Public Review: Resolution of Comments on Draft ETSI *EN 319 162-1 V0.0.3*- 31 May 2014

Associated Signature Containers (ASiC); Part 1: Core Specification

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.

ID	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	Resolution on each comment submitted
1				Authors of this comment: (not reported)		

2			General	Without the usage of EvidenceRecords each archived document requires independent archive time stamps. Furthermore this approach is not integrated with the international archival architectures standardized in • *ISO 14721 "Space data and information transfer systems - Open archival information system - Reference model"* and • *ISO "14533-1:2012 Processes, data elements and documents in commerce, industry and administration -- Long term signature profiles -- Part 1: Long term signature profiles for CMS Advanced Electronic Signatures (CAdES) (2012)* • *OASIS DSS v1.0 Profile for Comprehensive Multi-Signature Verification Reports Version 1.0 Committee Specification 01 (2010)* and the German DIN-Standard and Technical Guideline • *DIN 31647, Information and Documentation - Preservation of evidence of cryptographically signed electronic records (Beweiswerterhaltung kryptographisch signierter Dokumente), DIN draft standard. (2013)* • *Federal Office for Information Security (BSI): Technical Guideline 03125 Version 1.1: Preservation of Evidence of Cryptographically Signed Documents (TR-ESOR), available from from* ***https://www.bsi.bund.de/EN/Publications/TechnicalGuidelines/TR03125/BSITR03125.html*** *. (2011).* An Evidence Record is a collection of evidence compiled for a given archive object over time. An Evidence Record includes ordered collection of Archive Times-stamps (ATS) , which are grouped into Archive Times-stamps Chains (ATSCs) and Archive Times-stamps Sequences (ATSSeqs). The Evidence Record Syntax enables processing of several archive objects within a single processing pass using a hash tree technique and acquiring only one Time-Stamp to protect all archive objects. Evidence Record Syntax is applicable to data of any type or format including digital signatures. Evidence Records facilitate provision of long term validation of data "by establish a common way for associating data objects with advanced signature or time-stamp tokens" [chap. 4.1, p. 10] without the need to create "a data set which combines the signature and the data that was signed …" [chapter 4.1, p. 9].		Accepted to include ERS in ASiC. EN 319 162-1 draft to be updated so that ERS data objects (as defined in RFC 4998 and RFC 6283) can be included in ASiC-S with CAdES and XAdES allowing to provide evidence of data integrity in archives that uses ERS to protect integrity of data. No change to ASiC Baseline Profile as use of ERS is considered a specific case to be considered within the standardization activities required for long term preservation of signed documents an type of TSP present in the new EU Regulation. ETSI TS 101 533-1 already mentions ASiC as a possible format in support to long term preservation.
3	1		General	ASiC should allow for Evidence Records (ERS) according RFC 4998 as alternative for time stamp tokens. This relates to comments of BSI to *AdES core prENs.	Add support of • RFC 4998 / 6283 Evidence Records	See above, comment ID 2.
4	2.1		Editorial	See above	Add to normative references • RFC 4998 / 6283 Evidence Record Syntax	See above, comment ID 2

5	3.2		Editorial	Add definition of TST and ER	TST TimeStampToken according to RFC3161 ER Evidence Record according to RFC 4998 / 6283	See above, comment ID 2
6	4.2.2		Technical	See above	Add support of RFC 4998 / 6283 evidence records to both container types: • one or more ER and paragraph: ASiC is based on CAdES [1] or XAdES [2] Advances Electronic Signatures, evidence records conformant to RFC 4998 or RFC 6283 or time-stamp tokens conformant to RFC 3161 [3] that may be profiled as specified in TS 101 861 [i.8].	See above, comment ID 2
7	4.2.2 5 5.1		Technical	See above	Change text, add support of ERS in addition to TSP	See above, comment ID 2
8	5.2.2		Technical	See above	Add to 3) META-INF folder: d) evidenceRecord.ers containing one or multiple ERs in case data object (container) extracted from an archival systems providing ERs. Amend Figures 1 and 2 accordingly	See above, comment ID 2
9	5.4		Technical	See above	Add to alternative 3) (TSP) use of ERs ..if data object (container) extracted from an archival systems providing ERS, this (these) ERs should be included in .. (to be detailed) Amend Figures 4 and 5 accordingly	See above, comment ID 2
10	6 6.1		Technical	See above	Change text, add support of ERS in addition to TSP	See above, comment ID 2
11	6.2-6.3.1		Technical	See above	To be checked with regard to ERS, initially identified no needed changes	See above, comment ID 2

12	6.3.2		Technical	See above	Add to 4) - c) “META-INF/*evidenceRecord*.ers containing Evidence Records(s) as defined in RFC 4998 []. Text following to be amended with regard to ERS. Amend Figures 7 and 8 accordingly	See above, comment ID 2
13	6.5		Technical	See above	Add to ERS as alternative, review clause accordingly	See above, comment ID 2
14	7		Technical	See above	Add ASiC-S ERS long term Conformance Clause	See above, comment ID 2
15	7		Technical	See above	Add ASiC-E ERS long term Conformance Clause	See above, comment ID 2
16	A2		Technical	See above	Add and register at IANA (first suggestion): MIME media type name: Application MIME subtype name: vnd.etsi.evidence-record Required parameters: none encoding considerations: binary File extension: ers	See above, comment ID 2
17	A3 and A.4		TE	See above	ASiC XML Schema to be updated with regard to ERS usage	See above, comment ID 2

18	All ESI drafts		tech	The writing of all drafts needs improvements to enhance the quality	Apply the following rules: - the standard should specify all the requirements necessary to achieve its objective and ONLY include essential supporting information - use only appropriate verbal forms to express provisions, as defined in ETSI Drafting rules clause 14a (**http://portal.etsi.org/edithelp/HowToStart/home.htm?page=DraftingRules**) - shall/should/may are used only when writing provisions defined by the document itself. - do NOT use alternative forms such as is required to - "will/will not" shall be used to indicate behaviour of equipment or sub-systems outside the scope of the deliverable in which they appear - "can/cannot" shall be used for statements of possibility and capability. When document on signature policy says 'the signature policy may support X", a document on AdES format will say "the signature policy can support X" (a permissible actions defined in document D becomes a possibility in other documents) - never use present tense to express a provision. Present tense is only a description of facts - Clearly separate provisions (shall/should/may) from complementary informative text (e.g. using notes, examples, or moving it to informative annex) so that implementers clearly know what they have to implement.- never duplicate text. Only say things once.	Checked, no change required

18b	All ESI drafts		tech	The writing of all drafts needs improvements to enhance the quality	- do not copy provisions from other standards. If they are applicable, then write text like "RFC 5256 shall apply", "the attribute shall be as defined in <clause c> of XXX" - fully review scopes: scope defines without ambiguity the subject of the ETSI deliverable and the aspect(s) covered, thereby indicating the limits of applicability of the ETSI deliverable or particular parts of it. It shall not contain requirements. The scope shall be succinct so that it can be used as a summary for bibliographic purposes. Do not describe all clauses. - introduction: do not duplicate text with the scope. Introduction is not the scope. Introduction gives specific information or commentary about the technical content of the ETSI deliverable, and about the reasons prompting its preparation. It shall not contain requirements - keep it impersonal: do not use I, you, we - do not use colloquial language - tables: use ETSI drafting rules	Checked, no change required