Disposition of Comments for Draft ETSI EN 319 102 v0.2.1 – 31 may 2014

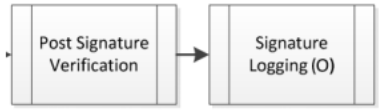
Electronic Signatures and Infrastructures (ESI); Procedures for Signature Creation and Validation

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

Nr.	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	OBSERVATIONS on each comment submitted
1.			General	The two main topics, i.e. Signature creation and Signature validation, are not correctly covered. Signature creation includes sections which relate to signature validation. This part has been fully corrected. However, it is unfortunately not the case of the second part on signature validation. The section on Signature validation attempts to "reinvent the wheel" and thus does not reuse the text and the concepts from CWA 14171:2001. While it has been possible to provide detailed text changes for the whole section 4 related to signature creation, providing the same level of changes for signature validation (section 5) has not been possible, despite the enormous amount of time that has been spent (more than 20 hours), since the current state of section 5 was too far away of what would be needed. Nevertheless, important efforts and a large amount of time have been spent to attempt to correct some parts of it.	Please revise the document according to the 80 detailed comments provided in the next 40 pages. It is strongly recommended to read all the comments before attempting to write a Disposition of Comments (DoC), since a lot of comments are interrelated. The STF should first take the time to read CWA 14171:2001. For the section on signature validation, it would be better and faster to rewrite the document from scratch using the material from the CWA 14171:2001 rather than trying to correct the current draft. The draft should be sent back to the STF, but more important **represented later on for a new set of public comments**. Note: the "CAdES keeper" should pay attention to the very last comment which raises a question.	The section on signature creation will be been completely rewritten in the next version of the draft. The section on validation will be improved, a complete rewrite is rejected since the STF is convinced that the approach taken is the correct approach.
2.	Scope	1	Technical	The text states: "The present document specifies procedures for: - Creating (Advanced) electronic signatures in a technology-agnostic way. (...) It is based on the use of public key cryptography to produce such signatures, which are supported by public key certificates. This is contradictory".	Replace with: "The present document specifies procedures for: Creating (Advanced) electronic signatures based on the use of public key cryptography to produce such signatures, which are supported by public key certificates. It introduces general principles, objects and functions relevant when creating signatures based on signature creation constraints and defines general forms of advanced electronic signatures that allow verifiability over long periods".	Accepted
3.	Scope	1	Technical	The text states: "Clause 1 introduces the lifecycle of an electronic signature and different forms of advanced electronic signatures that correspond to certain stages of this lifecycle". It is supposed that Clause 1 means Section 4.1. However section 4 is dedicated to signature creation and thus should not address topics that	Delete the quoted sentence. Note that further comments propose to delete that section.	Has been deleted due to restructuring anyhow

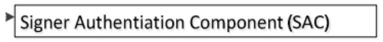
				re related to signature validation.		
4.	Scope	1	Editorial	The text states: Clause 5 It is supposed that Clause 5 means Section 5.	Replace with: Section 5.	Rejected. Clause is the term to be used here
5.	Scope	1	Technical	The text states: "It is agnostic to the type of security measures; while it is primarily aiming at Advanced Electronic Signatures, which provide such features intrinsically, but it also allows for variations, like classical archiving services, where the security measures may also be non-cryptographic." It is not fully agnostic.	Replace with: "While it is primarily aimed at Advanced Electronic Signatures, which provide intrinsically features to cover these security measures, it also allows for variations, like classical archiving services, where the security measures may also be non-cryptographic."	Has been deleted due to restructuring anyhow
6.	Definitions	3.1	Technical	The text states: Signature Upgrade: the process by which certain material (e.g. time-stamps, validation data and even archival-related material) is incorporated to an existing electronic signature aiming at making them more resilient to change or enlarging their longevity. This term is never used in this document, so it cannot remain. However, the term " Extended electronic signature" is used in particular in section 4.1.6 , but is defined nowhere. This term should be defined.	Replace with: "Extended electronic signature: It is a set of formats for electronic signatures built upon the basic electronic signature format (BES or EPES) which provides properties applicable for long term verification and that are intended for proper handling of certificate revocation, as well as certain disaster situations such as TSP key-compromise or broken algorithms.	Accepted with changes
7.	Definitions	3.1	Technical	It should be noticed that the term "Basic electronic signature" is being used, but it is defined nowhere. This term should be defined. The Note on page 16 of XAdES has been used to make a proposal: "NOTE 2: The XAdES-BES is the minimum format for an electronic signature to be generated by the signer. On its own, it does not provide enough information for it to be verified in the longer term. For example, revocation information issued by the relevant certificate status information issuer needs to be available for long term validation (see clause 4.4.3)".	Add : "Basic electronic signature: It is the minimum format for an electronic signature generated by a signer which protects with the digital signature the signature certificate used by the signer. On its own, it does not provide enough information for it to be verified in the longer term".	Accepted with changes
8.	Definitions	3.1	Technical	It should be noticed that the term "Explicit Policy-based electronic signature" is being used, but it is defined nowhere. This term should be defined. See the comment on section 4.1.2.2. before writing a disposition of comment for this comment.	Add : "Explicit Policy-based electronic signature: It is a basic electronic signature which protects with the digital signature the reference of a signature policy which shall be used by the verifier to identify which signature validation policy is appropriate to be used. NOTE: It is the first time a formal definition is provided. It is purposely different from the text originally present in section 4.3.2 of CAdES and in section 4.1.2 from XAdES.	Accepted with changes

9.	4.1.2.2.1		Technical	The text states: "A Basic Advanced Electronic Signature (BES) SHALL contain a reference to the signer's certificate as a signed qualifying property; they are designed to prevent simple substitution and reissue attacks and to allow for a restricted set of certificates to be used in verifying a signature." Since the figure below shows "signature attributes", the text is inappropriate. In addition, the reference is for one and only one certificate.	Change into: "A Basic Advanced Electronic Signature (BES) SHALL contain a reference to the signer's certificate as a signed attribute; it is designed to prevent simple substitution and reissue attacks and to allow for only one certificate to be used in verifying an electronic signature "	Accepted with changes
10.	4.1.1		Technical	The title of section 4 is "Signature creation", while the title of section 4.1 is "Lifecycle of an electronic signature". Figure 1 is supposed to "illustrate the potential life cycle an advanced electronic signature can potentially go through". There is several problems with Figure 1. Is it supposed to explain the life cycle for signature creation or the whole life-cycle ? If it is the whole, then it does not cover all the forms of extended signatures. If it is the life cycle for signature creation that some parts are mandatory while some other are optional. In any case, Figure 1 and the associated text is not adequate. The structure of the document appears to be correct since section 4 is called "Signature creation" while section 5 is called "Signature validation". The problem is that the content of section 4 is incorrect since it contains many sections dealing with signature verification. The whole section should be revised and restructured.	At this stage and given the fact that there are 20 other documents awaiting for comments before January 15, (more than 1000 pages) it is not possible to provide a whole text replacement. However some text and some guidance is given below. Delete sections Figure 1 and sections 4.1, 4.1.1 and 4.1.1. Replace with : 4.1. Introduction. Text for section 4.1 Introduction: "Section 4 deals with Signature creation. A signer must provide to a verifier, at the minimum, a basic electronic signature or an advanced electronic signature. A signer may also provide other signature formats corresponding to extended electronic signatures formats, but unless specified by the signature creation policy, is not forced to do so. In order to avoid duplications in this document, section 4 only deals with the formats that a signer must provide. Other formats are covered in section 5."	Section has been rewritten, comments no longer directly applicable. Need to recheck with current version
11.	4.1.2.	Figure 2	Technical	The text states: "Advanced electronic signatures conforming to [1,2,12] build on a base format (e.g. 10, 16) by incorporating qualified properties into the signature. Some of the properties will be covered by the signer’s signature (signed qualifying information) while others will not (unsigned qualifying information)". This section is using a vocabulary that is not coherent with the remaining of the document: "qualifying properties" whereas everywhere the term "attributes" is being used.	Change proposal: "Advanced electronic signatures conforming to [1,2,12] build on a base format (e.g. 10, 16) by incorporating attributes into the signature. Some of the attributes will be covered by the signer’s signature (signed attributes) while others will not (unsigned attributes)".	Accepted in principle. Changed whole text to using attributes an not properties.
12.	4.1.2.	Figure 2	Technical	Figure 2 includes two boxes:	Add in these boxes "Opt." to indicate that they are optional.	Accepted with modifications. (O) means optional

				 These two stages are optional.		
13.	4.1.2.	Top of page 17	Technical	There is some "floating" text without a subject: "shows the steps involved in creation a signature. Clauses 4.1.2.3.1 to 4.1.2.3.4 describe these steps while clauses 4.1.2.2.1 and 4.1.2.2.2 describe the two possible forms of Advanced Electronic Signatures resulting from this process." This text does not add anything useful.	Delete this "floating" text.	No longer applicable, section rewritten
14.	4.1.2.2.	Note	Technical	The text states: An Explicit Policy-based Electronic Signature (EPES) extends the definition of an electronic signature to conform to an identified signature policy. It incorporates a signed attribute indicating the signature policy that is recommended to being used to validate the signature. It would be appropriate to refer to a basic electronic signature. CAdES, section 4.3.2. states : "A CAdES Explicit Policy-based Electronic Signature (CAdES-EPES) incorporates a signed attribute (sigPolicyID attribute) indicating the signature policy that shall be used to validate the electronic signature". XAdES, section 4.1.2 states: "An Explicit Policy based Electronic Signature (XAdES-EPES) form in accordance with the present document, extends the definition of an electronic signature to conform to the identified signature policy. A XAdES-EPES builds up on a XAdES-BES forms by incorporating the SignaturePolicyIdentifier element. This signed property indicates that a signature policy shall be used for signature validation. It provides means for explicitly identifying the signature policy. Other properties may be required by the mandated policy. Well, this is not fully consistent, in particular for XAdES since anyway a signature policy will be used by the verifier ! In some implementations, the reference of the signature policy is the one for the signature CREATION policy which only includes rules for signature creation, but no rules at all for signature verification ! Nevertheless, it may be	Replace with: "An Explicit Policy-based Electronic Signature (EPES) extends the format of a basic electronic to incorporate a signed attribute indicating the reference of a signature policy which shall be used by the verifier to identify which signature validation policy is appropriate to be used". A Note is certainly needed. However, it is more appropriate to place it in the definitions section rather than in the middle of the document. See the comment made earlier on section 3.1.	Definition has been added before. Section completely rewritten

				used to identify which signature VALIDATION policy is appropriate. First, all three documents should be consistent, which may still lead to modify CAdES and XAdES... if not yet published. It would be more appropriate to relax the meaning of this attribute, by also allowing to reference the signature CREATION policy which should then be used by the verifier to identify which signature validation policy is adequate. Note: It took more than one hour to provide this comment.		
15.	4.1.2.3.3		Technical	The text states: The SCA should also check the revocation status of the certificate. It should be possible to create a BES or a EPES in an off-line mode. Thus "should" is inappropriate and should be changed into "may".	Replace with: "The SCA may also check the revocation status of the certificate.	Section completely rewritten
16.	4.1.2.3.4.		Technical	The text states: "According to its definition, an advanced electronic signature is uniquely linked to the signer (see). Technically, this is achieved in two steps: A link between the signer and the signature creation device (Unique link 1 in the figure) and a link between the signature creation device and the signature (Unique link 2). Unique link 1 means technically that the Advanced Electronic signature can only have been created by an SCDev with the related signature creation data corresponding to the signature verification data from a qualified certificate. Unique link 2 means technically that the SCDev has to verify that the legitimate signer is the one who requires a signature creation. If there are other means for keeping the SCDev under the sole control of the signer, then they are also applicable". This text is incorrect. The picture is incorrect too. Looking at the format of an AdES it is impossible, in general, to know whether a SCDev has been used or not. Since the title of this section is "Signature Invocation", it is not believed that the text should be maintained, since it is unrelated. In case, there is a wish to maintain it, an alternative text is provided.	Either delete the quoted text and Figure 5 or replace with: "According to its definition, an advanced electronic signature is uniquely linked to the signatory (see [i.15]). Technically, this is achieved in four steps: A link between the electronic signature and the signer's certificate, since the electronic signature includes a reference to the signer's certificate as a signed attribute. A link between the signer's certificate and a public key contained in that certificate which is guaranteed by the CA (Certification Authority) which has issued the signer's certificate. A link between the public key and the associated private key which is achieved by the properties of the asymmetric signature algorithm. A link between the private key and a SCDev which implements or contains the private key".	Since text is mostly explanatory, it has been removed.
17.	4.1.2.3.4.1.		Technical	The text states: To ensure the unique link between the electronic signature and the signer, the SCDev performs an	Replace with: The SCDev performs an authentication procedure to verify that the legitimate SCDev holder is the one requesting creation of an electronic	Accepted.

				authentication procedure to verify that the legitimate SCDev holder is the one requesting creation of an electronic signature. Delete" To ensure the unique link between the electronic signature and the signer" since this has nothing to do with signer authentication.	signature.	
18.	4.1.3.		Technical	This section is about AdES-T. In general, it is not required that the signer must provides this format. This section should be moved in section 5 (Signature validation).	Suppress section 4.1.3 and move it in section 5.	Rejected. While it is related to validation and can be done by the validator, it still is a creational process and should stay in creation.
19.	4.1.4	Note	Technical	This section is about Initial Signature Validation. It is not believed that this section should be maintained since it implies that the signature creation application is working in an on-line mode, whereas it should be possible to work in an off-line mode. it would also imply that a AdES-T format has been obtained, which is not necessary nor mandatory. Signature creation should be kept simple. If there is a wish on the signer's side to make a verification, then this should be done by a true verification application, rather than some forms of the verification included in the signing process.	Suppress section 4.1.4.	Rejected. The section has been moved but the content remained. The initial validation uses the true validation algorithm and is completely optional. A note regarding offline/online has been added.
20.	4.1.5.		Technical	This section is about electronic signature with complete validation data references. It is not believed that this section should be maintained. This section should be moved in section 5 (Signature validation).	Suppress section 4.1.5 and moved it in section 5 (Signature validation).	See comment 18
21.	4.1.6		Technical	This section is about extended electronic signature forms. It is not believed that this section should be maintained. This section should be moved in section 5 (Signature validation).	Suppress section 4.1.6 and moved it in section 5 (Signature validation).	See comment 18
22.	4.1.8.		Technical	This section is about Arbitration. It is not believed that this section should be maintained. This section should be moved in section 5 (Signature validation).	Suppress section 4.1.8 and moved it in section 5 (Signature validation).	Arbitration has been removed from the draft. Out of scope.
23.	4.2.	Figure 14	Technical	Figure 14 illustrates a Conceptual Model of Signature Creation. It is not believed that the figure is adequate. 1) It is confusing since the text talks about a Signature Creation System which is missing on the figure. Please depict the limits of the Signature Creation System. 2) A direct arrow should be added between the Signature creation Policy and the SCA. This is needed in particular when the SCA is able to "understand" directly a formal signature policy.	Revise the figure according to the comments	Accepted. Figure has been improved.

				3) The box" certificates" does not make sense and should be deleted since the DA normally does not the signer's certificates. Signer's certificates (or a URL and a hash value to retrieve certificates) shall be carried in the SCDev (see the end of section 4.3.6.4), so the box of the SCDev should show that it contains at least one signer's certificate (or a reference and a hash value to it) and the associated private key. 4) The UTC time is missing, so it should be added.		
24.	4.2.1.	page 27	Technical	A bullet states: "The SCDev Interface. The SCDev is considered to be external to the SCA and will need to interact with the SCA to receive the Signer's Authentication Data and DTBS if there is no direct user interface between the SCDev and the signer, and return the digital Signature to the SCA;" This is insufficient since the SCDev MUST contain both the signer's certificate and the associated private key.	Replace with: "The SCDev Interface. The SCDev is considered to be external to the SCA and will need to interact with the SCA to provide the signer's certificates, and once a certificate has been selected to select the corresponding private key, receive the Signer's Authentication Data and DTBS if there is no direct user interface between the SCDev and the signer, and return the digital Signature to the SCA;"	Accepted with modification
25.	4.2.1.	Figure 15	Technical	Figure 15 should be modified according to the comments made for Figure 14.	Revise the figure according to the comments	Revised
26.	4.2.1	page 28	Technical	The text states: "An interface to TSPs issuing certificates – over which Certificates and, optionally, Certificate Revocation Information may be obtained;" The word "optional" is misplaced.	Replace with: "An optional interface to TSPs issuing certificates – over which Certificates and Certificate Revocation Information may be obtained;"	Accepted
27.	4.2.1	page 28	Technical	The text states: "An interface to other TSPs – over which e.g. time-stamping services or signature policies may be obtained" The word "optional" is missing.	Replace with: "An optional interface to other TSPs – over which e.g. time-stamping services or signature policies may be obtained"	Accepted
28.	4.3.			It is very questionable whether this section should stay since it is more relevant for a Protection Profile rather than for a document related to "procedures".	Deleted section 4.3	Has been removed in new draft
29.	4.3.	Figure 16	Typo	 Signer Authentiation Component (SAC)	If section 4.3 is not deleted, replace Authentiation by Authentication.	Has been removed in new draft
30.	4.3.3.		Technical	The text states: "SCA returns error and status messages to the signer using the Signer Interaction Component. This interface is used for all interactions between the Signer and the SCA, including input/selection of the SD and Signature Attributes and Signature Policy with the	Replace with: "SCA returns error and status messages to the signer using the Signer Interaction Component. This interface is used for all interactions between the Signer and the SCA, including input/selection of the SD, the signer's certificate, other Signature Attributes and Signature Policy with the exception of the Signer’s Authentication Data.	Has been removed in new draft

				exception of the Signer’s Authentication Data". The list is missing to mention the signer's certificate.		
31.	4.3.6		Technical	The text states: "Its tasks are " This is certainly an error left intentionally by the editors to know how many persons approved the document without reading it.	Please, note that one person read the document and is not approving it. Please provide the text and re-submit the document to public comments.	Has been removed in new draft
32.	4.3.6.4.		Technical	The text states: "If the SCDev does not contain the certificate with the signature verification data (i.e. the public key of the signer) and possibly further certificates belonging to the signer’s certificate chain, then at least an unambiguous reference to the signer's certificate in the form of a Uniform Resource Locator (URL) or another form of reference (specified e.g. in the cryptographic token information) should be retrievable from the SCDev". An unambiguous reference to the signer's certificate in the form of a Uniform Resource Locator is insecure. A hash value of the certificate shall be present otherwise, it is possible to obtain a wrong certificate if there is a network attack. This is the Achilles' heel of the whole process, since the remaining text is missing to say what to do in that case.	Replace with: "If the SCDev does not contain the certificate with the signature verification data (i.e. the public key of the signer) and possibly further certificates belonging to the signer’s certificate chain, then at least an unambiguous reference to the signer's certificate in the form of a Uniform Resource Locator (URL), a hash value of it and information like the subject and the issuer name; the signer's certificate or another form of reference (specified e.g. in the cryptographic token information) should be retrievable from the SCDev".	Has been removed in new draft
33.	4.3.6.5		Technical	The text states: "If an SCDev holds more than one instance of signature creation data, then the one appropriate for the signer's intentions has to be selected. Even if the SCDev has only a single signature creation datum, it may require that a reference to it is set. To enable the selection of the correct signature creation data, the SCDev Token Information has to contain information denoting the link between a certificate (possibly selected by the signer) and the signature creation data reference. If the SCDev also requires a reference to an algorithm, then this also has to be indicated in the SCDev token information". It is always necessary to include a reference of the signer's certificate as a signed attribute. So it is necessary first to select the certificate and then the associated private key.	Replace with: "Before being able to select a private key (SDA), it is necessary to select the signer's certificate or a reference to it, since a reference of the signer's certificate must be included as a signed attribute. Once appropriate the signer's certificate has been selected, the corresponding private key can be selected. To enable the selection of the correct private key, the SCDev Token Information has to contain information denoting the link between a certificate (selected by the signer) and the signature creation data reference. If the SCDev also requires a reference to a signature creation algorithm, then this also has to be indicated in the SCDev token information.	Has been removed in new draft
34.	4.4		Technical	The text states: "The SCDev performs those functions that hold the signer's signature creation data, verify the signer's authentication data and create the electronic signature using the signer's signature creation data."	Replace with: "The SCDev performs those functions that hold the signer's certificates (or unambiguous references to them) and the corresponding private keys, that verify the signer's authentication data and that create the **digital** signature using the selected signer's private key".	Accepted with modifications. Section has been moved in new draft.

				It is missing to mention what section 4.3.6.2 (and the corrected section 4.3.6.4) stated earlier.		
35.	4.5	Figure 20	Technical	Figure 20 mentions the certificate identifier but omits to mention its relationship with one of the private keys hold on the SCDev.	Please expand the SCDev to show that it contains signer's certificates (or unambiguous references to them) as well as the corresponding private keys and add a doted arrow between the selected signer's certificate and the data box "Certificate identifier (M)". Please provide the text that is missing in the current explanations.	The SCDev is not part of that drawing and it would confuse the drawing too much to add it. It has been added in the other figures and the text will describe it appropriately.
36.	4.5	Figure 20	Technical	A direct input for the signature policy should be added when the SCA is able to directly process a formal signature policy.	Please add a data box "Signature Policy", make it optional (O), and provide a doted arrow with the data box "Other attributes (O)" and add above that arrow "Reference to the signature policy for EPES). Please provide the text that is missing in the current explanations.	EPES-pointer added.
37.	4.5.2	Second paragraph	Technical	The second paragraph states: "This clause specifies mandatory and optional signature attributes. Attributes can either be signed attributes, i.e. attributes that are covered by the signature, or unsigned attributes, i.e. attributes that are not secured by the signature. Unsigned attributes may also be added to a signature at a later stage. The set of attributes included in a signature is defined by the signature creation policy used or, when extending a signature, by the signature validation policy used and can also be format specific". With the exception of one type of unsigned attribute, only the signed attributes should be covered in section 4, since the other unsigned attributes are part of the signature validation process (section 5). In fact, unsigned attributes are NOT described in section 4.5.2 !	Replace with: "The set of attributes included in a signature is defined by the signature creation policy. This clause specifies mandatory and optional signed attributes, i.e. attributes that are covered by the signature and one unsigned attribute which shall contain the signer's certificate and optionally superior certificates. Other unsigned attributes, i.e. attributes that are not secured by the signature, are addressed in section 5".	Accepted with changes
38.	4.5.2		Technical	Section 4.5.21 and the sections whihc follow do not say whther the attributes are signed or unsigned. It is necessary to be explicit on this aspect. Since the difference between signed and unsigned attribute is rather fundamental, it is proposed to introduce two subsections: 4.5.2.1 Signed attributes 4.5.2.2. Unsigned attribute	Introduce two subsections: 4.5.2.1 Signed attributes 4.5.2.2. Unsigned attribute All sections currently numbered from 4.5.2.1 to 4.5.2.9 should be moved under section 4.5.2.1 Signed attributes.	No unsigned attributes are listed
39.	4.5.2.1		Technical	The text states: "This attribute may also contain references to other certificates. If so, they limit the set of certificates that are used during validation and typically form the chain for chain validation of the signers' certificate. For each certificate, the attribute also contains a digest together with a unique identifier of the	Please delete this quoted text .	Rejected. The inclusion of the whole certificate path is possible and supported.

				algorithm that has been used to calculate that digest. " It has never been intended to include more than one certificate.		
40.	4.5.2.2		Technical	The text states: "This reference indicates to the verifier which is the correct signature policy to be used during the verification process". In order to align with previous comments, this sentence needs to be modified.	Replace with: "This reference indicates to the verifier the signature policy which shall be used by the verifier to identify which signature validation policy is appropriate to be used".	Rejected. The verifier is free to ignore this information. The current text indicates this intention.
41.	4.5.2.6.		Technical	The text states: "This attribute contains the time at which the signer claims to have performed the signing process". The UTC time is mandatory.	Replace with: "This attribute contains the UTC time at which the signer claims to have performed the signing process".	Rejected. This document does not specify such details.
42.	4.5.2.9		Technical	After section 4.5.2.9, add the new section 4.5.2.2. Unsigned attribute. There is a single unsigned attribute to be considered.	Text proposal: "4.5.2.2. Unsigned attribute In order to ease signature validation, if the signer's certificate is not directly protected by the digital signature then the signer's certificate should be part of the electronic signature In as an unsigned attribute. Since a reference to that certificate is always included as a signed attribute, it is possible to make sure that no substitution has been made to that unsigned attribute."	Accepted with modification. A Note has been added, an attribute is only one of the possible places.
43.	4.5.11		Technical	Delete section 4.5.11 since it relates to section 5 rather than section 4.	Delete section 4.5.11.	Rejected. While it is true that this relates more to the validation, this data can still be collected during signature creation
44.	5.1		Technical	There is a major problem with the table of contents of this section. The various topics detailed in the Introduction (section 5.1) are going much further than a simple introduction. A new table of contents is being proposed.	Proposed table of contents: 5.1. Conceptual Model of Signature Validation 5.2 Initial and subsequent validations 5.2.1 Initial validation 5.2.2 Subsequent validation 5.3 Revocation checking 5.3.1 Revocation checking during an initial validation 5.3.2 Revocation checking during a subsequent validation 5.3 The various forms of AdES 5.3.1 Electronic signature with time (AdES-T) 5.3.2 Electronic signature with complete validation data references (AdES-C) 5.3.3 Extended electronic signature forms 5.3.3.1 Extended signatures with time indication (AdES-X) 5.3.3.2 Extended long signatures with time indication (AdES-X-L) 5.3.3.3 Long Term Validation Data (AdES-LT)	Rejected. The STF sees no need to completely restructure the validation draft.

					5.3.4 Archive signature (AdES-A) 5.3.5 Arbitration 5.4. Signature validation status and signature validation report 5.5 Extended electronic signature output	
45.	5.1		Technical	Section 5.1 is currently called Introduction. Section 5.1 should be renamed Conceptual Model of Signature Validation.	Rename Section 5.1 :Conceptual Model of Signature Validation.	Accepted with modification.
46.	old 5.1		Technical	There is a major problem with this section. The text states: "A signature validation application (SVA) receives signed data and other input from the driving application (DA), validates the electronic signature against a set of validation constraints and outputs a validation report. This report consists of ...". In addition to the validation report a SVA may provide an extended electronic signature. This is an output that is NOT part of the validation report. The validation is performed against a signature validation policy, from which validations constraints may be derived.	Text replacement proposal: "A signature validation application (SVA) receives signed data and other inputs from the driving application (DA), validates the electronic signature against a signature validation policy and outputs a validation report and optionally an extended electronic signature. The report consists of ...".	Rejected. The validation as described here is not concerned with extending the signature. This is described elsewhere. While it would be possible to describe it as suggested ("against a signature validation policy"), the STF decided to keep the term validation constraint to avoid confusing a formal policy with the overall validation policy, which may include a formal validation policy.
47.	5.1	Figure 21	Technical	Figure 21 is too simplistic and is missing many aspects. Figure 21 is missing to mention the signature validation policy. A direct arrow should be added between the Signature Validation Policy (which is missing on the figure) and the SVA. This is needed in particular when the SVA is able to "understand" directly a formal signature validation policy. Figure 21 is missing to mention a second major output: Extended electronic signature (O). Figure 21 is missing to mention "Additional data to be used to validate the signature" provided by the DA (see the text in the current section 5.1.5). Figure 21 is also missing to mention that on-line access to some TSP information is required (in particular for obtaining revocation information and TSTs). It should be noticed that the figure on page 25 from CWA 14171:2001 is much better, since it provides clearer information. Figure 21 is clearly a regression towards the figure on page 25 from CWA 14171:2001. Please reconsider Figure 21 to the light of the	Please reconsider Figure 21 to the light of the figure on page 25 from CWA 14171:2001, correct and complement the figure.	Unfortunately no copy of the 2001-version at hand. The 2004 version must be a regression too, since no related figure could be identified. The formal policy has been added. The extend signature is not an output of the validation process. X.509 Meta Data aka "Additional Data" has been added The figure does not show interactions with e.g. TSPs to keep it simple.

				figure on page 25 from CWA 14171:2001.		
48.	5.1.1		Technical	The title of this section is: 5.1.1 Types of Validation It should rather be called: Initial and subsequent validation.	Rename section 5.1.1: Initial and subsequent validations	Accepted
49.	5.1.1 New section 5.2		Technical	The rational for the initial validation and subsequent validations is not provided. The current text is: "Validation of signatures is different, depending on the time of the validation and the form of the signature to validate. We distinguish the following basic validation types: • Initial Validation: This validation is done on one of the base forms of the signature (BES/EPES) immediately or shortly after creation of the signature. It can be done by the signer or a verifier. Certificate and revocation information collected during that validation may be used to create an extended signature form. Signature and other timestamps may only be applied after successful initial validation. • Subsequent Validation: This validation type uses references to certificates and revocation information or certificate and revocation information stored within the signature for validation as well as time-stamps protecting signature elements. It may also collect further certificates and revocation information if applicable". These explanations are fairly insufficient. Note: it took more than two hours to build the text proposal.	Text proposal: "5.2 Initial and subsequent validations The validation of an electronic signature may be performed during two time periods: - during the validity period of the signer's certificate, or - beyond the validity period of the signer's certificate. Since revocation information is available during the validity period of the signer's certificate, at a first glance, it might be thought that the signature validation simply consists to demonstrate that the signer's certificate was not revoked using the available revocation information. This works well as long as the signer's certificate is not revoked. If it is revoked, it cannot be determined whether the revocation happened before the signature was made or after the signature was made. Since it is impossible to know exactly at which time the signature has been made, an upper limit of this time is being used instead. It consists of applying either a Time Stamp Token (TST) or a time mark (TM) on the digital signature, therefore applied after the signature was made. In order to minimize the risk of a revocation which would happen after the signature was made, the TST or the TM should be captured as soon after the signature was received by a verifier. Alternatively, the signer or another entity may apply the TST or the TM. 5.2.1 Initial validation The first goal of an *initial validation* is to verify the signature at the current time. When there is a need to verify an electronic signature during the validity period of the signer's certificate, the second goal is to provide an extended electronic signature form, in particular to apply a TST or TM on a BES/EPES signature in order to obtain an AdES-T form of electronic signature. When there is a need to verify an electronic signature beyond the validity period of the signer's certificate, the third goal of an *initial validation* is to collect the certificates from the signer's certification path and the associated revocation information, as well as the certificates needed to verify the certificates from the TST's path while they are still available using some an on-line access. This allows to obtain either an AdES-C or AdES-XL form of electronic signature. An AdES-XL form includes all the *values* of the certificates from the signer's certification path and of the associated revocation information. Alternatively, an AdES-C form of electronic signature may be used. This form only includes the *references* to the certificates and the revocation information but requires to be able to store and retrieve the values of the certificates and of the revocation information from some repository maintained by the signature validation process. Hence, each AdES-C is shorter than the AdES-X form.	Rejected, this and some of the comments following try to rewrite the draft via comments. Valuable parts of the new proposal may be integrated into text.

					Figure X [re-use Figure 1 from the original section 4.1] illustrates the beginning of the life cycle an advanced electronic signature. Figure X: Beginning of the Signature Lifecycle. In order to validate an electronic signature it is necessary to make sure that none of the certificates being used to validate a certification path has been revoked. Further details on how to check the revocation status of a certificate during initial validation are provided in section 5.1.2. 5.2.2 Subsequent validation As long as the certificates to verify the signer's certification path are available and an on-line access to revocation information is available, a *subsequent validation* can be done at any time during the validity period of the signer's certificate using an AdES-T form of electronic signature. When a signature validation needs to be performed beyond the validity period of the signer's certificate, the second goal of a *subsequent validation* is to re-use the AdES-C form or the AdES-XL form of electronic signature provided during an initial validation. A *subsequent validation* can be done as long as an on-line access to check the revocation status of the TST is available and as long as the validity period of the certificate to be used to validate the TST has not expired. Both an initial validation and an subsequent validation may provide additional forms of electronic signatures that are able to counter security threats such as TSP key-compromise or soon to be broken hash algorithms. This allows to obtain either an AdES-X form or an AdES-A form. The AdES-A form is NOT simply an extension of a AdES-X form since it is required to compute a new hash value using a new hash algorithm covering not only a AdES-X form but also the signer's document".	
50.	New 5.1.2		Technical	This text has been provided and placed there after considering the text from section 5.1.7 and the text about the grace period in section 4.1.1.1.	Text proposal: 5.3 Revocation checking 5.3.1 Revocation checking during an initial validation". To check the revocation status of a certificate during an initial validation, it is necessary to obtain recent revocation status information about that certificate. However, obtaining revocation status information issued at the current time is (in practice) impossible even with schemes providing real time revocation information (e.g. OCSP). Most of the time, revocation status information issued shortly before the current time is being used and the approximation that the information it contains is still reliable at the current time is being made. However, a signature validation policy may require that the extended electronic signature provided as an output of the initial validation shall be able to demonstrate that the signer's certificate was not revoked at the time indicated in the Time Stamp Token (TST) or a time mark (TM). If such a requirement exists, a grace period will be present in the signature validation policy. A grace period permits certificate revocation information to propagate through the revocation processes. This period could extend from the time an authorized entity requests certificate revocation, to when relying parties may be expected to have access to such revocation information. This typically means the issuance of a new CRL or the availability of the new certificate status to the OCSP responder. In order to make sure that the certificate was not revoked at the time the signature was time-marked or time-stamped, a	See comment 49.

					signature validation policy MAY force verifiers to wait until the end of the grace period. Note: In many scenarios, waiting for an extended time until accepting a signature will be incompatible to standard business requirements. The validation policy used should reflect such requirements. Another concern needs to be taken into consideration: whether the revocation status information that is being used is "fresh enough". The freshness of the revocation status information is the maximum accepted difference between the date the revocation status information was captured and the current time. When the date the revocation status information was captured is unknown, then the issuance date of the revocation status information shall be used instead. A signature validation policy may require that all the revocation status information used to validate a certification path shall have been captured less than a given time period T. This is particularly useful when using CRLs, since the time period between the thisUpdate field and nextUpdate field may be quite large (e.g. one month or even one year for root CAs). If CRLs that is in cache are always used in priority, emergency CRLs will only be taken into consideration when the current date exceeds the nextUpdate field. Defining a time period for the freshness of revocation information can be seen as a way to flush the cache in order to avoid using information that is too old. Note: whether a constraint on the freshness of revocation information has been defined or not in a signature validation policy is not visible when looking to the components of an extended electronic signature.	
51.	New 5.1.3		Technical	This comment originally come from a further comment made on section 5.1.7. Since it is proposed to delete section 5.1.7, the text within it has been reused (with major corrections). See the comments made on that section to know what the major comments are. Since there is now a section devoted to Revocation checking during an initial validation, there needs to be a companion section dealing with Revocation checking during a subsequent validation. A text proposal is provided.	5.1.3 Revocation checking during a subsequent validation At the minimum, an AdES-T form of electronic signature shall be used. This form always includes a TST or a TM applied on the signer's digital signature. The trustd time included in the a Time Stamp Token (TST) or in the time mark (TM) allows to know whether the revocation aroused before or after the trusted time indicated in the TST or the TM. If the revocation aroused after that trusted time, then the electronic signature is considered valid (pending other conditions are also verified. If the revocation aroused before that trusted time, then the signature is considered as invalid. Besides the fact that the date included in that TST or in that TM shall be used as the reference for revocation checking, another checking needs to be done if a grace period is indicated in the signature validation policy.	See comment 49.
52.	current section 4.1.6		Technical	The text and the figure that were previously in section 4.1.6 is not correct. Since it would take too long to correct it, it is proposed to keep only the title of the section. The text that follows in the various sections is much clearer.	Do NOT re-use the text that was previously in section 4.1.6. Keep only the title of the section, i.e. "Extended electronic signature forms".	Clause 4 has been rewritten.
53.	New 5.3.4 was 4.1.6.3	Figure 12	Technical	Figure 12 has been wrong for years. It is time to correct it. Note that the text states on page 23 :	Add a "signer's document" box, so both that the signed data and the AdES-X-L format are protected by the hash of the TST. Also add the following text:	Rejected. The figure may be an oversimplification, but it illustrates the points. Since the signers document is in the core of all the boxes, the outermost box illustrates the fact

				"the signed data, the AdES-C, and any additional information (i.e. any AdES-X) should be time-stamped". The Archive time stamp does not simply apply to the AdES-X-L format as illustrated on Figure 12, but both to the AdES-XL format and the signed data. Whereas in all the other cases, there is a Russian puppet scheme which apply to some previous form of electronic signature, in that case, the Russian puppet scheme does not apply here since it is necessary to get the original signed data again.	" In order to create this form of signature, it is necessary to have access to the original signer's document, i.e. not simply to the AdES-X-L format. Since the goal of an AdES-A format is to protect a valid signature in case some hash function originally used is suspected to become weak, this form of electronic signature will usually only be produced several years after an initial validation".	that the ATS covers the document, even if it is not calculated exactly as drawn.
54.	New 5.3.5 was 4.1.8		Technical	The original text for Arbitration was provided in section 4.1.8. In general, this text is rather good, ... but it only addresses the case of the -C format. The case of the other formats should be addressed as well.	Please provide the text for the other formats, otherwise delete that section since otherwise it would be "unbalanced".	Arbitration text has been removed.
55.	Current 5.1.2		Technical	This section should be deleted since after the detailed examination of the content of Table 3, only two cases remains: CRYPTO_CONSTRAINTS_FAILURE_NO_POE and NO_POE CRYPTO_CONSTRAINTS_FAILURE_NO_POE and NO_POE can easily be understood without this section. In addition, such a section with that level of indentation as high as the next section is not appropriate.	Delete section 5.1.2.	Agreed. The section has been changed to a definition with note
56.	5.1.3 New section 5.4		Technical	At the bottom of the page the text states: "For the certificate chain validation algorithm, the following assumptions are made: 1. If an intermediate certificate in a chain is revoked, and if no "better" chain can be found, a conformant SVA shall return INDETERMINATE, since another chain may exist (that the SVA cannot build due to missing certificates). 5) If a valid chain has been found (certificate path validation procedures defined in [4], clause 6 were successful and none of the intermediate certificates has been revoked) and the signer's certificate is revoked, the chain validation algorithm shall return INDETERMINATE/REVOKED_NO_POE. NOTE 1: This does not mean that the overall signature validation result will be INVALID. Long term validation may still find the signature to be valid at the time of signing."	Delete the quoted text.	Rejected. The algorithm cannot return INVALID if PoE prove the contrary.

				Assumption "1." is incorrect. If an intermediate certificate in a chain is revoked, then a conformant SVA shall return INVALID. Assumption "5)" is incorrect. If the signer's certificate is revoked, then a conformant SVA shall return INVALID. These two "assumptions" SHALL be deleted (using the IETF RFC vocabulary).		
57.	5.1.3 New section 5.4	Table 2	Technical	The table on page 41 states for the VALID case: "The validation process shall output the following: • For each of the validation constraints, the result of the validation. • The validated certificate chain, including the signer's certificate, used in the validation process". No. This is too much demanding. Most existing implementations only return the first error that is encountered and usually do not disclose in which order the tests are being made. Since the text is using a "shall" this is clearly not acceptable. When the main status is VALID, there is no need to report anything except any error encountered when attempting to produce an extended form of electronic signature.	Text replacement proposal: "The validation process shall report any error encountered when producing the requested extended form of electronic signature"	Accepted with modification. The validation process shall output the validated certificate chain, including the signer's certificate, used in the validation process. In addition, the validation process may provide the result of the validation for each of the validation constraints,
58.	5.1.3 New section 5.4	Table 2	Technical	The table on page 41 states for the INVALID case: "The validation process shall output additional information to explain the INVALID indication for each of the validation constraints that have been taken into account and for which a negative result occurred.". No. This is too much demanding. Most existing implementations only return the first error that is encountered and usually do not disclose in which order the tests are being made. Validation is stopped after each fatal error.	Text replacement proposal: "The validation process shall report : • the first error encountered when validating the electronic signature. • any error encountered when producing the requested extended form of electronic signature"	Rejected. If the validation stops at the first error, and no further checking is done, then only one validation constraints have been taken into account and only one error message is required.
59.	5.1.3 New section 5.4	Table 3 Page 42	Technical	There is no text to explain or support Table 3. Is it informative ? Is it normative ?	Proposed text to introduce Table 3: "Table 3 provides sub indications which may be used to complement the main status indication, i.e. VALID, INVALID and INDETERMINATE. These sub indications are not normative. However, implementations developed after the publication of this EN should consider them, and adopt them whenever possible".	Accepted with modification.
60.	5.1.3 New section 5.4	Table 3 Page 42	Technical	The text in the column "Associated Validation report data" states everywhere : "The validation process shall ..." Since the table is not intended to be normative, using a "shall" is clearly not acceptable.	Change into: "The validation process should ..."	See remark to point 59

61.	5.1.3 New section 5.4	Table 3 Page 42	Technical	The text states for : EXPIRED: "The signature is considered invalid because the Signature Validation Algorithm can ascertain that the signing time lies after the expiration date (notAfter) of the signer's certificate". The signing time cannot be known. The trusted time included in the TST or in the TM may be known.	Change into: "The signature is considered invalid because the Signature Validation Algorithm can ascertain that the trusted time included in the TST or in the TM lies after the expiration date (notAfter) of the signer's certificate".	Rejected. Of course the signing time is not known. The algorithm however is able to determine that the signing time lies after the expiration date of the certificate e.g. because the content time stamp, covered by the signature, has been produced at a time the certificate has already expired.
62.	5.1.3 New section 5.4		Technical	The text states for : NOT_YET_VALID: "The signature is considered invalid because the Signature Validation Algorithm can ascertain that the signing time lies before the issuance date (notBefore) of the signer's certificate". The signing time cannot be known.	Change into: "The signature is considered invalid because the Signature Validation Algorithm can ascertain that either the current time or the trusted time included in the TST or in the TM lies before the issuance date (notBefore) of the signer's certificate".	Similar to 61.
63.	5.1.3 New section 5.4		Technical	On page 43, the table indicates: UNKNOWN_COMMITMENT_TYPE The signature was created using a policy and commitment type that is unknown to the SVA. Since the syntax is correct, such an error cannot occur, since it is always possible to indicate the OID or the character string.	Delete that case.	Rejected. This status is a valid status when the DA relies on the SVA to validate also the commitment types.
64.	5.1.3 New section 5.4		Technical	The major additional sub indication to consider is : ON_LINE_ACCES_CURRENTLY_UNAVAILABLE The associated validation report MAY then indicate which data structure cannot be accessed. This allows to remove the following two sub indications: NO_SIGNER_CERTIFICATE_FOUND NO_CERTIFICATE_CHAIN_FOUND	Suppress the two following sub indications: NO_SIGNER_CERTIFICATE_FOUND NO_CERTIFICATE_CHAIN_FOUND Add: ON_LINE_ACCES_CURRENTLY_UNAVAILABLE; The associated validation report data should mention for this case: "The validation process should indicate which kind of data structure cannot be obtained via an on line access".	Rejected. There are situations possible where the signers certificate cannot be identified, e.g., even if online-access was available.
65.	5.1.3 New section 5.4		Technical	The sub indication REVOKED_NO_POE is a case which should never happen under the main indication INDETERMINATE. If it is an immediate verification, then in the absence of a TST the current time will be used. If a TST is already present, the TST will be used. If it is a subsequent verification, then if a TST is already present, it will be used. If it is not present, it is not the duty of the SVA to get it and thus the signature is invalid. This highlights the importance to make a difference between an immediate and a subsequent validation: the validation algorithms are NOT fully identical.	Suppress the following sub indication: REVOKED_NO_POE	Rejected. This status is just telling that there is no PoE that the signing time lies before or after revocation time. This will de facto mean that the signature has to be considered invalid, as long as no such proof can be found.

66.	5.1.3 New section 5.4		Technical	The sub indication REVOKED_CA_NO_POE is a case which should never happen under the main indication INDETERMINATE If one CA certificate is revoked, then the status is INVALID.	Suppress the following sub indication: REVOKED_CA_NO_POE	As 65
67.	5.1.3 New section 5.4		Technical	The sub indication OUT_OF_BOUNDS_NO_POE is a case which should never happen under the main indication INDETERMINATE. If the TST is missing when performing a subsequent validation, it is too late to get one and thus the status is INVALID.	Suppress the following sub indication: OUT_OF_BOUNDS_NO_POE	As 65
68.	5.1.3 New section 5.4		Technical	The sub indication NO_POLICY is a case which should never happen under the main indication INDETERMINATE. It is the duty of the DA to indicate which signature validation policy shall be used by the SVA. If there is any error in that policy, then the error is fatal and it does not belong to the INDETERMINATE case.	Suppress the following sub indication: NO_POLICY	Accepted.
69.	5.1.3 New section 5.4		Technical	The sub indication SIGNED_DATA_NOT_FOUND is a case which should never happen under the main indication INDETERMINATE. It is the duty of the DA to provide the signed data if it is not already embedded in the signature. Should it be obtained on-line, then the ON_LINE_ACCES_CURRENTLY_UNAVAILABLE sub indication should be used instead.	Suppress the following sub indication: SIGNED_DATA_NOT_FOUND	Rejected. The suggested status code is not used and does not provide any advantage.
70.	5.1.3 New section 5.4		Technical	The sub indication CHAIN_CONSTRAINTS_FAILURE is a case which should never happen under the main indication INDETERMINATE. If it happens it belongs to the INVALID case. Such a case already exits: CHAIN_CONSTRAINTS_FAILURE	Suppress the following sub indication: CHAIN_CONSTRAINTS_FAILURE	Accepted.
71.	5.1.3 New section 5.4		Technical	The sub indication CERTIFICATE_CHAIN_GENERAL_FAILURE is a case which should never happen under the main indication INDETERMINATE. If it happens it belongs to the INVALID case. The difference with the previous case is so subtle, that it does not make sense to add it to the INVALID case.	Suppress the following sub indication: CERTIFICATE_CHAIN_GENERAL_FAILURE	Accepted.
72.	New section 5.5		Technical	As indicated earlier, there should be a section called : 5.5 Extended electronic signature output.	Text proposal: 5.5 Extended electronic signature output. When performing an initial validation, a SVA shall able to provide, upon request, some forms of extended electronic signatures.	Rejected. Belongs to the creation part

					If these operations are provided in the same step, then the validation report shall contain two separate statuses: - one for the status of the electronic signature (valid, invalid or indeterminate), - another one for signaling any error in the production of the extended electronic signature. If the augmentation of the signature is provided in a separate step, then the validation report shall signal any error in the production of the extended electronic signature. When performing a subsequent validation, a SVA should be able to provide, upon request, some forms of extended electronic signatures.	
73.	Current section 5.1.4 New section 5.1.1		Technical	The title of this section is: Validation Constraints. The section should be placed at the bottom of page 39 and be re-numbered 5.1.1.	Rename this section 5.1.1. Validation Constraints	Unclear. The section has the requested title. Movement of section will be considered.
74.	Current section 5.1.4 New section 5.1.1		Technical	At the bottom of the page, in the current section 5.1.4, the text states: "In such cases, the SVA shall return, in its final report to the DA, the list of checks that were disabled due to the policy". The use of "shall" is to strong. Change into "may".	Change "shall" into "may".	Accepted with changes. Used should instead of may.
75.	Current section 5.1.5 New section 5.1.2		Technical	The title of that section is odd: "X.509 certificate meta-data". The text is interesting since it talks about "additional information to correctly validate the signature". The use of the term meta-data is not justified. It is proposed to rename that section: "Additional data to be used to validate the signature". However, this additional data is not part of the conceptual model (figure 21) which talks only about "validation constraints". Figure 21 should be revised to include this input.	Rename this section into: "5.1.2.Additional data to be used to validate the signature". Revise Figure 21 to include that input.	Will consider a better title. Have <one> section where we talk about where the information to check constraints can be taken from… e.g. local source (covering this point)
76.	Current section 5.1.5 New section 5.1.2		Technical	In order to avoid the use of the odd term: "X.509 certificate meta-data", the text should be revised. The text should also be made simpler.	Text replacement proposal: "Additional data to be used to validate the signature. Additional data may be required to allow the SVA to correctly validate a signature (e.g. to obtain data which is not or not easily available to the SVA). Such additional data may be : a CA certificate, a CRL, an OCSP response, a Trust-service Status List (TSL) or a Trusted List, This data is made available to the SVA by the DA.	Rejected. The suggested text restricts the kind of data too much, it really is intended to allow any kind of metadata a DA/SVA may support to do that job.

					Making such data available to the SVA will therefore result more often in a VALID or INVALID response, where the SVA would need to return INDETERMINATE or INVALID should that information not be available. Information needed by the DA may be, e.g. • taken from the certificate content TS 101 862 [5], TS 101 456 [7] and TS 102 042 [8]; • derived from a Trust-service Status List [3] entry, or a full Trust-service Status List.	
77.	Current section 5.1.6		Technical	The title of that section is odd: "taken from local configuration Trust Management". The content does not really make sense, since trust anchors are part of a validation policy and if there is such a discussion, it should rather be on how to construct a validation policy. Therefore, it is proposed to suppress this section.	Suppress section 5.1.6.	Accepted
78.	Current section 5.1.7		Technical	The title of this section is "The concept of revocation freshness". It defines the freshness of the revocation status information in the following way: "The freshness of the revocation status information is the maximum accepted difference between the issuance date of the revocation status information and the current time". The major problem is that this definition is incorrect. Before providing a corrected definition, let us consider an example. A Root CA issues a CRL which lasts one year. It will issue a new CRL in case a sub CA is revoked. When is important is the time the CRL was captured by a verifier rather than the time the CRL was issued. The sentence should be corrected in the following way: "The freshness of the revocation status information is the maximum accepted difference between the date the revocation status information was captured and the current time. When the date the revocation status information was captured is unknown, then the issuance date of the revocation status information shall be used instead". The section is also missing to consider another important aspect: the concept of grace period which has been introduced earlier. The section is however coming out of the blue and is misplaced.	It is proposed to delete section 5.1.7, since its content has now be moved (with major changes into the new section 5.3.1 (Revocation checking during an initial validation).	Deletion rejected, since first it is not true that the content has been moved. The change regarding “capturing time” is rejected, since the freshness obviously has been intended to go in line with the grace period concept, which likely needs to be better presented.

79.	Current section 5.2		Technical	This section introduces "Basic building blocks". Figure 23 is a new picture which is in contradiction with Figure 21. It looks that if there were two different editors, each one placing its own Figure. It suffers from the same problems as Figure 21, but the situation is worse: the description only considers the current time, so it may possibly work for an initial validation but may not work for a subsequent validation. E.g. section 5.2.3.4: "Check that the current time is in the validity range of the signer's certificate". There are to many problems in that section to be able to provide corrections for each problem. As an example: section 5.2.2.4.1 "Processing commitment type indication. If this signed property is present, it allows identifying the commitment type and thus affects all rules for validation, which depend on the commitment type that shall be used in the validation context initialization". On the contrary, the commitment type never affects the rules for validation. It is simply reported if present and then it is up to DA to consider whether it is acceptable or not. Section 5.3 looks better at a first glance, but is not much better after further examination. The remaining sections of the document are badly structured since there is: "5.3 Basic Validation Process 5.3.1 Description This clause describes a validation process for basic short-term signature validation .." and "5.6 Validation of LTV forms This clause describes a validation process for signatures with long-term validation (LTV) information ..."" There should rather be two sections, at the same indentation level : - one dealing with the details for initial validation, - another one dealing with the details for subsequent validation. The text from section 5.2.2.4.2 is one of the worse and when it possible to understand a part of it (after three readings) it appears to be	The current sections 5.3 and 5.4 are a mess. It is quite hard to say what to do in this situation, since more than 16 hours have already been spent on this document. It is not possible to spend 16 hours to finish to correct it. Once again, the editors should have read CWA 14171:2001 and complement it with more details. The structure of this section of the document should be considered again. It is suggested to continue with two sections, at the same indentation level, called: - 5.6 Processing details for an initial validation. and - 5.7 Processing details for a subsequent validation.	Rejected. The figures intention is to show the relationship of the building blocks and the motivation will be better explained in the text “the commitment type never affects the rules for validation.” This is not true. A policy may contain different rules to follow depending on different commitment types.

				incorrect.		
80.	new section 5.6		Technical	A last before the end contribution. Since it is important to explain which signature validation policy shall be used both in the case of BES and of EPES, text is provided for the new section : 5.6 Processing details for an initial validation	Text contribution for 5.6 Processing details for an initial validation: "When the electronic signature does not contain a signature policy identifier, then the SVA should use the signature validation policy of its choice, based either on the context where the electronic signature was received or based on the semantics of the signed document. When the electronic signature contains a signature policy identifier, then the SVA should first verify that the attribute or property is correctly signed using the public key that is present in the signer's certificate. The signature policy identifier contained in the signed attribute or the signed property indicates the reference of a signature policy which shall be used by the verifier to identify which signature validation policy will be appropriate to be used. If this signature policy identifier is known to the DA, and if it matches with the context under which the electronic signature was received, then it shall be considered, otherwise the electronic signature shall be discarded. When the electronic signature is not discarded, two cases need to be considered: - If a formal definition known to the DA exists for this signature policy identifier, then that formal definition shall be selected or transmitted to the SVA. - If no formal definition known to the DA exists for this signature policy identifier, then the DA shall use an equivalent signature validation identifier. If there exists a formal definition for this equivalent signature identifier, then it shall be selected or transmitted to the SVA. If such formal definition does not exist, then the rules and the parameters corresponding to this equivalent signature policy identifier shall be selected or transmitted by the DA to the SVA.	Rejected. No such section is needed. Also, the SVA cannot use a policy "of its choice". This is a DA issue. The selection of a validation policy is not part of this specification but covered elsewhere
81.	5.4		Technical	A final comment, otherwise comments will not be finished before two working days. The text from section 5.4 Validation Process for Time-Stamps includes a major error, which should be mentioned. The text states: "An RFC 3161 [11] time-stamp token is basically a CAdES-BES signature. Hence, the validation process is built in the validation process of a CAdES-BES signature". Unfortunately this is not the case. Hence section 5.4.4 Processing is wrong. If a TSU certificate has been revoked, a TST issued by a TSS (Time-Stamping Server) using that TSU certificate remains valid if it has been produced while the TSU certificate was not revoked for any reason except (key compromise), but is invalid if the revocation reason is a key compromise. For a real time revocation checking of the last applied	If, in the next draft version, there still exists a section on Validation Process for Time-Stamps, that section should be rewritten to take advantage of the explanations that are provided on the left column.	A TST can be valid, even if the certificate of the TSA has been revoked, if there is a proof of existence that the TSA was "good" at the time of producing the TST. However it is true that the revocation case when there is no key compromise has not been covered. The only valid reason for revoking a TSA-certificate I see is when the TSA goes out of business or so. Not sure we need to specify this exactly. Will be reconsidered.

				TST, it is thus necessary to capture the current CRL. If the TSU certificate is revoked and if there is no reason code, the worse shall be assumed and thus the TST shall be considered as invalid. If the reason code is available, then two cases shall be considered: 1) The revocation reason is any reason except key compromise. The TST is valid if it has been issued before the revocation time. 2) The revocation reason is key compromise. The TST is valid whatever the time indicated in it may be. As it can be seen, the rules are fairly different from the validation process of a CAdES-BES signature. In addition this is the story for the "last applied TST". If there is a chain of TST, how shall the chain of TSTs be composed ? For each previous TST, it is necessary to demonstrate that is was still valid when the next TST was applied. This means that a CRL (or an OCSP response) must be captured and placed in the extended electronic signature. For XAdES, TimeStampValidationData allows to include RevocationValues. For CAdES, only the Archive time-stamp attribute includes extraRevocation. This means that the only way to maintain the signature time-stamp is to use the archive format. The problem is that it is impossible to maintain detached signatures unless having an access to the signer's document to recompute a hash on the document. Should a new unsigned attribute be defined as this has been the case for XAdES V1.4.1 (2009-06) ?		
82.	**general**			**Many pictures cannot be read**	**Updated all pictures so that a reader can read them**	Considered, need to check on printout, TODO
83.	**general**		**ed**	**Do not use "it is recommended", use "should"**	**Make appropriate changes**	Accepted
84.	**general**		**ed**	**This document introduces many abbreviations which are very difficult to remember and confuses the reader**	**Reduce the number of abbreviations to the terms very often used and not for others.**	Considered, TODO
85.	**general**		**ed**	**Keep the deliverable impersonal and use consistently "the SVA shall/should/may" everywhere**	**Remove any use of the 1st person (I, we), 2nd person (you).** **and use consistently "the SVA shall/should/may" everywhere**	accepted
86.	**general**		**tech**	**Throughout the document, there are occurrences of statements like "this may not be secured", "securely", "secure path" with no further specification/details -> useless**		not clear, agree to this in 4.3.8, where else specifically?
87.	**Foreword**		**ed**		**Use foreword of an EN**	Accepted, TODO

88.			tec	Do not use Must	Replace with shall	accepted
89.	introduction		tec	No requirement in introduction	To ensure trust in the electronic signature, several aspects ~~must~~ need to be considered. The different players and the environment of the signature creation and validation ~~have to~~ follow rules to allow them to be trusted. The present document concentrates on policy and security requirements ~~that must be considered~~ when creating and validating signature in a trustworthy manner.	Accepted with changes
90.	introduction	Last paragraph	ed	All standards tend to have this introduction. I would suggest to have it in the 119 x00 series only.	delete	Accepted
91.	scope		tec	Too long. ETSI drafting rules: the scope defines without ambiguity the subject of the ETSI deliverable and the aspect(s) covered, thereby indicating the limits of applicability of the ETSI deliverable or particular parts of it... The "Scope" shall be succinct so that it can be used as a summary for bibliographic purposes	Modify as follows: The present document specifies procedures for • Creating (Advanced) electronic signatures in a technology-agnostic way. It introduces general principles, objects and functions relevant when creating signatures based on signature creation constraints and defines general forms of advanced electronic signatures that allow verifiability over long periods. It is based on the use of public key cryptography to produce such signatures, which are supported by public key certificates. ~~Such signature creation constraints may be specified as part of a formal signature policy.~~ • Establishing whether an (Advanced) electronic signature is technically valid ~~based on the considerations specified in the present document and the validation constraints are applied to the verification procedures. These constraints may be specified as part of a formal signature policy~~. Most procedures are applicable to any format of an electronic signature. The following aspects are ~~considered to be~~ out of scope: • Generation and distribution of Signature Creation Data (keys etc.), and the selection and use of cryptographic algorithms; • Format, syntax or encoding of data objects involved, specifically format or encoding for documents to be signed or signatures created; • The legal interpretation of any form of signature	Done, but need to check if any of the removed parts is essential and needs to be put elsewhere
92.	scope		tec	Cannot define options, recommendations or requirements in the scope; moreover the fact that the constraints may be part of a signature policy is out of scope of the present document. Such statement should be in the signature policy documents:	Delete: Such signature creation constraints may be specified as part of a formal signature policy Delete: These constraints may be specified as part of a formal signature policy	Accepted
93.	scope		tec	What does mean "advanced" in parenthesis. Clause 4.1 only refers to AdES. Clearly define to which type of signature the document applies. Then use consistent phrasing throughout the document	If only advanced electronic signatures are covered, then remove parenthesis If electronic signatures and advanced electronic signatures are covered, then say "creating electronic signatures and advanced electronic signatures" and similarly for the second bullet. Then update clause 4.1	Accepted. Potentially this has an impact to the whole document. I would like to write it generically for "electronic signatures" and explain once the relationship to advance es. Discuss
94.	references				Check that all reference are correctly listed in the normative clause and information clause.	TO BE Done at the end
95.	definitions	general	ed	The term defined uses lower case letter There is no ending full-stop or semi colon at the end of a definition		Accepted

96.	definitions	general	ed		Remove "a", "an", "the" at the beginning of definitions Do not capitalize every single word of the term	Accepted
97.	definition	general	tec		Use consistently "signature", "advanced electronic signature", "electronic signature". Depending on the clarification of scope as asked above, use the appropriate term	Accepted, TO BE CHECKED
98.	definition	general	ed	This standard has many definitions complex to understand. Why over complicating it with several terms having the same definition.	Use only 1 term per definition and remove the alternative term (e.g.: Signature Process Result Object (SPRO) or Signature Process Output, signature attributes and signature properties...)	accepted
99.	definitions		ed	Modify definition of AdES	**Advanced Electronic Signature (AdES):** ~~advanced electronic signature means an~~ electronic signature that meets the following requirements [i.15]: 1) it is uniquely linked to the signatory; 2) it is capable of identifying the signatory; 3) it is created using means that the signatory can maintain under his sole control; and 4) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable. NOTE: In the rest of the present document the term "signature" is used to denote an Advanced Electronic Signature.	accepted
100.	definitions		ed	Certificate identifier is not properly defined	Certificate Identifier – an unambiguous identifier of a Certificate	corrected
101.	definitions	constraints	ed	How the formulation can be abstract? And delete "as defined above"	Remove "abstract" Delete "as defined above"	corrected
102.	definitions	Data to be signed	ed	Don't use abbreviations in definitions as it make it very difficult to understand In note: remove "actual"	Expand SDR	corrected
103.	definitions	Long term validation	ed	Cannot have examples in the definition itself.	Is the fact that the certificate expired, was revoked or the algorithms were broken essential to the definition. if yes, then it is part of the definition but not as examples If not, then remove this part from the definition and you can add an example.	corrected
104.	definition	Proof of existence	ed		Proof Of Existence (POE): evidence that proves that an object ~~(a certificate, a CRL, signature value, hash value, etc.)~~existed at a specific past or present date/time~~, which may be a date/time in the past~~	corrected
105.	definition	Signature creation data	ed		Change to: Signature Creation Data (SCD): unique data~~, such as codes or private cryptographic keys, which are~~ used by the signatory to create an electronic signature [i.15]; EXAMPLE: codes, private cryptographic keys.	rejected; comes directly from the directive;
106.	definition	Signature invocation	Ed/tec	"non trivial" is a very subjective word. Move "It is the 'Wilful Act' of the Signer" to a note		corrected
107.	definitions	Signature properties	ed		Move " also called *signature attributes"* to a note	corrected

108.	definitions	Signature upgrade	ed		Signature Upgrade: the process by which ~~certain material (e.g. time-stamps, validation data and even archival-related material)~~ is incorporated to an existing electronic signature aiming at making ~~them~~ it more resilient to change or enlarging ~~their~~ its longevity EXAMPLE: time-stamps, validation data and archival-related material are examples of incorporated material	corrected
109.	definitions	SVA	ed	This is not a definition. Isn't the SVA the application running the signature validation Do we need a definition for that?		Accepted, definition deleted
110.	definitions	Signature verification	ed		Signature verification: process of checking the cryptographic value of a signature ~~using signature verification data~~	corrected
111.	definitions	Signature Process Result Object	tec	It is not formulated as a definition And use only 1 term and why no "signature creation output"? The format is not part of the definition	Proposal: Signature creation output: set of the electronic signature over the Data to be Signed, the signer document representation and the signature attributes Remove: it is in a format specified by the signer selected Signed Data Object Type;	Accepted with modification, now called signed data object
112.	definitions	Signed data objet type	tec	Cannot understand it without the definition of "signed data object" From this definition, it seems that the signed data object is the same as the signature process result object	clarify	accepted, see discussion of above
113.	definition	Signer's Authentication Data	ed	Not part of definition: The signer's authentication data may be referred to as 'Activation Data' in other documents;	Move to NOTE: it is called 'Activation Data' in other documents. Move examples as follows after the definition: EXAMPLE: PIN, password or biometric data.	corrected
114.	definitions	SDR	ed	Move examples	Move to EXAMPLE: hash of the SD or some element including the hash of the SD or the SD itself.	corrected
115.	definition	Validation constraint	tec	Wrong use of may in the note	Modify note to: NOTE: Validation constraints are defined in a formal signature policy, or are given in configuration parameter files or are implied by the behaviour of the SVA.	corrected
116.	definitions	Validation data	tec	Incorrect phrasing of the note	Modify to ~~NOTE~~EXAMPLE: ~~It may include:~~ certificates, revocation status information (such as CRLs or OCSP-Responses)~~,~~ time-stamps or time-marks	corrected
117.	4	Signature creation	tec	This section is written as a narration and not as a standard. Present tense is mostly used. Implementers have no clue what they shall implement, should implement and may implement	Fully review all clauses in 4 to clearly write normative requirements (using only shall), recommendations (using only should), options/permissible action (using only may). Use verbal forms defined in ETSI Drafting rules clause 14a (http://portal.etsi.org/edithelp/HowToStart/home.htm?page=DraftingRules)	

				-> complete re-writing needed	Clearly separate requirements from complementary informative text (e.g. using notes, examples) See attached revised draft where I started proposing changes. I could not fully review the draft but the changes I proposed need to be applied similarly in all clauses.	
118.	4.1.1	introduction	tec	Misuse of "can" in first sentence -> reword. It is not clear whether the life cycle in the figure is an example, or an exhaustive/complete life cycle. Need to be more precise		Rejected, believe that "Most signatures created will only encounter some of the steps in the life cycle" makes that clear.
119.	4.1.1	introduction	ed		~~This section will describe~~ The following clauses describe each step in the life cycle.	Merge conflict, resolved
120.	4.1.1	introduction	ed		~~This c~~Clause 4.1 is applicable to all implementations of advanced electronic signatures, irrespective of the format used	Merged changes here and change edited into document, both by ETSI
121.	4.1.1.1	Grace period	tec	Is it in the scope of this document to specify requirements on signature policies? If so, it needs to be clear in the scope and the relationship with the Signatures policy standards needs to be clear. If not, then remove any requirement on signature policy as the one below: a signature validation policy MAY force verifiers to wait until the end of the grace period and only point to the appropriate standard defining the signature policy.		Accepted. Section removed.
122.	4.1.1.1	Grace period	tec	Does this document define requirements on the grace period? Don't think this document does. Then point to the standard defining the grace period and strictly avoid any duplication of text with the reference standard	Clause to be reviewed pending on answer to questions.	Accepted. Section removed.
123.	4.2		Tec	It is not clear on which functional components the standard define requirements (normative, recommendations or permissible actions)	Clearly state that the present documents define requirements for the SCA, the SCDev?...	Section rewritten
124.	5	general	Tec	Inconsistent use of appropriate verbal forms.	Review to clearly write normative requirements (using only shall), recommendations (using only should), options/permissible action (using only may). Use verbal forms defined in ETSI Drafting rules clause 14a (http://portal.etsi.org/edithelp/HowToStart/home.htm?page=DraftingRules) Clearly separate requirements from complementary informative text (e.g. using notes, examples) See attached revised draft where I started proposing changes. I could not fully review the draft but the changes I proposed need to be applied similarly in all clauses. In particular: - the process shall input - the process shall output - in the processing clauses, clearly use shall/should/may at the different steps - don't write permissible actions (may) and recommendations (should) in notes	Accepted but yet to be implemented
125.	5	general	ed	Use consistent terminology, i.e. SVA everywhere	Use consistent terminology, i.e. SVA everywhere	Accepted but yet to be checked

126.	5	general	tech	**Don't use the phrasing** " The following steps shall be performed" followed by a bullet list where it is then not clear what's mandatory from what's recommended or permissible	**Rephrase with** The following steps are performed: 1. the SVA shall.... 2. when <condition X>, then SVA shall/should	Accepted but yet to be implemented
127.	5.1		ed	**Define a sub-clause of the first part**	**Introduce sub-clause number and title just after 5.1 title**	Accepted
128.	5.1		tech	I disagree with the statement below. The processing steps defined in clause 5 are mostly mandatory. You then cannot say here that you are not required to implement them "The present document presents the validation process in the form of algorithms to be implemented by a conforming signature validation application. Conforming implementations however are not required to implement these algorithms but shall provide behaviour that is functionally equivalent, i.e. they produce semantically equivalent results given the same set of input information"	**Delete:** The present document presents the validation process in the form of algorithms to be implemented by a conforming signature validation application. Conforming implementations however are not required to implement these algorithms but shall provide behaviour that is functionally equivalent, i.e. they produce semantically equivalent results given the same set of input information	Accepted with changes. Changed to “shall produce results” and “should use this algorithm”
129.	5.2.5.4		ed	**Introduce a sub-clause title as you define provisions in the beginning of the clause** **And** **Clauses 5.2.5.4.2 to 5.2.5.4.8 seem to be sub-clauses of 5.2.5.4.1**	**5.2.5.4.1 General processing** **And** **Check sub-clause hierarchy**	reorganized
130.	5.2.5.4.2		tech	**You can define provisions for the SVA not the verifier**	**Rephrase to define provisions on the SVA**	accepted
131.	5.6.1.1.1		tec	The phrase "The rationale of the algorithm described below are given in [i.4]" is not necessary for the specification.	**Delete** "The rationale of the algorithm described below are given in [i.4]" And the related reference i.4	Accepted
132.	4.1.2.2.1		tech	Changes in 4.1.2.2.1, not listed in comment document	BES shall contain• the document, or document hash	rejected. This gets complicated here. A detached signature doesn’t contain any of them. Need to allow them since a countersignature may be detached and thus does not contain any of them.
133.	2.2	[i.4]	Technical	A normative text in 5.6.1.1.1 contains a reference to an informative document [i.4]. Not acceptable to make the informative reference as a source of information for description of normative rules. Text of the informative document [i.4] is not accessible as a document.	Delete [i.4] from: Subclause 2.2 and Subclause 5.6.1.1.1.	accepted
134.	3.2		Editorial	OCSP does not mean Online Certificate Status Provider but Online Certificate Status Protocol	Replace Provider with Protocol according to RFC 6960 in many paragraphs.	accepted
135.	4.1.1.1		Technical	The definition of Grace Period is incomplete. The note is vague.	There must be a clear sentence with the meaning: Grace Period is used for long term validation systems and it is a period which starts at the time to which the validation is realized and ends when an appropriate CRL or OCSP response is updated after the time to which the validation is realized. The time value when CRL or OCSP response is updated is stored in the field thisUpdate. Grace Period is not applicable for the system where the result is acceptable also when the validation is incomplete and the status can be later changed.	Rejected. The definition of the grace period is fine as it is.

					Or The Grace period is not a fixed time period for application to wait for CRL or OCSP. It is an interval in which an appropriate CRL or OCSP can be received not waiting longer than is defined in Grace period field of e.g. as a cautionPeriod field in a signature policy.	
136.	**4.1.4**	**Note 2**	Technical	A term "not fresh enough" is vague.	Replace all sentences where "fresh" is used with an appropriate text "the revocation information updated after the validation time".	Rejected, since freshness is discussed and it is a policy issue
137.	**4.1.5**		Technical	Formats BES, EPES, T and A in a new EN AdES defined as main formats. Any other experimental formats defined by ESI must be moved to separate a clause for backward compatibility. For example references in C form are not applicable for open systems because a hash value in references is not helpful for downloading referenced values. It is applicable only for local closed systems which are able to manage the database of objects which are referenced from the signature.	Move formats other than BES, EPES, T and A into a separate clause as experimental formats which are not required to be implemented.	Nothing is required to implement. Check if this is made clear or not.
138.	**4.1.7**		Editorial	Typo, delete "two". Add AdES examples.	Replace with "which fall into ~~two~~ basic categories: • independent signatures (XAdES, parallel CAdES); • embedded signatures (PAdES, CAdES or XAdES of any AdES) • countersignatures "	Accepted with changes: Two → the following Rest: rejected. No Formats to be named here. Format-agnostic.
139.	**4.2,** **4.3,** **4.4,** **4.5,**		General	Clauses 4.2, 4.3, 4.4, 4.5 are not normative. They are only a kind of report.	Delete clauses 4.2, 4.3, 4.4, 4.5 from the document or move them to another multi part document as a technical report.	Accepted. Whole section rewritten.
140.	**5.1.3**	**Table 2**	Technical	This status TIMESTAMP_ORDER_ FAILURE is applicable only for deprecated types of archiving timestamps techniques.	Delete line with TIMESTAMP_ORDER_ FAILURE	Rejected. This is a generic error message that may also apply in non-deprecated cases.
141.	**5.1.7**		Technical	The concept of revocation freshness is applicable for SSL/TSL online systems. Copy paste of SSL/TSL validation algorithm into the long term signature validation system is not possible. It is not applicable according to EU Member States legislation for long term validation. The concept of revocation freshness is ignoring OCSP. OCSP is not used in algorithm, only CRL fields. The long term validation status must be stable. The concept of revocation freshness is not stable and with different validation data the status can be different.	Delete clause 5.1.7 or any parts where the concept of revocation freshness is used in long term validation.	Rejected. Freshness is a generic concept that is explained in 5.1.7. It applies irrespective of usage of OCSP or CRL.
142.	**5.2.2.4.2**		Technical	TR 102 038 [i.3] will be updated and for that reason must not be included.	Delete sentence "TR 102 038 [i.3] specifies an "XML format for signature policies" that may be automatically processed. "	Accepted
143.	**5.2.3.4**		Technical	An algorithm provides vague results according to vague requirements like a usage of "current date/time" and "is considered fresh".	Delete not deterministic "is considered fresh". In the text there must be included exact rules according to actualization time value stored in CRL or OCSP response in thisUpdate field for validation.	Rejected. Freshness is clearly defined and can be required in a policy
144.	**5.3.4**	**Point 6**	Technical	Old usage of a grace period. The grace period is the maximum interval which is finished when CRL or OCSP response is updated after the time to which the validation is realized.	Correct the algorithm with checking the thisUpdate fields of CRL or OCSP responses.	Rejected. There is no “old usage” of grace period, or we don’t understand the comment.

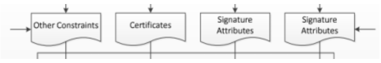
145.	**5.6.1.2.4**		Technical	An algorithm is ignoring OCSP. OCSP is not used in algorithm, only CRL fields. The algorithm provides vague results according to vague requirements like a usage of "is not considered "fresh"".	Delete the rules where a vague "fresh" is included and provide rules according to thisUpdate field of CRLs or OCSP responses.	Rejected. The algorithm does not ignore OCSP. It talks about revocation status information, which covers OCSP. Freshness is clearly defined an needs to be covered since it can be part of the policy.
146.	**5.6.1.3.4.5**		Technical	The usage of a long-term-validation attribute was deprecated with ATSv3.	Update text where long-term-validation will be replaced with ATSv3 objects referenced from ATSHashIndex.	Accepted with modification. The deprecated text may remain since there may be LTV-attributes. ATSv3 needs to be added.
147.	**A.1**	**Table A.3**	Technical	Concept Revocation Freshness is not applicable to long term validation. For LTV is vague.	Delete line with "Revocation Freshness Constraints"	Rejected.
148.	chapter 2.1	Normative references p. 10	T		**Proposal:** **Please Add:** **[24]** OASIS DSS v1.0 Profile for Comprehensive Multi-Signature Verification Reports Version 1.0 Committee Specification 01 (2010)	**Signature Validation report**
149.	Chapter 3.1	Definitions p.12	T	**Current Text:** The definition of “Evidence Record” is missing.	**Proposal: New definition** Evidence Record: An Evidence Record is a collection of evidence compiled for a given archive object over time. An Evidence Record includes ordered collection of Archive Time-stamps (ATS) , which are grouped into Archive Time-stamp Chains (ATSCs) and Archive Time-stamps Sequences (ATSSeqs).	**Accepted with modification. This would need to define the subterms too which are not necessarily used later**
150.	Chapter 5.1	Introduction p.38	T	**Current Text:** The output of the SVA is meant to be processed by the DA (e.g. to be displayed to the verifier). Annex E will specify a structure for a signature validation report in a later version of this draft. There is already an international standard concerning “Comprehensive Multi-Signature Verification Reports” which should be used as basis of a *AdES-Profiling.	**Proposal:** The output of the SVA is meant to be processed by the DA (e.g. to be displayed to the verifier). Annex E will **profile** a structure for a signature validation report **according to [24]** in a later version of this draft.	**Rejected. There will be a new document for the validation report.**
151.	Chapter 5.1	Introduction p.39	E	**Current Text:** Any format-specific processing is specified in 1.	**Question:** What is meant by “1” ?	**Accepted, fixed**
152.	Chapter 5.1.2	p. 40	E	**Current Text:** …a status indication of the results of the signature validation process. Table 1 lists the possible values of the main status indication and their semantics	**Question:** Is **table 1** the right reference ?	**Accepted, fixed**
153.	Chapter 5.5.1	Validation Process for AdES-T Description	T	**Current Text:** Table 15: Inputs to AdES-T validation Input /Requirement • Signature / Mandatory • Signed data object (s) / Optional • Trusted-status Service Lists / Optional • Signature Validation Policies / Optional • Local configuration / Optional • Signer's Certificate / Optional	**Proposal:** **According to CAdES (**ETSI EN 319 122) and **XAdES (**ETSI *EN* 319 102) a Signed data object is mandatory and for example Signature and Signer’s Certificate, etc. are part of the Signed data object **Proposal for Signed Data (CAdES-T):** CMSVersion / Mandatory (M) DigestAlgorithmIdentifiers / M EncapsulatedContentInfo / M eContentType / M eContent / Optional =O	**Rejected. The validation must remain format independent. CAdES-specific validation info has been decided to remain in the CAdES-documents. Also, anything that is optional here may well be mandatory for CAdES.**

					CertificateSet (Certificates) / O RevocationInfoChoices (crls) / O SignerInfos / M **Proposal for Signer Info (CAdES-T):** CMSVersion / M SignerIdentifier / M DigestAlgorithmIdentifier / M SignedAttributes / M SignatureAlgorithmIdentifier / M SignatureValue / M UnsignedAttributes / M	
154.						
155.	Chapter 5.6.2	Long Term Validation Process	E		**Question:** What is meant by clause 8, clause 7, clause 9 , etc. ?	**Accepted, references fixed**
156.	Chapter 5.6.2	Long Term Validation Process	T	**Current Text:** 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 8 for the signature itself and clause 7 for the time-stamps).	**Proposal:** Starting from the most external layer (e.g. the last Archive-time-stamp **or Evidence Record**) to the most inner layer (the signature value to validate), the process performs the basic signature validation algorithm (see clause 8 for the signature itself and clause 7 for the time-stamps).	**Accepted.**
157.	Chapter 5.6.1.3.4.5	Extraction from a long-term-validation attribute	T	**Current Text:** This process applies only to CAdES [1]. If the long-term-validation attribute does not include the poeValue field, no POEs are extracted. If the poeValue field is present with a time-stamp, perform the process below. Processing poeValue field when an ERS [17] is present is out of the scope of the present document.	**Proposal:** This process applies only to CAdES [1]. If the long-term-validation attribute does not include the poeValue field, no POEs are extracted. If the poeValue field is present with a time-stamp, perform the process below. ~~Processing poeValue field when an ERS [17] is present is out of the scope of the present document.~~	**Accepted.**
158.	Chapter 5.6.1.5	Evidence Record Validation Process	T	**Current Text:** The description of an “Evidence Record Validation Process” is missing. The description of the Input is missing.	**Proposal (New):** 5.6.1.5 Evidence Record validation process 5.6.1.5.1 Description This process is used to validate an Evidence Record. For a non-repudiation proof of the data object to be proved, the last Archive Time-Stamp of the Archive Time-stamp Sequence of the Evidence Record MUST be valid at the time of the verification process and the processes described in chapter 5.6.1.5.4 MUST be successful. 5.6.1.5.2 Input	**Considered but the text must be improved.** The current proposal has been integrated without guarantees but has some problems. • SDO (group) as input is not defined. • Unclear what happesn with the current status code as unput • How is the has value of the data object or data object group calculated • Statements like “this algorithm MUST be secure” don’t work in the current structure • Non-repudiation proof is not defined • Needs more proofreading to ensure correctnes and understandability
159.	Chapter 5.6.1.5.2	Input	T	**Current Text:**	**Input** **Requirement**	

<table>
<tr><td></td><td></td><td></td><td></td><td></td><td><table><tr><td>Signed Data object (group)</td><td>Mandatory</td></tr><tr><td>Set of POEs (=Evidence Record(s))</td><td>Mandatory</td></tr><tr><td>The current status indication/Subcode</td><td>Mandataory</td></tr></table></td><td></td></tr>
<tr><td>**160.**</td><td>Chapter 5.6.1.5.3</td><td>Output</td><td>T</td><td></td><td>**Proposal (New):**
5.6.1.5.3 Output
This process outputs one of the following status codes: VALID or NOT-VALID</td><td></td></tr>
<tr><td>**161.**</td><td>Chapter 5.6.1.5.4</td><td>Processing</td><td>T</td><td>**Current Text:**
The description of an “Evidence Record Validation Process” is missing.</td><td>**Proposal (NEW):**
5.6.1.5.4 Processing
An Evidence Record shall prove that an archive object existed and has not been changed from the time of the initial Time-Stamp Token within the first Archive Time-stamp (ATS). In order to complete the non-repudiation proof for an archive object, the last ATS has to be valid and ATSCs and their relations to each other have to be proved. Therefore the following steps are necessary:
1. Verify that the first Archive Time-stamp of the first Archive Time-stamp Chain (the initial Archive Time-stamp) contains the hash value of the data object or data object grooup.
2. Verify each Archive Time-stamp Chain. The first hash value list of each Archive Time-stamp MUST contain the hash value of the Time-stamp of the previous Archive Time-stamp.
Each Archive Time-stamp MUST be valid relative to the time of the following Archive Time-stamp . All Archive Time-stamp s within a chain MUST use the same hash algorithm and this algorithm MUST be secure at the time of the first Archive Time-stamp of the following Archive Time-stamp Chain.
3. 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.
Verify that this Archive Time-stamp was generated before the last Archive Time-stamp of the Archive Time-stamp Chain became invalid.
In order to complete the non-repudiation proof for the data objects, the last Archive Time-stamp has to be valid at the time the verification is performed.
If the proof is necessary for more than one data object, steps 1 and 3 have to be done for all these data objects.
To prove that the Archive Time-stamp Sequence relates to a data object group, verify that each first Archive Time-stamp of the first Archive Time-stamp Chain of the Archive Time-stamp Sequence of each data object does not contain other hash values in its first hash value list than the hash values of the other data objects.
4. To prove that the Archive Time-Stamp Sequence relates to a data object group, verify that the first Archive Time-Stamp of the first Archive Time-Stamp Chain does not contain other hash values in its first hash value list than the hash values of those data objects.
For non-repudiation proof for the data object, the last Archive Time-Stamp MUST be valid at the time of verification process.</td><td></td></tr>
</table>

162.	Chapter 5.6.2.1	Long Term Validation Process Description	T	**Current Text:** An AdES-A (Archival Electronic Signature) is built on an XL signature (EXtended Long Electronic Signature). Several unsigned attributes may be present in such signatures: • Time-stamp(s) on the signature value (AdES-T). • Attributes with references of validation data (AdES-C). • Time-stamp(s) on the references of validation data (AdES-XT2). • Time-stamp(s) on the references of validation data, the signature value and the signature time-stamp (AdES-XT1). • Attributes with the values of validation data (AdES-XL). • Archive time-stamp(s) on the whole signature except the last Archive time-stamp (AdES-A).	**Proposal:** An AdES-A (Archival Electronic Signature) is built on an XL signature (EXtended Long Electronic Signature) **or CMS signature**. Several unsigned attributes may be present in such signatures: • Time-stamp(s) on the signature value (AdES-T). • Attributes with references of validation data (AdES-C). • Time-stamp(s) on the references of validation data (AdES-XT2). • Time-stamp(s) on the references of validation data, the signature value and the signature time-stamp (AdES-XT1). • Attributes with the values of validation data (AdES-XL) • Archive time-stamp(s) on the whole signature except the last Archive time-stamp (AdES-A). • **Evidence Records on part or the whole signature (AdES-A).**	Accepted with modifications (what does the AdES-A at the end of the sentence mean?
163.	Chapter 5.6.2.4	Prosessing	T	**Current Text:** **The following steps shall be performed:** 1. POE initialization: Add a POE for each object in the signature at the current time to the set of POEs**....** **2. Basic signature validation:** Perform the validation process for AdES-T signatures (see clause 9) with all the inputs, including the processing of any signed attributes/properties as specified... 3. If there is at least one long-term-validation attribute with a poeValue, process them, starting from the last (the newest) one as follows: Perform the time-stamp validation process (see clause 8) for the time-stamp in the poeValue: .. 4. If there is at least one Archive-time-stamp attribute, process them, starting from the last (the newest) one, as follows: perform the time-stamp validation process (see clause 8): .. 5. If there is at least one time-stamp attribute on the references, process them, starting from the last one (the newest), as follows: perform the time-stamp validation process (see clause 8):.. 6. If there is at least one time-stamp attribute on the references and the signature value, process them, starting from the last one, as follows: perform the time-stamp validation process (see clause 8): .. 7. If there is at least one signature-time-stamp attribute, process them, in the order of their appearance starting from the last one, as follows: Perform the time-stamp validation process (see clause 8) .. 8. Past signature validation: perform the past signature validation process with the following inputs: the signature, the status indication/subcode returned in step 2, the signer's certificate, the X.509 validation parameters, certificate meta-data, chain constraints, cryptographic constraints and the set	**5.6.2.4 Processing** **Proposal:** The following steps shall be performed: **If there is one or more Evidenc Records, an Evidence Record validation process is done according to chapter 5.6.1.5.4** **otherwise the following steps are to be performed:** 1. POE initialization: Add a POE for each object in the signature at the current time to the set of POEs**....** **2. Basic signature validation:** Perform the validation process for AdES-T signatures (see clause 9) with all the inputs, including the processing of any signed attributes/properties as specified... 3. If there is at least one long-term-validation attribute with a poeValue, process them, starting from the last (the newest) one as follows: Perform the time-stamp validation process (see clause 8) for the time-stamp in the poeValue: .. 4. If there is at least one Archive-time-stamp attribute, process them, starting from the last (the newest) one, as follows: perform the time-stamp validation process (see clause 8): .. 5. If there is at least one time-stamp attribute on the references, process them, starting from the last one (the newest), as follows: perform the time-stamp validation process (see clause 8):.. 6. If there is at least one time-stamp attribute on the references and the signature value, process them, starting from the last one, as follows: perform the time-stamp validation process (see clause 8): .. **7.** If there is at least one signature-time-stamp attribute, process them, in the order of their appearance starting from the last one, as follows: Perform the time-stamp validation process (see clause 8) .. 8. Past signature validation: perform the past signature validation process with the following inputs: the signature, the status indication/subcode returned in step 2, the signer's certificate, the X.509 validation parameters, certificate meta-data, chain constraints, cryptographic constraints and the set of POEs. If it returns VALID go to the next step. Otherwise, abort with the returned indication/subcode and associated	Considered and put in text. Unclear if this works in all cases, i.e. is it either ERs or the other stuff? What if there is a mixture of methods? May not make sense but is it "outlawed"?

				of POEs. If it returns VALID go to the next step. Otherwise, abort with the returned indication/subcode and associated explanations. ..	explanations. ..	
164.						
165.	**2.1 [3]**		**G**	**ETSI TS 012 213 is not the current TSL specification**	**Replace TS 102 231 with TS 119 612**	**accepted**
166.	**2.2 [i.6]** **A.5**		**G**	**Decision 2009/767/EC has been amended**	**Include CD 2013/662/UE, amending the Commission Decision 2009/767/EC**	**accepted**
167.	**5.2.1.3**		**T**	**In signature verification INVALID / FORMAT FAILURE output is missing. This output is referred to in paragraph 5.2.2.2**	**Include INVALID/FORMAT FAILURE output in 5.2.1.3**	**Accepted optionally with changes (TBD)**
168.	**5.2.2.2**		**T**	**Shouldn’t the certificate be an optional input for the VCI process?**		**Rejected, the certificate doesn’t play a role in the processing of this process**
169.	**3.1**		**General**	The term ***Signatory*** should be extended not to be aimed only for smartcards or USB tokens. Currently it is defined that a signatory is a person who holds a signature creation device.	The term *Signatory* should be defined as a person that uses a signature creation device for the purpose of producing an advanced electronic signature	**Accepted with changes** The current definition is not aimed for smart cards and tokens. Adding “for the purpose of producing an advanced electronic signature” → Suggest
170.	**4.1.2.3.4**	**First**	**Editorial**	Missing reference – an advance signature is uniquely linked to the signer (see ???)	Provide a reference (probably to the EC 93/99 directive)	**Accepted but section completely rewritten anyhow**
171.	**4.1.2.3.4.1**	**First**	**General**	The “something the user has” is not included in the list, only “something the user knows” (password) and “something the user is (“biometric”)	The following item should be listed as well: • Ownership based authentication . for example, an OTP device or the mobile phone of the user. This mechanisms should be listed also in 4.1.2.3.4.1.*	**Accepted but section completely rewritten anyhow**
172.	**4.3.4**	**First**	**General**	As the above remark, the list should also include authentication data that the signers owns such as OTP device or a mobile phone	List an OTP device or such as something the signer has that is used for authentication.	**Accepted but section completely rewritten anyhow**
173.	**4.1.2.3.4.1.1**	**First**	**General**	For generality, the SCDev should make sure that the signer is authorized to use…	Remove brackets such that: “…must make sure that the signer is authorised to use the SCDev…”	**Accepted but section completely rewritten anyhow**
174.	**4.3.6.1**		**General**	The list of example devices should also include server side signature SCDev and not a typical single user devices	Extend the listed items to include other technologies such as server-side signature SCDev. As an interface include a secured network communication in addition to link based interfaces such as infrared	**Accepted but section completely rewritten anyhow**
175.	**4.3.8**	**3**	**Editorial**	The sentence **This is even strong** should be changed to **this is even stronger.**	Change to **this is even stronger**	**Accepted but section completely rewritten anyhow**
176.	**Scope**	**1**	**Editorial**	Clauses are note described in the logical order. Clause 1 appears after clause 4.	**Clause 1 introduces the lifecycle of an electronic signature and different forms** **Clause 2 …** **Clause 3 …** **Clause 4 covers signature creation and […]**	**Comment accepted. Scope to be rewritten anyhow.**

177.	**Basic Advanced Electronic Signature (AdES-BES)**	**4.1.2.2.1**	**Editorial**	Sentence not understood: “NOTE 1: Additional mandatory attributes may be format specifically defined.”		**Section has been rewritten**
178.	**Explicit Policy-based Electronic Signature (AdES-EPES)**	**4.1.2.2.2**	**Editorial**	“TODO notes” should be removed from the document.		**Accepted**
179.	**Document Selection**	**4.1.2.3.1**	**Technical**	In all cases, the signer must have the possibility to select the document to sign.		**Section has been rewritten**
180.	**Conceptual Model of Signature Creation**	**Figure 14**	**Technical**	The conceptual model might not be complete: two arrows pointing towards the boxes called “Other constraints” and “Signature attributes” have no origin. The model has two identical boxes called “Signature  Other Constraints Certificates Signature Attributes Signature Attributes		**These open arrows indicate that the driving application may provide additional inputs to the attributes into the signature and also to the constraints.** **The other arrow has been removed.**
181.	**Arbitration**	**4.1.8**	**Technical**	*“In case of arbitration, a form conformant to the –C level or higher provides reliable evidence for a valid electronic signature, provided that:* *when time-stamping in the AdES-T is being used, the certificate from the TSU that has issued the time-stamp token in an AdES-T is not revoked at the time of arbitration“* I Don’t think so : At arbitration time, the –C level or higher signature provides only reliable evidence that the certificate from the TSU **was** not revoked **at the time the time-stamp token was created.**	*“when time-stamping in the AdES-T is being used, the certificate from the TSU that has issued the time-stamp token in an AdES-T was not revoked at the time the time-stamp token was created “*	Arbitration removed fom draft
182.	**Arbitration**	**4.1.8**	**Technical**	*“In case of arbitration, a form conformant to the –C level or higher provides reliable evidence for a valid electronic signature, provided that:* *when time-stamping in the AdES-T is being used, the certificate from the TSU that has issued the time-stamp token in an AdES-T is still within its validity period “* I Don’t think so : The –C level or higher signature provides only reliable evidence that the certificate from the TSU **was** still within its validity period **at the time the time-stamp token was created.**	*“when time-stamping in the AdES-T is being used, the certificate from the TSU that has issued the time-stamp token in an AdES-T was still within its validity périod at the time the time-stamp token was created “*	Arbitration removed fom draft
183.	**Subscriber obligations**	**6.2**	**technical**	*i) the subject's private key has been lost (e.g. by forgetting the PIN number needed to use the key) or stolen; or*	*i) the subject's private key has been lost (e.g. by forgetting the PIN number needed to use the key) or stolen; or compromised*	**Rejected. Text not part of the draft**