

1	2	(3)	4	5	(6)	(7)
NB <sup>1</sup>	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment <sup>2</sup>	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
US 1	Introduction		ge	<p>The distinction between time-stamp signatures and stand alone time stamps are poorly motivated and defined.</p> <p>The time-stamp signature defined in this document has no defined relationship with CMS. One could guess that it is implied but it is not specifically stated. The definition of TimeStampToken on the other hand implies that a token can be both a time-stamp signature (as defined in 6.1) or as a stand alone evidence (as defined in 6.2). This creates a very confusing circularity.</p> <p>If Time-stamp signatures are clearly defined as signatures for a defined document encapsulation format, containing the signed document (specifically CMS for 6.1), then there is no need to make a TimeStamp token a CHOICE between ContentInfo and SignerInfo.</p>	<p>Restore the ASN.1 of RFC 3161 and define:</p> <pre>TimeStampToken ::= ContentInfo</pre> <p>For ASN.1 type definitions, either clearly motivate and define Time-stamp signatures as an extra signature to a CMS encapsulated document (where contentType is id-signedData), or remove stand alone evidence time-stamping signatures all together from the standard</p>	
US 2	1		ed	The text past the first two paragraphs ("The following entities..." till the end of page 1) is a general discussion of timestamping, entities, protocols, and renewal. The scope should contain a few short sentences; it shouldn't go into detailed discussion of specifics.	Move the text past "The following entities..." till the end of page 1 to a separate Clause within the document.	
US 3	1		ed	The term "time-stamp verification requester" is not defined in 18014-1. The term "time-stamp verifier" is defined differently in 18014-1.	Use the "time-stamp verifier" term only, and use it as defined in 18014-1 (definition repeated in Clause 3 of 18014-2).	
US 4	6.1		ge	The need for and use of time-stamping signatures needs to be elaborated. The statement "The aim is to provide one more signature for a document, being this additional signature of special relevance with respect to the time." seems to be out of context and hard to understand unless one knows if this structure can be stand alone or must be part of a full CMS construct.	<p>Clearly define the use of SignerInfo.</p> <ul style="list-style-type: none"> <li>To what extent it MUST be associated with a complete CMS message.</li> <li>What CMS content type MUST be used (SignedData)</li> </ul>	

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by \*\*)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

**NOTE** Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
NB <sup>1</sup>	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment <sup>2</sup>	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
				<p>If the SignerInfo is part of a CMS message, then this would not necessarily provide "one more signature" but could also just add time stamping information to a signature, given that the signer acts as the TSA. It's not clear if that is part of the purpose, or even allowed.</p> <p>As there is no clear definition for how this SignerInfo is related to a complete message (CMS, RFC 3852) there is consequently no clear definition of what the hash of the signature is calculated over. If SignerInfo is a stand alone object, then the context of CMS is broken, which requires the hash to be calculated over the message content (encapContentInfo) and, if present, any signed attributes.</p> <p>If this construct is used outside of the context of CMS, then the rules for using it must be provided here.</p>	Reference to the rules of CMS regarding, in particular the calculation of the Hash for the signature	
US 5	6.1		te	The definition of TS-Signature is redundant as it just repeats the structure of TSTInfo	Replace current definition with: TS-Signature ::= TSTInfo	
US 6	6.1		ge	<p>The use of time-stamp signatures represents an alternative way to protect time-related info (e.g. TstInfo) using a digital signature. Other than the ability to combine multiple SignerInfos in one container of signed data on the client side(!), it is not clear that this variation offers any benefit.</p> <p>Having multiple TSAs assert time-related data in the same multi-signed "token" at once adds significant complexity to any software application that supports token verification for the variety of tokens described here. Each signature may carry different time/policy/nested renewal chain, so the validity of an asserted time value and policy for the whole multi-signed token can no longer be a true/false proposition.</p>	Preferably delete Clause 6.1. Update text in Introduction Clause accordingly.	

1 MB = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by \*\*)

2 Type of comment: ge = general te = technical ed = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
NB <sup>1</sup>	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment <sup>2</sup>	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
				This added complexity is better handled at the application level. Timestamp requesters can handle multiple tokens from different TSAs for the same or different documents through appropriate workflows, document management system rules, and business logic for verification (i.e. which token to verify for a given document on behalf of the relying party).		
US 7	6.2		te	<p>The encapsulation of TSTInfo within a TimeStampToken is missing in the document.</p> <p>Following CMS and RFC 3161, the encapsulation must be as follows:</p> <pre>SignedData ::= (Defined in CMS)</pre> <pre>EncapsulatedContentInfo ::= SEQUENCE {     eContentType      ContentType,     eContent          [0] EXPLICIT OCTET STRING                     OPTIONAL }</pre> <pre>ContentType ::= OBJECT IDENTIFIER</pre> <p>The fields of type EncapsulatedContentInfo of the SignedData construct have the following meanings:</p> <p>eContentType is an object identifier that uniquely specifies the content type. For a time-stamp token it is defined as:</p> <pre>id-ct-TSTInfo OBJECT IDENTIFIER ::= { iso(1) member-body(2)us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) ct(1) 4 }</pre> <p>eContent is the content itself, carried as an octet string.</p> <p>The eContent SHALL be the DER-encoded value of TSTInfo.</p>	Clarify the encapsulation of TSTInfo in TimeStampToken and include necessary normative references and a way that aligns with RFC 3161.	

1 MB = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by \*\*)

2 Type of comment: ge = general te = technical ed = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
NB <sup>1</sup>	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment <sup>2</sup>	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
US 8	6.2.5		ge	The use of this extension depends on the construct of signatures/standalone tokens, both for ASN1 and XML tokens. If this distinction is not applicable, this extension is no longer needed.	Preferably delete Clause 6.2.5.	
US 9	6.2.6		ge	The use of this extension is not well defined, and it may even be out of scope for 18014-2 ("mechanisms producing independent tokens").  Details: ISO/IEC 18014-3 defines data type BindingInfo and describes how the linking TSA populates an instance of BindingInfo for every generated TSTInfo. It also describes a signing mechanism that further protects the TSTInfo and accompanying BindingInfo within a signed data content info. The signed time-stamp token generated in this manner is backwards compatible with the ones generated by the digital signature mechanism in 18014-2 (i.e. the additional BindingInfo element appears as a signed attribute). It is not clear how the definition of ExtLink presented here relates to the data types and mechanisms defined in 18014-3.	Delete Clause 6.2.6.	
US 10	7.2		ge	Dividing XML timestamps into two classes (signatures and standalone containers) adds the same complexity as the equivalent split of signatures/standalone tokens for ASN1 time-stamps. No justification is offered why this is beneficial. It is preferable to merge 7.1 and 7.2 into one Clause, "XML timestamps using XML Dsig". In this case, XMLDsig (which also supports MACs) is the protection mechanism for the XML tokens.	Merge 7.1 and 7.2 into a single clause for XML time-stamp tokens.	
US 11	11		ge	An effort should be made to keep the definitions provided here in sync with the OASIS DSS Core and Timestamping documents. For example, the placement	Track the DSS documents to avoid discrepancies (especially on renewal).	

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by \*\*)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

**NOTE** Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
NB <sup>1</sup>	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment <sup>2</sup>	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
				of the renewal element may not be compatible with the latest DSS time-stamping profile document (wd-11).	Remove Format element.	
US 12	Annex A			<p>Current definition:</p> <pre>tss-attribute OBJECT IDENTIFIER ::= { tss extension(10) }</pre> <p>This attribute definition seems wrong considering the definitions:</p> <pre>tss-attribute OBJECT IDENTIFIER ::= { tss extension(10) }</pre> <pre>tss-ext OBJECT IDENTIFIER ::= { tss extension(1) }</pre> <p>It seems that the definition should either say:</p> <pre>tss-attribute OBJECT IDENTIFIER ::= { tss attribute(10) }</pre> <p>or</p> <pre>tss-attribute OBJECT IDENTIFIER ::= { tss-ext 10 }</pre>	Clarify definition of tss-attribute.	
US 13	Annex C		ge	It is not clear why this informative Annex is being added to this part of 18014. Most, if not all, of the material included here applies to all mechanisms of time-stamping. A large portion of the material included here falls strictly under the auspices of WG1.	Determine if the proposed Annex is better moved to 18014-1, or to its own separate part of the 18014-* series; seek close collaboration with WG1 experts.	

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by \*\*)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

**NOTE** Columns 1, 2, 4, 5 are compulsory.