Public Review: resolution of public comments on Draft ETSI EN 319 132-1 V0.0.9

XAdES digital signatures;

Part 1: Building blocks and XAdES baseline 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		The present document specifies XAdES digital signatures. XAdES signatures build on XML digital signatures ~~as specified in~~ [1], 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.	Accepted
A 03	2.2		ed	119 172-1 is a TS	ETSI ~~EN 319~~ **TS 119** 172-1: "Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 1: Framework".	Accepted
A 04	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 unit.	Accepted
A 05	4.3.1		ed		Otherwise, its not fragment part need**s** not	Accepted

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted
					be empty. (appears twice)	
A 06	4.3.1		tec	Is it correct to refer to 319 102 in the `QualifyingProperties`'s `version`? "The value for `version` attribute of XAdES signatures specified within the present document shall be "ETSI_EN_319102_v111"		Accepted It should read: "ETSI_EN_319132_v111"
A 07	2.1		ed	These references are not normative	Move the following references to informative clause 2.2: [9] ETSI TS 119 312: "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites".	Accepted .
A 08	2.2		ed		i.7 is TS 119 172-1 (and not EN 319 xxx) i.10 duplicates i.3	Accepted Agreed i.7 Agree delete i.3, keep i.10.
A 09	4.3.1	418-422	ed	It is duplicated text	Delete duplication	Accepted
A 10	4.5	697	ed	Duplicated "the"	this qualifying property shall include the ~~the~~ canonicalization algorithm identifier	Accepted
A 11	5.1.4.2	844	ed		Annex A specifies two qualifying properties that contain electronic ~~time-stamps~~ time-stamping qualifying properties that contain references to validation data	Implemented as below Agreed with changes, although the original text does not seem incorrect Annex A specifies two qualifying properties that contain electronic time-stamps on qualifying properties that contain references to validation data, namely: `SigAndRefsTimeStamp` and

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted
						`RefsOnlyTimeStamp`
A 12	5.1.4.3	850	ed	Add reference	• Allow encapsulating RFC 3161 [7] electronic time-stamps as well as XML electronic time-stamps [1].	Rejected
A 13	5.2.6	1312	ed	Duplicated words	NOTE 1: The namespaces given to the corresponding XML schemas allow their unambiguous identification in the case these attributes are expressed in XML syntax (e.g. SAML assertions [i.9] of different versions ~~of different versions~~).	Accepted
A 14	5.2.9.1	1439	ed	Relying and not relaying	The SignaturePolicyIdentifier qualifying property shall contain either an explicit identifier of a signature policy or an indication that there is an implied signature policy that the ~~relaying~~ relying party should be aware of. NOTE 1: ETSI ~~EN 319 172-1~~ **TS 119 172-1** specifies a framework for signature policies.	Accepted
A 15	5.2.9.2		Ed		NOTE 3: This qualifier allows identifying whether the signature policy document is human readable, XML encoded, or ASN.1 encoded, by identifying the specific ~~Technical Specifications~~ technical specifications where these formats will be defined.	Accepted
A 16	5.4.3	1763	Ed		The ~~for~~ `AttrAuhtoritiesCertValues` qualifying property shall be defined as in XML Schema file	Accepted
A 17	5.5.3	Note 1	ed		NOTE 1: When a certain digest algorithm is becoming weak, one or more	Accepted

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted
					detached data objects have been indirectly signed using that algorithm with a signed ds:Manifest, and when suspected that some **of** the aforementioned data objects might be substituted by others	
A 18	6.1		ed		NOTE 3: Conformance to B-LT level, when combined with appropriate additional preservation techniques tackling the long term availability and integrity of the validation material is sufficient to allow validation of the signature long time after its generation. The assessment of the effectiveness of preservation techniques for signed data other than implementing the B-LTA level are out of the scope of the present document. The reader is advised to consider legal instruments in force and/or other standards (for example TS 101 533 1) that ~~may~~ **can** indicate other preservation techniques.	Accepted
A 19	6.2.2		ed		5) Column "Presence in B-LTA level". This cell contains the specification of the presence of the qualifying property or other signature's element, or the provision of a service, for XAdES-B-LTA signatures. Below follows the values that ~~may~~ **can** appear in columns "Presence in B-B", "Presence in B-T", "Presence in B-LT", and "Presence in B-LTA": … "~~conditoned~~ **conditioned** presence": means that the incorporation to the signature of the item identified in the first	Accepted

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted
					… 7) Column "References": This **cell** ~~shall~~ contain**s** either the number of the clause specifying the qualifying property in the present document, or a reference to the document and clause that specifies the other signature's element.	
A 20	6.3		tec	shouldn't the whole clause 4 of part 1 apply?	The four XAdES signature levels specified in the present clause shall be built **as specified in clause 4 and only** ~~on XMLDSIG [¡**Error! No se encuentra el origen de la referencia.**] signatures~~ by direct incorporation of XAdES qualifying properties, as specified in clause **¡Error! No se encuentra el origen de la referencia.** ~~of the present document~~.	Agreed with changes: The four XAdES signature levels specified in the present clause shall be built as specified in clause 4. The XAdES qualifying properties specified in clause 5 shall be incorporated to the signature using only the direct incorporation mechanism specified in clause 4.4.
A 21	6.3		tec	The condition for presence of CertificateValues, `RevocationValues`, `AttrAuthoritiesCertValues`, `AttributeRevocationValues`, SPO: `TimeStampValidationData`, SPO: certificate and revocation values embedded in the electronic time-stamp itself is not defined		Agreed. Implemented dispositions below PART 1 of the resolution: Improve algorithm for computing the message imprint for ArchiveTimeStamp, as this text specifies when these properties have to be incorporated to the signature. The proposed text, in clauses 5.5.2.2 and 5.5.2.3 is as follows: "a) The CertificateValues qualifying property shall be incorporated into the signature if it is not already present and the signature misses some of the certificates listed in clause 5.4.1 that are required to validate the XAdES signature. Otherwise it shall not be incorporated. If CertificateValues

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted
						qualifying property is incorporated into the signature it shall contain the aforementioned missing certificates. □ b) The RevocationValues qualifying property shall be incorporated into the signature if it is not already present and the signature misses some of the revocation data listed in clause 5.4.2 that are required to validate the XAdES signature. Otherwise it shall not be incorporated into the XAdES signature. If RevocatioValues qualifying property is incorporated into the signature it shall contain the aforementioned missing revocation data.□ c) The AttrAuthoritiesCertValues qualifying property shall be incorporated into the signature if not already present and the following conditions are true: attribute certificate(s) or signed assertions have been incorporated into the signature, and the signature misses some certificates required for their validation. Otherwise it shall not be incorporated. If AttrAuthoritiesCertValues qualifying property is incorporated into the signature it shall contain the aforementioned missing certificates. And□ d)The AttributeRevocationValues qualifying property shall be incorporated into the signature if not already present and the following conditions are true: attribute certificates or signed assertions have been incorporated into the signature, and the signature misses some revocation values required for their validation. 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
						If AttributeRevocationValues qualifying property is incorporated into the signature it shall contain the aforementioned missing revocation data.And“ PART 2 Of the resolution: Include requirements for conditioned presence referencing the former text, after the table: For CertificateValues: Requirement for incorporation of CertificateValues. If a XAdES-B-LT or a XAdES-B-LTA signature is generated, the incorporation of CertificateValues shall be determined by requirements specified in clause 5.5.2.2, step 4.a of the algorithm specified for computing the input to the electronic time-stamp's message imprint For RevocationValues Requirement for incorporation of RevocationValues. If a XAdES-B-LT or a XAdES-B-LTA signature is generated, the incorporation of RevocationValues shall be determined by requirements specified in clause 5.5.2.2, step 4.b of the algorithm specified for computing the input to the electronic time-stamp's message imprint. For AttrAuthoritiesCertValues: Requirement for incorporation of AttrAuthoritiesCertValues. If a XAdES-B-LT or a XAdES-B-LTA signature is generated, the incorporation of AttrAuthoritiesCertValues shall be

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted
						determined by requirements specified in clause 5.5.2.2, step 4.c of the algorithm specified for computing the input to the electronic time-stamp's message imprint. For AttributeRevocationValues Requirement for incorporation of AttributeRevocationValues. If a XAdES-B-LT or a XAdES-B-LTA signature is generated, , the incorporation of AttributeRevocationValues shall be determined by requirements specified in clause 5.5.2.2, step 4.d of the algorithm specified for computing the input to the electronic time-stamp's message imprint. PART 3 OF THE DISPOSITION: For service “incorporation of validation data for electronic time-stamps”: The validation data for electronic time-stamps shall be present within the `TimeStampValidationData` qualifying property or embedded in the electronic time-stamp itself. For the service “incorporation of validation data for electronic time-stamps” and its two options: Requirement for service "incorporation of validation data for electronic time-stamps" and its two options. The validation data for electronic time-stamps should be included in the

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted
						`TimeStampValidationData` qualifying property.
A 22	A.1.2	2432	ed		`URI` attribute of `CRLRef` element shall indicate one place where the referenced CRL ~~may~~ **can** be found.	Accepted
A 23	A.1.5.1.1	2535	ed		The `SigAndRefsTimeStamp` qualifying property shall be an ~~optional~~ unsigned qualifying property qualifying the signature.	Accepted
A 24	A.5.2.1	2593	ed		The `RefsOnlyTimeStamp` qualifying property shall be an ~~optional~~ unsigned qualifying property qualifying the signature.	Accepted

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted
B	6.2.2 6.3	Table2	Technical	"*": means … should not be incorporated We interpret "should not" as "not recommended" but there may exist valid reasons in particular circumstances when the elements need to be used. For example when using XAdES-B-B there may be the need to provide revocation information for an offline scenario. It should be stated clearly that such an extension is allowed.	"*": means that the qualifying property or signature's element (Service) identified in the first column is not intended to be incorporated into the signature (provided) in the corresponding level. But in case such a property is needed a profile may define their usage.	Rejected: In fact the actual meaning of "should not" according to Clause 3.2 of ETSI Drafting Rules (EDR hereafter), is precisely this. However it is an agreement taken not to duplicate the information present in the aforementioned clauses (this would repeat information) of ETSI EDR or try to explain them with different wording (this could lead to contradictions). The solution implemented in **all** the ETSI deliverables has been to add Clause "Modal verbs and terminology". This clause makes it clear that "should not" (as well as the rest of modal verbs"are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions)". The aforementioned clause of EDR states for "should" and "should not": "The verbal forms shown in table 3 shall be used to indicate that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required, or that (in the negative form) a certain possibility or course of action is

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted
						deprecated but not prohibited. Verbal form / Equivalent expression **should** / It is recommended that. Ought to **should not** / It is not recommended that. Ought not to NOTE: "exceptional cases" means where the ETSI Drafting Rules, if applied, would change the meaning of the sentence or make it difficult to understand. " In the yellow mark, and it can be seen that in fact a "should not" allows that if some implementer has good reasons for not following the recommendation, just ignores it….and the signature will still be conformant.

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted
C	5.4.1		Technical	Why in the CertificateValues element whole certificate path is necessary if the certificate of the trust anchor is already present in TSL? It is not consistent with the requirement described in baseline profile which claims that in the CertificateValues certification path shall be present until the the certificate of the trust anchor.		Rejected. Leave the document as it is. It is the same also for CAdES. CertificateValues is mandated to be added (under certain conditions) in XAdES-B-LT and XAdES-B-LTA. These levels, by definition, are specified for incorporating ALL the validation material into the signature, regardless how easy or difficult is to access to it….if one does not want to have all this material, then one should not generate XAdES-B-LT or XAdES-BLTA. Despite the fact that the certificate is already present in the TSL, it is considered that as the initial step of long term, all the material required for validating the signature has to be incorporated to it, including the certificate containing the trust anchor. Additionally EN 319 132-1 does not specify in its baseline profile that the certificate of the trust anchor shall not be present within CertificateValues. .
C	5.4.1	Paragraph 4	Technical	Why the CertificateValues qualifying property shall contain certificates used to sign revocation status information, if it is present in OSCP response?		Accepted The text is modified as follows: Shall contain certificates used to sign revocation status information (e.g. CRLs or OCSP responses) of certificates in 1), 2), and 3), and certificates within their respective certificate paths that are not present the signature. Certificate values present within the signature, including

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted
						certificate values within the revocation status information themselves should not be included ALSO change text for AttrCertificateValues as follows: 3) May contain the certificate values used to sign CRLs or OCSP responses and the certificates values within their respective certificate paths, used for validating the signing certificate(s) of the attribute certificate(s) and signed assertion(s) incorporated into the XAdES signature. Certificate values present within the signature, including certificate values within the revocation status information themselves should not be included
C	5.5.1		Editorial	The time-stamping certificate and revocation data could be included respectively into CertificateValues or RevokationValues paragraph blocks.		Rejected. If the comment is saying that the certificates and revocation data exclusively related to time-stamp tokens should be added to CertificateValues and RevocationValues qualifying property, this is rejected: once the first ArchiveTimeStamp is added these properties are time-stamped and can not be modified afterwards..and arrival of new ArchiveTimeStamps could require to incorporate to the signature new certificates/revocation data for these new time-stamp tokens.

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted
C	6.3		Technical	Why it does not contain B-T level time-mark? Previous version of technical standard (TS 103 171, v.2.1.1) allowed to use time-mark instead of time-stamp. Also ETSI EN 319 102-1 (ver. 0.12.0) „Procedures for Signature Creation and Validation“ clause 4.3.3.1 Note1 allows the time-mark. Estonian digital signatures would be not compliant to the baseline profile.	To add possibility to use B-T level time-mark instead of time-stamp.	REJECTED AS PER DECISION AT ESI#49: It was decided to leave out of this profile the time-marked signatures….although it is true that this leaves these signatures out of the playfield No standard does exist for time-marks. The profiles are defined for maximizing interoperability cross-border.
C	6.3		Technical	Do you mean here IssuerSerial element: „j) Requirement for SigningCertificate/Cert. The generator shall not generate the X509IssuerSerial element.“? In previous version of technical standard (TS 103 171, v.2.1.1) it was the mandatory element. Why this is changed?		Decision: not changed. W3C XML Signature has deprecated the ds:IssuerSerial element because it seems that a number of XML Schema validating tools can not properly deal with the validation of integer values with decimal data exceeding 18 decimal digits. In order not to use deprecated elements, ESI decided to define a new IssuerSerial with SerialNumber being a string containing the textual representation base 10 of the serial number. In addition to that checking match of DNs string representations against the actual Distinguished Names has proved to bring problems to implementers. All this lead ESI to consider the whole IssuerSerial as a hint, instead an element whose contents need to be checked against the corresponding field

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted
						values in the certificate….for matching the certificate, its digest value is actually enough. As for the baseline profile, following the rule of making it as basic as possible, it has been decided not to generate this element, which is considered in the EN 319 132 only a hint.
C	6.3		Editorial		The name of SigningTime element should be ClaimedSigningTime, since it concerns the time of signature creation by user, which is not reliable. This name would be similar to the ClaimedRole used for the claimed signer role.	Rejected. The label in the table is the actual name of the XAdES qualifying property. Consequently, it can not be changed as it would imply to change the name of the property and the XML Schema itself. Additionally clause 5.2.1 makes it clear that this is only a claimed time.

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted
D 01	all		tech	It would be better to introduce new element names, and not redefine the old element name		Old namespace is kept.
D 02	?		Tech	the procedure for determining the evaluation date of a certificate mentions the revocation date. There are two dates of interest – the date the revocation was generated, and the effective date. Most operators will ensure that these are the same, but this is not guaranteed.		ISSUE For EN 319 102. Disposition created in the corresponding dispositions document
D 03	?		TECH	A greater concern, and I did not notice this covered in the new documents, is the following scenario: Signature is generated Due to a race condition, or possibly due to the effective date of revocation being prior to the issue date, the signature is evaluated as valid, and time stamped, even though it is truly revoked. If the signature is verified during the validity period of the certificate, at some time after the race condition has been resolved, then it will evaluate as revoked. A CA operator is only obligated to keep revocation information for two CRLs past the validity period of the certificate, and the		ISSUE For EN 319 102. Disposition created in the corresponding dispositions document

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted
				revocation information then ages out of the CRL. If the signature is evaluated at this point, then it will evaluate as valid. I ran into this while discussing how to use XAdES for official business purposes with the government of Costa Rica. I can think of two approaches that would solve this problem: 1) Have a trusted evaluator evaluate the signature while the certificate is still within the validity period (which ensures revocation information should still be available), generate an evaluation report, and add it as a countersignature on the full signature. 2) Require that a set of revocation information be present which was created during the validity period of the certificate, but at some suitable time after the signature time. If there is a requirement that already covers this, and I have somehow missed it, my apologies.		

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted

E			te	to solve the problem with decoding of ASN.1 issuerSerrial from certificate and encoding it in XML signed element, where the name is a sequence of certificate issuer DN components not unique transformed to the XML element,
				can be proposed to use a type="xsd:base64Binary" of "IssuerSerialV2".
				
				The content of "IssuerSerialV2" is a binary value defined in **https://tools.ietf.org/html/rfc5035** as
				IssuerSerial ::= SEQUENCE {
				issuer GeneralNames,
				serialNumber CertificateSerialNumber
				}
				
				<xsd:complexType name="CertIDTypeV2">
				<xsd:sequence>
				<xsd:element name="CertDigest" type="DigestAlgAndValueType" />
				<xsd:element name="IssuerSerialV2" type="xsd:base64Binary" minOccurs="0"/>
				</xsd:sequence>
				<xsd:attribute name="URI" type="xsd:anyURI" use="optional"/>
					The content of "IssuerSerialV2" is a binary value defined in **https://tools.ietf.org/html/rfc5035** as
					IssuerSerial ::= SEQUENCE {
					issuer GeneralNames,
					serialNumber CertificateSerialNumber
					}
					
					<xsd:complexType name="CertIDTypeV2">
					<xsd:sequence>
					<xsd:element name="CertDigest" type="DigestAlgAndValueType" />
					<xsd:element name="IssuerSerialV2" type="xsd:base64Binary" minOccurs="0"/>
					</xsd:sequence>
					<xsd:attribute name="URI" type="xsd:anyURI" use="optional"/>
					</xsd:complexType>
					
					Peter Rybar
						The change in syntax was accepted: The content of `IssuerSerialV2` element shall be the base-64 encoding of one DER-encoded instance of type `IssuerSerial` type defined in IETF RFC 5035
						
						In baseline signatures, "shall not" is kept.
						
						In other signatures, "should not" is kept.
						
						Validation is kept as it is.

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted
				</xsd:complexType>		