Public Review: resolution of public comments on Draft ETSI EN 319 122-2 v0.0.8

CAdES digital signatures;

Part 2: Extended CAdES signatures

Organization name	**Clause/ Subclause**	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change**	**RESOLUTION** on each comment submitted
A 01	all		ed	Use reference to Regulation consistent with other deliverables	Replace “EU Regulation Nº 910/2014” with “Regulation (EU) No 910/2014”	Accepted.
A 02	foreword		ed		The present document is part 2 of a multi-part deliverable ~~covering~~ specifying CAdES digital signatures. Full details of the entire series can be found in part 1 [1]. The present document partly contains an evolved specification of ~~forms~~ CAdES **signatures** previously published as TS 101 733.	Accepted.
A 03	scope		ed	Suggest some rewording to show link between the levels	The present document specifies CAdES digital signatures. CAdES signatures are built on CMS signatures ~~as specified in~~ [i.7], by incorporation of signed and unsigned attributes, which fulfil certain common requirements (such as the long term validity of digital signatures, for instance) in a number of use cases. The present document specifies a number of CAdES signature levels, ~~each one based on different combinations of attributes,~~ **addressing incremental requirements to maintain the validity of the signatures over the long term, in a way that a certain level always addresses all the requirements addressed at levels that are below it. These PAdES extended signatures offer** ~~with~~ a higher degree of optionality than the CAdES baseline signatures specified in part 1 of ETSI EN 319 122.	Accepted.

Organization name	**Clause/ Subclause**	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change**	**RESOLUTION** on each comment submitted
					The present document ~~CAdES digital signatures specified in the two parts of ETSI EN 319 122~~ aims at supporting ~~electronic~~ digital signatures in different regulatory frameworks. NOTE: Specifically but not exclusively, CAdES digital signatures specified in the present document aim at supporting electronic signatures, advanced electronic signatures, qualified electronic signatures, electronic seals, advanced electronic seals, and qualified electronic seals as per EU Regulation Nº 910/2014 [i.6].	
A 04	2.1		ed		[i.6] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. ~~OJ L 257, 28.8.2014, p. 73–114.~~	Accepted
A 05	3.1		ed	Definition of digital signature is missing	Add definition of digital signature (from 119 172-1) data associated to, including a cryptographic transformation of, a data unit that: a) allows to prove the source and integrity of the data unit, b) allows to protect the data unit against forgery and c) allows to support signer non-repudiation of signing the data	Accepted

Organization name	**Clause/ Subclause**	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change**	**RESOLUTION** on each comment submitted
					unit.	
A 06	3.1		Ed		**Legacy CAdES 101 733 signature:** CAdES signature generated according to ETSI TS 101 733 [i.1] ~~before the publication of the present document~~	Accepted.
A 07	4.2		Ed	“described” is too weak.	The general CMS syntax shall be as ~~described~~ **specified** in EN 319 122-1 [1], clause 4.	Accepted
A 08	4.3		ed		Annex A specif~~y~~**ies** CAdES-E-C, CAdES-E-X (of Type 1 and of Type 2), CAdES-E-X-Long, and CAdES-E-X-L (of Type 1 and of Type 2) signatures, and CAdES-E-A built on them	Accepted
A 09	4.3	Note 1	ed		NOTE 1: The signature policy ~~may~~ **can** establish specific requirements for other attributes.	Accepted
A 10	A.1		ed	Extra “a” before “at least and extra “s” in “signedAssertions)	g) The attribute-certificate-references and the attribute-revocation-references attributes shall be present if ~~a~~ at least a certified signer attribute (certifiedAttributesV2 as defined in clause 5.2.6.1 of EN 319 122-1 [1]) or a signed assertion (signedAssert~~s~~ions as defined in clause 5.2.6.1 of EN 319 122-1 [1) is present within the signer attributes in the ~~electronic~~ signature.	Accepted
A 11	A.1	Notes 2 & 3	ed		NOTE 2: If the signer provides as a minimum the CAdES-E-BES or CAdES-E-EPES, then as long as the signature is	Accepted.

Organization name	**Clause/ Subclause**	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change**	**RESOLUTION** on each comment submitted
					still valid it can be extend**ed** to CAdES-E-C. NOTE 3: Time-stamp tokens ~~may~~ **can** themselves include unsigned attributes required to validate the time-stamp token.	