ISO/IEC/JTC 1/SC 22/WG 23 N0494

Text

Ballot Information

Reference	ISO/IEC DIS 17960	**Committee**	ISO/IEC JTC 1/SC 22
Edition number	1		
English title	Information technology -- Programming languages, their environments and system software interfaces -- Code signing for source code		
French title	Titre manque		
Start date	2014-06-25	**End date**	2014-09-25
Opened by ISO/CS on	2014-06-25 00:04:43	**Closed by ISO/CS on**	2014-09-27 00:08:50
Status	Closed		
Voting stage	Enquiry	**Version number**	1
Note			

Result of voting

P-Members voting: 12 in favour out of 13 = 92 % (requirement >= 66.66%)

(P-Members having abstained are not counted in this vote.)

Member bodies voting: 1 negative votes out of 14 = 7 % (requirement <= 25%)

Approved

Votes by members

Country	Member	Status	Approval	Disapproval	Abstention
Armenia	SARM	P-Member			X
Australia	SA	P-Member			X
Austria	ASI	P-Member			X
Belgium	NBN	P-Member			X
Canada	SCC	P-Member	X		
China	SAC	P-Member	X		
Costa Rica	INTECO	P-Member			X
Côte d'Ivoire	CODINORM	P-Member			X
Czech Republic	UNMZ	P-Member	X		
Denmark	DS	P-Member	X		
Finland	SFS	P-Member			X
France	AFNOR	P-Member			X
Gabon	ANTT				X

Germany	**DIN**	**P-Member**			X
India	**BIS**	**P-Member**			X
Ireland	**NSAI**	**P-Member**	X		
Italy	**UNI**	**P-Member**	X		
Japan	**JISC**	**P-Member**	X *		
Kazakhstan	**KAZMEMST**	**P-Member**			X
Korea, Republic of	**KATS**	**P-Member**	X		
Lebanon	**LIBNOR**	**P-Member**			X
Malaysia	**DSM**	**P-Member**			X
Malta	**MCCAA**	**P-Member**			X
Netherlands	**NEN**	**P-Member**	X		
Norway	**SN**	**P-Member**			X
Peru	**INDECOPI**	**P-Member**			X
Russian Federation	**GOST R**	**P-Member**	X		
Singapore	**SPRING SG**	**P-Member**			X
Slovenia	**SIST**	**O-Member**			X
South Africa	**SABS**	**P-Member**			X
Spain	**AENOR**	**P-Member**			X
Sweden	**SIS**	**P-Member**			X
Switzerland	**SNV**	**P-Member**			X
Ukraine	**DTR**	**O-Member**	X		
United Arab Emirates	**ESMA**	**P-Member**	X		
United Kingdom	**BSI**	**P-Member**		X *	
United States	**ANSI**	**Secretariat**	X		
P-Member TOTALS Total of P-Members voting: 13			12	1	21
TOTALS			13	1	23
(*) A comment file was submitted with this vote					

Comments from Voters

Japan	**JISC**	**P-Member**	ISO_IEC DIS 17960_JISC.doc
United Kingdom	**BSI**	**P-Member**	ISO_IEC DIS 17960_BSI.doc

Template for comments and secretariat observations

Date:2014-10-22	Document:	Project:

MB/ NC[1]	Line number	Clause/ Subclause	Paragraph/ Figure/Table	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.	
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'.	
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		
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	
JP 1				ed	The terms “this document”, “this specification”, and “this International Standard” are used to refer to the standard itself.	A single term such as “this standard” should be used throughout the standard.	0
JP 11				ed	The standard name given in footnote 2 is not consistent with Bibliography 16 in the use of uppercase letters.		
JP 2				ed	The standard number 16960:201X at the beginning of page 1 is not correct.	17960 is the correct number.	
JP 3				ed	The second part of the title “Programming Languages” is not appropriate.	It should be replaced by “Programming languages, their environments and system software interfaces”.	
JP 20		Bibliography	[4]	ed	The font for the standard number “ISO/IEC 9594-8:2008” should not be Italic.		
JP 21		Bibliography	[4],[8],[9]	ed	These three standards are listed in 3. Normative references, but are not mentioned in the normative text. We consider that they should be removed from 3. Normative references. 13888-1 and 9594-8 are		

[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:2014-10-22	Document:	Project:

MB/ NC[1]	Line number	Clause/ Subclause	Paragraph/ Figure/Table	Type of comment[2]	Comments	Proposed change	Observations of the secretariat
					referred to in a quite indirect manner, and are not considered normative references. 10118-3 is referred to in 6.2, but not in a normative sentence.		
JP 4		Copyright notice		ed	There are two "Copyright notice"s. One of them should be deleted.		
JP 5		Footer of each page		ed	The copyright declaration in the footer on each page says "ISO 2013". "2013" should be changed to "2014".		
GB	5	Introduction		ed	The phrase 'protection' is unnecessarily vague'.	Insert 'integrity' before 'protection of the source code'.	
JP 6		Table of Contents		ed	The page title "Table of Contents" should be changed to "Contents" as specified in 6.1.2, Table of contents, in the Directives Part 2.		
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'.	
JP 7		1.	paragraph 1	ed	The term “previous signed versions” is not correct.	It should be “previously signed versions”.	
JP 8		1.	last two bullets	ed	The description sentences for “Metadata” and “Transmission and representation issues” do not have periods at the end of the sentence.		
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?	Delete this phrase.	

[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:2014-10-22	Document:	Project:

MB/ NC[1]	Line number	Clause/ Subclause	Paragraph/ Figure/Table	Type of comment[2]	Comments	Proposed change	Observations of the secretariat
					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	
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.	
JP 9		3.		ed	The font for the standard number “ISO/IEC 9594-8:2008” should not be Italic.		
GB	1 clause 3	4		ed	Improve wording.	Insert 'the' before 'purposes'.	
JP 10		4.4		ed	The term “source” is not a defined term. The same word is often used.	We suspect it should be replaced by “originator”.	
GB	4 page 9	5		ed	The term 'meta data' is usually written as a single word.	Change to 'metadata'.	
JP 12		5.	bullet 1	ed	The term “origin” is not defined. The same word is often used.	We suspect it should be replaced by “originator”.	
JP 13		5.	paragraph after bullets	ed	The second word of “Code Signing” should not be capitalized.		
JP 14		6		ed	Three paragraphs before 6.1 are inhibited in 5.2.4, Paragraph, in the Directives Part 2, since they cannot be identified as being in Clause 6 which also includes 6.1, 6.2, etc. A new subclause, 6.1 General, should be added and these paragraphs should be moved to new 6.1.		
JP 15		6.	paragraph 2	ed	The terms “originator” and “recipient” are defined in this clause, but their definitions are already given in 4.7 and 4.11.		

[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:2014-10-22	Document:	Project:

MB/ NC[1]	Line number	Clause/ Subclause	Paragraph/ Figure/Table	Type of comment[2]	Comments	Proposed change	Observations of the secretariat
JP 16		6.	bullet 1	ed	The term “hash code” should be “hash-code”.		
JP 17		6.	last two bullets	ed	These two bullets are not consistent in the use of “of” just after “at a minimum”.		
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].	
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.	
GB		11			An article is missing at the beginning of each of numbered paragraphs 1-4	In each case insert 'The' before 'Originator'.	
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.	

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:2014-10-22	Document:	Project:

MB/ NC[1]	Line number	Clause/ Subclause	Paragraph/ Figure/Table	Type of comment[2]	Comments	Proposed change	Observations of the secretariat
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.	
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].	
GB	Ref 4	15			The title of ISO/IEC 9796-2 is incorrect.	Change 'signatures with appendix' to 'signature schemes giving message recovery'.	
JP 18		Annex A	2-1 and 2-2	ed	This page is a list of items in two levels. The numbering for the second level should be different from that for the first level. We think that the numbering for the first level cannot be changed. The second level would better be listed using bullets.		
JP 19		Annex A	5	ed	The term “CA” should be spelled fully.		

[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