

Public Review: resolution of public comments on Draft ETSI EN 319 422 V0.0.9

Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and electronic time-stamp profiles

Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted
1	2	Editorial	Typo: “time-tamping”.	Change to: “time-stamping”.	ACCEPTED
5.2.2	2	Technical	<p>The requirement that “a genTime parameter limited to represent time with a precision limited to one second shall be supported” effectively forbids inclusion of fraction-of-second details, which is necessary to support a higher accuracy.</p> <p>According to RFC 3161, the “accuracy represents the time deviation around the UTC time contained in GeneralizedTime”, so the precision of one second might be not enough for the declared accuracy.</p> <p>For example, if a time-stamp was produced at 19920722132100.6Z, but the value included in the genTime is 19920722132101Z (due to the precision being limited to 1 second), and the declared accuracy is 0.1 second, the upper limit of the time at which the time-stamp token has been created, obtained by adding the accuracy value to the genTime, would be 19920722132101.1Z, and the lower limit would be 19920722132100.9Z (as per</p>	Change the requirement to “a genTime parameter representing time with a precision necessary to support the declared accuracy shall be supported”.	ACCEPTED

Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted
			<p>RFC 3161 clause 2.4.2), which is incorrect as the time the time-stamp was produced at (19920722132100.6Z) is not within this interval.</p> <p>Moreover, if the declared accuracy is 1 second, and genTime does not include fractions of a second, the maximum permissible drift of the TSU clock in regard to UTC would be 0.5 second. If, for example, the UTC time is 19920722132100.9Z, TSU time is 19920722132101.5Z (so the drift is 0.6 second), and this time is included in the genTime as 19920722132102Z (i.e. rounded to the nearest second), the UTC time will not fall within the interval of 19920722132101Z... 19920722132102Z.</p>		
6.1, 6.2		General	<p>These clauses define requirements for TSU certificates issued for natural persons, but, according to the draft ETSI EN 319 421 V0.0.6 clause 7.2, “The TSA shall be a legal entity according to national law”, so it is not clear when such requirements should apply.</p>	<p>In line with the draft ETSI EN 319 421 V0.0.6, the requirements for certificates for natural persons should be removed.</p>	<p>A natural person may be a legal entity.</p> <p>So in the case of a natural person, the certificate shall be issued according the corresponding certificate profile.</p> <p>REJECTED</p>

Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted
Title page	N/A	Editorial	The identification of the standard “Draft EN 319 422 V0.0.9 (2015-01)” is missing the word “ETSI”	“Draft ETSI EN 319 422 V0.0.9 (2015-01)”	ACCEPTED
9	Additional requirements for Regulation (EU) No 910/2014	Technical	A qualified time-stamping authority should be able to use the qcStatements extension as defined in RFC 3739 [2].	Qualified French TSPs would like to be able to differentiate Qualified timestamps and non qualified timestamps. This qcStatements extension will be very useful and could even help trust service application providers to enable control on that specific field. Make the use of the qcStatements extension possible for TimeS tamping Authorities.	ACCEPTED
Annex A			In policy field, time-stamp policy OID (02023) is not correct, it should be (2023). OID specification does not allow this and also software may not interpret this in the right way.	Change time-stamp policy OID for (2023)	ACCEPTED