Public Review: resolution of public comments on Draft ETSI EN 319 421 V0.0.6

Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Electronic Time-Stamps

Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted
Introduction	**3**	**General**	**The term "digital signature", used together with "electronic signature", is confusing: "In order to verify an electronic signature, it can be necessary to prove that the digital signature from the signer was applied when the signer's certificate was valid."**	**The proposal is to simplify the sentence: "In order to verify an electronic signature, it can be necessary to prove that the signature from the signer was applied when the signer's certificate was valid."**	**The only instance of the word digital in the document so, agree to remove it in order to avoid confusion.** **ACCEPTED**
7.6.1	**d)**	**Technical**	**Unless "different" in "TSU's signing key should not be imported into different cryptographic modules." means different products, this requirement prohibits redundant system setups, designed to ensure availability.**	**Redundancy should be allowed with proper controls.**	**Best practices is to provide TSU redundancy with different keys.** **This requirement does not prohibits high availability, "should" is only a recommendation.** **One implementation may import the same key in different TSUs.** **REJECTED**
			Same proposal as to ETSI EN 319 401 and ETSI EN 319 411-1 and 2, internal structure of document could be coherent with other ETSI standards for trust service provider requirements.		**The requirements addressed in each of the documents are quite different and so the internal structure is structured to take account of the particulars of of each trust service.** **REJECTED**