Public Review: Resolution of Comments on Draft ETSI *EN 319 411 - 2* V1.2.0 – 31 May 2014

<Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Policy requirements for certification authorities issuing qualified 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**
Company 1	0		G	This document looks to be far from a stable draft. Moreover, a version without the change tracking would have been more readable		The document is based on ETSI TS 101 456 which is a document used for many years by many countries and many CAs. The track changes were provided on purpose in order to draw the attention of the reader on new elements.
Company 1	0		G	The document is too bound to the EU Directive. It should be more general, in order to be referred to by a forthcoming legislation	The risk is the document becomes superseded just after its issuing.	EN 319 411-2 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 319 411-2, 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.
Company 2 1	0	General	G	Many lists are bulleted, while it is better to have them as numbered lists for better reference		**Agree.** The a) i) 1) hierarchy is now used as far as possible.

Company 2 2	0 Foreword	3rd paragraph	T	This wording can be interpreted as if TS 101 456 has been blindly copied and pasted. Please specify that is has been updated and that updates are referred to in Annex F		**Agree**. The sentence is now completed by “that has been updated according to elements referred to in Annex F.”
Company 2 3	0 Foreword	“National transposition dates”	E	Is “2013” correct?		**Corrected.** Revised to give dates from publication
Company 2 4	1	4th paragraph	E		Please fix singular/plural in “These policy addresses”	**Agree.** Corrected into “These policy requirements address”
Company 1	2.1	References	G	In the TSA policy the CEN docs are referred by the new name/version. It would be nice that the set of policies be harmonized		**Agree.**
Company 2 5	2.2	Item i.6	T	In 2012 a new version was issued of ISO/IEC 27002		**Agree.**
Company 1	3.1	Definitions	G	The term “qualified” should be used in a consistent way in the entire set of policies. Here it refers to the EU Directive but also to a Qualified auditor that was not in the directive. In the TSA policy (QTSP) is clearly stated that Qualified does not refer to law (yet).		**Agree** “recognised” is used now. Qualified auditor appears in CA/B Forum but with a slightly different definition. The draft regulation uses “recognised” but may switch to “certified”: when the document will be updated for the regulation alignment, this term might be adapted accordingly.
Company 2 6	3.1	Definition of “certificate”	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**
Company 3	4.1	4.1	Technical	What is the meaning of the following sentence : “Where a CA systems include a sub-CA as well as a root CA then similarly, the Root CA is responsible for ensuring the sub-CA complies with the these policy requirements unless the sub-CA also acts as		**Partly Agree** These concepts are clarified to the extent of providing technical requirements. The policy requirements however do not enter into legal considerations (e.g. legal structure and links rootCA /

				a root CA for purposes of trust in which it may be required to be independently assessed before inclusion in the trusted list .” what is the relation between : - A CA system and a trust service provider delivering certificates? - A sub-CA and a trust service provide delivering certificates? The concept of AC hierarchy should be explained here? Could root CA and subordinate CA be independent organisations? How can a sub-CA act as a root CA?		subCA) The definitions have been improved (CA, CSP, TSP, Root-CA, Trust Anchor) and the related sentence modified accordingly. CD 2013-662 EU is used as a basis. Section 4.2 has been updated as well.
Company 3	4.2	4.2	Editorial	Sub-CA should be replaced with subordinate CA		**Partly agree** The acronym sub-CA is used a lot in the series, it has been added in the definitions and acronyms.
Company 2 7	4.2 Page 10	1st Paragraph	E		“in which case it may	**Agree**
Company 2 8	4.3	5th bullet “real time service”	T	If this refers to OCSP, then "online" is better, because more often than not an OCSP server updates its data base periodically, i.e. not in "real time". Besides, “online” is more appropriate, recalling the OCSP meaning.		**Agree**
COMPANY 4	4.4.1	1	E	Reference [6], clause 4.3.1 is wrong, because old clause 4.2 is deleted	Change to 4.2.1.	**Agree**
COMPANY 4	4.4.2	1	E	Reference [6], clause 4.3.1 is wrong, because old clause 4.2 is deleted	Change to 4.2.2.	**Agree**
COMPANY 4	4.4.3	1	E	Reference [6], clause 4.3.1 is wrong, because old clause 4.2 is deleted	Change to 4.2.3	**Agree**
COMPANY 4	4.5	Last	E	There seems to be a word missing in the	"The only exception is when the organisation running	**Agree**

				last sentence.	the CA is…."	One of the “is” was incorrect
Company 5	4.5	To avoid any conflicts of interests, the Subscriber and RA organisation entity are separated entities	General	As we see it, a subscriber who wishes to apply for certificates, for example, for its employees, already performs a lot of the tasks of RA, such as identifying subjects, keeping records on them and store documents on the identity of the subjects (eg photocopies of ID). At the end it is the CA and not the RA who has to approve the issuance of such certificates. So we do not see any conflicts of interests. Allowing a subscriber to be its own RA will ease the procedures of issuance and, therefore, to break down barriers in the adoption of electronic signature. Remember, at the end, it is the CA the responsible of approving the issuance of a certificate.	Eliminate paragraph	**Partly agree** The way RA & CA are defined in Sections 3.1 “definitions” and 4.2 considers RA as a sub-entity of the CA. The document does not prevent a CA to delegate part or all RA tasks to a subscriber, but the CA remains responsible for these tasks. To make sure that this case is well covered, we propose: “the only exception is the organisation running all or part of the RA tasks subscribing a certificate for itself or persons identified in association with it (as a subject).”
Company 1	4.5	Subscriber and subject	T,E	Subscriber is not defined, neither in the Definition clause nor in the present one, but it is referred in the clause name and in the		**Reject** The definition section 3.1 clearly states: “For the

				text. Please put a recall to 319401 or defines it in this document		purposes of the present document, the terms and definitions given EN 319 401 [6] apply”
Company 3	4.5	4.5	Editorial	“To avoid any conflicts of interests, the Subscriber and RA organisation entity are separated entities. The only exception is the organisation running the RA is subscribing a certificate for itself (as a subject).” The problem here lies in the fact that RA employees won’t be able to request and obtain a certificate for themselves.	“To avoid any conflicts of interests, the Subscriber and RA organisation entity are separated entities. The only exception is when a member of an organisation running the RA is subscribing a certificate for himself (as a subject).”	**Agree with change**
Company 2 9	4.5		E	Please, add a definition for “subscriber”. A good definition should be taken by deleted text; “who contracts with the certification authority for the issuance of certificates”		**Reject** The definition section 3.1 clearly states: “For the purposes of the present document, the terms and definitions given EN 319 401 [6] apply”
Company 2 10	4.5	“Qualified Signature certificate for natural person”	E	Please add "Request for a " before. It is not the Qualified Signature certificate itself to be signed by the subject. Same comment to the following bulleted item		**Agree** “a certificate can be subscribed” can be interpreted as “a certificate can be signed” (as per Oxford dictionary); this was confusing since only a CA can sign the certificates. The sentence has been clarified as follows: “To request a Qualified Signature certificate for natural person the subscriber is …”
Company 2 11	5.1	1st paragraph	T	1) It is not clear why this definition is repeated here. 2) It would be appreciated to specify this reference [5] in the Definition Clause.	1) Please remove the definition	**1) Agree** 2) Agree
Company 2 12	5.4.3	Item b)	E		Please add “items” before “e) and f).”	**Agree**
Company 2 17	6.2 Page 16	Note 1	E	An extra “1” has been deleted from 19 312		**Corrected**
Company 1	6.2		E	Note it seems pleonastic, since the		**Agree**

				subscriber is clearly present both in d) and f)		=> note deleted
Company 3	6.2	6.2	Editorial	i) the subject's private key has been lost (e.g. by forgetting the PIN number needed to use the key) or stolen; or	i) the subject's private key has been lost (e.g. by forgetting the PIN number needed to use the key) or stolen; or compromised	**Reject** The “or” is a “logical or” with the next items (covering key compromise).
Company 3	6.2	6.2	Editorial	Sentence not understood : “If the subject and subscriber are separate entities, and the subject is a natural person, the subscriber agreement part dedicated to the subject (see clause 4.5 and 7.3.1) shall specify the responsibility of the subject to comply to its obligations and shall a minima include b) c) e) g) h) and i):”		**Agree** **Clarified by** changing into “the part of the subscribed agreement dedicated to …”
Company 2 13	6.2	1st paragraph	E	Shouldn’t “comply to” be “comply with”?		**Agree** Comply “with”
Company 2 14	6.2	Item d)	T	Please specify that in any case algo and key length must be approved by the CA		**Partly agree** It is not the case necessarily that the CA “approves” algorithm. This may be national issue. Rather the acceptable algorithms and key lengths should be laid out in the subscriber agreement. Changed with “as laid out in the subscriber agreement” to item i) and ii).”
Company 2 15	6.2	Item f)	T	Please add somewhere that the CA must ascertain that the subject's keys is generated within the SSCD to be used for signing;		This is covered in 7.3.1 m)
Company 2 16	6.2	Note	E	The Note text is clearly specified at the mentioned items, so why repeating it here?		**Agree** => note deleted

Company 2 18	6.2 Page 16	Item g) ii)	E	The word "potentially" here must refer to both cases: compromise and loss. Please amend		**Agree**
Company 2 19	6.3	2nd paragraph	E		"it shall" is inconsistent with plural (relying parties) Please fix it, for example by replacing "it" with "the relying party"	**Agree**
Company 6	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.	**Reject** Unfortunately the Directive and the Draft Regulation are in contradiction on this particular point. It will be considered in the version issued at the occasion of the publication of the Regulation.
COMPANY 4	7.2.1	f)	T	The requirement about video recording: We see at least two issues: 1) The video should not record typing og security officer passwords etc. 2) Root-CAs are usually long-lived. There is a certain risk that an archived video which is 10 or 20 years old cannot be played or watched.	Consider deleting video recording as a requirement, or at least say that security officers passwords shall not be visible on the recording	**Agree with change** The bullet f) has been re-written
COMPANY 4	7.2.1	f)	T	Last bullet point says that the TSP shall have a report from the qualified auditor. It would perhaps be better if the CA security officer writes the report himself and gets an attestation of correct procedure from the auditor. After all: The security officer is the person that knows the key ceremony script best.	Add as an option that the security officer writes the report and gets an attestation from the auditor.	**Agree with change** The bullet f) has been re-written
Company 1	7.2.1	Note 2	T/E	Reference to TS 102 176-1 is wrong	TS 119 312	**Corrected**
Company 2 20	7.2.1	Unnumbered "Note" after item b)	E	1) Please give this Note a number 2) Please specify "The above applies …" for a better understanding		**Agree** **Agree**
Company 2 22	7.2.1	Item e)	T	Based on our experience please require that between the CA certificate Expiry date and the last certificate signed with the corresponding private key a suitable		**Agree with change** This is considered within NOTE 4 now.

				interval must exist.		
Company 2 23	7.2.2 Page 18	Item f)	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.		**Agree with change** The bullet f) has been re-written
Company 2 21	7.2.2 Page 18	Note 2	E/T		Replace TS 102 176-1 with TS 119 312	**Agree**
Company 2 24	7.2.2 Page 18	Item f)	T	The term “shall” in “the TSP shall record a video” 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. This applies to both CA Root Key generation and subordinate CA Key generation	A "should" would be enough.	**Agree with change** The bullet f) has been re-written
Company 1	7.2.4	Key escrow	T	The CA shall not hold subject private keys once they have been delivered to the subject (commonly called key escrow) (see the Directive 1999/93/EC [i.1], annex II (j)). This clause limits the capability to offer server side signature, where the keys are stored in a HSM kept and managed by a TSP, often a QCSP	The CA shall ensure that the subject private keys are I any moment under the control of the subject	**Reject** Unfortunately the Directive and the Draft Regulation are in contradiction on this particular point. It will be considered in the version issued at the occasion of the publication of the Regulation.
Company 1	7.2.8	Note	T/E	Reference to TS 102 176-1 is wrong	TS 119 312	**Agree**
Company 1	7.2.8	Letter e)	T	This clause limits the capability to offer server side signature, where the keys are stored in a HSM kept and managed by a TSP, often a QCSP		**Reject** Unfortunately the Directive and the Draft Regulation are in contradiction on this particular point. It will be considered in the version issued at the occasion of the publication of the Regulation.
Company 2 25	7.2.8	Note	E/T		Replace TS 102 176-1 with TS 119 312	**Agree**

Company 2 26	7.2.9	2nd Paragraph	T	If the text is hinting to the referred to Directive Annex III, it is absolutely obscure and no linkage is apparent. If instead a secure delivery was meant, then more details are necessary.	For example: "The CA shall ensure that, if it issues a secure user device to the related subject, the issuance and, where applicable, delivery, are carried out in a way to prevent tampering and/or misuse."	**Agree with change**. Conforming to Annex III is more than what the proposition suggests (the key generation deserve care, etc.). The following sentence is proposed: “The CA shall ensure that if it issues a SSCD to the related subject, the issuance and, where applicable, delivery, are carried out in a way that does not infringe any of the requirement from the Directive 1999/93/EC [i.1], annex III.”
Company 6	7.3.1		General	It seems to be assumed that the subscriber or the subject provides all data such as full name, date and place of birth, a national recognized identity number.	It should be stated that data (such as full name) can be retrieved from national databases if applicable within the law in the country.	**Reject**. Unless we misunderstand the request, we believe it is already covered by the text. The document does not specify who provides the data. It just requires evidence on the data (and this can be done through any authorised source as mentioned in the intro of the section). It is however assumed that the request for certificate provided by the subscriber/subject contains a minimal set of information (as per applicable policy), that the subscriber/subject must sign as engagement. It seems logical that the name to be certified is part of this info (and again, nothing prevent to download it from a trusted source).
Company 1	7.3.1	Letter f	T	It’s not clear what do you mean “by physical presence of a person” when the person is a legal one		**Agree and Clarified.** The requirement is to have a physical presence (or equivalent) of a physical person at registration. Text in f) and g) have been clarified for the cases where the subscriber is itself not a natural person.
Company 1	7.3.1	Letter f	T	Note: it is recalled the above-mentioned note 7 but it should not be applicable to a legal person		**Partly agree.** Note 7 applies to legal person (ISO 29115 is not limited to physical persons and fully applicable to legal persons), but note 4 on “birth” does not. Note 4 has been excluded from the recalling note.
Company 1	7.3.1	Letter f	E	Should this note be numbered?		**Agree**
Company 1	7.3.1	Letter g	E	assocaited	Associated	**Corrected.**

Company 1	7.3.1	Letter m	T	How should the proof of possession give evidence of having been generated in a SSCD?		**Rejected.** We understand it may be difficult to implement in absence of procedures discussed between the CA and the customer (e.g. key generation witnessing, audit of key generation process at customer's end, …) but we would like to keep this requirements (it is a requirement since many years already present in ETSI TS 101 456). The CA is free to forbid SSCD preparation by the customer when not in a state to control it.
Company 2 27	7.3.1	Item d)	E	"checked against a natural person" "natural person" is a useless repetition	Please remove "natural person"	**Rejected & clarified.** The requirement is to have the evidences checked against a natural person, physically present, but it is not always necessarily the subject. Proposition: "where the subject is a natural person, evidence of the identity shall be checked against a natural person (the subject or a duly mandated subscriber)…"
Company 2 28	7.3.1	Item d)	E	"the RA validates their genuinity"	This term "genuinity" can be found neither in Merriam Webster nor in Encyclopaedia Britannica. Maybe it must be replaced with "authenticity"	**Agree** "RA validates that the presented evidences appear to be genuine"
Company 2 29	7.3.1	Item d) second bullet	E	"identity number"	"identity document"	**Rejected & clarified** It is meant "number". Clarified by adding "in countries where such numbers are used"
Company 2 30	7.3.1	Item e)	E	"genuinity"	Same as above	**Agree** as above
Company 2 31	7.3.1	Item f)	E	"genuinity"	Same as above	**Agree** as above
Company 2 32	7.3.1	Item g) 2nd bullet	E	"assoaicated"	"associated"	**Agree**
Company 5	7.3.1 d)		General	This subclause should make more clear	To extend NOTE 6 with something	**Agree** An example of evidence checked indirectly against a

				that signing a requests with QES is a mean to fulfil the d) requirement. Indeed, signing a request or application form with QES provides to the RA with the data required and provides evidence that these data have been checked.	similar to: "An example of evidence checked indirectly against a physical person is to sign an electronic application form with QES"	physical person is the use of means which were acquired as the result of an application requiring physical presence and whose unambiguous link with the physical person can be proved (e.g. registration document(s) electronically signed (as per article 5.1 of Directive 1999/93) by a person trusted to have checked the persons' identity in line with the requirements of this clause).
Company 7	7.3.1 d) and NOTE 6 (page 22)		G/T	Evidence of the identity shall be checked either against natural person directly or indirectly using means which provides equivalent assurance to physical presence. Example in NOTE 6 says that it can be documentation which was acquired as the result of application requiring physical presence. We want to draw your attention that the example in NOTE 6 is not adequate. This kind of documentation can be for example (copy of) birth certificate or passport/physical ID-card etc. sent by 3rd person. To verify person based solely on documents might lead to issuance of certificates to the wrong person. This flaw could be avoided when there would be requirement to sign application documents with qualified electronic signature. The other option is to require physical presence in post-issuance i.e. when handing over certificates.	Change 7.3.1 d) and NOTE 6 (page 22) according to the comment.	**Agree**
Company 5	7.3.1, NOTE 10	This agreement	General	It seems this paragraph lacks of specificity. An Electronic Signature should	This agreement may be in electronic form, signed with Qualified Electronic	**Agree with change.** This agreement may be in electronic form, signed with an Advanced Electronic Signature as recognised

		may be in electronic form.		be a requirements We are promote the advantages and use of electronic signature so, let's preach by example	Signature	by applicable legislation.
Company 1	7.3.2		T	Letter c and seems at odds	Remove “or the previous certificate has been revoked” or add, after revoked, “for reason that does not include possible security breaches”	**Disgaree** **It is assumed that this is read as though other requirements in this clause do not also apply. In case of security breach other items also apply including item d.**
Company 8	7.3.3	Letter d second bullet	T	This clause limits the capability to offer server side signature, where the keys are stored in a HSM kept and managed by a TSP, often a QCSP		**Reject** Unfortunately the Directive and the Draft Regulation are in contradiction on this particular point. It will be considered in the version issued at the occasion of the publication of the Regulation.
Company 2 33	7.3.5	Item f)	T	If the CA ensures that provided signature generation application inserts the subject’s certificate in signed document, make all the certificates publicly and internationally available is unuseful, Please, note that this is what generally happen.	Split point f) as follows: f) If the CA does not assure that provided signature generation applications insert the subject’s certificate in each signed document, the information identified in b) above shall be publicly available; g) the information identified in c) above shall be publicly available.	**Party agree.** In general the CA has no power on the signature format. This cannot be a requirement, and ensuring the correct operation of the signature generation application is out of scope. Made it “should” for “b)” shall for “c)” as one still need to have requirements for conforming to the Directive.
Company 6	7.3.6		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”	**Party agree.** There will not be a specific policy for Root CA, but well clearly identified requirements for Root CA. In this case, additional requirements on revocation for CA as current CRL requirements relate to end user certificates.

Company 2 34	7.3.6	Note2 1st bullet	T	The text is not clear, in particular if it is matched with the following example. One subscriber, due to one of its subject's planned cessation from his/her duties, requests for a revocation of this subject's certificate at the end of one month.	Please reword the Note clarifying and taking into account also the case in the side box example.	**Agree** However it seems that it's not the note but the item below that needs clarification.
Company 2 35	7.4.1 Page 27	Editor's note	T	One day as an interval between two consequent CRLs 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.		**Partly agree** Added a note making clear that a CA may give faster process times for certain revocation reasons.
Company 2 36	7.4.1 Page 27	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**
Company 2 37	7.4.1 Page 27	Item g)	T	This practice of issuing a new CRL long before the previous one expires, 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.		**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. The policy states maximum's how a TSP implements, this policy requirement is outside scope.
Company 2 38	7.4.1 Page 27	Item m)	E	Please add RFC 6960 to clause 2.1		**Agree**
Company 2 39	7.4.1 Page 27	Note 6	E	Please add reference to EN 319 412		**Agree**
COMPANY 4	7.4.3		T	Are these roles really needed. (The ones described in 319 401 are.) If it is decided that these roles are needed, a note should	Perhaps delete points a) and b).	**Reject**

				perhaps say that these two roles may be assigned to the same individuals. In addition, there is a fundamental difference between the roles defined in 319 401 which are high privileged security relevant roles, and the ones of this section, to which a large number of individuals will be assigned.		Role registration officer and revocation officer are defined and used in prCEN/TS 419 261 “Security requirements for trustworthy systems managing certificates for electronic signatures”. This TS has been approved for formal vote and is referenced in 411x (under the old reference CEN Workshop Agreement 14167-1) as note in section 7.4.7. Both roles are needed for the operation of a TSP and are indirectly defined in sections ‘subject registration’ and ‘certificate revocation and suspension’.
Company 2 40	7.4.4.	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		**Partly Agree** Added in the requirement c) “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.” The initial item b) says « any person », so it’s up to the TSP to decide how to apply this constraint and whether (and how) it covers authorized person as well, and (2) by adding the new item c) we increase the requirement on the security of the access to the room, including for authorized persons.
Company 2 41	7.4.6	Item a)	T	Please add “and logically”, as pointed out in Note 2	“kept in a physically and logically secure environment”	**Agree** However note 2 seems more oriented toward physical protection
Company 2 42	7.4.8	Item a)	T	Please highlight the need for disaster recovery sites to be remotely located	“stored in safe places, preferably also remote, suitable …”	**Agree**
Company 2 43	7.4.8	Note 1	T	“ISO/IEC 27002 [i.7i.6], clause 10.5.1:” Please check if in ISO/IEC 27002 - 2012 version clause numbering has not changed		**Agree** 10.5.1 replaced by 12.3.
Company 2 44	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.		**Partly agree** Agree include as informative note.

Company 2 45	7.4.11	Item c) 2nd bullet	E/T		“driver’s license number code”	**Partly agree** Driver’s license can have a number or can be a code, depending on the member state of issuance.
Company 2 46	7.4.12	1st Paragraph	E/T	“clause 6.4.12” This clause does not exist in the currently available EN 319 401		It exists but may be only in the version issued for public comments.
Company 6	7.5	Bullet a)	General	The demand for independency will probably pose great challenges to many CA’s.	Consider modifying the demands or ensure proper and timely announcement specifically on these demands.	**Rejected** We had the same requirement in 101456 so this shall not be an issue for existing CAs. However this clause is susceptible to evolve in the version of the document published at the occasion of the Regulation publication.
Company 2 48	8.1	Item c	T	Please specify the maximum interval between two Risk Assessments		**Rejected** 319 401 clause 6.4.1 already gives guidance regarding risk assessment.
Company 2 47	Annex B Page 39		E/T	“line 2 above)...” What is this line 2)		**Agree. Clarified** It is meant that this information can alternatively be provided trough information due in virtue of line 2 of the table…
Company 2 49	Annex C2	Acronym	E	Please add “PDS” to clause 3.2		**Agree**
Company 2 50	Annex E	3rd paragraph	T	“ETSI grants that users of the present document may freely reproduce the check list file identified in this annex …” Pity this check list file is protected from changes so users cannot directly use it ...		**Agree** The idea was to leave it partly free, but it was not implemented yet at the moment of public review, sorry for this inconvenient.
Company 2 51	Annex F		E	“TS 19 312”	“TS 119 312”	**Agree** **Corrected**
Company 2 52	Annex F		E	“Addition of a recommandation and related requirement”	“Addition of a recommendation and related requirement”	**Agree** **Corrected**

Company 2 53	Annex G			Why a few withdrawn documents are listed too?		All withdrawn docs are now removed