

Public Review: resolution of public comments on Draft ETSI EN 319 401 V1.1.9

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

Organization name	Clause/Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted
A	2	2.2	General	Informative references should include RFC 3647. This RFC is an internationally recognized and utilized template for expressing policy and practice for issuers of X.509 certificates. The requirements published in Regulation (EU) No 910/2014 relative to Qualified Certificates should be aligned with the RFC 3647 template to enable TSPs to ensure full compliance and to enable trust mapping across TSPs.	Include the RFC Clause/Subclause/Paragraph number in parentheses next to each Clause/Subclause/Paragraph in this document. Where this document introduces new requirements that do not appear in RFC 3647, note that fact as well. Absent this, early notice of the presence of a mapping to the RFC should appear in Clause 1, Scope.	This is CA specific. No change
B	7.1.1	b)	General	There is no obligation to contract for TSPs	“should” instead of “shall”	No change There is an already an obligation to produce terms and conditions (see 6.2). Contracts required depend on trust service.
B	7.1.1	Note 1	Editorial	Clause 6.1 is about the initialization and control of the implementation and operation of information security within the organization and not about the liability of the organization	The reference should be adjusted	Accepted – reference removed as no direct guidance on organisation reliability
B	7.2	Notes 4 to 6	Editorial	Clause 7.2.1 is about management responsibility and not about job descriptions or procedures of personnel	The references should be adjusted	Suggest reference 27002 7.2.1 for further guidance on management responsibilities in stablishing roles and responsibilities.
B	7.2	i)	General	The roles of System Administrator and Operator shall distinct from	Add Application Administrator role	Additional application specific roles depends on application. E.g. 411

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted
				the role of the Application Administrator		includes Registration Officers and Revocation Officers Note added indicating additional application specific roles may be required for particular trust services.
B	7.4	b)	General	The administration of the user access is usually carried out by a trusted role and not by the “TSP”. Furthermore, administration of user access shall not include auditing.		No change: It is for the TSP procedures who looks after access management. Accept remove auditing.
C	7.8	e)	Technical	The requirement of separate rooms for test platform and production platform may cause issues in relation to pre-production test environments where part of the tests is related to the security of the production platform.	Pre-production test environment should be excluded from requirement e).	Accept with changes: Re-word that production should be separate from other environments not concerned with live operations (e.g development).
B	7.9.1	g) Note 2	Editorial	Clause 16 is about the management of information security incidents and improvements in general and contains no guidance for the review of audit logs	The reference should be adjusted Should be “NOTE 3”	Accepted
D	7.9.2		G	Clause 7.9.2 Collection of evidence could be separate subclause under 7 TSP management and operation, since this part is not relevant only to incident handling process. In ETSI EN 319 411-1 and 2 it is separate clause (7.5.11 in both).	Clause 7.9.2 Collection of evidence could be separate subclause under clause 7 TSP management and operation.	Accepted

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted
B	7.11	b)	General	<p>The subscribers may need time for saving data stored by the TSP. Therefore, the TSP shall not be allowed to terminate its services immediately.</p> <p>The TSP should be required to try to transfer the service to another provider if possible.</p>		<p>No change – The text already includes requirements for “maintaining information required for evidence”. See also below.</p> <p>No change: 7.11 b iii) already requires that essential evidence is saved before termination.</p> <p>Accept with changes, this is a commercial issue and may well not be possible and so can only be informative. “Note: Where possible TSP should make arrangements to transfer provision of trust services for its existing customers to another TSP.”</p>