Resolution of public comments on Draft ETSI <*EN*> <*319 102-1*> V<0.12.0>

Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation

A

Organization name	**Clause/ Subclause**	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change**	**RESOLUTION** on each comment submitted
A	General suggestion		Technical		Standard should contain also information which validation status all in all should be provided in case of two signatures in the container (for example ASiC container), from which one is valid and another invalid.	102 is not concerned with containers and how to behave if you have such a case is implementation dependent. In the case mentioned there should be two signature validations done and what the overall result is will be policy dependent
A	4.1		Editorial	Same picture is presented twice.		Fixed
A	4.2.11 and 5.6.2.1.1 (a)		Technical		Our suggestion would be that in validation process is mandatory to use in first order those validation data, which are included already in the signature (for example time-stamp value, OSCP value). If SVA does not use validation data included initially in the signature, but new validation data (new time-stamp or OSCP obtained during validation process), it should be also reflected in validation report. User should know that result of validation does not respond to the data included initially into signature, but are provided as result of new validation process. Also it should be indicated, which additional data are used in	Rejected. This is too implementation dependent. It has been tried to make it clearer however

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted
					validation process.	
A	5.1.3		Editorial		Instead of phrase „the date and time for which the validation status was determined“ could be defined notion, which could be used in current standard and in the validation report. Our suggestion is to use "validated signing time". It is distinguishable from the similar notion "claimed signing time".	Rejected. The term "validated signing time" would be misleading since we cannot identify the exact signing time at all.
A	5.2.5 (a)		Editorial	Notions "validation time" and "validation date" are confused.		Accepted and fixed.
A	5.2.5 (c)		Technical	Using NextUpdate value Revocation freshness checking is problematic. For example in the case of real-time OSCP responders that leave empty the NextUpdate value which is indicating that newer revocation information is available all the time (see RFC 6960, 4.2.2.1). When we initiate revocation freshness checker with such OSCP response, then the result will be FAILED.		We use NextUpdate only, if there is no value set for freshness in the constraints. And we are only talking on the default behavior when the constraints do not direct us properly – we need to define an algorithm that always produces correct results. If we have no constraints set, "failing" is certainly a better default behavior since it will trigger getting fresh revocation information.
A	5.6.2.2.4 (2b)		Technical	What can be considered POE of certificate and revocation status information in case of XAdES-B-LT level signature? Is the SignatureTimeStamp value considered as sufficient for the POE?		A POE proves all that is covered by the proof. A SignatureTimeStamp, only covers the signature value and not the certificate or revocation status, it cannot be a POE for that.
A	5.6.2.2.4	Paragraph	Editorial	Something is wrong with		OK

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted
		2.c		wording "The update the value of control-time is as follows:".		
A	5.6.2.2.4	Paragraph 2.c	Technical		The revocation freshness check process should be not mandatory; its usage depends on the validation policy rules.	Rejected. The policy has the last word for all of these checks. This has been made clearer in the text now using this as an example.
A	5.6.2.2.4	Paragraph 2.c	Technical		We suggest to use as control-time value the revocation data issuance date, not "current time" value.	Unclear since this does not reflect the text in 2c

B

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted
B	5.1.4 5.2.6.4	Last one before example Step 1 Step 3a	Technical	A DA should not only be possible to force the SVA to omit checks on some constraints so that it results in TOTAL-PASSED instead of INDETERMINATE. When allowing omitting checks consequentially, the DA should also be able to control the time used for verification of the signing certificate. The DA should be able to set that time as assumed signing time or the DA should control the SVA to use claimed signing time.	Add a paragraph to sub-clause 5.1.4 that is not only possible to skip checks but also to modify input parameters to those checks in additional constraints with an example of defining certificate validation as input to X.509 certificate validation building block. Modify step 1 and 3a in sub-clause 5.2.6.4 of X.5009 certificate validation building block to take X.509 Validation constraints on time to be used in that check into	There are things that are policy based, like which things should be checked, and there is the logic of validation, which always starts at current time. There is no value in setting assumed signing times for the algorithm since it does not use such values directly. To achieve said behaviour, current time would need to be changed.

Organization name	**Clause/ Subclause**	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change**	**RESOLUTION** on each comment submitted
					account or use time as input given by DA.	
B	5.2.4.3	Table 10	Editorial	Sub-Indication “SIGNATURE_POLICY_NOT_AVAILABLE” is missing in Table 6 Validation Report Structure	Add this sub-indication to Table 6 with appropriate description its semantics.	OK
B	5.2.4.4.	Paragraph before last one	General	“Otherwise, the building block shall return …” What is meant with “Otherwise”, other than what? Is it related to the paragraph before: “If the signature is implied …”	Please describe explicitly what shall be returned by the building block in case it does not return PASSED.	Otherwise removed. Was a “left over”
B	5.2.1	Figure 11	Editorial	Figure is missing FAILED indication for Format Checker building block. As per 5.2.2.3 this building block just outputs FAILED or PASSED and never INDETERMINATE.	Please adapt figure 11 accordingly.	It is correct, that the building block outputs FAILED, the overall result however is INDETERMINATE. Agreed this may be confusing. Changed the figure to represent that
B	5.2.1	Figure 11	Editorial	The name of building block “Identification of Signers Certificate” should be “Identification of the signing certificate” as per 5.2.3	Please correct the name of the building block in figure 11 accordingly.	OK
B	5.2.1	Figure 11	Editorial	Revocation Freshness Checker basic building block is missing in figure 11.	Please add this building block to figure 11 as part of X.509 Certificate Validation.	OK
B	5.2.3.4	Step 3	Technical	“… if they do not match, an additional warning shall be returned with the output.” What kind of warning is meant here? Does it result in INDTERMINATE indication or is it still PASSED in this case?	This situation should result in INDETERMINATE indication.	Rejected. This behaviour has been agreed on in ESI for legacy reasons.
B	4.3.1	Figure 3	Editorial	What is the meaning of the different line types of the rectangles? Do dashed lines mean that	Please check the correct meaning	Dashed lines indeed indicate that the element is optional. It

Organization name	**Clause/ Subclause**	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change**	**RESOLUTION** on each comment submitted
	4.3.2.3	Figure 6		this component is optional? If so, a Signer's Document is optional in a signature as well. Or, should Signer's Document rather be replaced by DTBSR? In this case it wouldn't be optional.	of the rectangle Signer's document.	also should indicate what contributes to the signature calculation, and the signer's document certainly does. These figures are on purpose kept simple.
B	4.2.8	First sentence	Editorial	"The data hashing component (DHC) …" This component is named DTBS preparation function in figure 2.	Please rephrase this sentence using the correct function name.	OK
B	4.2.7	General	Technical	Is DTBS Formatter responsible to execute transformations on the document, like canonicalization/normalization or XSL transformation before signing?	Please add those normalizations at least as a note in order to make it clear to the reader of the document when to do it.	OK
B	4.2.5.3	Last paragraph	Technical	When adding a digest to that attribute it is necessary to add the algorithm to calculate that digest as well.	Please add the algorithm to that attribute like done in 4.2.5.2.	OK
B	4.2.1	Figure 2	Technical	Validation data as described in 4.2.11 are missing in this figure.	Please add validation data as input to SDOC	OK
B	4.2.1	Figure 2	Technical	Input to DTBS Composer could alternatively be SDR instead of SD.	Please add SDR as alternative input to DTBS composer in figure 2.	OK
B	4.3.2.3	Bullet points	Technical	The description of the content of SDO does not fit to what is described in 4.2.10. It should contain DTBSR instead of DTBS and signature value.	Please align those chapters.	OK
B	4.3.2.4	General	Technical	4.3.2.4.1 describes that existing signatures on or attached to the document shall be validated. But DA has no control over the handling of those signatures in signature creation process, i.e. if those signatures will be taken into account during signature creation or not. There seems to	Please add such control to the signature creation process.	In 4.3.2.4.1 the DA is the actor that allows the signer to select the document and can do the handling of the validation. Counter/Parallel signatures can

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted
				be a need to have control over creation of either counter signatures or parallel signatures.		be handled by the DA by constructing an appropriate SD. Adding this would make the text more complex than necessary.
B	5.2.6.4	Step 3	Technical	"Two validity models may be supported." These validity models are different in the sense that using the first one a signature validation might result INDETERMINATE indication while using the latter one result in PASSED indication. This should not be implementation dependent. This should at least be controllable by DA what kind of validity model to be used in the context of the signature validation.	Please add additional input parameter or X.509 validation constraint to give the control over validity model to the DA rather than to the implementer.	This is implicitly part of the X509 validation constraints. Made explicit.
B	5.5.4	Note 2, 3, 4, 6	Editorial	References to step 5a/5b/5c seem to be wrong. It looks like the references should point to step 4a/4b/4c instead.	Please change references accordingly.	Yes
B	5.5.4	Step 4a	Editorial	Reference to step 5d is invalid, it should be 4d.	Please change the reference accordingly.	Yes
B	5.6.3.4	Step 3 2nd bullet point	Editorial	"Otherwise, the SVA shall got to step 3" It looks like it should be step 4 instead.	Please change the reference accordingly.	Yes
B	5.2.1	Figure 11	Technical	The result of the signature validation process must not depend on the proposed order of independent validation steps. E.g. following the processing flow given in Figure 11 a signature, that is cryptographically not valid and lacks some information for X.509 Certificate Validation ends with state INDETERMINATE – but should be TOTAL-FAILED.	In the case of insufficient information to ascertain a validation check to PASS the processing shall not stop. In cases where the processing of the validation must be stopped it shall always be a TOTAL-	Accepted. Changed the order such that crypto validation is done first and the algorithm will stop before any checks that lead to INDETERMINATA are done

Organization name	**Clause/ Subclause**	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change**	**RESOLUTION** on each comment submitted
				Note: This issue is not solved by "5.3.4 Note1" as the result depends on the order.	FAILED. Following this logic e. g. a wrong format shall be a TOTAL-FAILED, too.	
B	5.2.1	Figure 11	Technical	Early stopping of validation in case of the first INDETERMINATE could be an option but it should not be the default and the DA should decide.	The SVP could offer the option to stop the processing when finding the first INDETERMINATE status on a building block validation. The default should be not to stop processing on INDETERMINATE. The DA should be the one to decide to pull that option.	Same as above
B	5.1.1 + 5.1.3	Definition of main status	Technical	The definition of the status of a validation is lacking - precision on distinguishing between TOTAL_FAILED and INDETERMINATE - aggregation logic of the status from single validation building blocks	The status on a single validation building block shall be PASSED: When all checks that the signature validation policy prescribed have been passed for the particular validation building block. INDETERMINATE: When the available information is insufficient to full process all checks that the signature validation policy prescribed have been passed for the particular validation building block. FAILED: If not PASSED or INDETERMINATE. The status on the full validation in the context of a particular signature	Accepted with modifications. The overall status may be indeterminate if one of the building blocks has failed. TOTAL_FAILED is restricted to the cases listed.

Organization name	**Clause/ Subclause**	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change**	**RESOLUTION** on each comment submitted
					validation policy: TOTAL_PASSED: If all validation building blocks are PASSED. TOTAL_FAILED: If at least one of the building blocks has status FAILED. INDETERMINATE: If not TOTAL_PASSED and not TOTAL_FAILED.	
B	5.1.2		Technical	“SVA shall select the process best suited for that signature”	Define what “best suited” means.	Ok
B	5.1.4		General	“Such overruling by the policy is in theory possible for all decisions made by the present document and cannot be mentioned in all places they can appear” describes the general possibility to overrule any decision in this specification by a particular policy.	Place this overruling statement at a prominent position. Leave out the words “in theory” in favour for stating the not allowed overrulings, like “TOTAL-FAILED shall not be overruled”.	Added a rule according to this. Discuss where the more prominent place could be
B	1	The following aspects are considered to be out of scope: […] • The legal interpretation of any	general	The legal interpretation on signatures should not be completely out of scope. Because the present document produced for M/460 standardisation mandate should be fully compatible with the legal view of the Regulation (EU) No. 910/2014.		Rejected. Being compatible with a regulation does not mean we deal with legal interpretations of signatures.

Organization name	**Clause/ Subclause**	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change**	**RESOLUTION** on each comment submitted
		signature, especially the legal validity of a signature.				
B	5.1.3	"validation process. Table 2 lists the possible values of the main status indication"	editorial	It seems to be a broken table reference.		fixed
B	5.1.3	"validating T, LT and LTV-level signatures"	editorial	T and LT are not defined as abbreviations		fixed
B	5.1.3	"in Table 6 by listing the main sub codes"	editorial	It seems to be a missing word.	"the main and sub codes"	Ok
B	5.2.6.4	3. "The validation shall be following the PKIX Certification Path Validation [5], clause 6.1 with the exception of	technical	If a CA certificate in the path of the signing certificate has been revoked before the signing time, the signature is considered to be invalid in the PKIX validation model (all certificates must be valid at current time). This also means that the latest time a user can provide a valid signature is the revocation time of the CA certificate in the path. After this time the user cannot generate valid signatures with its private key in conjunction with this user certificate, even if the certificate was not explicitly revoked. This behaviour of the validation algorithm is	"Two validity models shall be supported selectable by Chain Constraints: • All certificates must be valid at current time; and • All certificates must be valid at the time they were used for issuing a certificate."	The Chain model had already been integrated

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted
		the validity model. Two validity models may be supported: • All certificates must be valid at current time; or • All certificates must be valid at the time they were used for issuing a certificate."		acceptable for nonqualified signatures but noncompliant for qualified signatures according to the Regulation (EU) No. 910/2014 Article 32 (Requirements for the validation of qualified electronic signatures). Compared with the formulation of Article 32 in conjunction with Article 24 paragraph 4, 2h and 2i, the PKIX model is too restrictive: in case of cessation of a CA service it delivers a negative technical judgement for a signature that is valid in the legal sense. Trust service providers (issuing qualified certificates) wanting to provide technical products that exactly fulfil the validity requirements of the Regulation (EU) No. 910/2014 implement a slightly different variant of the PKIX model, called the chain model (all certificates must be valid at the time they were used for issuing a certificate). Additional information about this validation model can be found in Common PKI specification, Part 9, www.common-pki.org. This means, the X.509 certificate validation building block should require mandatory supporting both validity models, PKIX (shell) and chain. This should be selectable by validation constraints.		
B	5.4.4	1. "Token signature validation: the building block shall perform the validation process for	technical	Chapter 4.3.5.1 describes the target of archival time stamps: "Before algorithms, keys, and other cryptographic data used at the time a signature was built become weak and the cryptographic functions become vulnerable, or the certificates supporting previous time-stamp tokens expire or are revoked, the signed data, the signature as well as any additional	**The core architecture of the validation algorithms in the present EN draft do not seem suitable for EU qualified electronic signatures and should fundamentally revised to be compliant to the legal view of Regulation (EU) No. 910/2014.**	Rejected. There are other ways to avoid disasters than making the chain model default.

Organization name	**Clause/ Subclause**	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change**	**RESOLUTION** on each comment submitted
		Basic Signatures as per clause 5.3 with the time-stamp token.”		information should be protected by applying time-stamp tokens. Such additional time-stamp tokens are called archive validation data. The time-stamping process should be repeated in time before the protection provided by a previous time-stamp token becomes weak and should make use of stronger algorithms or longer key lengths than have been used in the original signatures or time-stamp tokens.” With the Basic Signature Validation building block and the PKIX validation model (all certificates must be valid at current time), this target is not achieved. Because, at the time one of the certificates in the chain of the time-stamp signature is revoked, instantly all signatures protected by this TSA lose their validity. Since such TSA revocation nobody can foresee, the user (or the archival system) cannot know when to apply a new time-stamp, preventing this disaster situation.	**We recommend, using the Common PKI specification, www.common-pki.org, as a basis to achieve this.**	
B	5.5.4	NOTE 3 “(step 5-b)”	editorial	It seems to be a broken reference.		fixed
B	5.5.4	NOTE 4 “(step 5-c)”	editorial	It seems to be a broken reference.		Fixed
B	5.5.4	4. a) “perform step 5d”	editorial	It seems to be a broken reference.		fixed
B	5.5.4	6. “or time-mark”	technical	Time-marks are not defined under 3.1 because they should not be used in the normative building blocks.		Leftover extracted
B	5.5.4	NOTE 6	editorial	It seems to be a broken reference.		fixed

Organization name	**Clause/ Subclause**	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change**	**RESOLUTION** on each comment submitted
		"(step 5-a)"				
B	5.6.2.1.1	"(see clause 5.2.4)" "processing in 5.2.4)"	editorial	It seems to be broken references.		fixed
B	5.6.2.1.4	2. "The building block shall run the Certification Path Validation [5], clause 6.1, with the following inputs"	technical	If a CA certificate in the path of the signing certificate has been revoked before the signing time, the signature is considered to be invalid in the PKIX validation model (all certificates must be valid at current time). This also means that the latest time a user can provide a valid signature is the revocation time of the CA certificate in the path. After this time the user cannot generate valid signatures with its private key in conjunction with this user certificate, even if the certificate was not explicitly revoked. This behaviour of the validation algorithm is acceptable for nonqualified signatures but noncompliant for qualified signatures according to the Regulation (EU) No. 910/2014 Article 32 (Requirements for the validation of qualified electronic signatures). Compared with the current formulation of Article 32 in conjunction with Article 24 paragraph 4, 2h and 2i, the PKIX model is too restrictive: in case of cessation of a CA service it delivers a negative technical judgement for a signature that is valid in the legal sense. Trust service providers (issuing qualified certificates) wanting to provide technical products that exactly fulfil the validity requirements of the Regulation (EU) No. 910/2014 implement a slightly different variant	The validation shall be following the PKIX Certification Path Validation [5], clause 6.1 with the exception of the validity model. Two validity models shall be supported selectable by Chain Constraints: • All certificates must be valid at current time; and • All certificates must be valid at the time they were used for issuing a certificate.	Rejected. The result in all of these cases will be INDETERMINATE and the policy may allow for accepting the signature even if a CA cert is revoked etc. The chain model is supported anyhow.

Organization name	**Clause/ Subclause**	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change**	**RESOLUTION** on each comment submitted
				of the PKIX model, called the chain model (all certificates must be valid at the time they were used for issuing a certificate). Additional information about this validation model can be found in Common PKI specification, Part 9, www.common-pki.org. This means, the X.509 certificate validation building block should require mandatory supporting both validity models, PKIX (shell) and chain. This should be selectable by validation constraints (see also our comment above to 5.2.6.4).		
B	5	5.5 Validation process for Signatures with time and 5.3 Validation process for Basic Signatures	technical	The described validation processes assume that after the validity period of the certificate ended no longer status information is receivable from the CA. In the case of qualified trust services this assumption is wrong, because Regulation (EU) No. 910/2014 Article 24 paragraph 4 requires from CA: “With regard to paragraph 3, qualified trust service providers issuing qualified certificates shall provide to any relying party information on the validity or revocation status of qualified certificates issued by them. This information shall be made available at least on a per certificate basis at any time and beyond the validity period of the certificate in an automated manner that is reliable, free of charge and efficient.” This argumentation is further confirmed by Draft TS 119 172-1 V0.0.9 chapter A.4.2.1 table 2: “(m)2.3. **RevocationInfoOnExpiredCerts**: This constraint mandates the signer's certificate used in validating the signature to be issued by a certification authority that keeps revocation notices for revoked certificates even after they	Please take this into account for the optimization of the validation processes to minimize the cases returning INDETERMINATE.	This is covered already partially.

Organization name	**Clause/ Subclause**	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change**	**RESOLUTION** on each comment submitted
				have expired for a period exceeding a given lower bound.” At least the behaviour should be selectable by constraints.		
B	all	all	**general**	**The described algorithms force the use of time-stamps and completely ignore other sources of the time of signing. This would be acceptable if the Regulation (EU) No. 910/2014 would also mandatory require qualified time-stamps for a qualified signature to be valid.** **But this is not the case, so the core architecture of the validation algorithms in the present EN draft do not seem suitable for EU qualified electronic signatures and should fundamentally revised to be compliant to the legal view of the Regulation (EU) No. 910/2014. Especially Article 32 in conjunction with Article 24 paragraph 4, 2h and 2i are important and must be reflected by technical algorithms for creation and validation of EU qualified electronic signatures. Losing the technically validity of already created signatures, triggered by revocation and expiring of certificates isn´t acceptable from the user point of view, because signatures have the equivalent legal effect of a handwritten signature and so are used also for long term legal transactions.** **Another important aspect is that creation of qualified signatures should also be possible during offline situations where time-stamps are not available.**		Rejected. The signature-with-time-validation indeed focuses on time stamps. Long Term Validation is able to use any kind of proofs of existence, which the time stamp is a specific instance of. A qualified signature can always be made offline since there is no requirement whatsoever for a time stamp to be used.

C

Organization name	**Clause/ Subclause**	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change**	**RESOLUTION** on each comment submitted
C -1	Chap. 2.1	Page 9	Editorial	There are two RFCs concerning "Evidence Record" [15] IETF RFC 4998: "Evidence Record Syntax (ERS)". [16] IETF RFC 4998: Evidence Record Syntax (ERS)	[15] IETF RFC 4998: "Evidence Record Syntax (ERS)". [16] IETF RFC **6283: "Extensible Markup Language** Evidence Record Syntax (**XML**ERS)	**Not relevant since we don't talk about the XML stuff and the references are only to contain things that are referenced**
C -**2**	Chap. 3.1	Page 11	Editorial	Evidence and Evidence Records SHOULD be defined in chap. 3.1	**evidence: Information that may be used to resolve a dispute about various aspects of integrity and authenticity of archived data objects.** **evidence record: collection of evidence compiled for one or more given archived data objects over time [15, 16]**	**OK**
C-3	Chap. 3.1	Page 11	Editorial	Time assertion **SHOULD** be defined in chap. 3.1	**Time assertion: a time-stamp token or an evidence record**	**Accepted**
C-4	Chap. 4.2.11	Page 20	Editorial	"time-stamp assertion" SHOULD be replaced by "time assertion"	4.2.11 Validation data Some classes of AdES signatures incorporate additional data needed for validation. This additional data is called validation data, is the result of a signature augmentation process and shall include: • Public Key Certificates (PKCs) and Attributes Certificates (ACs); • revocation status information for each PKC and AC (Certificate Revocation Lists (CRLs) or certificate	**Accepted**

Organization name	**Clause/ Subclause**	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change**	**RESOLUTION** on each comment submitted
					status information (OCSP)); and • **time assertion** applied to the signature;..”.	
C-5	Figure 4	Page 21	Editorial	“Add Archive Time Stamp” SHOULD be replaced by “Add Archive Time Assertion”		**Accepted**
C-6	Chap. 4.3.4.1	Page 26	Technical	Here is a **contradiction** between “**Draft EN 319 102 V0.12.0**”: and **“Draft EN 319 122-1V0.0.3”/“Draft EN 319 122-1 V0.0.8”**, page 37 item t) , u): “t) When the full set of revocation data contains CRLs [6], then the CRL values shall be included within **SignedData.crls.crl.”** u) When the full set of revocation data contains OCSP responses [11], then the OCSP response values shall be included within **SignedData.crls.other** as specified in RFC 5940 [10].”	“As long as a validation algorithm can assess the validity of a Signature With Time, it can be augmented to a Signature With Long-Term Validation Data by adding **signed** attributes.”	No. The attributes that are added are themselves unsigned. They will obviously contain signed stuff….
C-7	Figure 8	Page 26	Technical/ Editorial	According to Draft EN 319 122-1 V0.0.8 “Complete Certificate and revocation data on signature and time-stamp” are signed data.	“Complete Certificate and revocation data on signature and time-stamp” shall be integrated in “**signed** data”.	**See above.**
C-8	Chap. 4.3.5.1	Page 27	Technical	**“4.3.5.1 Description** Time assertion SHOULD be integrated	“4..5.1 Description Before algorithms, keys, and other cryptographic data used at the time a signature was built become weak and the cryptographic functions become vulnerable, or the certificates supporting previous signatures or **time assertions** expire or are revoked, the signed	**Accepted**

Organization name	**Clause/ Subclause**	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change**	**RESOLUTION** on each comment submitted
					data, the signature as well as any additional information, should be protected by applying time **assertions**. Such additional time **assertions** are called archive validation data. The **creation of time assertions** should be repeated in time before the protection provided by a previous time **assertions** becomes weak and should make use of stronger algorithms or longer key lengths than have been used in the original signatures or time **assertions**. Several instances of **archive time assertions** may occur with a signature**.”**	
C-9	Figure 9	Page 27	Technical	The right ”Time Stamp” SHOULD be replaced by “Time Assertion”.		**Accepted**
C-10	Figure 9	Page 27	Technical	and “Complete Certificate and revocation data on signature and time-stamp” shall be integrated in “**signed** data”.		**No. See above.**
C-11	Chap. 4.3.5.3	Page 27	Technical	“time-stamp(s)” SHOULD be replaced by “time assertion(s)”	“4.3.5.3 Outputs The process for creating a Signature With Archival Data shall return the signature provided with an added unsigned attribute containing **an archive time assertion**. e.g. a time-stamp token **or evidence records**, on the signature.”	**Accepted**
C-12	Chap. 4.3.5.4	Page 27	Technical	”Time Stamp” SHOULD be replaced by “Time Assertion”.	**“**4.3.5.4 Process The signature augmentation process shall 1. Add any validation material required for validating the signature that is not already present in the signature.	**Accepted with modification. Referencing format-specific aspects is not appropriate here.**

Organization name	**Clause/ Subclause**	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change**	**RESOLUTION** on each comment submitted
					This shall include any validation data of previously added time **assertions**. 2. Request one or more time **assertions** from appropriate TSAs as defined in the signature policy or local configuration. The time **assertions** shall cover all data objects contained **in the element " SignedData.encapContentInfo.eContent" as a DER-coded instance of TST-Info according to RFC3161 .** 3. Produce signature attribute(s) encapsulating the time **assertion**(s) produced in step 2. And 4. Add the **time assertion** as unsigned attribute(s) to the signature."	
C-13	Chap. 5.1.3	Page 30, last paragraph	Editorial	Table No. **2** seems to be wrong.	"In all cases, the signature validation process shall output • a status indication of the results of the signature validation process. Table **5** lists the possible values of the main status indication and their semantics;"	**Already fixed**
C-14	Chap. 5.2.6.3	Page 41	Editorial	Question: Is "for issuing a certificate" correct ?	"3. The building block shall perform validation of the prospective certificate chain with the following inputs: the prospective chain built in the previous step, the trust anchor used in the previous step, the X.509 parameters provided in the inputs and the current date/time. The validation shall be following the PKIX Certification Path Validation [5], clause 6.1 with the exception of the validity model. Two validity models may be supported: • All certificates must be valid at current time; or • All certificates must be valid at the time they were	**Rejected. The chain model text is only relevant for certificates. Signatures (other than those within a certificate) and timestamps are not used in X.509 chain validation.**

Organization name	**Clause/ Subclause**	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change**	**RESOLUTION** on each comment submitted
					used for issuing a **signature or timestamp.** NOTE: This allows to support the shell model (where all certificates must be valid) as well as the chain model. The latter is e.g. required to be used by law in countries like Germany."	
C-15	Chapter 5.4.3 5.3.3 5.5.3 5.6.3.3	Page 49 47 50 59	Editorial	Question: What kind of additional information ? Is the link 5.1.2 correct ? For example: "Chap. 5.4.3: The main output of the time-stamp validation is a status indicating the validity of the time-stamp. This status may be accompanied by additional information (see clause 5.1.2)."		**Link fixed**
C-16	Chapter 5.6.1	Page 51	Technical	"time-stamp token" SHOULD be replaced by "time assertion":	"NOTE 1: This is in particular useful in the case where the SVA takes as input, in addition to the Basic Signature to validate, additional evidences derived from previous validation (e.g. a proof of existence derived from the validation of a time **assertion**)."	**accepted**
C-17	Table 22/23	Page 52	Technical/ Editorial	Please change input and output: See Chap. 5.6.2.1.4: "5.6.2.1.4 Processing 1. The building block shall build a new prospective certificate chain that has not yet been evaluated. The chain shall satisfy the conditions of a prospective certificate chain as stated in [5], clause 6.1, using one of the **trust anchors** provided in the inputs:"	Input Signature or time-stamp token …. **Trust Anchor List** **Output:** Passed + validation time **+ certificate chain**	**Partially Accepted. The Trust Anchor List is part of the X509 validation constraints that was provided as output by the VCI step. This allows filtering any list of trust anchors provided using the validation policy in use. Changed some text in**

Organization name	**Clause/ Subclause**	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change**	**RESOLUTION** on each comment submitted
				See: “5.The building block shall return the current status . If the current status is PASSED, the building block shall also return the **certificate chain** as well as the calculated validation time returned in step 3.”		**5.2.6.4**
C-18	Chap. 5.6.1.4 No. 2	Page 53, 2rd paragraph ff	Technical	It seems that the loop (step 1 ==> step 2 ==> step 1) will never be ended, if it is not possible to find a valid certificate chain.		**No. The first step says: “**shall build a new prospective certificate chain that has not yet been evaluated.”. This set is finite.
C-19	Table 22	Page 53, last paragraph and page 54, first paragraph	Editorial	Seems to be a wrong table number See “5.6.2.2.2 Input Table 22: Inputs to the validation time sliding building block” … Table 22	Table **24** **…** Table **25**	**Already fixed**
C-20	Table 26	Page 55	Technical/ Editorial	Question: only a signature ?	“Table 26: Inputs to the POE extraction building block Input Signature **or data (group) which needs a POE** An attribute with a time -stamp token A set of POEs”	**Agreed that it could be more generic- but it is currently used only with a signature and changing that would make it less understandable**

Organization name	**Clause/ Subclause**	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change**	**RESOLUTION** on each comment submitted
C-21	Chapter 5.6.2.3.4	Page 55/56	Technical/ Editorial	Question: only a signature ?	"1. The building block shall determine the set S of references to objects and objects that are part of the signature **or data (group) that needs a POE** and are protected by the time-stamp. ………"	**As above**
C-22	Chapter 5.6.2.4.4 , No. 2	Page 56, 4th last paragraph	Technical	According to our comment concerning "**Draft ETSI EN 319 122-1 V0.0.8 (2015-02)'/C-20":** 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 5.6.2.4.1 at all. Therefore this section **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.	Completely revise section 5.6.2.4.1 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 5.6.2.4.1 **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.	**Disagree to the statement that algorithm transition is not considered. The assumption is that at this step all PoE are already extracted and available. Thus, proof exists that the algorithm has been used when valid – or not, irrespective of the type of time stamp or mechanism used.**
C-22	Chap. 5.6.2.5	Page 57	Editorial	[16] SHOULD be included.	"5.6.2.5 Evidence record validation building block 5.6.2.5.1 Description This process is used to validate an Evidence Record as specified in ([15]**, [16**])."	**See above**

Organization name	**Clause/ Subclause**	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change**	**RESOLUTION** on each comment submitted
C-23	Chap. 5.6.2.5.2	Page 57	Technical	An Evidence Record includes all Archive Time-stamps (within structures of Archive Time-stamp Chains and Archive Time-stamp Sequences) and additional verification data, like certificates, revocation information, trust anchors, policy details, role information, etc.” (see [17], p. 6) To validate an Evidence Record, the signed data object (group) is a mandatory input and **SHOULD** be included as input.	“5.6.2.5.2 Input Table 28: Inputs to the evidence record validation building block Input **Signed Data Object (group) (mandatory)** Evidence Record(s) Cryptographic constraints Trust anchor list (e.g. TSL) Signature Validation Policies Local configuration Time-Stamp Certificate”	**OK**
C-24	Chap. 5.6.2.5.2	Page 57	Technical	The Evidence Record Validation Process **SHOULD** only output the following status codes: PASSED and **no POEs**, because the Evidence Record (ER) itself is a POE and the POEs in form of time-stamps in the ER are already verified during the Evidence Record Validation Process.	“Time-Stamp Certificate 5.6.2.5.3 Output This process shall output one of the following status codes: **PASSED or FAILED.”**	**Changed ER handling after discussion at ESI#49**
C-25	Chap. 5.6.2.5.4	Page 57	Technical	The evidence record validation process **SHOULD** be done according to [15] or [16]**.**	**Proposal:** “1. The building block shall initialise the set of POEs with the set of hashes of the data objects and members of the data object groups covered by the Evidence Record. **2. Verify that the first Archive Time-stamp of the first Archive Time-stamp Chain (the initial Archive Time-stamp) of the Evidence Record**	**Changed ER handling after discussion at ESI#49**

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted
					contains the hash value of the data object or data object group according to the EncapsulatedContentInfo of .the Signed Data object (group). If this is the case, the building block shall go to the next step. Otherwise, the building block shall return the indication FAILED. 3. The building block shall verify each Archive Time-stamp Chain. a) The building block shall check that the first hash value list of each Archive Time-stamp **(except the initial Archive Time-stamp)** shall **contain** the hash value of the Time-stamp of the previous Archive Time-stamp. If this is the case, the building block shall go to the next step. Otherwise, the building block shall return the indication FAILED. b) **Performing the time stamp validation process ((see clause 5.4)) and if necessary, the past signature validation process (see clause 5.6.2.4), t**he building block shall check **b1)** that each Archive Time-stamp is valid relative to the time of the following Archive Time-stamp. If this is the case, the building block shall go to the next step. Otherwise, the building block shall return the indication FAILED. **b2)** The building block shall check that the hash algorithm used in all Archive Time-stamps within in a chain is considered secure at the creation time of the first Archive Time-stamp of the following Archive Time-stamp Chain. If this is the case, the building block shall go to the next step. Otherwise, the	

Organization name	**Clause/ Subclause**	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change**	**RESOLUTION** on each comment submitted
					building block shall return the indication FAILED. 3. The building block shall verify that the first hash value list (partialHashtree) of the first Archive Time-stamp of all other Archive Time-stamp Chains contains a hash value of the concatenation of the data object hash and the hash value of all older Archive Time-stamp Chain. If this is the case, the building block shall go to the next step. Otherwise, the building block shall return the indication FAILED. 4. The building block shall verify that each Archive Time-stamp was generated before the last Archive Time-stamp of the **preceding** Archive Time-stamp Chain became invalid. If this is the case, the building block shall go to the next step. Otherwise, the building block shall return the indication FAILED. 5. The building block shall verify the **last Archive Time-Stamp** using the validation process for time-stamps (see clause 5.4). If the process returns PASSED, **return with the indication PASSED**. 6. Otherwise, return with the indication FAILED."	
C-26	Table 28	Page 58	Editorial	The input parameter "Signed data object(s)" **SHOULD** be changed to "Signed data object (group)"		
C-27	Chap. 5.6.3.4	Page 59	Technical	See our comments "C-21 and C-22 of **Draft ETSI EN 319 122-1 V0.0.8 (2015-02)":**	Section 5.6 of **Draft ETSI EN 319 122-1 V0.0.8 (2015-02)" SHOULD** be completely revised 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, covering the aspect of **NESTING** of archive time stamps in order to ensure the "long term viability" of	**Out of scope of 102**

Organization name	**Clause/ Subclause**	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change**	**RESOLUTION** on each comment submitted
					the specified archive validation data. Therefore the long term validation process **SHOULD** be completely revised in order to support the new forthcoming data structures for long term archive validation data.	
				Besides this aspect there are more questions and proposals concerning chapter 5.6.3.		
C-28	Chap. 5.6.3.1	Page 59, 2rd last paragraph	Technical	"The process handles the signature as a succession of layers of signatures. Starting from the most external layer (e.g. the last archive-time-stamp) to the most inner layer (the signature value to validate), the process performs the Basic Signature validation algorithm (see clause 5.3 for the signature itself and clause 5.4 for the time-stamps)."	There seams to be a contradiction: The **recursive** performance of the **Basic Signature validation** algorithm form the most external layer to the most inner layer is not found in chapter 5.6.3.4.	**Sentence deleted, no requirements and too confusing.**
C-29	Chap. 5.6.3.1	Page 59, 2rd last paragraph	Technical		Question: Why should there be the performance of the basic Signature validation algorithm from **the most external layer to the most inner layer** and not from the most inner layer to the most external layer ?	
C-30	Chap. 5.6.3.1	Page 59, 2rd last paragraph	Technical	"• In all other cases: If no specific constraints mandating the validity of the attribute are specified in the validation constraints, the long term validation process shall ignore the attribute and shall consider the next time-	Question': What is meant by "consider the next time-stamp attribute" ? Will step 4 be repeated with another time-stamp ? Why don't we need a timely ordered list of POEs ?	**Made more clear.** **The PoEs are assumed to contain a time value. How the PoE list is managed in an implementation is**

Organization name	**Clause/ Subclause**	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change**	**RESOLUTION** on each comment submitted
				stamp attribute. Otherwise, the long term validation process shall fail with the returned indication/sub-indication and associated explanations.”		**implementation dependent.**
C-31	Chap. 5.6.3.1	Page 59, 2rd last paragraph	Technical	“… If it returns PASSED the long term validation process shall go to the next step. Otherwise, the long term validation process shall return the indication/sub-indication and associated explanations returned from the past signature validation process.”	What happens if the past signature validation process is not passed ? Will the next step 6 be performed ?	**No, since the algorithm has to return.**
C-32	Chap. 5.6.3.1	Page 59, 2rd last paragraph	Technical	“3. The long term validation process shall perform the validation process for Signatures with Time as per clause 5.5 with all the inputs, including the processing of any signed attributes as specified. If the validation outputs PASSED If there is no validation constraint mandating the validation of the LTV attributes, the long term validation process shall return the indication PASSED. Otherwise, the SVA shall go to step 3.” Question: Is “step 3” right ?	.. step **4**	**corrected**
C-33	Chap.	Page	Technical	The Integration of the Evidence Record validation process **SHOULD** be changed	**Proposal:**	**No. The Building Blocks are not self-executable,**

Organization name	**Clause/ Subclause**	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change**	**RESOLUTION** on each comment submitted
	5.6.3.4	59		because the Evidence Record is already verified by the "Evidence record validation building block" and must not be verified a second time in the "long term validation process". **See also the following questions:** What is meant by "objects".	"5.6.3.4 Processing 1. **1.** POE initialization: the long term validation process shall add a POE for each **object** in the signature at the current time to the set of POEs. NOTE 1: The set of POE in the input may have been initialized from external sources (e.g. provided from an external archiving system). These POEs will be used without additional processing. **2.** The long term validation process shall perform the validation process for Signatures with Time as per clause 5.5 with all the inputs, including the processing of any signed attributes as specified. If the validation outputs PASSED If there is no validation constraint mandating the validation of the LTV attributes, the long term validation process shall return the indication PASSED. Otherwise, the SVA shall go to step 3. If the validation outputs one of the following indications/sub-indications:INDETERMINATE/REVOKED_NO_POE, INDETERMINATE/REVOKED_CA_NO_POE, INDETERMINATE/OUT_OF_BOUNDS_NO_POE or INDETERMINATE/CRYPTO_CONSTRAINTS_FAILURE_NO_POE, the long term validation process shall go to the next step.	**they need to be invoked in the processing. AH you moved it "down" to step 3 – no problem doing so but is this necessary or just meaningful…** **Object: anything that is part of the signature. Obviously restricted to objects (potentially) involved in validation, but a signature should not contain many useless objects anyhow…**

Organization name	**Clause/ Subclause**	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change**	**RESOLUTION** on each comment submitted
					In all other cases, the long term validation process shall fail with returned code and information. NOTE 2: long term validation is done in the cases INDETERMINATE/REVOKED_NO_POE, INDETERMINATE/REVOKED_CA_NO_POE, INDETERMINATE/OUT_OF_BOUNDS_NO_POE and INDETERMINATE/ CRYPTO_CONSTRAINTS_FAILURE_NO_POE because additional proof of existences can help to go from INDETERMINATE to a determined status. NOTE 3: Performing the long term validation part of the algorithm even when the basic validation returns PASSED can be useful in the case the SVA is controlled by an archiving service. In such cases, it can be necessary to ensure that any long term attribute present in the signature is actually valid before making a decision about the archival of the signature. NOTE 4: Steps 3 and 4 below are not part of the validation process per se, but are present to collect PoEs for step 5.” **3. If there is one or more evidence records, the long term validation process shall perform the evidence record validation process for each of them according to clause 5.6.2.5. If the evidence record validation process returns PASSED, the long term validation process shall add the returned POEs to the set of POEs. And goes to step 6 .** **Otherwise, the long term validation process shall fail with the returned indication/sub-indication and associated explanations.**	

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted
					4. If there is at least one time-stamp attribute, the long term validation process shall perform the time-stamp validation process, starting from the last (the newest) one, as per clause 5.4: a)If PASSED is returned and the cryptographic hash function used in the time-stamp (messageImprint.hashAlgorithm) is considered reliable at the generation time of the time-stamp, the long term validation process shall perform the POE extraction process with the signature, the time-stamp and the cryptographic constraints as inputs. The long term validation process shall add the returned POEs to the set of POEs. b) Otherwise, the long term validation process shall perform past signature validation process with the following inputs: the time-stamp, the indication/sub-indication returned by the time-stamp validation process, the TSA's certificate, the X.509 validation parameters, X.509 validation constraints, cryptographic constraints and the set of POEs. • If it returns PASSED and the cryptographic hash function used in the time-stamp is considered reliable at the generation time of the time-stamp, the long term validation process shall perform the POE extraction process and shall add the returned POEs to the set of POEs. In all other cases: If no specific constraints mandating the validity of the attribute are specified in the validation constraints, the long term validation process shall ignore the attribute and shall **go back to the beginning of step 4 (see C-**	

Organization name	**Clause/ Subclause**	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change**	**RESOLUTION** on each comment submitted
					28 **), if there exist a next time-stamp attribute.** Otherwise, the long term validation process shall fail with the returned indication/sub-indication and associated explanations. 5. Past signature validation: the long term validation process shall perform the past signature validation process with the following inputs: the signature, the status indication/sub-indication returned in step 2, the signing certificate, the X.509 validation parameters, certificate meta-data, chain constraints, cryptographic constraints and the set of POEs. If it returns PASSED the long term validation process shall go to the next step. Otherwise, the long term validation process shall return the indication/sub-indication and associated explanations returned from the past signature validation process. 6) Data extraction: the SVA shall return the success indication PASSED. In addition, the long term validation process should return additional information extracted from the signature and/or used by the intermediate steps. In particular, the long term validation process should return intermediate results such as the validation results of any time-stamp token. What the DA does with this information is out of the scope of the present document.”	

D

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted
D 1	**4.3.1**	**3**	**General**	The claim here seems to be that if the CA provides historical revocation data, then we can check the revocation status for the time of signing. This does not seem right. With a Basic Signature, you do not know the time of signing, so such historical revocation data will be of no value for the validation process. This is actually confirmed in the draft, under the description of the validation process for Basic Signatures. Section 5.2.6.4, step 1, states that the return if the certificate is expired shall be INDETERMINATE/OUT_OF_BOUNDS_NO_POE. **See also *)**	**Remove the sentence: "If the issuing CA keeps revocation information on expired certificates available, such signature** **can also be validated long after expiration of the certificates used."**	First of all, this is partially a result from changing all MAYs to CANs, so the sentence is too strict when using CAN, MAY makes a lot of difference. But does not solve the issue. • The sentence is wrong: because the algorithm indeed will need to return INDETERMINATE • The sentence is right in spirit: but explaining what actually is meant makes the text likely confusing. decided to remove the sentence.
D 2	**5.1.2**	**Bullet point 1.2**		(Same as above)	**Remove the bullet point: "the time of validation lies beyond the validity period of the signing certificate when the certification** **authority provides revocation information for expired certificates."**	**Not removed. But clarified**
D	**5.5.4**			It is not clear why the time-stamp does not protect against certificate expiration. You can, using the	**Provide explanation why time-stamp does not protect against expiration.**	**improved explanation in Note 6**

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted
				time-stamp, be able to prove that the signature was created in the certificates validity period. But you will of course need historical revocation data, and maybe this is the reason? The standard could explain this better.		

E

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted
E			Ge	An additional minor point – the procedure for determining the evaluation date of a certificate mentions the revocation date. There are two dates of interest – the date the revocation was generated, and the effective date. Most operators will ensure that these are the same, but this is not guaranteed.		The revocation date to be used is the effective revocation date.
				A greater concern, and I did not notice this covered in the new documents, is the following scenario: Signature is generated Due to a race condition, or	I can think of two approaches that would solve this problem: 1) Have a trusted evaluator evaluate the signature while the certificate is still within the validity period (which ensures revocation	1) Out of scope for 319 102 2) This approaches the “grace period” question which is not new and a policy issue.

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted
				possibly due to the effective date of revocation being prior to the issue date, the signature is evaluated as valid, and time stamped, even though it is truly revoked. If the signature is verified during the validity period of the certificate, at some time after the race condition has been resolved, then it will evaluate as revoked. A operator is only obligated to keep revocation information for two CRLs past the validity period of the certificate, and the revocation information then ages out of the CRL. If the signature is evaluated at this point, then it will evaluate as valid. I ran into this while discussing how to use XAdES for official business purposes with the government of Costa Rica.	information should still be available), generate an evaluation report, and add it as a countersignature on the full signature. 2) Require that a set of revocation information be present which was created during the validity period of the certificate, but at some suitable time after the signature time.	

F

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

Organization name	**Clause/ Subclause**	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change**	**RESOLUTION** on each comment submitted
F 1.	Foreword	2nd paragraph.	Ge & Te	A companion document, i.e. TS 119172-1 v009 Signature Policy Framework**,** indicates that a signature policy is : a signature creation policy, signature augmentation policy, signature validation policy or any combination thereof. So this series of documents should address signature augmentation in addition to signature creation and signature validation. Signature augmentation is concerned with: 1) Signatures With Time, and 2) Signatures With Long-Term Validation Data, and 3) Signatures with Archival Data. The content of sections "4.3.3 Creation of a Signature with Time", "4.3.4 Creation of Signatures With Long-Term Validation Data" and "4.3.5 Creation of Signatures with Archival Data" should be placed under a new section 5 called: "Signature augmentation".	The structure of the document should be changed. Instead of having two major sections: 4. Signature creation 5. Signature validation there should be three major sections: 4. Signature creation 5. Signature augmentation 6. Signature validation The new section 5, should contain: - Section 5.1 Augmentation of a Signature with Time, - Section 5.2 Augmentation of Signatures With Long-Term Validation Data" and - Section "5.3 Augmentation of Signatures with Archival Data Note that the three above operations should be done under a signature augmentation policy.	REJECTED. The term “signature augmentation” has been introduced though in the discussion of the lifecycle.
F 2.	Foreword	2nd paragraph	Te	This document indicates that there will be two parts: Part 1: Creation and Validation Part 2: Validation Report Structure There is no reason to make Part 2 normative. A TS or a TR would be sufficient.	Part 2 should not be part of this EN. It should only be a TS or a TR. The references to the current Part 2, i.e. "Validation Report Structure", should be deleted.	Rejected. This was requested by the EC.

Organization name	**Clause/ Subclause**	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change**	**RESOLUTION** on each comment submitted
F 3.	Title	.	Ge & Te	The current title of the document is: Procedures for Creation and Validation of AdES Digital Signatures Part 1: Creation and Validation 1° Since AdES means "Advanced Electronic Signature", speaking of "AdES Digital Signatures" i.e. "Advanced Electronic Signature Digital Signatures" does not make sense. 2° Since the content includes augmentation of signatures, the augmentation process is not captured in the title. The title should be revised.	Replacement proposal for the title: Procedures for Creation, Augmentation and Validation of AdES containing digital signatures. Part 1: General See a further comment (Comment 6) , to understand why "Part 1: General has been added".	While one can certainly discuss if "AdES Digital Signature" make sense, AdES has been selected as a kind of "Trade Mark" and is that term is used throughout the documents, Rejected as are all similar comments below.
F 4.	Scope	Page 8. second sentence	Te	The text states: The present document specifies procedures for: (...) - establishing whether an AdES digital signature is technically valid, There can be different kinds of AdES. This document is concerned with AdES containing a digital signature (among other data elements). The word "containing" is missing.	Change into: The present document specifies procedures for: - the creation of AdES containing digital signatures, - establishing whether an AdES containing a digital signature is technically valid,	See above
F 5.	Scope	Page 8. second sentence	Te	The text states: whenever the AdES digital signature is based on public	Change into: whenever the AdES containing a digital signature is based on public key cryptography	See above

Organization name	**Clause/ Subclause**	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change**	**RESOLUTION** on each comment submitted
				key cryptography and supported by public key certificates. To improve readability of the document, AdES digital signatures are meant when the term signature is being used. Same remark as the previous one.	and supported by public key certificates. To improve readability of the document, an AdES containing a digital signature is meant when the term signature is being used.	
F 6.	Scope		ge & te	It is quite strange to see that there is no indication in the current document about the specificities related to <u>qualified</u> electronic signatures, in the three previous contexts: creation, augmentation and validation.	It would make sense to have an additional part to this series of documents called: Part 2: Specificities applicable to qualified electronic signatures. Apparently, the "Rationalized framework" missed that point.	Rejected. Decided by ESI as is.
F 7.	Section 2.1. Normative references	Page 9. Third paragraph	Te	The text states: The following referenced documents are necessary for the application of the present document. All these references are not necessary. A company may choose to support only XAdES so the references to PAdES or CAdES do not make sense. A company may choose to support only signature creation, so the reference to RFC 3161 does not make sense when time-stamping is done by the verifier. EditHelp! should be contacted to see how to address this issue.	Contact EditHelp! to address the issue of the normative references. This is an important topic which might require an important restructuring of the whole document.	EditHelp is always contacted. References certainly will be re-checked. Comment regarding 3161 irrelevant.
F 8.	Section 3.1. Page 11		te	The text defines "certificate" whereas it should define : "certificate for electronic signature"	Replace with: certificate for electronic signature: an electronic attestation which links electronic signature validation data to a natural person	Definitions taken from common set of definitions in TR 119 001

Organization name	**Clause/ Subclause**	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change**	**RESOLUTION** on each comment submitted
				which is defined in the EU Regulation.	and confirms at least the name or the pseudonym of that person.	
F 9.	Section 3.1. Page 11		te	The text states: signature creation system: the overall system, consisting of the signature creation application and the signature creation device, that creates a *digital* signature. Such a system creates an AdES rather than simply a digital signature. Replace "digital" by "electronic.	Replace with: signature creation system: the overall system, consisting of the signature creation application and the signature creation device, that creates an *electronic* signature.	Definitions taken from common set of definitions in TR 119 001
F 10.	Section 3.1. Page 12		te	The text states: digital signature : data associated to, including a cryptographic transformation of, a data unit that a) allows to prove the source and integrity of the data unit, b) allows to protect the data unit against forgery, and c) allows to support signer non-repudiation of signing the data unit. A **digital signature does NOT allow by its own to support signer non-repudiation of signing the data unit** (i.e. as indicated in the third item) since it does not include a key to verify the digital signature, nor a time-stamp token which is necessary to have an upper limit of the time when the signature was generated if the public key (in practice, the certificate containing	Replace with: digital signature: data appended to a data unit that allows the recipient of the data unit to prove the source and integrity of the data unit *if it knows the verification data to be used* and protect against forgery e.g. by the recipient.	Definitions taken from common set of definitions in TR 119 001

Organization name	**Clause/ Subclause**	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change**	**RESOLUTION** on each comment submitted
				the public key) has been revoked. a **digital signature** is a cryptographic checksum generated using the private key of an asymmetric algorithm. The public key to be used for verification is NOT indicated and has to be known by "some means" by the recipient.		
F 11.	Section 3.1. Page 12		Te	The text defines: secure signature creation device: a signature creation device which meets the requirements laid down in Annex III of Directive 1999/93/EC. Definitions should not reference the EU Directive anymore and such a definition has been removed in the new EU Regulation. This term has been replaced by "qualified electronic signature creation device", i.e. an electronic signature creation device that meets the requirements laid down in Annex II of the EU Regulation.	Either delete or replace by the definition for a "qualified electronic signature creation device" which does not need to be exactly identical to the one present the EU Regulation.	Definitions taken from common set of definition in TR 119 001
F 12.	Section 3.1. Page 12		Te	The text states: signature creation policy: set of rules, applicable to a single digital signature *or to a set of interrelated digital signatures*, that defines the technical and procedural requirements for their creation, in order to meet	Replace with: signature creation policy: set of rules, applicable to a single electronic signature, that defines the technical and procedural requirements for its creation, in order to meet a particular business need, and under which the electronic signature can be determined to be conformant.	Definitions taken from common set of definitions in TR 119 001

Organization name	**Clause/ Subclause**	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change**	**RESOLUTION** on each comment submitted
				a particular business need, and under which the digital signatures can be determined to be conformant. A signature creation policy applies to an electronic signature. When multiple signatures are needed, each one may have its own signature policy. The use of the words " *or to a set of interrelated digital signatures* " is inappropriate. See the other comments about TS 119172-1.		
F 13.	Section 3.1. Page 12		Te	The wording "signature scheme" is not used anywhere in this document, except in the definition of a cryptographic suite. The wording "cryptographic suite" is not used anywhere in this document. cryptographic suite: combination of a digital *signature scheme* with a padding method and a cryptographic hash function. signature scheme: triplet of three algorithms composed of a signature creation algorithm, a signature verification algorithm and a key generation algorithm.	Delete the two following definitions: cryptographic suite: combination of a digital *signature scheme* with a padding method and a cryptographic hash function. signature scheme: triplet of three algorithms composed of a signature creation algorithm, a signature verification algorithm and a key generation algorithm. Note: They would have been deleted by EditHelp! anyway, but it is a loss of time for reviewers.	See TR 119 001
F 14.	Section 3.1. Page 12		Te	The text states: signature verification device: configured software or hardware used to implement the signature-verification data. The EU Regulation is only using the term device in the context of	Delete the definition of a "signature verification device". Note that this wording is not used anywhere else in this document. It would have been deleted by EditHelp! anyway. Delete the definition of a "signature verification data": data, such as codes or public cryptographic keys, which are used for the purpose of verifying an electronic signature.	Definitions taken from common set of definitions in TR 119 001 A normal reader should be able to understand the difference between – and so should an experienced reader.

Organization name	**Clause/ Subclause**	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change**	**RESOLUTION** on each comment submitted
				signature creation, but not in the context of signature verification. The EU Regulation is no more using the term "signature-verification data" which was ambiguous. This document is however using the following definitions: signature verification data": data, such as codes or public cryptographic keys, which are used for the purpose of verifying an electronic signature. but also : signature verification: process of checking the cryptographic value of a signature using signature verification data. The former definition refers to an electronic signature, while the later to a digital signature !!! Since we also have " signature verification" defined, what is the difference between : "signature verification" and "signature validation" ??? A normal reader as well as an experienced reader is completely lost.	Note that the wording "signature verification data" is not used in the main body of the document (except in a single note) and in the definitions section. Replace the definition of "signature verification" by "digital signature verification": digital signature verification: process of checking the cryptographic value of a digital signature using a public key. Delete " signature verification data" since we are now in the context an electronic signatures containing digital signatures and everybody should know what a public key is.	**signature validation:** process of verifying and confirming that a signature is valid **signature verification:** process of checking the cryptographic value of a signature using signature verification data

F 15.	Section 3.1. Page 12		Te	This document defines: signature validation: process of verifying and confirming that a signature is valid and signature validation application: application that implements signature validation. It is very unclear to understand whether these two definitions relate to the validation of a digital signature or to the validation of an electronic signature that contains a digital signature. When reading the content of the document, it appears that it relates to the validation of an electronic signature.	Replace the definition of "signature validation" by: signature validation: process of verifying and confirming that an electronic signature containing a digital signature is valid	Rejected. This definition will hold for any form of signatures.
F 16.	Section 3.1. Page 12		Te	The text states: trusted list: profile of the trust service status list that is the national supervision / accreditation status list of certification services from Certification Service Providers, which are supervised / accredited by the referenced Member State for compliance with the relevant provisions laid down in Directive 1999/93/EC. It is irrelevant to continue to speak about the Directive 1999/93/EC. The content of the document does not address Qualified electronic signatures, nor trusted lists.	Delete the definition of trusted list. However, speaking of " trusted lists" in the new proposed Part 2, i.e. "Part 2: Specificities applicable to qualified electronic signatures" would make sense;	Accepted

F 17.	Section 3.2. Page 13		Te	The text states: QCP Qualified Certificate Policy The acronym is not used in the main body of the document.	Delete. EditHelp! will make that check, anyway, but it is a loss of time for reviewers. There may be other deletions to be performed.	ok
F 18.	Section 4.1 Page 14		te	The text states: The objective of signature creation is to generate a signature covering the Signer’s Document (SD), the signing certificate or a reference to it, as well as signature attributes supporting the signature and its interpretation and purpose. The text is ambiguous since the word digital signature is not used, but this is not the single objective.	Replace with: The objective of electronic signature creation is to generate a digital signature covering the Signer’s Document (SD), the signer's certificate or a reference to it, as well as signature attributes which will be used by a verifier when verifying later on that electronic signature.	Rejected. We are only talking about AdES digital signatures in the whole document. No need to mix up things here.
F 19.	Section 4.1. Pages 14 & 15	Figure 1	Te	The Figure has an horizontal arrow at the bottom called: authentication data. The arrow denotes the signature invocation which is the 'Wilful Act' of the signer, as defined in section 3.1 of this document.	Change "authentication data" into: "signature invocation" or into: "signature invocation, e.g. using authentication data".	Rejected, not needed.
F 20.	Section 4.2.5.2 Page 18	Note	Te	The text states: 4.2.5.2 Signing certificate identifier This attribute shall be a signed attribute. The text is ambiguous since it does not say whether this attribute shall be present or not. The same comment applies for the following attributes.	Replace with: 4.2.5.2 Signing certificate identifier This attribute shall always be present and shall be a signed attribute.	Rejected. It has been decided that this document does not specify which attributes are required and which are not.
F 21.	4.2.5.3 Page 18		Te	The text states: 4.2.5.3 Signature policy identifier This attribute shall be a signed	Replace with: When this attribute is present, it shall be a signed attribute.	Rejected. It has been decided that this document does not specify which attributes are required and

				attribute. The same comment applies for the following attributes.	Please address every attribute and make the adequate changes.	which are not.
F 22.	Section 4.2.5.6. Page 19		Te	The text states: NOTE: If an AdES signature does not contain a recognized commitment type then the semantics of the AdES signature is dependent on the document being signed and the context in which it is being used.	Change into: NOTE: If an AdES signature does not contain a recognized commitment type then the semantics of the AdES signature is dependent upon the semantics of the document being signed and the context in which it is being used.	Accepted with changes
F 23.	Section 4.2.9. Page 20		Te	The text states: 4.2.9 Signature The SCDev shall take the DTBSR and apply the signature algorithm specified in the signature suite. The result of this process shall be *the signature val*ue. Since the definition of signature creation device is configured software or hardware used to implement the signature creation data and to create a digital signature, it will be more precise to add the word "digital".	Change into: 4.2.9 Signature The SCDev shall take the DTBSR and apply the signature algorithm specified in the signature suite. The result of this process shall be a digital signature value.	Rejected. It has been clearly stated in the scope that *AdES digital signatures* are meant when the term *signature* is being used
F 24.	Section 4.2.11 Page 20	Second sentence	Te	The text states: This additional data is called validation data, is the result of a signature augmentation process and shall include: ... and Attributes Certificates (ACs) The use of Attributes Certificates (ACs) is not mandatory. Delete "and Attributes Certificates (ACs)".	Delete "Attributes Certificates (ACs)".	Changed avoiding giving the impression ACs shall be contained there.

F 25.	Section 4.3.1 Page 21	Figure 3	Te	The figure is not correct. "Signature value" should be replaced "Digital Signature" while "Digital Signature" should be replaced by "Electronic signature". The title of the figure should be replaced by : "Figure 3: Electronic Signature". It then becomes crystal clear that an electronic signature includes a digital signature among other data.	Replace "Signature value" by "Digital Signature" Replace "Digital Signature" by "Electronic signature". Replace The title "Figure 3: Digital Signature" by : "Figure 3: Electronic Signature".	Rejected. See discussion on digital/electronic/signature above.
F 26.	Section 4.3.1. Page 21	Second paragraph	Te	The text states: Figure 4 illustrates the life cycle of a signature.	Change into Figure 4 illustrates the life cycle of an electronic signature.	Rejected. See discussion on digital/electronic/signature above.
F 27.	Section 4.3.1 Page 21	Third paragraph. Second sentence	Te	The text states: A Basic Signature is a signature that can be validated as long as the corresponding certificates are neither revoked nor expired. It would be worthwhile to add: "and thus cannot be validated anymore as soon as one of the certificates that has been used to build a certification path up to a trusted root has expired or has been revoked".	Change into : A Basic Signature is a signature that can be validated as long as the corresponding certificates are neither revoked nor expired and thus cannot be validated anymore as soon as one of the certificates that has been used to build a certification path up to a trusted root has expired or has been revoked. Otherwise replace with: A Basic Signature is a signature that cannot be validated as soon as one of the certificates that has been used to build a certification path up to a trusted root has expired or has been revoked.	Rejected. Deemed sufficient as is.
F 28.	Section 4.3.1 Page 21	Third paragraph. Third sentence.	Te	The text states: If the issuing CA keeps revocation information on expired certificates available, such signature can also be validated long after expiration of the certificates used. This is untrue. If revocation information on expired	Delete the sentence.	Sentence has been deleted.

				certificates is maintained after the expiry of the certificate, then it is the status of the certificate at the end of the validity period which is retained and not the status at the current time. So if the private key has been compromised one month after the expiry of the certificate, nobody will know and the end result will be fully wrong. It is necessary to know that the digital signature was computed prior to the expiry of the signer's certificate but a Basic Signature is unable to accomplish this. The sentence is very dangerous and should be deleted.		
F 29.	Section 4.3.1 Page 21	Note 1	Te	The text states: NOTE 1: It can be used to validate a signature when a certificate has been revoked after the signature has been created. This is true but insufficient. It can also be used to validate a signature when a certificate has NOT BEEN revoked. So, it is not a main property The key point is that the signature can be validated during the validity period of the signer's certificate, since all the revocation information is still available during the validity period of the signer's certificate.	Change into : NOTE 1: It can be used to validate a signature during the validity period of the signer's certificate. Otherwise, suppress the note and change the previous line with: A Basic Signature with Time is a signature that proves that the signature already existed at a given point in time and which may be validated during the validity period of the signer's certificate."	Rejected. Changes not correct.
F 30.	Section 4.3.1 Page 21	Note 3	Te	NOTE 3 states: NOTE 3: Archival data can be an archive time-stamp token. At this point of time, the reader has no clue of what an "archive time-stamp token" may be, since this term is not defined before.	Either delete the Note or add a definition of "archive time-stamp token" in the Definitions section.	Removed the NOTE.

				Either delete the Note or add a definition of "archive time-stamp token" in the Definitions section.		
F 31.	Section 4.3.2.1 Page 22	Figure 5	Te	Figure 5 is missing to show one major box : some signature creation policy MUST be selected or used immediately after the document(s) to be signed has been selected to know which certificate may be adequate and which other rules must be applied during the signature creation process. A box showing the "signature creation policy" is missing.	Add a box to Figure 5 in the second position showing the "signature creation policy".	accepted
F 32.	Section 4.3.2.2 Page 22	Table 1	Te	An input to Table 1 is missing: the signature creation policy.	Add a line at the top of table 1 for the "Signature creation policy". It should be made "mandatory".	accepted
F 33.	Section 4.3.2.2 Page 22	Table 1	Te	An input to Table 1 is missing: the current time. When a smartcard contain several certificates, it can be used to know which one is currently valid. Note that section "4.3.2.4.5 Signing" states: Before invoking use of the signature creation data, the SCS (SCA or SCDev) should check that the signing certificate is valid (cryptographically correct, within its validity period and not revoked). If the current time is not available, this cannot be done.	Add a line to Table 1 for the "Current time". It should be made "optional'.	rejected. The current time is assumed to being available to the SCS implicitly. Added note to that fact.
F 34.	Section 4.3.2.3 Page 22	Figure 6	Te	Figure 6: Basic Signature" has the same problems as Figure 3. See comment n° 24.	Replace "Signature value" by "Digital Signature". Replace "Basic (Digital) Signature" by "Basic	Rejected. See discussion on digital/electronic/signature above. BES and Basic

				Replace "Basic (Digital) Signature" by "Basic Electronic signature". The acronym "BES" has been used for more than 13 years and it is not this very last version of the documents (that nobody will have the time to read in full) which should change this ! BES means Basic ELECTRONIC signature. These documents should not re-invent the vocabulary !!!	Electronic Signature". Replace The title "Figure 3: Digital Signature" by : "Figure 6: Electronic Signature".	Signature are mapped in Annex B.
F 35.	4.3.2.4.1 Page 23	The NOTE.	te	The text states: NOTE: Legal requirements can mandate explicit signer involvement in selection of document to sign. This may also be coming from the signature policy rather than by the application which translated the legal requirements.	Change into:: NOTE: Legal requirements and/or the signature creation policy can mandate explicit signer involvement in selection of document to sign.	Well, yes and no. Actually, the legal requirements will force to select a policy that mandates explicit signer involvement. Since we do not state the involvement of policy in every place where policy may be involved (this could be <everywhere>, almost), we will not do that here (and not in a note)
F 36.	4.3.2.4.1 Page 23	Third paragraph.	te	The text states: When a document is selected for signing, any existing signature on or attached to the document should be validated. If the signature is validated, a warning shall be provided in case validation of an existing signature yields a TOTAL-INVALID or INDETERMINATE result. This depends whether the signatures are made in parallel or are embedded. In case of parallel signatures, this should be left fully open. The first sentence uses a	Delete this paragraph and add a second NOTE: When a document is selected for signing, any existing signature on or attached to a document on which the new signature will apply should be validated. In such a case, a warning should be provided in case validation of an existing signature yields a TOTAL-INVALID or INDETERMINATE result.	Rejected. This has been agreed on as is.

				"should" while the second uses a "shall". It is proposed to use a NOTE, rather to place this wording in the main body of the document and to modify the text.		
F 37.	4.3.2.4.2 Page 23	New section 4.3.2.4.2	Te	The first sub-section is about : 4.3.2.4.1 Selection of documents to sign. The next step should be : 4.3.2.4.2 Selection of the signature creation policy to use. A new section should be added. See the text proposal.	Add a new section: 4.3.2.4.2 Selection of the signature creation policy to use The Driving Application shall either select the signature creation policy or such a selection shall be explicitly done by the signer through a user interface.	Rejected. The SCP is now available as an optional input. The use of a policy is not mandatory.
F 38.	4.3.2.4.3 Page 23	New section 4.3.2.4.3	Te	The next step should be : 4.3.2.4.3 Selection of the signer's certificate to use A new section should be added. See the text proposal.	Add a new section: 4.3.2.4.3 Selection of the signer's certificate to use The SCA should identify which signer's certificates are appropriate according the signature creation policy and which is within its validity period at the current time. If only one certificate corresponds to these criteria, then no specific user involvement is needed for the certificate selection. If there is more than one certificate which satisfies to the criteria then the selection shall be explicitly done by the signer through a user interface.	Rejected. The certificate is assumed to be available as an input to the process. Any certificate selection is assumed to already have happened within the DA
F 39.	4.3.2.4.2 Page 24	First sentence.	Te	The text states: The signing certificate identifier attribute (see 4.2.5.2) shall be included in the DTBS whenever required by the format and the contents of the signature. It is important to add a sentence	Before the first sentence, add: Once the signing certificate has been selected, ...	Rejected. See above.

				to indicate that the certificate to be used should be selected.		
F 40.	4.3.2.4.5 Page 24	Second paragraph.	Te	The text states: Before invoking use of the signature creation data, the SCS (SCA or SCDev) should check that the signing certificate is valid (cryptographically correct, within its validity period and not revoked). The text is going too far. 1° It should be possible to sign off-line. Thus revocation checking is not always possible. As a consequence, the requirement about "not revoked" should be deleted. 2° In order to verify that he certificate is cryptographic correct, a CA certificate should be locally available, which is usually not the case. As a consequence, the requirement about "cryptographically correct" should be deleted. 3° It is easy to check using the current time that the signer's certificate is within its validity period. This requirement should be made mandatory, hence why the "should" for that case (and that case only) should be changed into a "shall". 4° Since the SCDev has no clock and the content of the certificate is opaque to the SCDev (see TC 224 WG 16), the SCDev is not able to do it, hence why the term SCDev should be deleted.	Change into : Before invoking use of the signature creation data, the SCA shall check that the signing certificate is within its validity period. It is also possible to also a NOTE. NOTE: Whenever the SCA application is aware about which signature verification policy should be used, it may check that the signing certificate is valid against that signature verification policy.	Rejected: it’s optional and not required, thus it is fine not to do it. Also, There are SCDevs that have a clock and that can do more than a smart card.

F 41.	4.3.2.4.6 Page 24	First sentence.	Te	The text states: Access to the signer's signature creation data (the private key) in the SCDev may require the user to enter specific signer authentication data. The sentence is ambiguous, since the user nor the SCA has an access to any private key, however, it can "use" it; hence why the term "use" is more appropriate. Using the word 'the" in front of "private key" may let think that there is only one private key.	Change into: The use of the signer's signature creation data (the private key) in the SCDev corresponding to the selected certificate may require the user to enter specific signer authentication data.	Accepted adding "The use of". Rejected the second part. Does not add anything that is not obvious
F 42.	4.3.3. Page 25	New section 5	te	As indicated earlier, a new section 5 called : "5. Signature augmentation " Should be placed here.	Add: "5. Signature augmentation "	Rejected as discussed above.
F 43.	4.3.3. Page 25	New section 5	te	Before diving into the details, additional explanations should be provided. See the text proposal.	Text proposal: Signature augmentation is a process where various data elements can be added to a Basic Electronic Signature (BES). The goal of these additional elements is to allow to validate an electronic signature "in the future" and to provide validation results that are consistent with those obtained at an initial validation. These additional data elements may be placed into an electronic signature either by the SCA, or by the SVA or by a third party. Either a local configuration and a signature augmentation policy shall be used to know the rules and the parameters to capture and to add to these data elements. This document considers three kinds of data	Rejected as discussed above.

					additions which cover different goals: 1. Augmentation of a Signature with Time (see section 5.1), 2. Augmentation of a Signature with long term validation data (see section 5.2), and 3. Augmentation of a Signature with Archival Data (see section 5.3).	
F 44.	4.3.3. Page 25	New section 5.1	te	As indicated earlier, section 4.3.3 should be placed under a new section 5 called "5. Signature augmentation " and thus be renamed: 5.1 Augmentation of a Signature with Time.	Rename section "4.3.3 Creation of a Signature with Time" with "5.1 Augmentation of a Signature with Time".	Kept 4.3.3 as is
F 45.	4.3.3. Page 25	Figure 7	Te	Figure 7 : Signature with time" has the same problems as Figure 3. Replace "Basic (Digital) Signature with Time " by "Basic Electronic signature with Time ".	Replace "Signature value" by "Digital Signature". Replace "Basic (Digital) Signature" by "Basic Electronic Signature". Replace the title "Figure 7: Signature with time " with : "Figure 7: Electronic Signature with time".	Rejected as Above
F 46.	4.3.3.2 Page 25	Table 2	Te	A sentence in 4.3.3.4 states: "The signature augmentation process shall request one or more time-stamp tokens from appropriate TSAs as defined in the signature policy," hence why the signature augmentation policy should be one of the inputs.	Add one line at the top of Table 2 for : "Signature augmentation policy". This input should be optional (since a "local configuration" is another alternative).	Accepted

F 47.	4.3.3.2 Page 25	Table 2	Te	Does it make sense to augment a signature with a TST if the signer's certificate has already expired ? It does not. It would make sense to an add an optional input to Table 2: the current time.	Add a line to Table 1 for the "Current time". It should be made "optional'. See an additional text proposal later.	Rejected. The current time can be assumed to being available anyhow.
F 48.	4.3.3. Page 25	NOTE 2 and NOTE 3	Te	NOTE 2 states: NOTE 2: Time-stamp token provides the initial steps towards providing long term validity. The time-stamp tokens need to be created before a certificate has been revoked or expired. If this cannot be achieved, validation of the created signature can fail. This NOTE, nor the next one, does clearly not clearly explain why a TST is needed, even if "long term validity" is not required. It is required to make sure that a signature checked as valid today, will be still be checkable as valid by someone else one day after. Is it "*long term validity*", a term that is not even clearly explained ? NOTE 2 should be melted with NOTE 3 which starts with the right explanation, i.e. "The Signature with Time provides independent evidence of the existence of the signature prior to the time-stamp token indication", but is missing one major indication.	Replace NOTE 2 and NOTE3 with the following text which should be moved in the main body of the document rather than in a NOTE. A Time-stamp token (TST) applied either directly on the digital signature or on a data structure that includes the digital signature provides independent evidence of the existence of the digital signature prior to the time contained in the time-stamp token. The time contained in the time-stamp token shall be used to check whether the signer's certificate was revoked, suspended or not revoked at that time. To reduce the risk of repudiating signature creation, the time-stamp token ideally should be as close as possible to the time the signature was created. The signer or a TSP may provide the Signature with Time. If the signer did not provide it or the TSA the signer used is not trusted by the verifier, the verifier should create a Signature with Time on first receipt of a signature.	Rejected. the notion that a TST is required to be able to check a signature “tomorrow” is rejected but this is a discussion not for here. This is not the place to define what shall be used for checking, this is not the validation part. Since this is not the place to formulate any requirements, it is preferred to leave this as notes.

				It is proposed to replace NOTE 2 and NOTE 3 with a text using most of their content and which should be moved in the main body of the document.		
F 49.	4.3.3.4. Page 26	New section 5.1.4	te	At the end of section 4.3.3.4 Process, (now section 5.1.4) the way to use the current time should be indicated.	Additional text proposal: The signature augmentation process should check that the signer's certificate is still within its validity period, otherwise the process would be ineffective since a TST shall be applied as soon as possible after the instant of the creation of the signature but before the end of the validity period of the signer's certificate.	Rejected, since it is not mandatory and there may be use cases that do as described. Added as a note however.
F 50.	4.3.4. Page 26	New section 5.2	te	As indicated earlier, section 4.3.4 should be placed under a new section 5 called "5. Signature augmentation " and thus be renamed: 5.2 Augmentation of a Signature with Long-Term Validation Data.	Rename section "4.3.4 Creation of a Signature With Long-Term Validation Data" by "5.2 Augmentation of a Signature with Long-Term Validation Data".	rejected as above
F 51.	4.3.4. Page 26	Figure 8	Te	Figure 8 : Signature with long term validation data " has the same problems as Figure 3. See comment n° 24.	Replace "Signature value" by "Digital Signature". Replace "Basic (Digital) Signature" by "Basic Electronic Signature". Replace "Basic (Digital) Signature with long term validation data " by "Basic Electronic Signature with long term validation data". Replace The title "Figure 7: Signature with long term validation data " by : "Figure 6: Electronic Signature with long term validation data ".	Rejected as Above
F 52.	4.3.4. Page 26	Table 3	Te	An input to Table 3 is missing, for the Signature augmentation policy.	Add one line at the top of Table 3 for : "Signature augmentation policy". This input should be optional (since a "local configuration" is another alternative).	Accepted

F 53.	4.3.4. Page 26	Table 3	Te	Does it make sense to augment a signature with long term validation if the signer's certificate has already expired ? It does not. It would make sense to an add an optional input to Table 2: the current time.	Add a line to Table 1 for the "Current time". It should be made "optional'. Add the appropriate text to explain more in the main body of the document.	Rejected. The current time is assumed to being available to the SVA.
F 54.	4.3.4.1 Page 26	First sentence	Te	The text states: As long as a validation algorithm can assess the validity of a Signature With Time, it can be augmented to a Signature With Long-Term Validation Data by adding unsigned attributes. A validation algorithm can ONLY assess the validity of a Signature With Time during the validity period of the signer's certificate. This should be mentioned. The second part of the sentence is using "it". - If the "it" refers to the validation algorithm, it does not make sense. - If the "it" refers to the Signature With Time, it can be augmented to a Signature With Long-Term Validation Data, but the reader has no clue for which reason. In both cases, this sentence does not help. See the text on the right to support more complete explanations.	Change into: A signature validation algorithm can assess the validity of a Signature With Time only during the validity period of the signer's certificate, when the validation data required to validate the signature is still on-line available to the verifiers. In case it is unsure that the validation data required to validate the signature will still be on-line available to the verifiers or that some verifiers cannot access that data, then it is necessary to capture that data inside the electronic signature. According to X.509 and to RFC 5280, CAs are not mandated to maintain the revocation status of the certificates they have issued beyond the end of their validity. This is the reason of another format of electronic signatures called " Electronic Signatures With Long-Term Validation Data". A Signature With Time may then be augmented to a Signature With Long-Term Validation Data by adding unsigned attributes. This augmentation can be done either by the SCA, or by a third party or by a verifier using a SVA. NOTE: While this document attempts to hide as much as possible the differences between the three forms of electronic signatures that have been defined in other ETSI documents, namely CAdES, PAdES and XAdES, the	No. It can also validate it after, assuming some conditions are met. If a reader thinks one can augment an algorithm to a signature, then we will have lost him a while earlier. Taken some of the text proposals with modification as helpful explanatory note.

					present description is indeed valid for CAdES and XAdES, but not necessarily for PAdES. With the PAdES format, it is possible to first capture the validation data required to validate the signature and then to apply one or more time-stamp tokens. The ultimate goal is the same: get a reference of time that can be used to check the revocation status of the certificates from the certification path and include within the electronic signature the validation data required to validate the signature.	
F 55.	Section 4.3.4.1 Page 26	The NOTE	Te	This NOTE does not clearly explain why long term validation is necessary. It is required to make sure that a signature checked as valid one day, will be still be checkable as valid by someone else long after, even if the validation data which has been used to check the signature as valid is no longer available on-line. It is proposed to remove this NOTE with a text using most of its content and which should be moved in the main body of the document.	Remove this NOTE and add the following text in the main body of the document: A signature with long term validation data includes the validation data that is necessary to verify the signature beyond the end of the validity of the signer's certificate, in particular to ascertain the revocation status of all end-entity certificates (signer certificate, time-stamping units certificates, attribute certificates ...) contained in the signature. There can be more elements than necessary and can also be fewer elements than necessary if it is expected that recipients have an alternate means of obtaining the missing elements.	Agree that the text of the note needs improvement. Taken the text but left as a note because it does not add any requirements.
F 56.	4.3.5. Page 27	New section 5.3	te	As indicated earlier, section 4.3.5 should be placed under a new section 5 called "5. Signature augmentation " and thus be renamed: 5.3 Augmentation of a Signature with Archival Data.	Rename section "4.3.5 Creation of a Signature With Archival Data" by "5.3 Augmentation of a Signature with Archival Data".	Rejected as above
F 57.	4.3.5.1 Page 27	New section 5.3.1 First sentence.	te	The text states: (...) the signed data, the *signature* as well as *any additional information* should be protected by applying time-	Change proposal for the first sentence: Before algorithms, keys, and other cryptographic data used at the time a signature was built become weak and the cryptographic functions become vulnerable,	Accepted with modifications.

				stamp tokens. Firstly, the wording "the signed data" should be changed into "the Signer's Document", which is clearly shown on Figure 9. Secondly, if the word "*signature*" in the above sentence means the box "Signature value" on Figure 9, then the protection is very weak. If the word "*signature*" in the above sentence means the box "Signature with long term validation data" on Figure 9, then the protection is much better, since both certificates and revocation information will be protected. Whatever, the current sentence is ambiguous and should be clarified. It is also rather obscure to say: "as well as any additional information" without other precision. Since the real intent of the editors is unknown, the text proposal on the right might not be what the editors had in mind.	or the certificates supporting previous time-stamp tokens expire or are revoked, the signer's document and the signature with long term validation data should be protected by applying one or more time-stamp tokens.	
F 58.	Section 4.3.5.1 Page 27	First sentence	Te	The text states: (...) the signed data, the signature as well as any additional information should be protected by applying time-stamp tokens. The description is not sufficient. Before applying a new time-stamp token, it must be demonstrated that the previous new time-stamp token was still	Add the following text immediately after the first sentence. Before applying a new time-stamp token, it must be demonstrated that the previous new time-stamp token was still valid at the time the new TST has been applied. It is thus necessary to capture the revocation status of all certificates used to build a certification path up to a trusted root to verify the TSU certificate(s) at the current time and to store that data within the electronic signature with long term	Idea accepted. Impementation different as suggested.

				valid at the time the new TST has been applied. This means that it is necessary to capture at least the revocation status of the TSU certificate at the current time and to store it within the electronic signature. The wording " as well as any additional information" might cover that case, but the reader may not discover it nor even think about it. More explanations are indeed needed.	validation data before applying the new time-stamp token. NOTE: In case of a detached signature, it is necessary to have access to the Signer's Document so that a new hash value can be computed over it. This will only be possible if the party attempting to build the Archival Data has an access both to the detached electronic signature and to the Signer's Document.	
F 59.	Section 4.3.5.1. Page 27	Second sentence.	Te	The text states: The time-stamping process should be repeated in time before the protection provided by a previous time-stamp token becomes weak and should make use of stronger algorithms or longer key lengths than have been used in the original signatures or time-stamp tokens. The problem with such a sentence and the current Figure 9 is that it is no understandable how the process can be repeated since a new block of validation data must be added every time a new TST is added. Figure 9 does not show this.	A new figure 10 should be added, so that it becomes understandable how the process can be repeated. Since there are already more than 50 comment for 27 pages it is not possible to provide text proposal for every comment. The explanations given for the rational should help to build the missing a text.	Accepted
F 60.	Section 4.3.5.3. Page 27	Table 4		The current description of the inputs parameters is too simplistic. There is only one input whereas there should be five inputs. The following four inputs to Table 4 are missing: - for the signer's document,	Add the following inputs to Table 4: - "Signer's document", - "Current time", - "Signature augmentation policy". - "Information about weak algorithms". For the signer's document, it shall be made	The document is part of the signature. Current time is assumed to be available. Information about weak algorithms does not make sense here. This is assumed to be part of the policy.

				- for a "signature augmentation policy", - for the "Current time", and - for "Information about weak algorithms". A signature augmentation policy should be used to know where from the time-stamping tokens should be obtained. Remember that section 4.2.5.1 states: The set of attributes included in a signature (...) is defined, when augmenting a signature, by the signature augmentation policy used and can also be format specific. If the current time is unknown, it is not possible to know whether the algorithms have become weak. In an algorithm becomes weak, additional information shall be captured /used in order to know this. That additional information should / may be stored within the electronic signature in case it is no more available on-line.	"conditional" with the following explanation in a foot note: If the signer's document is not included within the Signature with Long Term Validation Data, then it shall be provided as a separate input. The "current time" shall be made mandatory otherwise the process would not know whether the certificates supporting previous time-stamp tokens will soon expire. The two remaining inputs should be mentioned as optional, if and only if ... it is believed that an augmentation policy may not care about weak algorithms. See also the next comment.	
F 61.	Section 4.3.5.3. Page 27		Te	The text states: 4.3.5.3 Outputs The process for creating a Signature With Archival Data shall return the signature provided with an added unsigned attribute containing a time-stamp token on the signature. This is in contradiction with the current sentence placed above	Change into: 4.3.5.3 Outputs The process for augmenting a Signature with Archival Data shall return the electronic signature with Long Term Validation Data originally provided with modified and added unsigned attributes containing: a) revocation status information to demonstrate that the last applied time-stamp token was not revoked at the time the new time-stamp token was applied, and	Rejected, since the suggested changes are not accurate (tst cannot be revoked, TST also on revocation status info added). Text has been improved though.

				which states: "the signed data, the signature as well as any additional information should be protected by applying time-stamp tokens." The "signed data" (i.e. the "signer's document") is missing, since it may be only present in a detached electronic signature and hence not be placed inside the electronic signature that is given as an input to the process.	b) a new time-stamp token computed both on the signature with Long Term Validation Data and on the Signer's Document.	
F 62.	Section 4.3.5.4. Page 27		Te	The process is dependant upon the content of the signature augmentation policy which may care about all the threats previously mentioned or only some of them. Before the first sentence (*The signature augmentation process shall*) additional explanations should be given.	Additional text proposal: The process is dependant upon the content of the signature augmentation policy which shall always care about the weakness of the hash function used to originally hash the signer's document but may care either only about some of the threats previously mentioned or about all of them: - certificates supporting previous time-stamp tokens will soon expire, - certificates supporting previous time-stamp tokens might soon be revoked, - some cryptographic functions might soon be vulnerable, - some key sizes might be not long enough anymore according to the cryptographic functions that used them.	Rejected, since no requirements contained. Caring about the weakness is undefined. Also, we simply add a time stamp and don't really describe "caring" in the text.
F 63.	Section 4.3.5.4. Page 27	Item 2.	Te	The text states: 2. The time stamp token shall cover all data objects contained in the signature. This is in contradiction with the current sentence placed above which states: "the signed data, the signature as well as any additional	Text replacement proposal: 2. The time stamp token shall cover the "signer's document and all data objects contained in the signature.	accepted

				information should be protected by applying time-stamp tokens." The "signed data" (i.e. the "signer's document") is missing, since it may be only present in a detached electronic signature and hence not be placed inside the electronic signature that is given as an input to the process.		
F 64.	Section 5. Page 28	Section 5	ed	Since it has been proposed to add a new section 5, this section should now become section 6.	Change "5 Signature validation" into " "6 Signature validation".	Rejected as above
F 65.	Section 5.1.1. Page 28	2 nd paragraph;	Te	The text states: A signature validation application (SVA) receives *signed data* and other input from the driving application (DA). Since the wording "*signed data*" is not defined, this sentence is unclear. Should the reader understand that "*signed data*" is : 1) a signer's document that includes an electronic signature (e.g. PAdES) ? 2) an electronic signature that encapsulates the signer's document ? 3) a detached electronic signature and the signer's document ? 4) a detached electronic signature without the signer's document ? The reader is fully lost. In the case of PAdES, it is	Replace with: A signature validation application (SVA) receives the signer's document and/or an electronic signature or alternatively a hash value computed over the signer's document and an electronic signature as well as other inputs from the driving application (DA). and add other sections to specify the input and the output parameters. See also a related comment about Figure 10.	Accepted with modifications. Signed data is obviously not a good choice. This is introductory text that should not be made more complex to avoid losing the reader. The verification of the hash value is part of the crypto-building block.

				mandatory to provide the signer's document. It includes the electronic signature which means that the verification of the hash value computed over the signed portion of the pdf will be done by the SVA. But what about the other cases ? In which cases do we mandate the verification of the hash value over the signer's document ? By the DA, by the SVA ... or by nobody ? Whereas all the previous functions include a table with the inputs parameters and the output parameters, it can be noticed that this is no the case with this function. Why ? As a result, the reader may not know what is meant by "*signed data*" and where is the responsibility to check that the hash value computed over the signer's document. ENs need to be precise and cannot be ambiguous; ... (otherwise the document should be changed into an ETSI Technical Report. it is proposed to change the text so it can support the four cases mentioned above.		
F 66.	Section 5.1.1. Page 28		Te	The text states: • TOTAL_FAILED: All checks failed, or the cryptographic checks of the signature failed, (including checks of hashes of individual data objects that have been signed indirectly) or it is proved that the generation of	Replace with: • TOTAL_FAILED: when anyone of the checks that the signature validation policy prescribed has a permanent failure;	Rejected. TOTAL_FAILED is the contrary of the Union of TOTAL_PASSED and INDETERMINATE. It would indeed be lovely, if there was a way to describe "permanent failure".

				the signature was after the revocation of the signing certificate; or There is a failure as soon as one check failed and not when all checks failed. The definition is also far too long and incomplete. It is much simpler to define TOTAL_FAILED as the contrary of TOTAL_PASSED.		
F 67.	Section 5.1.1. Page 28	The NOTE	Te	The text states: NOTE: EN 319 102 Part 2 specifies a structure for a signature validation report. The reality is that it would mandate a structure, which is not acceptable.	Please delete the NOTE.	Rejected. The reality is that this document has not yet been written, Also, it does not mandate a structure but specifies one.
F 68.	Section 5.1.1. Page 29	Figure 10	Te	The Conceptual Model of Signature Validation includes an entry on the left called "signed document" that is as ambiguous as the previously mentioned sentence, i.e. *A signature validation application (SVA) receives signed data and other input from the driving application (DA).* What is the difference, if any, between "signed data" and "signed document" ? Why are two different terms being used ? The reader is lost. Four cases, should be supported: 1) a signer's document that includes an electronic signature (e.g. PAdES), 2) an electronic signature that	The entry on the left called "Signed Document" should be renamed: "Signer's document and/or an electronic signature OR a hash of the signer's document and an electronic signature ".	Figure updated

				encapsulates the signer's document, 3) a detached electronic signature and the signer's document, 4) a detached electronic signature without the signer's document. The following is being proposed. The entry on the left called "Signed Document" should be renamed. " Signer's document and/or an electronic signature OR a hash of the signer's document and an electronic signature". In addition some more details should be provided in the text.		
F 69.	Section 5.1.1. Page 29	Figure 10	Te	Why is the signature validation policy not represented on the Figure ? What is the difference if any between "validation constraints" and a "validation policy" ? The reader is lost.	Please add "Validation policy" on Figure 10.	Accepted.
F 70.	Section 5.1.1. Page 29	First sentence	Te	The text states: The present document does not stipulate any required behaviour by the DA, especially no processing requirements for any of the returned information, since this is application specific and out of the scope of the present document. As explained above, four cases, should be supported: 1) a signer's document that	Change into: The DA is able to request to the SVA the validation of : a) a detached electronic signature, or of b) an enveloped electronic signature, or of c) an enveloping electronic signature. In the case of a detached electronic signature, besides this electronic signature, the DA shall either provide the signer's document or an appropriate hash value computed over the signer's document. In the case of an enveloped electronic	Reject the idea of stipulating requirements for the DA. For Validation the DA does not have to calculate any hashes. It has to provide a hash value, wherever it comes from.

				includes an electronic signature (e.g. PAdES), 2) an electronic signature that encapsulates the signer's document, 3) a detached electronic signature and the signer's document, 4) a detached electronic signature without the signer's document. In the last case, the SVA shall receive a hash value computed by the DA, which means that the DA is indeed involved. .. which comes into contradiction with the current sentence. The current sentence needs to be corrected. It only applies to the processing of the returned information. More details are provided about the requirements applicable to the input parameters.	signature, the DA shall provide the signer's document. In the case of an enveloping electronic signature, the DA shall provide the electronic signature. The present document does not stipulate any required behaviour by the DA for the processing for any of the returned information, since this is application specific and out of the scope of the present document.	
F 71.	Section 5.1.1. Page 29	NOTE 3:	Te	Be careful, on that page there are two notes numbered: NOTE 3. This comment is about the first one. Note 3 is rather controversial since the claimed signing time is an indication that may be returned to the DA by the SVA, if present, but that is never checked by the SVA. The DA may check it, but this is out of the scope off this document.	Please delete NOTE 3.	Rejected. Note is an example only.
F 72.	Section 5.1.2. Page 30	First bullet	Te	The text states: This process may be selected	See the next comment, to see how to solve this issue.	See the next comment

				for signatures where : o the time of validation lies within the validity period of the signing certificate and the signing certificate has not been revoked; or The goal of an SVA is to subcontract the difficulty of a signature validation to the SVA. which means that the DA does not need to check whether the signing certificate has been revoked or not, nor whether it is within its validity period. Digging the signers certificate within a signed PDF document is far from easy for a DA. The process can be selected at any time, however TOTAL_FAILED will be returned if the time of validation does not lie within the validity period of the signing certificate or if the signer's certificate has been revoked.		
F 73.	Section 5.1.2. Page 30	First bullet	Te	The text states: This process may be selected for signatures where : o (...) or o the time of validation lies beyond the validity period of the signing certificate when the certification authority provides revocation information for expired certificates. The goal of an SVA is to subcontract the difficulty of a signature validation to the SVA. which means that the DA does not know whether the certification	It is thus proposed to fully delete the following text: "This process may be selected for signatures where : o the time of validation lies within the validity period of the signing certificate and the signing certificate has not been revoked; or o the time of validation lies beyond the validity period of the signing certificate when the certification authority provides revocation information for expired certificates."	Rejected. We added a paragraph making clear that this is a question of policy. It is not true that one can never accept a signature where the certificate has expired but no time stamp or other PoE exists.

				authority provides revocation information for expired certificates. This sentence does not make sense for the SVA either. If the time of validation lies beyond the validity period, it should be remembered that some certification authority may provide revocation information for expired certificates, but the revocation status is the one captured at the end of the validity period of that certificate. So if the key private is really compromised after the end of the validity of the certificate, this will NOT be reported by the CA. As a consequence an attacker could present a forged signature made after the expiry of the certificate and which would be accepted as valid !!! It is not possible to keep this sentence.		
F 74.	Section 5.1.2. Page 30	First bullet	Te	The text states: "When supporting only validation of Basic Signatures, the SVA shall support the Validation Process for Basic Signatures (clause 5.3). (...) This may be done irrespective of the class of signature present: Basic Signatures, Signatures with Time, Signatures with Long Term Validation Data and Signatures with Archival Data. Any additional material present in attributes may be ignored." This is contradictory.	It is suspected, but not sure, that the editors wanted to say: "When supporting only validation of Basic Signatures, the SVA shall support the Validation Process for Basic Signatures (clause 5.3). (...) This may be done irrespective of the type of electronic signature presented: a detached electronic signature, an enveloped electronic signature or an enveloping electronic signature".	No. The change to “class of signature presented” is accepted. The rest is as intended since one may be able to validate a Signature with Archival data, e.g., using basic signature validation, ignoring all unneeded unsigned attributes. Signature Classes have been defined in section 4.3

				it is suspected that the editors introduced a voluntary error to know how many people read the document.		
F 75.	Section 5.1.2. Page 30	Second bullet	Te	The text states: When supporting validation for Basic Signatures and Signatures with Time, the SVA shall support the Validation Process for Signatures with Time (see clause 5.5). This is true, but not sufficient.	Add the following sentence. This means that the SVA shall support validation for Basic Signatures (see section 6.3), augmentation of signature with time (see section 5.1) and validation for Signatures with Time (see section 6.5)	Accepted with changes. Validation for Signatures with Time requires basic sign.val. anyhow, so would not need to be listed separately, but agreed it makes it clearer. Augmentation however cannot be required.
F 76.	Section 5.1.2. Page 30	Third bullet	Te	The text states: • When supporting validation for Basic Signatures, Signatures with Time, Signatures with Long Term Validation and/or Signatures with Archival Data, the SVA shall support the Validation process for Signatures with Long-Term Validation Data and Signatures with Archival Data (see clause 5.6). It is not acceptable to mandate to support Signatures with Archival Data as soon as Signatures with Long-Term Validation Data is supported. Signatures with Archival Data is useful in practice in two cases: - the hash function initially used to hash the signer's document becomes weak. This might happen about 10 years after the signature creation and many documents are destroyed or not used anymore 10 years after they were signed.	This bullet should be split into two parts: • When supporting validation for Basic Signatures, Signatures with Time, Signatures with Long Term, the SVA shall support the Validation process for Signatures with Long-Term Validation Data (see clause X.Y). • When supporting validation for with Long Term Validation and Signatures with Archival Data, the SVA shall support the Validation process for Signatures with Archival Data (see clause X.Z).	rejected, but modifications were required. Signature with Long-Term-Validation-Data can be validated by the Signature-With-Time algorithm.

				- the certificate of the TSU has expired. Most certificates last 5 or 6 years and many documents are destroyed or not used anymore 5 years after they were signed This means that Signatures with Archival Data are usually not needed for documents that have a time life less than 5 years. Mandating to support this format when documents are useful, for example, during 3 years only, would not be reasonable.		
F 77.	Section 5.1.2. Page 30		te	The text states: When validating an instance of a signature, the SVA should select the process best suited for that signature. Whenever the DA specifies the process to be used, the SVA shall select that process. These two sentences seem to be contradictory and placed in the wrong order. It is believed that the SVA is a slave application and that the DA is the master application. A slave obeys to the master, hence the master shall always indicate to the slave what to do and the slave shall have no initiative.	Replace with: When validating an instance of a signature, the SVA shall select the process best suited for that signature. Whenever the DA specifies the process to be used, the SVA use that process.	Rejected. First, there is not much difference, and also there is a contradiction since the SVA cannot select the best suited process if the DA decides otherwise.
F 78.	Section 5.1.2. Page 30		Te	The text states: "Whenever the SVA has no indication which class the signature to be validated belongs to, the SVA should select the process to use as follows: • If the SVA supports the	Delete all this text.	Rejected. Who talks about augmentation here? Nobody. We just describe where to start when starting blindly.

				Validation process for Signatures with Long-Term Validation Data and Signatures with Archival Data, it should select that process; • Otherwise: If the SVA supports the Validation Process for Signatures with Time, it should select that process; • Otherwise, the SVA shall select Validation Process for Basic Signatures". This approach is not acceptable. Signature augmentation may be done by the SVA, but also by a third party. It does not need to be necessarily done by the SVA. The format Signatures with Archival Data is rather "heavy", but the manufacturers of storage equipments would certainly be very supportive of such an approach ! The DA shall inform the DA which process he would like to be executed when validating an electronic signature and hence which format he would like to receive back.		
F 79.	Section 5.1.3. Page 30		Te	The text states: This clause specifies <u>minimum</u> requirements for the content of such a report. The minimum requirements are : a major status and a secondary status. Everything else is "recommended".	Change into : This clause specifies <u>recommended</u> requirements for the content of such a report.	Rejected. What are “recommended requirements” within a standard?
F 80.	Section 5.1.3.		ed	The text states:	Change Table 2 into Table 5	Fixed.

	Page 30			Table 2 lists the possible values of the main status indication and their semantics; Change Table 2 into Table 5, since Table 2 is : Inputs to the creation process for Signatures with Time.		
F 81.	Section 5.1.3. Page 30		Te	The text states: In all cases, the signature validation process shall output • a status indication of the results of the signature validation process. Table 2 lists the possible values of the main status indication and their semantics; • an indication of the policy or set of constraints against which the signature has been validated; • the date and time for which the validation status was determined; and • additional validation report data as specified in Table 5 and Table 6, The minimum requirements are: a major status and a secondary status which should remain specific to every implementation. Everything else should only be "recommended". In the optional output, the set of constraints against which the signature has been validated is so complex that even an expert engineer may be lost. This is why a signature validation policy is being used. Such signature	Change into: In all cases, the signature validation process shall output • a major status indication of the results of the signature validation process. Table 5 lists the possible values of the main status indication and their semantics; • a secondary status indication of the results of the signature validation process. This secondary status shall be specific to every implementation. When the major status indication is TOTAL-PASSED, the signature validation process should also output: • a copy of the input parameters (except the electronic signature and/or the signed document); • the date and time for which the validation status was determined; and • an additional validation report data as specified in Table 6, When the major status indication is TOTAL-FAILED or INDETERMINATE, the signature validation process should also output information allowing to understand with more precision the reason of the secondary status.	Rejected. We made clear that an indication of the set of constraints is sufficient. If no policy is being used, some indication of the rules the signature was checked against is helpful for the DA.

				validation policy may be quite complex and should be expressed using a formal language.		
F 82.	Section 5.1.3. Page 31		Te	The text states: • When the result is TOTAL-PASSED or TOTAL-FAILED: a) Any execution of a SVA with the same inputs shall return TOTAL-PASSED or TOTAL-FAILED, respectively. b) Any execution of a SVA with the same inputs and additional validation data (e.g. more certificates) shall return the same result as it has returned in a) (i.e. TOTAL-PASSED or TOTAL-FAILED). This is quite strange. There is certainly an hidden idea for putting such a sentence which is not explained. Suppose some attacker filters some accesses and prevents the SVA to fetch all the certificates that have been generated, then a certification path cannot be constructed. The end result is TOTAL-FAILED. Another retry is done one day after when the attacker is no more present then a certification path can be constructed and the end result is TOTAL-PASSED. Item b) would exhibit a problem. Note also that in addition to the inputs, the SAV is free to fetch, request any information. If the information received is not the same the result may change.	The text should be deleted.	Rejected. The attack does not work since the algorithm will return INDETERMINATE. The assumption here is that the SVA does not fetch anything – and if it does, one would need to consider it as INPUT.

				This text is very dangerous and should be deleted.		
F 83.	Section 5.1.3. Page 31		Te	The text states: When the result is INDETERMINATE: a) Any execution of a SVA with the same inputs shall return INDETERMINATE. b) Any execution of a SVA with the same inputs and additional validation data shall return TOTAL-PASSED, TOTAL-FAILED or INDETERMINATE. Item a) is incorrect. The status INDETERMINATE is mainly used to handle the case of a certificate suspension. If a certificate is suspended, it cannot be said that the end result is TOTAL-PASSED nor TOTAL-FAILED, hence why it is aid to be INDETERMINATE. But since a suspension state is not for ever, at the end of the suspension period the status will necessarily change to TOTAL-PASSED or TOTAL-FAILED (if the revocation information is accessible from the SVA). Saying that "Any execution of a SVA with the same inputs shall return INDETERMINATE" is wrong.	Change text into: When the result is INDETERMINATE any other execution of a SVA for the same electronic signature may return TOTAL-PASSED, TOTAL-FAILED or INDETERMINATE. Sub-indications may help to understand whether a retry at a later time might return a result different from INDETERMINATE.	Rejected. “The status INDETERMINATE is mainly used to handle the case of a certificate suspension.” Is very untrue
F 84.	Section 5.1.3. Page 31		Te	The text states: In the case of a TOTAL-FAILED or INDETERMINATE validation result, an SVA should provide validation results for as many validation	Change into: In the case of a TOTAL-FAILED validation result, an SVA should stop the validation after the first fatal error that has been encountered and shall provide a secondary status able to identify the first error	Accepted with modification

				constraints as possible, as long as processing is possible and the results of the processing are meaningful. Most implementations make a stop on the first error encountered. Since implementers do not perform the checks in the same order, if an electronic signature has several problems, only the first one will be reported. Continuing the tests, most often, show errors which are the consequences of the first error. So there could be an accumulation of errors. A SVA should not be confused with an application attempting to make an exhaustive report of all the failures, but this is exactly what the current text intends to do !!!	encountered. In the case of an INDETERMINATE validation result, an SVA should provide a secondary status able to identify the first error encountered.	
F 85.	Section 5.1.3. Page 31	Note 2	Te	The text states: NOTE 2: The date/time at which the SVA is executed is an implicit input to the validation process. Running the SVA at a later point in time can give different results in case additional data becomes available (e.g. new certificate status information). This is to vague and slightly misleading. As soon as a Time-stamp token has been applied hence a Signature with Time is being used, if a signature has been checked as valid, it will continue to be checked as valid until the end of the validity period of the signer's certificate.	It is proposed either to delete the Note or to change it into : NOTE 2: If a signature with a Basic Signature format has been checked as valid, running the SVA at a later point in time can give different results in case different revocation certificate status information becomes available. If a signature with a Signature with Time format has been checked as valid, it will continue to be checked as valid until the end of the validity period of the signer's certificate. If a signature with a Signature with Long-term validation Data has been checked as valid, it will continue to be checked as valid until the end of the validity period of the TSU's certificate (unless some crypto happens to be broken).	Rejected. This NOTE is only to explain that the rule “same input” → “same result” needs to understand that “time” is an input.

				As soon as a Signature with Long-term validation Data has been obtained, if this signature has been checked as valid, it will continue to be checked as valid until the end of the validity period of the TSU's certificate (unless some crypto happens to be broken). So saying that "*Running the SVA at a later point in time can give different results in case additional data becomes available (e.g. new certificate status information)*" is misleading since in the above cases, the result remains stable. It is also very curious to have so many notes here and there, which come out of the blue and which are most often wrong or misleading.		
F 86.	Section 5.1.3. Page 31	Note 3	Te	The text states: NOTE 3: The term "same inputs" includes the validation constraints to be used. Different validation constraints will in general result in different validation results. Why is this note really useful ? Validation constraints are usually not used at the level of the SVA interface, but a reference to a signature validation policy which is much simpler. It is nevertheless rather difficult o interpret.	Please delete Note 3.	Rejected. Tried to make Note clearer.
F 87.	Section 5.1.3.	Table 5	Te	The text states in the column called : Associated Validation	Replace with: The validation process shall extract all the	Accepted with modification. It does not make sense to

	Page 31			report data in conjunction with line TOTAL-PASSED: The validation process shall output the validated certificate chain, including the signing certificate, used in the validation process. In addition, the validation process may provide the result of the validation for each of the validation constraints. It does not make sense to mandate to include this information unless it is requested by the DA. What should be mandated and which is NOT indicated in the current text, is the extraction of all the signed attributes, if present, such as: the claimed signing time, the claimed location, a commitment type, a claimed role, a certified role and of any particular extension in the signer's certificate like : the fact that it is a claimed to be a qualified certificate and that a Secure creation device is being used to carry the private key and the certificate.	signed attributes present in the electronic signature, such as: the claimed signing time, the claimed location, a commitment type, a claimed role or a certified role and shall also identify the signer by producing a unique identifier composed of a sequence of Distinguished Names (DNs) up to (and including) the Distinguished Name of a trust anchor recognized under the signature validation policy. It shall also indicate any particular extension in the signer's certificate like the fact that it is a claimed to be a Qualified Certificate and that a Secure creation device is being used to carry the private key and the certificate. It may also, if requested by the DA, output the validated certificate chain, including the signing certificate, used in the validation process.	mandate to extract this information unless it is requested by the DA.
F 88.	Section 5.1.3. Page 31 and 32	Table 5	Te	The text states in the column called : Associated Validation report data in conjunction with line TOTAL-FAILED: The validation process shall output additional information to explain the TOTAL-FAILED indication for each of the validation constraints that have been taken into account and for which a negative result occurred.	Replace with: After the major and the secondary status indication of the results, the validation process shall output additional information to explain the TOTAL-FAILED indication for the first error encountered.	Rejected, It is realistic to include all results for all constraints that have been checked. If the process terminates after a single check, fine.

				As explained earlier, providing an indication for each of the validation constraints that have been taken into account and for which a negative result occurred is not realistic. Only the first error encountered should be taken into consideration.		
F 89.	Section 5.1.3. Page 32		Te	The text states in the column called : Associated Validation report data in conjunction with line INDETERMINATE: The validation process shall output additional information to explain the INDETERMINATE indication and to help the verifier to identify what data is missing to complete the validation process. In particular it shall provide validation result indications for at least those validation constraints that have been taken into account and for which an indeterminate result occurred. As explained earlier, a SVA is not a debugging application. Only the first error encountered should be taken into consideration.	Replace with: After the major and the secondary status indication of the results, the validation process shall output additional information to explain the INDETERMINATE indication for the first error encountered.	IF there is more than one check resulting in INDETERMINATE done, the SVA will be able to return multiple reasons. If the SVA stops after the first one, only one needs to be returned anyhow
F 90.	Section 5.1.3. Page 32	Table 6	Te	The text states: "The validation report data associated to the TOTAL-FAILED and INDETERMINATE indications status resulting from the validation of an AdES signature should be structured as in Table 6 by	Delete the quoted sentence from the main body of the document and move Table 6 into a new informative annex, called: Signature Validation Failure Report Structure (Informative annex) The first sentence should be modified in the following way: The validation report data associated to the	Made sub-indications normative.

				listing the main sub codes to be returned by the validation process. These sub-indications are not normative". Since the sub-indications are not normative, this table should be moved into an informative annex.	TOTAL-FAILED and INDETERMINATE indications status resulting from the validation of an AdES signature may include some sub-indications structured as in Table 6. Sub-indications may be used to complement the secondary status indication of the results of the signature validation process. The list of these sub-indications is not limited to the sub-indications indicated hereafter.	
F 91.	Section 5.1.3. Page 32	Table 6	Te	Since Table 6 should be moved into an informative annex, all the "shall" contained in Table 6 should be changed into "should".	All the 'shall' contained in Table 6 should be changed into "should".	See Comment 90
F 92.	Section 5.1.3. Page 32		Te	The text mentions two sub-indications: HASH_FAILURE SIG_CRYPTO_FAILURE In most formats (PAdES, CAdES and XAdES), it is impossible to make a difference between these two cases.	Reconsider these two cases and melt them in one case.	Rejected. In these cases SIG_CRYPTO_FAILURE will be returned.
F 93.	Section 5.1.3. Page 32	Table 6	Te	The text mentions the sub-indication: REVOKED The text states: The signature validation process results into TOTAL-FAILED because: • The signing certificate has been revoked and • The signing time lies after the revocation time The second bullet should be deleted, since the signing time is always unknown.	Delete the second bullet, since the first bullet is sufficient.	Rejected. The second bullet changed to • There is no PoE available that the signing time lies before the revocation time.

F 94.	Section 5.1.3. Pages 32 and 33	Table 6	Te	The text mentions the main indication: INDETERMINATE Many of the sub-indications related to INDETERMINATE are inappropriate and should be moved to the main indication TOTAL-FAILED. Once again INDETERMINATE is a case that has been planned to address the case of certificate suspension, with in mind, if you test again later, the result might change and in fine it WILL change either to TOTAL-PASS or to TOTAL_FAILURE, but will NEVER stay for ever as INDETERMINATE, as long as an access to the revocation information is accessible. A few additional comments: 1° REVOKED_NO_POE The signature validation process results into INDETERMINATE because the signing certificate was revoked at the validation date/time. The acronym REVOKED_NO_POE is meaningless. NO_POE is not explained and does not make sense. The grace period has been introduced and if there is one it should be applied if there is none the comparison is done strictly. So that case does not exist and should be removed. **It is quite "curious" that the concept of "grace period" does**	The following sub-indications should be moved to the main indication: TOTAL-FAILED. SIG_CONSTRAINTS_ FAILURE The signature validation process results into TOTAL-FAILED because one or more attributes of the signature do not match the validation constraints. CHAIN_CONSTRAINTS_FAILURE The signature validation process results into TOTAL-FAILED because the certificate chain used in the validation process does not match the validation constraints related to the certificate. CERTIFICATE_CHAIN_GENERAL_FAILURE The signature validation process results into TOTAL-FAILED because he set of certificates available for chain validation produced an error for an unspecified reason. EXPIRED The signature validation process results into TOTAL-FAILED because either the electronic signature includes a TST which date is after the expiration date (notAfter) of the signing certificate or in no TST is present, the current time lies after the expiration date (notAfter) of the signing certificate. NOT_YET_VALID The signature validation process results into TOTAL-FAILED because the signing time lies before the issuance date (notBefore) of the signing certificate. FORMAT_FAILURE The signature validation process results into TOTAL-FAILED because the signature is not conformant to one of the base standards. TIMESTAMP_ORDER_FAILURE	Rejected INDETERMINATE is not only for suspension.

				not appear anymore in the whole document. Have the editors of the document considered at any point of time the principle of "backwards compatibility" ? 2° *OUT_OF_BOUNDS_NO_POE* comes in part in duplication of NOT_YET_VALID 3 ° *CRYPTO_CONSTRAINTS_FAILURE_NO_POE* comes in part in duplication of *CRYPTO_CONSTRAINTS_FAILURE.* 4° *TRY_LATER* it is indeed a sub-indication fitting well under the main indication INDETERMINATE. However, *the text is too vague: "*not all constraints can be fulfilled". Change into: *TRY_LATER* The signature validation process results into *INDETERMINATE* because the revocation status of some certificates in the certification path are indicated as being suspended. However, it may be possible to check again using additional revocation information that will be available at a later point of time. 5° *SIGNED_DATA_NOT_FOUND* Either the signed data is included in the AdES, or provided separately or a hash of it is provided. The signed data must be provided or referenced for XAdES.	The signature validation process results into TOTAL-FAILED because some constraints on the order of signature time-stamps and/or signed data object(s) time-stamps are not respected. NO_SIGNING_CERTIFICATE_FOUND The signature validation process results into TOTAL-FAILED because the signing certificate cannot be identified. NO_CERTIFICATE_CHAIN_FOUND The signature validation process results into TOTAL-FAILED because no certificate chain has been found for the identified signing certificate. REVOKED_CA The signature validation process results into TOTAL-FAILED because at least one certificate chain was found but an intermediate CA certificate is revoked. *OUT_OF_BOUNDS_NO_POE* The signature validation process results into TOTAL-FAILED because the signing certificate is expired or not yet valid at the validation date. *NO_POE* The signature validation process results into TOTAL-FAILED because a proof of existence is missing to ascertain that a signed object has been produced before some compromising event (e.g. broken algorithm). *SIGNED_DATA_NOT_FOUND* Either the signed data which should be included in the AdES in missing, or the signed data has not been provided separately or a hash of it has not been provided or the reference where the signed data was supposed to be located does not contain it. . The signature validation process results into TOTAL-FAILED because the signed data could not be obtained.	

					See also the next comment.	
F 95.	Section 5.1.3. Page 34	Table 6	Te	A "star attraction" is the next sub-indication placed under the indication INDETERMINATE. *GENERIC* The signature validation process results into *INDETERMINATE* because of any other reason. This may be interpreted as INDETERMINATE is the main result for any other reason not indicated in this list. After attempting to correct Table 6 , it seems much better to delete it in full, even in an informative annex.	Remove Table 6 in full, even in an informative Annex.	Rejected. While GENERIC is certainly “strange”, can we be sure to have covered all reasons?
F 96.	Section 5.1.3. Page 35	3 rd paragraph	Te	The text states: In such cases, the SVA should return, in its final report to the DA, the list of checks that were disabled due to the policy. This should be removed. An SVA is not a debugging application.	Delete the sentence.	Rejected. It is “should”, not “shall”.
F 97.	Section 5.1.3. Page 35	Note 3	Te	The text states: NOTE 2: The verifier can consider additional constraints that are not mentioned in the present document. It is not foreseeable, which constraints a DA will impose on the SVA. It is assumed that an implementation handles all constraints properly. In order to make signature	Please delete the NOTE.	Rejected. Tried to improve Note

				validation easy for a DA, the concept of a signature validation policy has been introduced, so that it is sufficient for the DA to identify the right signature validation policy and to provide to the SVA a reference to it. So speaking of additional constraints that are not mentioned in the present document is more relative to a debugging application which should not be considered or otherwise should be mentioned separately in an informative annex. The text in the main body of the document would then become much more readable, since here and there, there are NOTES which do not ease to understand the text.		
F 98.	Section 5.1.3. Page 35	Text above section 5.2;	Te	Another "**star attraction**": The set of validation constraints used for validation may force the SVA not to check a constraint that, when checked, would, according to the present document, lead to an *INDETERMINATE* result. The SVA shall report such cases in the validation report. Who is able to understand this ? The example which follows is even worse. The goal of signature validation is to make sure that the signature was valid, ALWAYS taking into consideration the revocation status of the certificates.	Please delete the quote text and the following example.	The goal of signature validation is of course to make sure the signature was valid. However, a policy may still allow to accept expired or revoked certificates even without –T.

F 99.	Section 5.2. Page 36	Figure 11	Te	Figure 11 suffers from similar problems like Figure 10. Figure 10 has one major input: the Signed Document. Figure 11 has one major input: the Signature. Isn't it something wrong ? When an XML document is being provided, a pointer to one of the electronic signatures contained in the XML document also needs to be provided. The same applies to a PDF document. When a PDF document is being provided, a pointer to one of the electronic signatures contained in the PDF document also needs to be provided.	The entry on the left called "Signature" should be renamed: "Signer's document and/or an electronic signature OR a hash of the signer's document and an electronic signature". It is also suggested to add another entry for a "pointer to an electronic signature" when either the electronic signature or the signer's document contains more than one electronic signature. This will allow to identify which electronic signature should be validated.	Figure adapted
F 100.	Section 5.2.2.2 Page 36	Table 7	Te	Taking into consideration the previous comment, the entry should be changed from: Signature into: Signer's document and/or an electronic signature OR a hash of the signer's document and an electronic signature. There should be another optional entry for the pointer to an electronic signature when either the electronic signature or the signer's document contains more than one electronic signature. This will allow to identify which electronic signature format should be validated.	Change the entry in Table 7 from the entry should be changed from: Signature into: Signer's document and/or an electronic signature OR a hash of the signer's document and an electronic signature; Add another optional entry for the "pointer to an electronic signature" when either the electronic signature or the signer's document contains more than one electronic signature. Add explanations.	Accepted with modifications

F 101.	Section 5.2.2.2 Page 36		Te	Since the first building block is the "format checking building block" what kind of checks should be done on the signer's document when the signature is not contained in the signer's document ? The present document is fully silent about that case. Shouldn't there be two different building blocks ?	Consider another building block about what kind of checks should/may be done on the signer's document when electronic signatures are not contained inside the signer's document. In particular, whether the document is in a stable format, e.g. a PDF/A document.	The SVA is agnostic about signer's documents.
F 102.	Section 5.2.3.3 Page 37		Te	Another "**star attraction**": In case the signing certificate cannot be identified, the output shall be the indication INDETERMINATE and the sub-indication NO_SIGNING_ CERTIFICATE_FOUND. The text on page 32 said: These sub-indications are not normative. Thus the use of the word "shall" is this inadequate, otherwise the use of such sub-indication would become mandatory. .. but in that case, the result should not be INDETERMINATE but TOTAL_FAILURE.		subindications made normative. Rest rejected.
F 103.	Section 5.2.3.3 Page 37		Te	Another "**star attraction**": The text states: NOTE: If the signature creation process has been compliant with the present document, the process will only return *INDETERMINATE* in the case of unavailability of an external resource pointed to by the signature reference.	Delete the NOTE.	Fixed Note.

				This is simply wrong, since somebody could modify the bit string while being transferred. Why again, here and there, so many Notes ?		
F 104.	Section 5.2.3.4 Page 37		Te	**Yet another** "**star attraction**": The text states: If no certificate can be retrieved, the building block shall return the indication *INDETERMINATE* and the sub-indication *NO_SIGNING_CERTIFICATE_FOUND* The text on page 32 said: These sub-indications are not normative. Thus the use of the word "shall" is this inadequate, otherwise the use of such sub-indication would become mandatory. .. but in that case, the result should not be INDETERMINATE but TOTAL_FAILURE.	Delete the sentence The proposed algorithms seem wishing to return as much as possible INDETERMINATE rater than TOTAL_PASSED or TOTAL_FAILURE.	subindications made normative.
F 105.	Section 5.2.3.4 Page 37		Ge	Final comment Only 36 pages have been reviewed and up to that point there are more than 100 comments. About one full week of work has been spent on that document. Since there are 69 pages, it is likely that about another set of 100 comments would be added. The editing committee and the TC ESI chairman should consider that it is not possible to spend more time.		Left uncommented.

				It is proposed to forward the document to another team of editors, so that it can be reviewed in depth and reconstructed in depth. A new version of this document should be re-submitted for public review. A disposition of comments would nevertheless be appreciated in a short time frame.		

G

Organization name	**Clause/ Subclause**	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change**	**RESOLUTION** on each comment submitted
G	5.1.3	Table 6 Validation Report Structure	Technical	HASH_FAILUE column on Associated Validation report data currently states "The validation process shall provide: • An identifier (s) (e.g. an URI or OID) uniquely identifying the signed data object that caused the failure." It is unclear what OIDs / URI this refers to. 4.2.10 identifies elements which together "compose" the signed data object (SDO). The	Replace bullet item with "An identifier (s) (e.g. an URI or OID) uniquely identifying the element within the signed data object (such as the signature attributes, DTBSR or SD see 4.2.10) that caused the failure." Or provide other clarification as to what the OID/URL refers to.	accepted with modifications; agree to add the examples, disagree with the reference since this might also be the case when an "indirect" hash breaks – like in a manifest or XML-reference.

Organization name	**Clause/ Subclause**	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change**	**RESOLUTION** on each comment submitted
				overall signed data itself may not necessarily have identifiers and the SDO can be a single hash derived from multiple other hashes for the elements within the SDO.		
	3.1, 4.2.2 & 5.1.4	Signature creation & validation constraints	T	In general the use of term signature creation and validation constraints is very fuzzy in this document and there no indication that such constraints may defined in term of signature policy constraints as defined in TS 119 172-1 even though this document is listed in the normative references (without any other mention in the document). These constraints are an essential element of validation (and to a lesser extent creation) and without further clarity this document cannot be implemented!	Several, see following lines	
	2				Clause 2 Move reference ETSI TS 119 172-1 from normative to informative reference	Rejected
	3.1				Replace existing “(Signature) Constraints” definition as definitions of validation constraints.	Accepted
	3.1				Create new definition of (Signature) Creation along the lines of (Signature) Validation constraints	Accepted

Organization name	**Clause/ Subclause**	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change**	**RESOLUTION** on each comment submitted
	5.5				Replace this one occurrence of Signature constraints with Validation Constraints	Accepted
	4.2.2				Replace: using a formal policy specification, e.g. a (machine processable) signature creation policy By using a formal policy which should be as specified in TS 119 172-1 or machine processable equivalents. ACCEPTED	Accepted
	4.2.2				The following constraints shall be supported: • Cryptographic constraints as defined in ??? (Comment note: if ESI agrees that there are to be no constraints then this can be removed. Or additional mandatory constraints may be added. The definition of each constraint needs to be referenced.)	rejected
	5.1.4				Replace: • using a formal policy specification, e.g. a (machine processable) signature creation policy By • using a formal policy which should be as specified in TS 119 172-1 or machine processable equivalents.	Accepted

Organization name	**Clause/ Subclause**	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change**	**RESOLUTION** on each comment submitted
	5.1.4				The following constraints shall be supported: • chain constr*aints*, as defined in ??? [see comment below], • cryptographic constraints as defined in ???? [see comment below] • signature elements constraints as defined in ??? [see comment below], Where other constraints are implemented their meaning shall be explicitly documented for an implementation either directly or indirectly by reference to a standard or publically available specification. (Comment note: these constraints are used in 5.2.4 and so need to be defined.)	Accepted with modifications
	5.1.4.x		T		a) Put current 5.1.4 text under new sub-heading; 5.1.4.1 General Requirements b) Add new section 5.1.4.2 chain constraints [copy text from 119 172-1 A.4.2.1 table 6 row m common terms needs to be used across both document. 119 172-1 should reference 319 102 for this definition.] c) Add new section 5.1.4.3	Accepted with modification by referencing 119 172-1

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted
					cryptographic [suite] constraints [copy text from 119 172-1 A.4.2.1 table 6 row p common terms needs to be used across both document. 119 172-1 should reference 319 102 for this definition.] d) Add new section 5.1.4.4 signature elements constraints [copy text from 119 172-1 A.4.2.1 table 6 row b common terms needs to be used across both document. 119 172-1 should reference 319 102 for this definition. This could possibly be simplified here to just presence. What about unsigned properties here and in 119 172.]	