Resolution of comments on Drafts ETSI *EN 319 142-1 to* ETSI *EN 319 142-7 – 31 May 2014*

PAdES

Foreword: Please note that the following disposition of comments is provided to the light of the current context of the m460 mandate, in particular with regards to Directive 1999/93/EC. It should be noted that such disposition should be reviewed to the light of the eIDAS Regulation.

Comment number	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	Resolution on each comment submitted
Comment 1	**Introduction**	**7th paragraph**	**ed**	Not each electronic signature authenticates the identity of the person signing the pdf as described in " ISO 32000-1 [1] identifies the ways in which an electronic signature may be incorporated into a PDF document to authenticate the identity of the user and validate integrity of the document's content." Authentication of a person requires electronic signatures issued in a standardized process where the person needs to proof his or her identity first before the electronic signature can be used for identity claiming purpose. An alternative is to identify a signatory based on biometric data. Unfortunately providing biometric data in a PAdES defined data format is not defined or referenced within the PAdES document.	Delete "authenticate the identity of the user and"	**The authentication of the identity of the signer should be guaranteed if the signer is using a qualified certificate. In all other cases there is, however, a policy which manages the life cycle of the certificate (from the authentication of the certificate requestor data to the generation of the certificate and so on to the expiring or revocation of the certificate). So each electronic signature, in a more or less precise way, authenticates the identity of the signer.** Actual clause: Clause 12.8 of ISO 32000-1 [1] identifies the ways in which an electronic signature may be used to authenticate the identity of a user and the accuracy of the document's content. These electronic signatures are based on the same CMS [10] technology and techniques on which EN 319 122 [3] (CAdES) is

						based too, without the extended signature capabilities of CAdES itself, i. e.for the purposes of long term validation. New clause: Clause 12.8 of ISO 32000-1 [1] identifies the ways in which an electronic signature may be used to authenticate the accuracy of the document's content and the signatory identity information included in the signing certificate (whose level of trust depends on the certificate policy). These electronic signatures are based on the same CMS [10] technology and techniques on which EN 319 122 [3] (CAdES) is based too, without the extended signature capabilities of CAdES itself, i. e.for the purposes of long term validation.
Comment 2	**5.1.2**		**ed**	See comment 1 for authentication of signatory d) Signature protects integrity of the document and authenticates the signatory.	**Delete** "authenticates the signatory."	Actual clause: Signature protects integrity of the document and authenticates the signatory. New clause: Signature protects integrity of the document and authenticates the signatory identity information included in the signing certificate.
Comment 3	**5.2.2**		**ed**	See comment 1 for authentication of signatory d) Signature protects integrity of the document and authenticates the signatory.	**Delete** "authenticates the signatory."	**Obsolete by document restructuring**

Comment 4	**5.3.2**		**ed**	See comment 1 for authentication of signatory d) Signature protects integrity of the document and authenticates the signatory.	**Delete** "authenticates the signatory."	**Obsolete by document restructuring**
Comment 5	**5.7.2**		**ed**	See comment 1 for authentication of signatory b) The XAdES signature protects integrity of what is signed and authenticates the signatory.	**Delete** "authenticates the signatory."	**Obsolete by document restructuring**
Comment 6	**5.8.2**		**ed**	See comment 1 for authentication of signatory b) The XAdES signature protects integrity of what is signed and authenticates the signatory.	**Delete** "authenticates the signatory."	**Obsolete by document restructuring**
Comment 7	**5.1** **[EN 319 142-6]**		**T**	In the representation of a PAdES signature, it is said that one of the recommended information to be displayed is the name of the signatory. In Spain, and in some other countries, the CN can carry not just the full name but also the local identifier (ie: national ID number). This information is frequently required when signing documents and therefore it should be displayed.	**a) Name of signatory, mandatory, and other ID data, if relevant (as in CN)**	**Accepted clause 5.1 and 6.2 of EN 319 142-6 ws modified as asked by the Spanish Ministry.**
Comment 8	**2.1 [7]** **[EN 319 142-7]**		**G**	TS 102 176-1 could be replaced with TS 119 312		**Accepted. It was modified in version 0.0.3 of [EN 319 142-7]**
Comment 9	**general** **ETSI EN 319 142-1 v0.0.3**		**tech**	**draft has no normative requirements (§4 informative, §5 copies normative requirements from other parts, §6 informative).** **Requirements are never duplicated between standards; so all clause 5 can be deleted**	**Drop this part** **move clause 4 to informative annex of part 2** **clause 5 is already covered by the other parts** **clause 6: split the bullets and assign them to each relevant profile (bullet a in part 4...)**	**Accepted. Produced new docs according ETSI comments.** **Part 1 will disappear and a note will be added to part 2, explaining the history of the multipart standard.**

					change part numbering of other parts	
Comment 10				**2 Security Problem 1: Forged Certificate Replacement Attack (The problem of overwritten Object ID)** **2.1 Description of the problem** **This problem is concerned with the property of Object ID defined in the PDF specification. It is possible that the valid certificate stored in the PAdES-LTV can be replaced by the forged certificate.** **The objects of the PDF are identified by Object ID and the numbers of Object ID are assigned by a PDF software.** **According to the property of the PDF, if the new object (object A) is appended by using incremental update and it uses the same Object ID as the object (object B) that has already stored in the PDF data, only the object A can be referred by the latest reference table of the PDF data and the object B logically disappears from the latest reference table. By using this property, the attacker can replace the validation information that stored in the PAdES-LTV data by the forged validation information (Figure 1).** **If the signature uses the form of the PAdES-Enhanced, the forged certificate can be detected by comparing ESSSigningCertificate attribute. But if the PAdES-Basic is used, the detection of the replacement can not be expected.** **In another case, the attacker might replace the revocation information by the forged one in order to repudiate the signature. The replacement of the revocation information can be detected by the attribute.**	**Because this problem is based on the general property of the PDF, it is difficult to solve the problem by making a limitation of generating Object IDs. The verifier needs to detect the overwritten validation information in order to prevent from the attack. An additional rule of validation should be described in the PAdES specification as follows:** **"The validation application shall trace the history of the cross reference table and check that the Object ID of the validation information is not overwritten. If the overwritten Object ID is found, the posterior object overwriting the Object ID shall be ignored."**	Partly rejected. After a deep investigation with Adobe engineers the STF came to the conclusion that this type of attack should not be considered feasible or at least dangerous. The reasons are the following: The certificates that are represented as individual objects in PDF are not related to signatures and timestamps but only to revocation material (CRL and OCSP). The certificates related to signatures and timestamps are embedded in the CMS or CAdES objects and are not available as individual objects in the PDF. Therefore, there is no way to replace them with incremental updates using the same Object ID. The certificates related to revocation material are used for trust chain building and they represent an additional source of the potential pool of certificates that might also come from other sources. The /Certs array in DSS just specifies one more source for this pool. If someone replaces a good (usable for the chain building) certificate in DSS with a bad (unusable for the chain building) certificate in DSS, the only effect this may have is that a conforming Reader may not be able to build the chain to verify the validation materials, possibly (but not necessarily) making the signature status as Unknown. This situation applies to OCSPs and CRLs collected as validation material. They are signed and must be checked against a

						trusted root. If their signatures cannot be validated they should be discarded, as if they would not be there at all. For the validation to succeed, both the CRL/OCSP and the replaced certificate associated to it must chain up to the same trusted root, with the exception of indirect CRLs. Yet, even in the case of indirect CRL the signature over the CRL must chain up to a trusted root. The result is that you cannot just replace a certificate to inject a fake CRL and let the signature validator to use this CRL indiscriminately. Any more sophisticated attacks that would succeed in producing a valid but fake CRL or a valid cert to verify a fake CRL would be based on more generic cryptographic failures that are not specific to PAdES standards or implementations and should not be covered here. The only relevant risk related to malicious Object ID replacement is then to override existing and valid validation material with fake or invalid validation material with the scope to prevent the full validation of the signature according to an LTV profile (sort of Denial of Service). A note to implementers will be added warning about the risk of re-using Object IDs because of the possibility to “hide” existing validation material. Implementers may check the existence of older validation material having the same Objec IDs if they want to be explicitly aware of the fact that the latest objects contain invalid or unusable validation material.

Coment 11				**3 Interoperability Problem 1: Signing to Encrypted PDF** **3.1 Description of the problem** **The PDF data can be encrypted by the method described in ISO 32000-1. But the method of signing to the encrypted PDF data is unclear.** **ISO 32000-1 describes fields excluded from the encryption. Because the signature data in the Content of the signature dictionary is not contained in the fields, it is possible to consider that the signature data in the Content of the signature dictionary shall be encrypted.** **But Adobe products apply unencrypted signature data to the Content of the signature dictionary and there are many implementations following the specification of Adobe. The stream objects of certificates and revocation information used in the PAdES-LTV data have the same problem. While the necessity of encrypting these objects is unclear in ETSI TS 102 778, Adobe products set unencrypted objects in the PAdES-LTV data.** **The lack of the rule for the encryption will cause interoperability problem of implementations.**	**An additional rule of the encryption should be described in ETSI TS 102 778. But more discussion is necessary to the rule.**	Accepted. The proposal is to add a new Encryption section which replicates the beginning of the ISO paragraph on encryption and then adding the exception. **A PDF document can be encrypted to protect its contents from unauthorised access. When encryption and signatures are combined together in a single PDF document, encryption shall be applied to its content before any signatures may be incorporated into it.** **Encryption applies to all strings and streams in the document's PDF file, with the following exceptions:** **• The values for the ID entry in the trailer** **• Any strings in an Encrypt dictionary** **• Any strings that are inside streams such as content streams and compressed object streams, which themselves are encrypted** **• Any hexadecimal strings representing the value of the Contents key in a Signature dictionary.** Clause 7.6 of ISO 32000-1 contains detailed information about the use of encryption in PDF files. In PAdES Part 2, a new clause will be created as 5.7 (Requirement on Encryption) Part 3 will add the same requirement by referencing to part 2 As a reference, in ISO 32000-2

						Adobe will propose to modify clause 7.6.1 as follows: **A PDF document can be encrypted (PDF 1.1) to protect its contents from unauthorised access. Encryption applies to all strings and streams in the document's PDF file, with the following exceptions:** **• The values for the ID entry in the trailer** **• Any strings in an Encrypt dictionary** **• Any strings that are inside streams such as content streams and compressed object streams, which themselves are encrypted** **• Any hexadecimal strings representing the value of the Contents key in a Signature dictionary**
Comment 12				**4 Interoperability Problem 2: Hash calculation for VRI key** **4.1 Description of the problem** **Annex A.1 of ETSI TS 102 778-4 describes the target of the hash used for VRI key as follows:** **"For a document signature the bytes that are hashed are those of the signature's DER-encoded PKCS#7 (and its derivatives) binary data object (base-16 decoded byte string in the Contents entry in the signature dictionary). For the signatures of the CRL and OCSP response, it is the respective signature object represented as a BER-encoded OCTET STRING encoded with primitive encoding. For a Time-stamp's signature it is the bytes of the Time-stamp itself since the Time-stamp token is a signed data object."** **In calculating the hash on the signature(or the timestamp), some implementations include the zero padding of the Contents**	**4.2 Proposal** **The specification shall clarify the inclusion(or exclusion) of the zero padding.**	Resolution: Agree with the suggested clarification. **NOTE 1:** • **For document signatures or document timestamp signatures, the bytes that are hashed are those of the complete hexadecimal string in the Contents entry of the associated signature dictionary, containing the signature's DER-encoded binary data object (e.g. PKCS#7,**

				entry and others exclude the zero padding. For example, Adobe Acrobat includes the zero padding in the hash calculation of the signature, but it excludes the zero padding in the case of the timestamp. **A problem of the VRI is that the range of field protected by the timestamp in TS entry of VRI is missing in the specification. The range of fields used to calculate MessageImprint needs to be added to the explanation of TS entry.**		**CMS or CAdES objects).** • **For the signatures of CRLs or OCSP responses, the bytes that are hashed are the respective signature objects represented as BER-encoded OCTET STRING encoded with primitive encoding.** • **The inclusion of VRI dictionary entries is optional. All validation material referenced in VRI entries is included in DSS entries too.** Regarding the range of field protected by the timestamp TS entry of VRI, the comment from JNSA seems due to the fact that in Note 2 of the table "Entries in a Signature VRI dictionary" there is no explicit reference to TS entry of VRI dictionary (even if it should be clear that the Note is referred to MessageImprint calculation of timestamp stored in TS entry itself). In such case, we could solve the comment adding the reference to TS entry in Note 2 that would state as following.

						For PKCS#7 signatures the datum that is hashed and included in the messageImprint field of the DER-encoded time-stamp stored in TS entry (see RFC 3161 [6]) is the encryptedDigest field in the signature's PKCS#7 object (see RFC 2315 [4]).
Comment 13				Does PAdES allow to generate a PAdES-LTV with document timestamp on PAdES-BES?	Proposal Could PAdES-LTV be aligned with CAdES-A and XAdES-A regarding the mandatory presence of a signature timestamp?	In the PAdES core specification it is allowed to add a document time-stamp on a PAdES-BES. To implement a change to be aligned with CAdES-A or XAdES-A, alignment to ISO 32000 must also be considered. The presence of the signature time-stamp is recommended but not mandatory in the core specification.
Comment 14				5 Interoperability Problem 3: Validation process of PAdES-LTV 5.1 Description of the problem Section 4.2 of ETSI TS 102 778-4 describes the validation process of PAdES-LTV as follows: " 1) The "latest" document Time-stamp should be validated at current time with validation data collected at the current time. 2) The "inner" document Time-stamp should be validated at previous document Time-stamp time with the validation data present (and time-stamped for the successive enveloping time-stamps) in the previous DSS. 3) The signature and the signature Time-stamp should be validated at the latest innermost LTV document Time-stamp time using the validation data stored in the DSS and time-stamped (by the successive enveloping time-stamps)"	5.2 Proposal The item 3) of Section 4.2 in ETSI TS 102 778-4 should be described as follows: "3) The signature should be validated at the earliest signature Time-stamp and the signature Time-stamp should be validated at the latest innermost LTV document Time-stamp time. The signature and the signature Time-stamp should be validated using the validation data stored in the DSS and time-stamped (by the successive enveloping time-stamps)"	Rejected. This point should have been resolved by referring to the validation in EN 319 102

				The description of item 3) is inconsistent with the processes of CAdES and XAdES, the procedures defined in ETSI TS 102 853. In these processes, the signature should be validated at the time of the earliest signature timestamp.		
Comment 15	**All ESI drafts**		**tech**	**The writing of all drafts needs improvements to enhance the quality**	**Apply the following rules:** **- the standard should specify all the requirements necessary to achieve its objective and ONLY include essential supporting information** **- use only appropriate verbal forms to express provisions, as defined in ETSI Drafting rules clause 14a (http://portal.etsi.org/edithelp/HowToStart/home.htm?page=DraftingRules)** **- shall/should/may are used only when writing provisions defined by the document itself.** **- do NOT use alternative forms such as is required to** **- "will/will not" shall be used to indicate behaviour of equipment or sub-systems outside the scope of the deliverable in which they appear** **- "can/cannot" shall be used for statements of possibility and capability. When document on signature policy says 'the signature policy may support X", a document on AdES format will say**	**Rejected: we are currently not aware of any violations to this rules in the draft for EN319 142**

					"the signature policy can support X" (a permissible actions defined in document D becomes a possibility in other documents) **- never use present tense to express a provision. Present tense is only a description of facts** **- Clearly separate provisions (shall/should/may) from complementary informative text (e.g. using notes, examples, or moving it to informative annex) so that implementers clearly know what they have to implement.- never duplicate text. Only say things once.** **- do not copy provisions from other standards. If they are applicable, then write text like "RFC 5256 shall apply", "the attribute shall be as defined in <clause c> of XXX"** **- fully review scopes: scope defines without ambiguity the subject of the ETSI deliverable and the aspect(s) covered, thereby indicating the limits of applicability of the ETSI deliverable or particular parts of it. It shall not contain requirements. The scope shall be succinct so that it can be used as a summary for bibliographic purposes. Do not describe all clauses.** **- introduction: do not duplicate text with the scope. Introduction is not the scope. Introduction**	

					gives specific information or commentary about the technical content of the ETSI deliverable, and about the reasons prompting its preparation. It shall not contain requirements **- keep it impersonal: do not use I, you, we** **- do not use colloquial language** **- tables: use ETSI drafting rules**	
Comment 16	**General**			XXX highly appreciates the activities at ETSI M/460 phase 2, which address particularly long term aspects of electronic signatures. However it seems that the current scope of the proposed • "Draft ETSI EN 319 142-5 V0.0.3 (2013-11) Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 5: PAdES for XML Content -Profiles for XAdES signatures " only covers those approaches without an optional usability of evidence records according RFC 4998, which are not optimal with respect to scalability -- each archived document requires independent archive time stamps -- and are not integrated with the international archival architectures standardized in • ISO 14721 "Space data and information transfer systems - Open archival information system - Reference model" and • ISO "14533-1:2012 Processes, data elements and documents in commerce, industry and administration -- Long term signature profiles -- Part 1: Long term signature profiles for CMS Advanced Electronic Signatures (CAdES) (2012) and	Therefore it is proposed to enlarge the scope of the Draft ETSI EN 319 142-5 V0.0.3 (2013-11) to cover the alternative approach as well, which is based on the Evidence Record Syntax normalized in RFC 4998 or and RFC 6283. and may be integrated with archival systems based on ISO 14721 and ISO 14533 {C,X}AdES, OASIS DSS v1.0 Profile for Comprehensive Multi-Signature Verification Reports, DIN 31647 and TR 03125..	1. The STF 458 Area 1 Task 2 team proposes not to incorporate ERS management within all the AdES formats at this point in time. 2. The STF 458 Area 1 Task 2 team proposes to incorporate ERS management within ASiC packages so that signatures (CAdES, XAdES, ...) that have been archived and preserved using ERS mechanisms, may be extracted from the archive, be packaged with the signed data objects, partial hash tree, and archive time-stamps, and be securely transferred to a different destination, where a relying party may still successfully validate the signatures. The new text will also provide guidance on the data objects that should also be securely archived within the ERS archive, for ensuring that the signature and all the required validation material is correctly preserved, and that once the signature and all the required validation material are extracted and incorporated to the ASiC package, the signature may be successfully validated.

				• ISO 14533-2:2012 Processes, data elements and documents in commerce, industry and administration -- Long term signature profiles -- Part 2: Long term signature profiles for XML Advanced Electronic Signatures (XAdES) (2012) • OASIS DSS v1.0 Profile for Comprehensive Multi-Signature Verification Reports Version 1.0 Committee Specification 01 (2010) **and the German DIN-Standard** • DIN 31647, Information and Documentation - Preservation of evidence of cryptographically signed electronic records (Beweiswerterhaltung kryptographisch signierter Dokumente), DIN draft standard. (2013) and even • EN 319 122 CMS Advanced Electronic Signatures (CAdES) Part 1 <http://docbox.etsi.org/ESI/Open/Latest_Drafts/prEN-319122-1v003-CAdES-core-STABLE-DRAFT.pdf> : Core Specification.		3. The STF 458 Area 1 Task 2 team does not close the door to a potential incorporation of ERS within the different AdES formats, once analyzed the requirements for such an incorporation (which could also include an analysis of alternative archival systems), as all the different AdES formats include at this point in time extension mechanisms that would easily allow the definition of a potential new attribute (CAdES), property (XAdES), or dictionary (PAdES).
Comment 17	Chapter 2.1	Normative references	E		**Proposal:** Please add: [8] IETF RFC 4998 (2007): "Evidence Record Syntax (ERS)" [9] IETF RFC 6283 (2011): "Extensible Markup Language Evidence Record Syntax (XMLERS)"	**See above**
Comment 18	Chapter 4.3.4	Validation Process	T		**Proposal:** Please add: Any timestamp present within an Evidence Record should be validated according to [8] or [9].	**See above**

Comment 19	Chapter 5.3.3	General Requirements	T	**Current Text:** Conforming signature handlers shall be able to sign and/or verify signed XFA dynamic forms with XAdES-LTV signatures aligned with the present profile. In addition, conforming signature handlers shall support PDF documents with: a) Document security store information as specified in clause A.1 of [i.9]. b) Document time-stamps as specified in clause A.2 of [i.9].	**Proposal:** Conforming signature handlers shall be able to sign and/or verify signed XFA dynamic forms with XAdES-LTV signatures aligned with the present profile. In addition, conforming signature handlers shall support PDF documents with: a) Document security store information as specified in clause A.1 of [i.9]. b) Document time-stamps as specified in clause A.2 of [i.9]. **c) Document time-stamps as specified in clause A.3 of [i.9].**	**See above**
Comment 20	Chapter 5.3.4	Validation Process	T		**Proposal:** Please add: Any timestamp present within an Evidence Record should be validated according to [8] or [9].	**See above**
Comment 21	Annex A (informative):	Matching of Basic PAdES-LTV XAdES-based profiles to XAdES		**Current Text in Entry 4:** • The certificates and cert status data (CRLs or OCSP responses) referencing by DSS as specified in clause A.1 of EN 319 142-4. • A document Time-stamp as specified in clause A.2 of TS EN 319 142-4 [i.9].	**Proposal for Entry 4** • The certificates and cert status data (CRLs or OCSP responses) referencing by DSS as specified in clause A.1 of EN 319 142-4. • A document Time-stamp as specified in clause A.2 of TS	**See above**

					EN 319 142-4 [i.9]. • **An Evidence Record as specified in clause A.3 of TS EN 319 142-4 [i.9].**	
Comment 22				**Current Text in Entry 5:** • The certificates and cert status data (CRLs or OCSP responses) referencing by DSS as specified in clause A.11 of EN 319 142-4. • A document Time-stamp as specified in clause A.2 1 of EN 319 142-4 [i.9]	**Proposal for Entry 4** • The certificates and cert status data (CRLs or OCSP responses) referencing by DSS as specified in clause A.11 of EN 319 142-4. • A document Time-stamp as specified in clause A.2 1 of EN 319 142-4 [i.9] • **An Evidence Record as specified in clause A.3 of TS EN 319 142-4 [i.9].**	**See above**
Comment 23	**General**			XXX highly appreciates the activities at ETSI M/460 phase 2, which address particularly long term aspects of electronic signatures. However it seems that the current scope of the proposed • "Draft ETSI EN 319 142-4 V0.0.3 (2013-11) Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 4: PAdES Long Term - PAdES-LTV Profile" only covers those approaches without an optional usability of evidence records according RFC 4998, which are not optimal with respect to scalability -- each archived document requires independent archive time stamps -- and are not integrated with the international archival architectures standardized in • ISO 14721 "Space data and information transfer systems - Open archival information system -	Therefore it is proposed to enlarge the scope of the Draft ETSI EN 319 142-4 V0.0.3 (2013-11) to cover the alternative approach as well, which is based on the Evidence Record Syntax normalized in RFC 4998 and may be integrated with archival systems based on ISO 14721 and ISO 14533 {C,X}AdES, OASIS DSS v1.0 Profile for Comprehensive Multi-Signature Verification Reports, DIN 31647 and TR 03125..	**See above**

				Reference model" and • ISO “14533-1:2012 Processes, data elements and documents in commerce, industry and administration -- Long term signature profiles -- Part 1: Long term signature profiles for CMS Advanced Electronic Signatures (CAdES) (2012) and • ISO 14533-2:2012 Processes, data elements and documents in commerce, industry and administration -- Long term signature profiles -- Part 2: Long term signature profiles for XML Advanced Electronic Signatures (XAdES) (2012) • OASIS DSS v1.0 Profile for Comprehensive Multi-Signature Verification Reports Version 1.0 Committee Specification 01 (2010) **and the German DIN-Standard** • DIN 31647, Information and Documentation - Preservation of evidence of cryptographically signed electronic records (Beweiswerterhaltung kryptographisch signierter Dokumente), DIN draft standard. (2013) and even • EN 319 122 CMS Advanced Electronic Signatures (CadES) Part 1 <http://docbox.etsi.org/ESI/Open/Latest_Drafts/prEN-319122-1v003-CAdES-core-STABLE-DRAFT.pdf> : Core Specification.		
Comment 24	Chapter 2.1	Normative references	E		**Proposal:** Add: [11] IETF RFC 4998 (2007): "Evidence Record Syntax (ERS)"	**See above**
Comment 25	Annex A (normative) ISO 32000-1 LTV	New chapter A.3	T		**Proposal:** Proposed solution for PadES-LTV:	**See above**

	Extensions				**Add specific Evidence Record signature dictionary** (e.g. in TS 102778-4, § A.3) with the following characteristics: • Type (optional): Evidence Record • SubFilter (required): ETSI.RFC4998 • Contents (required): Byte string representing the Evidence Record according to RFC 4998 • V (optional): Version, default value: 0	
Comment 26	**Annex B**	**p. 20**	**T**	**Current Text:** NOTE 3: The process for upgrading the signature with successive document time-stamps and their corresponding validation data (certificates and certificate status) is equivalent to the process for upgrading a CAdES-A signature by adding successive archive-time-stamps.	**Proposal:** NOTE 3: The process for upgrading the signature with successive document time-stamps and their corresponding validation data (certificates and certificate status) is equivalent to the process for upgrading a CAdES-A signature by adding successive archive-time-stamps **or Evidence Record**.	**See above**