Public Review: Resolution of Comments on Draft ETSI *EN 319 411 - 3* v1.2.0 – 31 May 2014

<Policy and security requirements for Trust Service Providers issuing certificates; Part 3: Policy requirements for Certification Authorities issuing public key 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.

Organization name	**Clause/ Subclause**	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change**	**resolution** on each comment submitted
	7.2		General	The draft EU regulation on electronic identification and trust services for electronic transactions in internal market Annex II bullet 3) and 4) allows schemes where the subjects private keys are protected and used in a central secure environment.	Clause 7.2.8 should be extended or a new clause should be added to include requirements to the CA managing the subjects private keys throughout the lifecycle of the keys to ensure the subjects sole control.	EN 319 411-3 is prepared within the framework of a Mandate (M.460) where the EC contractually requires ETSI to write deliverables in line with the EU Directive. Except for some very likely requirements considered in the draft EN 319 411-3, the draft Regulation is not sufficiently stable to be considered at the time of edition of the document. Moreover, for some requirements, it contradicts with the existing Directive. The STF is in discussion with EC in order to be able to work on a new version based on a stable version of the Regulation ASAP.

	Clause/ Subclause	**Paragraph Figure/ Table**	Type of comment (General/ Technical/Editorial)	**COMMENTS**	**Proposed change**	**resolution** on each comment submitted
	General		**G**	Bulleted items lists should be changed in numbered items lists, for a better reference		Agree
	Foreword	**2nd Paragraph**	**E**	This wording can be interpreted as if TS 102 042 has been blindly copied and pasted.	Please specify that TS 102 042 has been updated with this EN and that such updates are referred to in Annex C	Agree. The sentence is now completed by “that has been updated according to elements referred to in Annex c.”

	Foreword	**Table "National transposition dates"**	**E**	Is year "2013" correct?		The first version of 319 411-3 was issued in January 2013
	2.2	**Item [i.2]**	**E**	The referred to document seems being different		changed
	2.2	**Item [i.7]**	**T**	In 2012 a new version was issued of ISO/IEC 27002		Agree, changed
	2-2	**Item [i.11]**	**E**		ETSI TS ~~1~~119 31	changed
	3.1	**Definition of "certificate"**	**T/E**	It would be honest to state that this definition has been taken from ISO/IEC 9598-4 clause 3.3.46, where it is the definition of public-key certificate (PKC). This applies to a number of other definitions too.		Agree. Note added
	3.1	**Definition of Root CA**	**E**		"trusted List [i.13] ***o***r a"	changed
	4.2	**2nd paragraph**	**E**		for purposes of trust in which ***case*** it may	changed
	4.3	**5th bullet**	**E/T**	If this refers to OCPS, then "online" is better, because more often than not an OCSP server updates its data base periodically, i.e. not in "real time	"or a real time service" ➔ "or *an online* service"	changed
	Page 13	**1st bullet**	**E/T**	It is not the certificate itself to be signed by the subject. Same comment applies to the subsequent dotted items	"***Request for a***~~A~~ certificate for natural person is subscribed by:"	Agree, changed
	5.1	**1st para**	**T**	1) It is not clear why this definition is repeated here 2) Reference [7] ➔ It would be appreciated to specify this reference in the Definition Clause too.		1.+2 agree deleted,

	6.2	**Item h) ii)**	**T**	"the subject's private key has been potentially compromised…" "potentially" here must refer to both cases: compromise and loss. Please amend		Agree, changed
	6.3	**1st para**	**E**	"if it is to reasonably rely upon a certificate, ***it*** shall:" This "it" is inconsistent with plural ("*relying parties*") Please fix it, for example by replacing "it" with "the relying party"		Agree, changed
	7.2.1	**Item d)**	**E**		Replace "TS 102 176-1" with "TS 119 312"	Its still a draft, but agree and changed
	Page 18	**2nd Bullet**	**T**	"this ceremony shall be witnessed by a qualified auditor or a notary," A notary is not aware of all technical subtleties, therefore the locution "or a notary" should be complemented with "with the assistance of an expert". Similar comment on a "qualified auditor" in order to avoid misinterpretations.		Important comment TBD
	Page 18	**3rd Bullet**	**T**	"the TSP shall record a video …" "Shall" is too much. This video, in fact. would require to be notarized from its very first moment up to the end to be reliable. Too complex. The same for "For Subordinate CAs key generation"	A "should" would be enough.	Not agree, taking the Video can be interurpted
	7.2.7	**Item b)**	**T**	"cryptographic hardware is not tampered with while stored" The storing phase shall be addressed too	"cryptographic hardware is not tampered with *when being stored and* while stored"	Not agree, being stored is part of the storage process
	7.2.7	**Item e)**	**T**	"This destruction does not affect all copies of the private key."	"This destruction does not ***necessarily*** affect all copies of the private key."	Agree, added
	7.2.8	**Note**	**E**	TS 102 176-1	TS 119 312	Agree, changed

	7.2.8	**Item e)**	**T**	"…once delivered to the subject, the private key can be maintained under the subject's sole control" "can" is utterly inappropriate here. It is necessary to specify "Must"	"…once delivered to the subject, the private key ***must*** be maintained under the subject's sole control"	NOT agree, TDB, very strict for NCP This depends on key usage .The scope of this document is not limited to advanced electronic signatures. Also, user control over key is outside scope. If so required the user CAN apply sole control..
	7.2.9	**1st para**	**T**	More details are necessary.	E.g.: "[NCP+] The CA shall ensure that, if it delivers a secure user device to the related subject, the delivery is carried out securely, i.e. in a way to prevent tampering and/or misuse."	NOT agree, TDB, very strict for NCP The first paragraph lays out the general objective. Subsequent items list more specific requirements. Item b) covers secure distribution.
	7.3.1	**Item c)**	**E**	"genuinity" This term cannot be found neither in Merriam Webster nor in Encyclopaedia Britannica.	Maybe it must be replaced with "authenticity"	TBD Agree
	7.3.1	**Utem d) ii)**	**T**	1) "checked against a natural person" ➔ "a" is too generic. "This", instead, refers exactly to the person at issue. 2) However. the whole paragraph is too convoluted: please slim it down		1) agree changed 2) agree, but not changed because of keeping track to TS 102 042 practise
	7.3.1	**Item f)**	**E**	"with an organisation" is repeated twice		Agree
	7.3.1	**Item g) iv)**	**E**	"a nationally recognized identity number,"	"a nationally recognized identity ***document***,"	Not agree, Tbd, its on legal persons, normaly covered by Business Register with number
	7.3.1	**Item h) 2nd bullet**	**E**	"not assoaicated"	"not associated"	Agree, thanks
	7.3.5	**Item g) ii)**	**T**	"[NCP] the information identified …"	Pleased insert also "[NCP+]" for a better understanding. Nowhere, in fact. is said that where only [NCP] is mentioned, by default it is intended [NCP+] too.	Agree, TBD Agree add NCP+

	7.3.6	**Editor's note**	**T**	One day is usually a reasonable period, although in particularly delicate cases it is better to keep this interval as short as possible, for example 3 - 4 hours. It would beneficial to add an explanatory note on this.		Not agree, its stated: "This shall be at most"
	7.3.6	**Item d)**	**T**	Waiting for confirmation is not the only case where a suspension may be useful.	"…suspended, for example whilst the revocation is being confirmed, in which case the CA ... "	Agree, "for example" added
	7.3.6	**Item h) ii)**	**T**	The practice of issuing a new CRL before expiration time of the previous one is not to be recommended, taking into account that CRLs are mostly cached, 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 small technical inconveniences at CRL issue time."	Needs to be discussed Dispose as in 319 411-2
	7.3.6	**Item n)**	**E**	"RFC 6960" 1) Please add this to Clause 2.1 2) Add the related reference number		Agree, added
	7.4.4	**After item b)**	**T**	A Note here would be helpful to clarify that even authorized persons must not be left alone in these premises, lest readers may infer this requirement applies only to non authorized persons.		Agree, added
	7.4.5	**Item a) i)**	**T**		"[LCP] no ***additional*** requirement"	Agree, added
	7.4.6	**Item a)**	**T**	As asserted implicitly in the subsequent Note, also logical security is to be assured.	"are kept in a physically ***and logically*** secure environment"	Not agree, a "logically unsecure environment" does not exist
	7.4.8	**Item a)**	**T**	Please highlight that disaster recovery sites must be remotely located	backed up and stored in safe places , ***preferably also remote,*** suitable"	Agree added
	7.4.8	**Note 1**	**E**	"In line with ISO/IEC 27002 [i.7], clause 10.5.1" Please check if in ISO/IEC 27002 - 2012 version clause numbering has not changed		Agree - 27002 (2013) adopted

	7.4.11		**T**	It would be useful to inform the reader that provisions on how to preserve digital data objects are given in ETSI TS 101 533.		Agree added
	7.4.11	**Item c) ii)**	**T/E**		"driver**'**s license ~~number~~ ***code***"	Agree with changes: number or code
	7.4.12	**1st para**	**T/E**	"clause 6.4.12" This clause does not exist in the currently available EN 319 401		No Change, Latest Version covers 6.4.12 "General protection for the network and supporting system"

			General	There are 40 comments and 20 pages of comments. The time needed to produce these comments is roughly 12 hours. The introduction has been changed to include certificates to be used for encryption ! The scope of the document has been changed to include "devices or system operated by or on behalf of an Organisation or a unit or a department identified in association with an Organization" ! The content of the document has been changed to include text about root CAs and subordinate CAs ! The list of changes on page 40 is not trustworthy, since it is silent about the major changes introduced in this version. People looking at that list may think that there are only minor changes and thus that it is not necessary to read the whole document. **This is rather unfair.** The content of the document is fully missing to address CRL issuers, and OCSP responders as well as certificates issued for them by the CA. NOTE : The two most important comments are the one marked as **Major Technical** and the one before the last comment.		Disagree - This document is mainly as published in EN 319 411-3 v1.1.1. Most of the text being commented on has been developed over the last decade in TS 102 042.

	Introduction		Technical	The text states: "EN 319 401 [10] identifies general policy requirements for Trust Service Providers supporting Electronic Signatures"; A new title has been proposed for this document: "Policy Requirements for Trust Service Providers delivering trust service tokens".	Change into: "EN 319 401 [10] identifies general policy requirements for Trust Service Providers delivering trust service tokens "; 	Partially agree: EN 319 401 now identifies general policy requirements for Trust Service Providers. Not limited even to trust service tokens.
	Introduction		Technical	The text states: "The present document is based on the same approach as EN 319 411-2 [i.5] but is applicable to the general requirements of certification in support of cryptographic mechanisms, including other forms of electronic signature as well as the use of cryptography for authentication and encryption. Moreover, where requirements identified have general applicability they are carried forward into the present document." Encryption has never been considered in the past and should not be considered. " other forms of electronic signature" does not mean anything. The second paragraph on page 6 covers the same topic. Two paragraphs covering the same topic are not needed. Since the second paragraph is better phrased, this paragraph should be deleted.	Delete this paragraph.	Disagree: this is the scope of the earlier TS 102 042 and published EN 319 411-3. There is no reason for changing the scope.

	Scope		**Major Technical**	The text states: "The first reference policy defines a set of requirements for TSPs providing a level of quality the same as that offered by qualified certificates, without being tied to the Electronic Signature Directive ...." Before speaking of a level, the scope should to who the certificates may be issued. The text scope in the scope does not allow to image that the content of the document has been extended far beyond its original limits. It is needed to read section 4.5 to be able to identify to who the certificates may be issued. Section 4.5 states: "Subjects can be: • natural person, • natural person identified in association with an Organization (having a legal identity), • legal person (that can be an Organisation or a unit or a department identified in association with an Organization), • devices or system operated by or on behalf of an Organisation or a unit or a department identified in association with an Organization". Covering devices or systems is a major change of the initial scope. Issuing certificates to machines should be done in a very different way and should not be covered within the same document. Furthermore, it is really out of the scope of the Mandate which was focusing on certificates issued to persons. Extending the scope in the final document is not acceptable. Later on the scope states: "Certificates issued under these policies requirements may be used in support of any asymmetric mechanisms requiring certification of public keys	Change proposal: Change the first quoted paragraph into: "The present document is applicable to the general requirements of certification in support of public key certificates issued to : • a natural person, • a natural person identified in association with an Organization (having a legal identity), • a legal person (that can be an Organisation or a unit or a department identified in association with an Organization). Two types of certificates are considered whether they can be used for: - authentication or data origin authentication, or - non-repudiation (i.e. electronic signatures)" It is also applicable to the general requirements of certification in support of public key certificates issued to: - CRL issuers, and - OCSP responders. Delete the second quoted paragraph. Create a separate document to address Root CAs and Subordinates CAs. Be ready to have an informative reference to this document in this draft.	Disagree: this is the scope of the earlier TS 102 042 and published EN 319 411-3. There is no reason for changing the scope.

	Scope		Editorial	The text states: "In addition, the present document does not address requirements for Certification Authority certificates, including certificate hierarchies and cross-certification". This sentence is in contradiction with the extension "done at the last minute" to cover certificates issued by root CAs or subordinate CAs issuing CA certificates. It is basically correct, but its wording can be improved.	Change proposal: "The present document does not address requirements for Certification Authorities issuing CA certificates, whether they are root CAs or subordinates CAs. These requirements are covered in ....[ ]."	Disagree The document includes requirements relating to issuing (subordinate) and root CAs. Delete “Certification Authority certificates, including certificate hierarchies and” in current text.
	Section 3.1			There are two definitions that are not aligned: "certificate: public key of a user, together with some other information, rendered unforgeable by encipherment with the private key of the Certification Authority which issued it." "Public-key certificate (PKC): public key of a user, together with some other information, rendered unforgeable by digital signature with the private key of the CA which issued it"; Two definitions are not needed. The former definition was written at the time RSA was the single known asymmetric algorithm, hence the word encryption was being used. The later definition allows to use algorithms devoted to digital signature and thus is correct. Delete the first definition and mention that it is a synonym of "certificate" since we only consider PKCs.	Delete the first definition. Change the second definition into: "Public-key certificate (PKC): public key of a user, together with some other information, rendered unforgeable by digital signature with the private key of the CA which issued it. Synonym of "certificate". Modify 319 401 accordingly.	Disagree: This adopts standard terminology of X.509.

	Section 3.1		Technical	The text states: "secure user device: device which holds the user's private key, protects this key against compromise and performs cryptographic functions on behalf of the user". Since there may be a key for authentication and a key for non-repudiation, the plural should be used. The device also contains the certificates. It is also important to mention that the secure user device maintains the use of the private keys under the sole control of the user.	Change proposal: "secure user device: device which holds the user's public key certificates and the associated private keys, maintains the use of the private keys under the sole control of the user, protects these keys against compromise and performs cryptographic functions on behalf of the user".	Partially agree: secure user device may contain several keys. Reject more specific details depend on the type of service provided.
	Section 3.1		Technical	"OCSP Online Certificate Status Protocol" is indicated in section 3.2 but there is no definition in section 3.1. Add a definition.	Add the following definition: "Online Certificate Status Protocol (OCSP) : a protocol that allows determining the current revocation status of a public-key certificate (PKC)."	Not agree, link to RFC 6960 added in document
	General		Technical	The Major comment has implications in the whole document. There is not enough time to mention them, but starting from the definitions sections, many deletions should be done.	Perform the deletions and the modifications that are relative to the Major Technical comment.	This document primarily based on existing publication of EN 319 411-3
	Section 4.2		Technical	The text states: "The Certification Authority is identified in the certificate as the issuer and its private key is used to sign certificates". A CA has more that one public key. make the sentences plural. The key may also be used to signed CRLs or OCSP responses. This is not indicated.	Change into: "The Certification Authority is identified in the certificate as the issuer and its private keys are used to sign certificates and may also be used to sign CRLs or OCSP responses".	Disagree – at any one time it, relating to a single certificate, uses a specific private signing key.

	Section		Technical	The text states: "A Certification Authority is a Trust Service Provider, as described in EN 319 401 [10], and also a form of certification service provider as defined in the Electronic Signatures Directive 1999/93/EC [i.1], which issues public key certificates". The second part of the sentence has noting to do in this document. It should be deleted.	Delete: "and also a form of certification service provider as defined in the Electronic Signatures Directive 1999/93/EC [i.1], which issues public key certificates".	Disagree – This document is currently written in the context of the Directive.
	Section 5.4.1		Technical	The text states: "The CA shall only claim conformance to the present document as applied in the certificate policy (or policies) identified in the certificate that it issues:" followed by items a) , b) and c). However the text from the first sentence does not match in continuation with the text from items b) and c): b) If the CA is later shown to be non-conformant ... c) The CA conformance shall be checked on a regular basis ...	The sentence within item b) and c) should be kept, but should not be part of the three cases. There should be only one case: "The CA shall only claim conformance to the present document as applied in the certificate policy (or policies) identified in the certificate that it issues, if either: i) ... ii) ..."	Agree with changes Logic should be: (a – i or a-ii) and b and c

	Section 5.4.1	Page 15	Technical	NOTE 3 states: "NOTE 3: Even if a CA is known to be critically non-conformant, it may issue certificates for internal and testing purposes provided that such certificates are not made available to for any other uses." The problem is that the text does not say how to identify test certificates even if the CA is known to be conformant. Should a specific form of name should be used to allow to distinguish them ? In any case, such a requirement should not be placed into a NOTE, but in the main body of the document.	Change into: "Certificates issued for testing purposes shall be clearly identifiable as such using a qualifier in the DN. NOTE 3 : It is recommended to include the following four characters at the beginning of the CN attribute: TEST. Add the two following abbreviations in section 3.2 : DN: Distinguished Name CN: Common Name	Disagree: How it implements this requirement is up to the CA.
	Section 6.2 Item c)		Technical	The text states: "c) reasonable care is exercised to avoid unauthorized use of the subject's private key;" As a subscriber obligation, this does not mean anything.	Please delete.	**Disagree**

	Section 6.2 Item e)		Technical	The text states: e) [CONDITIONAL] if the subscriber or subject generates the subject's keys and then the private key is for creating electronic signatures the subject's private key is maintained under the subject's sole control; This sentence is not grammatically correct. Further more, if the if the subscriber generates the subject's keys, how can the private key be maintained under the subject's sole control ? Further more, why should such a case be restricted to private key is for creating electronic signatures ? Further more, this requirement is not conditional, since it applies to NCP.	Change into: e) [NCP and NCP+] if the subject generates the subject's keys, reasonable care shall be taken so that the private key remains under the subject's sole control;	**Disagree – the subscriber may be trusted to generate the key depending on the key usage.**
	Section 6.2 Item f)		Technical	The text states: f) [NCP+] use the subject's private key for cryptographic functions within the secure user device only; Since there may be a key for authentication and a key for non-repudiation, the plural should be used.	Change into: f) [NCP+] use the subject's private key<u>s</u> within <u>a</u> secure user device only;	Agree with changes may be one or more keys

	Section 6.2 Item h)		Technical	The text states: "h) notify the CA without any reasonable delay, if any of the following occur up to the end of the validity period indicated in the certificate: i) the subject's private key has been lost, stolen; or ii) the subject's private key has been potentially compromised or control over the subject's private key has been lost due to compromise of activation data (e.g. PIN code) or other reasons; and/or" What means : "without any reasonable delay" ? How can a user "loose the private key" ? This does not mean anything for him. However, it can loose the control of the private key or it can loose the secure user device. This applies to any of the certificates.	Change into: "h) notify the CA <u>within a reasonable delay</u>, if any of the following occur<u>s</u> up to the end of the validity period indicated in one of the certificates: i) the control over one of the subject's private key has been lost due to a compromise of the activation data (e.g. PIN code) or other reasons; and/or ii) [NCP and NCP+] the secure user device has been lost or stolen; and/or"	Agree "<u>within a reasonable delay</u>"
	Section 6.2 Item i)		Technical	The text states: i) following compromise, the use of the subject's private key is immediately and permanently discontinued; The text is not precise enough to address the two cases.	Change into: "i) following the notification to the CA, in case of : i) a loss of subject's private key control, the user shall stop using that subject's private key, ii) [NCP and NCP+] a loss of the secure user device, the user shall stop using that all the subject's private keys, even if the user recovers the use of the secure user device."	Disagree – these are just example of compromise

	Section 6.2 Item j)		Technical	The text states: j) in the case of being informed that the CA which issued the subject's certificate has been compromised, ensure that the certificate is not used by the subject in any new signatures. This case is irrelevant. If the CA key has been compromised, it will be revoked by the upper CA and all the new signatures will be invalid. The user may continue to use the key, but its signatures will not be accepted. So there is no requirement to be placed on the user.	Delete item j)	Disagree – even if this may be protected by CA revocation the user should not be using the private key
	Section 6.3 Item a)		Technical	The text states: "a) verify the validity, suspension or revocation of the certificate using current revocation status information as indicated to the relying party (see clause 7.3.4); and" This is fairly insufficient. It is needed to verify a certification path up to a root CA. Each segment from the path shall be checked to make sure that the CA certificate has not been revoked. Also the verification is not done necessarily at the current time.	Change into: "a) verify the validity, suspension or revocation of all the certificates that have been used to construct a certification path from the user's certificate up to a trusted root, using revocation status information as indicated to the relying parties (see clause 7.3.4); i) if the verification is done at the current time, then current revocation information shall be used, ii)) if the verification is done at a time in the past, then revocation information captured at that time or close to that time in the past shall be used, and"	Disagree – the details of what is needed to verify a certificate and all the path is not relevant here.

	Section 7.2.1		Technical	The title is: "7.2.1 Certification Authority key generation" The subtitle is: "Certificate generation" When looking at the content of this section, the subtitle does not make sense, since there is no "Certificate generation" at that stage. However, the text is silent about the way the CA obtains a CA certificate from another CA. This should be addressed in section 7.2.3.	The subtitle "Certificate generation" should be deleted.	Agree with changes The aim of this is to clarify that this requirement relates to certificate generation Change sub-heading to Note: The following requirements relate to the Certificate generation components of the CA (see 4.3)
	Section 7.2.1 Item e)		Technical	The text states: "e) A suitable time before expiration of its CA signing key (for example as indicated by expiration of CA certificate), the CA shall generate a new certificate-signing key pair and shall apply all necessary actions to avoid disruption to the operations of any entity that may rely on the CA key. The new CA key shall also be generated and distributed in accordance with this policy". The example is wrong, since there is a difference between the expiration of the CA private key and the expiration of CA certificate. This text is not sufficient, since CRLs must continue to be issued, up to the end of the validity of the CA certificate.	Change into: "e) The CA shall generate a new key pair in a timely manner in order to guarantee the validity period of the certificates it issues. It shall use the new private key to generate new certificates and, for the certificates issued under the old key, it shall continue to use the old private key to issue CRLs and/or OCSP responses until the end of the validity of the corresponding certificate."	Disagree – whilst this relates to certificate lifetime – the requirement relates to the key.

	New section 7.2.2	Last sentence	Technical	The text states: "[NCP] When outside the signature-creation device (see a) above) the CA private signing key shall be protected in a way that ensures the same level of protection as provided by the signature creation device". Above the text states: "[NCP] The CA private signing key shall be held and used within a secure cryptographic device which: "	Change into: "[NCP] When outside the signature-creation device (see a) above) the CA private signing key shall be protected in a way that ensures the same level of protection as provided by the secure cryptographic device".	Agree with changes First “the signature-creation device” should also be a secure cryptographic device

	Section 7.2.3		Technical	The subtitle is: "Certificate generation and certificate distribution" However, the text speaks about the distribution of the CA public key instead of the way the CA obtains a CA certificate from another CA and then distribute it. Since the document should only cover certificates issued to persons, the CA which issues these certificates is never a root CA. So the CA shall always obtain a certificate from another CA. The first sentence should be kept. However, the remaining of this section should be changed.	Text change for the remaining of this section: "Once a CA key pair is generated by personnel in trusted roles under, at least, dual control (see section 7.2.1), the CA public key shall be exported and a hash value of that public key shall be computed. The end of the key ceremony shall be concluded by the signature of a document signed by a witness and the personnel in trusted roles and which shall mention the value of the hash value. This signed document and the value of the CA public key may then be communicated to another CA in order to obtain a CA certificate from that other CA. That other CA is then able to verify the genuiness of the key that is presented by recomputing a hash value over the value of the CA public key and comparing it to the hash value indicated in the signed document. The CA shall also indicate to the upper CA : a) the validity period of the requested certificate and b) whether it directly issues the CRLs and/or the OCSP responses under that key. Once the CA certificate has been contained from the upper CA, the CA shall make available the new CA certificate to its relying parties.	See earlier comment regarding certificate generate heading -> note

	Section 7.2.4. Item a)		Technical	This section comes out of the blue, since the other sections are devoted to CA keys rather than subject's keys. Furthermore, the text states: "a) [CONDITIONAL] If the subject's key is to be used for electronic signatures with the meaning of Directive 1999/93/EC [i.1], then the CA shall not hold the subject's private signing keys in a way which provides a backup decryption capability (commonly called key escrow)". A signature key is not an encryption key. So this sentence speaking of a "decryption capability" is irrelevant. Section 7.2.8 already covers correctly the topic: "e) [CONDITIONAL] If a copy of the subject's private key is not required to be kept by the CA, or other authorized entity, (see clause 7.2.4), once delivered to the subject, the private key can be maintained under the subject's sole control. Any copies of the subject's private key held by the CA shall be destroyed".	Delete the whole section.	Disagree – scope can include encryption. Also main clause covers key management including subject keys.
	Section 7.2.5 Item a)		Technical	The text states: a) CA signing key(s) used for generating certificates, as defined in clause 7.3.3, and/or issuing revocation status information, shall not be used for any other purpose. The use of " and/or " is inadequate. This is also not precise enough.	Change into: a) CA signing key(s) shall only be used for : i) generating subject's certificates, as defined in clause 7.3.3, ii) generating CRLs, iii) generating certificates for CRL Issuers, iv) generating OCSP responses, v) generating certificates for OCSP Responders.	Disagree – this does not add any further information

	Section 7.2.6		Editorial	The text states: Certificate generation This floating subtitle is not related to the following text. Please delete.	Please delete.	Change sub-heading to note as above
	Section 7.3.2. Item d)	Page 25	Technical	The text states: d) The CA shall issue a new certificate using the subject's previously certified public key, only if its cryptographic security is still sufficient for the new certificate's validity period and no indications exist that the subject's private key has been compromised. The word "may" should be used instead of "shall" since the CA may choose to change the subject's key at every key renewal.	Change into: d) The CA may issue a new certificate using the subject's previously certified public key, only if its cryptographic security is still sufficient for the new certificate's validity period and no indications exist that the subject's private key has been compromised.	Disagree – The wording “shall …. only" makes the requirement clear.
	Section 7.3.3 Item vii)		Technical	The text states: vii) the electronic signature of the Certification Authority issuing it; Please do not confuse an digital signature with an electronic signature, even if the EU Directive has this mistake (since the EU Directive was not written by technicians).	Change into: vii) the digital signature of the Certification Authority issuing it;	Disagree - the wording is based on the legal requirements.

	Section 7.3.3 Items ii) and iii) from item d)		Technical	The text states: d) [CONDITIONAL] if the CA generated the subject's key: ii) [LCP], [NCP] the private key shall be securely passed to the registered subject; iii) [NCP+] the secure user device containing the subject's private key shall be securely passed to the registered subject. The subtitle of this section is: "Certificate generation". The text speaks about the private key but omits speaking about the certificate.	Change into: d) [CONDITIONAL] if the CA generated the subject's key pair: " ii) [LCP], [NCP] both the subject's certificate and the subject's private key shall be securely passed to the registered subject; iii) [NCP+] the secure user device containing both the subject's certificate and the subject's private key shall be securely passed to the registered subject".	Disagree The certificate does not need to be afforded the same protection as the private key. Requirement for certificate generation is covered in other items
	Section 7. Item d)		Technical	The text states: d) [CONDITIONAL] if the CA generated the subject's key: However there is no section to deal with the other case where the secure user device generates the key pair.	Add a new section called: e) [NCP+] if the secure user device generated the subject's key pair, then the subject's public key shall be securely passed to the CA.	Disagree – the same protection need not be afforded to the public key as the private key. Protection of public key covered in 7.3.3 c)

	Section 7.3.4.		Technical	The text states: 7.3.4 Dissemination of terms and conditions (...) In addition the CA shall ensure that the terms and conditions are made available to subscribers and relying parties. The certificates may NOT be issued to the public, but relying parties may include the public. In such a case, the terms and the conditions made available to subscribers should not be made available to the public. There should be two separate sections: 7.3.4. Terms and conditions to be made available to subscribers 7.3.5. Terms and conditions to be made available to relying parties	Separate that section into two sections: 7.3.4. Terms and conditions to be made available to subscribers 7.3.5. Terms and conditions to be made available to relying parties Due to the numerous number of comments, there is a lack of time to provide detailed changes.	Disagree – the information provided is of concern to both.
	Section 7.3.6 Item vi)		Technical	NOTE 2 states: "NOTE 2: If the revocation request cannot be confirmed within 1 day then the revocation status may not be changed" This note is coming out of the blue, since it is unrelated with the previous sentences which does not speak of a revocation confirmation. Furthermore, it is wrong.	Delete NOTE 2.	Disagree – this note relates to delay

	Section 7.3.6 Item vii)		Technical	The text states: "vii) 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. This shall be at most [CHOICE] - [LCP] 24 Hours - [NCP] 60 minutes". The time should be set to 24 hours in both cases. The wording " the confirmation of the revocation of a certificate to become effective" is not adequate.	Change into: "vii) the maximum delay between the confirmation of the revocation request for a certificate and the actual change of the revocation status information of this certificate being made available to relying parties shall be at most 24 hours".	Disagree
	Section 7.3.6 Item h) Sub item iii)		Editorial	The text states: "iii) the CRL shall be signed by the Certification Authority or an authority designated by the CA". The "authority designated by the CA" is a CRL Issuer.	Change into: iii) the CRL shall be signed by the Certification Authority or an authority designated by the CA (i.e. a CRL Issuer).	Disagree – in both cases the CRL Issuer applies.

	Section 7.3.6 Item j)		Technical	The text states: "j) If a CA supports multiple methods (e.g. CRL and OCSP) to provide Revocation Status, any updates to revocation status shall be available for all methods, and the information provided by all services shall be consistent". Consistency is not always possible. Usually CRLs offer a renewal every 24 hours. There is no guarantee that an emergency CRL will be ever seen, unless polling every minute a CRL repository (and assuming there is no man-in-the-middle replaying the current CRL). OCSP servers using a direct access to a copy of the CA database will always provide a better information. The consistency requirement should be deleted.	Change into: "j) If a CA supports multiple methods (e.g. CRL and OCSP) to provide Revocation Status, updates to revocation status shall be available through these methods ".	Disagree – even though the information may take longer to be distributed they can be considered consistent.
	Section 7.3.6 Item l)		Technical	The text states: l) [CONDITIONAL] If the CA is issuing certificates to the public, Revocation status information shall be publicly and internationally available. CRLs may be made publicly available, while OCSP responders may be restricted to a limited population.	Change into: l) [CONDITIONAL] If the CA is issuing certificates to the public, revocation status information made available using CRLs shall be publicly and internationally available.	Disagree – if OCSP is to be main means of verification then this needs to be made public

	Section 7.3.6 Item n)		Technical	The text states: "n) It is recommended that both OCSP responders conforming to RFC 6960 be supported and CRLs be issued to maximise interoperability". Firstly, RFC 6960 is worse than RFC 2560 on several aspects, in particular when dealing with non issued certificates. So a choice between RFC 6960 and RFC 2560 should be left. Secondly, this requirement should not apply to LCP.	Change into: NOTE: [NCP , NCP+] It is recommended to support both CRLs conforming to RFC 5280 and OCSP responders conforming either to RFC 2560 or to RFC 6960 in order to maximise interoperability".	Disagree - RFC 6960 obsoletes 2560

	Section 7.4.8 Item e)		Technical	The text states: "Revocation status e) In the case of compromise the CA shall as a minimum provide the following undertakings: i) inform the following of the compromise: all subscribers and other entities with which the CA has agreements or other form of established relations, among which relying parties and CAs. In addition, this information shall be made available to other relying parties; ii) indicate that certificates and revocation status information issued using this CA key may no longer be valid; iii) when a CA is informed of the compromise of another CA, any CA certificate that has been issued for the compromised CA is revoked". As said earlier, the CA which issues certificates is never a root CA. So the CA shall always obtain a certificate from another CA. It should be said that it MUST inform the upper CA. Key compromise is not the single case for a revocation.	Change into: "e) In the case of key compromise or of a revocation for another reason, the CA shall as a minimum provide the following undertakings: i) inform the CA which has issued its CA certificate(s) to revoke the CA certificate(s), ii) inform the CA which has issued its CA certificate(s) of the reason for the revocation".	Needs to be discussed

	Annex C. Page 40		Technical	The text is supposed to identify the revisions made since TS 102 042 V2.1.3. The list of changes is not trustworthy, since it is silent about the major changes introduced in this version which are mentioned in the third comment and that is indicated as "Major Technical". People looking at the list may think that there are only minor changes and thus that it is not necessary to read the whole document. **This is rather unfair.** In addition, this list is not accurate. For example, there exists a version ETSI TS 102 042 V2.4.1 (2013-02). It is impossible to follow which changes have been made in which version.	Once the document will be revised, update the list of changes.	Needs to be discussed
	History	Page 43	Editorial	The text is supposed to identify the various versions of TS 102 042. This list is not accurate, since there exists a version ETSI TS 102 042 V2.4.1 (2013-02) which is not even mentioned.	Update the list.	Needs to be discussed