

MB/ NC	Line number (e.g. 17)	Clause/ Subclause (e.g. 3.1)	Paragraph/ Figure/ Table/ (e.g. Table 1)	Type of ² comment	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. Due to reformatting, the clause numbers were necessarily changed to match the 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 existence 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	Change 'is informative, providing' to 'provides'.	Changed

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

MB/NC	Line number (e.g. 17)	Clause/ Subclause (e.g. 3.1)	Paragraph/ Figure/ Table/ (e.g. Table 1)	Type of ² comment	Comments	Proposed change	Observations of the secretariat
					normative by definition?		
GB	4 page 9	5		ed	The term 'meta data' is usually written as a single word.	Change to 'metadata'.	Changed
GB	Page 10	6.2		ge/te	The description of signature generation is inconsistent with modern cryptography. In particular, generating a signature does not involve 'encrypting' a hash code.	Replace all but the final sentence of the text 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].	Changed
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.	Usage of the terms is correct, however clarifying words have been added.
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.	Changed
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 recipient obtaining a copy of the public key	Added, removed "shall" from suggested text since this is a notional process and the annex is informative.

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

MB/ NC	Line number (e.g. 17)	Clause/ Subclause (e.g. 3.1)	Paragraph/ Figure/ Table/ (e.g. Table 1)	Type of ² comment	Comments	Proposed change	Observations of the secretariat
						certificate of the originator, and verifying it using a trusted copy of the public key of the CA that generated the certificate.	
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].	Accepted in principle. As this is a notional process and the annex is informative, "shall" was not used.
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 used.
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 existence of this issue, and either explain why it is not an issue in this case or how it is to be addressed	It is agreed that transmission and representation could be an issue, but this is outside of the scope of this document. As this is a known issue, it is covered in many other

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

MB/ NC	Line number (e.g. 17)	Clause/ Subclause (e.g. 3.1)	Paragraph/ Figure/ Table/ (e.g. Table 1)	Type of ₂ comment	Comments	Proposed change	Observations of the secretariat
							documents and standards. To clarify that this issue is outside of the scope of the standard, added in clause 1, Scope, that transmission and representation issues are outside of the scope of the document.
GB						Reformat using the template.	Reformatted
JP 1				ge	<p>In the NP proposal for this project (SC22 N4698), the scope of this standard is explained as follows.</p> <p>Scope</p> <p>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.</p> <p>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.</p>		Changes have been made throughout the working draft that aligns it with the NP proposal. Of particular note regarding the APIs, requirements have been added in clause 6. Conformance with the standard requires the APIs outlined in Clause 6 to be specified. It was agreed at meeting number 26 of WG 23 that specific definitions of APIs and data structures could be done in later revisions

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

MB/ NC	Line number (e.g. 17)	Clause/ Subclause (e.g. 3.1)	Paragraph/ Figure/ Table/ (e.g. Table 1)	Type of ² comment	Comments	Proposed change	Observations of the secretariat
					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.		of IS 17060.

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