

CS1/06-0214 Surety Contribution

[MB¹] NB comments on ISO/IEC 3rd WD 18014-2 (revision)

Date: 2006-MM-DD	Document: SC27 N5134
------------------	-----------------------------

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
US	1 Scope		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	1 Scope		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	6.1 Time-stamping Signatures		ge	The motivation behind this Clause is unclear. This 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(!), this variation doesn't seem to offer any benefit. Having multiple TSAs assert time-related data in the same multi-signed "token" adds significant complexity to any software application that supports tokens of the variety described here. Each signature may carry different time/policy/nested renewal chain, so the validity of the asserted time value and policy in the multi-signed token can no longer be a true/false proposition. If multiple tokens from different TSAs for the same document are warranted, it should be the application's responsibility to manage them. The verification of an individual token should not be further complicated.	Preferably delete Clause 6.1. Update text in Introduction Clause accordingly.	
US	6.2.5 ExtFormat extension		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.	

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 ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
US	6.2.6 ExtLink extension		ge	<p>The use of this extension is not well defined, and it may even be out of scope for 18014-2 (“mechanisms producing independent tokens”).</p> <p>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.</p>	Delete Clause 6.2.6.	
US	7.2 Standalone evidences		ge	<p>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.</p>	Merge 7.1 and 7.2 into a single clause for XML time-stamp tokens.	
US	11 XML protocols		ge	<p>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 of the renewal element may not be compatible with the latest DSS time-stamping profile document (wd-11).</p>	Track the DSS documents to avoid discrepancies (especially on renewal). Remove Format element.	
US	Annex C Best		ge	<p>It is not clear why this informative Annex is being added to this part of 18014. Most, if not all, of the material</p>	Determine if the proposed Annex is better moved to 18014-1, or to its own	

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.

CS1/06-0214 Surety Contribution

[MB¹] NB comments on ISO/IEC 3rd WD 18014-2 (revision)

Date: 2006-MM-DD	Document: SC27 N5134
------------------	-----------------------------

1	2	(3)	4	5	(6)	(7)
NB¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of com- ment²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
	Practice			included here applies to all mechanisms of time-stamping. A large portion of the material included here falls strictly under the auspices of WG1.	separate part of the 18014-* series; seek close collaboration with WG1 experts.	
US	Annex D		te	No justification is provided for the fact that the serialNumber element of TSTInfo is defined to be OPTIONAL. This is incompatible with the definition in 18014-1.	Make the definition of TSTInfo match the definition already present in 18014-1.	

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.