Public Review: Resolution of Comments on Draft ETSI EN 319 132 parts 1 and 2 V0.0.4 (2013-11) – 31 May 2014

XAdES

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.

Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signatures (XadES); Part 1: Core Specification

Organization name	**Clause/ Subclause**	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change**	**Resolution** on each comment submitted
	In General 1:		T	Germany highly appreciates the activities at ETSI M/460 phase 2, which particularly address long term aspects of electronic signatures. - However, it seems that the current scope of the proposed “Draft EN 319 132-1 V0.0.4 (2013-11) Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signatures (XAdES); Part 1: Core Specification” only covers approaches without an optional usability of Evidence Records according RFC 4998 and RFC 6283, which is not optimal with respect to scalability because without the usage of Evidence Records each archived document requires independent archive archive timestamps.		**General disposition to all the comments derived from the general request of including ERS support in XAdES specification follows below. Nevertheless, this does not mean that some specific reaction or consideration is done to specific comments also derived from this general request, whenever is considered worth.** **The STF 458 made the resolutions copied below in its meeting held in 24/2/2014:** **1. The STF 458 Area 1 Task 2 team proposes not to incorporate ERS management within all the AdES formats at this point in time.** **2. The STF 458 Area 1 Task 2 team proposes to incorporate ERS management within ASiC packages so that signatures (CAdES, XAdES, PAdES?) that have been archived and preserved using ERS mechanisms, may be extracted from the archive, be packaged with the signed data objects, partial hash tree, and archive time-**

Organization name	**Clause/ Subclause**	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change**	**Resolution** on each comment submitted
						stamps, and be securelly transferred to a different destination, where a relying party may still successfully validate the signatures. The new text will also provide guidance on the data objects that should also be securely archived within the ERS archive, for ensuring that the signature and all the required validation material is correctly preserved, and that once the signature and all the required validation material are extracted and incorporated to the ASiC package, the signature may be successfully validated. **3. The STF 458 Area 1 Task 2 team does not close the door to a potential incorporation of ERS within the different AdES formats, once analyzed the requirements for such an incorporation (which could also include an analysis of alternative archival systems), as all the different AdES formats include at this point in time extension mechanisms that would easily allow the definition of a potential new attribute (CAdES), property (XAdES), or dictionary (PAdES).**
	In General 2:		T	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) and • ISO 14533-2:2012 Processes, data elements and documents in commerce, industry and	Therefore, it is proposed to enlarge the scope of the Draft ETSI EN 319 132-1 V0.0.4 (2013-11) to cover alternative approaches as well, which are based on the Evidence Record Syntax normalized in RFC 4998 and RFC 6283 and may be integrated with archival systems based on ISO 14721, ISO 14533 {C,X}AdES, OASIS DSS v1.0 Profile for Comprehensive Multi-Signature Verification Reports, DIN 31647 and BSI-TR03125 . **Proposed solution for XAdES:** The Evidence Record attribute shall be integrated into XAdES (as well as in in XAdES and PAdES) as an ordinary attribute.	**The change proposed mentions OASIS DSS v1.0 Profiel for Comprehensive Multi-Signature Verification Reports. . This document was born, among other reasons, as intent of standardizing the contents and format of a validation report of a XAdES signature. In consequence this document complements XAdES core specification. In fact the STF 458 is also in charge of proposing a standard for a validation report fully aligned to the ETSI EN 319 102, and one of the starting points being considered is the OASIS Profile. The editor, in consequence, disagrees the sentence that claims that the ETSI EN 319 132 is not integrated within this**

Organization name	**Clause/ Subclause**	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change**	**Resolution** on each comment submitted
				administration -- Long term signature profiles -- Part 2: Long term signature profiles for XML Advanced Electronic Signatures (XAdES) (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). and even • EN 319 122 CMS Advanced Electronic Signatures (CadES) Part 1 <http://docbox.etsi.org/ESI/Open/Latest_Drafts/prEN-319122-1v003-CAdES-core-STABLE-DRAFT.pdf> : Core Specification.!		**particular profile. More on the contrary, the profile tried to fill an existing gap within the management of XAdES and CAdES signatures, and as such the union of XAdES/CAdES specs, the TS 102 853 on procedures for validation, and the OASIS profile on a format for validation report, formed a coherent set of specifications, which will be now improved once the new EN 319 102 will also incorporate the new validation report specification.**
	Motivation		T	**Advantages of the Evidence Record syntax concept according RFC 4998 and RFC 6283:** • **Better Cost effectiveness and Performance:**		**First bullet: certainly it is true that within an archive, only one time-stamp token is required to cover the whole contents of the archive. This applies only when a signature is placed within**

Organization name	**Clause/ Subclause**	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change**	**Resolution** on each comment submitted
				o Whereas XAdES-A requires one time-stamp per signature for a re-signing document the Evidence Record syntax standardised by IETF in RFC 4998 and RFC 6283 uses Merkle Hash Trees so that **only one time-stamp** is required for a complete re-signing **cycle of different documents.** • **Data Economy** o For any particular data object, the **hash tree can be reduced** to a few sets of hash values **(reduced hash trees**), which are sufficient to prove the existence of a single data object or data group**.** • **Data Protection** o Aspects with regard to **data protection technology** are also taken into account because with the ERS standard it is also **possible to delete parts of the document database** without compromising the conclusiveness of the remaining parts. • **Similar Processes independent of data formats** o The Evidence Record Syntax (ERS) specifies **similar processes** concerning generation, verification, timestamp-renewal and hashtree-renewal of Evidence Records independent from the used data formats (e.g. CMS- or XML-based data formats) whereas the actual proposals for CAdES-A (e.g. archive-time-stamp-v3, ats-hash-index attribute) and XAdES-A (e.g.		**an archive and does not embed itself any archive-time-stamp. But if a XAdES signature, as requested, would embed an ERS archive time-stamp and was not placed within an ERS archive, then one new archive time-stamp would be required for enlarging the “life” of the signature, although it is true that the computation of its message imprint would be different: in XAdES it is required to concatenate once again all the time-stamped objects, while in ERS this is not required.** **It must be noted that the STF has already agreed to deal with the use case of signatures placed within an ERS archive and being extracted for transmission or validation by allowing incorporation of ERS constructs within ASiC containers.** **As for the rest of the bullets, 2 and 3 seem to apply to ERS archives.** **The STF proposes that all this material is actually taken into consideration when implementing resolution 3 aforementioned.**

Organization name	**Clause/ Subclause**	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change**	**Resolution** on each comment submitted
				xadesv141:ArchiveTimeStamp element, xadesenv111:RenewedDigests and xadesv141: TimeStampValidationData) look quite different. • **Combination of existing *AdES-A attributes with ERS is possible** o E.g. ats-hash-index attribute could be a data object, which is part of the hashed data object group. o E.g. the Timestamp of the root hash value of the ERS could be a Time-Stamping Authority (TSA) according to [RFC3161] or other data structures and protocols e.g. an xadesv141:ArchiveTimeStamp element or e.g. an archive-time-stamp-v3 attribute. • **Ordered list of POEs according to a clear life cycle concept and functional model** • In the Evidence Record Syntax (RFC 4998 and 6283) there is a clear life cycle model and functional model. • Therefore the ERS consists of a timely ordered and nested sequence of chains of archive timestamps (POEs) which facilitates the validation process. • In *AdES-A without Evidence Records and no timely ordered and nested POEs the validation process depends on low level data attributes and is more complicated (more test-cases in 8 steps, different status values, etc.) .		

Organization name	**Clause/ Subclause**	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change**	**Resolution** on each comment submitted
	Use Cases		T	**Use Cases:** • Preservation of the integrity and authenticity of digital records to maintain the conclusiveness of the documents supporting legal claims of the issuer or third parties and the proof of their correctness in electronic legal and business transactions, especially for **Administration, Business and Science** in connection with o Secure electronic communication o Replacement through scanning o Documentation and analysis of processes o Electronic record and document management o Electronic filing and archiving o Proper administration o Electronic publication and promulgation of official leaves o **…** • **Exemplary Fields of Application** o E-Government o Pharmaceutical Industry o Electronic payment o Car - and Aircraft Industry o Health care		**See resolution 1.**

Organization name	**Clause/ Subclause**	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change**	**Resolution** on each comment submitted
				o …		
	Conclusion			**Conclusion: In most use cases it is a great advantage to have only one time-stamp for a complete re-signing cycle of many different documents and to have similar processes independent of the used data formats and data elements .**		**See resolution 1.**
	In Detail					
	Chapter 2.1 Normative references		T		**Proposal:** Please Add: [14] IETF RFC 4998 (2007): "Evidence Record Syntax (ERS)" [15] IETF RFC 6283 (2011): "Extensible Markup Language Evidence Record Syntax (XMLERS)"	**Rejected to implement this addition now as per resolution 1. Indeed to keep this and use it depending on results after having implemented resolution 3**
	Chapter 4 Overview	p. 11 Time-stamp token container properties	T	**Current text:** The definition of "Evidence Record" is missing	**Proposal: New definiton** Evidence Record: 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).	**Rejected now as per resolution 1. Indeed to keep this and use it depending on results after having implemented resolution 3**
	Chapter 4.1.3.2	Archival electronic signatures (XAdES-A)	T	**Current text:** Archival signatures in accordance with the present document incorporate CertificateValues unless the ds:KeyInfo element does contain the full set of certificates used to validate the electronic signature. They also incorporate RevocationValues unless the ds:KeyInfo element contains the revocation information that has to be shipped with the electronic signature. Archival signatures also incorporate one or more xadesv141:ArchiveTimeStamp unsigned properties. They	**Proposal:** Archival signatures in accordance with the present document incorporate CertificateValues unless the ds:KeyInfo element does contain the full set of certificates used to validate the electronic signature. They also incorporate RevocationValues unless the ds:KeyInfo element contains the revocation information that has to be shipped with the electronic signature. Archival signatures also incorporate one or more xadesv141:ArchiveTimeStamp **or Evidence Record** unsigned properties. They may	**Rejected now as per resolution 1. Indeed to keep this and use it depending on results after having implemented resolution 3**

Organization name	**Clause/ Subclause**	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change**	**Resolution** on each comment submitted
				may contain other properties. Each xadesv141:ArchiveTimeStamp element contains time-stamp tokens covering among other elements, those ones that contain validation data. These forms are used for archival of signatures. Successive archive time-stamps protect the whole material against vulnerable hashing algorithms or the breaking of the cryptographic material or algorithms and the expiration of the time-stamp token certificate. Below follows the structure of a XAdES-A built on a XAdES-T by incorporation of at least one xadesv141:ArchiveTimeStamp element. In the figure below, the prefix "xadesv141" prefix corresponds to XML Namespace whose URI value is "http://uri.etsi.org/01903/v1.4.1# "	contain other properties. Each xadesv141:ArchiveTimeStamp element contains time-stamp tokens covering among other elements, those ones that contain validation data. These forms are used for archival of signatures. Successive archive time-stamps protect the whole material against vulnerable hashing algorithms or the breaking of the cryptographic material or algorithms and the expiration of the time-stamp token certificate. **In Evidence Records the validationdata is to be found within the <TimeStampToken> element itself or within the <CryptographicInformationList> element or in <SupportingInformationList>.** Below follows the structure of a XAdES-A built on a XAdES-T by incorporation of at least one attribute “archivingType” with a choice beetwen an xadesv141:ArchiveTimeStamp element or an Evidence Record or other elements. In the figure below, the prefix "xadesv141" prefix corresponds to XML Namespace whose URI value is "http://uri.etsi.org/01903/v1.4.1# "	
	Chapter 6.5 Properties for XadES-A form	New chapter 6.5.4: The Evidence Record Element	T	**Current text:** A description of the Evidence Record attribute is missing.	**Proposal:** Please create a new chapter 6.5.4 The Evidence Record according to this document, **chapter 6.5.4 “The Evidence Record”**	**Rejected now as per resolution 1. Indeed to keep this and use it depending on results after having implemented resolution 3**
	Chapter 7.4	XAdES with Archive-time-stamp (XAdES-A) conformance level	T	**Current text:** “A XAdES signature claiming conformance to XAdES-A level shall be built upon signatures compliant with XadES-T, XAdES-C, XAdES-X (type 1 or 2), and XAdES-XL (type 1 or 2) conformance levels. In addition it: • shall directly or indirectly incorporate one or more	**Proposal:** “ A XAdES signature claiming conformance to XAdES-A level shall be built upon signatures compliant with XadES-T, XAdES-C, XAdES-X (type 1 or 2), and XAdES-XL (type 1 or 2) conformance levels. In addition it: • shall directly or indirectly incorporate one or more	**Rejected to add the mention to the ERS. However, and coming from an ulterior comment the text should read:** **“**A XAdES signature claiming conformance to XAdES-A level shall be built upon signatures compliant with XadES-T, XAdES-C, XAdES-X (type 1 or 2), or XAdES-XL (type 1 or 2) conformance levels**”**

<table>
<tr><th>Organization name</th><th>Clause/ Subclause</th><th>Paragraph Figure/ Table</th><th>Type of comment (General/ Technical/Editorial)</th><th>COMMENTS</th><th>Proposed change</th><th>Resolution on each comment submitted</th></tr>
<tr><td></td><td></td><td></td><td></td><td>instances of xadesv141:ArchiveTimeStamp property.”</td><td>instances of xadesv141:ArchiveTimeStamp property <b>or Evidence Record.”</b></td><td><b>Please note the “or” instead of “and”, meaning that a XAdES-A may be built from any of the aforementioned forms by directly incorporating the required validation material.</b>
<b>To do: accordingly modify the text</b></td></tr>
<tr><td></td><td>Chapter B.4</td><td>Archival Electronic Signature complete</td><td>T</td><td><b>Current text: :</b>
“xadesv141:ArchiveTimeStamp
(xadesv141:TimeStampValidationData| xadesv141:ArchiveTimeStamp)”</td><td><b>Proposal:</b>
“xadesv141:ArchiveTimeStamp
(xadesv141:TimeStampValidationData? | xadesv141:ArchiveTimeStamp)*
<b>Evidence Record</b> “</td><td><b>Rejected. The proposal would allow to have as last element of a XAdES-A a xadesv141:TimeStampValidationData containing the validation material of a formerly included xadesv141:ArchiveTimeStamp, which is not the intention of the specification. The latest element within a XAdES-A signature is the archive time-stamp. The validation material element is added, if necessary, just before a new archive time-stamp is added to the signature.</b></td></tr>
<tr><td></td><td>Chapter 6.5.2</td><td></td><td>T</td><td><b>Question</b>
Why is there no introduction of
the archive-time-stamp (ATSv3)
according to Draft EN 319 122-1 V0.0.3 (2013-11) ?</td><td></td><td><b>ACCEPTED if the comment suggests to include in 6.5 an introductory text similar to the text that appears in 6.5.</b>
<b>TO DO: include text similar to text in CAdES immediately below 6.5.</b></td></tr>
<tr><td></td><td><b>New</b>
<b>Chapter 6.5.4</b></td><td colspan="4"><b>Chapter 6.5.4 The Evidence Record</b>
The following description is based on [14] and [15].
“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. The leaves of the hash tree are hash values of the data objects in a group. A Time-Stamp is requested only for the root hash of the hash tree. The deletion of a data object in the tree does not influence the provability of others. For any particular data object, the hash tree can be reduced to a few sets of hash values, which are sufficient to prove the existence of a single data object. Similarly, the hash tree can be reduced to prove existence of a data group, provided all members of the data group have the same parent node in the hash tree.” (see [15])
The Evidence Record Syntax (ERS) specifies processes for the generation and verification of Evidence Records.</td><td><b>Rejected now as per resolution 1. Indeed to keep this and use it depending on results after having implemented resolution 3</b></td></tr>
</table>

Organization name	**Clause/ Subclause**	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change**	**Resolution** on each comment submitted
		The standard defines in detail how re-signing and re-hashing, even for **large amounts of documents**, can be carried out automatically. Furthermore, the standard defines the data formats in which the Evidence Records are provided for an **unlimited period of time** and can be exchanged. Aspects with regard to **data protection technology** are also taken into account because with the ERS standard it is also possible to delete parts of the document database without compromising the conclusiveness of the remaining parts. Whereas XAdES-A requires one time-stamp per signature for a re-signing document the Evidence Record syntax standardised by IETF in RFC 4998 and RFC 6283 uses Merkle Hash Trees so that only one time-stamp is required for a complete re-signing cycle of a large amount of documents..				
	New Chapter 6.5.3.1	**6.5.3.1 Data Structures** The Evidence Record attribute is an optional unsigned attribute. Several instances of this attribute may occur within the list of unsigned attributes. The Evidence Record attribute is a proof of existence (PoE) at a certain past date, computed over many signed archived data objects or archived data object groups of signed documents together with their signatures, including signed attributes and all other essential components of the signature. In XML syntax the Evidence Record according to [15] is represented by namespace="urn:ietf:params:xml:ns:ers" schemaLocation="http://ws.openecard.org/schema/xml-ers-rfc6283.xsd" based on xmlns="http://www.w3.org/2001/XMLSchema" The Evidence Record contains an Archive Timestamps Sequence, generated during a long archival period, and possibly useful data for validation. An **Archive Timestamp Sequence** is a part of the Evidence Record, which " is a sequence of Archive Timestamp Chains, where each Archive Timestamp Chain preserves non-repudiation of the previous Archive Timestamp Chains, even after the hash algorithm used within the previous Archive Timestamp's hash tree became weak. Non-repudiation is preserved until the last Archive Timestamp of the last chain becomes invalid. The process of generating such an Archive Timestamp Sequence is called Hash-Tree Renewal. ([14], p.5)" An **Archive Timestamp Chain** is part of an Archive Timestamp Sequence, which " is a time-ordered sequence of Archive Timestamps, where each Archive Timestamp preserves non-repudiation of the previous Archive Timestamp, even after the previous Archive Timestamp becomes invalid. Overall non-repudiation is maintained until the new Archive Timestamp itself becomes invalid. The process of generating such an Archive Timestamp Chain is called Timestamp Renewal. ([14], p. 5)" An **Archive Timestamp** is "a timestamp and typically a list of hash values, which allow the verification of the existence of several data objects at a certain time.([14], p.5) …. The lists of hash values are generated by the reduction of an ordered Merkle hash tree [MER1980]. The leaves of this hash tree are the hash values of the data objects to be timestamped. Every inner node of the tree contains one hash value, which is generated by hashing the concatenation of the children nodes. The root hash value, which represents unambiguously all data objects, is timestamped ([14], p. 11).				**Rejected now as per resolution 1. Indeed to keep this and use it depending on results after having implemented resolution 3**

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	Resolution on each comment submitted
		A **Reduced Hashtree** contains lists of hash values. These hash values can be derived by reducing a hash tree to the nodes necessary to verify a single data object according to ([15], 3.2.2. Reduction of Hash Tree, p 9). Hash values are represented as octet strings. If the optional field reducedHashtree is not present, the Archive Times-stamp simply contains an ordinary timestamp. A **Timestamp** is a cryptographically secure confirmation generated by a Time-Stamping Authority (TSA), e.g., [RFC3161], which specifies a structure for Time-Stamps and a protocol for communicating with a Time-Stamp Authority. Besides this, other data structures and protocols may also be appropriate.				
	New Chapter 6.5.3.2	**6.5.3.2 Processes** **6.5.3.2.1 Initial Archive Times-stamp in General** According to ([15], p. 16ff), "the lists of hash values of an Archive Timestamp can be generated by building and reducing a Merkle hash tree [MER1980]. Such a hash tree can be built as follows: 1. Collect data objects to be timestamped. Note 1: The validationDate of the signature of an data object could be stored in a data object which becomes part of an data object group together with the original data object , which has to be hashed according No. 3. 2. Select a canonicalization method if the archive data is represented in XML format. 3. Choose a secure hash algorithm H (shall be the same as the hash algorithm used in the Time-Stamp Token and for the has tree) and generate hash values for the data objects. These values will be the leaves of the hash tree. 4. Create a Hash Tree according to ([15], p. 17 ff) 5. Obtain a timestamp for this root hash value..." Note1: A Timestamp is a cryptographically secure confirmation generated by a Time-Stamping Authority (TSA), e.g., [RFC3161] , which specifies a structure for Time-Stamps and a protocol for communicating with a Time-Stamp Authority. Besides this, other data structures and protocols may also be appropriat, e.g. an xadesv141:ArchiveTimeStamp element. Instead of using a xadesv141:ArchiveTimeStamp element to secure the validationData, the validationData of the Archive Timestamp or Archive Timestamp Sequence (e.g. certificates, revocation information, etc.) could be stored in <CryptographicInformationList> or in <SupportingInformationList>which are OPTIONAL elements that allow the storage of data needed in the process of Time-Stamp Token validation in case when such data is not provided by the Time-Stamp Token itself.				**Rejected now as per resolution 1. Indeed to keep this and use it depending on results after having implemented resolution 3.** **Apart from the initial rejection, some remarks to the text proposed:** **. Do not understand the mention to validationDate in the context of step 1..is it validation data. Did the authors mean validation data or validation date?** **. The text should clearly specify what are the data objects to be time-stamped by the archive-time-stamp, as it is clearly specified by XAdES, or alternatively rely on the list of objects specified in the other XAdES archive time-stamped.**

Organization name	**Clause/ Subclause**	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change**	**Resolution** on each comment submitted
	New chapter 6.5.3.2.2			**6.5.3.2.2 Validation of the EvidenceRecord** According to ([14], p. 15ff), “an Archive Timestamp shall prove that a data object existed at a certain time, given by timestamp. This can be verified as follows: 1. Calculate hash value h of the data object with hash algorithm H given in field digestAlgorithm of the Archive Timestamp. 2. Search for hash value h in the first list (partialHashtree) of reducedHashtree. If not present, terminate verification process with negative result. 3. Concatenate the hash values of the actual list (partialHashtree) of hash values in binary ascending order and calculate the hash value h’ with algorithm H. This hash value h’ MUST become a member of the next higher list of hash values (from the next partialHashtree). Continue step 3 until a root hash value is calculated.” 4. “Check the validity of the Time-Stamp Token. If the needed information to verify formal validity of the Time-Stamp Token is not available or found within the <TimeStampToken> element or within the <CryptographicInformationList> element or in <SupportingInformationList> (..., exit with a negative result (see [15], p. 22)“. 5. The verification of Archive Timestamp Chains and Archive Timestamp Sequences is done according to [15]. If a proof is necessary for more than one data object, steps 1 and 2 have to be done for all data objects to be proved. If an additional proof is necessary that the Archive Timestamp relates to a data object group (e.g., a document and all its signatures), it can be verified additionally, that only the hash values of the given data objects are in the first hash-value list.”		**Rejected now as per resolution 1. Indeed to keep this and use it depending on results after having implemented resolution 3.**
	New Chapter 6.5.3.3			**6.5.3.3 TimeStamp Renewal** According to ([14], p. 17): “ The initial Archive Timestamp relates to a data object or a data object group. Before cryptographic algorithms that are used within the most recent Archive Timestamp (which is, at the beginning, the initial one) become weak or their timestamp certificates become invalid, Archive Timestamps have to be renewed by generating a new Archive Timestamp. In the case of Timestamp Renewal, the content of the timestamp field of the old Archive Timestamp has to be hashed and timestamped by a new Archive Timestamp. The new Archive Timestamp MAY not contain a reducedHashtree field, if the timestamp only simply covers the previous timestamp. However, generally one can collect a number of old Archive Timestamps and build the new hash tree with the hash values of the content of their timestamp fields. “If the current <ArchiveTimeStamp> element does not contain needed proof for long-term formal validation of its Time-Stamp Token within the <TimeStamp> element, collect needed data such as root certificates, Certificate Revocation Lists, etc., and include them in the <CryptographicInformationList> element of the last Archive Time-Stamp (each data object into a separate <CryptographicInformation> element). (see [15], p. 25)”		**Rejected now as per resolution 1. Indeed to keep this and use it depending on results after having implemented resolution 3.**

<table>
<tr><th><b>Organization name</b></th><th><b>Clause/ Subclause</b></th><th><b>Paragraph Figure/ Table</b></th><th><b>Type of comment</b>
(General/ Technical/Editorial)</th><th><b>COMMENTS</b></th><th><b>Proposed change</b></th><th><b>Resolution</b>
on each comment submitted</th></tr>
<tr><td></td><td></td><td colspan="4">The new Archive Timestamp MUST be added to the Archive Times-stamp Chain.
The new Archive Timestamp and its hash-Tree MUST use the same hash algorithm as the preceeding one, which is specified in the <digestMethod> field of the <ArchiveTimeStampChain>.</td><td></td></tr>
<tr><td></td><td>New Chapter 6.5.3.4</td><td colspan="4"><b>6.5.3.4 HashTree Renewal</b>
Before the hash algorithm used to build the hash trees in the Archive Timestamp loses its security properties, the Hash-Tree Renewal is required.
In case of Hash-Tree-Renewal, the Archive Timestamp and the archived data objects covered by the Archive Timestamp must be hashed and timestamped again, as described in [15], p. 26ff.</td><td><b>Rejected now as per resolution 1. Indeed to keep this and use it depending on results after having implemented resolution 3.</b></td></tr>
</table>

Public Review: Comments on Draft EN 319 132-1 V0.0.4 (2013-11)

XAdES - XML Advanced Electronic Signatures - Part 1: XAdES - Core specifications.

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	OBSERVATIONS on each comment submitted
	4.1.3.2 7.4	Whole 4.1.3.2 1st sentence of 7.4	Technical	There seems to be a significant inconsistency on what level(s) a -A level can be built. It seems that there is a huge change from previous versions of XAdES as *clause 4.1.3.2 Archival electronic signatures (XAdES-A)* seems to allow building a XAdES-A level directly from a XAdES-T level. Clause 4.1.3.2, to the contrary of clauses 4.1.1, 4.1.2 and 4.1.3.1, does not clearly state on what to build an –A level. The example given leaves the impression that –A level can be built on a –T level directly. Both having put definitions of levels -C, –X1/2 and –X-L1/2 in an Annex and not mentioning at all such levels in clause 4.1.3.2 reinforce this interpretation. However, last sentence of clause 4.1.3.2 states that “Conformance requirements for this form of XAdES signatures are specified in clause 7.4.”). Such clause 7.4 reveals quite contradictory (or at least confusing with regards) to clause 4.1.3.2 as first sentence of 7.4 states that: “A XAdES signature claiming conformance to XAdES-A level shall be built upon signatures compliant with XAdES-T, XAdES-C, XAdES-X (type 1 or 2), and XAdES-XL (type 1 or 2) conformance levels.”. This strictly speaking means that to build a XAdES-A level you must implement a XAdES-T, and a XAdES-C, and a XAdES-X (type 1 or 2), and a XAdES-XL (type 1 or 2). Clause 7.4 does not make it possible to build a –A level directly from a –T level unless implementing C, X1 (or X2) and X-L1 (or X-L2) levels before. Should the “and” present in line 298 (clause 7.4) be changed into a “or” or clause 4.1.3.2 clearly state that -A level must be built from -C, X1or2, and XL1or2 successively ?	• Clarify on what levels a -A level can be built. In particular, it must be very clear what are the possible construction and which are not possible, e.g. o BES/EPES → T → C → X1/2 →XL1/2 → A o BES/EPES → T → A (however in this case is it really the same A than above ? strictly speaking this is more an Abis level ... what is the difference between such an Abis level and the LTA level ...) o BES/EPES → T → LT → LTA (possible to build an LTA directly ?) o ... ? • Make the above clear from clause 4.1.3.2. Explain also why intermediate forms are made available and why they are provided in annex. • Update clause 7.4	Partially accepted. Indeed clause 7.4 is not correct. It should read: “A XAdES signature claiming conformance to XAdES-A level shall be built upon signatures compliant with XAdES-T, XAdES-C, XAdES-X (type 1 or 2), or XAdES-XL (type 1 or 2) conformance levels” It is not shared the opinion that this adds confusion with XAdES Baseline Profile conformance levels. Below follows some rationale. The comment includes two additional issues: 1. A new XAdES-A bis? It is rejected to distinguish within the core specification between different types of XAdES-A based on the different combinations of properties, as what is essential to any XAdES-A signature is the presence of all the required validation material for validating the signature and any present time-stamp (except the last archive time-stamp) and at least one archive time-stamp that covers them. A XAdES-A directly built on a XAdES-T incorporates the validation material of the signing certificate, the signature time-stamp token, its validation material and one or more archive time-stamp tokens. In terms of validation capability is the same situation as a XAdES-A that is built on a XAdES-X-L, the only difference being that in the second one the life cycle of the signature has required incorporation of references to the validation material, and some time-stamps on these references before adding the validation material

				However-A can be built directly from T, is it really the same A than the "complete one" ? Strictly speaking this would be more an Abis level ... BUT what is the difference between such an Abis level and the LTA level ? Really confusing !!!!	**accordingly.**	**itself and the archive time-stamp…what we have here are different combination of properties that allow getting certain XAdES form. In fact this kind of things also happen with XAdES-BES: also there one may have different combinations of properties, and in the extreme cases, one could have a XAdES-BES without any XAdES property only including the signing certificate and covering it with the signature. In consequence the STF team considers that adding new sub-types would generate confusion among implementers and readers.** **2. The comment mentions LTA signatures in XAdES Baseline Profile and claims that this is confusing. The STF accepts that a note within the Baseline Profile explaining that XAdES signatures conformant to LTA-level are a specific instantiation of XAdES-A signatures. The STF has decided not to include any mention to LTA level within the core specification document.** **TO DO: change sentence in 7.4 to:** **“A XAdES signature claiming conformance to XAdES-A level shall be built upon signatures compliant with XAdES-T, XAdES-C, XAdES-X (type 1 or 2), or XAdES-XL (type 1 or 2) conformance levels”** **Add a note within the XAdES Baseline Profile (and also in the CAdES Baseline Profile) explaining that XAdES (CAdES) signatures compliant with LTA-level of Baseline Profile are specific instantiations of XAdES (CAdES)-A signatures.**

Public Review: Comments on Draft ETSI EN 319 132

XML Advanced Electronic Signatures (XAdES)

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	OBSERVATIONS on each comment submitted
	4.1.3.1 (EN 319 132-1)		General	FEEDBACK TO EDITOR NOTE It is considered useful to include a referencing mechanism to the time-mark to allow automatic processing	.	Rejected. The feedback was very useful. However, the STF finally decided to reject the possibility to include a reference to a time-mark into the signature, due to several reasons: 1. The reference can only be an unsigned reference, thus as long as it is not covered by another time-stamp, it has no sure information. 2. There is no specific format for time-marks. It could have multiple forms, like a within a Trusted Service Provider, a signed document, etc. As long as there is no information on in which form the time-stamp is stored, it is not feasible to provide a link to the time-mark that can be automatically processed.
	2.1 [8] (EN 319 132-2]		General	TS 102 176-1 could be replace with TS 119 312		Accepted. Also, a note will be added explaining that TS 119 132 was already published by TS 102 176-1

Public Review: Comments on Draft EN 319 132-1 V0.0.4 (2013-11)

Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signatures (XAdES); Part 1: Core Specification

Organization name	**Clause/ Subclause**	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change**	**OBSERVATIONS** on each comment submitted
			General	**It would have been interesting to define the term "Attribute certificate" since this notion is used several times.**		**Rejected. Instead it is proposed to make an explicit reference to the normative specification that defines its format (RFC), as in CAdES:** [8] IETF RFC 5755 (2010): "An Internet Attribute Certificate Profile for Authorization"
	Keywords		**Technical**	**Keywords are missing**		**Accepted. Add some keywords. Align with CAdES, ASiC and PAdES in order to share the common keywords.**
	Informative references	**2.2**	**Technical**	**"[i.2] ETSI TS 101 903 v1.4.2: Electronic Signatures and Infrastructures (ESI); XML Advanced 281 Electronic Signature (XAdES)"** **From my understanding, this reference become deprecated par the issuance of new standards on XML Advanced Electronic Signatures (XAdES).** **Is it really necessary to mention deprecated standards as informative references**		**Accepted: Elimination of informative reference to ETSI TS 101 903 v1.4.2.** **Reject the elimination. But eliminate the version number.** **Make similar usage as in CAdESin foreword:** The present document was previously published as TS 101 903 [i.??].

	Overview	**4**	**Technical**	**The present document defines a set of signature properties that may be combined to obtain electronic signature forms providing satisfaction of different requirements. Below follows a short overview of the properties:** **• SigningCertificate and xadesenv111:SigningCertificate .** **Why do we have 2 attributes with the same name that reference the same information, i.e., the signing certificate?** **It's a little confusing** **If xadesenv111:SigningCertificate is used for acknowledging deprecation of ds:X509IssuerSerial, why don't we mentioned the two properties** **SigningCertificate and ds: X509IssuerSerial (deprecated).**		**Accepted deprecation of all the XAdES properties that build on ds:X509IssuerSerial element, moving them to the annex and making it clear that new signatures shall generate the new properties, but applications shall also be able to validate legacy XAdES signatures including old properties. Affected properties:** **xades:SigningCertificate, xades:CompleteCertificateReferences, xades:AttributeCertificateRefs.** **To be decided the deprecation strategy. Interim period for leaving time to implementers to change their applications?**
	Basic electronic signature (XAdES-BES)	**4.1.1**	**Technical**	**Line 516 : the node <([Ref.to signing certificate])> should be replaced by <SigningCertificate>, as in the previous standard (TS 101 903 v010401)** **In §6.2.2.1 an element SigningCertifcate id defined as a property that "contains references to certificates and digest values computed on their DER encodings."**		**Agreed. Change to xadesenv111:SigningCertificate** **Apply the same change in every occurrence.**
	Basic electronic signature (XAdES-BES)	**4.1.1**	**Technical**	**New element should defined in this standard should be based on URI value is http://uri.etsi.org/19132/v0.0.4 instead of http://uri.etsi.org/01903/v1.1.1**		**Rejected. The v1.1.1 corresponds to the version number that the ETSI EN shall have when it will be published as European Standard.**

	Basic electronic signature (XAdES-BES)	**4.1.1**	**Technical**	**Line 512** **Node <SignedProperties> is not mandatory. It should be, as in the previous standard (TS 101 903 v010401)**		**Rejected: Specifications 101903 v1.4.1 was wrong as a XAdES-BES can be built without adding any XAdES qualifying property by incorporating the signing certificate within the ds:KeyInfo and covering such certificate with the signature.** **Additionally, the XML Schema of xades:QualifyingProperties clearly specify xades:SignedProperties as optional (minOccurs=”0”) in its clause 6.2.** **The absence of the question mark character is clearly a mistake that the EN 319 132 fixes.**
	Basic electronic signature (XAdES-BES)	**4.1.1**	**Technical**	**Line 510** **Node <QualifyingProperties> is not mandatory. It should be, as in the previous standard (TS 101 903 v010401)**		**Rejected: same reasons as in previous disposition.**

Public Review: Comments on Draft ETSI <EN> <319 132-2 > V<V0.0.4 (2013-11)>

< XML Advanced Electronic Signatures (XAdES); Part 2: XAdES Baseline Profile >

Organization name	**Clause/ Subclause**	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change**	**OBSERVATIONS** on each comment submitted
	General			Germany highly appreciates the activities at ETSI M/460 phase 2, which address particularly long term aspects of electronic signatures. However it seems that the current scope of the proposed • "Draft EN 319 132-2 V0.0.4 (2013-11) Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signatures (XAdES); Part 2: XAdES Baseline Profile" only covers approaches without an optional usability of Evidence Records according RFC 4998 and RFC 6283, which are not optimal with respect to scalability because without the usage of Evidence Records each archived document requires independent archive time stamps.		**See resolutions 1, 2 and 3 on the incorporation of ERS within (C/P/X)AdES specifications.**

	General			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) and • ISO 14533-2:2012 Processes, data elements and documents in commerce, industry and administration -- Long term signature profiles -- Part 2: Long term signature profiles for XML Advanced Electronic Signatures (XAdES) (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/BSI TR03125.html . (2011). and even • EN 319 122 CMS Advanced Electronic Signatures (CadES) Part 1 <http://docbox.etsi.org/ESI/Open/Latest_Drafts/prEN-319122-1v003-CAdES-core-STABLE-DRAFT.pdf> : Core Specification. ! Whereas XAdES-A requires one time stamp per signature for a re-signing document the Evidence Record syntax standardised by IETF in RFC 4998 and RFC 6283 uses Merkle Hash Trees such that only one time stamp is required for a complete re-signing cycle of different documents.	Therefore it is proposed to enlarge the scope of the Draft ETSI EN 319 132-2 V0.0.4 (2013-11) to cover alternative approaches as well, which are based on the Evidence Record Syntax normalized in RFC 4998 and RFC 6283 and may be integrated with archival systems based on ISO 14721, ISO 14533 {C,X}AdES, OASIS DSS v1.0 Profile for Comprehensive Multi-Signature Verification Reports, DIN 31647 and BSI-TR03125 . **Proposed solution for XAdES:** The Evidence Record attribute shall be integrated in XAdES (as well as in in CAdES and PAdES) as an ordinary attribute. .	**See resolutions 1, 2 and 3 on the incorporation of ERS within (C/P/X)AdES specifications**

	Chapter 2.1 E	Normative references	E		**Proposal:** Add: [11] IETF RFC 4998 (2007): "Evidence Record Syntax (ERS)" [12] IETF RFC 6283 (2011): "Extensible Markup Language Evidence Record Syntax (XMLERS)"	
	Chapter 4	Conformance Levels	T	**Current Text:** d) LTA-Level profiles the incorporation of time-stamp tokens that allow validation of the signature long time after its generation. This level is understood to tackle the long term availability and integrity of the validation material.	**Proposal:** d) LTA-Level profiles the incorporation of time-stamp tokens **or Evidence Records** that allow validation of the signature long time after its generation. This level is understood to tackle the long term availability and integrity of the validation material.	**See resolutions 1, 2 and 3 on the incorporation of ERS within (C/P/X)AdES specifications.**
	Chapter 9	Requirements for LTA-Level Conformance	T	**Current Text:** “A XAdES signature conformant to LTA-Level shall be a signature conformant to LT-Level to which one or more xades:ArchiveTimeStamp (or xadesv141:ArchiveTimeStamp) have been directly incorporated.”	**Proposal:** “A XAdES signature conformant to LTA-Level shall be a signature conformant to LT-Level to which one or more xades:ArchiveTimeStamp (or xadesv141:ArchiveTimeStamp) **or Evidence Record** have been directly incorporated.”	**See resolutions 1, 2 and 3 on the incorporation of ERS within (C/P/X)AdES specifications.**
	Chapter 9	Requirements for LTA-Level Conformance	T	**Current Text:** Evidence Record is missing in Table 17	**Proposal:** Please add Evidence Record in Table 17	**See resolutions 1, 2 and 3 on the incorporation of ERS within (C/P/X)AdES specifications.**

Service/Protocol element	XAdES [1] Reference		Generator requirement
Service: add archive time-stamp	Clause 6.5		M
xadesv141:ArchiveTimeStamp	Clause 6.5.2		**O**
Evidence Record	**Clause 6.5.4**		**O**

Public Review: Comments on Draft EN 319 132-2 V0.0.4 (2013-11)

Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signatures (XAdES); Part 2: Baseline Profile

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	OBSERVATIONS on each comment submitted
	Conformance Levels	4	Editorial	What's the meaning of this sentence: "c) LT-Level profiles the incorporation of all the material required for validating the signature in the signature."?		Indeed the wording was wrong and needs to be improved. Proposed alternative: c) LT-Level profiles the incorporation in the signature of all the material required for its validation."
	Requirements for LT-Level Conformance	8	Technical	The standard does not specify which signature form (BES, EPES,T or A) can claim conformance to the LT-Level. Does a XADES-A signature have to claim conformance to the LTA-Level?		Add an explanatory note to the baseline profile explaining that the combination of properties for LT conformance level does not correspond to any of the XAdES forms defined within XAdES core specification. As for the second question, NO. A XAdES signature conformant to LTA-Level in XAdES Baseline Profile is a specific instantiation of a XAdES-A signature. In summary, any XAdES LTA-conformance level conformant signature is a XAdES-A signature, but it is not true that any XAdES-A signature is a Baseline XAdES-LTA conformant signature….Please refer to a former disposition of the STF consisting in adding an explanatory note on this issue within the XAdES (CAdES) Baseline Profile specification.