Template for comments and secretariat observations

Date: 2013-06-03	Document: **WG 23/N0455** Document: **SC 22N4781**	Project: ISO/IEC 17960

MB/ NC[1]	**Line number** (e.g. 17)	**Clause/ Subclause** (e.g. 3.1)	**Paragraph/ Figure/ Table/** (e.g. Table 1)	**Type of comment**[2]	**Comments**	**Proposed change**	**Observations of the secretariat**
GB				ge	The document has not been prepared using the ISO template.	Reformat using the template.	Document has been reformatted according to ISO STD template 2.1
GB	5	Introduction		ed	The phrase 'protection' is unnecessarily vague'.	Insert 'integrity' before 'protection of the source code'.	Changed
GB	11	1		ed	The text 'can be easily spoofed' reads awkwardly. It is believed that work on code signing already exists in SC7/WG21. It would be helpful if this work was referenced and its relationship with this proposal established	Change to 'can easily be spoofed'.	Changed
GB	4 clause 1	2		te	The text 'not within the same entity' unnecessarily restricts the scope. Why should a large organisation be prevented from applying this standard for internal use? There are numerous known problems with digital signatures, caused by transmission media modifying the data sent to logically equivalent but representationally different forms - see the attached document "Representation issues in file transfer"	Delete this phrase. The document should acknowledge the existance of this issue, and either explain why it is not an issue in this case or how it is to be addressed	Deleted Second issue is a duplicate of the last GB comment.
GB	9/10 clause 2	3		te	There is an ISO/IEC equivalent to X.509 (ISO/IEC 9594-8).	Add ISO/IEC 9594-8.	Added
GB	1 clause 3	4		ed	Improve wording.	Insert 'the' before 'purposes'.	Changed
GB	3 clause 4			te	Is it permitted to state that a clause in the main body of a standard is informative ? Surely the contents of the main body is normative by definition?	Change 'is informative, providing' to 'provides'.	Changed
GB	4 page 9	5		ed	The term 'meta data' is usually written as a single word.	Change to 'metadata'.	Changed
GB	Page	6.2		ge/te	The description of signature generation is	Replace all but the final sentence of the text	***Will discuss with

1 **MB** = Member body / **NC** = National Committee (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

Template for comments and secretariat observations

Date: 2013-06-03	Document: **WG 23/N0455** Document: **SC 22N4781**	Project: ISO/IEC 17960

MB/ NC[1]	**Line number** (e.g. 17)	**Clause/ Subclause** (e.g. 3.1)	**Paragraph/ Figure/ Table/** (e.g. Table 1)	**Type of comment**[2]	**Comments**	**Proposed change**	**Observations of the secretariat**
	10				inconsistent with modern cryptography. In particular, generating a signature **does not** involve 'encrypting' a hash code.	of 6.2 with the following. A digital signature shall be generated on the source code, using the private key of the originator. The signature technique to be used shall be one of those specified in ISO/IEC 9796 or ISO/IEC 14888. Generation of a signature using one of the techniques specified involves the use of a hash-function to compute a hash-code of the source code. The hash-function to be used should preferably be Secure Hash Algorithm-256 (SHA-256), as specified in ISO/IEC 10118-3:2004; alternatively, another hash-function specified in ISO/IEC 10118-3:2004 or its later revisions could be used. [Then insert the final sentence of the current text].	the SC22 WG23 at meeting #26.
GB	1 (clause 6.3)	10		Te/L	The text 'in snapshot or changeset' does not make any sense. Similar problems arise with 'Changeset shall'.	Please express in English, using articles, etc.	Use of expressions is correct; modification made to clarify.
GB		11			An article is missing at the beginning of each of numbered paragraphs 1-4	In each case insert 'The' before 'Originator'.	Changed
GB		12			Numbered steps 3 and 4 incorrectly refer to generating a signature as computing a hash-code and then encrypting it (see also the comment on 6.2).	Reword as a single step in line with the changed text proposed for clause 6.2.	
GB		13			There is no reference to how the recipient obtains the public key of the originator necessary to verify the signature on the source code.	Add an additional step after the current step 5, worded as follows. The recipient shall obtain a trusted copy of the public key of the originator. This can be achieved by the recipent obtaining a copy of the public key certficate of the originator, and verifying it using a trusted copy of the public key of the CA that generated the certificate.	Added, removed “shall” from suggested text since this is a notional process.

[1] **MB** = Member body / **NC** = National Committee (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

Template for comments and secretariat observations

Date: 2013-06-03	Document: **WG 23/N0455** Document: **SC 22N4781**	Project: ISO/IEC 17960

MB/ NC[1]	**Line number** (e.g. 17)	**Clause/ Subclause** (e.g. 3.1)	**Paragraph/ Figure/ Table/** (e.g. Table 1)	**Type of comment**[2]	**Comments**	**Proposed change**	**Observations of the secretariat**
GB		14			Numbered steps 6-8 are incorrect.	Replace these three steps with a single step along the following lines. The recipient shall verify the digital signature using the originator's public key. If the signature verifies correctly then the recipient has assurance that the source code has not been altered since it was digitally signed. To verify previously signed [text continues as in step 8].	***Will discuss with the SC22 WG23 at meeting #26.
GB	Ref 4	15			The title of ISO/IEC 9796-2 is incorrect.	Change 'signatures with appendix' to 'signature schemes giving message recovery'.	Corrected
GB					It is believed that work on code signing already exists in SC7/WG21. It would be helpful if this work was referenced and its relationship with this proposal established		SC7/WG21 is working on software identity (SWID) tags which attach metadata to software executables. The format of the SWID tags is specified in ISO/IEC 19770-2. The relationship is very distinct and so a reference is not recommended.
GB					There are numerous known problems with digital signatures, caused by transmission media modifying the data sent to logically equivalent but representationally different forms - see the attached document "Representation issues in file transfer"	The document should acknowledge the existance of this issue, and either explain why it is not an issue in this case or how it is to be addressed	***Will discuss with the SC22 WG23 at meeting #26.
GB						Reformat using the template.	Reformatted

[1] **MB** = Member body / **NC** = National Committee (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

Template for comments and secretariat observations

Date: 2013-06-03	Document: **WG 23/N0455** Document: **SC 22N4781**	Project: ISO/IEC 17960

MB/ NC[1]	**Line number** (e.g. 17)	**Clause/ Subclause** (e.g. 3.1)	**Paragraph/ Figure/ Table/** (e.g. Table 1)	**Type of comment**[2]	**Comments**	**Proposed change**	**Observations of the secretariat**
JP 1				ge	In the NP proposal for this project (SC22 N4698), the scope of this standard is explained as follows. Scope This International Standard uses a language and environment neutral description to define the application program interfaces (APIs) and supporting data structures necessary to support the signing of code and executables. It is intended to be used by both application developers and systems implementers. Regrettably, the current draft (SC22 N4781) does not follow this plan. It does not have any concrete requirements on APIs or data structures. It simply contains a few vague guidelines probably to be followed by human operators. Based on this observation, Japan disapproves the CD. It seems useless to have such a standard. However, Japan considers that a standard on code signing is necessary and the intended scope in the NP proposal is appropriate.	***Will discuss with the SC22 WG23 at meeting #26.	

[1] **MB** = Member body / **NC** = National Committee (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