Public Review: Resolution of Comments on Draft ETSI TR 119 100 v0.0.3. – 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	Line 1194		Ed	Text reads: "signature ma be"	**Text should read "signature may be"**	Accepted.
[Entity 1] 2	Line 1196		Ed	Text reads: "or the brack of"	**Text should read "or the lack of" or rather "or the weakness of"**	Accepted with changes: the word misstyped was: "break" ("break of some of the algorithms")
[Entity 1] 3	Line 741			Text reads: "AdES-NoXML signatures are not allowed to envelop the data object they sign document they sign, by their own"	**Text should read: "PAdES-NoXML signatures are not allowed to envelop the data object document they sign, by their own"**	Accepted

Organization name: [Entity 2]	**Clause/ Subclause**	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change**	**OBSERVATIONS** on each comment submitted
[Entity 2] 1.	**General**		**E and T**		1) Please transform all bullet items lists in numbered items list, for an easier future reference 2) Please take into account all previous [Entity 2] comments from [Entity 2]13 on that have been overlooked. They are to be considered as submitted again.	1)Partially accepted. The editor will review the lists and assess which ones should be changed from non numbered to numbered. 2) Indeed the editor apologizes for that. The actual truth is that they were overlooked just because there was a "copy and paste" error from the original document to the document that served as compilation of all the documents on 119 100 v0.0.2. The editor adds as an annex to this document all the [Entity 2] comments from [Entity 2]13, with the proposed dispositions at the end of the present document.
[Entity 2] 2.	**General**		**E**	Please make all bulleted items lists become numbered items lists for a better future reference.		See resolution on [Entity 2] 1.
[Entity 2] 3.	**Lines 111-116**		**E**	All three instances	"with respect ***to*** the signed"	Accepted. To do: add "to" in the definitions as suggested by the comment.
[Entity 2] 4.	**Line 175**		**E/T**	"… that they ***must*** know in detail for a proper development)" Being this document a TR, the verbal form "must" seems misplaced, albeit it does not set requirements related to the document itself. Propose to use "are supposed to know" instead.		Accepted. Indeed the verbal form must, although does not set a requirement, should not be used. To do: change "must know" to "are supposed to know".
[Entity 2] 5.	**Line 219**		**E/T**	"the data to be signed" ➔ "data object" is better		Accepted. To do: change "data to be signed" to "data object to be signed"

[Entity 2] 6.	**Line 228**		**E**	"… that a signer has to ***detent*** …" "detent" is a substantive, not a verb, meaning: "device that holds one object in a certain position relative to another object"	"detain"	Accepted To do: change "detent" to "detain".
[Entity 2] 7.	**Line 251**		**T**	"which the to be designed signature policy is subordinate" It MUST be clarified that Signature Policies are NOT always necessary, nor even legally required.	Please add at the end: "(where applicable)".	Rejected: there is always a signature policy applicable understood as the set of rules followed for validating the signature….a different story is the existence or not of a signature policy document.

Public Review: Draft Disposition of Comments on Draft ETSI TR 119 100 : Business Driven Guidance for Signature Creation and Validation v0.0.2, for non resolved comments raised by [Entity 2]

Organization name: [Entity 2]	**Clause/ Subclause**	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change**	**OBSERVATIONS** on each comment submitted
[Entity 2] 13.	Lines 259 – 260		E/T	Line 259 reads “data”, while line 260 reads “data object”	Please align terminology	Already accepted in disposition to comment [Entity 2] 5 to v0.0.3
[Entity 2] 14.	Line 268		E	Please replace “detent” with “detain”		Already accepted in disposition to comment [Entity 2] 6 to v0.0.3
[Entity 2] 15.	Lines 270 – 272		E/T	Text “These are business scoping parameters not inherent to the particularities of the business process but consequence of the legal and/or regulatory framework where it is conducted.” Is redundant	Please remove it	Accepted. To do: delete sentence.
[Entity 2] 16.	Lines 272 – 273		E/T	“Lack of consideration of these parameters when defining the strategy for implementing electronic signatures …”	Please change as follows: “Lack of consideration of parameters depending on legal/regulatory framework when defining the strategy for implementing electronic signatures …”	Accepted. To do: reword the sentence as suggested by the comment.
[Entity 2] 17.	Lines 285 . 289		E/T	Text “These Business scoping parameters include: the quality level that the legal/regulatory framework impose to certain signatures of certain business processes, parameters derived from what the legal/regulatory framework establishes with regards to the scope and purposes of signatures, parameters related to the formalities of signing, and those that come from requirements on the longevity and resilience to change of signatures.” Is redundant	Please slim down the document by removing this text	Rejected: this text anticipates the BSPs that are part of this type, just as done in the other types.
[Entity 2] 18.	Line 280		E	Replace “From the actor …” with “Regarding the actor…”		Accepted. To do: reword the sentence as suggested by the comment.

[Entity 2] 19.	Line 291		T	It MUST be clarified that Signature Policies are NOT always necessary, nor even legally required.	Please add at the end: "(where applicable)".	See disposition on the comment Alg ID 7 to v0.0.3
[Entity 2] 20.	Line 297		E	“phasp”	“phase”	Obsoleted by text in v0.0.3. This text does not contain any more “phasp”.
[Entity 2] 21.	Page 13, end of clause 4		T	An important topic is lacking here. Readers must be made aware that, MOST LIKELY, in the marketplace they live in, a number of SCA SVA are already available, not to mention off the shelf products like Adobe Acrobat as far as PAdES is concerned. Without this clarification readers would be definitely scared.	Please add a specification to address the side comment.	Accepted to make mention (maybe in the form of a NOTE) to the fact that there are SCA and SVA applications out there…however do not understand the “add a specification”. This note should be enough and no new mentions to existence of applications should be done in the rest of the document. Proposed note: NOTE: Readers should be aware that Signature Generation Applications and Signature Validation Applications might likely exist in the marketplace they live in. This document highlights a number of relevant aspects that readers should take into consideration also when assessing the suitability of using one of these within their business processes.
[Entity 2] 22.	Line 345		E	“applies”	“apply”	Accepted. To do: change the term.
[Entity 2] 23.	After line 376		T	Please highlight that most likely such SCA and SVA are already available in the market and that these checks have already been done by the applications developers. This is soothing end users, that otherwise would be scared.		Guess that this refers to line 367 instead of 376 due to the fact that 376 is a line of a bulleted item and part of clause 7, whose comments start after this one. Rejected as a mention to the existence of applications has been made before.
[Entity 2] 24.	Clause 7		G	Excellent clause: just small comments.		
[Entity 2] 25.	Lines 375-377		E	“related with”	“related to”	Accepted

[Entity 2] 26.	Clause 7.1.1.2		T	It should, no: "must", be clarified that, apart from some specific cases, time stamping/marking is always recommended to provide signature verifiers with the possibility to ascertain if one signature was generated when its supporting certificate was still valid. This, obviously, applies to the case where such certificate expires or is revoked before the expected verification, but, since one can never be 100% sure his/her certificate won't be revoked in the near future, it is strongly advised to apply time stamps/marks.	Please add the requested clarification	Rejected. It is proposed to give the message that in general a time-stamp/time-mark is recommended. The editor does not share this view. The goal of this clause is to emphasize the need of a careful analysis of the requirements so that the need for a time-stamp/time-mark or not may be derived from this analysis.
[Entity 2] 27.	Line 512		E	"would always be most suitable one"	"would always be the most suitable one"	Accepted
[Entity 2] 28.	Line 582		T	Here it would be useful to repeat previous comment ¡**Error! No se encuentra el origen de la referencia.** on the need of TST/TM to help verifying a signature validity.		Rejected by the same reason.
[Entity 2] 29.	Clause 726		T	Another paragraph should be added to 7.2.6, clarifying that in certain cases providing signatures with technical means to assure them long time validity may not be the only way.	Please add a paragraph clarifying that there are cases where a trusted archival service provider receives signed data objects, ascertains their signatures validity at that moment and securely keeps them henceforth. This TSP will therefore be able to assert in the future that the data object was valid when received and that it has been kept in a trusted way, thus preventing any modification or substitution. Therefore such signature will be valid as long as the TSP keeps it or trusts it to another equally trusted TSP.	Rejected. The text in 7.2.6 implicitly includes this kind of services, as it refers to "archiving" in general, without giving preference to any way/strategy/mechanism.
[Entity 2] 30.	Line 671		T	It should be clarified for each item that in most cases signatures do not require information specified in clause 7.4.1.	Please add "In some cases" at the beginning of the paragraph	Accepted with changes: instead of "in some cases" use "if considered necessary".
[Entity 2] 31.	Lines 695-697	2nd para	E	Sentence "In particular it is suggested to identify whether it is required (or even could be required in a future) allowing that the generation and/or validation of certain signatures applied to certain document to be done, not only in classical environments, but also within mobile environments." is not crystal clear	Please review this sentence the reading of which is somewhat difficult. Maybe some word is missing.	Accepted: consider: "In particular it is suggested to identify whether it is required (or even could be required in a future) allowing that the generation and/or validation of certain signatures should be done, not only in classical environments, but also within mobile environments" It is shorter and the verb tense (should be done) instead (to be done) seems more appropriate.

[Entity 2] 32.	Before clause 8		T	Given the presumable low technical knowledge level of most readers, in particular managers, it would be advisable to add a subclause summarising (at "executive summary" level) the characteristics of "actual" data objects that would be signed with CAdES, XAdES, PAdES, as well as advantages/disadvantages of enveloped, enveloping, detached signatures. Similar summary should be drafted for multiple signatures advantages/disadvantages, as well as of ASiC.		Rejected.
[Entity 2] 33.	Before clause 8		T	It might be useful to add another subclause, highlighting that it is possible to apply separate PAdES signatures to different parts of one pdf document and, finally, to sign the whole pdf document, signatures included, and, possibly, also parts of such document that have not been previously signed. This should be possible with XAdES too.		Rejected.
[Entity 2] 34.	Line 707		E	“and” in “and PAdES” is pleonastic, being part of a bulleted line		Accepted. “and” shall be deleted.
[Entity 2] 35.	Line 811		T	What is proposed in the side cell might slip away from the readers' attention if not specified	Please add: "Additionally, it is possible with PAdES to have different signers signing different parts of the same document and, finally, to have one signer signing the whole or part of such document, including unsigned and signed parts, signatures included."	Rejected. In fact the sentence is not correct. PAdES part 2 clearly specifies: “The signature information shall be embedded into the document itself and the ByteRange shall be the entire file, including the signature dictionary but excluding the PDF Signature itself.” PAdES part 3, in its turn reads: “The ByteRange shall cover the entire file, including the signature dictionary but excluding the PDF Signature itself.” In summary, PAdES signatures conformant to PAdES parts 2, and 3 sign the whole pdf document….not parts of it
[Entity 2] 36.	Line 860		E		“… CAdES, ASiC containers puts in place a mechanism …”	Accepted: “put” instead “puts”
[Entity 2] 37.	Line 885		T	“3) The Independent Assurance on (2),” is not enough: also SSCDs are addressed by certification.	“3) The Independent Assurance on (1) and (2),”	Accepted.

[Entity 2] 38.	Line 928		T	“generated before a certain given time instant” See nearby cell	"... instant. It should be noticed, though, that such time reference can be fraudulently replaced with a subsequent one, signing the data again, disposing of the previous signature. So particular attention should be given when using this feature."	Rejected.
[Entity 2] 39.	Line 934		T	“This proves…”	"This time-stamp token, that is calculated on the signature, proves ..."	Accepted.
[Entity 2] 40.	Line 1075		T	Please ad a paragraph (or sentence) specifying that certain type of attacks can be countered by mime type specification.	"By specifying the mime-type, it is possible to counter attacks based on adding html commands into a pdf, jpg, bmp, etc. file, and changing the filetype in "html". This attack would change the data object presentation, since this file would likely be opened as an html file."	Accepted.
[Entity 2] 41.	Line 1891		E		“8.9.3 1081 Including indication of the signature production place”	Accepted: delete the second “of the” in “of the of the”
[Entity 2] 42.	Line 1102		T	It would be beneficial to the reader, probably not very skilled in e-signatures issues, to add some comments on when these pieces of information can be of use. For example, please refer to next comment on CA certificates. Similar comment could be added regarding CRLs included just after signing time, specifying, for example, that this CRL timing should be chosen carefully to be meaningful and that, where CRLs keep the references to revoked certificates forever, adding this CRL provides little additional information. And so on.		
[Entity 2] 43.	Line 1115		T	It can be added, for completeness sake, that in the EU it is not necessary to fetch the CA certificates at the CA's, since, throughout the EU, Trust Lists are in force, listing, among other things, CA certificates.		Accepted with changes. Add a note in 8.10.2 of version 0.0.4 (new 8.10.2 corresponds to old 8.10.1) Add text
[Entity 2] 44.	Clause 8.10.2		T	Also here it would be beneficial to add some discussion on when this piece of information is useful and when the same goal is achievable differently, say by means of trusted preservation.		Obsoleted by version 0.0.3. Comments were raised to former 8.10.2 Time-stamping references to validation data, which were accepted and implemented. These comments, in editor’s opinion obsolete this comment: new material discussing facts that would justify the usage of such time-stamps, has been added. Within version 0.0.3 the clause is now 8.10.3

[Entity 2] 45.	Clause 8.10.3		T	Also here, a discussion would be useful on trusted data preservation services that may make not necessary to add archive time-stamp tokens.		Accepted to mention the existence of such a service, without further discussion.
[Entity 2] 46.	Lines 1450 – 1452		E/T	The paragraph at issue is not clear	Please review “X.509 Certificate path validation constraints, Additional Chain Constraints, Additional Revocation Constraints, Additional Time-Stamp Trust Constraints, Constraints on X.509 Certificate meta-data, and Cryptographic Constraints”	Accepted: the paragraph should be the last bulleted item of the list, i.e, a building block. To do: reorganize the material.