Public Review: Resolution of Comments on Draft ETSI EN 319 411-4 v 0.0.2 – 31 May 2014

Trust Service Providers issuing certificates; Part 4: Policy requirements for certification authorities issuing Attribute 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
Title		GE	The current title is "Policy requirements for certification authorities issuing Attribute Certificates" but Attribute Certificates are issued by Attribute Authorities	Policy requirements for Attribute Authorities issuing Attribute Certificates	Accepted
2.2	First note	ED	There is a typo: EN 119 403 should be EN 319 403	Change to "NOTE: TS 119 403 will be replaced by EN 319 403"	Accepted
Annex A		TE	An Attribute Certificate, according to ISO/IEC 9594-8/ITU-T Recommendation X.509 (and also RFC 5755 An Internet Attribute Certificate Profile for Authorization) is not necessarily linked to a PKC	Change as follow: c) specific attributes of the subject ~~as identified in the Certificate~~ to which the AC is linked; d) an unambiguous link to a subject ~~Certificate~~;	Accepted (already discussed at ESI#42)
All		TE	It is premature to go directly to the EN status for this document. The concept of "Attribute certificate" can be used wuth other standarization activities such as eDelivery and eID frameworks	It is suggested to target a TS status to allow more flexibility and simplify its integration in different contexts	Accepted (already discussed at ESI#42; technical justification needed for the change)
Annex A		TE	The Annex A addresses	Create a (set of) TS addressing AC semantic definition/syntax profiles	Added a note on ANNEX A that its content will be moved to another deliverable

General	-	General	The market in attribute certification is still young, and it is not yet clear what direction that market will take. In particular, it will be interesting to see how the draft eIDAS Regulation impacts developments in the field. The draft Regulation may be significant not only insofar as it relates to electronic signatures but also in what it says about mutual recognition of electronic identification between Member States. Whilst the draft EN is written in the context of electronic signatures, the development of an EN on attributes would have an impact on any future work that might be done on attributes in relation to identity assurance or in other contexts. Given that attribute certificates still have a way to go before their use is widespread, and in light of the work being done in a large number of European countries to develop solutions on electronic identity, the interplay between the two and the way that attribute certificates in relation to electronic signatures might relate to any attribute certificates related to electronic identification remains unclear at present. Were this document to be turned into an EN, further consideration would be needed about the extent to which it is useful to have an EN on attribute certificates that applies only in the context of electronic signatures. For these reasons, until there is more maturity in the market on attribute provision and more certainty around the technical specifications required here, we feel that it is appropriate for this document to retain the flexibility of a TS rather than turning it into an EN at this stage	Publish specification as a Technical Specification rather than a European Standard (EN)	Accepted (already discussed at ESI#42; technical justification needed for the change)
General		G	There are some misalignments between this prEN and other prENs of the 319 411 family. Please double check and fix them Note: obviously the identified misalignments refer to provisions that are applicable to the present prEN.		accepted
General		E	There are many bulleted items list that should be numbered items lists for a better reference		accepted
Contents		E	Please check the page numbering here.		accepted
2.2	Item [i.6]	E/T	In 2012 a new version was issued of ISO/IEC 27002		accepted

2.2	Item [i.12]	E/T	ETSI TS 102 176-1 is being replaced with TS 119 312		accepted
3.1		E	If alphabetic order is to be abided by, please swap “attribute certification period” and “Attribute Certification Disclosure Statement (ACDS)”		accepted
3.1	Definition of CPS	T/E	This term "CPS" was defined in ISO/IEC 9594-8, so it is not permissible to modify it in such a way.	New proposed text: "A statement of the practices that a Certification Authority employs in issuing certificates [5]. In the case of an Attribute Authority it describes the practices it employs in issuing Attribute Certificates."	Definition deleted as Attribute Certification Practice Statement (ACPS):is used for this purpose
4.3	1st para	T/E	This para repeats words of the AA definition, to no avail. Additionally, there is a “ “ missing		Accepted, sentence deleted
4.4	Fig. 1	E	Figure 1 is missing		Accepted
4.6	Bullets related to subjects	E	Please align singular / plural		accepted
4.6		T	To prevent misunderstandings a Note would be useful, specifying that AGAs are not always subscribers. For example in the case where an AGA is a University issuing degrees that subjects can exhibit at the AA to be published an AC.		Not accepted. In the example given the AGA is acting outside the scope of the document and it is up to the AA to decide how to act (according to applicable policies/laws)
4.7	Note	E	1) “Itis in this way” ➔ “It is in this way 2) Given the X.509 size it would be helpful to specify also the X.509 clause/s where these standard attributes are defined		accepted
5.1	1st and 2nd para	E	Having the ACP been defined in clause 3.1 what is the reason to repeat it here?		Accepted, sentence deleted
5.2	Editor’s note	T	It is doubtful that such policy is necessary		Accepted. Being now the document a TS it can be updated more easily in case a new policy is needed (e.g. for eID)

5.3		T	“under *this* policy” Which policy? The one to be defined, the usefulness of which in the previous comment was defined as "doubtful"? Why only QES as per Art. 5(1) are to be addressed here? All in all: this clause seems either pleonastic or lacunose. Please review.		Accepted. Now a reference to policy specified in 5.2 is present and use other than qualified signatures is addressed
6.3	2nd para	T	Consistently with previous comment to clause 4.6, it is recommended to reword this locution. For example: "... the subject, where applicable under agreement with the subscriber, to be bound to:" In fact a subject can request for an AC without any third party involved as subscriber.		accepted
6.3	Last two para	E/T	1) please use a numbered items list for an easier reference; 2) consistently with the previous comment, please modify the second item as follows: "notify the subscriber, where applicable, ..."		Accepted (see previous comment)
6.4	1st para	E		“Attribute Certificate, ~~it~~ *the relying party* shall”	accepted
6.4	Note	T		“This delay *, that shall be consistent with provisions in clause 7.2.7 item h),*”	Accepted with modification (no “shall” allowed in a note)
7	1st para	E	“The present document is concerned with AAs issuing Attribute Certificates” Useless repetition. Please delete		accepted
7	1st para	T		Consistently with the previous comment please change “This includes” in "AA practice requirements include ..."	Accepted

7.1	Note 1	T	This Note text sounds odd: in the bottom line it is the AA that defines in its ACPS how Attributes are published in ACs. Please be more specific.		Accepted, note modified as follows: NOTE 1: the set of attributes to be placed in a single AC may be defined by the subscriber or by the AA. In the former case they can be limited to a selection of subset of attributes made available to the subject. In the later case the AA informs the subject and, where applicable, the subscriber about which attributes a given subset contains.
7.1	Item f)	T	"The AA shall specify in its ACPS whether and how a subject can inform the AA that he/she wants to delegate one or more of his/her attributes to another subject. " Incomplete	""The AA shall specify in its ACPS whether and how a subject *or, where applicable, a subscriber, can inform the AA that one subject's attribute/s are to be delegated, in toto or partly, to another subject*	accepted
7.2.1	Item d)	E	Please make these sub-items a numbered list		accepted
Page 18	Note 5	T		"…the AA should ascertain the identity *and rightfulness* of that representative"	accepted
Page 18	Item i)	E	Please make the sub-items a numbered list		accepted
7.2.2	1st para	E	"The AA shall ensure that subjects' attributes to be registered or renewed are properly verified and that they relate to an already registered subject." Please reword.	"The AA shall ensure that *one subject's attributes to be renewed* [since this clause addresses "renewal" a new registration does not apply] *are properly verified and that they relate to the subject they are to be renewed to*"	Rejected. New attributes can be registered during renewal
7.2.2	Item k)	E	Please make subitems a numbered list		accepted
7.2.3.1	"Disseminati on"	E	Please correct font		accepted
7.2.4	Note 3	T	"This can be done using a subject's previously registered QC." "using " is a too generic term. Please be more specific		Accepted, note modified as follows NOTE 3: The subject can be identified for example with a signature based on a subject's previously registered QC.

7.2.7	1st para	T	"The AA shall ensure that either attributes and/or ACs are revoked in a timely manner" Please address the possibility not to revoke very short living ACs	"The AA shall ensure that either attributes and/or ACs are revoked, *where applicable,* in a timely manner"	accepted
7.2.7	Item c)	T		"Requests and reports relating to *urgent* revocation …"	accepted
7.2.7	Item h) 2)	T	This practice is not to be recommended, taking into account that ACRLs are mostly cached, especially if the interval between two ACRLs is longer than 3 - 4 hours. When caching ACRLs, an ACRL issued much earlier than expected can create great disasters.	Please replace with: "ii) a new ACRL may be published shortly before the stated time of the next CRL issue. This "shortly" would address cases where inconveniences at the AA may occur hindering and delaying the new ACRL issuance. NOTE: by "shortly" it is intended few minutes, to let the AA handle small technical inconveniences at CRL issue time."	Not accepted. No argumentation is given on the reason why issuing a CRL earlier than expected can create issues. When possible this clause has been aligned with other related deliverables (EN 319 411-X and EN 319 421)
Page 23	"Revocation status"	E		Please fix font	Accepted
7.2		T	How come provision in prEN 319 411-2, clause 7.3.6, item m) is not replicated here? "m) It is recommended that both OCSP responders conforming to RFC 6960 be supported and CRLs be issued to maximise interoperability."		Accepted with modification. The following text has been added (added "when applicable" because non X.509 AA can use different methods): m) When applicable, both OCSP responders conforming to RFC 6960 should be supported and CRLs should be issued to maximise interoperability
7.3.1		T	"A different key should be used for each different purpose." It is not clear why different keys should be used, in particular to sign ACs and ACRLs		Accepted, chanded as follows: A different key can be used for each different purpose
7.3.1		E	Please make all bulleted items lists as numbered lists		Accepted

7.3.1	Item b)	T	It is not clear why CWA 14167-4 is not listed, given that its Clause 1.2 "Protection Profile Overview" currently reads: "*The Cryptographic Module, which is the Target of Evaluation (TOE), is used for the creation of CSP key pairs, and their usage for the creation and verification of advanced electronic signatures in qualified certificates or certificate status information*."		Accepted. Reference to CEN TS 419 221 now replaces CWA 14167
7.3.2	"Keys backup and recovery"	T	A Note here wold be useful to remind that CWA 14167-4 does not allow for key export and consequently back-up		Accepted
7.3.6	Item b)	T	The storing phase must be addressed too	"the cryptographic hardware is not tampered with *when being stored and* while stored;"	accepted
Page 26	Note 1	T	Given the importance of this Note its content should be an item itself.		Accepted with changes: inserted in item b)
7.4.6	Item b)	T	"are kept in a physically secure environment" Logical security must be addressed too	"are kept in a physically *and logically* secure environment"	accepted
7.4.8	Item b)	E	Make it a numbered items list	Accepted	accepted
Page 28	Note 3	E	Please swap the following words: "this is accuracy ensured"	this *accuracy is* ensured"	accepted
8.1	Item d)	T	"that the attribute certificate policies are supported by the Attribute Certification Practices Statement (ACPS)." One ACP may be supported by more than just one ACPS, so please reword:	"... each attribute certificate policy is supported by at least one ...ACPS"	accepted
Annex A	Item a)	T	Does not this sentence exclude ACPs specifically developed as per clause 8?	Maybe a different wording would be more suitable, for example: "... under one Attribute Certificate Policy, for example one of the two identified in clause 5.2;"	Accepted, Annex A will migrate to a new TS as decided in ESI#42
Annex A	Items b) and c)	E	For a better understanding please replace "certificate" with "public key certificate"		Not applicable any more as it was decided to not mandate that an AA is linked to a PKI certificate
Annex D		E/T	Why many withdrawn documents are listed here? Addressing them may be misleading.		accepted