**	**Item a)**	**T**	"kept in a physically secure environment" This conflicts with Note 3 that mentions "intrusion detection system,"	"kept in a physically ***and logically*** secure environment"	Agreed.
411-1 **411-2** **411-3**	**7.4.8**	**Item a)**	**T**	"stored in safe places"	Please add ", preferably also remote ,"	Agreed

411-1 **411-2** **411-3**	**7.4.11**		**G**	It would be useful to inform the reader that provisions on how to preserve digital data objects are given in ETSI TS 101 533.		Include as informative note
411-1 **411-2**	**7.4.12**		**E**	"The requirements identified in EN 319 401 [10], clause 6.4.12 shall apply."	This clause does not exist in the currently available EN 319 401	It already exists
411-1 **411-2** **411-3**	**8.3**	**Item b)**	**E**	This item b) is ill placed in this list. Remove it from this list and make it an independent paragraph, preferably at the end of this clause.		Reject
411-1 **411-2** **411-3**	**Annex Bibliography**			Why listing withdrawn docs?		Remove all withdrawn docs