Public Review: resolution of public comments on Draft ETSI <TS**> <**119172-1**> V<**009**>**

<Signature Policy Framework**>**

Organization name	**Clause/ Subclause**	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change**	**RESOLUTION** on each comment submitted
A 1.			Ge & Te	The present document ignores the work that has already been done on this topic and omits to re-use it: ETSI TR 102 041 V1.1.1 (2002-02) which is a Technical Report about Signature Policies. The document indicates that there will be three other parts, namely: - Part 2: XML Format for Signature Policies - Part 3: ASN.1 Format for Signature Policies - Part 4: European qualified electronic signature validation policy but does not explain or discuss anything about these other parts and thus their relationships, if any. The content of the present document is not really a framework since its main content is a **NORMATIVE** Annex A for a table of contents for signature policies expressed as human readable documents. It is abnormal that a framework contains a normative annex that is unrelated to the framework. If it is believed that annex A should be normative, then it should be placed in an independent part.	The whole document should be rewritten to take advantage of ETSI TR 102 041 V1.1.1. In particular section 4 "Signature policy definition and scope" should be re-used and these sentences in particular: Signature policy is a set of rules to create and validate electronic signatures, under which an electronic signature can be determined to be valid in a particular transactions context. A signature policy may be written using a formal notation like ASN.1 or in an informal free text form provided the rules of the policy are clearly identified. Note, at that time, the XML format was not yet defined.	**Partly agreed**: The title should indeed better reflect the scope of the document. Suggested to change it into: Signature policies; Part 1: Building blocks and table of contents for human readable signature policy documents. **Rest of comments are rejected**: Having a short text to be displayed to the user to describe/identify/summarise the scope of the applicable policy (per signature or group of signatures covered by the policy) is foreseen. This is the purpose of the "signature policy statement summary" (see Table A.1 e.g. one-pager) that even allows a summary statement (short text). Since 2002, several documents and studies have been issued on signature policies and their implementation in business implementation all recognising the need to address signature policies to be used in the management of multiple signatures within extended business models (e.g. ETSI TR 102 045 "Signature policy for extended business model"). More recently, the CROBIES study, an EC referred input to the execution of Mandate M460 has fully addressed the concept of signature policies in its deliverable "Work Package 5-1 - Guidelines and guidance for cross-border and interoperable implementation of electronic signatures". (**http://ec.europa.eu/information_society/** **newsroom/cf/dae/document.cfm?doc_id=976**) This study recommended "*further work on the standardisation aspects of Signature Policies as the current standardisation framework in this matter is quite incomplete. In particular the following aspects should be considered:*

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted
				However, while TR 102 041 defines in Annex C, a signature policy in an i*nformal free text form*, the new document defines a formal format. However the current document does not address the relationship between : - a signature policy expressed as human readable document, and - a signature policy expressed as machine processable document. In particular in case of differences, which one should have the priority ? In ETSI TR 102 041, the idea was that there was only one expression: the machine processable description whereas the human readable text was a **short text** to be displayed to the user to express only the main features of the policy, e.g. short enough to fit on one page. The new document negates the previous work since it states: When there is a need for expressing a signature policy in a human readable form, **the table of content (ToC) specified in annex A shall be followed** to establish the corresponding signature policy document, ..		*o Taking into account signature flows involving multiples signatures and modelling mechanisms for both human readable and machine processable signature policies;* *o Taking into account trust models based on Trusted Lists and other Trust Service Status Lists;* *o Allow hierarchical (and or nested) use of signature policies;* *o The relationship and mapping between human readable and machine processable signature policies."* Part 1 is mainly extending the concept of signature policy to allow issuers (e.g. business organisations, governments) to cover into one documents the expression of the applicable rules for the creation, augmentation and validation of digital signatures into flows involving multiple signatures. Part 1 does not prevent and even allows to identify different set of rules specific for each signature as part of the flow. It also extend the limited model of TR 102 041 to take into account as well trust models based on Trusted Lists and other Trust Service Status Lists. It is not the scope of Part 1 to describe the relationship and mapping between human readable and machine processable signature policies. This is expected to be done in other parts (2&3) when work on signature creation and validation procedures (EN 319 102) would be finalised as there are evident dependencies. CROBIES study and M460 mandate urged ESO's to better align their deliverables with business domain driven considerations and be less academically or technically driven only. There was a clear need to better link the business domain driven requirements and assist stakeholders in deriving adequate signature policies. This is addressed by TR 119 100 which

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted
				This means that it would not be anymore possible anymore to have a short term description. This is not acceptable. The other content of the current document is section 4 which is **less than two pages**. The single benefit of the document is to recognize the fact that in addition to a creation signature policy and a verification signature policy, there is also a augmentation signature policy.		is referred as a possible method to implement the underlying the analysis of the requirements applicable to the implementation of digital signatures into a specific business electronic process or application domain. The signature policy should be derived from such an analysis.
A 2.	Introduction		Te	The text states: NOTE 2: When not stated otherwise in the present document, "signature" denotes "digital signature". This creates a confusion between digital signature and electronic signature. See also the next comment.	Delete this NOTE, or change into: NOTE 2: When not stated otherwise in the present document, a "signature" denotes "an electronic signature".	**Rejected**. "electronic signature" is used in ETSI ESI deliverables to denotes the legal signatures as defined in Directive 1999/93/EC or Regulation 910/2014. ETSI ESI deliverable focus on digital signature as possible means to implement electronic signatures and/or electronic seals.
A 3.	Section 4 and 3.1	First sentence	Te	The text states: A digital signature is always used in a context, either implicit or explicit, e.g. as part of a business process. The document is talking about "digital signatures" whereas it should talk about "electronic signatures". The definition found in the eIdAS Regulation is the following: 3.23 electronic signature : data in electronic form which are attached to or logically associated with other electronic	The document omits to define an "electronic signature" since it defines something quite strange : (electronic) signature making deliberately a confusion between digital signatures and electronic signatures. As defined, a (electronic**) signature does NOT allow to support signer non-repudiation of signing the data unit (**i.e. as indicated in the third item) since it does not include a key to verify the digital signature, nor a time-stamp token which is necessary to have an upper limit of the time	Accepted with changes: It was foreseen to use the definitions of digital signature as provided in CCITT Rec. X.800 | ISO 7498-2: digital signature: data appended to, or a cryptographic transformation (see cryptography) of a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient.

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted
				data and which are used by the signatory to sign. It is not understandable by technicians, maybe by lawyers ? **The fact an electronic signature cannot be forged by the recipients is fully missing**. In addition, the word "which" does not clearly refer to some previous words in the sentence: "Which are used by the signatory to sign" ? "data in an electronic form" which is rather vague and does not characterize what an electronic signature really is. *In the context of this series of documents*, an electronic signature should rather be defined as: electronic signature : data appended to a data unit, protected against forgery, e.g. by a recipient, that allows a recipient of the data unit to prove the integrity and the origin of the data unit and that include a digital signature generated by a certificate owner. Then the position of the digital signature versus an electronic signature clearly appears: an electronic signature includes a digital signature *but also other data*, before and after augmentation. A digital signature cannot be	when the signature was generated if the public key has been revoked. The two following definition are proposed instead of "(electronic) signature": electronic signature : data appended to a data unit, *protected against forgery, e.g. by a recipient,* which include a digital signature generated by a certificate owner, that allows a recipient of the data unit to prove the integrity of the data unit and *to know* and prove the origin of the data unit. digital signature: data appended to a data unit that allows the recipient of the data unit to prove the source and integrity of the data unit *if it knows the verification data to be used* and protect against forgery e.g. by the recipient . In other words, a **digital signature** is a cryptographic checksum generated using the private key of an asymmetric algorithm. The public key to be used for verification is NOT indicated and has to be known by the recipient. If an ICC (e.g. smartcard) is being used, the ICC generates a digital signature (a string of bits), but does not generate an electronic signature. On the contrary, when an **electronic signature** is being received, the signer is not a priori know and thus the electronic	

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted
				'augmented'.	signature includes a public key certificate which *allows the recipient to identify the signer* and to know which public key should be used, whether the certificate and the public key is trustable (depends from the CA which issued the certificate) and so on. In all the document, most occurrences of "digital signature" should be replaced by "electronic signature".	
A 4.	Section 4. Page 12		Te	The text indicates in a NOTE: NOTE: A signature policy document can cover a group of several signature policies, in which case each signature policy defines the set of rules applicable to one or several signatures to which the same set of rules applies. The case of a policy which applies to multiple signatures should not be addressed in a NOTE. However, it should be remembered that the current definition of "signature policy" is the one indicated in TR 102 041. which is: signature policy: set of rules for the creation and validation of an electronic signature, under which the signature can be determined to be valid. The singular is being used, which means that a signature policy applies to ONE	Add the following definition: "workflow signature policy: signature creation policy, signature augmentation policy, signature validation policy or any combination thereof, applicable to a single document signed by a set of electronic signatures. A new section should detail the content of a workflow signature policy. Annex B.1 (Multiple signatures) from TR 102 041 may be quite useful.	Rejected: the definitions are clear. A signature policy document means a document expressing one or more signature policies in a human readable form. A signature policy means a signature creation policy, a signature augmentation policy, a signature validation policy or any combination thereof, applicable to the same signature or set of signatures [to whom the same set of rules apply]. A signature creation policy is a set of rules, applicable to one or more digital signatures, that defines the technical and procedural requirements for their creation, in order to meet a particular business need, and under which the digital signature(s) can be determined to be conformant. A single signature is ruled by a single set of rules. More than one signature may be ruled by the same set of rules.

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted
				electronic signature, i.e. not several signatures, as the new definition now states: signature policy: signature creation policy, signature augmentation policy, signature validation policy or any combination thereof, applicable to the same signature or set of signatures. Definitions cannot be changed "on the fly" since many companies have implemented and followed the ETSI documents. So a different name should be used instead to designate a policy that applies to a document signed using multiple electronic signatures. Since such electronic signatures are most often produced in a workflow process, it is proposed to use the wording "workflow signature policy". The following definition is proposed: "workflow signature policy: signature creation policy, signature augmentation policy, signature validation policy or any combination thereof, applicable to a single document signed by a set of electronic signatures. A workflow signature policy will *reference* for each possible or mandatory electronic signature,		

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted
				a signature policy. This is of particular importance since different set of rules may apply for each electronic signature. This has also the merit to simplify the description of a signature policy, since it only applies to a single electronic signature.		
A 5.	Whole document		Ge & Te	The current document does not solve the dilemma when there is a difference between the text description and a formal description since it simply ignores the topic. A new idea is being submitted which was not possible to propose in 2002 was the TR was published. There is a need to have a machine processable description of the signature policy and there should be no conflict between the formal description and the text description. This implies that the reference description shall be the machine processable description, while the text description should be derived from the formal description. The description of a signature policy should be done using a XSD schema. Then, when a policy has been described in an XML document using that XSD schema, it is possible to use XSL (Extensible Stylesheet	Part 1 should remove the reference to the coming Part 3: ASN.1 Format for Signature Policies. Part 1 should mention that the XML description of a signature policy is mandatory and that two text descriptions may be derived from the XML description. The automatic tools to be used to transform a signature policy described using an XSD schema into a text format should be defined by ETSI TC ESI. Part 1 should be placed on hold until a new work plan is being established.	The approved strategy at ESI#50 is to start working on the XML format and later produce the ASN.1 version to ensure consistency. Rejected to mandate implementation of machine processable version of the signature policies expressed in a signature policy document as implementers may limit to the human readable version. When there is a need for expressing a signature policy in a machine processable form, the corresponding specifications shall indeed ensure that (or when) a human readable statement is derived from it (then it shall be) describing exactly the same rules as those described in the signature policy document.

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted
				Language). XSL is a set of W3C technologies designed for the transformation and formatting of XML data. It is composed of: XSLT (XML Stylesheet Language Transformation), XPath and XSL-FO (XML Stylesheet Language - Formatting Objets). XSL allows to transform an XML document into a printable document, e.g. PDF or into a displayable document, e.g. HTML. For that purpose, two languages need to be used in sequence : a) XSLT which transforms an XML document into another XML document. b) XSL-FO which is a pagination language. There could be two transformations: a) into a short text description, or b) into a full text description. The last question is whether the ASN.1 description should be maintained or made historical. Since developments will be needed for the workflow signature policy, it does not seem economical to develop such policy using both XML and ASN.1, since when the policy is described using		

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted
				ASN.1 what is visible is the BER which is not possible to interpret for a human being. When XML is being used, at least it is easily possible to see the various components. It is proposed to stop further developments or standardization of signature policies using ASN.1. In other words, Part 1 should remove the reference to the coming Part 3: ASN.1 Format for Signature Policies. However, there exist some tools that allow to map XSD schemas into ASN.1 modules. This would give a path for the few companies using ASN.1 to continue to use BER starting from an XSD schema rather than directly from an ASN.1 description.		
A 6.	Section 4. Page 12		te	The text states: The signature policy document shall at least be provided in the form of a PDF/A-2 document according to ISO 19005-2 [2]. This sentence should be removed. There is no need to have a PDF/A2 document. An HTML document is "as good". Note that a PDF/A1 document would be also "as good", since there is no high quality picture incorporated. A TXT document would also be "as good".	Remove the following sentence: The signature policy document shall at least be provided in the form of a PDF/A-2 document according to ISO 19005-2 [2]. Remove the normative document [2] from the list of normative documents.	Rejected.

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted
				It is premature to say anything about the printable or displayable signature policy before understanding and explaining the articulation between the text description and the processable description of a signature policy. Note also that the current sentence does not prevent to use in addition another format. What will happen if their content is different ? The text is silent.		
A 7.	Section 4. Page 12		te	The text states: It shall be digitally signed according to PAdES baseline signatures TS 103 172 [3] or EN 319 142-1 [1] In order to make sure that the description comes from an authoritative source, it is not necessary to use "a hammer and an anvil". A hash value associated with a hash algorithm is sufficient. It should also be remembered that a PAdES baseline signature is only a format but the verification rules are so flexible in ISO 3200-2 that it is not easy to know against which rules the signature verification will be made. Some software even change automatically the root keys at each new version without saying it. Should a way be described to	Remove the following sentence: It shall be digitally signed according to PAdES baseline signatures TS 103 172 [3] or EN 319 142-1 [1] Remove the normative document [3] and [1] from the list of normative documents. This means that the three referenced normative documents should be removed.	Rejected. A hash value only does not provide same assurance as a digital signature. Actually it is left as option for the signer to implement an electronic signature, an advanced electronic signature, a qualified electronic signature, an electronic seal, an advanced electronic seal, or a qualified electronic seal. Suggesting this could be an option or adding a note.

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted
				be able to verify the integrity of "something", then the use of a hash value associated with a hash algorithm should be made mandatory while the use of any kind of signature should be made optional.		
A 8.	ANNEX A		Ge & Te	Annex A, as it is, should be deleted.	This Annex is not needed, since the content of the "human understandable" policy should be derived from Part 2 dedicated to the XML format of the signature policy. However, in the main body of Part 1, it should be explained how to use automatic tools to derive "human understandable" policies from the XML format of the signature policy.	Rejected. See Row 1.
A 9.	Annex A		ge	Since the whole document should be rewritten, the following comments only give some hints about the topics which should be addressed.		No comment to be disposed.
A 10.	Annex A. Page 20 Section A.3.2.5		Te	The text states: A.3.2.5 BSP (j): Longevity and resilience to change. For each signature identified in the concerned workflow (see BSP(a)), this clause shall describe and specify the expected longevity and resilience to change of the signature such that it is verifiable up to a given period of time. This is not understandable.	Explain differently.	Rejected (clear enough in UK English).
A 11.	Annex A. Page 20 Section		Te	The text states: A.3.2.6 BSP (k): Archival	Explain differently.	Rejected (clear enough in UK English).

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted
	A.3.2.6			For each signature identified in the concerned workflow (see BSP(a)), this clause shall describe and specify archival requirements. This is not understandable.		
A 12.	Annex A. Page 31 Section (m)		Te	The text states: **(m)** LoA on signer authentication **(m)1. X509 Certificate Validation Constraints**: This set of constraints indicates requirements for use in the certificate path validation process as defined in RFC 5280 [i.13]. These are certainly the most important constraints .... which are buried inside the document, since it is necessary to wait until page 31 to find them. However, this is missing the main point since it is necessary to say that it is needed to validate the signer's certificate and the TSU certificates and for that purpose, there is a need to validate separately: a) the signer's certificate against one set of trust anchors and of certificate constraints, and b) the TSU certificate against another set of trust anchors and of certificate constraints.	General rules for validating an electronic signature should be indicated in the main body of the document. There is no indication at all about the importance and the need of time-stamping.	Rejected: TR 119 100 is providing guidance on signature creation and validation. EN 319 102 is providing specifications for signature creation and validation procedures. LoA on timing evidences are covered by A.3.2.3 and (h).
A 13.	Annex A. Page 34 Section (n)		Te	The item (n)1. LoAOnSCD should be generalized, since it is a specific extension which is		Rejected: not necessarily related to a specific extension, not related to whether or not the certificate is qualified. Not talking about SSCD

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted
				looked for in a certificate. In some cases, two extensions are being looked for , e.g. to know whether the certificate claims to be a qualified certificate and claims that the private key is placed in a SCD. This information is currently missing in the XML (and the ASN.1) formats of the signature policy.		but SCDev here.
A 14.	Annex A. Page 41		Te	The text states in editorial note 3: Editorial note 3: Additional commitment types (description, object identifier, URI) could be defined including but not limited to cover the fact that: - (...) - the signature is intended for entity authentication purposes only, or It is quite strange to read such a note, since an electronic signature is not intended to support entity authentication since different certificates SHALL be used for authentication and non repudiation.	Please delete : - the signature is intended for entity authentication purposes only, or	Editorial note to be removed before publication.

A 15.	Annex C Page 42		ed	There is currently Annex B (normative): Commitment types Annex C (normative): Commitment types This means two annexes with the same title. The text states: Annex C (normative): Commitment types The following constraints indicates requirements ... The list provided on that page has nothing to do with the title. The title of Annex C is wrong.	Please correct the title of Annex C.	Copy/Paste typo. Title corrected from B comments
A 16.	Annex C Page 42		te	The content of Annex C is inadequate, since all these "constraints" may be indicated by mandating one or more specific extensions in a certificate. So this should be changed by giving the content of these extensions which are "Qualified Certificate Statements". This will allow a much easier check of the content of the certificate.	Change the content of Annex C accordingly to the comment.	Rejected as nothing mandates CSPs issuing QCs to use QcStatements defined by ETSI. This may be implemented differently. The constraints are therefore generalised to cover the base requirements.

Org° name	**Clause/ Subclause**	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change**	**RESOLUTION** on each comment submitted
B	Annex B		ed	Procedures for requesting allocation of OIDs or URI is detailed here: **https://portal.etsi.org/PNNS.aspx**	Any organization may choose to create its own URIs **and OIDs** for its own specific purposes commitment types. ~~or request ETSI to register a specific commitment description, object identifier and URI.~~ **Any organization may request an object identifier under the etsi-identified--organization node or a URI root as detailed**	OK. Updated accordingly

Org° name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted
					on https://portal.etsi.org/PNNS.aspx.	
B	Annex C		ed	Update title to distinguish from annex B	Commitment types **in the context of EU legislation**	Copy/paste typo: the actual title should be “Constraints in the context of EU legislation”.
B	D.1		ed	Wrong use of may	EXAMPLE 1: A community of users ~~may~~ **can** define as part of a signature policy the applicable requirements with regards to those practices any application will have to meet in order to comply with the community signature policy. EXAMPLE 2: A signature policy ~~may~~ **can** also refer to an external set of practices statements that describes the practices used by an application or an application provider that generate/validate signatures according to several signature policies defined by several communities of users. EXAMPLE 3: A signature policy ~~may~~ **can** also be defined in the context of a specific legal context and define a set of rules to create or validate a signature meeting specific legal requirements (e.g. a qualified electronic signature as defined in the applicable European legislation framework) including specific requirements on signature creation applications (SCAs) and signature validation applications (SVAs) and their environments.	Ok, corrected.