Public Review: Resolution of Comments on Draft EN 319 421 V0.0.1 (2013-11) – 31 May 2014

Policy and Security Requirements for Trust Service Providers providing Time-Stamping Services

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.

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

		General	This is a summary of the main issues. However, see also the next comment which is a major issue. The attempted distinction between a Baseline service and a Qualified service is not adequate The document needs to be restructured to distinguish between two different architectures to build a time-stamping service: one architecture involves three components to build the service component that generates time-stamp tokens, while for the other one all the components are within a single cryptographic module. Currently, both types of implementations exists today. Annex D was informative. Since verification of time stamps beyond the end of the validity of a TSU certificate is necessary, the text has been made normative. The previous text was incomplete and incorrect. It has been corrected and expanded. Note: about 18 hours have been necessary to write these comments.	Much time has been spent to provide new text. A restructuring of several sections from this draft is proposed. A new draft should be resubmitted for public comments (this draft was the first draft : 0.0.1).	--

Title		Major Technical	The title of the document is : "Policy and Security Requirements for Trust Service Providers providing Time-Stamping Services" The series EN 319 411-1 to - 4 is about: "Policy requirements for " There is no need to add "and Security" The title should be changed into: "Policy requirements for Trust Service Providers providing Time-Stamping Services". If this document is published as an EN, no other document covering the same scope could exist in the European countries, because there would already be an EN transposed into a national norm. Any other national norm covering the same scope or not fully compliant to this text could not exist.	Change the title into: "Policy requirements for Trust Service Providers providing Time-Stamping Services". Change the EN into a TS.	REJECTED
		Editorial	The draft is using in many places : "time-stamp policy" and "time-stamping policy".	Change into: "time-stamping policy" everywhere in the document.	OK
Introduction	item 1)	Technical	The text states: "1) during the validity period of the signer's certificate, should the signer's private key be compromised and thus revoked for that reason;" The reason is not specific to key compromised.	Change into: "1) during the validity period of the signer's certificate, should the signer's certificate be revoked before the end of its validity, e.g. because the signer's private key has been compromised;"	OK
Introduction		Editorial	The text states: Another one consists to use a time-stamp which allows to prove that a datum existed before a particular time.	Change into: Another one consists to use a time-stamp token which allows to prove that a datum existed before a particular time.	OK

Introduction		Editorial	The text states: "The electronic time stamp is gaining .."	Change into: "Time-stamping is gaining ..."	OK
3.1		Technical	The text states: "Time-Stamping Authority (TSA): authority which issues time-stamp tokens" It would be clearer to say: "Time-Stamping Authority (TSA): authority which issues time-stamp tokens using one or more time stamping units (TSUs)".	Change into: "Time-Stamping Authority (TSA): authority which issues time-stamp tokens using one or more time stamping units (TSUs)".	OK

4.4.1		Major Technical	The text states: "The present document specifies a time-stamp policy to meet general requirements for trusted time-stamping services". However, the text from section 3.2 item c) stated: "with a subsequent indicator relating to the relative quality: - "[BTSP]", "[QTSP]" While section 3.1 when indicating "BTSP Baseline Time-Stamp Policy" "QTSP Qualified Time-Stamp Policy" At this stage of reading, it seems that there are two policies, but the reader has still no clue about the rational for each of them, and that information is not present in the introduction. Further reading is necessary to understand, but we are already on page 10/ 32. The explanations are only provided on page 13: "The present document specifies two time-stamp policies: 1) A baseline time-stamp policy (BSTP) for TSAs issuing time-stamp tokens, supported by public key certificates, with an accuracy of 1 second or better. 2) A qualified time-stamp policy (QTSP) for use where a risk assessment justify the additional costs of meeting more onerous requirements of the BTSP. The requirements of which may be used where higher level of service can be justified through risk analysis". The qualified time-stamp policy, as defined, is rather vague. As stated, it is the baseline plus "anything else". So there is not a single qualified time-stamp policy but as many as we want with some enhanced features. They cannot be compared between them, so	In order to build the service component that generates time-stamp tokens, three major parts are needed: 1. a TSU private key, 2. a local UTC time, and 3. signing software that "understands" the Time-Stamping Protocol (TSP) and which generates the TSTs. These parts can be implemented in many ways. Among these ways: a) the TSU private key is protected by a cryptographic module, the local UTC clock synchronized with a UTC time source, while the signing software supported by a server which is connected both to the time source and to the cryptographic module. These three components need to be placed in a physically protected area. b) the TSU private key, the local UTC synchronized with one or more one line untrusted time server(s), the signing software are all placed into the same cryptographic module which does NOT need to be placed in a physically protected area. c) the TSU private key, the local UTC clock synchronized with one or more on line trusted time server(s), the signing software are all placed into the same cryptographic module which does NOT need to be placed in a physically protected area. The cryptographic module is configured in such a way that it can only receive the UTC time from the designated on line trusted time server(s). As an example, this model has been initially invented in the US and implemented in Brasil. The main difference between option b) and option c) is that, in the later case, a time-stamping module can be made operational automatically, whereas for the former case, there needs to be a "time ceremony" for the initial setting of the module (made simultaneously with a key ceremony).	REJECTED QSTP has been removed

4.4.1		Major Technical (Continuation)	The text states: "The present document specifies a time-stamp policy to meet general requirements for trusted time-stamping services".	Proposed change: "The present document specifies two time-stamping policies corresponding to different security requirements".	REJECTED Only one policy
5.1		Editorial	The text states: "Time-stamp token issued in accordance with the present document include a policy identifier which can be used by relying parties in determining the time-stamp token suitability and trustworthiness for a particular application". The word "shall" is missing.	Change into: "Time-stamp tokens issued in accordance with the present document shall include a policy identifier which can be used by relying parties in determining the time-stamp token suitability and trustworthiness for a particular application".	OK

5.1		Technical	The text states: "The present document specifies two time-stamp policies: 1) A baseline time-stamp policy (BSTP) for TSAs issuing time-stamp tokens, supported by public key certificates, with an accuracy of 1 second or better. 2) A qualified time-stamp policy (QTSP) for use where a risk assessment justify the additional costs of meeting more onerous requirements of the BTSP. The requirements of which may be used where higher level of service can be justified through risk analysis." The text should be revised according to the Major Technical previous comment.	Proposed change: "The present document specifies two time-stamping policies corresponding to different security requirements. The first one is called server based policy, while the second one is called security module based policy. 4.4.1.1 Server based policy In this policy, the service component that generates time-stamp tokens is composed of three parts: - a local clock synchronized with a UTC time source, - a cryptographic module that contains one or more TSU private keys, - a server for generating TSTs. These three parts shall be placed in a physically protected area. The security relies on management procedures performed in the secure area that need to be maintained on these three parts during the whole life of this service component. 4.4.1.2 Security module based policy In this policy, the service component that generates time-stamp tokens is composed of a single part: a time-stamping module. The time-stamping module is composed of a cryptographic module that contains: - a local clock synchronized with a UTC time source, - one or more TSU private keys, - hardware and software for generating TSTs. The security relies on management procedures that need to be applied at the time this service component is made operational".	REJECTED QSTP has been removed

5.1		Technical	The text states: "NOTE 1: Without additional measures the relying party may not be able to ensure the validity of a time-stamp token beyond the end of the validity period of the supporting certificate. See annex D on verification of the validity of a time-stamp token beyond the validity period of the TSU's certificate". This note is misplaced. The text should not be in a Note and should be moved in the section dedicated to the relying party.	Delete NOTE 1.	OK
5.1		Technical	The Editor's NOTE 2 should be removed since it is no more needed according to the previous comments.	Delete NOTE 2.	REJECTED KEPT as no QTSP policy is defined yet
5.1		Technical	The text states: "NOTE 3: It is required that a time-stamp token includes an identifier for the applicable policy (see clause 7.3.1)". Since it is a requirement, this cannot be placed within a NOTE.	Change into: "It is required that a time-stamp token includes an identifier for the applicable policy (see clause 7.3.1)".	OK Reworded : Time-stamp token shall include an identifier for the applicable policy (see clause 7.3.1).

5.2		Technical	The text states: "The identifier of the time-stamp policies specified in the present document is: itu-t(0) identified-organization(4) etsi(0) time-stamp-policy(02023) policy-identifiers(1) baseline-ts-policy (1) NOTE: Additional OIDs for qualified time-stamp policy may be added following on the agreement of such a concept in a regulation on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market. By including this object identifiers in a time-stamp token the TSA claims conformance to the identified time-stamp policy. A TSA shall also include the identifier for the time-stamp policy being supported in the TSA disclosure statement made available to subscribers and relying parties to indicate its claim of conformance " The text should be changed according to the previous comments.	Change into: "The identifier of the time-stamp policies specified in the present document are : itu-t(0) identified-organization(4) etsi(0) time-stamp-policy(02023) policy-identifiers(1) server-based-ts-policy (1)" itu-t(0) identified-organization(4) etsi(0) time-stamp-policy(02023) policy-identifiers(1) security-module-based-ts-policy (2)" By including one of these object identifiers in a time-stamp token the TSA claims conformance to the identified time-stamp policy. It may however include a different object identifier and indicate its claim of conformance to one of these policies in the TSA disclosure statement made available to subscribers and relying parties."	REJECTED QSTP has been removed

6.2		Technical	The text states: "NOTE: It is advisable that, when obtaining a time-stamp token, the subscriber verifies that the time-stamp token has been correctly signed and that the private key used to sign the time-stamp token has not been compromised". The case of key compromise is true, but is too specific. Other important controls are also missing. In addition the text should not be placed in a Note since these verifications are necessary.	Change into: "When obtaining a TST, the subscriber shall verify that a certification chain can be constructed from the TSU certificate up to a trusted root, that the TSU certificate is within its validity period and has not been revoked and that the TST has been correctly signed by using the public key contained in the TSU certificate. In addition it shall verify that the TST is current, i.e. either it is close to the current time or it includes the same challenge as the one sent in the request".	OK but reworded in should
6.3	item a)	Technical	The text states: " a) verify that the time-stamp token has been correctly signed and that the private key used to sign the time-stamp has not been compromised until the time of the verification; NOTE: During the TSU's certificate validity period, the validity of the signing key can be checked using current revocation status for the TSU's certificate. If the time of verification exceeds the end of the validity period of the corresponding certificate, see annex D for guidance". The case of key compromise is true, but is too specific. Other important controls are also missing. The case indicated in the Note is the usual case and thus should be placed in the main body of the document rather than in a Note.	Change into: " a) when the time of the verification is within the validity period of the TSU certificate, verify that a certification chain can be constructed from the TSU certificate up to a trusted root, that none of the certificates from the chain of CAs has not been revoked, that the TST has been correctly signed using the public key contained in the TSU certificate and that the TSU certificate has not been revoked using the current revocation status for the TSU's certificate. b) when the time of the verification is outside the validity period of the TSU certificate, verify that a certification chain can be constructed from the TSU certificate up to a trusted root, that none of the certificates from the chain of CAs has not been revoked and that the TST has been correctly signed using the public key contained in the TSU certificate. See annex D (normative) for additional controls which shall be performed".	Rejected This procedures for time-stamp verification are included in EN 319 102

7		Technical	The current table of contents of section 7 is a "pot pourri" that is not fully logical. It is copied below: 7 Requirements on TSA practices 7.1 Practice and Disclosure Statements 7.1.1 TSA Practice statement 7.1.2 TSA disclosure Statement 7.2.1 TSU key generation 7.2.2 TSU private key protection 7.2.3 TSU public key certificate 7.2.4 Rekeying TSU's key 7.2.5 End of TSU key life cycle 7.2.6 Life cycle management of cryptographic module used to sign time-stamps 7.3 Time-stamping 7.3.1 Time-stamp token 7.3.2 Clock Synchronization with UTC 7.3.3 Dissemination of Terms and Conditions 7.4 TSA management and operation 7.3.3 "Dissemination of Terms and Conditions" should be places after section "7.1.2 TSA disclosure Statement". For another reorganization of the structure see the next comment.	Change the general structure into: "7 Requirements on TSA practices 7.1 Practice and Disclosure Statements 7.1.1 TSA Practice statement 7.1.2 TSA disclosure Statement 7.1.3 Dissemination of Terms and Conditions"	OK Reorganized in line with 319 401

7.2		Technical	The title of the section is: "7.2 Key management life cycle" Later on, there is another section called "7.3.2 Clock Synchronization with UTC" These two sections are not at the same level and cannot be dissociated for the security-module-based time-stamping policy. In accordance with section 4.1, it is proposed to have two sections: 7.2 Requirements on the service component that generates time-stamp tokens (Time-stamping provision) 7.3 Requirements on the service component that that monitors and controls the operation of the time-stamping services (Time-stamping management).	Change the general structure into: "7.2. Requirements for Time-stamping provision The requirements are not the same for the server-based time-stamping policy and for the security-module-based time-stamping policy. 7.2.1 Requirements for the server-based time-stamping policy (...) 7.2.2 Requirements for security-module-based time-stamping policy (...) 7.3. Requirements for Time-stamping management (...)". The details for each new section are given hereafter.	REJECTED Only one policy

New section 7.2.1.		Technical	"7.2.1 Requirements for the server-based time-stamping policy The current content is: 7.2.1 TSU key generation 7.2.2 TSU private key protection 7.2.3 TSU public key certificate 7.2.4 Rekeying TSU's key 7.2.5 End of TSU key life cycle 7.2.6 Life cycle management of cryptographic module used to sign time-stamps 7.3 Time-stamping 7.3.1 Time-stamp token 7.3.2 Clock Synchronization with UTC It is proposed to place first the Clock Synchronization with UTC and then the TSU key and finally the section about Time-stamp token which should be recalled Time-stamp token generation and makes use of both. "TSU private key protection" and " Life cycle management of cryptographic module used to sign time-stamps" should be merged together.	Text proposal: "7.2.1 Requirements for the server-based time-stamping policy 7.2.1.1 Clock synchronization with UTC [use the current text from section 7.3.2] 7.2.1.2 TSU key management 7.2.1.2.1 TSU private key protection [use the current text from section 7.2.2, followed by the current text from section 7.2.6. However, change in section 7.2.6 " Time-stamp token signing cryptographic hardware" into "signing cryptographic hardware" " since the module signs a hash and not the data of the TST.] 7.2.1.2.2 TSU key pair generation [use the current text from section 7.2.1. However, item b) fully duplicates the text in the previous section; Change it into: b) The TSU private signing key shall be held and used within a cryptographic module which conforms to the requirements stated in section 7.2.2.1 and which will be used by the TST generation software] 7.2.1.2.3 TSU public key certificate [use the current text from section 7.2.3. However, in item c) there is the following sentence: " with revocation status service that is publicly and internationally available". Delete "internationally" since it is possible to use such a service on a network that is not connected to the Internet] 7.2.1.2.4 TSU key termination [use the current text from section 7.2.5. However, delete item c) which is misplaced and belongs to TST generation] 7.2.1.2.5 TSU key pair rekeying [use the current text from section 7.2.4] 7.2.1.3 Time-stamp token generation [use the current text from section 7.3.1. However, item c) should be deleted (i.e. traceability to at least one of the real time values distributed by a UTC(k) laboratory, since it is too much demanding). It is also possible (and better) to use another text provided later on]	OK - PARTIAL Some comments taken into account

New section 7.2.2		Technical	7.2.2 Requirements for security-module-based time-stamping policy	Text proposal: "7.2.2 Requirements for security-module-based time-stamping policy The service component that generates time-stamp tokens shall be composed of a cryptographic module that contains: - a local clock synchronized with a UTC time source, - one or more TSU private keys, - hardware and software for generating TSTs. A cryptographic module configured in this way is called a time-stamping module. 7.2.2.1 Clock synchronization with UTC The time-stamping module shall ensure that its clock is synchronized with UTC within the declared accuracy. In particular: a) The synchronisation of the time-stamping module's clock with an external UTC time reference shall be performed and checked during a key/time ceremony under dual control and with at least one witness. b) The calibration of the time-stamping module's clock shall be maintained such that the clock shall not be expected to drift outside the declared accuracy. c) The time-stamping module's clock shall be protected against threats which could result in an undetected change to the clock that takes it outside its calibration. NOTE 1: Threats may include tampering by unauthorized personnel, radio or electrical shocks. d) If it is detected that the time indicated in a TST drifts or jumps out of synchronization with UTC, the time-stamping module shall stop time-stamp token issuance. e) When the time-stamping module has stopped time-stamp token issuance because of a drift or a loss of synchronization with UTC, then the time-stamping module can only be made operational again under dual control and if the drift has felt	REJECTED Only one policy

New section 7.2.3		Technical	7.2.2.3 Time-stamp token generation The text proposal is provided in the right column. The same text may be used for the new section 7.2.1.3 simply by changing the beginning of the first sentence into: "The TSA shall ensure ... " rather than : "The time-stamping module shall ensure ..."	Text proposal: "7.2.2.3 Time-stamp token generation The time-stamping module shall ensure that time-stamp tokens are issued securely and include the correct time. In particular: a) if the TST request includes a nonce, the same nonce shall be included in TST response, b) an identifier for the time-stamp policy shall be included in every TST. c) a unique identifier shall be included in every TST. d) the time included in the TST shall be a UTC time synchronized with UTC within the accuracy defined in this policy and, if present, within the accuracy defined in the time-stamp token itself. e) If the time-stamping module's clock is detected as being out of the stated accuracy then time-stamp tokens shall not be issued. f) The TST shall include a hash value together with a hash algorithm identifier of the datum being time-stamped as provided by the requestor. g) The TST shall include: - where applicable, an identifier for the country in which the TSA is established; - an identifier for the TSA; - an identifier for the TSU which issues the time-stamps. h) The TST shall be signed using a key generated exclusively for this purpose. NOTE 1: A protocol for a time-stamp token is defined in RFC 3161 [i.2] and profiled in EN 319 422 [i.4]. NOTE 2: In the case of a number of requests at approximately the same time, the ordering of the time within the accuracy of the TSU clock is not mandated".	REJECTED Only one policy

7.4		Technical	This section is called : 7.4 TSA management and operation The previous (new section) is called: "7.2. Requirements for Time-stamping provision As indicated earlier, there should now be a section called: 7.3. Requirements for Time-stamping management	Text proposal: "7.3. Requirements for Time-stamping management Unless otherwise indicated, the requirements are the same for the server-based time-stamping policy and for the security-module-based time-stamping policy. [Sections 7.4.x can then be re-used by changing their numbering into 7.3.x. However, the current section 7.4.4 "Physical and environmental security" is not the same for the server-based time-stamping policy and for the security-module-based time-stamping policy. The text proposal is provided in the next comment.]	REJECTED Only one policy

New section 7.3.4		Technical	7.3.4 Physical and environmental security :	Text proposal: "7.3.4 Physical and environmental security The requirements identified in EN 319 401 [8], clause 6.4.4 shall apply. In addition the following particular requirements apply: a) The following additional controls shall be applied to time-stamping management: - The time-stamping management facilities shall be operated in an environment which physically protects the services from compromise through unauthorized access to systems or data. - Any persons entering this physically secure area shall not be left for any significant period without oversight by an authorized person; - Physical protection shall be achieved through the creation of clearly defined security perimeters (i.e. physical barriers) around the time-stamping management. Any parts of the premises shared with other organizations shall be outside this perimeter. - Physical and environmental security controls shall be implemented to protect the facility that houses system resources, the system resources themselves, and the facilities used to support their operation. The TSA's physical and environmental security policy for systems concerned with time-stamping management shall address as a minimum the physical access control, natural disaster protection, fire safety factors, failure of supporting utilities (e.g. power, telecommunications), structure collapse, plumbing leaks, protection against theft, breaking and entering, and disaster recovery. - Controls shall be implemented to protect against equipment, information, media and software relating to the time-stamping services being taken off-site without authorization. NOTE : Other functions may be supported within the same secured area provided that the access is limited to authorized personnel. b) Access controls shall be applied to the cryptographic module(s). For the server-based time-stamping policy, access controls shall meet the requirements of security of cryptographic modules as identified	REJECTED Only one policy

Annex D		Technical	The title is: "Annex D (informative): Long term verification of time-stamp tokens" Annex D was referenced on page 13, section 5.1 NOTE 1 and on page 15, section 6.3 NOTE. NOTE 1 has been removed, since the NOTE has nothing to do in the Overview section the Time-stamping policies section. The text from section 6.3 has been revised (see item b)) since the verification of TST by relying party, once the TSU certificate has expired is a very common operation and thus the text should not be placed in an informative annex. Also the text currently placed in Annex D has several errors and omissions. In particular, the following sentence is incorrect: " ..if it can be known that: • the TSU private key has not been compromised at any time up to the time that a relying part verifies a time-stamp token;" This does not cover the case where the TSU certificate has been revoked for a reason that is different from key compromised and does not allows for the re-time-stamping case. It is also missing to indicate how the revocation information may be obtained beyond the end of the validity of the TSU certificate, since the presence of the ExpiredCertsOnCRL CRL extension is not mentioned.	Text proposal: "Annex D (normative): Long term verification of time-stamp tokens" Usually, a time-stamp token becomes unverifiable beyond the end of the validity period of the certificate from the TSU, because the CA that has issued the certificate does not usually warrant any more that it will publish revocation data, including data about revocations due to key compromises. In order to verify a TST beyond the end of the validity period of the certificate from the TSU, it is always necessary to be able to know that : • the hash algorithms used in the time-stamp token exhibits no collisions at the time of verification, • the signature algorithm and signature key size under which the time-stamp token has been signed is still beyond the reach of cryptographic attacks at the time of verification. D.1. When the CA that has issued the TSU certificate makes an exception and thus publishes revocation data beyond the end of the validity period of the TSU certificate, then this can be known because the CA publishes CRLs using the ExpiredCertsOnCRL CRL extension defined in X.509. The date contained in the ExpiredCertsOnCRL extension shall however be earlier than the end of the validity of the TSU certificate. In such a case, verification of a TST might still be performed beyond the end of the validity period of the certificate from the TSU, if, at the time of verification, CRL indicates that the TSU certificate has not been revoked. If, at the time of verification, the TSU certificate has been revoked, then the revocation reason needs to be considered : - If the revocation reason is anything else than "key compromise", then the date contained in the TST shall be compared against the revocation date. If the date contained in the TST is earlier than the revocation date, then the TST shall be considered as being valid. Otherwise, it shall be considered as being invalid.	OK - PARTIAL Some comments taken into account

Clause/ Subclause	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change**	**OBSERVATIONS** on each comment submitted
2	**Note**	**E**	**(their**	**Their**	**OK**
2.1	**Normative references**	**T**	**Reference 1 and 7 are duplicated and superseded**	**Refer to ITU-R.TF.460-6**	
2.1	**Normative references**	**E**	**Bullet 5: [ISO**	**ISO**	**OK**
3.1	**Definitions**	**E**	**ITU TF.460-5**	**ITU TF.460-6**	**OK**
B.1	**Introduction**	**E**	**Makinginformed**	**Making informed**	**OK**
Annex C		**T**	**Reference to ITU.R.TF.460-4 should be updated in conformity with the previous comment**		**OK**

Clause/ Subclause	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change**	**OBSERVATIONS** on each comment submitted
General		**E**	Pleased double check the verbal forms: some of them are in CAPITAL letters		OK
Title		**E**	Shouldn't this be "prEN"?		OK
Foreword		**E**	Since TS 102 023 has been amended in this prEN, it should be better write something like "The present document is ***an improvement and amendment of*** TS 102 023."		REJECTED obvious: Latest version automatically applies New version is for improvement

Introduction	**Numbered list item 2**	**T**	The second part of the sentence (“since CAs are not …”) is misleading. Please reword in a more straightforward way. Currently it may be (wrongly) interpreted as if CAs are not mandate to revoke certificates after expiration.		REJECTED This is clearly stated that : CAs are not mandated to process revocation status information
Scope	**6th paragraph**	**E**	“time stamp policy”.	Isn’t it better “time stamping policy”?	OK
Scope	**Note 1**	**E**	Please notice that RFC 3161 was updated by RFC 5816		OK
Scope	**Note 2**	**T**	The referenced TS seems be dealing with cryptographic devices, so it is not clear why it is referenced here		OK Bad reference from previous TS Was : CWA 14172-2 EESSI Conformity Assessment Guidance - Part 2: Certification Authority services and processes Updated to : ETSI EN 319 403
2	**Entire text before list items**	**E**	This part is different from analogue parts in other ETSI publications, why? This may puzzle end users		OK Update according to 319 422
2	**Note**	**E**	Please remove left parenthesis		OK
2.2	**Note 1**	**E**	Each listed document has been amended in the relative prEN, it should then be better write something like "***[ix+] is an improvement and amendment of NN xxx yyy***."		REJECTED obvious: Latest version automatically applies New version is for improvement
3.1	**Last line**	**T**	“QTSP Qualified Time-Stamp Policy” Please add a definition of “Qualified Time-Stamp Policy”		OK QTSP has been removed

4.2	**2nd last paragraph**	**T**	Each unit “has” a different key	Maybe it is better to mandate this requirement by specifying "must have" instead.	OK removed from this definition. Recommendations on keys are in in : 7.2 Key management life cycle
4.3	**Title**	**T**	In order to be clearer, it would be better to provide a definition of subscriber in clause 3.1		OK
5.1	**1st paragraph**	**E**	This para is a useless duplication of definition in clause 3.1 Please remove.		OK
5.4	**1st paragraph**	**T**	Please review as suggested. As a matter of fact it is not correct to impose on a TSA to use a predefined TSP and, consequently, TSA policy id.	“The TSA can **~~shall~~** use the identifier for the time-stamp policy in time-stamp tokens as given in clause 5.2, or**, alternatively, shall** define its own time-stamp policy…”	REJECTED TSA SHALL use a policy identifier
5.4	**Sentence “A conformant TSA must demonstrate that:”**	**T**	“Must demonstrate” to whom? It is better to reword as suggested	A conformant TSA must **be able to** demonstrate that:…”	OK
6.2	**Note**	**T**	Please replace the following words as suggested: “that the private key used to sign the time-stamp token has not been compromised.” It is in fact impossible to the end user to ascertain if a Private key was compromised. Furthermore, there are other reasons for revoking one certificate.	Please change this sentence as follows (kind of): "... that the certificate associated to the signature in the TST has not been revoked"..	OK
6.3	**Item a)**	**T**	Same as in AgID 17		OK
6.3	**Note**	**T/E**	“… the validity of the signing key can be checked using …” Please reword consistently with the previous comment		OK
7.1.2	**Note 1**	**T/E**	“the mean time to recovery”	“the **expected** mean time to recovery”	7.1.1 OK

7.2.1	**b) 3rd bullet**	**T**	Is there ay reason to specify only part 2 of the TS 419 221? Also parts 3 and 4 look like being able to generate keys suitably to TSA purposes		OK Added part 3 & 4
7.2.1	**Note 1**	**E**	Please remove colon	“See ETSI TS 119 312~~:~~ [i.10]”	OK
7.2.2	**a) 2nd bullet**	**T**	Also part -4 can be used, in particular consistently with recommendation in the following NOTE		OK
7.2.3	**Note**	**T**	The purpose of this Note is not clear: it says nothing specific nor worth conveying. Please delete it		OK Note is obvious, deleted
7.2.3	**Item d)**	**T**	Why? What matters is that such certificate is promptly available to relying parties. This may be achieved either by including it into the TST or by making it available in a directory, albeit the first solution is by far the best one, for obvious reasons. None of them, however, requires the certificate to be included in the TSU signing device: e.g. it can be in the TSU application! If this requirement really is to be kept, please at least, remove the verbal form "shall": "may" perfectly fits the purpose.		OK Changed to a recommendation note
7.2.3	**Item e)**	**T**	Affected by the previous comment		OK Reworded into TSU or crypto device.
7.2.4	**2nd bullet**	**T**	The certificate may be revoked for other reasons than key compromise	“… TSU signing certificate be compromised”	OK
7.2.4	**2nd bullet**	**E**		“the longer **its** ~~the~~ life-time,”	OK

7.2.5	**1st paragraph**	**T**	“This date SHALL not be longer than the end of validity of the associate public key certificate” Not clear. If the purpose is to have a key lifetime as short as possible, to reduce the number of TSTs affected by a possible certificate revocation, please reword this sentence referring to “notAfter“ and “privatekeyusageperiod” instead		
7.2.5	**2nd paragraph**	**E**		“should be ~~in~~ reduced”	OK
7.2.5	**2nd paragraph**	**E**	If the purpose is to have a key lifetime as short as possible, to reduce the number of TSTs affected by a possible certificate revocation, please reword this sentence.		OK Reworded : However in order to be able to verify during a sufficient lapse of time the validity of the time-stamp tokens, the validity of the TSU’s signing key should be reduced (e.g. public key valid 4 years, and private key reduced to 1 year by using private key usage period).
7.2.6	**b)**	**T**	The act of "storing" must be secure too.	“is not tampered with **when and** while stored.”	OK
7.2.6	**e)**	**T**	Erasure must be secure.	“erased upon device retirement **in a way that it is practically impossible to recover them**.”	OK
7.3.1	**h)**	**T**	“where applicable” is ill fit: the country where it was generated must be specified, else end users would not be able to identify the TSA in order to contact it for any reason.		OK As countryName is mandatory in cert profile for natural and legal person, let’s add it in token also.
7.3.2	**d)**	**E**		“that th**e** time indicated”	OK
7.4.4	**b) 1st bullet**	**T**	Not only physical protection must be assured.	“which physically **and logically** protects”	OK

7.4.4	**b) 2nd bullet**	**T**	Please specify: 1) that even authorized persons shall not be left alone in the secure area; 2) that every entrance and exit to/from the protected premises must be logged, either manual or automatic.		OK but reworded as : Every entry to the physically secure area shall be subject to independent oversight and non-authorised person shall be accompanied by an authorised person whilst in the secure area. Every entry and exist shall be logged.
7.4.8	**Note**	**T**	“TSA” is to be replaced with “TSU”		OK
7.5	**c)**	**T**	This requirement should address also performing disaster recovery procedures.		REJECTED Already addressed in 7.4.8 Business continuity management and incident handling
Annex A	**2nd paragraph**	**E**	“increment” ➔ please replace with "increase": "increment" is not a verb		OK
B2	**Table**	**T**	Replace all occurrences of “TSU public key” with “TSU public key certificate”		OK
Annex D	**1st Paragraph**	**T**	“Usually, a time-stamp token becomes unverifiable beyond the end of the validity period of the certificate from the TSU, because the CA that has issued the certificate does not warrant any more that it will publish revocation data, including data about revocations due to key compromises.” This can be understood as if "post mortem" revocations would affect signatures issued before the expiry date. Please replace “publish” with “keep revocation information available”		OK Reworded : Usually, a time-stamp token becomes unverifiable beyond the end of the validity period of the certificate from the TSU, because the CA that has issued the certificate does not warrant any more providing revocation status information for expired certificates.

Annex D	**2nd Paragraph**	**T**	Sentence “As an example, should a CA guaranty to maintain the revocation status of TSU certificates after the end of its validity period, this would fulfil the first requirement.” Is to be reviewed as specified. Maintain, in fact, does not necessarily imply “make publicly available”	“As an example, should a CA guaranty to **make** ~~**maintain**~~ the revocation status of TSU certificates **available** after the end of its validity period, this would fulfil the first requirement.”	OK Reworded : As an example, should a CA guaranty to make the revocation status information of TSU certificates available after the end of its validity period, this would fulfil the first requirement.

Clause/ Subclause	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change**	**OBSERVATIONS** on each comment submitted
Notation	**3.2**	**Editorial**	**Number of paragraph is not correct**	**3.3 Notation**	**OK**
Time stamp policies	**5.1**	**Technical**	**QTSP OID is not known** **NOTE: Additional OIDs for qualified time-stamp policy may be added following on the agreement of such a concept in a regulation on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market.**		**OK** QTSP has been removed
TSU key generation	**7.2.1** **Note**	**Technical**	**Recommending that same key should not be imported to multiple modules**		**There is already note 2 :** NOTE 2: In order to be conformant with ETSI EN 319 422 [i.4] clause 5.2.2, it is not recommended to import the same key into different cryptographic modules.