Public Review: Resolution of Comments on Draft ETSI *EN 319 401* V1.1.2 – 31 May 2014

Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers

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.

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

A 1	Title		Major Technical	The title of the document has been changed from : "General Policy Requirements for Trust Service Providers" to: "General Policy Requirements for Trust Service Providers supporting electronic signatures" The scope has been extended and thus now applies to any TSP. However, the text only applies when the TSP is delivering some "trust service tokens". See section 6.2. b) See also section 6.3.2: "private signing keys" There are some TSP which are not delivering trust service tokens, but only status information through a secure channel (e.g. TLS). The title should be changed into: "General Policy Requirements for Trust Service Providers delivering trust service tokens". If this document is published as an EN, no other document covering the same scope could exist in the European countries, because there would already be an EN transposed into a national norm. Any other national norm covering the same scope or not fully compliant to this text could not exist.	Change the title into: "General Policy Requirements for Trust Service Providers delivering trust service tokens". Change the EN into a TS.	Rejected

B 1	Foreword	National transposition dates	E	Please review the specified dates		Agree. This text was provided by ETSI. To review.
B 2	3.1	Definition of “subject”	T	Why has this definition been removed? A Subject can be either a natural or a legal person		Rejected. Although the concept of “subscriber” can be generalised (or applies) to any type of services offered by any type of TSP, the concept of “subject” is more relevant to Certification Services. The meaning of subject is specific to class of TSP. Not all TSP have subject (e.g. time-stamp).
A 2	Definitions		Editorial	There is a definitions in this section which is not used in the document. It should be deleted. EditHelp! will certainly notice it.	Delete: - "attribute".	It is only used in reference [i.10] Propose to delete
B 3	Numerous Notes		E	The reference to ISO/IEC 27002 has been updated to 2013 edition	Please add a reference to this 2013 edition into clause 2.2 and add a reference to this entry in the notes	Addressed in reference [i.2]
A 3	4.2.1		Editorial	The text states: "which may be referenced by a policy identifier in a token", "token" is undefined whereas "trust service token" is defined.	Change into: "which may be referenced by a policy identifier in a trust service token",	Accepted

C 1	6.3		G or E	Clauses about key management life cycle are very short and nondescriptive. At the same time in drafts of ETSI EN 319 411-1,2,3,4 and ETSI EN 319 421 in respective clauses most requirements about key management life cycle (mostly under 7.3) are overlapping. They could be defined as generic requirements in ETSI EN 319 401.	Bring overlapping requirements of key management life cycle from drafts ETSI EN 319 411 (1-4) and ETSI EN 319-421 to the EN 319 401.	To be discussed. Need to identify the overlapping. Clarify relevant reference. It seems to refer to 7.2. Current text on 411 is too specific for CA
A 4	6.1	NOTE 1	Editorial	The text states: NOTE 1: This policy makes no requirement as to the structure of the trust service practice statement.	Change into: NOTE 1: This document makes no requirement as to the structure of the trust service practice statement.	Accepted
A 5	6.2		General	The document is mentioned to be a STABLE DRAFT. However this section includes: Editor's note 1: Editor's note 2: So it is not a stable draft.	No additional text should be added. Delete the two editor's notes.	These notes were deleted before the text was circulated for public review.

A 6	6.4.3	item f)	Technical	The text states: f) Managerial personnel shall be employed who possess experience or training in the electronic signature technology and familiarity with security procedures for personnel with security responsibilities and experience with information security and risk assessment sufficient to carry out management functions. The service does not necessarily require "experience or training in the electronic signature technology".	Proposed change: f) Managerial personnel shall be employed who possess experience or training with respect to the trust service that is provided and familiarity with security procedures for personnel with security responsibilities and experience with information security and risk assessment sufficient to carry out management functions.	Accepted
A 7	6.4.5	Item g)	Editorial	The text states: g) TSP shall act	Proposed change: g) The TSP shall act	Accepted
A 8	6.4.5	Item j)	Technical	The Note states: Note: Further recommendations are given in the CAB Forum network security guide [i.11] item 4 f). The text in j) is not specific to network.	Delete the Note.	Rejected

A 9	6.4.6	Item f)	Editorial	The Note states: NOTE 3: Further recommendations regarding authentication is given in the CAB Forum network security guide [i.11] section 2. The Note should be rephrased in the same style as the Note above: NOTE 2: see section 9 of ISO/IEC 27002/2013 for guidance.	Proposed change: NOTE 3: see also section 2 of the CAB Forum network security guide [i.11] for guidance.	Rejected
D 1	6.4.9	Bullet a) i)	General	The requirement does not state how to inform. Shall the TSP send information directly (and may this be via e-mail) or can the TSP announce termination through media?	Explicitly state how to inform regarding termination	No proposal provided.
D 2	6.4.9	Bullet a) i)	General	The term “other form of established relations” is very open for interpretation.	Clarify i.e. with examples	No proposal provided.
D 3	6.4.10		General	It is unclear if the sentence ”The TSP shall ensure compliance with legal requirements” is for the country/memberstate where TSP is located or the countries/memberstates where the TSP are doing business?	The sentence ”The TSP shall ensure compliance with legal requirements” should be extended to clarify the jurisdiction for which the TSP shall ensure compliance.	The sentence is clear. No change.

D 4	6.4.12	Bullet c	General	Operating with requirements for having both a Root CA and subordinate CAs and keeping Root CA in an offline or air-grapped state is making infrastructures robust. But this also means the requirement to the Root CA should differ from the requirements for the subordinate CAs. E.g. the frequency of CRL generation can be significant lower for the Root CA.	It is suggested to extend the ETSI 319 411-x series to have a part dedicated to “Policy requirements for Root CA’s issuing certificates to subordinate CA’s”	This comments should be addressed in the edition of the ETSI 319 411-x serie
A 10	6.4.12	Item d)	Editorial	The Note states: NOTE: Recommendation regarding the time period is given in the CAB Forum network security guide [i.11] item 4c. The Note should be rephrased.	Proposed change: NOTE : see item 4c of the CAB Forum network security guide [i.11] for guidance regarding the time period.	Accepted
B 4	6.4.12	Item e)	T	Why “on at least an annual regular basis” has been removed? A periodic repetition of penetration tests must be performed		Rejected
A 11	6.4.12	Item e)	Editorial	The Note states: NOTE: Recommendation regarding the time period is given in the CAB Forum network security guide [i.11] item 4d. The Note should be rephrased.	Proposed change: NOTE : see item 4d of the CAB Forum network security guide [i.11] for guidance regarding the time period.	Accepted

A 12	History	Page 20	Editorial	There are several versions 1.1. at different dates. This is rather odd.	Please correct.	See with edithelp
E 1	Definitions	3.1	Editorial	*subscriber definition : "entity subscribing with a trust service provider who is legally bound to any subscriber obligations"*	*"entity or person adhering to an agreement with a trust service provider in order to access or use services. This person or entity is legally bound by terms and conditions of that agreement"*	Accepted
E 2	Information for relying parties	5.3	Editorial	*"The terms and conditions made available to relying parties (see clause 6.2) shall include a notice in order to identify under which conditions is reasonably to rely upon a service."*	*"The terms and conditions made available to relying parties (see clause 6.2) shall include a notice identifying the conditions under which a service can reasonably be relied upon."*	Accepted
E 3	TSP Dissemination of Terms and Conditions	6.2	Editorial	*f) limitations of liability;*	*f) any limitations of liability, including the purposes/uses for which the TSP accepts (or excludes) liability;*	Redundant. No rationale provided
E 4	TSP key generation	6.3.1	Technical	*"The TSP shall ensure, where applicable, that any cryptographic keys are generated under controlled circumstances and are issued securely."*	*"The TSP shall ensure, where applicable, that any cryptographic keys are generated under controlled circumstances and are issued securely..* *In particular, any TSP private key generation shall be undertaken in a physically secured environment by personnel in trusted roles under, at least, dual control. "*	Rejected

E 5	TSP key generation	6.3.1	Technical	*The TSP shall ensure, where applicable, that a cryptography algorithm used for key generation is recognized as appropriate for the time period of the key usage."* Is there a standard somewhere listing the cryptography algorithms recognized as appropriate for each key usage? If so, we should mention this standard as a reference.		Informative reference could help. Can reference TS 119 312
E 6	Security management	6.4.1	Editorial	*"c) The TSP management shall define a set of policies for information security appropriate for the trust services it is providing,…"*	*"c) The TSP management shall define a set of policies for information security appropriate for the trust services it provides,..."*	No reason to change the text.
E 7	Physical and environmental security	6.4.4	Editorial	*"The TSP shall ensure that physical access to critical services is controlled and risks related to physical security minimized "* What is a critical service? What is the difference between a critical and a non-critical service?		Could be clarified: Particularly, !services" Suggest "access to components of the TSP's system whose security is critical to the provision of its trust services to all its users.". Similar change to item (a)
D 2	6.4.9	Bullet a) i)	General	The requirement does not state how to inform. Shall the TSP send information directly (and may this be via e-mail) or can the TSP announce termination through media?	Explicitly state how to inform regarding termination	This is to be addressed in EN 319 401

D 3	6.4.9	Bullet a) i)	General	The term “other form of established relations” is very open for interpretation.	Clarify i.e. with examples	This is to be addressed in EN 319 401
D 4	6.4.10		General	It is unclear if the sentence ”The TSP shall ensure compliance with legal requirements” is for the country/memberstate where TSP is located or the countries/memberstates where the TSP are doing business?	The sentence ”The TSP shall ensure compliance with legal requirements” should be extended to clarify the jurisdiction for which the TSP shall ensure compliance.	This is to be addressed in EN 319 401
D5	6.4.12	Bullet c	General	Operating with requirements for having both a Root CA and subordinate CAs and keeping Root CA in an offline or air-grapped state is making infrastructures robust. But this also means the requirement to the Root CA should differ from the requirements for the subordinate CAs. E.g. the frequency of CRL generation can be significant lower for the Root CA.	It is suggested to extend the ETSI 319 411-x series to have a part dedicated to “Policy requirements for Root CA’s issuing certificates to subordinate CA’s”	This is to be addressed in EN 319 401