Public Review: Resolution of the comments on Draft ETSI TR 119 200 V0.0.2 – 31 May 2014

Business Guidance for Signature Creation and other related Devices

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	**General Comment**	**Entire Document**	**General**	As specified in TR 119 000 (Rationalized structure for Electronic Signature Standardization) the aim of TR 119 200 is quoted as followed: 'when a stakeholder is facing the need or wish to use or design signature creation devices, it should consider the business scoping parameters and guided selection of standards as described in TR 119 200 on "Business driven guidance for Signature Creation and other related Devices" taking into account business requirements that come from other areas as shown below;' Instead of exploring a variant of options to use signature creation devices, the standard presents only the smartcard as a signature creation device and is full with the terms of the signatory "holding" the signature for the purpose of signing. Also, [i.13], which is referred in this standard (Proposal for a regulation of the…) defines the terminology of sole control usage of the SCD and the usage of server-side signatures. The Server side signatures are only mentioned in clause 7.3 as a future trend.	Investigate and implement business guideless to using server side signatures as an option for the stakeholder as defined in the TR 119 000. There are many outstanding projects in variant countries such as Italy, Austria and the Netherlands as well as implementations that can be provided to show the rationale of when to deploy server side signatures.	The text of reference for the work in M/460 Phase 2 is the European Directive EC/1999/93 on electronic signature, and not the Regulation. The text will be amended to be more technology–neutral. For information, the server side signature is currently investigated within CEN TC24 WG17, to determine which security level and evaluation assurance level could be reached depending on mainly the means of authentication of the signatory.

ENTITY 1	**4.2**	**Last three paragraphs**	**General**	The three last paragraph of section 4.2 are aimed to guide the reader to deduce that the only option to use an SSCD is by using a smartcard. The deduction is based on existing available standards. There are several issues that we find wrong in these statement by definition: • This overrides the technology neutrality of the directive and focus on existing technologies and standards. • There are different implementations of the Electronic signature law in the member states. Some countries, such as Italy, allow using other architectures for an SSCD. For example, the Italian signature law permit using remote signatures (server side signatures. • The new standard, *Security Requirements for Trustworthy Systems Supporting Server Signing – TS 419 241* is in its finalization stage and should be referred.	• The three last paragraphs of section 4.2 should also refer to other technologies such as the server side signatures technology and maybe others. • TS 419 241 should be referred and described. • The Server Side signature, which is implemented in many electronic signature related systems should be described.	The three last paragraphs are dealing with **Secure** signature creation devices (SSCD), and it is commonly implemented with a smart card. The server-based solution is not a SSCD; this is why there are discussions within CEN TC224 WG17 to create a new protection profile for server signing. The text will be amended to reflect the other solutions. The standards are hopefully not necessary technology neutral, since aim is to help the developer to make products. There are different implementations of the Electronic Signature Directive in the Member States; this is why the European Commission proposed to have a Regulation to avoid these different interpretations within national laws, bringing no interoperability and no security level homogeneity.
ENTITY 1	**4.3**	**Whole Section**	**General**	Clause 4.3 has a general title, but practically talks only about smartcards. The terminology of “card”, “card holder” is used.	Either change the title of the section so it is clearly referred to using smartcards in trusted or un-trusted environment or change the content of the section.	The terminology “for end-user” was supposed to clarify the paragraphs which deal with smart card. This will be removed.
ENTITY 1	**5.1**	**Whole Section**	**General**	Although the title is named: “ For end User (SSCD)” it is mostly describes scenarios that relates to Smart Cards. For example, Figure 5, describes variant signature scenarios performed with contact/contactless smartcards.	Either name the sections only for smartcards or extend the section for other typical usages. For example, Figure 4 that explains the relationship between the SCA and the SSCD can be extended for other types of signature devices as well.	See previous resolution of comment.
ENTITY 1	**5.1.1 and throughout the document**	**Internal Bullet number 4 and throughout the document**	**General**	The term “card holder” is used, which mandates using a smartcard.	Should use the term “Signatory” throughout the document	Ok

ENTITY 1	**5.1.3, 5.1.4 and 5.1.5**	**Whole section**	**General**	Not clear the relationship between these sections and the aim of the whole document. For example, why the fact that smartcards are used for EMV or smartcard is used by the US government for physical and logical access has anything to do with signing operation by end users.	Either described the reasoning for this sections or remove them.	The title of the document is “signature creation devices” but also “other devices”, meaning signing devices that could be used to provide other services, as explained in the beginning of section 4.2.
ENTITY 1	**Annex A and Annex B**	**Whole Sections**	**General**	Examples such as the *Austrian Mobile Phone* server side signature system (more than 400,000 users) or other deployment s in other European countries or other worldwide countries should be described as well. Follows a list of public and private organizations in Italy that use server side and qualified signature solutions: - Ministry of Economy - Italy - Ministry of Transport – Italy - Ministry of Interior - Police department – Italy - Ministry of Education – Italy - INAIL - work security institution – Italy - Equitalia - tax collector – Italy - Sisal Spa - bets and games - Italy - Poste Vita Spa - Insurance – Italy - Aruba Spa - Certification authority (remote signature service) – Italy - Actalis Spa - Certification authority – Italy - Postecom Spa - Certification Auhtority (remote signature service) – Italy - Foster Wheeler - engineering – Italy - Val d’Aosta Hospital – Italy And many other organizations in Italy, Spain, The Netherlands and other European Countries	Provide examples of other types of usages for signature creation devices.	The section will be amended.

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	OBSERVATIONS on each comment submitted
ENTITY 1	Whole		General	Generally it looks like whole the raised remarks are addressed, but it is hard to tell from the response to what extent changes will be performed in the document. I would like to cite the intended scope of the document as it appears in the TR 119 000 document: "Signature Creation and Other Related Devices: This area focuses on standards related to Secure Signature Creation Devices as defined in the Signature Directive, on signature creation devices used by Trust Service Providers as well as other types of devices supporting electronic signatures and related services such as authentication."	So, it is very important that the TR-419-200 will be written in the eyes of this sentence and also to have the document be consistent with the full set of L19-2XX set of documents (which BTW also includes today the 419-241 – Trustworthy Systems supporting Server Signing).	Agreed The aspects of server signing are taken into account in the document notably in: - see end of section 4.2 for description of alternative solutions to SSCD, including the Italian case; - the table in section 6.3 adding the standard 419 241; - and the introduction of Annex B, and the Austrian deployment in Annex B.2.3.
ENTITY 1	4.2		General	I have a remark regarding the response: "The title of the document is "signature creation devices" but also "other devices", meaning signing devices that could be used to provide other services, as explained in the beginning of section 4.2.".	I would expect here to see either a device that is used for producing a digital signature or an authentication device that enables you to access a digital signature device for example, using a biometric device to access a digital signature device or a OTP device used for accessing a trusted service. I think that proving a list of other usages of smartcards for example as an EMV card or physical access is not relevant to the 19-2XX section.	The intention of this terminology "other signature-related devices" is to describe signature devices that could offer other security features, including identification or authentication, and is explained in the beginning of section 4.2. These devices are not limited to smart cards implemented as SSCDs. The description of the other services is described in details in the section 5.1; it includes authentication devices and is not limited to smart card. The intention of this section is not to describe a complete list of devices, but rather a list of features other than signature that could be offered by signature devices. The list of standardized and deployed SE in the field of identification is very useful to show the extra-possibility of having other security features (than electronic signature) like identification and perfectly fits with the expectations from the new eIDAS regulation. This shows a SE implemented as a SSCD could be deployed as an identification device.

Entity 2	Page 5		Editorial	Extra “.” at the end		Agreed
Entity 2	Page 8	4.2	Editorial	- encompasses the signature creation device, the secure signature creation device (twice)		Agreed
Entity 2	Page 8	4.2		- « to obtain a legally recognized signature, the signature must be processed with a secure signature creation device » : this sentence is incorrect and should be modified ; the lega recognition is not linked to the use of a SSCD (Art.5.2 Directive). But it is right to indicate the SSCD is part of the conditions to obtain a signature of type 5.1 (QES), which is equivalent to hand-written signature within UE. But the SSCD is not a condition to recognize the signature in a legal way.		Agreed, the sentence is replaced by « An advanced electronic signature based on a qualified certificate and created by a SSCD is equivalent to a hand-written signature and is legally recognized.”
Entity 2	Page 10		Editorial	« may be seen as an key element”		Agreed
Entity 2	Page 11	Figure 4	General	What is DF.CIA		Agreed Description is added below the figure : Dedicated File for Cryptographic Information Application defined in ISO/IEC 7816-15 (application in a card that contains information on cryptographic information objects, other security data elements and their intended use)
Entity 2	Page 14	5.2.1	Editorial	Seems incorrect		Agreed The subsection is not necessary, and removed.
Entity 2	Page 14		Editorial	Is « This concerns trustworthy systems managing certificates for electronic signatures. » at the right place?		Agreed This sentence is removed.
Entity 2	Page 17	6.2.3	Editorial	Missing spage after dot		Agreed
Entity 2	Page 17	6.2.3	Editorial	Do not use two references for the same document, 14890 and 419 212.		Agreed

Organization name: Entity 3	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	OBSERVATIONS on each comment submitted
Entity 3 - 1.	**General**		**E**	Generally speaking, this document is in need of a revision by a native English speaking person		Solved ETSI has reviewed the document.
Entity 3 - 2.	**General**		**E**	Please make all bullet items list as numbered items list, for an easier future reference		Solved This is not systematically relevant. Some numbered items have been added.
Entity 3 - 3.	**General**		**E**	Please move all definitions to clause 2, if necessary rewording the nearby sentences referring to them		Solved Some definitions are needed in the core text, especially as extract of the Directive. Some definitions have been moved to clause 2.
Entity 3 - 4.	**Introduction**	**1st paragraph**	**T**	"standards for electronic signatures." Please add: "and specifications": not only standards (i.e. EN) are addressed to in TS 119 000, but also TS		Rejected The term "standards" is very generic and covers all types of ESO deliverables, including European Standard (EN) but also Technical Specification (TS).
Entity 3 - 5.	**Introduction**	**1st paragraph**	**T**	"electronic signature standards and options" Same as above. Similar comment applies to a number of analogous occurrences of "standard"		See above
Entity 3 - 6.	**Introduction**	**2nd last paragraph**	**E**		"(not exhaustive***ly***)"	Agreed
Entity 3 - 7.	**1**	**2nd bulleted item**	**E**		"will gain a better ~~***and***~~ understanding"	Agreed
Entity 3 - 8.	**4.1**	**1sr paragraph**	**E**		"equivalent to a***n*** hand-written signature"	Agreed

Entity 3 - 9.	**4-1**	**Definition of "electronic signature"**	**T/E**	Please move this definition to clause 2, also rewording the previous paragraph		Agreed Also moved the definition of "advanced electronic signature".
Entity 3 - 10.	**4.2**	**2nd paragraph**	**T/E**	Delete 1st sentence, since its gist is already present in clause 4.1		Rejected This sentence introduces the SSCD.
Entity 3 - 11.	**4.2**	**definitions**	**T/E**	Pleased move all definition to clause 2		Solved Moved definitions for "signature creation device" and "signature validation device" to clause 2, but kept SSCD definition in the current clause; this is not really a definition, but an aggregation of definition and requirements from several parts of the Directive.
Entity 3 - 12.	**Page 8**	**Last paragraph**	**T/E**	"From the definition and the security requirements above, a common~~ly~~ interpretation …" Once moved all definitions to clause 2, please replace "above" with "of a Secure signature-creation device"		Agreed
Entity 3 - 13.	**4-2**	**2nd last para**	**E**		"it can be fully recognized as fully compliant …" Delete one "fully": redundant!	Agreed
Entity 3 - 14.	**4.3**	**3rd paragraph**	**T**	"If the SCA is in un-trusted environment, a device authentication shall be used if …" This is a TR: No "shall"! Try with "should"		Agreed
Entity 3 - 15.	**5**	**1st paragraph**	**E**		"… will highly impact ~~in~~ the selection …"	Agreed
Entity 3 - 16.	**Page 11**	**1st paragraph**	**E**	"(e.g. airport, merchandise, POS). » Merchandise refers to the goods being sold Try with "Shopping malls"		Agreed

Entity 3 - 17.	**Page 11**	**After 2nd bullet item**	**E**	"Signature creation demands the end-user to perform a user verification in order to create a qualified electronic signature." Maybe this paragraph is to be moved up to before the bullet items list and reworded in order to achieve a seamless link to the list itself		Solved The sentence is reworded.
Entity 3 - 18.	**Figure 3**		**E/T**	1) Please provide explanations of the conditional features, more in detail, explaining in what cases they can be overlooked. 2) Please review alignment below the figure		Conditional features in the Figure are removed; this does not bring any additional information to the reader at this level.
Entity 3 - 19.	**Figure 4**		**E/T**	What is this "star" (*) for? Nor it is clear what does the two-pointed arrow mean.		Solved Additional sentence is added before the figure.
Entity 3 - 20.	**5.1.5**	**2nd paragraph after "–Role authentication"**	**E**	"(acc. X.509)" What does "acc" stand for?		Solved acc. is replaced by according
Entity 3 - 21.	**Fig 6**		**T**	Taking into account that among the TR intended users are listed "Business managers", who not necessarily are familiar with this kind of coding, please add a legenda box where "E[K.sym]" and the likes are clarified. Similarly, an explanation of this figure, clarifying that it depicts the secure transmission of a document, by encrypting it with a Private key that is in turn encrypted for the SSCD that renders it in clear to the recipient's PC that eventually decrypts the document, would be useful to such audience. If this description does not fit, this demonstrates that the figure needs being explained: someone else might misunderstand it.		Solved Legend is added to the Figure, explaining the role for symmetric key, asymmetric key pair and document.
Entity 3 - 22.	**5.1**	**Last bulleted items list, first bullet**	**T**	"– the hash value" It is not the hash value (i.e. "digest") that is necessary for a signature verification: this digest is not immediately available since it is exactly the document's digest that is encrypted with the signer's private key, thus producing the raw signature! Replace it with "hash algorithm", by which the verifier is able to re-create the document digest to be compared with the result of the signature decryption,		Solved Replaced by "data to be hashed or digest"

Entity 3 - 23.	**5.2**	**Definition of "Certification-service-provider"**	**E/T**	1) Move this definition to clause 2 2) "an entity or a legal or natural person …" In this domain an "Entity" is either a natural or a legal person, so please remove this repetition.		1) Agreed 2) Rejected, this is exactly the text from the Directive, and cannot be changed.
Entity 3 - 24.	**Pag. 17**	**1st paragraph**	**T**	"certificate must be delivered" Being this a TR. using the verbal form "must" is not to be used. Try this: "is expected to "		Agreed
Entity 3 - 25.	**6.2.1**	**EN 419 261**	**E**	**EN 419 261**Security A blank is missing here		Agreed
Entity 3 - 26.	**6.2.2**	**EN 419 212**	**E**	Identification, Authentication and Electronic Signature (IAS) services. It would be better to "decode" IAS in clause 3		Agreed
Entity 3 - 27.	**6.3**	**3rd paragraph**	**T/E**	"The following standard must be taken …" This is TR: no "Must" nor "shall"! Try with "should"		Agreed
Entity 3 - 28.	**Table 3**		**E**	Please endeavour to have this table in one page only, or, at least, to repeat the table headings in every page		Agreed
Entity 3 - 29.	**7.1**	**1st paragraph**	**E**	"The regulation proposes …"	"The ***R***egulation ***[13]*** proposes …"	Agreed
Entity 3 - 30.	**7.1**	**Definitions**	**E**	Please move these definitions to clause 2 and review accordingly the previous paragraph		Agreed
Entity 3 - 31.	**7.3**	**2nd paragraph**	**T**	"The architecture of possible solutions is currently under development in ETSI ESI." Being these documents under development in ETSI ESI, their title and even document No are already defined, so it would be far better to list them with a caveat that their titles might slightly eventually change.		Solved Added the reference SR 019 020.
Entity 3 - 32.	**B.3.2**	**3rd bulleted item**	**E**	"(la photo n'est pas stockée dans la carte)" Is this to be kept in French? And first of all, is it a meaningful piece of information?		Solved The French text is removed.