Public Review: resolution of public comments on Draft ETSI EN 319 122-1 v0.0.8

CAdES digital signatures;

Part 1: Building block and CAdES baseline signatures

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change (by the organisation)	RESOLUTION on each comment submitted
A-1	Foreword (page 6)	In front of the box	Editorial		Replace “an evolved specifications” by “evolved versions”	Fixed according to the comment “C 02”
A-2	1	2nd NOTE on page 7	Editorial	The second note (including introductory sentence) is redundant.	Remove second note.	Accepted
A-3	2		Editorial	The note that references are either specific or non-specific applies to normative and informative references.	Move note (“References are either … http://docbox.etsi.org/Reference.” to the beginning of section 2.	The duplication of the note originates from ETSI template.
A-4	2.1	NOTE in front of references	Editorial	There are no hyperlinks.	Remove the note which addresses hyperlinks.	The duplication of the note originates from ETSI template.
A-5	2.1	[1]	Editorial	There seems to be an inconsistency between reference [1] (ETSI TS 103 173) and its usage in section 5.6 (ETSI 101 733).	Remove inconsistency.	Inconsistency fixed.
A-7	2.1	NOTE in front of [12]	Editorial		Replace “RFC 2660” by “RFC 2560”.	Fixed.
A-8	2.1	NOTE after [12]	Editorial		Replace “Recommendations” by “Recommendation”.	Fixed.
A-9	2.1	[18]	Editorial	The reference is too unspecific. There are different SAML versions (v1.0, v1.1 v2.0), which consist of different parts.	Clearly specify which version and part of SAML is meant to be referenced here.	Fixed. Use the last version.
A-10	2.2	NOTE in front of	Editorial	There are no hyperlinks.	Remove the note which	ETSI template.

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change (by the organisation)	RESOLUTION on each comment submitted
		references			addresses hyperlinks.	
A-11	3.1	Certificate Revocation List (CRL)	Editorial		Add missing "."	Fixed.
A-12	4.1	3rd paragraph.	Technical	The relationship between EN 319 122 and EN 319 102 should be clarified. Maybe the "should be taken into account" should probably be a "must …"?	Check "should" vs. "must".	Paragraph has been removed. We already say in the Scope clause that validation is out of the scope of the document.
A-13	4.4 / 4.5		Editorial	The note "The degenerate case …" would better fit in Section 4.6, which deals with the `SignerInfo` type.	Remove notes in Section 4.4 and 4.5 and insert it in Section 4.6.	Accepted.
A-14	5.1	3rd (=last) paragraph	Editorial		Replace "fileds" by "fields".	Accepted.
A-15	5.3.2.2		Technical	As SHA-1 is known to have severe weaknesses and the cryptographic community expects that collisions will soon be found for the full 80 rounds of SHA-1[1] and one may expect that suitable certificates can be constructed as it was the case for MD5[2]. While existing signatures which use the SHA-1-based ESSCertID must be verifiable, there is no reason why signatures with this attribute should be generated anymore.	The SHA-1-based signing-certificate attribute should be deprecated for the generation of new signatures and moved to annex A.2.	Rejected. If we do that, we need a general note in the document to say "should" not use SHA-1. There is a clause "Algorithm requirements" in Clause 6 that allows "National legislation can define requirements regarding algorithms and key lengths"
A-16	5.3.2.3	Paragraph between the two NOTEs.	Editorial		Replace "used.If" by "used. If"	Accepted.

1 See http://eprint.iacr.org/2011/641.pdf for example.

2 See http://eprint.iacr.org/2006/360.pdf .

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change (by the organisation)	RESOLUTION on each comment submitted
A-17	5.3.6.1	NOTE 3 (Page 19)	Editorial	Whether a signed assertion is less restrictive (whatever this means) than an attribute certificate depends on the policy of the CA / IdP which creates the attribute certificate / assertion.	Replace "However, it is less restrictive…" with "However, it may be less restrictive…".	Accepted.
A-18	5.3.6.1	NOTE 4 (Page 19)	Editorial	The term "SAML token" is not defined in the SAML specification. Is a SAML "assertion" meant here?	Clarify terminology and fix sentence (e.g. by replacing "SAML token, see of SAML [18]" by "SAML assertion, see [18]".	Accepted.
A-19	5.3.10	`sigPolicyLocalURI`	Technical	It is not clear why the `sigPolicyLocalURI` choice makes sense in addition to the `SPuri` element within the `SigPolicyQualifierInfo` element. Furthermore it is by no means clear what "local" means here.	Clarify why the `sigPolicyLocalURI` choice is necessary or drop this option.	Rejected. `SPuri and sigPolicyLocalURI are different` Note in 5.2.10: NOTE 1: Contrary to the `SPuri`, the `sigPolicyLocalURI` points to a local file.
A-20	5.5.2.1	OCSP response types	Technical	It is not clear why both `OCSPResponse` and `BasicOCSPResponse` should be allowed to be used here. From an interoperability point of view it would be advisable to remove the option and clearly specify how the OCSP response should be embedded	Remove the `BasicOCSPResponse` option and require that OCSP responses are to be embedded in the other field of the `RevocationInfoChoices` as `OCSPResponse` and explain this choice by referring to RFC 5940 [10].	Minor update. In 5.5.2.2: added "using the encoding of OCSPResponse" in 5.5.2.2 to clearly say that OCSPResponse should be used within `RevocationInfoChoices` Allowing both OCSPResponse and BasicOCSPresponse is for backward compatibility.

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change (by the organisation)	RESOLUTION on each comment submitted
				here. Against the background of the `RevocationValues` attribute and the fact that embedding unsuccessful OCSP responses in a CAdES signature does not make sense, the better choice (modulo RFC 5940) would seem to be `BasicOCSPResponse`. As RFC 5940 however requires to embed the `OCSPResponse` structure it should also be used here.		
A-21	5.6		General	The archive validation data presented in section 5.6 **FAIL** to provide an effective, comprehensive and harmonized solution for long term archiving of electronic signatures! A central problem with respect to the **LONG TERM** archiving of electronic signatures is that the conclusiveness of the signature and additional data, which is used within the verification process (e.g. certificates, revocation information and related proofs of existence (i.e. time stamps, evidence records)), need to be preserved over long periods of time for	Completely revise section 5.6 in order to provide effective data structures for archive validation data in which it is outlined how existing archive validation data can be incorporated and maintained over a long period of time. The revised section 5.6 **MUST** explain how archive time stamps can be nested to preserve the evidence over long periods of time and the revised presentation **SHOULD** explain how the different versions of legacy archive time stamps defined in previous CAdES version can (and should) be integrated and preserved in a unifying manner. This revised	Rejected. See details below the table

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change (by the organisation)	RESOLUTION on each comment submitted
				which formats[3], custodians and especially cryptographic algorithms are likely to change. This means that an effective solution for long term archiving of signed data **MUST** be capable of handling the transition from one generation of cryptographic algorithms (i.e. hash algorithm and signature algorithm) to the next generation of cryptographic algorithms. This important aspect does **NOT** seem to be considered in Section 5.6 at all. Therefore section 5.6 **MUST** be revised and extended to cover the aspect of **NESTING** of archive time stamps in order to ensure the "long term viability" of the specified archive validation data. Given the current understanding of the specified archive-time-stamp-v3 attribute together with the auxiliary ats-hash-index-v2 attribute (see figure at the end of this comment sheet) it seems that these attributes in the currently specified form are	section **SHOULD** also consider archive time stamps based on hash trees as specified in RFC 4998 and RFC 6283 as they allow to protect a large number of signatures with a single archive time stamp. If section 5.6 cannot be revised in a timely manner the long term validation aspects MUST be removed from this specification.	

3 The various formats for archive time stamps specified in the different versions of ETSI TS 101 733 may illustrate this point.

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change (by the organisation)	RESOLUTION on each comment submitted
				NOT SUITABLE to support the nesting of archive-time-stamps in a way which would allow to preserve the evidence of the signature under consideration (i.e. by covering certificates and revocation information of previous archive time stamps for example). In particular it seems that certificates and revocation information of previous archive time stamps can NOT be protected by new archive time stamps (without introducing nasty distinction of cases). Please note, that archive validation data which does not allow to preserve the evidence of the archived data over long periods of time **CAN NOT** be tolerated to be referenced in an implementing act of the eIDAS regulation as this would simply seem to be **NEGLIGENT**.		
A-22	5.6		General	There are already different formats for archive time stamps which are **standardized and used in practice**. An effective solution for long term archiving of electronic signatures should be	Completely revise or drop section 5.6. The revised section 5.6 needs to explain how the different versions of legacy archive time stamps defined in previous CAdES versions can (and	Rejected. See details below the table.

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change (by the organisation)	RESOLUTION on each comment submitted
				able to **incorporate existing formats** and contribute to the harmonization of data structures. The archive validation data structures presented in section 5.6 however are not even capable to incorporate the data structures in the previous version v2.2.1 of ETSI TS 101 733 not to talk about relevant data formats standardized elsewhere. The "solution strategy" specified in section 5.6 and 6, i.e. that an existing long-term-validation attribute is to be maintained as such and that an archive-time-stamp-v3 attribute (including ats-hash-index-v2 attribute) is created otherwise does NOT seem to be a mature solution. This general impression seems to be backed up by the different specific observations mentioned below.	should) be integrated and preserved in a unifying manner. In order to achieve this it may be advisable to define a new archive-time-stamp-v4, which is powerful enough to cover all previous versions and which may be used within an evidence record according to RFC 4998.	
A-23	5.6.1		Editorial	The relation between the `ats-hash-index-v2` attribute and the `archive-time-stamp-v3` attribute should already be clarified in the introduction. Furthermore the archive-time-	At least revise the first sentence.	Accepted.

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change (by the organisation)	RESOLUTION on each comment submitted
				stamp-v3 attribute is not *new* (as it already appeared in ETSI TS 101 7333 v2.2.1).		
A-24	5.6.1		Technical	The archive time stamp attribute defined in the present document should be a generalization of the existing archive time stamp formats in order to support the incorporation of already existing formats. That the defined archive time stamp (`archive-time-stamp-v3`) cannot be used together with other archive validation data (e.g. archive time stamps from previous CAdES-specifications, the long-term-validation attribute or archive time stamps within evidence records) is not optimal and probably not even tolerable if one aims at an effective and broadly acceptable solution.	Create an archive time stamp format, which is a harmonized superset of existing archive time stamp formats. This topic should be subject of a more detailed technical discussion in order to come up with a sound solution for this problem.	Rejected. See details below the table.
A-25	5.6.1		Editorial	The reference to annex A.2.5 does not seem to be appropriate as this annex does not really provide details.	Drop the reference to annex A.2.5 or extend the explanation of details there.	**Rejected**. Keep the reference. A.2.5 gives details about the case where a long-term-validation attribute is already used.
A-26	5.6.2		Editorial	As the `archive-time-stamp-v3` attribute is the leading data structure it should	Switch order of sub-sections in order to explain `archive-time-stamp-v3` attribute	Rejected. The current order seems consistent.

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change (by the organisation)	RESOLUTION on each comment submitted
				be explained first.	first.	
A-27	5.6.2		Editorial	That the `ats-hash-index-v2` attribute provides an unambiguous imprint of the essential components of a CAdES-signature is somewhat misleading as it only specifies the additional data besides the `SignerInfo`-structure (which seems to be "the essential component" of the CAdES-signature).	It should be mentioned that the `archive-time-stamp-v3` also covers the signature itself.	**Rejected**. The details of the "objects" covered by the archive-time-stamp are in clause 5.6.3.
A-28	5.6.2	Semantics, 3rd paragraph (before bullets)	Technical	It is not clear why the `ats-hash-index-v2` attribute needs to be invalid if it points to something which is not existing.	Provide clarification why this requirement is necessary.	Added a sentence "the validation of the archive-time-stamp-v3 requires to have all the original values referenced in the `ats-hash-index-v2` attribute" just before the sentence "The `ats-hash-index-v2` is invalid if it contains a reference for which the original value is not found"
A-29	5.6.2	ASN.1 structure in combination with sentence before NOTE 2.	Technical	If the algorithm specified in the ATSHashIndexV2 structure is the same as in the archive time stamps message imprint the `hashIndAlgorithm` element is redundant.	Remove `hashInAlgorithm` element from the `ATSHashIndexV2` structure or explain why the redundancy is necessary.	The rational for this duplication is to have "standalone" attribute. No strong opinion. Would like to hear others' opinions.
A-30	5.6.3	`ArchiveTimeStampToken`	Technical	`ArchiveTimeStampToken` is simply defined as `TimeStampToken`. In order to allow that more efficient archive time stamp	Replace "`TimeStampToken`" by "`ArchiveTimeStamp -- according to RFC 4998`"	**`Rejected`**. `archive-time-stamp-v3` is not intended to hold ERS. See the accompanying document.

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change (by the organisation)	RESOLUTION on each comment submitted
				constructions based on Merkle's hash trees can be used the definition of `ArchiveTimeStampToken` should be based on the `ArchiveTimeStamp` structure defined in section 4.1 of RFC 4998.		
A-31	5.6.3	2nd line of comment in Figure 1	Editorial	The meaning of the text "as are in binary encoded from (without modification)" is not clear.	Check and correct the text.	Accepted. Will use the same text as in 5.6.3: "in their binary encoded form without any modification and including the tag, length and value octets"
A-32	5.6.3	Sentence before NOTE 4.	Editorial	"…then the whole **the** set of CRLs"	Remove superfluous "the".	Accepted.
A-33	6.1	NOTE 3	Editorial	TS 101 533-1 is not among the references in section 2.	Add reference.	Accepted.
A-34	6.1	NOTE 3	Technical	RFC 4998 and the forthcoming EN 319 533 should be mentioned in NOTE 3 as well.	Add references in NOTE 3 and in section 2.	The list here is not intended to be exhaustive. Would like to hear others' opinions.
B	6.2.2 6.3	Table2	Technical	"*": means … should not be incorporated We interpret "should not" as "not recommended" but there may exist valid reasons in particular circumstances when the elements need to be used. For example when using CAdES-B-B there may be the need to provide revocation information for an offline	"*": 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.	The definition of "should not" already "allow" using the service qualified with "should not". No change needed

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change (by the organisation)	RESOLUTION on each comment submitted
				scenario. It should be stated clearly that such an extension is allowed.		
C 01	all		ed	Use reference to Regulation consistent with other deliverables	Replace “EU Regulation Nº 910/2014” with “Regulation (EU) No 910/2014”	Accepted.
C 02	foreword		ed	Extra s at specification	The present document partly contains an evolved specifications	Accepted.
C 03	scope		ed		The present document specifies CAdES digital signatures. CAdES signatures are built on CMS signatures ~~as specified in~~ [Error: Reference source not found], by incorporation of signed and unsigned attributes, which fulfil certain common requirements (such as the long term validity of digital signatures, for instance) in a number of use cases. … ~~CAdES digital signatures specified in the two parts of ETSI EN 319 122 aim at supporting electronic signatures in different regulatory frameworks.~~	Accepted

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change (by the organisation)	RESOLUTION on each comment submitted
					~~NOTE 1: Specifically, but not exclusively, CAdES digital signatures specified in the present document aim at supporting electronic signatures, advanced electronic signatures, qualified electronic signatures, electronic seals, advanced electronic seals, and qualified electronic seals as per EU Regulation Nº 910/2014 [~~Error: Reference source not found~~].~~ Procedures for creation and validation of CAdES digital signatures are out of scope and specified in EN 319 102 [i.6]. The present document aims at supporting ~~electronic~~ **digital**	

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change (by the organisation)	RESOLUTION on each comment submitted
					signatures in different regulatory frameworks. NOTE ~~2~~1: Specifically but not exclusively, CAdES digital signatures specified in the present document aim at supporting electronic signatures, advanced electronic signatures, qualified electronic signatures, electronic seals, advanced electronic seals, and qualified electronic seals as per Regulation (EU) No 910/2014 [i.13].	
C 04	3.1		ed	Definition of digital signature is missing	Add definition of digital signature (from 119 172-1) data associated to, including a cryptographic transformation of, a data unit that:	Accepted.

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change (by the organisation)	RESOLUTION on each comment submitted
					a) allows to prove the source and integrity of the data unit, b) allows to protect the data unit against forgery and c) allows to support signer non-repudiation of signing the data unit.	
C 05	4.1		ed		CAdES signatures shall build on Cryptographic Message Syntax (CMS), as defined in RFC 5652 [Error: Reference source not found], by incorporation of signed and unsigned attributes as ~~described~~ **defined** in clause Error: Reference source not found.	Accepted.
C 06	4.1		tec	Scope states that "Procedures for creation and validation of CAdES digital signatures are out of scope" while clause 4.1 partly addresses it	Delete 3rd paragraph: The processes for the signature generation shall be as defined in RFC 5652 [Error: Reference source not found] clause 5.5. The process of the signature verification shall be as defined in RFC 5652 [Error: Reference source not found] clause 5.6. In addition, for the validation, the algorithm described in	Accepted.

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change (by the organisation)	RESOLUTION on each comment submitted
					EN 319 102 [Error: Reference source not found] should be taken into account.	
C 07	5.2		ed	No hanging paragraph + info is already included in the sub-clauses	Delete sentence below 5.2 title: The attributes in this clause are signed attributes as defined in CMS (RFC 5652 [7]).	Accepted.
C 08	5.3.2.2 & 5.3.2.3		ed	typo	If the `issuerAndSerialNumber` field in `SignerIdentifier` field of the `SignerInfo` and the `issuerSerial` ~~filed~~ **field** in `ESSCertID` are present, they shall match. Same in 5.3.2.3	Accepted.
C 09	5.3.3		ed		NOTE 1: The commitment type can be: - defined as part of the signature policy, in which case, the commitment type has precise semantics that are defined as part of the signature policy; or be a registered type, in which case, the commitment type has precise semantics defined by registration, under the rules of the registration authority. Such a registration authority ~~may~~ **can** be a trading association or a legislative authority.	Accepted.

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change (by the organisation)	RESOLUTION on each comment submitted
C 10	5.3.4.1		ed		• the `contentDescription` shall be used to indicate the encoding and the intended presentation application of the data, in accordance with the rules defined **in** RFC 2045 [Error: Reference source not found]; see annex Error: Reference source not found for an example of structured contents and MIME.	Accepted.
C 11	5.3.6.1		ed		NOTE 2: Clause 5.3.6.2 defines a new attribute that ~~may~~ **can** be used to describe a claimed role by encapsulating a SAML token.	Accepted.
C 12	5.3.9		ed	No hanging paragraph	Rename 5.3.9 title to "The signature-policy-identifier attribute and SigPolicyQualifierInfo type" Create sub-heading 5.3.9.1 The signature-policy-identifier attribute Increase heading number for	Accepted.

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change (by the organisation)	RESOLUTION on each comment submitted
					ex-5.3.9.1	
C 13	5.3.9.1		ed		NOTE: This qualifier allows identifying whether the signature policy document is human readable, XML encoded, or ASN.1 encoded, by identifying the specific ~~Technical Specifications~~ **technical specifications** where these formats will be defined.	Accepted.
C 14	5.4		ed		• NOTE: In the case of multiple signatures, it is possible to have a: • - signature-time-stamp computed for each and all signers; or - signature-time-stamp on some signers' signatures ~~an~~ **and** none on other signers' signatures.	Accepted.
C 15	6.1		ed		NOTE 3: Conformance to B-LT level, when combined with appropriate additional preservation techniques tackling the long term availability and integrity of the validation material is sufficient to allow validation of the signature long time after its generation. The assessment of the effectiveness of	Accepted.

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change (by the organisation)	RESOLUTION on each comment submitted
					preservation techniques for signed data other than implementing the B-LTA level are out of the scope of the present document. The reader is advised to consider legal instruments in force and/or other standards (for example TS 101 533 1) that ~~may~~ **can** indicate other preservation techniques.	
C 16	6.2.2		ed		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** ~~shall~~ contain**s** either the number of the clause specifying the attribute in the present document, or a reference to the document and clause that specifies the signature field.	Accepted.
C 17	6.3		ed	Add a dash between BB, BT and LT	Table 2 shows the presence and cardinality requirements on the attributes, signature fields, and services indicated in the first column for the four CAdES baseline signature levels, namely: CAdES-B-B, CAdES-	Accepted.

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change (by the organisation)	RESOLUTION on each comment submitted
					B-T, CAdES-L-T, and CAdES-B-LTA). Additional requirements are detailed below the table suitably labelled with the letter indicated in the last column.	
C 18	6.3		ed	Items k and l are duplicates	Delete one	Accepted.
C 19	6.3		ed	Item y refers to wrong clause 6.5	Update clause reference	Accepted.
C 20	A.1.2.1		ed		NOTE 2: The absence of the ocspRefHash field makes OCSP responses substitutions attacks possible, if for instance OCSP responder keys are compromised. In this case, out-of-band mechanisms ~~might~~ **can** be used to ensure that none of the OCSP responder keys have been compromised at the time of validation.	Accepted.
C 21	A.1.2.2		ed		The revocation-values attribute should be used in preference to the OtherRevocationInfoFormat specified in RFC 5652 [7] to maintain backwards compatibility with the earlier version of TS ~~103 733~~**101 733**.	Accepted.
C 22	A.1.5.2		ed	Delete extra s in encapsulate	The `CAdES-C-time-stamp` attribute shall encapsulate~~s~~ one time-stamp token	Accepted.

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change (by the organisation)	RESOLUTION on each comment submitted
					… NOTE: This time-stamp covers the CAdES-E-C level signature as defined in **EN 319 122-2** ~~part 2~~ [Error: Reference source not found] ~~of the present document~~.	
C 23	B		tec	Is it really needed to keep X.208 declaration? Can't the document impose using the latest ASN.1 X.680? Between the 2 ASN.1 declarations, isn't there one which takes precedence?		X.680 ASN.1 Syntax made normative and X.208 ASN.1 Syntax made informative
C 24	B		ed	Cannot have hanging paragraph just before B.1	Either created new sub-heading B.1 or more the text to B.1 and B.2	Accepted. Duplicated the text in B.1 and B.2
C 25	B.2		ed	Something missing after `FROM CryptographicMessageSyntax 2004 { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9)`		Accepted.

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change (by the organisation)	RESOLUTION on each comment submitted
C 26	C		ed	No hanging paragraphs	Insert sub-headings	Accepted.
C 27	C.1.1		ed	Use bullet list to make sense of the clause		Accepted.
C 28	C.2.1		ed		The data to be signed ~~may~~ **can** be included in the `SignedData` within CAdES, which itself ~~may~~ **can** be included in a single S/MIME object.	Accepted.
C 29	C.2.2		ed	First paragraph needs to be in "normal" style		Accepted.
C 30	C.3		ed		Thus these attributes allow ~~allows~~ to give the application useful information. … ~~We will give~~ two examples **follow.** … 2) In the case that the driving application is interested in all the details of the MIME header, it ~~might~~ **can** put the whole header as MIME-type into the signature, like for example:	Accepted.

Archive time-stamp:

There were several comments on clause 5.6 Archive validation data from A. This text addresses them in detail.
The ATSv3 was developed to have a similar functionality than the previous archive time stamp, with the main advantage that it is possible to add unsigned attributes, certificates and validation data to the main signature after the first archive time-stamp was created and that there is no problem of the order of the unsigned attributes if they are not DER encoded.
Each creation of the ATSv3 will cover:

- The signed document
- The whole information of the signerInfo at the moment of the creation of the ATSv3
- The SignedData.certificates at the moment of the creation of the ATSv3
- The SignedData.crls at the moment of the creation of the ATSv3

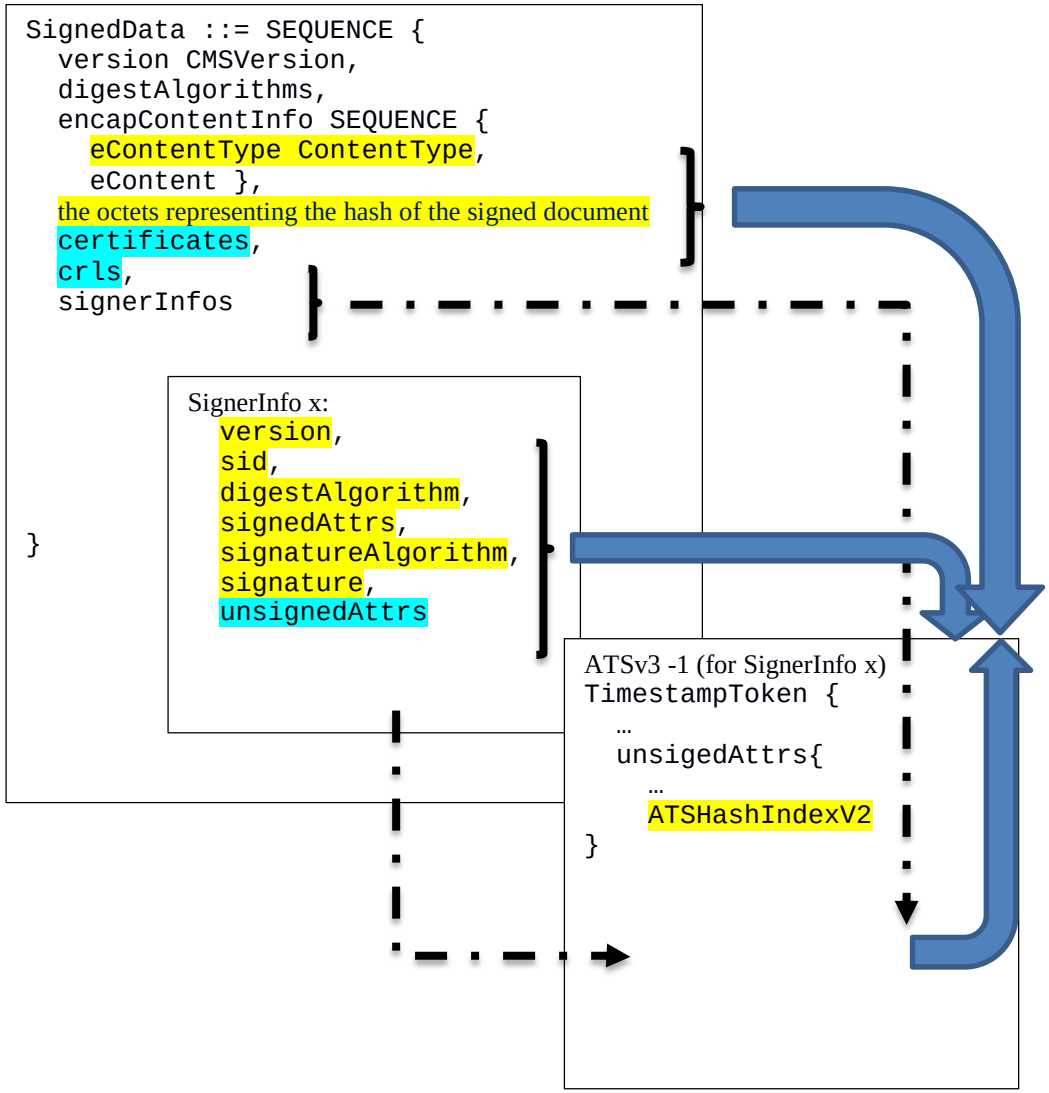
The information of SignedData.certificates, SignedData.crls and SignerInfo.unsignedAttributes is covered indirectly. The hash of each element in these sequences is included in a new hash-index-v2 element and this new element is then covered by the time-stamp of the ATSv3. The hash-index-v2 is included in the ATSv3 attribute as unsigned attribute.
The hash-index-v2 allows to know exactly which elements were contained in the signature at the moment of the creation of a specific ATSv3
Each time a new ATSv3 element is created, first all missing validation data shall be included into the signature, and will then be covered by the new ATSv3.
The new ATSv3 will cover previous unsignedAttributes including any previous ATSv3. In particular, the hash-index-v2 included in the previous ATSv3 is protected by the new ATSv3.
When a cryptographic algorithm is threatened to be compromised, it is sufficient to create a new ATSv3 with a new hash algorithm. This new, stronger hash algorithm will be used to compute again the hash of the signed document, the signature, the certificates, the validation data, the previous ATSv3, etc.
More formally, say we add a first ATSv3 at t1 using the hash algorithm H1, and a second ATSv3 at t2 using the hash algorithm H2. If the renewal is to prevent close compromise of H1, H2 must be a stronger algorithm. Otherwise, H2 may be equal to H1. The renewal mechanism must allow proving (at any date after t2 and provided the last ATSv3 can be validated at this date) that any validation data protected by the old ATSv3 exists at t1. For example, for a certificate C in the signature, we have the following situation when validating the last ATSv3:

- The last ATSv3 gives a POE for the data H2(C) at t2. Using the indirect hash proof of existence (assuming that we have C now and that H2 is secure now), this gives a POE of C at t2.
- The previous ATSv3 will give a POE for the data H1(C) at t1. Using the indirect hash proof of existence (assuming that C exists at t2 > t1 and that H1 is ok at t2), this gives a POE of C at t1.

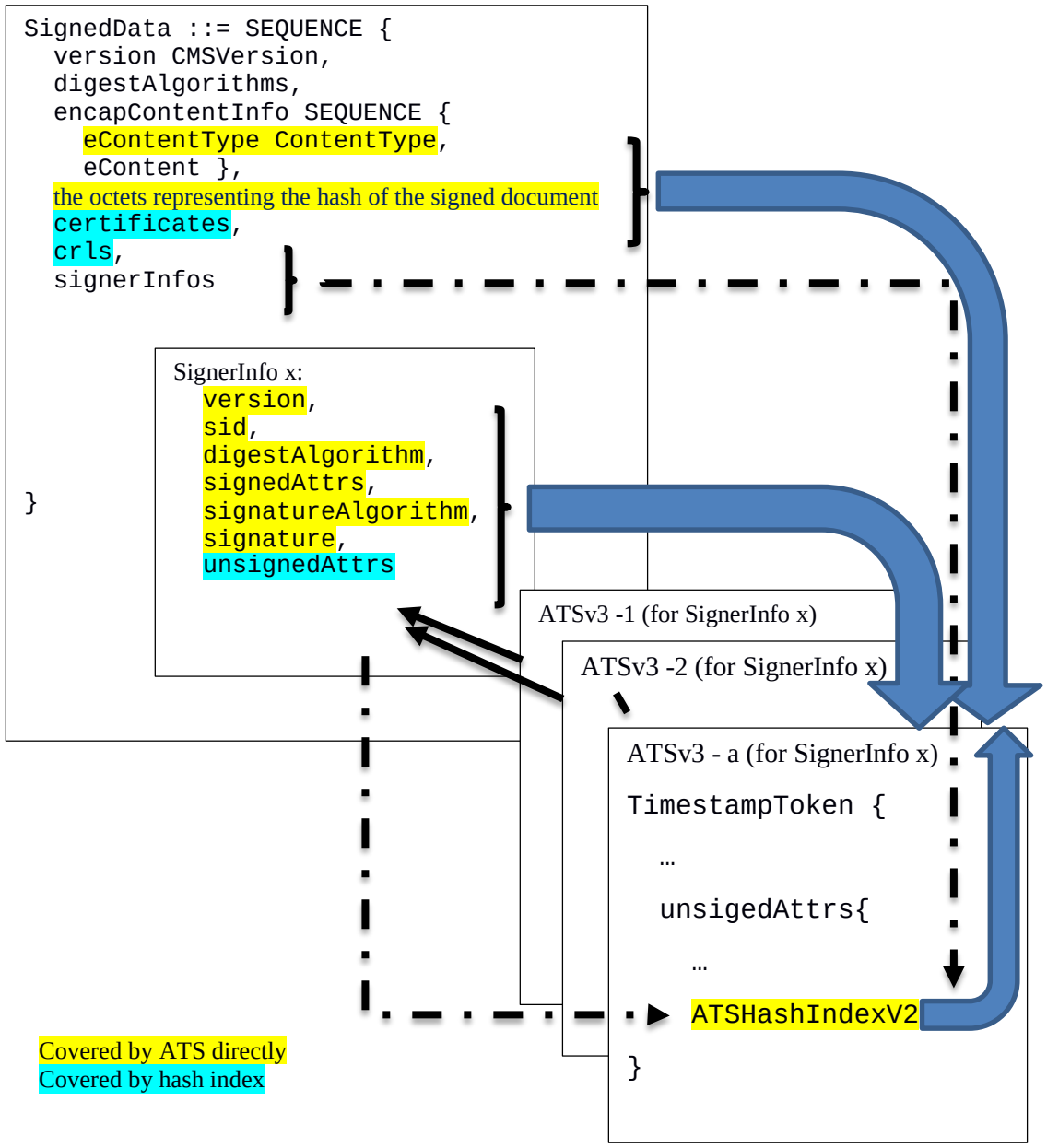
Concerning previous versions of archival: It is true that it is not possible to combine the ATSv3 with the long-term-validation attribute, since once the long-term-validation attribute is created, no other unsigned attributes are allowed to be added. Thus the new standard states that once such an attributed is contained in the signature, the archival should be continued using this attributes.
In the case where an old archival time-stamp (ATSv2 or older) is contained in the signature, the signature shall be extended using the new ATSv3. However in this case, the certificates and validation data shall not be added to SignedData.certificates and SignedData.crls of the main signature, but added within the time-stamp token of the previous archive-time-stamp. This point is probably not well described.
The hash-index-v2 was developed such that it might be used also in other situations (which is not the case for the moment), thus the hash algorithm was added, even if it will be the same as used in the time-stamp.

It was decided that for the moment in CAdES (XAdES and PAdES) we only use time-stamps and no ERS.
In the following some graphs explaining a bit more the usage of the ATSv3:

Single ATSv3:



Covered by ATS directly
Covered by hash index



More than one ATSv3