

Public Review: resolution of public comments on Draft ETSI EN 319 142-2 v0.0.8

PAdES digital signatures;

Part 2: Extended PAdES signatures

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted
A 01	title		ed	Title is not coherent with structure of the document. Title only refers to extended PAdES signatures, which are defined in clause 4; title does not cover clauses 5 and 6	Find a more general title encompassing the content of the document	Accepted and change title to Additional PAdES signatures profiles
A 02	Structure of the draft		ed	XAdES signatures are between CMS signatures. This is odd Also why not keeping the order there was in 102 778: - CMS very basic signatures - extended CMS signatures - XAdES Also couldn't the CMS basic signatures be merged in the extended CMS signatures and part of the same single table? It would be a way to better see the differences between the levels? Call it PAdES-E-Basic. If not merged, CMS basic (clause 6) needs at least to be structured the same way as extended PAdES signatures (using a table)		Partly accepted: Well reordering was done intentionally. The order was by the relevance of the profiles with extended CMS as the most used and origin of the baseline profiles, embedded XML-Signatures as relevant but hardly used and former part 2 as legacy, with the problem of certificate replacement. After a review in the STF we decided to put the CMS profile to the front. Regarding merging former part 2 and part 3: The STF decided to not accept the comment because we do not see any true benefit for that in terms of comprehensibility of the document.
A 03	all		ed	ESI agreed avoiding using the term profile for AdES	Remove "profiles" and only write "signatures" which may then have different levels	Not accepted. Coming from the history of PAdES the term profiles are well established for the things defined in this document. In this

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted
						respect it is quite different from CAdES and XAdES. But the extra PAdES "Profiles" defined in this document are rather orthogonal addressing different demands.
A 04	all		ed	Insert the reference identifier before the reference number in the body of the document as simply using the reference number may lead to wrong references	e.g. insert ISO 32000-1 before all [1]	Accepted
A 05	scope		ed		<p>The present document defines multiple profiles for PAdES digital signatures, which are digital signatures embedded within a PDF file.</p> <p>The present document defines three levels of PAdES extended signatures 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 PAdES baseline signatures specified in part 1 of ETSI EN 319 142. extends the scope of the profile in PAdES part 1 [5], while keeping some features that enhance interoperability of PAdES signatures. These profiles in the present document provide equivalent requirements to profiles found in ETSI TS 102 778 [i.12].</p> <p>The present document also contains a profile for the use of PDF signatures, as described in ISO 32000-1[1] and based on CMS digital signatures [i.7], that enables greater interoperability for PDF signatures</p>	<p>Only partly accepted</p> <p>The Text provides is right when applied to the extended PAdES profiles and is used in the scope in that context.</p>

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted
					<p>by providing additional restrictions beyond those of ISO 32000-1 [1].</p> <p>The present document defines a third profile for usage of an arbitrary XML document signed with XAdES signatures that is embedded within a PDF file.</p> <p>The present document does not repeat the base requirements of the referenced standards, but instead aims to maximize interoperability of CMS-based digital signatures in various business areas.</p> <p>NOTE: The profiles in the present document provide equivalent requirements to profiles found in ETSI TS 102 778 [i.12].</p>	
A 06	2.1		ed	The following references are informative and not normative	<p>Move the following references to 2.2</p> <p>[9] Adobe XFA: "XML Forms Architecture (XFA) Specification" version 2.5, (June 2007), Adobe Systems Incorporated".</p>	<p>Rejected</p> <p>In the following statement: "Signatures shall sign the ds:SignatureProperties element containing the additional XML elements not specified within [9] that are incorporated by XFA processors.</p> <p>" it is used in a requirement, and without knowledge of XFA the requirement is not implementable.</p>
A 07	2.1 & 2.2		ed	The following references are not really of any use	<p>Delete the following references</p> <p>[3] Recommendation ITU-T X.509 (2008)/ISO/IEC 9594-8 (2008): "Information technology - Open Systems Interconnection - The Directory: Public-key and Attribute Certificate frameworks".</p> <p>And delete note in clause 3.1</p> <p>[4] IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate</p>	<p>Partly accepted.</p> <p>[3] [i.9] and [i.13] were removed as suggested</p>

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted
					<p>and Certificate Revocation List (CRL) Profile".</p> <p>Assuming the clauses using it will be removed as suggested</p> <p>[10] W3C Recommendation: "XML-Signature Syntax and Processing. Version 1.1".</p> <p>[i.9] IETF RFC 6960: "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol OCSP".</p> <p>Assuming the clauses using it will be removed as suggested</p> <p>[i.13] IETF RFC 3161 (2001) "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)"</p> <p>Assuming the clauses using it will be removed as suggested</p>	
A 08	2.1 & 2.2		ed	Turn note into editor's note as it will disappear once the draft is TB approved	<p>Editor's NOTE: The ENs mentioned in [5], [6], [7] and [8] are published in the context of the work in Mandate M460. They might not yet be published</p> <p>Same for 2.2</p>	Accepted
A 09	3.1			<p>The use of the word "conforming" is of no use</p> <p>Pdf serial signature is not a workflow</p>	<p>conforming signature handler: software application, or part of a software application, that knows how to perform digital signature operations (e.g. signing and/or validating) in conformance with ISO 32000-1 [1] and the requirements of the appropriate profile</p> <p>PDF serial signature: specific digital signature workflow where the second (and</p>	Accepted

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted
					<p>subsequent) signers of a PDF not only sign the document but also the signature of the previous signer and any modification that can also have taken place (e.g. form fill-in)</p> <p>signature dictionary: PDF data structure, of type dictionary, as described in ISO 32000-1 [1], clause 12.8.1, table 252 that contains all the of information about the digital signature</p> <p>validation data: data that may can be used by a verifier of digital signatures to determine that a digital signature is valid (e.g. certificates, CRLs, OCSP responses)</p>	
A 10	4 & 5		ed	There should an introductory clause explaining the different levels, similar to clause 6.1 in part 1		Accepted Proposed texts was added to the draft as sections 4.1, and 5.1 (which is now (5.1 and 6.1)
A 11	4.1.2		ed	See comments made on part 1		Comments 1, 3 and 11 of the A on 319 142-1 are considered to apply also to part 2. and are accepted Comment 36 also applies to 4.1.2 of part 2 Are there more?
A 12	4.2, 4.3, 4.4		ed		Merge the 3 clauses into one as done for part 1, with a single table + merge also the clause 6 with them and call it PAdES-E-Basic	Not accepted. The reason to have one table in each baseline profile was to have a representation that is comparable between all baseline profiles in each format. This reason does not apply in this case, because it does not match directly to another

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted
						format. It is more important to have an match to the way the requirements were represented in the former TS 102 778
A 13	5		ed	Why not again using tables as done for baseline and extended signatures?		Not accepted: For the same reason as stated above. In a discussion during a STF conference call we tried to compare the pros and cons of such and restructuring, and came to the conclusion that a table though more concise would not necessary help the comprehensibility of the document.
A 14	5.1.1		ed	Wrong references to clauses	Update clauses references within this clause	Accepted: Double checked all references to subclauses.
A 15	5.1.1		Tec/ed	These XAdES signatures are built on XAdES extended signatures	Refer to 319 142-2 and not 319 142-1: The scenario for usage of the second profile, specified in clause 4.5.3, is described below and shown in figure 2: 1) The PDF container with the signed XML document is received by the verifier. The verifier extracts the embedded file and validates the XAdES signature. 2) The verifier can augment the XAdES signature to upper levels as specified in EN 319 132-1-2 [8].	Accepted: Now 6.2.1 Change reference to 319 132-2
A 16	5.1.2.2		Tec/ed	Same as above + need to specify clearly which XAdES signatures are used (not in a note)	The signatures shall be XAdES signatures XAdES-E-BES, XAdES-E-EPES, or XAdES-E-T with the syntax specified in EN 319 132-1-2 [8] with the restrictions specified in this profile the present document. NOTE 1: The XAdES signatures levels profiled by the present document are the	Accepted: This is now section 6.2.2.2

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted
					following ones: XAdES E BES, XAdES E EPES, and XAdES E T.[8]	
A 17	5.1.2.3		ed		<p>The signed XML document to be embedded within the PDF container shall satisfy the following requirements:</p> <p>1) ———The signed XML document to be embedded within the PDF container shall be created independently of the final PDF container. No further requirements are specified on the environment for creating this XML document or the XAdES signature(s) within the document.</p> <p>2) ———The signed XML document to be embedded within the PDF container shall contain at least one XAdES signature and one or more signed data objects.</p>	Accepted: Now clause 6.2.2.3
A 18	5.1.2.3		ed	<p>Is it the correct reference ([3]) in 2) If a signed data object is detached from the signed XML document, a ds:Reference element shall reference it according to the rules of [3].</p> <p>And in note 2 below</p>		Now Section 6.2.2.3 This is an mistake it should read XML Signatures Syntax and Semantics [10]
A 19	5.1.2.4.1		ed	Use adequate terminology for expressing recommendation + reword	<p>This profile recommends using the inclusion of</p> <p>The signing certificate shall be referenced in the SigningCertificate element or shall be included in the ds:KeyInfo element. the SigningCertificate qualifying property should be used for securing the signing certificate. Nevertheless,</p>	Accepted Now clause 6.2.2.4.1

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted
					applications may use the other technique. At least one of the SigningCertificate element and the signed certificate in ds:KeyInfo shall be present.	
A 20	5.1.2.4.1		ed		NOTE: Readers are warned, nevertheless that signing the whole ds:KeyInfo, locks the element and any addition of a certificate or validation data will invalidate the signature. Applications may, alternatively, use XPath transforms for signing at least the signing certificate, leaving the rest of the ds:KeyInfo element open for addition of new data after signing	Accepted
A 21	5.1.2.5		ed	Wrong use of can	The following properties defined in XAdES can may be used. If present their syntax, semantics and usage shall be as specified in EN 319 132-1 [7].	Accepted
A 22	6.2 & 6.3		Ed	These clauses are totally out of context now that 142 has restructured and that procedures are in 102	Delete the clauses	Accepted but for slightly other reasons. Resolution to delete clauses 6.2 and 6.3 because it is informative. EN 319 102 can be applied to this profile but validation must be further profiled for this profile since the certificate hash is not signed.
A 23	6.4		ed	This is background information on pdf	Move to annex A	Accepted:
A 24	6.5		ed	Either merge with clause 5 or rework to present with a table as for clause 5 Delete any item dealing with creation and validation procedures not specific to PAdES		Not accepted. We don't merge the sections for reasons given above in response to comments 22 as well as in 12 The reason to keep the requirements on creation and validation is subtle. EN

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted
				and covered by 102 (e.g. 6.5.1 e), 6.5.3, 6.5.4.2, 6.5.5		319 102 can be applied to this profile but validation must be further profiled for this profile since the certificate hash is not signed. So the text on validation material here is still useful. This sections contains requirements that might be implemented in existing applications tested in the PlugTest
A 25	6.5.1		tec	This clause is technically incoherent/not precise enough as it first says that the PDF signatures shall be as per RFC 2315 (so totally disconnected from PAdES part 1) and then item i) says "The requirement c) in Clause 4.1 of EN 319 142-1 may be ignored" PAdES part 1 does not apply at all.	Delete item i)	Accepted, this would also mean to delete the following note. But more clarification that this profile is disconnected to 319-142-1 and this profile is for backwards compatibility should be clarified in the scope.
A 26	Annex A		ed	Review text to update references to parts or clauses as appropriate		Accepted, though I double checked the annex and failed to find a wrong reference.
A 27	A.6		ed	Reference of PDF/A-1 and PDF/A-2 are wrong	Update reference to PDF/A-1 and PDF/A-2	Accepted:

Public Review: Comments on Draft ETSI <prEN > <319142-2> V<008 >

<Extended PAdES signatures >

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

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted
B 1.	Page 13 Section 4.2	Table 1	te	<p>Section 4.2 PAdES-E-BES Level</p> <p>The M entry in the signature dictionary.</p> <p>ISO 3200-1 states:</p> <p>Optional) The time of signing. Depending on the signature handler, this may be a normal unverified computer time or a time generated in a verifiable way from a secure time server.</p> <p>This value should be used only when the time of signing is not available in the signature.</p> <p>The Note e) states:</p> <p>e) The generator should include the claimed UTC time of the signature as expressed in [1], clause 7.9.4 as content of this element.</p> <p>The note is providing an information that is not present in ISO 32000-1.</p> <p>It is believed that the entry M indicates a local time. Whatever, the ETSI document should not be more precise than ISO 32000-1. This is an additional argument for not using it or for deprecating its use.</p>	<p>Replace the note e) with:</p> <p>e) Since ISO 32000-1 does not say whether this time is a local time or a UTC time, the use of the M entry is deprecated and the claimed signing time which is a signed attribute defined as a being a UTC time should be rather used instead.</p>	<p>Not accepted. The point e) is not a Note but a requirement on the M entry. Change the requirement from the M entry to the signing-time would not only invalidate existing implementations but also existing signatures with all consequences for backwards compatibility. The requirement to use the UTC timezone comes from the present document, not from ISO 32000, so we suggest to reword “The generator should include the claimed UTC time of the signature in a format defined in ISO 32000-1 [1], clause 7.9.4 as content of this element”</p> <p>It is the sole purpose of the document to be more precise than ISO 32000-1, so it is okay to add further requirements on ISO attributes.</p>

B 2.	Page 13 Section 4.2	Table 1	te	<p>For the PAdES-E-EPES Level, the commitment-type-indication may be present while, it cannot be present for the PAdES-E-BES Level.</p> <p>The single difference between a the PAdES-E-BES Level and the PAdES-E-EPES Level should be the absence or the inclusion of the signature-policy-identifier.</p> <p>For more than 10 years, this has always been the single difference between BES and EPES, whatever the format is: XAdES or CAdES.</p> <p>The signature-policy-identifier. should be added to Table 1.</p>	Add the signature-policy-identifier to Table 1 and remove it from Table 2 (section 4.3).	<p>Partly accepted.</p> <p>We changed the header of table 1, to clarify that this only applies to PAdES-E-BES Level. Table 2 shows requirements that build on top of PAdES-BES</p> <p>In the PAdES-E-BES level there is no statement about the commitment-type-indication presence, so it could be there, though there is no really any value in it without a signature policy.</p>
B 3.	Page 14 Section 4.4		ed	<p>The text states:</p> <p>a) Document security store information as specified in clause 5.3.2 in [5].</p> <p>There is no section 5.3.2 in [5].</p>	Change 5.3.2 into 5.4.2.2	Partly Accepted, it is 5.4.2:
B 4.	Page 14 Section 4.4		ed	<p>The text states:</p> <p>b) Document time-stamps as specified in clause 5.3.3 in [5].</p> <p>There is no section 5.3.3 in [5].</p>	Change 5.3.3 into 5.4.3.	Accepted:
B 5.	Page 26 Section 6.2		te	<p>The text states on the fourth line:</p> <p>so the timestamp reflects <u>the time</u> at which the document was signed.</p> <p>This is not fully correct. This time is after the signature, it could be three weeks later.</p>	<p>Replace with</p> <p>Therefore a time-stamp token from a trusted TSA <u>should</u> be applied on the digital signature or on a data structure which contains the digital signature as soon as possible after the signature is created so the timestamp reflects <u>a time after</u> which the document was signed.</p>	Accepted

B 6.	Page 26 Section 6.2		te	<p>The text states on the fifth line:</p> <p>Electronic time-stamps fulfil a critical need in the validation process: if a conforming signature handler validates and timestamps the signature using a trusted TSA then the signer cannot later claim that it was signed by someone else, that the document was altered after they signed it, or that it was signed at a later time.</p> <p>The explanations are not correct. An electronic time-stamp has nothing to do with the case where the signer could later claim that it was signed by someone else: the signer's digital signature is sufficient for that purpose.</p> <p>In the same way, it is irrelevant to say the a time-stamp token is used to protect the document after it was signed: the signer's digital signature is sufficient for that purpose.</p> <p>Finally, saying that it offers a protection so that the signer cannot later claim that it was signed at a later time does not make sense since in any circumstance it is <i>impossible</i> to know the signing time.</p> <p>So none of the three arguments is valid.</p> <p>See the text proposal.</p>	<p>Change the text into:</p> <p>Time-stamp tokens fulfil a critical need in the validation process.</p> <p>The UTC time contained in a time-stamp token will be used to demonstrate that the document was signed while the signer's certificate was valid (1). In order to be useable, the UTC time contained in the time-stamp token shall be placed before the end of the validity of the signer's certificate. If this is not the case, the signature shall be considered as invalid.</p> <p>Revocation status information about the signer's certificate shall be collected before the end of the validity period of the certificate.</p> <ul style="list-style-type: none"> • If the certificate has not been revoked, then the document was indeed signed while the signer's certificate was valid. • If the certificate has been revoked, then the UTC time of the revocation shall be compared with the UTC time contained in the time-stamp token. <p>If the certificate has been revoked after the UTC time, then the document was indeed signed while the signer's certificate was valid.</p> <p>If the certificate has been revoked before the UTC time, then:</p> <ul style="list-style-type: none"> - If an additional information allows to know that the revocation reason is a suspension, then the time-stamp token is unusable and it cannot be determined whether the signature is valid or not. - If no additional information allows to know that the revocation reason is a suspension, then the signature shall 	<p>The content of the comment is correct .</p> <p>The intention of the text was to improve the description on how signatures were handled in ISO 32000.</p> <p>But Section 6.2 will be deleted, since it is considered to be purely informal. See Resolution to comment to A 22.</p>
------	------------------------	--	----	---	---	--

					<p>be considered as invalid.</p> <p>Note (1): "valid", in this context, means both : not revoked and within the validity period certificate of the certificate.</p>	
B 7.	Page 26 Section 6.3			<p>The second line states:</p> <p>In addition, the inclusion of the revocation information protects against some threats relating to <i>the use of previously revoked certificates</i> which affect the non-repudiation properties of the signature.</p> <p>As written, this sentence is not understandable to me.</p>	<p>Either rephrase, add a foot note to explain or delete.</p>	<p>Section 6.3 will be deleted, since it is considered to be purely informal. See Resolution to comment to A 22..</p>
B 8.	Page 27 Section 6.5.1		te	<p>Item e) is written as follows:</p> <p>Timestamping and revocation information should be included in the PDF Signature. This revocation information and as much of the complete chain of certificates as is available <u>shall</u> be captured and validated before completing the creation of the PDF Signature.</p> <p>Since the first sentence includes a "should", the second sentence should include a "should" rather than a "shall".</p>	<p>Replace with:</p> <p>Time-stamping and revocation information should be included in the PDF Signature. This revocation information and as much of the complete chain of certificates as is available <u>should</u> be captured and validated before completing the creation of the PDF Signature.</p>	<p>Accepted</p>
B 9.	Page 27 Section 6.5.3		te	<p>The text states at the bottom of the page:</p> <p>c) To achieve consistent validation results with existing signatures and existing implementations of signature handlers, that did not know this attribute, the signing certificate reference attribute itself <u>should be ignored during</u></p>	<p>Replace with:</p> <p>c) To achieve consistent validation results with existing signatures and existing implementations of signature handlers, that did not know this attribute, the signing certificate reference attribute itself <u>may be ignored by these signature handlers</u> during validation if present.</p>	<p>Not accepted: This Profile is not CADES based. The way the sentence is written, was intentional. To achieve consistent validation results old and new implementation should return the same results. This would also mean a signature with a wrong certificate hash</p>

				validation if present. While it is understood that old implementations will ignore this attribute, the way the sentence is written indicates that new implementations should ignore it. This is not acceptable.		should not pass as valid with one old implementation and as invalid with a new implementation.
B 10.	Page 28 Section 6.5.4.1		te	The text states a) An electronic time-stamp from a trusted TSA should be applied to the digital signature <u>immediately</u> after the signature is created so the electronic time-stamp reflects the time at which the document was signed. it is a mater of wording, but wording is important: in any circumstance it is <i>impossible</i> to know the signing time. See the change proposal.	Replace with: a) An electronic time-stamp from a trusted TSA should be applied to the digital signature <u>as soon as possible</u> after the signature is created so the electronic time-stamp reflects <u>a time as close as possible</u> at which the document was signed.	Accepted

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted
gematik (Society for Telematics Applications in the German health-care system)	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 PAdES-B-B there may be the need to provide revocation information for an offline scenario. It should be stated clearly that	“*”: 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).

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted						
				such an extension is allowed.		<p>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)”.</p> <p>The aforementioned clause of EDR states for “should” and “should not”:</p> <p>“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 deprecated but not prohibited.</p> <table border="1" data-bbox="1659 1002 2085 1321"> <thead> <tr> <th data-bbox="1659 1002 1872 1075">Verbal form</th> <th data-bbox="1872 1002 2085 1075">Equivalent expression</th> </tr> </thead> <tbody> <tr> <td data-bbox="1659 1075 1872 1198">should</td> <td data-bbox="1872 1075 2085 1198">It is recommended that. Ought to</td> </tr> <tr> <td data-bbox="1659 1198 1872 1321">should not</td> <td data-bbox="1872 1198 2085 1321">It is not recommended that. Ought not to</td> </tr> </tbody> </table> <p>NOTE: "exceptional cases" means where the ETSI Drafting Rules, if applied, would change the meaning of the sentence or</p>	Verbal form	Equivalent expression	should	It is recommended that. Ought to	should not	It is not recommended that. Ought not to
Verbal form	Equivalent expression											
should	It is recommended that. Ought to											
should not	It is not recommended that. Ought not to											

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted
						<div data-bbox="1659 284 2085 333" style="border: 1px solid black; padding: 2px;">make it difficult to understand.</div> <p data-bbox="1659 336 1675 352">”</p> <p data-bbox="1659 395 2085 571">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</p>