Public Review: resolution of comments on Draft ETSI TS 119 312 v0.0.5 – 31 May 2014

Electronic Signatures and Infrastructures (ESI); Cryptographic suites

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
Entity 1	6.1.2.1 7.2		**Technical**	Choice of padding between probabilistic and deterministic one: By using a deterministic padding, you obtain the same signature from the same message, that maybe not suitable, but this is not the case by using a probabilistic padding. This is applicable to RSA only. Could we add some sentence in TS 119 312 to reflect this statement?	In the section 6.1.2.1, the sentence « For RSA signatures also a padding method has to be specified.” could be completed by the following “depending on the choice of padding between probabilistic or deterministic, the signature can be unique or not”. In the section 7.2, the information about the paddings could be more specific, and mention the impact on the unicity of the signature. More generally, there is a “trend” (and this is good) to recommend algorithms with an established security proof, and this is in favour of PSS rather than PKCS#1 v1.5.	Agreed.