Public Review: Resolution of Comments on Draft ETSI TR 119 100 v0.0.2 - 31 May 2014

Business Driven Guidance 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.

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	Resolution on each comment submitted
[Entity 1] 1	all			There cannot be "must" in a TR	**Rephrase to remove any use of "must"**	**Accepted.** Action completed in version 0.0.2.a: changed by “will” or “need to” depending on the specific case.
[Entity 1] 2	Line 24/25		ed	Says twice "based on business requirements"	**Remove** 'based on an analysis of the business requirements' from sentence in line 24	**Accepted the suggestion of improving the two sentences that appear in lines 24 to 28. Indeed some parts of the sentences are repeated.** Action completed in version 0.0.2.a: Now it reads as follows: “This series is based on the selection of the business scoping parameters for each area of standardisation. The selection of these scoping parameters is based on a process involving an analysis of the business requirements and …”
[Entity 1] 3	Line 33/34			This sentence relates to the scope not the introduction	**Remove this sentence**	**Accepted.** Action completed in version 0.0.2.a: Removed the two lines. Reworded first sentence of clause 1.Scope as follows: “The scope of the present document, which addresses area 1 of the Rationalised Framework [i.1], is to propose **a business driven guided process for implementing**

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	Resolution on each comment submitted
						generation and validation of electronic signatures in business' electronic processes"
[Entity 1] 4	Line 42		ed	Missing "signature" at the end of sentence	**Add "signatures"**	**Accepted.** Action completed in version 0.0.2.a: added "signatures" at the end of the sentence.
[Entity 1] 5	Line 44			Remove last word "of"	**Remove last word "of"**	**Accepted. Actually the last of appears in line 45.** Action completed in version 0.0.2.a: deleted the last "of" in line 45

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	Resolution on each comment submitted
[Entity 1] 6	scope		tec	Far too long. 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.	**Replace with** The scope of the present document is to propose a **business driven guided process for implementing generation and validation of electronic signatures in business' electronic processes**. Starting from a business analysis and risk analysis of the business' electronic processes, stakeholders are guided for making the best choice among the wide offer of standards in order to ensure the best implementation of electronic signatures within the addressed application / business e-processes. The target audience includes business managers, application architects, systems developers and signature policy issuers. All other information currently in the scope should be deleted or moved to clause 4	**Accepted rewording of Scope clause contents to be the ones proposed. Indeed if the scope has to be "succinct so that it can be used as a summary for bibliographic purposes", the current scope is far too long.** **Initially Accepted to move part of the rest of the material to clause 4. The sentences listing the different clauses of the document do not fit in clause 4. Check with editHelp team where the list of the clauses in the document could go if worth.** Implemented actions in version v0.0.2.a: 1. Include as contents of Scope clause the text proposed in this comment. 2. Check with editHelp team if it is appropriate to have a set of sentences listing the clauses of the document with a brief summary of their contents. If so, also ask where this text would better fit. 3. Take the rest of the material that has been deleted from Scope clause and that is not the list of clauses in the document, and move it to clause 4 (this would obviously include any update considered worth: there have been some internal comments addressing the targeted audience that should be taken into account when doing this movement).
[Entity 1] 7	**4.1**		**Ed**	**In title replace "this document" by "the present document"**		**Accepted**. Action completed in version 0.0.2.a: Change implemented.
[Entity 1] 8	**Line 213**			**No capital to "Business"**	**Remove capital letter from "business"**	**Accepted**. Action completed in version 0.0.2.a: Change implemented.

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	Resolution on each comment submitted
[Entity 1] 9	**Line 222**		**ed**	**Replace "it is recommended" by**	**Reword sentence to "The table of content provided in xxx should be used to document the various decisions..."**	**Accepted**. Action completed in version 0.0.2.a: Change implemented.
¥	**Line 227**		**tec**	**Don't understand what" into such a standardised signature policy document" means. What is standardised?**		**Accepted that indeed the "standardised" is not indeed the best word here; it only raises doubts.** Action completed in version 0.0.2.a: Change implemented.
[Entity 1] 11	**Line 229**		**ed**	**Replace "this document" by "the present document"**		**Accepted**. Action completed in version 0.0.2.a: Change implemented.
[Entity 1] 12	**Line 232**		**ed**	**Replace "the figure" by "Figure 1"**		**Accepted**. Action completed in version 0.0.2.a: Change implemented.
[Entity 1] 13	**Line 234**		**ed**	**Replace "these two elements deserve some word" by "these two elements are addressed"**		**Accepted**. Action completed in version 0.0.2.a: Change implemented.
[Entity 1] 14	**Line 247**		**ed**	**Replace "this document" by "the present document"**		**Accepted**. Action completed in version 0.0.2.a: Change implemented
[Entity 1] 15	**Line 252**		**ed**	**"deals" instead of "deal"**		**Accepted**. Action completed in version 0.0.2.a: Change implemented
[Entity 1] 16	**Line 275**		**ed**	**No capital to "business"**		**Accepted**. Action completed in version 0.0.2.a: Change implemented

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	Resolution on each comment submitted
[Entity 1] 17	**Line 276**		**ed**	**"imposes" and not "impose"**		**Accepted**. Action completed in version 0.0.2.a: Change implemented
[Entity 1] 18	**Line 282**		**ed**	**Twice "owned by the signer"**	**Remove 1 occurence**	**Accepted**. Action completed in version 0.0.2.a: Change implemented
[Entity 1] 19	**Lines 253, 295**		**ed**		**Remove "in essence"**	**Accepted**. Action completed in version 0.0.2.a: Change implemented
[Entity 1] 20	**Line 297**		**ed**	**Phase and not phasp**		**Accepted**. Action completed in version 0.0.2.a: Change implemented
[Entity 1] 21	**Line 303**		**ed**	**Remove "standardised"** **Replace "is recommended to be used" by "should"**		**Accepted**. Actions completed in version 0.0.2.a: 1. Removed “standardised”. 2. Replaced “is recommended to be used” by “should be used”
[Entity 1] 22	**Paragraph starting Line 303**		**tech**	**This is the second this recommendation is made (first one in clause 4.1). No duplication please.**	**Remove one occurrence of the recommendation**	**Accepted**. Action completed. Decided to delete the one within clause 4.1 and leave the one at the end of clause 4.2, as this seems a general recommendation for users of the process.
[Entity 1] 23	**Line 321**				**Add "it" in front of "highly unlikely"**	**Accepted**. Action completed in version 0.0.2.a: Change implemented

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	Resolution on each comment submitted
[Entity 1] 24	**Line 324**		**Tec**	**Cannot make any requirement. "it is required to to have completed it" is NOT possible in a TR**	**Rephrase to remove any requirement**	**Accepted.** Action completed in version 0.0.2.a. Reworded to “However, it should have been completed at the end of all the iterations…”
[Entity 1] 25	**Line 326**		**Ed**	**Replace "it is recommended" by "should" statement**	**In a business with a certain degree of complexity this analysis should include...**	**Accepted.** Action completed in version 0.0.2.a: “When dealing with business with a certain degree of complexity this analysis should include the production of a business model, as a way of capturing all its relevant aspects”
[Entity 1] 26	**Line 336**		**Tec**	**In an ETSI standard your don't have different levels of recommendations. A recommendation is a recommendation; it is then up to the implementer to make its decision**	**Replace with "a risk assessment should be conducted..."**	**Accepted**. Action completed in version 0.0.2.a: Change implemented
[Entity 1] 27	**Line 340**		**ed**	**No capital to Policy and Security Requirements**		**Accepted**. Action completed in version 0.0.2.a: Change implemented
[Entity 1] 28	**Line 354**		**ed**	**No capital to "framework"**		**Accepted**. Action completed in version 0.0.2.a: Change implemented
[Entity 1] 28	**Line 354**		**ed**	**No capital to "framework"**		**Accepted**. Action completed in version 0.0.2.a: Change implemented

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	Resolution on each comment submitted
[Entity 1] 29	**Line 360**		**teh**	**Cannot make any requirement**	**Rephrase sentence to remove any requirements**	**Accepted**. Action completed in version 0.0.2.a: Changed the wording of the sentence for avoiding imposing a requirement, but instead, make that it transmits the idea that a complete set of requirements leads to implementing effective solutions. Make it an assertion instead a requirement. Proposal: "A complete set of these requirements is the starting point for the implementation of a solution that effectively supports the electronic business modelled"
[Entity 1] 30	**Paragraph starting Line 364**			**Why don't you say that EN 319 101 applies for this clause? Don't make a recommendation and simply states that it is the applicable document.**	**Rephrase to "EN 319 101... applies to perform this phase"**	**Rejected. This is not an editorial issue: recommending something to readers make them aware that they must have good reasons for not following what is stated in 319 101. The proposed text, could be interpreted as if the usage of 319 101 is merely optional, and in consequence be or not be used without actually needing very good reasons for one choice or the other. Summary: leave the recommendation. BUT change the wording** Proposed disposition: change the text to: "EN319 101 "Policy & Security Requirements for Signature Creation Applications and Signature Validation Applications" [i.8] should be used to perform this task."
[Entity 2] 1.	Title		E	"TR 119 100 V0.0.2 (2013-09)"	Is not "ETSI" missing here?	**Accepted. Indeed ETSI is missing!** Action completed in version 0.0.2.a: Change implemented
[Entity 2] 2.	Entire document		General	The first part of this document (up to clause 4) envisages a scenario far more complex, bordering scare, than it is in the real world for the end user. Please clarify also that, at least in the EUMS, legislations exist addressing most e-signature issues, thus relieving the	It is necessary to explain that most of the security issues hinted to, are actually covered by Certification Authorities, Time Stamping Authorities, preservation service providers, etc. so they are not necessarily to be dealt with by the end user. Again: please make it clear that in most countries SCAs and SVAs already exist in the market that have been developed abiding by	**Accepted to satisfy first two requests. The comment mentions end users as people that could be scared by the complexity of the methodology. However, it is clearly indicated in the document that end users are not part of the audience targeted by this document. The comment identifies**

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	Resolution on each comment submitted
				average user from many problems. A hint to the fact that in the near future a Regulation will be issued in the EU to achieve a more uniform legislative coverage in the EU, would be helpful too. More in general: please bear in mind that readers of this publication, more often than not, are not e-signature experts, so they do need a few comments on the usability of most of the services provided with AdES fields and attributes.	suitable security and policy requirements. If such clarifications are not provided, average end users, in particular managers who are not necessary e-signature experts, would be scared by these first clauses and would shun e-signature definitely. Complement the text with a few comments on the usability of most of the services provided with AdES fields and attributes.	**managers as end users, while the editor does not consider them as such. But the relevant fact for this comment is that there have even been comments claiming that managers should not be part of the targeted audience, and it has been agreed to remove them from this audience. The targeted audience will be better profiled in the next version, and the team thinks that the profiles identified there should not be overwhelmed by the degree of complexity of the document, as most of the targeted readers of this text will have a technical profile. In the end this document is a guide on how to use technical standards within the rationalized framework for implementing/integrating/deploying electronic signatures within business processes.** **As for the third request, it is not completely clear what is precisely requested by "Complement the text with a few comments on the usability of most of the services provided with AdES fields and attributes". Indeed the text identifies what kind of parameters of the business might be satisfied by using certain AdES fields and attributes. However, other comments have been raised (see DPS comments for instance) requesting inclusion of specific comments related to some of these fields and attributes, which the editor thinks might address this comment. If the authors of this request consider that they do not cover what they meant, the editor would kindly ask them to provide more specific requests where they think this information is missing.** Proposed disposition for addresing the first part of the request: 1. Provide text addressing the two first paragraphs of the "proposed change" column in clause 4. It may not be anywhere else as the scope clause will be substantially reduced as

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	Resolution on each comment submitted
						per comment from [Entity 1]retariat [Entity 1] 6. 2. As for the third request, wait for further specific requests by AgID if the processing of comments by DPS do not satisfy it. Action completed in version 0.0.2.a: Added within clause 4.2 (after speaking of policy and security requirements) the following note: NOTE: Readers of the present document are reminded that within the European Union legislation exists addressing the most relevant issues of electronic signatures and that a new Regulation is going to be produced to achieve a more uniform legislative coverage. Additionally, readers are also reminded that Signature Creation Applications and Signature Validation Applications already exist at the market, which have been developed abiding by suitable security and policy requirements, simplifying their usage and integration within complex systems.
[Entity 2] 3.	Clause 1		General	Overly verbose.	Please slim down in particular from line 46 on.	**Accepted.** Pending Action: implement proposed change by [Entity 1] 6. This will leave the Scope clause pretty short and concise.

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	Resolution on each comment submitted
[Entity 2] 4.	Line 42		E	"… creation and the validation of electronic."	Please specify what "electronic" refers to.	**Accepted. Same comment as [Entity 1] 4. It refers to "electronic signature"** Action completed in version 0.0.2.a: added "signatures" at the end of the sentence.
[Entity 2] 5.	Lines 46 – 48		E	Following text is redundant and it only distracts attention. "proposed by this guide is defined in a way that enables stakeholders to identify their requirements in a commonly understood way and facilitates the identification of the solutions to meet those requirements. This is so because the guide"	Please remove specified text.	**Accepted. In fact the essential pieces of information within this sentence have been given in the preceding paragraph so they are in fact redundant. Another issue to take into account is that the Scope will be reworded as suggested in [Entity 1] 6 comment, and as stated in the disposition of that comment, the rest of the material will be moved to clause 4 after its update. Deletion of this sentence will be part of the update** Action implemented in version v0.0.2.a: delete this sentence when moving this part of the material from Scope to clause 4.
[Entity 2] 6.	Page 6	All numbered items	E	Text is too prolix.	Please replace it with the following. "1) Business managers facing the integration of electronic signatures in their business electronic processes 2) Application architects 3) System developers 4) Signature policy issuers NOTE: A signature policy document is a declaration of the practices and rules (to be) used when creating, preserving and validating electronic signatures in a specific context (e.g. business process). It is recommended to use the standardised table of contents provided in ETSI EN 319 172 [i.10] as a way to document the various decisions taken it will help to finalise and formalise the declaration of the practices and rules (to be) used when creating, preserving and validating electronic signatures in the concerned specific context (e.g. business process) into such a standardised signature policy document.	**Partially accepted.** Proposed disposition. 1. Text on signature policy to be included in a note, The final text of this note will be the one obtained after processing comments by [Entity 1] on the corresponding sentences. 2. The commented text is going to be moved to clause 4. In that clause there are also mentions to the targeted audience, so the proposal is to address the targeted audience at that clause, and at the same time that the document provides suggestions on how the different readers types should read the document. Finally, as mentioned before, there are some other profiles captured by the team that shall be included and maybe some of the currently identified will be dropped. Actions implemented in version v0.0.2.a

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	Resolution on each comment submitted
[Entity 2] 7.	Line 82		E/T	"… process, emphasizing 82 the imperative need of developing …" Please …!	"…replace it with "process, starting with developing…"	**Partially accepted. After reconsidering the guidance by editHelp, it has been decided to delete the sequence of paragraphs shortly presenting the clauses of the document.** Actual action implemented in version v0.0.2.a: Deleted the list of paragraphs shortly describing the clauses of the document. The prolix text
[Entity 2] 8.	Lines 151 and 155		E/T	"ETSI TS 119 001: "Electronic Signature Infrastructure; Definitions and abbreviations." Are we sure it is a ***TS***? At page 20 it is a TR. Also the title is different	Please align the title	**Accepted**. Pending action: to put the correct type and title of the document. Actions implemented in version 0.0.2.a: Changed status after checking latest version of 119000: its type of document is actually TR. No mention to 119 001 in page 20 was found. There is only one reference to this document and it is as a TS in page 8.
[Entity 2] 9.	Lines 160, 162, 164		E	"respect" should be replaced with "with respect to"		**Accepted**. Action completed in version 0.0.2.a: Changes implemented.
[Entity 2] 10.	Line 194		E	"guidance documents on selection standards"	Please replace with "guidance documents on selection of standards"	**Accepted**. Action completed in version 0.0.2.a: Change implemented
[Entity 2] 11.	Clause 4.2		E/T	E-signatures are not as complex as the average reader would infer from this clause. Please entirely revise it to adapt it to the actual world.		**Rejected**. **This clause provides an overview of the methodology proposed for properly implement electronic signatures within a certain business, taking into account any kind of requirements that actually do exist (as the legal framework and the security requirements on IT systems, etc). Missing some of them, would lead to non-effective solutions. The sentence is adapted to the actual world, as any targeted reader (including implementers of electronic signatures, or integrators) should be aware**

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	Resolution on each comment submitted
						of. This document does not target final users of electronic signatures but people with enough technical background as not to be overwhelmed by its contents (see observations to comment AgID 2 and modifications to the targeted audience in the next version of the document).
[Entity 2] 12.	Page 11		E/T	The figure is utterly scaring	Please remove it from here, moreover because it is a repetition, being it present being in clause 11.	**Rejected. The figure summarizes the proposed methodology. Figure in clause 11 is a reworked version of the figure putting in relation the methodology and the framework of standards, so it is in fact, different**
[Entity 3] 1			General	Since numerous comments have been made on other drafts, these comments are not as accurate as the others. All comments are important. However, this general comment highlights the most important comments which are marked in yellow below: [1] The draft allows to use a non repudiation certificate for authentication purposes. This is particularly dangerous and thus one line should be deleted. [2] There has been an omission to indicate that the certificate status of time-stamp token (e.g. CRL) should also be placed within the signature, as soon as that is more than one time-stamp token applied to the digital signature. [3] The reason of time-stamping references to validation data has nothing to do with relying parties to		**All these comments are properly dealt with in rows below.**

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	Resolution on each comment submitted
				prove the time when they firstly validated a certain signature. [4] There is currently a misunderstanding about the primary reason for creating an archive format. [5] The description of the validation process omits to make the difference between the validation of an EPES and validation of a BES. The processes are rather different.		
[Entity 3] 2	Section 7.1.2	Line 464	Technical	The Note states: NOTE: At present, electronic signatures may be generated following XML, ASN.1 or PDF syntax. It is quite obvious to conclude that where the data to be signed are specified in one of the aforementioned syntaxes, a reasonable initial choice would be to select the electronic signature defined for that syntax, unless other business parameters clearly recommend to use another one. The note is incorrect and dangerous. If a document is in PDF there can be some good reasons to place the signature outside of the pdf document, in particular using an XAdES signature. In the signature is about an XML document, there may be some good reasons to place it in a pdf document which is then signed in a PAdES structure	Delete the Note.	**Partially accepted. Although the last two sentences tried to go in the direction expressed in the comment, the fact that this comment has been produced is an indication that some readers could read it in the same way as the author of the comment. The editor proposes then not to delete the note, as there is value in providing some discussion on the relationship between the syntax of the data objects to be signed and the syntax of the signatures themselves, but instead to reword it so that this is clear what the author of the comment claims: there will exist use cases where the syntaxes of the data objects to be signed and the syntax of the document will not be the same because of business process requirements** Action implemented in version 0.0.2.a: reworded the note as showing a process: NOTE: At present, electronic signatures may be generated following XML, ASN.1 or PDF syntax. Although implementers could think that where XML data objects need to be signed, XAdES should be used, that where PDF documents need to be signed, PAdES should be used, and where ASN.1 or binary data objects need to be signed, CAdES should be used, the actual truth is that the decision on the signature syntax to be used mainly depends on the specificities of the business process where these signatures are going to be implemented: for instance, under certain circumstances there could be good reasons for taking a PDF document and build an XAdES

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	Resolution on each comment submitted
						signature enveloping it, or conversely for including a XML document within a PDF document and use PAdES signatures. Implementers should, in consequence, take into account the specificities of the business process before making any decision on the format(s) of the signature(s) to be implemented.
[Entity 3] 3	Section 7.2.2	Line 553	Technical	The text states: "In particular, there is a need to be able to distinguish between: • electronic signatures intended for data authentication purposes only, NOTE: The generation of electronic signature for which the expression of the intention to sign is limited to ensure the authentication of the data to which it is associated (signed data object(s)) will serve the same purpose towards natural person signers while being electronic signatures in essence: electronic signatures created as the equivalent of a handwritten signature but not to indicate a will or intention to be legally bound by the content of the data which is signed (this could be an intention to sign a draft, an acknowledgement of receipt, or to indicate authorship or responsibility for a document)". An electronic signature is not intended for data authentication purposes. Lines 562 and later clearly indicate the purposes: "electronic signatures created with	Delete lines 553 to 559.	**Rejected to remove the mention to authentication data, but proposed to improve text.** **Rationale for rejection: two fundamental input documents, namely: ETSI TR 102 045: "Electronic Signatures and Infrastructures (ESI); Signature policy for extended business model", approved by ETSI ESI TC, and CROBIES Work-Package 5.1 Deliverable, explicitly identify electronic signatures for data authentication (i.e. corroboration of origin and integrity of the data). Additionally the European Directive on electronic signatures clearly associates electronic signatures to authentication. The team thinks, in consequence that it is worth keeping this bullet within the text.** **However, when discussing this comment within the team, it has been agreed to make some changes to the text within this clause so that the following principles are clearly stated:** **. The advanced electronic signatures supported by PKI technologies are linked to the signatory.** **. All the AdES signatures have mechanisms for indicating the commitment made by the signer when generating them.**

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	Resolution on each comment submitted
				the intention to sign the associated data (signed data object(s)): as a draft, as an acknowledgement of receipt, as an intermediate approval as part of a decision process, to indicate authorship or responsibility for a document (signed data), to indicate having reviewed a document (signed data), to certify that a document is an authentic copy, to indicate witnessing of someone else signature on the same document (signed data). to indicate having read, approving and being bound accordingly to the content of the data object that is signed etc." Delete lines 553 to 559.		**. Keep the list of different types of commitments and delete the sentence of "being bound by the content" at the end of the clause.** Actions implemented in version 0.0.2.a: Reworded the clause as indicated below: 1. Insert as second paragraph: "Implementers should also take into account that advanced electronic signatures supported by Public Key Infrastructure Technologies, uniquely link them to their signatories. 2. Change second current paragraph by: "Below follow some examples of different commitments:" 3. Delete the NOTE following the first bullet. 4. Delete last sentence of the clause following the last bullet: "and being, as a signatory, bound by the content of the data object that is signed"
[Entity 3] 4	Section 7.2.2.	Line 561	Technical	The text states: • electronic signatures intended for entity authentication purposes only, Entity authentication is performed by signing a challenge hat has no meaning. The challenge is NEVER the hash of a document. It would be particularly dangerous to use a non repudiation certificate to sign some data that is part of an authentication	Delete line 561.	**Rejected.** **The reasons are fundamentally the same as before. Even RFC 5280, when dealing with the key usage extension identifies the "digitalSignature" bit as directly related with "entity authentication service". In addition, the document uses the term "data object" for identifying what is signed. Only in certain specific occasions it uses the term "document". In the clause affected by this**

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	Resolution on each comment submitted
				exchange [1].		**comment, the term "document" is not used when mentioning the "entity authentication"; the term "document" appears only in some of the examples of the different types of commitments. So the text does not contradicts the assertion that in entity authentication what is signed is a nonce (a data object).**
[Entity 3] 5	Section 8.1.2.1	Line 766	Technical	The text states: "However, neither CMS nor CAdES specifications specify what exactly they actually sign under these circumstances. This means that very likely the scope of the signatures has to be specified separately, when specifying the syntax and semantics of the signed data object itself.". This roughly correct, although some terms would need to be changed.	Proposed change: "However, neither CMS nor CAdES specifications contains a mechanism for explicitly referencing signed data objects whihc are external to the signature. This means that the location of the signed data object (when not included within the signature) has to be specified separately. This may be done using ASiC structures (see section 8.2). The format of the signed data object may be specified using the content-hints Attribute defined in section 5.10.3 from CAdES."	**Partially accepted. Accept changing first sentence. Rejected changing the second sentence in clause 8.1.2. BUT add the second sentence proposed in the comment, slightly modified, to clause 8.1.2.3 that deals with detached signatures. See rationale for these dispositions below:** Actions implemented in version 0.0.2.a: 1. To reword the sentence as follows: "However, neither CMS nor CAdES specifications contains a mechanism for explicitly referencing signed data objects which are external to the signature. This means that very likely, under these circumstances, the parts of the enveloping data object actually signed have to be specified separately, when specifying the syntax and semantics of the enveloping data object itself." The reason for not accepting the rewording of the second sentence of the paragraph is that within the TR, the commented paragraph appears in clause 8.1.2 Enveloped Signatures; and that the first sentence of the paragraph commented is: "CAdES signatures may be embedded within objects whose structure is defined in ASN1. As long as this structure defines fields for

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	Resolution on each comment submitted
						embedding them". The proposed amendment speaks about "the location of the signed data object". The context described in this section makes it clear that the location is precisely the bytes that envelop the signature itself, but here the problem is what part of the bytes that envelop the signature are covered by the signature itself, and the second sentence of the text within the TR addresses this issue. 2. Implement the following change in clause 8.1.2.3 Detached signature: Add after: "However, neither CMS nor CAdES incorporate mechanisms that make it explicit any hint on how to retrieve the detached signed data object" The following sentence, which is the second sentence proposed in the comment although slightly changed: "This means that the location of the detached signed data object has to be specified separately. This may be done using ASiC structures (see section 8.2)" with this amendment, and for this use case, the text addresses exactly the issue of the location and not the scope, as in this case, the scope is clear: all the data object will be signed wherever it is located. The text reads: "However, neither CMS nor CAdES incorporate mechanisms that make it explicit any hint on how to retrieve the detached signed data object"

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	Resolution on each comment submitted
[Entity 3] 6	Section 8.1.2.3	Line 794	Technical	The text states: "Unlike CAdES, XAdES inherits the XML Signature mechanisms for explicitly referencing any signed data object, included the detached ones, and in consequence, a standardized way of retrieving such data objects". This is correct, but not sufficient.	Add afterwards: "Such reference may either be absolute or relative. Absolute references do not allow to move the signed data which is usually required when doing electronic transactions. Relative references can only be relative to the location of the XAdES signature, so the signed data object and the XAdES signature need to be moved together. ASiC structures allow to combine more easily the two structures (see section 8.2)".	**Partially Accepted.** **First, the terminology used in the comment is not accurate enough. Strictly speaking, XAdES uses URI references (not references in general) that the implementations parse for building a URI. As the comment seems to claim, URI reference may be absolute or relative. In this later case the URI referenced must be obtained applying an algorithm resolution indicated in RFC 3986, that implies manipulation of the relative URI reference and the base URI.** **Second the third sentence is not correct: it says that the "relative references can only be relative to the location of the XAdES signatures"… this is not true; for instance in ASiC, there are XAdES signatures that use relative URI References and Clause A.6 of ETSI TS 102 918-2 says:** **"When the relative URI contains an absolute path, it is resolved relative to the container root directory** **When the relative URI contains a relative path, it is resolved using the root directory as the base URI, not taking into account the "META-INF" folder where signature metadata are stored"** **In consequence, the base URI for obtaining the referenced URI may change depending on the context.** **Nevertheless, it is considered that the comment brings up to the front an interesting issue, which is that depending on the mechanism used, a signed data object may not be moved, or may be moved in a special way so that the resolution of the referenced URI gives the URI where the data object is located, and the resolution is to incorporate this material.**

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	Resolution on each comment submitted
						Proposed actions: Reword the text as follows: “Unlike CAdES, XAdES inherits the XML Signature mechanisms (URI references) for explicitly referencing any signed data object, included the detached ones, and in consequence, a standardized way of retrieving such data objects. As specified in RFC 3986 URI references may be absolute or relative. Use of absolute URIs does not allow changing the location of the signed data objects. Use of relative URIs does allow changing the location of the signed data objects as long as it is ensured that the URI obtained after completing the reference resolution process is the URI of the new location of the data object. This may be achieved for instance, changing properly also the XAdES signature location. ASiC containers allow carrying within a container both XAdES signatures and detached signed data objects using relative URI references. Within these packages the relative positions between signatures and signed data objects are preserved even if the location of the package (and in consequence of the signatures and the signed data objects) is changed.“
[Entity 3] 7	Section 8.2	Line 851	Typo	The title is: "A container for packaging together signed data objects and signatures on the objects?"	Suppress: ?	**Accepted.** Action completed in version 0.0.2.a: Change implemented
[Entity 3] 8	Section 8.4	Line 887	Technical	The text states: 5) The desired longevity of the signatures, The notion of longevity is not clear. The notion of protection fits better.	Change proposal: 5) The desired protections features for the signatures,	**Partially accepted. The longevity of a signature is a relevant issue. The comment, points out a need: to formally define the term “longevity” applied to electronic signatures. On the other hand it is worth to also include “the desired protections features for the signatures”.**

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	Resolution on each comment submitted
				See a similar comment on another document.		Actions Proposed: 1. Generate a formal definition of the term "longevity" applied to electronic signatures. 2. To keep bullet 5): 3. Add bullet 6) The desired protections features for the signatures Actions implemented in version 0.0.2.a: 1 Keep bullet 5 2 Added bullet "6) The desired protections features for the signatures" 3 Include the term "Electronic signature's longevity" within the clause Definitions. Action pending: Add a formal definition of the term "Electronic signature's longevity"
[Entity 3] 9	Section 8.9.2	Line 1065	Typo	The title is: Including indication of the of signed data object format	Change into: Including indication of the signed data object format	**Accepted** Action completed in version 0.0.2.a: Change implemented
[Entity 3] 10	Section 8.9.3	Line 1081	Typo	The title is: Including indication of the of the signature production place	Change into: Including indication of the signature production place	**Accepted** Action completed in version 0.0.2.a: Change implemented
[Entity 3] 11	Section 8.10	Line 1093	Technical	The title is: Supporting signatures lifecycle The notion of longevity or lifecycle is not clear. The notion of protection fits better.	Change proposal: Supporting signatures protection features	**Rejected. The notion of lifecycle of an electronic signature is formally dealt with within the new EN 319 102: "Procedures for signature creation and validation", whose stable draft for public commenting was completed by 30th November 2013. Clause 4.1 of this document is entirely devoted to**

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	Resolution on each comment submitted
						"Lifecycle of an electronic signature". Additionally, although it is true that the features mentioned in this clause (time-stamps) actually protect signatures against certain threats (among which time, which may see how certain algorithms are broken, and make certain validation material to expire) it is not less true that these threats need to be countered precisely for being able to validate a signature time after it was firstly generated, i.e. for making it possible that the "life" of the signature lasts longer. Also, these features are added after the first generation of the signature, which goes through a number of changes in its contents: Collins dictionary defines life-cycle as: "life - cycle of something like an idea or organization is the series of developments that take place in it from its beginning until the end of its usefulness". The perspective adopted in this business driven guidance is the one of emphasizing the set of features to be incorporated to the signature precisely for enlarging its "usefulness". Action implemented in version 0.0.2.a: 1. Reworded second paragraph of clause "8.10" to: It is, however, not unusual that business processes require that the technical validity of certain electronic signatures may be reassessed during a period of time long enough as to allow expiration or compromise of some PKI tokens (e.g. certificates) used for the validation process itself, or even the break of some cryptographic algorithm used in their generation. These electronic signatures, before being destroyed, go through cycles more complex than the simple cycle generation-initial validation by the signatory– almost immediate validation by the relying party. Instead, some other entities (e.g. arbitrator in case of conflict between the signatory and the relying party) may need to perform ulterior validations during a certain (long) period

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	Resolution on each comment submitted
						before the obligation of allowing this validity reassessing ceases. The advanced electronic signatures formats specified by ETSI satisfy this type of requirements allowing that additional data are added to the signatures after they have been generated for supporting their lifecycles. Part of these data is validation data, i.e., data that has to be used for validating the signature. Part of this data may also be data for increasing signatures' longevity. 2. Added at the end of the clause the following paragraph: Readers are referred to ETSI EN 319 102 [i.10] clause 4.1 for finding more details on electronic signatures lifecycle
[Entity 3] 12	Section 8.10.1	Line 1103	Technical	A section should be added before section 8.10.1. It stresses the importance of the inclusion of a time-stamp token on the signature. The current section 8.10.1 should be renamed 8.10.2.	Proposal for an additional text: "8.10.1 Including time-stamp tokens on the **digital** signature This inclusion allows to demonstrate that the digital signature has been generated before the time indicated within the time-stamp token. This inclusion has already been indicated under section 8.6.2.3. However, it is mentioned again here since it is required to be able to distinguish between : 1) signatures that have been done before or after the end of the validity of the signer's certificate, and 2) signatures that have been done while the certificate was valid or while it was revoked (or suspended). Since a time-stamp token has a limited validity period, it may be required to protect the time-stamp token itself. This may be achieved by using another time-stamp either directly on the previous time-stamp token or by applying	**Accepted. The proposed text has different parts, although closely related:** **1.usefulness of the signature time-stamp as a way to indicate whether the signature was generated during the validation period of the certificates within the certification path.** **2. Use for providing a time when validators make check if certificates within the certification path were valid or not** **3. Weaknesses of time-stamp token as it is a signature and in consequence need to also enlarge its longevity.** **4. Measures to extend time-stamp token longevity: to time-stamp the signature time-stamp token itself and its validation material** **It is accepted to address the first three issues mentioned in the comment, but not the fourth one. This last one should be addressed in clause related to archive time-stamp (a reference will be included in the**

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	Resolution on each comment submitted
					another time-stamp token on a larger structure that includes the times-stamp token. However it must be demonstrated that when the additional time-stamp token has been added, the inner time-stamp token was not revoked. So the revocation status of the certificate to be used to validate the inner time-stamp token need to be captured and included in the signature." Time is lacking for providing more details.	**text). Also these three first issues will be addressed, within clause 8.6.2.3 for making it as much self containing, instead of including a new clause 4 clauses after the presentation of the signature time-stamp. It is also proposed to take some of the text that appears in the informative annex D from EN 319 132-1, which provides rationale for the different XAdES properties (this material comes from rationale text spread through the normative body text of ETSI TS 101 903, which STF 458 has considered worth to move to an informative annex).** Action implemented in version 0.0.2.a: to insert a new clause "8.1.10 time-stamp tokens on the signature" with the following content: "The first measure, within ETSI advanced electronic signature formats, to allow that the technical validity of an electronic signature ma be reassessed during a period of time that goes beyond of the expiration or the revocation of any of the certificates within the certification path of the signer's certificate, is the incorporation of a time-stamp token on the signature before any of the aforementioned events occur. This time-stamp token provides evidence that the signature was properly generated with regards to these two crucial aspects. Validators may, in consequence, prove that the signature was valid even beyond the validity period of any of the certificates within the certification path of the signer's certificate, as long as: 1. they have access to the validation material of the certificates within the certification path of the signer's certificate, and that this material actually proves that at the time indicated within the signature time-stamp token none of them was revoked, and 2. none of the certificates within the certification path of the time-stamp token

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	Resolution on each comment submitted
						signing certificate, have expired and have not been revoked at the time when the validation is performed. In consequence, the signature time-stamp token may enlarge the longevity of a signature at most until the first expiration of a certificate within the time-stamp token certification path (if there has not been any revocation before) If there is the requirement of proving the correctness of the status of the certificates within the time-stamp token certification path beyond this time, then there is the need of extending the time-stamp token longevity. Clause 8.10.3 provides details on a mechanism for such a purpose.”
[Entity 3] 13	Section 8.10.1.2	Line 1128	Technical	The topic of this section is: "Including references to certificate status data " From the current text, it appears that there has been an omission to indicate that the certificate status of time-stamp token (e.g. CRL) should also be placed here, as soon as that is more than one time-stamp token applied to the digital signature [2]. Hopefully, most signatures do not need to be verified beyond the end of validity of the time-stamp token applied to the digital signature and the revocation for the reason "key compromise" is likely to be very seldom.	There is no time to propose a text, since other ENs are impacted as well. This problem should however not be ignored and it would be useful to know how this problem may/will be addressed.	**Accepted.** Actions implemented in version v0.0.2.a: 1. Add text making this clear within clause “Including references to certificate status data”. Below follow the text proposed: “CAdES and XAdES define containers for references to certificate status data. Both define references to OCSP responses and CRLs. They also define a placeholder for references to other types of certificate status data. These containers may include references to certificate status data corresponding to: 1) CA certificates within the certification path of the signer’s certificate, 2) Attribute Authorities certificates (the later ones are required when the signer signs attribute certificates or signed SAML assertions) and the certificates within its

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	Resolution on each comment submitted
						certification path, and 3) Time-stamp tokens certificates already present in the signature at the time of generating these containers, and the certificates within their certification paths. Each reference contains an identifier of the referenced certificate status data and a digest value computed on it using a specific digest algorithm. Relying parties may use this value for checking that the certificate status data retrieved is actually the referenced one. Implementers are referred to clause A.1.2 of EN 319 132 [i.3] part 2, when implementing XAdES signatures. This clause specifies the optional `xades:CompleteRevocationRefe rences` unsigned property, the container for references to certificates within the certification path of the signer's certificate, the time-stamp tokens certificates and the certificates within their certification paths. Also, implementers are referred to clause A1.3.2 of EN 319 132 [i.3] part 2 when the signature contains attribute certificates or signed SAML assertions. This clause specifies the optional `xades:AttributeRevocationRef s` unsigned property, a container able to contain references to the full set of certificate status data that have been used in the validation of the attribute certificate(s) or signed SAML assertions present in the signature. Implementers are referred to clause A1.2.1 of EN 319 122 [i.2] part 2, when implementing CAdES signatures. This

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	Resolution on each comment submitted
						clause specifies the optional `complete-revocation-references` unsigned attribute, the container for references to certificates within the certification path of the signer's certificate, the time-stamp tokens certificates and the certificates within their certification paths. Implementers are referred to clause A.1.4 of EN 319 122 [i.2] part 2 when the signature contains attribute certificates or signed SAML assertions. This clause specifies the optional `attribute-revocation-references` unsigned attribute, the container for references to certificate status corresponding to Attribute Authorities' certificates and the attribute certificates. " 2. Modify clause "Including references to certificates" Below follow the text proposed: " Both CAdES and XAdES signatures define containers for references to: 1) CA certificates within the certification path of the signer's certificate, 2) Attribute Authorities certificates (the later ones are required when the signer signs attribute certificates or signed SAML assertions) and the certificates within its certification path, and 3) Time-stamp tokens certificates already present in the signature at the time of generating these containers, and the certificates within their certification paths. Each reference contains an identifier of the referenced certificate and a digest value computed on it using a specific digest algorithm. Relying parties may use this value

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	Resolution on each comment submitted
						for checking that the certificate retrieved is actually the referenced one. Implementers are referred to clause A1.1 of EN 319 132 [i.3] part 2, when implementing XAdES signatures. This clause specifies the optional `xades:CompleteCertificateReferences` unsigned property, the container for references to certificates within the certification path of the signer's certificate, the time-stamp tokens certificates and the certificates within their certification paths. Implementers are referred to clause A1.3.1 of EN 319 132 [i.3] part 2 when the signature contains attribute certificates or signed SAML assertions. This clause specifies the optional `xades:AttributeCertificateRefs` unsigned property, the container for references to Attribute Authorities' certificates and the certificates within their certification paths. Implementers are referred to clause A.1.1.1 of EN 319 122 [i.2] part 2, when implementing CAdES signatures. This clause specifies the optional `complete-certificate-references` unsigned attribute, the container for references to certificates within the certification path of the signer's certificate, the time-stamp tokens certificates and the certificates within their certification paths. Implementers are referred to clause A.1.3 of EN 319 122 [i.2] part 2 when the signature contains attribute certificates or signed SAML assertions. This clause specifies the optional `attribute-certificate-references` unsigned property, the container for references to Attribute Authorities' certificates and the certificates within their certification paths. " .

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	Resolution on each comment submitted
[Entity 3] 14	Section 8.10.2	Line 1146	Technical	The text states: "Certain business processes may require relying parties to prove the time when they firstly validated a certain signature and, simultaneously, due to the fact that a good part of the validation data required by a relevant number of signatures is the same, also may require not including this validation material within the signatures". This rational is incorrect. The reason of time-stamping references to validation data has nothing to do with relying parties to prove the time when they firstly validated a certain signature. It is to protect the validation data about the possible key compromission of one of the issuers.	Change proposal: "When required by business processes, in order to keep the size of the electronic signatures to a minimum only the references to the validation data are included and thus not the values themselves. When the business requirements require a protection of the validation data against a possible compromission of one of the issuers keys, then a time-stamp token shall be applied over it".	**Partially Accepted. Indeed it is true that time-stamping references actually do protect the references to validation data, and as long as the digest algorithm used within the references is not broken, indirectly protect the referenced validation material. But it is not less true that these time-stamped references prove that the validator has gained access to the validation material and in fact has been able to validate the signature. In consequence the proposal is to include text that points in the direction of what the comment suggests, but still preserving the text on proving the validation time. Also the wording of the text proposed** Actions implemented in version v0.0.2.a: 1. Modify clause “Including references to validation data” as indicated below. The mention to the size of the signatures is better placed within “Including references to validation data”, which is the clause dealing with references. “Certain business processes might advice the signer to incorporate in the signature references of the validation data instead their values, in order to keep the size of the electronic signatures to a minimum. These references incorporate means for individually identifying the validation material and also its digest value computed with a certain hash algorithm. This would facilitate these parties to store the validation data outside the signatures, and still allow their identification and retrieval when validating the signature.” 2. Modify the first paragraph of clause “Time-stamping references to validation data” so that it reads: “Certain business processes may require to safeguard against the possibility of a CA key in the certificate chains ever being compromised.

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	Resolution on each comment submitted
						Under these circumstances, and when the signature incorporates references to validation material, implementers may opt for including references to validation data and time-stamp tokens on them. Using this combination a relying party may prove that at the time instant present within the time-stamp token the signature was safeguarded against the possibility of a CA key in the certificate chain ever being compromised. A relying party may also prove that at the time instant present within the time-stamp token it had gained access to the referenced material."
[Entity 3] 15	Section 8.10.2	Line 1150	Technical	The text states: "Using this combination a relying party may prove that at the time instant present within the time-stamp token it had gained access to the referenced material". This rational is incorrect. The reason of time-stamping references to validation data has nothing to do with relying parties to prove the time when they firstly validated a certain signature [3].	Change proposal: "Using this combination a relying party may prove that at the time instant present within the time-stamp token it has protected the validation data against a possible compromission of one of the issuers keys".	**Partially Accepted. Same rationale as before.** This comment is covered by action implemented to react to comment DP14 s:
[Entity 3] 16	Section 8.10.3	Line 1168	Technical	The text states: "Ensuring longevity and resilience to change of the signatures Certain business processes require large longevity and high change resilience to signatures. Under these circumstances, implementers may opt by building archival forms of electronic signatures". Reading this text is far from being crystal clear.	Change proposal: "8.10.3 Protecting against hash function collisions Using time-stamp tokens provide all forms of protections except one: if the hash function used to compute the digital signature over the signed data is broken (i.e. exhibits hash collisions) or is likely to be broken soon, then before such a situation happens, it is required to use and apply another unbroken hash function. The hash function shall be applied both upon the	**Rejected change of title. Same rationale as before. Accepted to include some parts of the text provided.** Actions implemented in version v0.0.2.a: 1. Change the title of the clause to "Ensuring longevity and resilience to change" 2. Change the first paragraph of the clause as indicated below:

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	Resolution on each comment submitted
				There is currently a misunderstanding about the primary reason for creating an archive format [4]. Using time-stamp tokens provide all forms of protections except one: if the hash function used to compute the digital signature over the signed data is broken (i.e. exhibits hash collisions) then before it is broken it is needed to use another unbroken hash function.	signed data (if it is a detached signature) and over the signature itself. The electronic signature is then augmented with that additional time-stamp token". Time is lacking for providing more details, but important changes are needed.	"Certain business processes require to allow that the technical validity of an electronic signature ma be reassessed during a period of time that goes far beyond of the expiration or the revocation of any of the certificates within the certification paths of the time-stamp token on the signature or the time-stamps on references to validation material, or the brak of some of the algorithms used for their generation. Before any of these situations occur, it is necessary: 1. to incorporate any missing validation material to the signature, 2. to protect all the material required to validate the signature (including the signed data objects and the validation material) generating a new time-stamp token using a stronger digest algorithm if required, and such as the certificates within its certification path enlarge signature's longevity. 3. to incorporate this time-stamp token to the signature This type of time-stamp tokens is known as archive time-stamp token, and the signatures incorporating them are referred to as archival forms of electronic signatures"
[Entity 3] 17	Section 8.14.3	Line 1393	Technical	The text states: "These validation constraints may be defined in different ways: - Using formal policy specifications. An example of such situations is signature policy files containing the signature policy validation expressed in ASN.1 or XML syntaxes as specified in ETSI EN 319 172 [i.10]: "Signature Policies" [i.10]. - Defined explicitly in system	Add the following: "These validation constraints may be obtained through different ways: If the electronic signature which has been received is a BES (Basic Electronic Signature) then the constraints are: 1) derived from the semantics of the signed document using a signature policy that is applicable to the type of document that has been received, or	**Rejected. This clause only provides a high level overview of the contents of ETSI EN 319 102. It is not conceived to provide details on the validation process. The details proposed in the comments go far beyond of the purpose of this clause. They should have been properly dealt with within EN 319 102, whose stable draft for public review was completed at 30th November. It is recommended to read the contents of this comment against the actual contents of the EN 319 102, in order to assess if this comment is still worth to be made within the scope of the EN 319 102 review.**

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	Resolution on each comment submitted
				specific control data: e.g. in conventional configuration-files like property or in-files or stored in a registry or database. - Implicitly by the implementation itself." The text above omits to make the difference between the validation of an EPES and of a BES. The processes are rather different [5].	2) derived from the context under which the signed document has been received. If the electronic signature which has been received is an EPES (Explicit Policy Electronic Signature) then : 1) the signature policy referenced within the electronic signature should be used, or 2) a signature policy corresponding to the reference of the signature indicated within the electronic signature should be used, or 3) a different signature policy may be used, at the risk of the verifier. It may be derived from the semantics of the signed document or from the context under which the signed document has been received.	
[ENTITY 4] 1	**1 Scope**	**Line 42**	**Editorial**	**Missing word "signature"**	**… into account when implementing the creation and validation of electronic signature**	**Accepted with changes. This is a comment already done by other parties. The missing word is "signatures".** Action completed in version 0.0.2.a: Change implemented.
[ENTITY 4] 2	**1 Scope**	**Line 52**	**Editorial**	**Indentation of 4th bullet**		**Accepted. It seems that in other bullets there were two tabs while in the 4th bullet there is only one. However, this text is part of the text that is removed from the scope and that, after processing, should be incorporated to clause 4.** Action to be performed: If this list of bulleted items is moved to clause 4, then assign it the right format according to ETSI styles.
[ENTITY 4] 3	**1 Scope**	**Line 73**	**Editorial**	**he → the**	**It is recommended to use the standardized …**	**Accepted. It seems that in other bullets there were two tabs while in the 4th bullet there is only one.** Action to be performed: If this list of bulleted items is moved to clause 4, then assign it the right format according to ETSI styles

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	Resolution on each comment submitted
[ENTITY 4] 4	**7**	**Line 375**	**Editorial**	**Indentation of first bullet**		**Initially Rejected. In the editor's copy the bullet is actually indented.** Action implemented in version v0.0.2.a. The bulleted list has now the right format according to ETSI styles and all the bulleted items are equally indented.