Public Review: resolution of public comments on Draft ETSI EN 319 132-2 V0.0.9

XAdES digital signatures;

Part 2: XAdES extended 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	scope		ed	Suggest some rewording to show link between the levels	The present document specifies ~~specifies~~ XAdES digital signatures. XAdES signatures are built on XML digital signatures ~~as specified in~~ [i.4], by incorporation of signed and unsigned qualifying properties, 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 XAdES signature levels, ~~each one based on different combinations of qualifying properties, with~~ **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** a higher degree of optionality than the XAdES baseline signatures specified EN 319132-1 [1]. The present document aims at supporting electronic signatures in different regulatory frameworks. NOTE: Specifically but not exclusively, XAdES digital	Accepted, but changing PAdES by XAdES

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted
					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.1].	
A 03	4.1		ed	As this is only an overview, move the normative requirements to 4.2 + shouldn't the whole clause 4 of part 1 apply?	Move to clause 4.2: Each level shall be generated by a different combination of the XAdES qualifying properties specified in EN 319 312-1 [1], and incorporated to the XAdES signatures using one of the two mechanisms (direct or indirect incorporation) ~~described~~ **specified** in clause 4.~~3~~**4** of EN 319 312-1 [1]. Or replace in clause 4.2 with XAdES signatures shall be as specified in EN 319 132-1 [xx]. And delete the first sentence of 4.2 as it is covered by the new sentence above	Accepted with changes: In 4.1 replace "shall be generated" by "will be generated" or "is generated" As for 4.2, rejected. The sentence "XAdES signatures shall be as specified in EN 319 132-1 " strictly speaking means that we are going to repeat EN 319 132-1, and this is not true. Part 2 uses the qualifying properties specified within part 1 and builds new combinations for getting new levels….
"A 04	4.2		tec	Is it correct to refer to 319 102 in the `QualifyingProperties`'s `version`? "The value of `QualifyingProperties`'s `version` attribute shall be		Accepted: Obviously it is not correct. It is an unfortunate typing mistake. It should read: "ETSI_EN_319132_v111"

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted
				"ETSI_EN_319102_v111" for any XAdES signature of any of the levels specified within the present document."		
A 05	4.2		ed		NOTE: ~~Readers are warned that~~ signing the whole ds:KeyInfo locks the element: any addition of a certificate or validation data would make signature validation fail. Applications can, alternatively, use XPath transforms for signing at least the signing certificate, leaving the ds:KeyInfo element open for addition of new data after signing.	Accepted
A 06	4.3		ed		Annex A specify~~y~~**ies** XAdES-E-C, XAdES-E-X (of Type 1 and of Type 2), XAdES-E-X-Long, and XAdES-E-X-L (of Type 1 and of Type 2) signatures, and XAdES-E-A signatures built on them	Accepted
A 07	4.3	Table 1	tec	The condition of the presence of SigningCertificate is not specified	Specify the condition for the presence of SigningCertificate	Accepted. Add note saying: SigningCertificate shall be present if the X509 signing certificate is not present within the ds:KeyInfo element, or if it is present there but it is not signed by the signature.
A 08	4.3				In item g, I, j, replace XAdES-A with XAdES-E-A	Accepted
A 09	4.3		tec	Item k misses the description of the condition for presence	Add to k: The validation data for electronic time-stamps shall be in the `TimeStampValidationData` qualifying property or embedded in the electronic	Accepted:

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted
					time-stamp itself.	
A 10	A.1	table A.1	tec	The condition of the presence of SigningCertificate, `SignaturePolicyStore`, `AttributeCertificateRefs`, `AttributeRevocationRefs` is not specified	Specify the condition for the presence	Accepted. For signingCertificate: Requirement for `SigningCertificate`. The `SigningCertificate` qualifying property shall be present if the signing certificate is not present within the `ds:KeyInfo` element, or if the signing certificate is present within the `ds:KeyInfo` element but it is not signed by the signature. Otherwise the `SigningCertificate` qualifying property may be absent. For SignaturePolicyStore: Requirement for `SignaturePolicyStore`. This qualifying property may be incorporated into the XAdES signature only if the `SignaturePolicyIdentifier` is also incorporated and it contains the `SigPolicyHash` element with the digest value of the signature policy document. Otherwise the `SignaturePolicyStore` shall not be incorporated into the XAdES signature. For AttributeCertificateRefs: Requirement for `AttributeCertificateRefs`. This qualifying property may be incorporated into the XAdES signature only if the XAdES signature incorporates attribute certificates or signed assertions within the SignerRole qualifying property. Otherwise it shall not be incorporated

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted
						into the XAdES signature. For AttributeRevocationRefs: Requirement for `AttributeRevocationRefs`. This qualifying property may be incorporated into the XAdES signature only if the XAdES signature incorporates attribute certificates or signed assertions within the SignerRole qualifying property. Otherwise it shall not be incorporated into the XAdES signature. Also, after proposing resolutions for this comment, the editor proposes the following change to the original text, also on requirements for incorporation of some properties, in order to improve wording and alignment with part 1: For CertificateValues: If a XAdES-E-X-Long or a XAdES-E-X-L signature is generated, `CertificateValues` qualifying property shall be incorporated if the signature misses some of the certificates listed in ETSI EN 319 132-1 [1], clause 5.4.1, that are required to validate the XAdES signature. Otherwise it shall not be incorporated into the XAdES signature. For RevocationValues: If a XAdES-E-X-Long or a XAdES-E-X-L signature is generated, `RevocationValues` qualifying property

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted
						shall be incorporated if the signature misses some of the revocation values listed in ETSI EN 319 132-1 [1], clause 5.4.2, that are required to validate the XAdES signature. Otherwise it shall not be incorporated into the XAdES signature. For `AttrAuthoritiesCertValues`: If a XAdES-E-X-Long or a XAdES-E-X-L signature is generated, `AttrAuthoritiesCertValues` qualifying properties shall be incorporated if the signature incorporates attribute certificates or signed assertions, and if the signature misses some of the certificates (including trust anchor(s) when available in the form of certificate(s)) required for validating the attribute certificates and/or signed assertions. Otherwise it shall not be incorporated into the XAdES signature. For `AttributeRevocationValues`: If a XAdES-E-X-Long or a XAdES-E-X-L signature is generated, `AttributeRevocationValues` qualifying properties shall be incorporated if the signature incorporates attribute certificates or signed assertions, and if the signature misses some of the revocation values required for validating the attribute certificates and/or signed assertions. Otherwise it shall not be incorporated into the XAdES signature.

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted
A 11	A.1		tec	For b,c, d, e, if the condition is not met, the properties shall not be present?	Add at the end: Otherwise, the qualifying property shall not be incorporated.	Accepted for b Not accepted for c (this is nothing on conditional presence) Not accepted for d (again, nothing to do with conditional presence). Not accepted for e.
A 12	A.2		ed		2) The incorporation of validation data for electronic time-stamps shall be provided to XAdES-E-A signatures specified in the present clause. **and**	Accepted And.