Public Review: resolution of public comments on Draft ETSI EN 319 142-1 v0.0.8

PAdES digital signatures;

Part 1: Building blocks and PAdES baseline signatures

Organization name	**Clause/ Subclause**	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change**	**RESOLUTION** on each comment submitted
A 1.	Title of the document			The current title is: Electronic Signatures and Infrastructures (ESI); PAdES digital signatures Since PAdES means "PDF advanced electronic signature" the wording "PAdES digital signatures" when expanded would mean " PDF advanced electronic signature digital signatures". This does not make sense. It is proposed to change the title either into: Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signatures (PAdES).	Change into: Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signatures (PAdES).	REJECTED. PAdES doesn't mean any long PDF Advanced Electronic Signatures. It's a sort of trademark and is maintained as is for historical reason as other terms CAdES and XAdES. The title was agreed and approved in ESI.
A 2.	Page 6 Scope	Fourth paragraph	te	The text states: Procedures for creation and validation of PAdES digital signatures are out of scope and specified in EN 319 102 [i.7] It would be nice if that sentence were true, but unfortunately this is not the case. EN 319 102 is not precise enough to understand how to verify a user's right signature, a	Change into: Procedures for creation, augmentation and validation of PAdES signatures are out of scope. General guidance about procedures for creation, augmentation and validation electronic signatures are indicated in EN 319 102 [i.7].	REJECTED. The sentence is aligned with the scope of EN 319 102.

Organization name	**Clause/ Subclause**	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change**	**RESOLUTION** on each comment submitted
				certification signature or an approval signature which are the three cases of signatures supported by a PAdES document. EN 319 102 [i.7] is at most a general guidance document, with a lot of errors in it : more than 100 comments have been raised on only the first 37 pages of that document. There is no section in it dedicated to PAdES and the rules to apply to verify the document are fully left open: there is not a single chance that two different implementations can interoperate, i.e. provide consistent results. Having a format is one thing, knowing how to use the format is another thing.		
A 3.	Page 7 Section 2.1	[14]	te	ETSI TS 103 172 Electronic Signatures and Infrastructures (ESI); PAdES Baseline Profile is referenced as a Normative reference. Section 6 of this document is about : 6. PAdES baseline signatures This document has a content which duplicates : ETSI TS 103 172 Electronic Signatures and Infrastructures (ESI); PAdES Baseline Profile This makes two many documents on the same topic.	Either ETSI TS 103 172 should be removed or section 6 should refer to it. Also, if in Section 3.1, the wording " Legacy PAdES baseline signature" is going to remain, please provide a definition.	PARTIALLY ACCEPTED. ETSI TS 103 172 has been referenced as an Informative reference.

Organization name	**Clause/ Subclause**	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change**	**RESOLUTION** on each comment submitted
				The only reference to document [14] within the whole document following: Legacy PAdES baseline signature: digital signature generated according to ETSI TS 103 172 [14] The word "Legacy" is used nowhere in that document. Then the single reference to a "Legacy PAdES baseline signature" in the present document is in section 6.4 6.4 Legacy PAdES baseline signatures When new unsigned attributes are incorporated to legacy PAdES baseline signatures, these attributes shall comply with the present document. Now we can tell what a *Legacy PAdES baseline signature* is ? *Mais de qui se moque t-on* ? In French in the text.		
A 4.	Page 9 Section 3.1		te	The text states: PAdES signature: digital signature that satisfies the requirements specified within EN 319 142 part 1 or part 2. As usual there is a confusion between digital and electronic signature. Furthermore, this is not understandable.	Change into: PAdES signature: a signature inserted into a PDF document why applies to the document.	REJECTED. The definition correctly concerns the signatures defined in the two documents referenced.

Organization name	**Clause/ Subclause**	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change**	**RESOLUTION** on each comment submitted
A 5.	Page 9 Section 3.1		te	The text states: electronic time-stamp: data in electronic form which binds other electronic data to a particular time establishing evidence that these data existed at that time. It would be more accurate to use "prior" rather than "at".	Change into: electronic time-stamp: data in electronic form which binds other electronic data to a particular time establishing evidence that these data existed prior to that time.	REJECTED. The term “prior” refers to a time that isn’t clearly defined. The term “at” refers to a clearly defined time (the one in the time-stamp) to which one can trust that the document exists so the signing certificate can be validated “at” that time.
A 6.	Page 9 Section 3.1	First sentence	te	The text states: verifier: entity that validates a digital signature	Change into: verifier: entity that validates an electronic signature	REJECTED. We use the term digital signature because is considered more technical than Electronic Signature that is more legal. The usage of the term digital signatures was agreed and approved in ESI.
A 7.	Page 10 Section 4.1		te	The text states: PAdES signatures profiled in the present document build on PDF signatures specified in ISO 32000-1 [1] with an alternative signature encoding to support digital signature formats equivalent to the signature format CAdES [2], by incorporation of signed and unsigned attributes described in clause 5. As usual a confusion between digital signature and electronic signature. "ES" means Electronic signature it does NOT mean	Change into: PAdES signatures profiled in the present document build on PDF signatures specified in ISO 32000-1 [1] with an alternative signature encoding to support electronic signature formats equivalent to the signature format CAdES [2], by incorporation of signed and unsigned attributes described in clause 5. The same kind of such change should be done through all the document.	REJECTED. We use the term digital signature because is considered more technical than Electronic Signature that is more legal. The usage of the term digital signatures was agreed and approved in ESI.

Organization name	**Clause/ Subclause**	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change**	**RESOLUTION** on each comment submitted
				Digital Signature (DS). This type of comment will not be repeated for the remaining of the document, but such changes should be done through all the document.		
A 8.	Page 10 Section 4.1			The text states: c) Some signature attributes found in CAdES have the same or similar meaning as keys in the signature dictionary described in ISO 32000-1[1]. The signature dictionary items should be used in preference to CAdES attributes unless specified otherwise in the present document. I disagree. Only one of them should be used. For example, the signing time in a signature attribute is always the UTC time, while with the M key is undefined in ISO 32000-1. So the signed attribute carrying the signing time is much better than the similar key entry. Be informed that this kind of approach is likely to be accepted for DIS 32000-2. See the proposed change.	Change into: c) Some signature attributes found in CAdES have the same or similar meaning as keys in the signature dictionary described in ISO 32000-1[1]. *For signature attributes and keys that have the same or similar meaning only one of them should be used. More details are indicated in this document about the keys and the signature attributes that are concerned.*	PARTIALLY ACCEPTED. What currently stated in item c) isn't misaligned with the proposed text. It's recommended the usage of signature dictionary items (that's only one of them) unless specified otherwise. The text was reworded as follows: c) Some signature attributes found in CAdES [2] have the same or similar meaning as keys in the Signature Dictionary described in ISO 32000-1 [1]. For signature attributes and keys that have the same or similar meaning only one of them should be used according to the requirements set in table defined in clause 6.3 in this document.
A 9.	Page 11 Section 5.4.1	Figure 1		Figure1 is not in accordance with the description of the key "Cert"	Please correct Figure 1 by removing the pointers to the certificates and instead of indirect references to certificates show a few	PARTIALLY ACCEPTED. The text defining DSS and VRI entries has been

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted
				contained in the VRI dictionary". Figure 1 has dotted arrows with pointers included in the VRI dictionary pointing to certificates present in the DSS dictionary. While this is the case for CRLs and OCSP responses, this is not the case for certificates since they are directly included in the key "Cert" of the VRI dictionary. Pointers to certificates do not exist. However, it must be admitted that the figure would have been much better. It is a pity that the description of the VRI dictionary is different from the figure.	certificates.	changed to reflect usage of indirect references instead of array of data.
A 10.	Page 13 Section 5.4.2.3		te	The text states: 5.4.2.3 Signature VRI Dictionary (...) The information consists of the validation time (indicated either by a date object, or a secure time represented by a time-stamp token, or implied by Document Time-Stamp applied to the PDF document immediately after the DSS) and revocation information (which can be either a CRL or an OCSP response). This description is not in	Change into: The information may include certificates, references to CRLs placed in the DSS dictionary, references to OCSP responses placed in the DSS dictionary and either a time-stamp token applied on the previous elements or a date at which the previous elements have been incorporated. Note: The use a time-stamp token applied on the previous elements or a date at which the previous elements have been incorporated	PARTIALLY ACCEPTED. The sentence has been deleted. The VRI table specifications has been moved to substitute the deleted sentence.

Organization name	**Clause/ Subclause**	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change**	**RESOLUTION** on each comment submitted
				accordance with the table on the next page about "Entries in a Signature VRI Dictionary". The description mentions two entries (*consists of*) ... which are both optional. These entries *may be included*. In addition the text is speaking of a " validation time" (.. or *implied by Document Time-Stamp applied to the PDF document immediately after the DSS*). This has nothing to do with the topic of this section which is only concerned with the "Signature VRI Dictionary".		
A 11.	Page 14 Section 5.4.2.3		te	The text states: Any values in the Cert, CRL and OCSP arrays of a Signature VRI dictionary shall also be present in the DSS dictionary applicable to the signature for which this Signature VRI dictionary is associated. This description is not in accordance with the table below about "Entries in a Signature VRI Dictionary". The sentence is not true for Cert. See the next comment for some additional explanations. The letters words "the Cert," should be deleted.	Change into: Any values in CRL and OCSP arrays of a Signature VRI dictionary shall also be present in the DSS dictionary applicable to the signature for which this Signature VRI dictionary is associated.	PARTIALLY ACCEPTED. The text defining DSS and VRI entries has been changed to reflect usage of indirect references instead of array of data.
A 12.	Page 14	Cert key	te	About the "Cert" key in the VRI	Change into:	REJECTED.

Organization name	**Clause/ Subclause**	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change**	**RESOLUTION** on each comment submitted
	Section 5.4.2.3			dictionary, the text states: This array should contain all certificates that were used in the validation of this signature. ... while the key "Certs" in the DSS dictionary indicates: This array contains certificates that can be used in the validation of any signatures in the document. If the key Cert in the VRI dictionary contains all the certificates for a given signature, then the key certs in the DSS dictionary will be empty ! It was believed that the idea was to factorize as much as possible the certificates that can be used to validate more than one signature. With such sentences this will not be the case. Suppress "all" in the first description, as this is the case for the description currently present in DIS 32000-2.	This array should contain certificates that were used in the validation of this signature.	REJECTED All the certificates referenced in the VRI dictionaries shall be referenced in the DSS dictionaries too. The intention is that of recommending the inclusion of all certificates used in the validation of this signature even if some certificate couldn't be included by a conforming signature handler.
A 13.	Page 14 Section 5.4.2.3	TU key	te	About the "TU" key, the text states: A conforming signature	Remove the quoted text.	REJECTED. It's clearly recommended not using the TU key.

Organization name	**Clause/ Subclause**	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change**	**RESOLUTION** on each comment submitted
				handler may ignore this entry and use a different time for the signature validation. The note a) adds: The TU key should not be used. Since using the key TU for validating a signature would be a very bad idea, it is proposed to remove that sentence.		Nevertheless while processing a document containing a VRI dictionary with a value in the TU key, a signature handler can decide to use a different time for signature validation or to use the time stated in the value of the TU key.
A 14.	Page 14 Section 5.4.2.3	TS key	te	About the "TS" key, the text states: .. .and which represents the secure time at which this signature VRI dictionary was created. It would be more accurate to say "before" rather than "at".	Change into: .. .and which represents the secure time before which this signature VRI dictionary was created.	REJECTED. The term before refers to a time that isn’t clearly defined. The term at refers to a clearly defined time (the one in the time-stamp) to which one can trust that the VRI dictionary exists (that’s was created).
A 15.	Page 15 Section 5.5		te	The text states: A PDF document can be encrypted to protect its contents from unauthorized access. This sentence is not correct. Everybody can have an access to the contents, but would not be able to understand its semantics. Encryption hides the semantics of the contents. See the proposed change.	Change into: A PDF document can be encrypted to protect the semantics of its contents.	REJECTED. The sentence can be easily understood as it is.

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted
A 16.	Page 16 Section 6.1		te	The text states: NOTE 1: It is considered that B-B level is sufficient to conform to the Commission Decision 2011/130/EU of 25 February 2011 [i.1]. It would be better to suppress the words "is sufficient to"	Change into: NOTE 1: It is considered that B-B level conforms to the Commission Decision 2011/130/EU of 25 February 2011 [i.1].	REJECTED. The commission decision concerns advanced electronic signatures that must comply with one of the cited ETSI technical specifications. So the conformance of the signature to B-B level is sufficient to conform to CD too. It isn't the B-B level specification that conforms to CD.
A 17.	Page 16 Section 6.1	NOTE 2	te	The text states: NOTE 2: The levels b) to d) are appropriate where the technical validity of signature needs to be preserved for a period of time after signature creation where certificate expiration, revocation and/or algorithm obsolescence is of concern. The specific level applicable depends on the context and use case. The levels d) to d) are not equivalent and with the current sentence it is impossible to understand the properties of each level. See the proposed change.	Change into: NOTE 2: The B-T level is appropriate where the technical validity of signature needs to be checked during the validity period of the signer's certificate. The B-LT level is appropriate where the technical validity of signature needs to be preserved beyond the end of the validity period of the signer's, while the B-LTA level is appropriate <u>when a time-stamp token renewal is needed or when algorithm obsolescence or key length is of concern (see Figure 3)</u>. The specific level applicable depends on the context and use case. However, this does not explain what really a B-LTA level is. It is believed that Figure 3) is appropriate. However the document is fully silent about this. In addition the text does not say that under such cases, that the current revocation status of the previous TSU certificate needs to be captured into the DSS (TS1).A lot of text is	REJECTED. The sentence "The specific level applicable depends on the context and use case" should solve every need to be so accurate in defining when using every single level. In the introduction it's clearly stated that ETSI TR 119 100 provides guidance on how to use the signatures defined in the present document.

Organization name	**Clause/ Subclause**	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change**	**RESOLUTION** on each comment submitted
					missing.	
A 18.	Page 16 Section 6.2.1		te	The text states: The algorithms and key lengths used to generate signatures shall comply with TS 119 312 [8]. (...) NOTE: national legislation can define requirements regarding algorithms and key lengths. This is contradictory. Change the "shall" into a "should".	Change into: The algorithms and key lengths used to generate signatures should comply with TS 119 312 [8].	ACCEPTED.
A 19.	Page 20		ed	Row: SPO: document-time-stamp There is no section 5.3.3 in this document	Please correct.	ACCEPTED.
A 20.	Page 20		ed	Row: SPO: DSS There is no section 5.3.2.2 in this document	Please correct.	ACCEPTED.
A 21.	Page 20		ed	Row: SPO: SPO: DSS / VRI There is no section 5.3.2.3 in this document	Please correct.	ACCEPTED.
A 22.	Page 20		ed	Row: SPO: SPO: document-time-stamp There is no section 5.3.3 in this document	Please correct.	ACCEPTED.
A 23.	Page 21 Item b)			The text states: And when the signature is to be validated through a Trusted List as specified in ETSI TS 119 612-1 [16], the generator should include all intermediary certificates forming a chain between the	Delete the quoted sentence since the previous sentence is sufficient.	ACCEPTED. Note 2 has been reworded as below. In the general case, different verifiers can have different trust parameters and can validate the signer certificate through different chains.

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted
				signer certificate and a CA present in the Trusted List, which are not available to verifiers. Currently, this sentence is incorrect, since TSLs do not include root CAs. It might become true if the content of the TSL is modified.		Therefore, generators may not know which certificates will be relevant for path building. However, in practice, generators can often clearly identify such certificates. In this case, including them in the signature is a good practice, unless verifiers can automatically retrieve them.
A 24.	Page 21 Item f)		te	The text states: f) The commitment-type-indication attribute may be incorporated in the CMS signature only if the signature-policy-identifier attribute is present. Otherwise the commitment-type-indication shall not be incorporated in the CMS signature. There is no reason to mandate this or if there is any there is no indication of that reason. During 10 years the single difference between BES and EPES is the presence or absence of a signature policy identifier. There is no reason to change the meaning.	Change into: Delete the item f) and in the table indicate "may be present"	REJECTED. The sentence doesn't mandate any obligation to include the commitment-type-indication attribute in EPES. The sentence mandates the obligation of not using the commitment-type-indication attribute in BES. This obligation is unchanged with respect of previous PAdES specifications.
A 25.	Page 21 NOTE 2		te	The text states: In the specific case of a signature meant to be validated through TSL, it is advised to include at least the unavailable intermediary certificates up to but not	Delete the sentence:	REJECTED. There is no statement in the sentence that TSLs include root CA certificates.

Organization name	**Clause/ Subclause**	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change**	**RESOLUTION** on each comment submitted
				including the CAs present in the TSLs, since the TSL is information that is shared globally by all verifiers. Currently, this sentence is incorrect, since TSLs do not include the root CA to be used for a given qualified CAs. It might become true if the content of the TSL is modified in the future.		
A 26.	Page 21 Item q)		te	This item relates to the SPO (Service Provision Option): document-time-stamp. The text states: q) The generator shall include the full set of certificates, including the trust anchor when it is available in the form of a certificate, that have been used to validate the signature and which are not already present. This set includes certificates required for validating the signing certificate, for validating any attribute certificate present in the signature, and for validating any time-stamp token's signing certificate (i.e. a TSA certificate) already incorporated to the signature. A "generator" is defined as **"**any party which creates, or adds attributes to, a signature". The use of such a wording is confusing since it is usually not	Change into: q) May be applied either to the document and to the first DSS dictionary or to a DSS dictionary used to capture the certificates and the revocation information related to a previous document-time-stamp (See Figure 3). In the first case, the DSS dictionary contains the full set of certificates, including the trust anchor when it is available in the form of a certificate, that have been used to validate the signature and which are not already present. In the second case, the DSS dictionary contains the full set of certificates, including the trust anchor when it is available in the form of a certificate, that have been used to validate the last document-time-stamp and which are not already present.	PARTIALLY ACCEPTED. The sentence has been changed as below. In situations different than those ones identified in the present clause requirements a) and b), applications should include certificate values within the DSS. The full set of certificates, including the trust anchor when it is available in the form of a certificate, that have been used to validate the signature and which are not already present shall be included. This set includes certificates required for validating the signing certificate, for validating any attribute certificate present in the signature, and for validating any time-stamp token's signing certificate (i.e. a TSA certificate) already incorporated to the signature.

Organization name	**Clause/ Subclause**	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change**	**RESOLUTION** on each comment submitted
				the party which creates the signature which does it. However, the word "shall" is being used. So party which creates a signature shall include the full set ? Obviously not. The impersonal form is proposed to be used to avoid the difficulty.		
A 27.	Page 22 Item t)		te	The text states: t) The generator Same problem as above with the use of the word generator. Please use the impersonal form to avoid the difficulty.	Due to lack of time (it is 11:20 p.m), there is no proposal, but the change should be easy. :	ACCEPTED. The sentence has been changed as in comment 26.
A 28.	Page 22 Item u)		te	The text states: u) The generator Same problem as above with the use of the word generator. Please use the impersonal form to avoid the difficulty.	Due to lack of time (it is 11:21 p.m), there is no proposal, but the change should be easy. :	ACCEPTED. The sentence has been changed as in comment 26.
A 29.	Page 22 Item v)		te	The text states: v) The VRI dictionary should not be used. This is not understandable why. Please explain better.	Please explain better.	ACCEPTED. Added the sentence below The inclusion of VRI dictionary entries is optional. All validation material referenced in VRI entries is

Organization name	**Clause/ Subclause**	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change**	**RESOLUTION** on each comment submitted
						included in DSS entries too.
A 30.	Page 22 Item x)		ed	The third bullet is missing.	Add the missing bullet.	ACCEPTED.
A 31.	Page 22. NOTE 3		te	The text states: NOTE 3: A PAdES-B-LTA signature helps to validate the signature beyond any event that would otherwise limit its validity. This is correct, ... but it is not sufficiently explained. An informative annex would be most welcomed.	Add an informative annex to explain better, the problem of TST renewal and of algorithm or key length obsolescence.	REJECTED In the introduction it's clearly stated that ETSI TR 119 100 provides guidance on how to use the signatures defined in the present document.
A 32.	Page 22 Section 6.4		te	This section is not understandable, see the earlier comment. Could this section be deleted ?	Delete or rewrite it.	ACCEPTED. The sentence has been rewritten.

Organization name	**Clause/ Subclause**	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change** **(added text in red and bold, deleted text is stricken)**	**RESOLUTION** on each comment submitted
B01	all		ed	Be consistent when using "signature dictionary", either with no capital letter everywhere or with	Either use "signature dictionary" or "Signature Dictionary" everywhere	ACCEPTED. The string "Signature Dictionary" has been used everywhere.
B02	scope		ed	"such as" and "for instance" are redundant	(such as the long term validity of digital signatures~~, for instance~~)	ACCEPTED. The string ", for instance" has been deleted.
B03	2.1		ed	There is no need to provide an	Delete all notes that indicate where to find	ACCEPTED. The notes indicating the

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change (added text in red and bold, deleted text is stricken)	RESOLUTION on each comment submitted
				URL for IETF documents	RFCs	URLs for IETF documents have been deleted.
B04	2.1		ed	Last note. Turn it into an editor's note as it won't be valid anymore when the draft ENs will be approved and go for ENAP (EN approval process)	**Editor's** NOTE: The documents [2] and [6] are published in the context of the work in Mandate M460. They might not yet be published.	ACCEPTED.
B05	2.1		Ed	The following references are not normative 319 132-1 TS 119 312 XFA 103 172 RFC 2315 119 612	Move the following references to clause 2.2: [6] EN 319 132-1: "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES Baseline Profile". [8] ETSI TS 119 312: "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites". [13] Adobe**®** ~~XFA: "~~XML Forms Architecture (XFA) Specification" version 2.5, (June 2007)~~, Adobe Systems Incorporated"~~. [14] ETSI TS 103 172 Electronic Signatures and Infrastructures (ESI); PAdES Baseline Profile [15] IETF RFC 2315 (1998) "PKCS #7: Cryptographic Message Syntax Version 1.5" [16] ETSI TS 119 612~~-1~~: "Electronic Signatures and Infrastructures (ESI). Trusted Lists".	ACCEPTED.
B06	2.1		ed	The following references are not used ECRYPT II	Delete the following references: [7] ECRYPT II (European Network of Excellence in Cryptology II): "ECRYPT II Yearly Report on Algorithms	ACCEPTED.

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change (added text in red and bold, deleted text is stricken)	RESOLUTION on each comment submitted
B07	2.2	i.1	ed	Decision was amended in 2014	Commission Decision **2014/148/EU amending Decision** 2011/130/EU ~~of 25 February 2011;~~ establishing minimum requirements for the cross-border processing of documents signed electronically by competent authorities under Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market ~~(notified under document C(2011) 1081)~~.	ACCEPTED.
B08	2.2	i.4	ed		~~"~~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, 28.08.2014, p. 73–114.~~	ACCEPTED.
B09	2.2		ed	Last note. Turn it into an editor's note as it won't be valid anymore when the draft ENs will be approved and go for ENAP (EN approval process)	**Editor's** NOTE: The document [i.7] is published in the context of the work in Mandate M460. It might not yet be published~~.~~	ACCEPTED.
B10	2.2		ed	i.2 is not really used	Delete i.2 and remove note after trust service provider definition	ACCEPTED.
B11	2.2	i.8	ed	Adobe is a registered name	Adobe **®** Supplement to ISO 32000-1. BaseVersion: 1.7 - ExtensionLevel: 5	ACCEPTED.
B12	3.1		ed	Note to generator: as the document avoids using the term seal, I suggest removing this reference to seal	NOTE: This can be the signer ~~or the creator of a seal~~ or any party that initially validates or further maintains the signature.	ACCEPTED.
B13	3.1		ed	Definitions are always within the context of the document, it doesn't need to be specifically indicated + the last part of the definition does not add anything	**proof of existence**: ~~in the contextof the present document, an~~ information that can be used to **prove** ~~proof~~ that some data existed before a given time~~, given in an electronic time-stamp when this electronic time-stamp is assumed to be trusted~~.	ACCEPTED.

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change (added text in red and bold, deleted text is stricken)	RESOLUTION on each comment submitted
B14	3.1		ed	Missing definition for signature handler (which is not in 32000-1)		ACCEPTED. The definition for signature handler has been added.
B15	all		ed	Do not use "conforming" signature handler as anyone claiming conformance with the spec is a conforming handler	Replace "confirming signature handler" with "signature handler"	ACCEPTED.
B16	3.2		ed	The note does not related to VRI	**Delete the note**	ACCEPTED.
B17	4.1	note	ed	No recommendation in a note. Simply state the fact + only saying "subtle dependencies exist" does not help much. Can't you give more hint on the dependencies?	NOTE: Given that PAdES signatures are enveloped inside a PDF document and are detached in the sense of a CMS signature, the signature placement is implied by ISO 32000-1 [1]. In ISO 32000-1 [1], section 12.8.3.3.1 reads "No data shall be encapsulated in the PKCS#7 SignedData field.", no re-statement will be given here, however ~~readers should be aware of the fact that~~ subtle dependencies exist.	PARTIALLY ACCEPTED. The fact that no data shall be encapsulated determines the values of some attributes included in CMS data such as contentType, content and encapContentInfo. We would prefer delete the phrase about these dependencies.
B18	4.1		tec	Why does item a) refer to RFC 5652 and not CAdES part 1? CAdES part 1 has everything needed. Also with current reference to 5652, item c) does not make full sense as CAdES was never introduced in the previous requirements		ACCEPTED. The reference has been updated to CAdES part 1.
B19	4.1		ed		c) Some signature attributes found in CAdES have the same or similar meaning as keys in the signature dictionary described in ISO 32000-1[1]. The signature dictionary items **from ISO 32000-1[1]** should be used in preference to CAdES attributes **[2]** unless specified otherwise in the present document.	ACCEPTED.

Organization name	**Clause/ Subclause**	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change** **(added text in red and bold, deleted text is stricken)**	**RESOLUTION** on each comment submitted
B20	5.2		ed	Wrong use of can and is. See **ETSI Drafting rules** clause 3.2	The attributes included in the following list ~~can~~ **may** be used to generate the DER-encoded `SignedData` object included as the PDF signature in the entry with the key `Contents` of the Signature Dictionary as described in ISO 32000-1 [1], clause 12.8.1. Their syntax ~~is~~ **shall be as** defined in EN 319 122-1 [2], clause 5.	ACCEPTED.
B21	5.2		tec	Can other CAdES attributes be used? I suggest clarifying this. If allowed: Other CAdES attributes as defined in [2] may be used If not allowed: Other CAdES attributes as defined in [2] shall not be used.		ACCEPTED In clause 6.3 it's stated "The attributes defined in ETSI EN 319 122-1 [2] and not listed in table 1 shall not be present". The obligation to refer to clause 6.3 for attributes usage was stated in clause 5.1 too.
B22	5.3		ed	Use shall to specify normative requirements	The entries of the Signature Dictionary **shall be as defined** ~~are set as described~~ in ISO 32000-1 [1], clause 12.8.1 unless specified otherwise in the present document.	ACCEPTED.
B23	5.4.1		ed	Sentence below figure 3 is redundant with all previous text	Delete: ~~Long Term Validaton of PAdES signatures is based on extensions to the PDF document structure described in ISO 32000-1 [1] as specified in clauses 5.4.2 and 5.4.3 which describe how to use the **DSS** dictionary and **VRI** dictionaries to incorporate information for the purposes of performing long-term signature validation.~~	ACCEPTED.
B24	5.4.1		tec	i.8 is an Adobe company specific supplement that does not define		This issue is a bit complicated to be solved.

Organization name	**Clause/ Subclause**	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change** **(added text in red and bold, deleted text is stricken)**	**RESOLUTION** on each comment submitted
				DSS. How can this extension be referred to here? And how come the <</ESIC <</BaseVersion /1.7 /ExtensionLevel 1 >> >> is not mandatory ? also this extension definition shall be in a clause separate from the overview		When using iText to include DSS you obtain <</ESIC <</BaseVersion/1.7 /ExtensionLevel 5>>>> I've seen a PAdES LTV file generated by Acrobat that contains an extension ADBE ExtensionLevel 8, so it's clear that the two extension values that appear in the PAdES document are not the only valid and really used ones. The use of should is due to the fact that adobe has defined its own extension for DSS dictionary. The extension level is an integer defined by the developer to denote the extension being used. If the developer introduces more than one extension to a given BaseVersion the extension level numbers assigned by that developer shall increase over time. In ISO 32000-2 there will be the definition of DSS dictionary. Probably it's better a statement as below The extensions dictionary (see ISO 32000-1 [1], clause 7.12) shall include an entry to define the DSS dictionary usage. The DSS dictionary extension should be defined with the entry: <</ESIC <</BaseVersion /1.7 /ExtensionLevel 1 >>

Organization name	**Clause/ Subclause**	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change** **(added text in red and bold, deleted text is stricken)**	**RESOLUTION** on each comment submitted
						>>
B25	5.4.2.2		Tec/ed	The DSS dictionary here introduces XML signatures while the clause 4 only deals with CMS signatures. It is very confusing	Add a note before the table: NOTE: see EN 3012 142-2 for specification of XAdES signatures of forms signing dynamic XFA.	ACCEPTED.
B26	5.4.2.2	Table, row on “Type”	ed	No need to write “if present” in the value column	(Optional) ~~If present~~ **It** shall be **DSS** for a document security store dictionary. Same applies to all following tables	ACCEPTED.
B27	5.4.2.3	Last note	ed	If there is an ongoing action to make in 32000-1, then write it or delete last sentence of the note	Remove last sentence of ending note: This provision will need to be changed in ISO 32000-1 [1], to allow for the inclusion of LTV, including **DSS** and Document Time-stamps	ACCEPTED. The sentence was removed. Indeed in the latest draft of ISO 32000-2 is stated the following exception in the case of the value 1 for P entry that is, any changes shall invalidate the signature with the exception of subsequent DSS (see 12.8.4.2, "Document Security Store (DSS)") and/or document time stamp (see 12.8.5, "Document level time stamps (PDF 2.0)") incremental updates
B28	5.4.3		ed	Remove parenthesis + clearly indicate that table is in 32000-1	A Document Time-stamp dictionary shall be a standard Signature dictionary ~~(~~as defined in ISO 32000-1 [1], clause 12.8.1~~)~~ ~~but~~ with the following changes. + in table: Modifications to table 252 for a **Document Time-stamp** Dictionary **of 32000-1 [1]**	ACCEPTED.
B29	5.4.3		ed	Wrong use of can	In SubFilter: A conforming reader ~~can~~ **may** use any ~~conforming~~ signature handler	ACCEPTED.

Organization name	**Clause/ Subclause**	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change** **(added text in red and bold, deleted text is stricken)**	**RESOLUTION** on each comment submitted
				+ Type value is always **DocTimestamp,** so the condition is always met	that supports the specified format ~~When the value of `Type` is **DocTimestamp**,~~ the value of `SubFilter` should be **ETSI.RFC3161**	
B30	5.4.3		ed		Since this information ~~may~~ **can** already be present inside of the TimeStampToken contained in Contents, a conforming reader should ignore these keys.	ACCEPTED.
B31	5.4.3		ed	The following sentence does not belong to this: When a PDF already contains a PAdES signature, there is the likely scenario that future updates to that signature and its revocation information may need to take place. This process is done using the same LTV methodology already described. And it is already covered by the sentence in 5.4.1: The life-time of the protection can be further extended beyond the life-time of the last document time-stamp applied by adding further DSS information to validate the previous last document time-stamp along with a new document time-stamp.	Delete: ~~When a PDF already contains a PAdES signature, there is the likely scenario that future updates to that signature and its revocation information may need to take place. This process is done using the same LTV methodology already described.~~	PARTIALLY ACCEPTED. New sentence defined. As the validation data for the last Document Time-stamp becomes at risk for obsolescence or when the encryption technology used for the Document Time-stamp signature becomes at risk for successful attack, there is the likely scenario that updates to the time stamp signature and its revocation information may need to take place. This process is done using the same LTV methodology already described.
B32	5.4.3		ed	The note is exactly the same as the one in 5.4.2.3	NOTE: **see note in clause 5.4.2.3**~~ISO 32000-1 [1], 12.8.2.2, addresses the DocMDP (Modification, Detection and Prevention) feature whereby a set of permissions can be associated with a PDF in conjunction with a certification signature. The permissions of DocMDP~~	ACCEPTED.

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change (added text in red and bold, deleted text is stricken)	RESOLUTION on each comment submitted
					~~are present in the P key of the DocMDP transform parameters dictionary, as an integer in the range 1 through 3. Values of 2 and 3 allow for additional signatures to be included after the certification but a value of 1 does not currently allow any change but allows Document Time-stamps~~.	
B33	6		ed	Use consistent terminology	Replace “PAdES-Baseline” with “PAdES baseline”	ACCEPTED.
B34	6.1		ed	Update note 1 to latest commission decision	NOTE 1: It is considered that B-B level is sufficient to conform to the Commission Decision **2014/148/EU** ~~2011/130/EU of 25 February 2011~~ [i.1].	ACCEPTED.
B35	6.2.1		ed	Align with CAdES and XAdES using should and not shall for the first sentence	The algorithms and key lengths used to generate signatures ~~shall~~ **should** comply with TS 119 312 [8]. + move reference [8] to informative references	ACCEPTED.
B36	6.2.2		ed		Delete: In case where a row specifies the requirements for an attribute or a signature field, the columns have the following meanings: … 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": … 7) Column "References": This **cell**	ACCEPTED.

Organization name	**Clause/ Subclause**	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change** **(added text in red and bold, deleted text is stricken)**	**RESOLUTION** on each comment submitted
					~~shall~~ contain**s** either the number of the clause specifying the attribute or signature field in the present document, or a reference to the document and clause that specifies the attribute or signature field. … EXAMPLE: In table 1, the row corresponding to SPO: DSS signature field has a value "*" in the cells in columns "Presence in B-B level" and "Presence in B-T level", and "shall be present" in cells in columns "Presence in B-LT level" and "Presence in B-LTA level". The cell in column "Cardinality" indicates the cardinality for each level as follows: "B-B, B-T: □0” -B-B and indicate PAdES-B-T signatures can incorporate zero or more instances of SPO: DSS signature field ; “B-LT, B-LTA: □1” indicates that PAdES-B-LT and PAdES-B-LTA ~~shall~~ incorporate**s** one or more instances of SPO: DSS signature field.	
B37	6.3		Tec/ed	Why refer to RFC 2634 and RFC 5035 for SPO: ESS signing-certificate and SPO: ESS signing-certificate-2 while CAdES contains them and eve further defined them?	Replace reference to RFC 2634 and RFC 5035 with reference to CAdES part 1	ACCEPTED. I changed the following sentence in clause 5.1 too. This clause provides details on attributes specified within ISO 32000-1 [1], CAdES [2], ESS (RFC 2634 [4], RFC 5035 [5]), and defines new attributes for building PAdES signatures.
B38	6.3	table	ed	SPO: document-time-stamp, clause number is wrong Item q) seems to relate to	Replace 5.3.3 with 5.4.3 Move q to “SPO:DSS” row	ACCEPTED.

Organization name	**Clause/ Subclause**	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change** **(added text in red and bold, deleted text is stricken)**	**RESOLUTION** on each comment submitted
				SPO:DSS		
B39	6.3		ed	Part of note 2 is redundant with item b	NOTE 2: In the general case, different verifiers can have different trust parameters and can validate the signer certificate through different chains. Therefore, generators may not know which certificates will be relevant for path building. However, in practice, such certificates can often clearly be identified **and included as recommended in item b) above**. ~~In this case, it is advised that generators include them unless they can be automatically retrieved by verifiers. In the specific case of a signature meant to be validated through TSL, it is advised to include at least the unavailable intermediary certificates up to but not including the CAs present in the TSLs, since the TSL is information that is shared globally by all verifiers~~.	PARTIALLY ACCEPTED. Note 2 has been reworded as below. In the general case, different verifiers can have different trust parameters and can validate the signer certificate through different chains. Therefore, generators may not know which certificates will be relevant for path building. However, in practice, generators can often clearly identify such certificates. In this case, including them in the signature is a good practice, unless verifiers can automatically retrieve them.
B40	6.3		ed		d) Generators shall use either the signing certificate or the signing-certificate v2 attribute, depending on the hash function ~~using~~, in accordance with RFC 2634 [4], clause 2. e) Generators should ~~migrate to the~~ use of ESS signing-certificate v2 in preference to ESS signing-certificate in line with the guidance given in TS 119 312 [8]. o) A PAdES-B-T signature ~~can~~ **may** contain several signature-time-stamp or document-time-stamp attributes.	ACCEPTED.

Organization name	**Clause/ Subclause**	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change** **(added text in red and bold, deleted text is stricken)**	**RESOLUTION** on each comment submitted
B41	6.3	Item p	tec	Cannot say first “shall reserve…” and then alternatively.	p) **if it is anticipated to propagate them to a higher level using the signature-time-stamp attribute [2],** The PAdES-B-B signatures ~~as profiled in clause 6.3~~ shall reserve space for the signature-time-stamp attribute [2], ~~clause 5.3, if it is anticipated to propagate them to a higher conformance level~~. ~~Alternatively a document-time-stamp can serve this purpose, which covers the whole document including the signature value and can be applied before the DSS and DSS/VRI~~	PARTIALLY ACCEPTED. New sentence. If it is anticipated to propagate PAdES-B-B signatures to a higher conformance level, they can reserve space for the signature-time-stamp attribute [2]. Alternatively a document-time-stamp, which covers the whole document including the signature value, can serve this purpose.
B42	6.3		ed	Merge q and r as for the time being the use of shall on q and should in r is confusing; and move text of q after text of r	q) In situations different than those ones identified in requirements a) and b), applications should include certificate values within the DSS. In this case, the generator shall include the full set of certificates, including the trust anchor when it is available in the form of a certificate, that have been used to validate the signature and which are not already present. This set includes certificates required for validating the signing certificate, for validating any attribute certificate present in the signature, and for validating any time-stamp token's signing certificate (i.e. a TSA certificate) already incorporated to the signature.	ACCEPTED.
B43	6.3		ed		w) PAdES-B-LTA signatures ~~can~~ **may** have more than one document-time-stamp applied after the DSS and DSS/VRI.	ACCEPTED.