Public Review: Resolution of comments on Draft ETSI TS 119 101 V0.0.3 – 31 May 2014

Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Electronic 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.

Comments on Draft ETSI 119 101 V0.0.3

Comment number	**Clause/ Subclause**	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change**	**Resolution** on each comment submitted
Commnet 1	**General**		**T**	**Very good TS**! Minor changes are proposed hereinafter, though.		Thanks
Commnet 2	**General**		**T/E**	1) Most often than not, signature policies are assumed as a given, overlooking that in some MS, Italy for example, explicit signature policies are forbidden, acting the applicable legislation as the de facto mandatory one. Please specify "explicit or implicit" wherever signature policies are mentioned, to avoid confusion. 2) Very often ISO/IEC standards are written "ISO xxxxx". Please double check and correct. 3) Is there a reason why in Annex A, and only there, the verbal form "should" is in bold type?		@ 1) **Accepted**, changed in the following places: - Control objective/Controls of SCP 35 - SCP 75, SCP 76 @ 2) **Accepted** and corrected. @ 3) **Accepted**, no there is no reason, this was corrected
Commnet 3	**3.2**		**E**	Please add "DA "		**Accepted**

Commnet 4	**4.1**	**2nd paragraph**	**E**	“see Figure 1 and Figure 2.” Being these figures far away, it would be better to specify they are respectively in clause 7 and 7.2. And why not adding a hypertext cross references?		**Accepted** Add reference to clauses. Move Figure 1 to clause 7.1 since it is signature creation specific. In the Windows file, there is a hypertext reference to the figures, but I’m not sure if this is translated to the pdf.
Commnet 5	**5**	**2nd paragraph**	**T/E**	“General requirements applying only for TSP are covered in …”	“General requirements applying only for TSP ***supporting Electronic Signatures*** are covered in …” Better being specific	**Accepted**
Commnet 6	**5.1**	**1st paragraph**	**E**	“The application *guarantees* that the treatment …” Being this a requirement and being this document a TS, shouldn't the correct verbal form be "shall guarantee"?		**Partly accepted** For this document, we have decided to but the requirements in the controls, and not in the explanatory text or the control objectives. Changed to: It is the responsibility of the application to treat and manager all personal data used is in compliance with Directive 95/46/EC.
Commnet 7	**5.2**	**SS1 – item c)**	**T**	“Be able to select a signature policy if …” Please add "where applicable”. Please do not forget that explicit SigPol are not always necessary and at times are even forbidden by the applicable law.		**Partly accepted** Be able to select a signature policy if more than one is available and, **if applicable**, to be informed of the content of that signature policy. If applicable makes only sense for the second part of the sentence. In the first part we state already that is should apply only if there is more than one signature policy.
Commnet 8	**5.2**	**SS1**	**T**	The newest Regulation text reads: "... ensure that the signatory has sole control over the use of his electronic signature creation data.” Proposal: please reword this sentence accordingly with this latest Regulation text.		**Agreed** to consider such change to the light of the eIDAS adopted text, see foreword
Commnet 9	**5.2**	**Note 2**	**T**	An example may help here: "An example of implicit signature policy is the applicable law."		**Accepted**

Commnet 10	**5.3**		**T**	It might be useful to the reader to add a Note specifying that in ISO 22301 and ISO 22313 useful information can be found on Business Continuity		**Accepted** Added in 5.3 main part: NOTE: Additional information on business continuity can be found in ISO 22301 [**Erreur ! Source du renvoi introuvable.**] and ISO 22313 [**Erreur ! Source du renvoi introuvable.**].
Commnet 11	**6.3**	**Control Objective**	**T**	"trigger suitable security alarms and are recorded, where applicable" This takes into account that in PC based SCA/SVA, it is not 100% guaranteed that security events can be detected, and recorded.		**Accepted**, changed also in ISP 4 **Control objective** Ensure that the information systems handling signature data and the environment of the SCA/SVA are secured against unauthorized access and misuse, **trigger suitable security alarms**, and, **when applicable**, that security events are recorded. **ISP 4:** **Detectable** security-related events shall be logged and monitored. Log files shall be stored and integrity protected in a secure location.
Commnet 12	**6.4**	**SIA 2**	**T**	"components that have been subject to such an attack can be properly *reorganized*." "Reorganising" can be misunderstood as "reset in their original status". Maybe "fixed" is better		**Accepted** **SIA 2:** Provisions shall be made to ensure that SCA/SVA components that have been subject to such an attack can be properly **repaired**.
Commnet 13	**6.5**	**DSS 2**	**T**	It is not ISO/IEC 27001 that "specifies security measures", rather it is ISO/IEC 27002		**Accepted**

Commnet 14	**6.6**	**ATS 2**	**T**	Trivial that this may be, it wouldn't hurt saying that the DA in turn shall log the event at issue.		**Accepted**: If needed, the SCA/SVA shall a) Be able to log the needed events itself; or b) Provide the necessary data to the driving application. In the latter case, the DA shall log the events.
Commnet 15	**Page 17**	**1st paragraph**	**E**		“Their functionality however ~~is~~ shall …”	**Accepted**
Commnet 16	**Page 18**	**SCP 15**	**E**		“I*f* …”	**Accepted**
Commnet 17	**7.1.2**	**SCP 22 2nd bullet**	**T**	A NOTE here would be welcome, explaining that it is advisable to protect the Data Content Type, a.k.a "file type" (i.e. .doc, .xlsx, jpg, etc.) as a signed attribute to prevent recent attacks based on inserting html instructions in the DTBS that, when the data type is replaced with "htm" lead to a completely different presentation		**Accepted** NOTE 1: It is advisable to protect the Data Content Type, a.k.a "file type" (i.e. .doc, .xlsx, jpg, etc.) as a signed attribute to prevent for example recent attacks based on inserting html instructions in the DTBS that, when the data type is replaced with "html" lead to a completely different presentation
Commnet 18	**7.1.2**	**SCP 29**	**T**	“inspect at least the ***major*** components” A NOTE should be added here to explain what are these "major components"		**Accepted**, added: The major components include: 1) The Distinguished Name (DN) of the subject; 2) The serial number; 3) The DN of the issuer;

Commnet 19	**7.1.2**	**SCP 31**	**T**	“it ***should*** verify the revocation” Why "should"? It must be a "shall"! If online access to revocation information is available, this MUST be done. At most the signer's decision can be taken into account, in which case it can be reworded as follows: "... certificate, and the signer does not choose to skip this step, it shall verify ..."		**Rejected** Even when the revocation status was checked before the signature, the certificate can be revoked at the time of the signature. The only way to be sure that the signature was valid is a validation after the signature was created. Checking the revocation status is often more resource expensive than the signature itself. It is better not to do it, when it is not necessary. Thus the “should” was changed into a “may”.
Commnet 20	**7.1.4**	**SCP 45**	**T**	Too generic. Please be more specific, at least by adding an explanatory Note.		**Accepted**, added: EXAMPLE: If the dialog is not clear, the user might enter confidential data into fields which are not secured.
Commnet 21	**7.1.6**	**1st paragraph**	**T**	“is important to guarantee the sole control of the signer” Please refer to Comment 8		**Agreed** to consider such change to the light of the eIDAS adopted text, see foreword
Commnet 22	**7.1.6.1**	**SCP 51**	**T**	“…the secret shall withstand practical guessing and brute force attacks.” This is wishful thinking, in particular as far "brute force attack" is concerned :-): it is wiser to use "should" or to add "consistently with the current cryptography attacks status"		**Accepted** **SCP 51:** For knowledge based Signer Authentication, the secret **should** withstand practical guessing and brute force attacks.
Commnet 23	**7.1.6.1**	**SCP 55**	**T**		“function for ***securely*** changing”	**Accepted**
Commnet 24	**7.1.6.1**	**SCP 58**	**T**		“reuses the last used passwords ***or PINs***”	**Accepted**
Commnet 25	**7.1.6.1**	**SCP 59**	**E**		“that the OTP is ~~send~~ ***sent*** to this number”	**Accepted**

Commnet 26	**7.1.6.1**	**SCP 69**	**T**	“Matching of biometric data should not occur inside the SCA computer.” This is the minimum, since, if the computer is not adequately protected, the reply fed back from the external device where the biometric data matching occurs (smart card or the likes) can be altered in the computer itself. Please add another recommendation (a mandatory requirement is practically unfeasible) to protect as far as possible the computer hosting the DA from attacks. If this requirement has already been specified elsewhere, please add a link to this reference.		**Accepted** **SCP 69:** Matching of biometric data should not occur inside the SCA computer. **Measure shall be in place to protect as far as possible the computer hosting the DA from attacks.**
Commnet 27	**7.1.11**	**SCP 84**	**T**	A reference to TR 119 300 and TS 119 312 would be welcome here		**Accepted**, added NOTE 2: Information on suitable algorithms and the time for which they are considered being secure can be found in TS 119 312 [xx].
Commnet 28	**7.1.13**	**SCP 86**	**T**	“The implementation shall allow the signer to individually display ***each*** SD” The term "each" may be misinterpreted that each SD must be displayed to the signer, which, in an automated signature application, is impractical. Please replace with "any", that means that the signer can choose at his/her own will a few sample documents to be checked.		**Accepted**
Commnet 29	**7.2**		**T**	Chances are that what follows is already covered elsewhere, but if it is so it has not been identified. Please add one simple requirement: all signed attributes shall be verified. A particular case regards the signed "Data Content Type", that should be verified against the signed data file type (see comment to SCP 22.2).		**Rejected**: For many signed attributes it is not clear what should be checked (signing time, an unknown mime type). In some formats, it is possible to have user defined signed attributes, the DA might not know them. Even for the data content type, it is not clear what this means. An application might just validate the signature and might not be able to check the content type.
Commnet 30	**7.2**	**1st paragraph**	**T**	“signature validation policy (SVP)” Please add: “, be it implicit or explicit ,"		**Accepted**

Commnet 31	**7.2**	**3rd paragraph**	**T**		"A signature validation is always based on a***n explicit or implicit*** signature validation policy."	**Accepted** but use "implicit and explicit" to be coherent with first paragraph
Commnet 32	**7.2**	**Paragraph after the billeted items list**	**T**	Not clear, especially if matched against the subsequent paragraph		**Accepted**, changed to: If the signature that is received does not contain a signature policy identifier, then the driving application provides the signature policy.
Commnet 33	**7.2.1**	**SVP 1**	**T**	"It is strongly recommended to use" Verbal form "strongly recommended" is not present in the ETSI Directives. Given the meaning of "recommended", this suffices. Please remove "strongly".		**Accepted**
Commnet 34	**Pag. 28**	**SVP 6 1st item**	**T**	Please take into account ASiC too	"the signed document***(s)*** to verify"	**Accepted**
Commnet 35	**Page 28**	**SVP 6 2nd item**	**T**		"the ***implicit or explicit*** signature validation policy"	**Accepted**
Commnet 36	**7.2.3**	**SVP 10**	**T**	Same as above		**Accepted**, also changed for SCP 9
Commnet 37	**7.2.4**	**2nd paragraph**	**T**		"(e.g. trusted time, ***token***". As a matter of fact "trusted time" conveys the concept of something intangible that cannot be carried along the signed object. "	**Accepted**, agreed that we need a token to include into the signature
Commnet 38	**7.2.4**	**SVP 12 & SVP 13**	**T**		"trusted time ***token***"	**Rejected**, SVP 12 & SVP 13 does not talk about the token covered in the signature, but about the fact that this must be covered by a trusted time.
Commnet 39	**7.2.5**	**1st bullet**	**T**		"requirements and the ***applicable*** Signature Validation Policy (SVP)," ***applicable*** refers both to the dichotomy between explicit and implicit, and to the possibility to choose among more policies	**Accepted**
Commnet 40	**8.2**	**1st paragraph**	**E**		1) "Ensure implementations are compliant ~~to~~ ***with*** the standards" 2) "implementations ~~implementing~~ ***of*** these standards.	**Accepted**

Commnet 41	**8.2**	**TCI 2.5 item (a)**	**T**	A new item should be added here specifying that those who have been previously involved in the tested objects' development shall not have performed the acceptance tests, in a way they could influence the tests results		**Partly accepted**, The proposed text is too strict for small companies. Proposed text: a) Who performed the tests and which test tools have been used, if applicable. **Measure should be in place to separate, as far as possible and according to the size and mean of the company, testing, development and acceptance activities;**
Commnet 42	**9.2**		**E**		"The SCA/SVA can ask for trust services of a Trust Service provide~~*d*~~***r***."	**Accepted**
Commnet 43	**9.3**	**GSM 2.4**	**T**		"shall ~~***not be retained***~~ ***be securely deleted at the session end*** by the Application" This is consistent with the subsequent GSM 2.5	**Accepted**
Commnet 44	**Annex A**	**clause 2**	**T**	It would be useful to add this text after the 1st paragraph: "Additionally, a legislation can be itself a signature policy, an "implicit" one, since where that legislation is in force it is not necessary to specify that signature policy ID."		**Rejected**, We already added in the main document that legislation can be an implicit policy. Annex A is the place for describing a signature application practice statement and not a signature policy
Commnet 45	**Definitions**		**T**	Signature application practice statement is missing in definitions and to the abbreviations	Add this term to the definitions: signature application practices statement: a set of rules applicable to the application and/or its environment implementing the creation, the {upgrade, extension, protection, maintenance, management} and/or the validation of electronic signatures. Note: select the appropriate term to cover the "extension" or "upgrade" of a signature. I personally like "upgrade" but this should be aligned in all RF relevant documents. Add the following abbreviations to the related clause 3: SAPS Signature Application Practices Statement	**Accepted** Add to definitions: signature application practices statement: a set of rules applicable to the application and/or its environment implementing the creation, the upgrade and/or the validation of electronic signatures Add to abbreviations: SAPS Signature Application Practices Statement

Commnet 46	**Annex A**		**T**	Make Annex A normative, clean up text, align with signature policy document	Proposed new version of Annex A	**Accepted** With two small changes: 1.2.2 Domain of applications This clause shall further describe each domain of applications that is considered for the use of the SCA/SVA. 1.5.2 Contact person When the contact point is a person, this clause shall include the: • name, • electronic mail address, • telephone number, and • fax number, if applicable, of the person.
Commnet 47			**General**	Align TS 119 101 with EN 319 102		**Accepted**, however, we need to wait until the structure of EN 319 102 is fixed
Commnet 48	**7.1**			TS 119 101 contains neither Signer Authentication Component (SAC) [which is in the list of abbreviations] nor SCDev/SCA Authenticator (SSA) [which is not in the list of abbreviations]. Was this done on purpose		SAC is used in SCP 57, added it to the list of trusted components. SSA is only conditional in EN 319 102. In any case, once EN 319 102 is fixed, it should be checked if any elements are missing in TS 119.

Comments on Draft ETSI 119 101 V0.0.2

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

Commnet 49	**6.6**		**G or E**	**Clause does not apply in the case if signature creation or validation does not require online service; it could be desktop-based offline application. For example in Estonian DigiDoc Desktop case validation is performed completely offline.**	**Change clause to enable offline SCA or SVA not to produce audit trails**	**No changes required** The audit trail does not need an online connection. It is sufficient to log the event locally. In addition, in the latest version we state that the audit trail is needed when a proof is need. I don't see any problem for off-line applications that don't need a proof of the validation/creation. For the revocation checks in the signature creation, we clearly state that they only apply if an access to the revocation data is possible, thus offline application would not have a problem.