



ISO/IEC JTC 1/SC 27 **N 7793**

ISO/IEC JTC 1/SC 27/WG 3 **N 993**

REPLACES: N

**ISO/IEC JTC 1/SC 27**

**Information technology - Security techniques**

**Secretariat: DIN, Germany**

**DOC. TYPE:** dispositions of comments

**TITLE:** Dispositions of comments on ISO/IEC 3<sup>rd</sup> WD 29128 (SC 27 N 7266)  
Information technology – Security techniques – Verification of cryptographic protocols

**SOURCE:** 38<sup>th</sup> SC 27/WG 3 meeting

**DATE:** 2009-05-06

**PROJECT:** 29128

**STATUS:** Output document of the editing session for ISO/IEC 3<sup>rd</sup> WD 29128 (SC 27 N 7266) held during the 38<sup>th</sup> SC 27/WG 3 meeting Beijing, China, 4th – 8th May 2009.

This document was available at the above-mentioned meeting. It is being circulated for information.

**ACTION:** FYI

**DUE DATE:**

**DISTRIBUTION:** P-, O-, and L- Members  
W. Fumy, SC 27 Chairman, M. De Soete, SC 27 Vice Chair  
E. Humphreys, K. Naemura, M. Ohlin, M.C. Kang, K. Rannenber, WG-  
Conveners

**MEDIUM:** Server

**NO. OF PAGES:** 1 + 7

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 com- ment	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
FR 1	1, 6		ge	The general goal of “verifying cryptographic protocols” is only partially addressed by the techniques described in this standard. In particular the model outlined in Section 6 is unlikely to cover many existing cryptographic protocols and does not address all the interesting security properties (authentication, strong secrecy, etc).	The status of Section 6 being unclear, it is asked to move this section to the appendices, as an example. Other models should also be mentioned (e.g. that of Bruno Blanchet's ProVerif).	Accepted  We will try to change Clause 6 drastically and make it more general.  Move current text to Appendix.
FR 2			ge	Generally speaking, this standard should acknowledge that protocol verification (understood: by means of logical methods) is still limited 1) to certain protocols (essentially, those that use standard cryptographic primitives in a modular way) 2) to certain security properties (attackers being generally restricted to a subset of algebraic operations). This does not mean at all that logical methods are useless, but the text should recognize that equivalent, and even higher assurance levels are achievable by conventional, pen-and-paper proofs of security, in particular publicly-available and widely-accepted proofs made in the stronger “computational” models used by cryptographers.	Mathematical proofs of security in asymptotic computational models should be recognized at level PAL3. Concrete security proofs (i.e. proofs that additionally indicate how to dimension keys and other security parameters in function of the attacker's computational power) should be recognized.  Note that a few formal tools now exist to address computational models and even concrete security (e.g. Bruno Blanchet's CryptoVerif).	Accepted.  1) Cryptographically-sound proofs will be recognized in the coming text as PAL4  2) Proofs only with pen-and-paper and no computer-aided verification applied are treated as PAL1 in the current text of 29128. (but we will try to make it more explicit)  3) Proofs with pen-and-paper proofs for limited number of theorems and most of the proofs are verified mechanically using those hand-proven theorems should be considered as PAL3 or higher (PAL4) depending on whether the proof is based on cryptographic-soundness (asymptotic) or symbolic.
FR 3	6.2.3		Te	The concept of “readability tests” is rather unusual. Do the authors intend to model the computability of pattern matchings on network messages ? (Note that this is not a security property but rather a sanity check for the protocol specifications.)	If the definition of “readability tests” refers to an existing publication, please cite it and explain the motivations. Otherwise, remove this paragraph and subsequent references to this notion.	Accepted.  “Readability test” is the one artificially introduced in the current text. We will make the Clause 6 more general. “Readability test” and other artificial notions will be removed from the coming

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 com- ment	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
						draft.
FR 4	7.1	Table, 3 <sup>rd</sup> row	Ed	There is a typo in "Operating environment"	Correct "Operating environmet" into "Operating environment"	Accepted.
FR 5	Annex A	Clause 1	Ge	The first sentence is unclear	Rephrase the sentence.	Accepted.
FR 6	Annex B.3	First note	Te	Extensive testing is not evidence of correctness	If the testing is exhaustive this should be specified. Otherwise, it is necessary to include the references to existing publications that studied the subject; moreover figures concerning the testing should be noted to apprehend the extent of the evidence.	Accepted.  Add some texts in Clause 8.4 "Evidence for verification" to describe what is required to apprehend to what extent the underlying verification tool is correct. This will include test results and verification results for existing protocols.

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 com- ment <sup>2</sup>	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
JP 1	2		ge	This standard refers to all parts of ISO/IEC 15408 (especially ISO/IEC 15408-3), so it would refer also ISO/IEC 18045 for detailed activities.	Add ISO/IEC 18045 in clause 2.	Partially accepted.  We will check when clause 9 complete, and change if necessary.  [see UK 5]
JP 2	3.8		ed	Algebra *over* a signature (not from)	Replace "from" with "over".	Accepted.
JP 3	4		te	Notion of "session" is pretty standard but note that agents may execute instances of their roles which are not involved in session in the conventional (e.g., matching-histories) sense. E.g., some messages they receive come from honest agents, others come from the intruder. You might consider where you can replace "session" by "role instance".	Replace "session" with "role instance".	Accepted.
JP 4	5		te	Code inspection of the tool requires heavy workload and is often impractical for protocol designer.  "a) The verification tools are sound.  The protocol designer shall provide evidence of the correctness of the verification tool used. This may, for example, be in terms of a pencil-and-paper proof of the soundness of the calculus used <u>plus code inspection to see that the tool properly implements the calculus.</u> "	Some description that says code inspection is NOT mandatory should be included.	Accepted.  Add some texts to explicitly say that code inspection is not mandatory.
JP 5	5		ed	"Verification of *a* cryptographic protocol" ("a" missing)	Add "a" between "of" and "cryptographic".	Accepted.
JP 6	6.1.2		te	It is unclear why a decision is explicitly being made to model protocols using terms rather than bit strings for the rest of the document.	Some description about reason of the decision should be included.	Partially accepted.  Add some description about reason of the decision. For PAL4, which will be introduced in the coming text according

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 com- ment <sup>2</sup>	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
						to the resolution for FR 2, bit strings might be used in the standard.
JP 7	6.1.4		te	Note that stronger models are also possible, e.g., where the intruder can corrupt agents.	Add some note about stronger models.	Accepted. Add some notes about stronger intruder model.
JP 8	6.1.4		ed	"can not intercept *them" (rather than "it")	Replace the word "it" with "them".	Accepted.
JP 9	6.2		Te	The role of this clause is not so clear. Is this intended to be just an example of how one can formalize protocol specifications? There are possible formalizations that differ in (often subtle) ways.	Clarify the purpose of the clause. If it is just an example of possible formalizations, clearly say so.	Partially accepted. We will try to change Clause 6 drastically and make it more general. Current text will be move to appendix as an example. [see FR 1]
JP 10	6.2		Te	Note that equations can be used to weaken the perfect cryptography assumption, e.g., formalize homomorphic properties of ciphers.	Add some notes about weaker assumptions.	Accepted. Add some notes about weaker assumptions.
JP 11	6.2.3		te	It is unclear whether you have a typed model or not. E.g., are keys different from terms? If they are, this needs to be explicit. Otherwise, you have limitations e.g., no composed keys. Also there is no discussion about if encryption is asymmetric or symmetric. Maybe it doesn't matter at this level, but the reader may wonder. Also there is no discussion about other functions, e.g., hashes, etc.	Some description about type should be included.	Accepted. Add some text about type.
JP 12	6.2.3		te	Point about "readability" is unclear. When an agent receives a non readable message (like a ticket), he should simply forward it to another agent.	Add some explanation about "readability".	Partially accepted. "readability" will be removed in coming text

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
						[see FR 3]
JP 13	6.3.1		ed	The word "falsify" is commonly used instead of "fake".	Replace "fake" with "falsify".	Accepted.
JP 14	6.3.4		ed	Do you use the phrase "a state transition" for "a reachable state"?	Replace "a state transition" with "a reachable state".	Accepted.
JP 15	6.4.1		ed	"\$m\$" is formatted funny	Replace the word "\$m" with "m".	Accepted.
JP 16	7.1		ge	In clause 7 "Protocol Assurance Level" are defined, whereas the name of the clause is "Cryptographic protocol security levels"	Change the name of clause 7 which would be consistent with content in the clause.	Accepted. We will make the name of clause 7 consistent with content in the clause.
JP 17	7.1		ed	"tool-specific specification languages" would be better phrase than "tool-dependent languages".	Replace the phrase "tool-dependent languages" with "tool-specific specification languages".	Accepted.
JP 18	7 and 8		te	In 3 <sup>rd</sup> WD 29128, protocol specification, operating environment, and security properties shall be described in a formal language on PAL2 and higher.  Informal description is also desirable to evaluate the security of cryptographic protocols even in PAL2 and higher.	Some description should be included. (e.g. "formal description" --> "formal description complement with informal explanation")	Accepted. Add some text about informal description in higher assurance levels.
JP 19	8.2.2		ed	The word "falsified" is commonly used instead of "deflected".	Replace the word "deflected" with "falsified".	Accepted.
JP 20	8.4.1		te	It is not always clear if "evidence" is INPUT or OUTPUT to process. E.g., 8.4.3 suggests it is input to the tool but 8.4.4 suggests it is constructed by (and therefore output from) the tool.	Add some explanation about "evidence".	Accepted. Add some explanation about evidence to clarify.
JP 21	Bibliography		ed	Below are the 2 publications you should add in bibliography:	Add these references in bibliography.	Accepted.

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 com- ment <sup>2</sup>	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
				<p>David Basin, Sebastian Mödersheim, Luca Viganò, "OFMC: A symbolic model checker for security protocols", International Journal of Information Security, Springer-Verlag, 2005</p> <p>Alessandro Armando, David Basin, Yohan Boichut, Yannick Chevalier, Luca Compagna, Jorge Cuellar, Paul Hankes Drielsma, Pierre-Cyrille Héam, Olga Kouchnarenko, Jacopo Mantovani, Sebastian Mödersheim, David von Oheimb, Michael Rusinowitch, Judson Santiago, Mathieu Turuani, Luca Viganò, Laurent Vigneron, "The AVISPA Tool for the Automated Validation of Internet Security Protocols and Applications", in Proceedings of CAV'2005, LNCS 3576, Springer-Verlag, 2005</p>		

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 com- ment <sup>2</sup>	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
UK 1	-	-	Ge	Other than clause 9, this Working Draft is complete and internally consistent. In our view, it indicates substantial consensus on structure and content, and would have been suitable for balloting as a Committee Draft.	Progress to CD on next revision.	Accepted.
UK 2	All	-	Ed	The document has no page numbers.	Restore missing footers.	Accepted.
UK 3	-	-	Ed	The Asian character “☒” is used to introduce lists within the document, displayed in pdf as the symbol “•”. This could cause problems with printing and/or searching.	Use the dash symbol (decimal 190) from the ISO template to introduce unnumbered list items.	Accepted.
UK 4	1	1	Ed	“specification” is mis-spelt as “spceification”.	Correct.	Accepted.
UK 5	2	-	Ed	Based on the editor’s notes, it is more likely that any normative reference will be to ISO/IEC 18045.	Check when clause 9 complete, and change if necessary.	Accepted.
UK 6	3.8	-	Te	Section 6.2.1 does not actually use the expression “term algebra”.	Delete definition.	Partially accepted. We will change the Clause 6 to make it more general. Definition of “term algebra” will be updated.
UK 7	7.1	Table	Ed	The table lacks a number and title.	Add.	Accepted.
UK 8	8.2.1	-	Te	For consistency, a note or notes is needed to give guidelines on how informal language might be used to give such a specification.	Perhaps this could be done by listing possible components of the model and channel that might be defined and explained.	Accepted. More texts will be added to 8.2.1 to specify the required components and channels to informal protocol specification.
UK 9	8.3.2	-	Te	For consistency, a note or notes is needed to give guidelines on what aspects of the properties should be described.	Perhaps this could be done by listing attributes that might be relevant.	Accepted. More texts will be added to 8.3.2 to specify the required attributes to informal security properties.

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.