Resolution of comment on Draft ETSI EN 319 403 V2.0.6 (2013-09) – 31 May 2014

TSP Conformity Assessment

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	Introduction	Final paragraph	Ed	Suggested change of wording regarding use of NABs	"In accordance with Regulation (EC) No. 765/2008, attestations issued by Conformity Assessment Bodies accredited by a National Accreditation Body can be formally recognised across Europe."	Accepted
B 1	1		General	In our view there is no need to use 'certification' and no harm in using 'assessment'. ISO 17065 also repeatedly uses 'assessment'.	None	No change needed

C 1	1	Scope	editorial	Current text : “The present document specifies requirements and guidance for the assessment of a Trust Service Provider (TSP) through the Conformity assessment against an ETSI document specifying policy and security requirements for a particular class of trust service (e.g. policy requirements for certification authorities issuing qualified certificates as in TS 101 456 [i.3]).”	The present document contains requirements for the competence, consistent operation and impartiality of conformity assessment bodies assessing conformity of Trust Service Provider (TSP) to standardized criteria for the provision of trust services.	Accept with changes It is assumed that proposed new text is given under “current text”. The first paragraph is aligned with ISO 17065. However, it is recognized that it is worth including examples of the criteria. Add after “conformity of Trust Service Provider (TSP) to standardized criteria for the provision of trust services defined as policy requirements such specified in EN 319 401 [i.8] or parts of EN 319 411 [i.2],[i.3].
A 2	1. scope	Requested comment	Ed	To answer the requested comments (in yellow)	It is suggested that it may be best to stick with Assessment of Conformity	No change needed
C 2	2	Normative reference	Technical	The following standard should be updated : ETSI TS 102 042	ETSI EN 319 411-2	Assume propose change to EN 319 411-2 TS 1042 No change the EN now is the relevant document
C 3	2	Informative reference	Technical	The following standard should be updated : ETSI TS 101 456	ETSI EN 319 411-3	No change the EN now is the relevant document
C 4	2	Informative reference	Technical	The following standard should be updated : ETSI TS 102 231 (V3.1.2)	ETSI EN 319 401	No change the EN now is the relevant document

C 5	3	Definition and abbreviations	Editorial	The definition of the technical expert is not clear enough. Does the technical expert belong to the TSP (is he Point of contact for assessors?)?	The definition could state that the technical expert assists the audit team and that he must not, under any circumstances, belong to the TSP.	Rejected This is a requirement not a definition. Already covered by ISO 17065 – clause 6.
D 1	3.1	19	E	Remove definition for "Trust Service status List (TSL)"	Delete definition This definition is only applicable to Annex B – where it is already defined.	Accepted
D 2	3.1	20	E	Remove definition for "trust service status Notification Body (Notification Body)"	Delete definition This definition is only applicable to Annex B – where it is already defined.	Accepted
A 3	4.1.3		te	Are they requirements on where and how the CAB mark shall be utilised? There might be needed as what is certified is a service and not product. Communication shall not be misleading	Consider	Current requirements in 4.1.3 sufficient for moment. For qualified this is an issue for the Notification Body.
A 4	4.2.1		ed	The term "Certification Assessment Body" should be replaced by "Conformity Assessment Body" to be in line with Definitions in Clause 3.1 and in the document.		Accepted
D 3	6.1.2		E	Delete text	None Delete this last clause as there are no requirements in 17065 for 6.1.2! Requirements for 6.1.2.1 and 6.1.2.2 are dealt with in the related clauses.	This is due to confusion over numbering of 6.1.2.1 and 6.1.2.2 not relating to the equivalent 17065 clauses Move 6.1.2.2. Internal resources (except 6.1.2.2.7 Competences for Technical Experts) under 6.2 Resources for evaluation/6.2.1.Internal, Resources . Structure to be aligned with 17065

D 4	6.1.2.1		E	Remove existing text. This does not align with content of 6.1.2.1 in 17065. I cannot see any need for any statement here because 17065 is generic about whatever competencies are required, so if specific competencies are required for Trust Services they would still be covered. So just say that clause 6.1.2.1 from 17065 shall apply.	Replace with "The requirements from ISO/IEC 17065 [1], clause 6.1.2.1 shall apply."	This clause is very confused. It does not relate to the equivalent clause in 17065. If refers forward to clause 7 then 6.1.2.2. Structure to be aligned with 17065
D 5	6.1.2.2		E	Reference to 6.2.1 is incorrect	Change to "6.1.2.2"	See resolution to D 3
B 2	6.1.2.2.4		General	The competence requirements are identical to the current legislation for electronic signatures in the Netherlands, except under (b): we prefer four years instead of three, and two instead of one year, applicable to auditors. Trainees with less experience could be part of the audit team but not in the formal role as auditor.	Change 'three' into 'four', and 'one' into 'two' years of experience for auditors.	Accepted
B 3	6.1.2.2.8		General	For your information: The competence requirements are identical to the current legislation for electronic signatures in the Netherlands	None	No resolution needed. Comment provided for information purposes only.
B 4	6.1.2.2.9		General	For your information: The competence requirements are identical to the current legislation for electronic signatures in the Netherlands	None	No resolution needed. Comment provided for information purposes only.
E 1	6.1.2.2.4	Item a)	E	A less convoluted wording would be appreciated.		Accepted: *Formal academic qualifications or professional training or extensive experience indicating general capability to carry out complex task in an intelligent manner.*
E 2	6.1.2.2.4	Items i), j)	T	These are not to be listed among "skills": they pertain to personality and current and future employment.	Please remove from the list and add to the top paragraph.	keep i) and redraft j) in the way that the auditor should maintain the knowledge and skills by continuous training…

E 3	7.1.1.1	1st para	T	Text: "*The evaluation of the TSP service(s) shall be performed in form of an audit against dedicated TSP audit criteria.*" This text is interpreted as these criteria are defined by the single Conformity Assessment Body. In order to achieve an assessment that is acceptable "cross border", these criteria shall not be defined by the single Conformity Assessment Body.	It is recommended that ETSI or some other standardization organization (at least at EU level), writes down these criteria.	Accepted with modifications: " (e.g. policy requirements as specified in EN 319 401 [i.8] or parts of EN 319 411 [i.2],[i.3"
F 1	7.1.1.1	Paragraph a	Technical	"a) take into account specificities of the type of trusted service to be assessed;". Regarding definition of CA, TSP, Subscriber and Subject it is really important to be more clear in this section and document in general because for example, and essentially, PKI deployment are very different between TSP and in same time can be grouped into some simple concepts as proposed. The idea of this proposition is to avoid to audit all entity of TPS in case of LRA deployment as mentioned below in this table and to set a clear scope in Europe to avoid different audit scenario and cost of audit. There is also a lack of definition and concept that will make very big problem for audit and simply understanding of standard and what to audit for TSP (PKI for example). Actually RFC provide more important definition than ETSI like Registration Authority (RA) that are very important for TSP deployment.	Refer to the proposition below in the section "Proposed definitions for EN and ETSI:" that gives a set of very important definition that are not all in ETSI or EN document and that are very useful in order to be sure to share the same concept on PKI components and to avoid to have to audit thousands of LRA. These propositions are very important to clarify the type of PKI component and to define audit scope of TSP for PKI.	No change: It is not for this standard to set the specific bounds on the type of TSP to be assessed. The body requiring the certification (e.g. supervisory authority./ application provider) should decide what type of service is needed. The rationalised framework and associated guidance documents sets out a list of standards considered appropriate for e-signatures.

C 6	7.1.1.1	Paragraph	Technical	“a) take into account specificities of the type of trusted service to be assessed;”. Regarding definition of CA, TSP, Subscriber and Subject it is really important to be more clear in this section and document in general because for example, and essentially, PKI deployment are very different between TSP and in same time can be grouped into some simple concepts as proposed. The idea of this proposition is to avoid to audit all entity of TPS in case of LRA deployment as mentioned below in this table and to set a clear scope in Europe to avoid different audit scenario and cost of audit. There is also a lack of definition and concept that will make very big problem for audit and simply understanding of standard and what to audit for TSP (PKI for example). Actually RFC provide more important definition than ETSI like Registration Authority (RA) that are very important for TSP deployment.	Refer to the proposition below in the section “Proposed definitions for EN and ETSI:” that gives a set of very important definition that are not all in ETSI or EN document and that are very useful in order to be sure to share the same concept on PKI components and to avoid to have to audit thousands of LRA. These propositions are very important to clarify the type of PKI component and to define audit scope of TSP for PKI.	see above.

F 2	7.1.1.1	Paragraph c	Technical	For the following sentence: “c) be based on standards, normative documents and/or regulations.” I strongly recommend to have a generic audit guidance of criteria like the French example available at the following address: **http://circulaire.legifrance.gouv.fr/pdf/2009/04/cir_1992.pdf** The idea is the following; Europe shall publish a technical audit guide to complete the present methodology guide in order to be sure that: – national accreditation body accredit auditor according same standards of auditing – auditor will audit TSP on the same perimeter and same audit criteria. If not, the most dangerous thing that will happen in Europe is that an auditor accredited by a national accreditation body will audit a TSP with different audit criteria form another country and without the same audit criteria. It means that TSP will be audit with security breach like Diginotar for example that will be a very serious problem if national accreditation body doesn’t share the same audit criteria to conduct assessment and audit of TSP.	Therefore audit technical criteria shall be defined by ETSI and applied by all auditors to audit and to make an audit report. Because, if audit report and audit criteria are not standards, therefore how to consider trust of audit?	Again, this comment doesn’t correspond to this document. EN 319 403 establishes requirements for the CABs to be accredited. It does not include audit methodology or techniques as the French reference does. The rationalised framework and associated guidance documents sets out a list of standards considered appropriate for e-signatures.

C	7.1.1.1	Paragraph	Technical	For the following sentence: “c) be based on standards, normative documents and/or regulations.” I strongly recommend to have a generic audit guidance of criteria like the French example available at the following address: **http://circulaire.legifrance.gouv.fr/pdf/2009/04/cir_1992.pdf** The idea is the following; Europe shall publish a technical audit guide to complete the present methodology guide in order to be sure that: – national accreditation body accredit auditor according same standards of auditing – auditor will audit TSP on the same perimeter and same audit criteria. If not, the most dangerous thing that will happen in Europe is that an auditor accredited by a national accreditation body will audit a TSP with different audit criteria form another country and without the same audit criteria. It means that TSP will be audit with security breach like Diginotar for example that will be a very serious problem if national accreditation body doesn’t share the same audit criteria to conduct assessment and audit of TSP.	Therefore audit technical criteria shall be defined by ETSI and applied by all auditors to audit and to make an audit report. Because, if audit report and audit criteria are not standards, therefore how to consider trust of audit?	Exactly the same comment as F 2. Suggest the same resolution
E 4	7.1.1.2	1st para	T	Specifying “…examine the structure, policies, procedures, practices, management, and operation of the TSP …” does not suffice.	Please specify “related logs/audit trails and records” too.	No change This is detailed requirements for examining the operation of the TSP and its implementation as addressed by the relevant criteria which is described by the second half of this document
D 6	7.1.1.2.2	(b)	E	(a) refers to auditors and technical experts but (b) only refers to auditors	There does not seem to be any reason to exclude the monitoring of the performance of technical experts. Add “and technical experts” to (b)	Requirements of the audit team are already covered in 7.1.1.2.1. This clause should just refer to technical experts

F 3	7.1.1.3 and 7.4.1	Paragraph	Technical	“The Conformity Assessment Body's audit procedures shall not presuppose a particular manner of implementation of a trust service or a particular format for documentation and records.” (7.1.1.3) and “The audit team shall audit the trust services of the TSP covered by the defined scope against all applicable certification requirements. The Conformity Assessment Body shall ensure that the scope and boundaries of the trust service of the TSP are clearly defined in terms of the characteristics of the business, the organization, facilities, assets and technology.” Therefore according first remark made in this table, it is important to have a clear type of scope that auditor is supposed to find in TSP that provides PKI services.	All TSP components SHALL be audited each year for CA by external auditor. RA is audited by external auditor each 3 years and every year by internal audit performed by CA (PKI Trust Provider). If external auditor has a doubt about RA and/or LRA auditor shall audit RA and sample of LRA to confirm the findings.”. When RA uses LRA (means there is a contract between them) then RA shall also be audited for its PKI services and LRA shall be audited using small sample of LRA but audit has to be conducted by CA (PKI Trust Provider).	No change 1) Requirements for internal audit and sub-contractors is addressed in EN 319 401 clause 6.4.1 as part of the TSP’s security management system and handling. 2) The current TSP standards (EN 319 411 etc) do not require a specific division of responsibilities between CA and RA / LRA. The audit is against the whole system. The internal structure of functions within a TSP will depend on the service. 3) Clause 7.4.3 addresses multiple site audit which can be applied to remote RA services 4) Given the potential variations of TSP implementation it is left to auditor to detail the specific requirements of multi-site sampling. 5) In line with ISO 17021 a full audit is required every 3 years with annual surveillance audit. 6) Could add informative reference to 319 401 clause 6.4.1 to 7.4.3.1 b) and possibly add requirement to 401 6.4.1 adding requirement for annual review of policies and their application.

C	7.1.1.3 and 7.4.1	Paragraph	Technical	"The Conformity Assessment Body's audit procedures shall not presuppose a particular manner of implementation of a trust service or a particular format for documentation and records." (7.1.1.3) and "The audit team shall audit the trust services of the TSP covered by the defined scope against all applicable certification requirements. The Conformity Assessment Body shall ensure that the scope and boundaries of the trust service of the TSP are clearly defined in terms of the characteristics of the business, the organization, facilities, assets and technology."	All TSP components SHALL be audited each year for CA by external auditor. RA is audited by external auditor each 3 years and every year by internal audit performed by CA (PKI Trust Provider). If external auditor has a doubt about RA and/or LRA auditor shall audit RA and sample of LRA to confirm the findings.". When RA uses LRA (means there is a contract between them) then RA shall also be audited for its PKI services and LRA shall be audited using small sample of LRA but audit has to be conducted by CA (PKI Trust Provider).	Exactly the same comment as F 2. Suggest the same resolution
B 5	7.1.1.3		General	A specification (such as: areas assessed, audit team staff, testing procedures, evidence observed, sites visited, findings, detailed description of evidence for non-conformities) of the contents of the report that is send to the TSP is missing.	Add specification for contents of the audit report that is send to the TSP.	No change The requirements on the content of the audit report is addressed in 7.4.4
B 6	7.1.1.3		General	For supervisory bodies it is very helpful if all testing procedures performed are included in the report that is send to the TSP.	Make the inclusion of testing procedures an obligation for the audit report to the TSP.	Agree with changes: Requirement to specify audit methodology covered in 7.4.4.1 d) suggest add after "methodology employed including sampling methodology" " and test procudures.
B 7	7.1.1.3		General	For our work as supervisory body it would be helpful if the audit report that the CAB sends to the TSP, is also submitted to the supervisory body as well.	Add requirement that the CAB sends the audit report in a secure way (including the certification decision) to both the TSP and the Supervisory Body.	Notification is out of scope
E 5	7.1.1.3	2nd para	E	Sentence "The plan for and the date of the audit shall be agreed to with the TSP." should be moved on top.		Agree (see also D 8) Paragraph move to be 1st paragraph of clause

E 6	7.1.1.3	3rd para	E	At the end of paragraph it should be better to mention ETSI EN 319 401	Please add at the end: "… standard(s) *such as ETSI EN 319 401."*	Accepted with mod
D 7	7.1.1.3	(b)	E	(a)(1) refers to 'particular certification requirements' but (b) refers to 'all of the certification requirements'. What is the difference?	Use same description in both cases.	Agree wording should be consistent. In 7.1.1.3 a 1) change "with the particular certification requirements." To "with all the policy requirements." b) change all of the certification requirements to "all of the policy requirements." (Also check consistent terminology throughout document Policy Requirements / Certification Requirements / Audit criteria -> Policy requirements.)
D 8	7.1.1.3	2nd para	E	It would read better if this paragraph was first i.e. planning when the audit will occur before talking about meeting client prior to leaving premises!	Swap order of first two paragraphs	Agree – E 5
D 9	7.1.1.3	3rd para	E	If allowance is made for using output from internal audits, it would seem reasonable to have a similar provision to take account of external audits as well.	Insert a paragraph that requires the CAB to have procedures in place that are able to verify whether any existing audit certifications exist that can be taken into account.	Agree with changes This need not be an internal audit, can also make use of external certifications. In 3rd paragraph remove "internal". Add extra paragraph That CAB may take into account existing audit certifications made known to the auditors. Don't think it necessary for CAB to look for this. The TSP should be able to inform the CAB auditors of any relevant audit.

D 10	7.1.1.3	3rd para	E	Since the list of '"policy requirements" standards' will grow and not all will be applicable to every audit there should be a mechanism whereby all relying parties can easily understand which were used for a particular audit.	Perhaps it should be a mandatory part of the Certification Scope statement.	Agree Suggest part of the audit report. (Do not specify any requirements on the certification report.) Update 7.4.4.1 to include a) the standard(s) against which the audit is carried out.
E 7	7.3.1	Title	T	The title is "7.3.1 Contract review". Which contract?	Which contract: that between the TSP and the Conformity Assessment Body or those between the TSP and its clients? If the first only applies, it is necessary to envisage a review also of contracts between TSP and its clients, to prevent the TSP from "cheating" with its, possibly unaware, clients.	Agree – It is unclear what the purpose of this clause. Which contract? I can't relate this to 17065 requirements. Needs rewording. Should ensure that auditor does not accept any application for which is not competent or otherwise unable to carry out audit.
E 8	7.3.1		T	The term "client" is used. It is not clear if "client" refers to the TSP clients or to the being Audited TSPs.	It is not clear if "client" refers to the TSP clients or to the being Audited TSPs, in which case "Audited TSP" is better: "client" might imply that a payment is due. If the first case applies, please specify "TSP client".	Client is defined 17065 Add clarification that in this case client is TSP. See also comment above
D 11	7.3.1	1st para	E	What is meant by "... each relevant sector ..."?	As I do not know which sectors are being referred to and the term is not used anywhere else in the document I cannot propose any specific change.	Accepted with mods "of the requirements of each relevant trust service prior…."
D 12	7.3.1	1st para, (b)	E	It is not clear what is meant by using the verb "to certify" in an intransitive way. One normally 'certifies' something.	Replace "to certify" by "to complete the certification process" Assuming this was what was the intent!	Accepted with modifications "b) define the competencies needed in the Conformity Assessment Body to assess the trust service (eg. identified activities, security risks, vulnerabilities, etc.)

D 13	7.3.1	1st para, (b)	E	The last half of this sentence is very poorly written and punctuated.	Replace with “in relation to the identified activities, and trust services of the TSP and the related security risks, vulnerabilities and impacts on the TSP”	Superseeded. See D 12
E 9	7.4.2.1		T	Same as in comment as in E 6		There may be confusion here between “policies and procedures of the CAB and audit team”, and those of the TSP. Suggest update as in quotes above.
E 10	7.4.3.2	Item b)	T	To the 10 listed items please add another one.	Please add something like: “sites under separate companies”. Free access of auditors to these “lower level” independent sites must be assured and this is to be addressed both in the auditing contract and in the intercompany agreements between TSPs and “subject” sites owners.	Accepted “whether the site is operated by a sub-contractor or other external organisation.”
A 5	7.4.3.2.e		te	In some TSP programs the sampling might be very different based on profiles (a profile presents characteristics similar and representative of a class of system). As a consequence, sampling might be important and the surveillance program might not cover all site in a reasonable time (but with no risk in this case this would not be added value)	Delete e)	Keep the assumption that all sites are covered, but allow discretion of auditor. Add “all sites of the TSP operations unless it can be demonstrated that this does not impact on the results of the audit. Change “organisation” to “operations”, as it is thos sites that provide the TSP function not parts of the organisations outside its trust service operations (e.g. administrative offices).
B 8	7.4.3.2	c	General	We believe the non-selective part should be specified.	We prefer that at least 25% of the sample should be selected at random. Currently that is the requirement in the Dutch TTP.NL scheme.	Rejected. The sampling has to be based on the judgement of the auditors with justification

B 9	7.4.3.2		General	A specification of the minimum sample size would be helpful.	Please take into consideration the following specification: sample size should be at least the square root of the number of sites, rounded up to a whole number. Currently that is the requirement in the Dutch TTP.NL scheme. The auditor may use a larger sample size if the risks and circumstances require	Rejected. The sampling has to be based on the judgement of the auditors with justification.
E 11	7.4.3.2	Item f)	T	It would be illogical to impose such corrective actions to sites where the non-conformity is not applicable. For making it better understood: an irregularity in keeping electronic records would not apply to offices storing solely paper documents.	Please add at the end: "… organisation likely affected by the same non-conformity".	"Likely" is not very specific. Suggest: "parts of the TSP operations which may be impacted by the same non-conformity."
B 10	7.4.4		General	As we understand the audit report in this section is for internal use of the CAB and is not the same audit report that is send to the TSP.	The term 'audit report' might need clarification, it could either be the audit report from the audit team to the CAB, or the audit report that the CAB sends to the TSP.	It is intended to be the same. To clarify. Clarify that this audit report provided to the TSP and any other party which has a legal reason for viewing the report (e.g. supervisory body).
E 12	7.4.5.1	1st para	T	TSP's subcontractors' sites must be subject to audit.	Please modify as follows: "…including provision for examining documentation and the access to all areas, , including subcontractors' ones,…"	Agree " … access to all areas, including those of sub-contractors,
C	7.4.5.1	General preparations for the initial audit	Technical	Documents mentioned here (certificate policy, certification practice statement) suggest that the TSP is in fact a CSP (Certification Service Provider). Could you confirm that other types of policies are required, depending on the type of assessed TSP/TASP?		No change This is addressed in EN 319 401 and other associated standards.
D 14	7.4.5.2	3rd para	E	Conduction usually refers to heat or electricity!	Replace 'conduction of' by 'conducting the'	Accepted
D 15	7.4.5.2	6th para, Stage 1	E	The term "TSP audited services system documentation" is very clumsy and not immediately comprehensible.	Replace with "the system documentation of the TSP service to be audited"	Accepted

D 16	7.4.5.2	6th para, Stage 1	E	"initiation notification" refers to the special case discussed in Annex B and is not a generic requirement for all certifications	Should this process refer to 9.2.3.1 of ISO 17021 [i.6] instead? Replace "initiation notification" with "Application process"	Accepted
D 17	7.4.5.2	6th para, Stage 1	E	Should be 'at this stage' not 'in this stage'	Replace "at the TSP's site in this stage" with "at the TSP's site at this stage" the TSP audited services system documentation	Accepted
D 18	7.4.5.2	6th para, Stage 1	G	Given that Stage 1 refers to observations made at the TSP's site, why is there an apparent distinction from Stage 2 as being the 'on-site' stage	If Stage 1 is indeed not supposed to require on-site observations, why is reference made to them here?	Accepted Change "observations made at the TSP's site in this stage" to To "observations made from the review of documentation and other information obtained at this stage"
D 19	7.4.5.2	8th para	E	Since the service may not be operational at stage 1, it should be clear that this requirement relates to the Stage 2 audit	Replace "prior to commencement of the audit" by "prior to commencement of the Stage 2 audit" Very often a service cannot be operational until a Relying Party contracts for it, but they might only contract for a service that has the relevant certification. This catch-22 is normally resolved by allowing a service to be operational (perhaps in a limited sense) following a successful Stage 1 audit report.	Accepted
E 13	7.4.5.3.1	Item a)	T	Where subcontractors are involved, this audit phase should ascertain if the agreement between the parties is satisfactory, i.e. if it allows the TSP sufficient control on the subcontractors' activities.	Please take into account assessment of such contracts too	No change Covered by EN 319 401 in several places including 6.5 f)
E 14	7.4.5.3.1	Item b)	T	These documents must give way to no misunderstanding. For instance, if one policy is badly written, bordering incomprehensibility, it would be meaningless to proceed to phase 2, since TSP officers would likely have misunderstood it.	Please add at the end "… and, where applicable, assessment of the documents comprehensibility".	No change This is just one aspect that should be covered by document review. It h) already gives recommendations – clearly if the documents cannot be understood then cannot cofirm whether compliant.

E 15	7.4.5.3.1	Item f)	E	The term “clarification” seems ill fit here	Please replace “clarification of nonconformities” with “details on nonconformities”	It is standard terminology, Keep the current text.
C	7.4.5.4	Stage 2 audit	Technical	« This stage shall always take place at the site(s) of the TSP » The word is, in the previous standard has been replaced with "shall". This replacement suggests that "stage 1" validation is required before stage 2.	Il stage 1 validation is not required before entering stage 2, the text should be set to « This stage always takes place at the site(s) of the TSP »	No change This is in line with ISO 17021
B 11	7.6		Editorial		‘Notification Body’ should be replaced by ‘Certification Body’	Accepted with mods
D 20	7.6		E	Production of a report for a Notification Body is not a generic requirement but particular to the kind of Certification Scheme discussed in Annex B	Delete all text after “The requirements from ISO/IEC 17065 [1] clause 7.6 shall apply.”	Rejected Suggest also identify the specify standard to which compliance is checked.(see earlier comment from D)
B 12	7.6		General	There should be period specified within major non-conformities should be solved.	Major non-conformities should be solved (or corrected in such way that the CAB lowers the non-conformity to minor) within the time limit required by the CAB, but at least within three months, and assessed with a follow-up audit by the CAB.	Agree with changes. Put in 3 months as guidance.
C	7.6	Certification decision	Editorial	Details on time limits related to each non-compliance type should be mentioned in this section (some time limits may already be defined in 17065)		See above
D 21	7.6	2nd para	E	Grammar	Replace “conditioned to” by “conditional upon” Note, this assumes that text will move to Annex B.	Agree with grammar correction. Disagree with moving to annex B. This is not dependent on how the result is adopted. .

D 22	7.6	2nd para	E	Grammar	Replace "... within a determined delay in function of the type and criticality ..." by "... within a stated time-frame dependent on the type and criticality ..." Note, this assumes that text will move to Annex B.	Agree with grammar correction. Disagree with moving to annex B.
A 6	7.9.1	1st para and 2nd para	te	The annually frequency for all sites is too heavy . How does it coordinates with the self declaration in second §? Bothe are necessary, one of them?	Reconsider	No change – see earlier discussion The surveillance audit need not require visits all sites. The stage 1 & 2 full audit only applies to recertification The proposed cycle is based upon 17021 clause 9.1.1.2 and is widely accepted Suggest need to clarify – copy 9.1.1.2 from 17021.
B 13	7.9.1		General	As a supervisory body, we would prefer a full certification audit every year. Acceptable but less preferable is a recertification audit every three years with yearly surveillance audits (so a cycle of a full [re]certification audit, followed by surveillance audits after one and two years).	Yearly full certification audit.	No change (see above)
E 16	7.9.1	1st para	E	Sentence "There should be a period of no greater than of one year for periodic surveillance."	Please remove "of"	Accepted
E 17	7.9.1	1st para	T	Sentence "There should be a period of no greater than ~~of~~ one year for periodic surveillance." Please take into account that, in addition to "technical provisions" exists legislation too.	Please add: "in some cases this is subject to the applicable legislation."	Rejected Requirements of applicable legislation should always apply. If we are not aligned with any EU regulations then we will need to adjust.

E 18	Annex A	Item b)	T	Refinement of “conflicts of interest”	It might be useful to specify that any person involved in auditing one organization should not have had work relationships in the previous two years, nor he/she should have any such relation in the following two years.	The aim is clear but “work relationship” is probably too ambiguous. An expert may be involved in advising a TSP, but should not have been employed in operations See earlier comment by C 5 – conflict of interest covered by 17065 clause 6
B 14	Annex B		General	In our view this Annex should not be part of this European Norm. Firstly it is informative. Secondly the way supervision is done is not relevant for the requirements of CABs. Thirdly, these models could change with the publication of the new regulation.	Remove Annex B	No change – useful informative text ?? remove to separate TR which can be updated once regulation has been agreed
C		Annex B	Editorial	Annex B (informative): Why is annex B only informative? The notification body is only mentioned in this annex. This body plays or could play an important role here. The European Co-operation for Accreditation (EA) is not defined. The form of the "Application Trust Information" could be specified here (and the trusted List as well?)		No change This is informative as it addresses issues outside the scope of the document.
D 23	Annex B		G	This needs to wait until the agreed text for the regulation is published as I understand there have been changes to the initial draft that differ from the detail written here.		Leave as is – may need to revise at a later stage.

B 15	B.1.1	B.1	General	There is no Supervisory Body in the diagram. The audit report should go to the TSP, which in turn submits it to the Supervisory Body. The Supervisory Body then sends a notification to the Notification Body if the trusted list needs updating. The SB makes the decision about TSP's status in the trusted list. A CAB's report is not the only way to change the status on the trusted list. For example, security incidents or audits by the Supervisory Body could also lead to changes in TSP's status in the trusted list.	Change diagram.	Trust Service Status Notification Body is in fact the Supervisory Body. See definition: trust service status Notification Body (Notification Body): body which issues a trust service status list (or lists) based on the results of conformity assessment of a Trust Service Provider Consider diagram clarification Agree – regulation requires TSP to provide audit report.
E 19	General		T	We fear that this document will not be useful with the adoption of Regulation eIDAS. We believe better wait till April, i.e. after the Regulation approval by the EU Parliament, and revise it on the basis of the Regulation. Currently contains several elements in opposition to the Regulation. Alternatively, it is suggested to remove any references to the models, notification Body, TSL, Supervisory body and Scheme operator. By doing so, will be the implementation acts of the Commission to refer to this standard.		This document is aligned with the Regulation as approved in the European Parliament
E 20	Introduction	4th paragraph	E		"ISO/IEC 17065 [1] but follows its document"	Rejected
E 21	Introduction	5th paragraph	E	"One principle aim of the present document …" "principle" is not an adjective, but a substantive.		No proposal
E 22	6.2.1.4	Item b)	E	"The values in brackets shall apply for lead auditors;" Which brackets?		Accepted

E 23	7.4.3.2	Item f)	E	Double full stops		Accepted
E 24	Figure B.2		E/T	Reference to ETSI TS 101 456 should be updated		Accepted
A 5	3.2		Ed	there is no need to have some ABs acronyms developed (and not all) : they appear in note 3 in annex B 1.2. and there is a link to EA which is sufficient for understanding	Remove the abbreviaztion references to DAkkS, ENAC, UKAS as these are not necessary in this list	Accepted
A 6	6.1	1 title (and also in the Contents	Ed	Certification Assessment body has been removed from the text and replaced by Conformity assessment body	replace “Certification Assessment Body personnel” by “Conformity Assessment Body personnel	Accepted
A 7	7	Varions (see text)	Ed	- In some occurrences the term “assessment” should be replaced by “audit” : o	7.4.5.2 end of § ”stage1” : “a plan for conducting stage 2 (on-site) assessment audit” 7.4.5.3.1 last § : “The Conformity Assessment Body shall make the TSP aware of assessment audit stage 2 planning and of the further types of information and records that may be required for detailed verification during audit stage 2. Annex A - first sentence “Auditors deployed for performing TSP assessments audits should observe a Code of Conduct fulfilling at least the following:”, §d) “other information obtained in the course of an assessment audit” Annex B1.1. (first sentence)	Accepted

A 8	Figure B1		Ed	Suggested for clarity	The arrow between the notification body and the TSP should be both ways, There should be an arrow from CAB to TSP for the assessment	Accepted

F

Many of the concepts defined below are defined in EN 319 401 and 411.

"Proposed definitions for EN and ETSI:

PKI trust service provider: Legal person which provides PKI services (registration, subject key pair management, token personalization, certificate delivery, revocation, suspension, publication and renewal). PKI trust provider deploys entity that CA, RA and TSP deploy PKI services according organization defined by TSP Management body.

Certification Authority (or CA) means one of the Public Key Infrastructure (PKI) components that issues and revokes Certificates upon request by the Registration Authority and manages them throughout their life cycle in accordance with the rules set out in its Certificate Policy (CP) and the Citification Practice Statement. In most PKI deployment PKI Trust Provider is the same legal person as CA and same vocabulary is used to identify CA and PKI Trust provider. In the same time CA is viewed as the technical means used to sign certificate and CRL and to validate certificate and CRL signature. It means that one PKI Trust provider can have several different CA(s).

Registration Authority (or RA) means one of the PKI components approved by the TSP to use a CA and whose role is to; identify and authenticate the Local Registration Authority, the Subscriber and the Subject, the Subscriber's and Subject's Legal Entity or, as appropriate, the Trusted Agent designated by the latter, register certificate requests for the issue and revocation request and deliver token and certificate. The Registration Authority shall implement identification and authentication procedures in accordance with the rules of the Certification Policy, the related CPS and the certificate management procedures laid out by PKI Trust Provider.

When the RA is a legal person different from TSP as CA, then a contract SHALL be signed between RA's legal entity and CA's legal entity. The contract SHALL describe at least the relation between RA and CA, PKI services delivered by the RA, audit performed on the RA and RA obligations regarding CP rules and PKI service deployed by RA.

Local Registration Authority (or LRA) means one of the PKI components approved by the RA and whose role is to provide some PKI services delegated by RA such as; identify and authenticate the Local Registration Authority, the Subscriber and the Subject, the Subscriber's and Subject's Legal Entity or, as appropriate, the Trusted Agent designated by the latter, register certificate requests for the issue and revocation request and deliver token and certificate. The LRA shall implement identification and authentication procedures in accordance with the rules of the Certification Policy, the related CPS and the certificate management procedures laid out by PKI Trust Provider.

When the LRA is a legal person different from RA, then a contract SHALL be signed between RA's legal entity and LRA's legal entity. The contract SHALL describe at least the relation between LRA and RA, PKI services delivered by the LRA, audit performed on the LRA and LRA obligations regarding CP rules and PKI service deployed by LRA.

Certificate application: means a signed Form(s) for Certificates for a Subject submitted by a Subscriber and then verified by the RA and/or LRA before used for certificate issuance. For physical person, a certificate application is a form containing information to produce certificate and also the legal terms of agreement with CA as requested by ETSI and signed by Subscriber (Person in Organization authorized to commit on behalf of the Organization, but not necessarily CEO of Organization, and who can be contacted for verification purpose) and Subject. For device, application is a form containing information to produce certificate and also the legal terms of agreement with CA as requested by ETSI and signed by Subscriber (Person in Organization, that owns FQDN or application referenced in CN of Subject field, authorized to commit on behalf of the Organization, but not necessarily CEO of Organization, and who can be contacted for verification purpose) and by the technical contact in charge of the device and key pair and CSR associated to the certificate. RA and/or LRA shall have evidence that for Professional identity, Subject and Subscriber are linked to the Organization. For physical person for personal identity, Subscriber and Subject are mixed and there is only one signature.

Organization: means a legal person indicated in the Certificate Request to be included in the field "O" of the Subject's DN to use certificate as a Professional Identity. Subject's DN can have the name of a legal person in the field "O" if only and only if the Subject is binding by contract to the legal person who's name appears in Subject's DN and if certificate request is approved by Subscriber of the Organization.

Professional Identity: means the identity created using the information collected by the RA and/or LRA from the Certificate request and set in the Subject's DN. This identity shall be used to authenticate the Subject as a physical person, using its name and first name set in the field "CN" of the Subject's DN, and her/his association to the Organization whose name appears in the Subject's DN in the field "O". If necessary, this identity may also be used to authenticate the professional title of the Subject in the Organization (field Title of DN).

Personal identity: means the identity created using the information collected by the RA and/or LRA from the Certificate request and set in the Subject's DN. This identity shall be used to authenticate the Subject as a physical person using its name and first name set in the field "CN", for example, of the Subject's DN and the country of the Subject.

Subscriber's agreement

The most important is the signed Subscriber's agreement that have to be collected by PKI Trust Provided either by CA or by RA or by LRA. Whatever the legal person which collect this agreement, the content of the agreement shall be approved by PKI Trust Provider in order to be sure that all requirements set in ETSI document regarding agreements content are fulfilled by the CA, RA or LRA which proposed this agreement to be signed to the Subscriber.".

C "Proposed definitions for EN and ETSI:

PKI trust service provider: Legal person which provides PKI services (registration, subject key pair management, token personalization, certificate delivery, revocation, suspension, publication and renewal). PKI trust provider deploys entity that CA, RA and TSP deploy PKI services according organization defined by TSP Management body.

Certification Authority (or CA) means one of the Public Key Infrastructure (PKI) components that issues and revokes Certificates upon request by the Registration Authority and manages them throughout their life cycle in accordance with the rules set out in its Certificate Policy (CP) and the Citification Practice Statement. In most PKI deployment PKI Trust Provider is the same legal person as CA and same vocabulary is used to identify CA and PKI Trust provider. In the same time CA is viewed as the technical means used to sign certificate and CRL and to validate certificate and CRL signature. It means that one PKI Trust provider can have several different CA(s).

Registration Authority (or RA) means one of the PKI components approved by the TSP to use a CA and whose role is to; identify and authenticate the Local Registration Authority, the Subscriber and the Subject, the Subscriber's and Subject's Legal Entity or, as appropriate, the Trusted Agent designated by the latter, register certificate requests for the issue and revocation request and deliver token and certificate. The Registration Authority shall implement identification and authentication procedures in accordance with the rules of the Certification Policy, the related CPS and the certificate management procedures laid out by PKI Trust Provider.

When the RA is a legal person different from TSP as CA, then a contract SHALL be signed between RA's legal entity and CA's legal entity. The contract SHALL describe at least the relation between RA and CA, PKI services delivered by the RA, audit performed on the RA and RA obligations regarding CP rules and PKI service deployed by RA.

Local Registration Authority (or LRA) means one of the PKI components approved by the RA and whose role is to provide some PKI services delegated by RA such as; identify and authenticate the Local Registration Authority, the Subscriber and the Subject, the Subscriber's and Subject's Legal Entity or, as appropriate, the Trusted Agent designated by the latter, register certificate requests for the issue and revocation request and deliver token and certificate. The LRA shall implement identification and authentication procedures in accordance with the rules of the Certification Policy, the related CPS and the certificate management procedures laid out by PKI Trust Provider.

When the LRA is a legal person different from RA, then a contract SHALL be signed between RA's legal entity and LRA's legal entity. The contract SHALL describe at least the relation between LRA and RA, PKI services delivered by the LRA, audit performed on the LRA and LRA obligations regarding CP rules and PKI service deployed by LRA.

Certificate application: means a signed Form(s) for Certificates for a Subject submitted by a Subscriber and then verified by the RA and/or LRA before used for certificate issuance. For physical person, a certificate application is a form containing information to produce certificate and also the legal terms of agreement with CA as requested by ETSI and signed by Subscriber (Person in Organization authorized to commit on behalf of the Organization, but not necessarily CEO of Organization, and who can be contacted for verification purpose) and Subject. For device, application is a form containing information to produce certificate and also the legal terms of agreement with CA as requested by ETSI and signed by Subscriber (Person in Organization, that owns FQDN or application referenced in CN of Subject field, authorized to commit on behalf of the Organization, but not necessarily CEO of Organization, and who can be contacted for verification purpose) and by the technical contact in charge of the device and key pair and CSR associated to the certificate. RA and/or LRA shall have evidence that for Professional identity, Subject and Subscriber are linked to the Organization. For physical person for personal identity, Subscriber and Subject are mixed and there is only one signature.

Organization: means a legal person indicated in the Certificate Request to be included in the field "O" of the Subject's DN to use certificate as a Professional Identity. Subject's DN can have the name of a legal person in the field "O" if only and only if the Subject is binding by contract to the legal person who's name appears in Subject's DN and if certificate request is approved by Subscriber of the Organization.

Professional Identity: means the identity created using the information collected by the RA and/or LRA from the Certificate request and set in the Subject's DN. This identity shall be used to authenticate the Subject as a physical person, using its name and first name set in the field "CN" of the Subject's DN, and her/his association to the Organization whose name appears in the Subject's DN in the field "O". If necessary, this identity may also be used to authenticate the professional title of the Subject in the Organization (field Title of DN).

Personal identity: means the identity created using the information collected by the RA and/or LRA from the Certificate request and set in the Subject's DN. This identity shall be used to authenticate the Subject as a physical person using its name and first name set in the field "CN", for example, of the Subject's DN and the country of the Subject.

Subscriber's agreement

The most important is the signed Subscriber's agreement that have to be collected by PKI Trust Provided either by CA or by RA or by LRA. Whatever the legal person which collect this agreement, the content of the agreement shall be approved by PKI Trust Provider in order to be sure that all requirements set in ETSI document regarding agreements content are fulfilled by the CA, RA or LRA which proposed this agreement to be signed to the Subscriber.".