



ISO/IEC JTC 1/SC 27 **N 8125**

ISO/IEC JTC 1/SC 27/WG 3 **N 38125**

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 1st CD 29128 (SC 27 N 7794)  
Information technology – Security techniques – Verification of  
cryptographic protocols

**SOURCE:** 39<sup>th</sup> SC 27/WG 3 meeting

**DATE:** 2009-11-03

**PROJECT:** 1.27.60

**STATUS:** Output document of the editing session for 1st CD 29128 (SC 27 N 7794) held during the 39<sup>th</sup> SC 27/WG 3 meeting Redmond, USA, November 2 – 6, 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. Bañón, M.C. Kang, K. Rannenberg,  
WG-Conveners

**MEDIUM:** Server

**NO. OF PAGES:** 1+ 20

**Attachment 1 to SC 27 N8026**  
**French comments on ISO/IEC 1<sup>st</sup> CD 29128**

Date: 2009-10-08	Document: <b>SC 27 N7794</b>
------------------	------------------------------

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
FR 1			ge	The document is not yet mature and is lacking important concepts.		Withdrawn after resolution of comments.
FR 2			ge	The document is lacking to take into consideration the environment of use, the security service to accomplished (e.g. authentication, integrity, confidentiality, confidentiality of use, etc ...), the number of parties involved in the protocol, the key distribution model, the security properties of the algorithms, their speed, the key size and much more important the time of resistance for each attack.		Accepted. Operating Environment is generalized and rigorously treated as Adversarial Environment. Security services accomplished is exactly defined as Security Property, but need to be expanded to cover many security properties or security goals. The number of parties involved is a part of Protocol Specification. How to make protocol specification is important, and hence need to be described. However, speed, key size and the time of resistance are currently out of scope of this standard. This will be discussed later. Combine with Simulation Modelling in PAL 1 at this moment. But it is an interesting research topic to deal with these points in higher level like PAL3.
FR 3			ge	The document is lacking to take into consideration the usual security properties that may be required: <ul style="list-style-type: none"> <li>a. Resistance against eavesdropping,</li> <li>b. Resistance against unauthenticated queries that might exploit responses,</li> <li>c. Resistance against replay attacks,</li> </ul>	Take into consideration the usual security properties that may be required: <ul style="list-style-type: none"> <li>g. Resistance against eavesdropping,</li> <li>h. Resistance against unauthenticated queries that</li> </ul>	Accepted. Add these "typical" Security property examples will be described in Informative Annex. Contribution is expected from FR. a is generalized as Secrecy property and b-d and f are generalized as Authenticity property. The current text

<sup>1</sup> **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 \*\*)

<sup>2</sup> **Type of comment:** **ge** = general **te** = technical **ed** = editorial

**NOTE** Columns 1, 2, 4, 5 are compulsory.

**Attachment 1 to SC 27 N8026**  
**French comments on ISO/IEC 1<sup>st</sup> CD 29128**

Date: 2009-10-08	Document: <b>SC 27 N7794</b>
------------------	------------------------------

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
				<p>d. Resistance against replay attacks against a different verifier,</p> <p>e. Resistance against relay attacks.</p> <p>f. Resistance against pre-dating or post-dating (e.g. for a non repudiation service).</p> <p>A given method of attack does not necessarily use one of the above methods, but in some cases a combination of them.</p>	<p>might exploit responses,</p> <p>i. Resistance against replay attacks,</p> <p>j. Resistance against replay attacks against a different verifier,</p> <p>k. Resistance against relay attacks.</p> <p>l. Resistance against pre-dating or post-dating (e.g. for a non repudiation service).</p>	<p>describes these properties in abstract way, thus we accept the comment and try to relate practical security issues with abstract security property concept.</p> <p><b>On the other hand, e is related to Relay Attack which is based basically on short-distance insecure channel. One solution to this is to utilize what-is-called "Distance bounding protocol". However, it is technically hard to prove its security at this moment.</b></p>
FR 4			ge	<p>While the main topic of this document is the verification of cryptographic protocols for a security perspective, another dimension is to take into consideration: denial of service.</p> <p>Suppose that two protocols are equivalent from a security point of view to achieve a given security service, a choice could be made by considering which one is less subject to denial of service attacks.</p> <p>The computation time of the protocol and the memory resources required for one or more exchanges should be considered.</p>	<p>Add a section to deal with denial of service.</p>	<p><b>Accepted. Contribution is expected from FR. Treated same as FR3.</b></p> <p>This is a great proposal to extend the content of this standard. But, seems hard to treat DoS formally at this moment. We in general agree that it should be there in the future.</p>
FR 5			ge	<p>The document seems to say that the use a formal description provides the ultimate security. It should be pointed that the formal description can only help once an attack has been conceived. A formal language description will only demonstrate that a given attack that has been envisaged is really impossible to succeed.</p>		<p><b>Withdrawn</b></p> <p>It is true that a new attack never be found which is not formalized in formal methods. Examples are DoS and Relay attack as described before. However, all</p>

<sup>1</sup> **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 \*\*)

<sup>2</sup> **Type of comment:** **ge** = general **te** = technical **ed** = editorial

**NOTE** Columns 1, 2, 4, 5 are compulsory.

**Attachment 1 to SC 27 N8026**  
**French comments on ISO/IEC 1<sup>st</sup> CD 29128**

Date: 2009-10-08	Document: <b>SC 27 N7794</b>
------------------	------------------------------

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
				This means that if someone has not imagined a given method of attack, the use of a formal language will not add anything.		attacks which is within the scope of the model in formal methods are completely found even if those attacks are not conceived by the protocol designers. Thus, you cannot say "it will not add anything." Examples are man in the middle attack in NS protocol and attacks recently found in 9798-2 mechanism 12.
FR 6	Introduction		ge	The document is stressing the importance of the "levels of confidence" whereas the general method for reaching the first level is not sufficient. The goal of the document should be first to define the general method and only then to define the levels of confidence.		<b>Accepted. Contribution is expected.</b> It is a very good point. We will try to describe the general method. However, need your contribution or any reference.
FR 7	5		te	The text states: "Verification of a cryptographic protocol shall consist of the following artifacts: a) specification of the cryptographic protocol; b) specification of the adversarial model; c) specification of the security objectives and properties; d) self-assessment evidence that the specification of the cryptographic protocol in its adversarial model achieves and satisfies its objectives and properties ».  These four steps are insufficient. Nine steps have been identified. The use of the term "artifact" is not adequate.	Text proposal for a replacement: " Verification of a cryptographic protocol shall follow the following steps: a) describe the environment of use, b) identify the number of parties involved in the protocol and their role, c) identify the security services to be accomplished (e.g. authentication, integrity, confidentiality, confidentiality of use, etc ...) d) specify the types of attacks that might be attempted,	<b>Accepted. Contribution is expected.</b> The comment is a good guide to help developers to design a protocol. Thus, adding the related texts is demanded.  The current text already includes the essence of the indicated steps: Adversarial Model: a), d), f) Protocol Specification: b), g) Security Property: c), h) Self-assessment Evidence: j).

<sup>1</sup> **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 \*\*)

<sup>2</sup> **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 the proposal. Each step should be covered by a separate section (or sub-section) in the document.	<ul style="list-style-type: none"> <li>e) identify the time of resistance for each attack,</li> <li>f) specify the key distribution model,</li> <li>g) specify the cryptographic protocol between the parties,</li> <li>h) specify the security properties and of the speed of the algorithms.</li> <li>i) specify the key sizes and of the various variables of the protocol,</li> <li>j) self-assessment evidence by the protocol designer followed by a assessment evidence from at least one third party that the cryptographic protocol resists to the different attacks that have been identified ».</li> </ul>	<p>These two styles of writing can coexist and they are just different in view-points. Editors strongly ask FR NB to provide related texts and references.</p> <p>By the way, e), i) and speed part of h are out of the scope of the current text. It is a challenging research topic to treat "time" concept in the formal methods, which potentially deal with DoS and Relay attack (distance –bounding protocols). Other feasible option may be just to leave some description related DoS, Key Length and Relay attacks in a (semi-) formal language without verification.</p>
FR 8	5		te	<p>The text states:                      “The artifacts shall clearly state parameters or properties relevant for the verification. Examples include the bound <i>k</i> used in bounded verification or assumed algebraic properties of cryptographic operators used in the protocol ».</p> <p>This wording is not understandable in a general section and these terms are not defined in section 3. Please delete or rephrase.</p>	Delete or rephrase.	<p>Accepted. Will be rephrased.</p> <ul style="list-style-type: none"> <li>- Bounded verification</li> <li>- Algebraic properties</li> </ul>
FR 9	5		te	<p>The text states:                      “The stated requirements are only for design verification not implementation verification ».</p>	Add an informative annex to explain the differences between : m. design verification, and	Accepted.

<sup>1</sup> **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 \*\*)

<sup>2</sup> **Type of comment:** **ge** = general **te** = technical **ed** = editorial

**NOTE** Columns 1, 2, 4, 5 are compulsory.

**Attachment 1 to SC 27 N8026**  
**French comments on ISO/IEC 1<sup>st</sup> CD 29128**

Date: 2009-10-08	Document: <b>SC 27 N7794</b>
------------------	------------------------------

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
				This is true. However there should be an informative annex which shows the difference. As an example: a buffer overflow or the use of an undefined command can lead to security breaches.	n. implementation verification ».	
FR 10	5		te	The text states: « Verification tools shall fulfill the following conditions ». Tools may be useful but are insufficient. They come once steps a) to i) have been accomplished. Guidance on the ways to correctly address steps a) to i) need to be provided.		Resolved with FR 7.
FR 11	5		te	The text states: « The protocol designer shall provide evidence of the correctness of the verification tool used. » It would be much better if the evidence was provided by someone that is NOT the protocol designer. If this is done first by the protocol designer, this should be verified by an independent third party. The same comments applies to items b) and c), which currently only involve the protocol designer.	Proposed text: "Both the protocol designer and an independent third party shall provide evidence of the correctness of the verification tool used".	<b>Not accepted. But add some text to explicitly state somewhere in the standard "This standard doesn't require third party evaluation."</b>  In Clause 8, this standard requires Evaluator to evaluate the document of self-assessment evidence as a third party. Therefore, third party evaluation is already mandatory in the current text. However, this will not restrict the protocol designer to ask a third party to produce the self-assessment evidence. Thus, Change the current text to " the protocol designer , or possibly an independent third party shall provide evidence of the correctness of the verification tool used".

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
FR 12	6		te	<p>The title of this section is:            “Specifying cryptographic protocols ».</p> <p>It corresponds to the first “artifact” identified in section 5. However, there is no section to deal with the “artifact” b) (i.e. specification of the adversarial model), nor c) (i.e. specification of the security objectives and properties).</p> <p>The sections, starting with section 6, should instead cover steps a) to i) identified above:</p> <ol style="list-style-type: none"> <li>6. Description of the environment of use</li> <li>7. Identification of the number of parties involved in the protocol and their role,</li> <li>8. Identification of the security services to be accomplished</li> <li>9. Specification of the types of attacks that might be attempted,</li> <li>10. Identification the time of resistance for each attack,</li> <li>11. Specification of the key distribution model,</li> <li>12. Specification of the cryptographic protocol between the parties,</li> <li>13. Specification of the security properties and the speed of the algorithms</li> <li>14. Specification of the key sizes and of the various variables of the protocol,</li> <li>15. Specification of the security properties of the cryptographic algorithms.</li> </ol>	<p>Add the following sections:</p> <ol style="list-style-type: none"> <li>6. Description of the environment of use</li> <li>7. Identification of the number of parties involved in the protocol and their role,</li> <li>8. Identification of the security services to be accomplished</li> <li>9. Specification of the types of attacks that might be attempted,</li> <li>10. Identification the time of resistance for each attack,</li> <li>11. Specification of the key distribution model,</li> <li>12. Specification of the cryptographic protocol between the parties,</li> <li>13. Specification of the security properties and the speed of the algorithms</li> <li>14. Specification of the key sizes and of the various variables of the protocol,</li> <li>15. Specification of the security properties of the cryptographic algorithms.</li> </ol> <p>and provide text for them.</p>	<p><b>Resolved with FR 7.</b></p> <p>Clause 6 is not intended to cover only “Protocol Specification,” but to cover the basic concept of formal verification. Thus, Clause 6 is related to all of the artefacts.</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.

**Attachment 1 to SC 27 N8026**  
**French comments on ISO/IEC 1<sup>st</sup> CD 29128**

Date: 2009-10-08

Document: **SC 27 N7794**

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
FR 13	6.1		te	<p>The text states:</p> <p>« The goal of this part is to provide with guidelines and minimal requirements for specifying cryptographic protocols ».</p> <p>The title of this section is: "Specifying cryptographic protocols" .</p> <p>The minimum requirements will be coming from the new proposed sections:</p> <ul style="list-style-type: none"> <li>8. Identification of the security services to be accomplished,</li> <li>9. Specification of the types of attacks that might be attempted,</li> <li>10. Identification the time of resistance for each attack.</li> </ul> <p>The guidelines will be coming from questions related to :</p> <ul style="list-style-type: none"> <li>o. Resistance against eavesdropping,</li> <li>p. Resistance against unauthenticated queries that might exploit responses,</li> <li>q. Resistance against replay attacks,</li> <li>r. Resistance against replay attacks against a different verifier,</li> <li>s. Resistance against relay attacks,</li> <li>t. Resistance against pre-dating or post-dating.</li> </ul>	Use the text of this section for the new proposed section 12.	<p><b>Resolved with FR7</b></p> <p>The "minimum requirements" is intended to describe "minimum requirements to specify formally verifiable specification of cryptographic protocols." Thus, it is relevant to all the artefacts.</p> <p>It is not intended to describe the minimum requirement for a protocol designer or a protocol user. The proposed items are also important and should be included in the text.</p>
FR 14	6.3.2.		te	The terms "arity" and "varyadic" are not defined in section	Please provide a definition for the terms	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.

**Attachment 1 to SC 27 N8026**  
**French comments on ISO/IEC 1<sup>st</sup> CD 29128**

Date: 2009-10-08	Document: <b>SC 27 N7794</b>
------------------	------------------------------

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
				3. Please provide a definition.	“arity” and “varyadic”.	
FR 15	6.3.2.		te	The term “formal description” is not defined in section 3. Please provide a definition.	Please provide a definition for the term “formal description”.	Accepted
FR 16	6.4.		te	Some text from this section may be re-used in the new proposed section 9: “Specification of the types of attacks that might be attempted”. This section should include: 9.1. Resistance against eavesdropping, 9.2. Resistance against unauthenticated queries that might exploit responses, 9.3. Resistance against replay attacks, 9.4. Resistance against replay attacks against a different verifier, 9.5. Resistance against relay attacks. 9.6. Resistance against pre-dating or post-dating (e.g. for a non repudiation service).	Add the following sub-sections in section 9: 9: “Specification of the types of attacks that might be attempted”. 9.1. Resistance against eavesdropping, 9.2. Resistance against unauthenticated queries that might exploit responses, 9.3. Resistance against replay attacks, 9.4. Resistance against replay attacks against a different verifier, 9.5. Resistance against relay attacks, 9.6. Resistance against pre-dating or post-dating (e.g. for a non repudiation service).	<b>Resolved with FR7</b> Try to describe and define those 6 attacks as important considerations in designing a cryptographic protocol in <b>informative annex</b> .
FR 17	6.5.1		te	The text states: « In view of the huge variety of security properties (at all levels of abstractions), it seems not possible at the time being to give a		<b>Resolved with FR7.</b>

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.

**Attachment 1 to SC 27 N8026**  
**French comments on ISO/IEC 1<sup>st</sup> CD 29128**

Date: 2009-10-08	Document: <b>SC 27 N7794</b>
------------------	------------------------------

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
				<p>general way of describing security properties ».</p> <p>It is indeed possible to give a general way of describing security properties. The security properties come from the new sections 8 to 14:</p> <ul style="list-style-type: none"> <li>8. Identification of the security services to be accomplished</li> <li>9. Specification of the types of attacks that might be attempted,</li> <li>10. Identification the time of resistance for each attack,</li> <li>11. Specification of the key distribution model,</li> <li>12. Specification of the cryptographic protocol between the parties,</li> <li>13. Specification of the security properties and the speed of the algorithms,</li> <li>14. Specification of the key sizes and of the various variables of the protocol.</li> </ul>		
FR 18	6.5.1		te	<p>The text states:</p> <p>“Furthermore, there is currently no way to specify (even simple) security properties, independently of the protocol specification language ».</p> <p>This statement is incorrect. Firstly, there is no need to have a protocol specification language. Secondly, the security properties can be expressed as:</p> <ul style="list-style-type: none"> <li>u. Resistance against eavesdropping,</li> <li>v. Resistance against unauthenticated queries that might exploit responses,</li> </ul>	Delete the sentence.	Resolved with FR7.

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.

**Attachment 1 to SC 27 N8026**  
**French comments on ISO/IEC 1<sup>st</sup> CD 29128**

Date: 2009-10-08	Document: <b>SC 27 N7794</b>
------------------	------------------------------

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
				<ul style="list-style-type: none"> <li>w. Resistance against replay attacks,</li> <li>x. Resistance against replay attacks against a different verifier,</li> <li>y. Resistance against relay attacks.</li> <li>z. Resistance against pre-dating or post-dating (e.g. for a non repudiation service).</li> </ul>		
FR 19	6.5.1		te	<p>The two classes of properties that are given, i.e. “trace properties” and “equivalence properties” are insufficient. Trace properties only addresses eavesdropping.</p> <p>“Equivalence properties” only address properties exhibited by zero-knowledge techniques which are not required in general, but only provide additional benefits.</p>		<p>Accepted. Explain the two properties in more detail.</p> <p>Trace property is typically used to express authenticity property as well as secrecy property, such as eavesdropping. Equivalence property is typically used to express widely used anonymity property. Therefore, these two are essential.</p>
FR 20	7		te	<p>It is very questionable why there are only 3 levels. The Common Criteria recognizes seven levels;</p> <p>EAL1: functionally tested  EAL2: structurally tested  EAL3: methodically tested and checked  EAL4: methodically designed, tested and reviewed  EAL5: semi-formally designed and tested  EAL6: semi-formally verified design and tested  EAL7: formally verified design and tested</p> <p>This document should recognize these seven levels so</p>	<p>This document should recognize seven levels so that cryptographic protocols can be verified as part of a CC evaluation:</p> <p>EAL1: functionally tested  EAL2: structurally tested  EAL3: methodically tested and checked  EAL4: methodically designed, tested and reviewed  EAL5: semi-formally designed and tested</p>	<p>Accepted. Add a map showing the correspondence between EAL and PAL.</p> <p>Components of Common Criteria usually have smaller number levels than seven. This standard followed the style of other CC components.</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.

**Attachment 1 to SC 27 N8026**  
**French comments on ISO/IEC 1<sup>st</sup> CD 29128**

Date: 2009-10-08	Document: <b>SC 27 N7794</b>
------------------	------------------------------

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
				that cryptographic protocols can be verified as part of a CC evaluation.	EAL6: semi-formally verified design and tested EAL7: formally verified design and tested	

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.

**Attachment 2 to SC 27 N8026**  
**[JP<sup>1</sup>] comments on ISO/IEC 1<sup>st</sup> CD 29128**

Date: 2009-09 -21	Document: <b>SC 27 N7794</b>
-------------------	------------------------------

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
JP 1	6.3.2		ed	"In this <u>section</u> ..." should be "In this <u>clause</u> ...".	Replace "section" with "clause".	Accepted.
JP 2	7.5		ed	"Difference between PAL1 and PAL2 is <u>that</u> all artifacts ..." should be "Difference between PAL1 and PAL2 is <u>whether</u> all artifacts ..."	Replace "that" with "whether".	Accepted.
JP 3	7.5		ed	"... such as Intranet" should be "... such as <u>an</u> Intranet".	Insert "an" between "as," and "Intranet".	Accepted.
JP 4	7.5		ed	"Difference between PAL2 and PAL3 is <u>that</u> evidence ..." should be "Difference between PAL1 and PAL2 is <u>whether</u> evidence ..."	Replace "that" with "whether".	Accepted.
JP 5	7.5		ed	"While in PAL2, verification is bounded" should be "While in PAL2, <u>verification</u> is bounded" (White space is missing.)	Insert white space between "PAL2," and "verification".	Accepted.
JP 6	Annex B		ed	Hanging paragraph should be avoided.	Resolve hanging paragraph. E.g. insert appropriate clause title.	Accepted.
JP 7						

<sup>1</sup> **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 \*\*)

<sup>2</sup> **Type of comment:** **ge** = general **te** = technical **ed** = editorial

**NOTE** Columns 1, 2, 4, 5 are compulsory.

**Attachment 3 to SC 27 N8026**  
**[MB<sup>1</sup>] comments on ISO/IEC 1<sup>st</sup> CD 29128**

Date: 2009-MM-DD	Document: <b>SC 27 N7794</b>
------------------	------------------------------

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
SG 1			ed	Many formulae are visually fuzzy. The reason is that the formulae were past in image format instead of text. Please correct it. Either MS Equation can produce fairly nice formulae.		Accepted.
SG 2						
SG 3						

<sup>1</sup> **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 \*\*)

<sup>2</sup> **Type of comment:** **ge** = general **te** = technical **ed** = editorial

**NOTE** Columns 1, 2, 4, 5 are compulsory.

**Attachment 2 to SC 27 N6988**  
**[UK] comments on ISO/IEC 2<sup>nd</sup> WD 29128**

Date: 2008-09-26	Document: <b>SC27 N6649</b>
------------------	-----------------------------

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
UK 1	general		Ge	Use of the first person is too informal for a standard. For example, in 6.2 " we can interpret..."	Change from first person to more impersonal language, throughout. For example, "We will call this abstraction the <i>symbolic</i> level" can be written as "This abstraction is referred to as the <i>symbolic</i> level."	Accepted.
UK 2	title and introduction		Ed	Introduction seems to vary from the title: the title is 'verification of cryptographic protocols' whereas the introduction refers to 'security of the specification of cryptographic protocols'. The title seems more correct.	Change the introduction to agree with the title of the standard.	Accepted. Change the last sentence in Introduction to "The goal of this standard is to establish means <b>for verification of cryptographic protocols</b> to provide defined levels of confidence concerning the security of the specification of cryptographic protocols."
UK 3	3 and 4		Te	There are many symbols and terms for cryptographic protocols used later in this document which are not defined in this clause.	Please provide formal definitions for the following symbols used later: aa. Role names: <i>A</i> , <i>B</i> , Message <i>m</i> , random nonce <i>r</i> , key <i>k</i> , and communication channel <i>c</i> . bb. Encryption and decryption functions: <i>enc</i> and <i>dec</i> . cc. Pairing operator: $\langle \dots, \dots \rangle$ dd. Processes: <i>Send</i> and <i>Receive</i> in Clause 6.3.5. ee. <i>generate</i> and <i>replicate</i> used in Clause 6.4.3.	Accepted.

<sup>1</sup> **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 \*\*)

<sup>2</sup> **Type of comment:** **ge** = general **te** = technical **ed** = editorial

**NOTE** Columns 1, 2, 4, 5 are compulsory.

**Attachment 2 to SC 27 N6988**  
**[UK] comments on ISO/IEC 2<sup>nd</sup> WD 29128**

Date: 2008-09-26	Document: <b>SC27 N6649</b>
------------------	-----------------------------

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
UK 4	3.4		Ed	The word 'secrecy' seems too general.	Change 'secrecy' to 'confidentiality'	Not accepted. The word 'secrecy' here is used as a technical term which is usually used to specify a security property of cryptographic protocols.  Define "Secrecy" in Clause 3.
UK 5	3.5		Ed	The definition of 'self-assessment evidence' does not actually require self assessment.	Change to 'evidence that the developer uses to verify whether a specified protocol fulfils its designated security properties'	Accepted
UK 6	3.7	Note	Ed	'process' and 'communication' should be in plural form.	Fix.	Accepted
UK 7	3.8		ed	The definition is unclear, but in any case the term "term algebra" is not used in the standard, and the word 'signature' is not used elsewhere.	Delete 3.8	Accepted
UK 8	5	Notes	Ed	Many notes within this clause are not numbered. Multiple notes under the same heading should be numbered, even if referring to different paragraphs.	Please number all of the notes in this clause.	Accepted
UK 9	5	Para 1	Ed	Verification does not consist of artifacts, but of checking or verifying them. Also, a definition is not a suitable place to specify a requirement.	Change "Verification of a cryptographic protocol shall consist of the following artifacts:" to "Verification of a cryptographic protocol involves checking the following artifacts:"	Accepted.
UK 10	6.3.2	1 <sup>st</sup> bullet	Ed	'a set of' should not be in italics to be consistent with other bullets	Fix.	Accepted
UK 11	6.3.2	1 <sup>st</sup> and 2 <sup>nd</sup> bullets	Ed	There is a problem with the style and font of symbols $F$ (set of functions) and $N$ (set of names). These are not consistent with other parts of the document, and appear blurred in the PDF document.	Please use notation or symbols provided by the ISO template.	Accepted.

<sup>1</sup> **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 \*\*)

<sup>2</sup> **Type of comment:** **ge** = general **te** = technical **ed** = editorial

**NOTE** Columns 1, 2, 4, 5 are compulsory.

**Attachment 2 to SC 27 N6988**  
**[UK] comments on ISO/IEC 2<sup>nd</sup> WD 29128**

Date: 2008-09-26	Document: <b>SC27 N6649</b>
------------------	-----------------------------

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
UK 12	6.3.2	3 <sup>rd</sup> bullet	Ed	Missing a full stop at the end of the sentence.	Fix.	Accepted
UK 13	6.3.2	Para starting with 'The set of valid....', and in EXAMPLE	Ed	There is a problem with the style, font and position of $T(F,N)$ and $T(F,N,X)$ in this paragraph. The same problem occurs with the function <i>enc</i>	Please use notation or symbols provided by the ISO template.	Accepted
UK 14	6.3.2	EXAMPLE	Te	The example is not clear. Why is <i>enc</i> (k,k,r) invalid? And, as written, only invalid examples seem to be shown.	Probably the first examples are intended to be valid examples. If not, please clarify the example, explain why <i>enc</i> (k,k,r) is invalid, and include some valid examples.	Accepted. Yes. The first examples are the valid examples. Thank you.
UK 15	6.3.2	EXAMPLE, last sentence.	Ed	Missing symbol 'll' after 'or the concatenation'	Fix.	Accepted.
UK 16	6.3.3	Para 3, line 1	Ed	Replace the preposition 'in' in 'This part consists in listing' with 'of'.	Fix.	Accepted.
UK 17	6.3.3	Para 3, last line	Ed	The use of '...' at the end of last line is too informal for an ISO standard.	Remove '...', and put 'and' before 'same_key'.	Accepted.
UK 18	6.3.4	Para 2		Wording seems odd. Should "we wish to state" say "we may wish to state"? Also, the example given is unclear.	Revise to make the meaning clearer.	Accepted.
UK 19	6.3.5	Bullets 1-5	Ed	Semicolons are missing at the end of these 5 bullets.	Add semicolons at the end of these bullets.	Accepted
UK 20	6.3.5	Bullet 6	Ed	There are problems with the font and style of the two mathematical symbols which use arrows, i.e. Send and Receive.	Fix these to make them have the same font and style as other mathematical symbols.	Accepted

<sup>1</sup> **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 \*\*)

<sup>2</sup> **Type of comment:** **ge** = general **te** = technical **ed** = editorial

**NOTE** Columns 1, 2, 4, 5 are compulsory.

**Attachment 2 to SC 27 N6988**  
**[UK] comments on ISO/IEC 2<sup>nd</sup> WD 29128**

Date: 2008-09-26	Document: <b>SC27 N6649</b>
------------------	-----------------------------

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
UK 21	6.3.5	EXAMPLE, bullets 1-3	Ed	Semicolons are missing at the end of these 3 bullets.	Add semicolons at the end of these bullets.	Accepted
UK 22	6.3.5	Last para, line 3	Ed	'),' is redundant	Remove this. Also insert a space before 'that'.	Accepted
UK 23	6.3.5	last para, Lines 3 and 4	Ed	'that will allow to distinguish different role instances' does not parse	Change this text to 'that will allow different role instances to be distinguished'.	Accepted
UK 24	6.4.1	Para 2, line 3	Ed	'But it could be more refined' does not parse.	Change to 'But it could be refined further'.	Accepted
UK 25	6.4.2	Para 2, line 1	Ed	The phrase 'so-called' is too informal for an ISO document.	Remove phrase.	Accepted
UK 26	6.4.2	Para 3, line 2/3	Ed	The index of 'section' is missing.	Fix.	Accepted
UK 27	6.4.3	Bullet 1	Ed	'The initial attacker's knowledge' does not parse correctly.	Change to 'The attacker's initial knowledge'.	Accepted
UK 28	6.4.3	Bullet 3, para 1	Ed	A full stop is missing at the end of line 1 of this bullet.	Fix.	Accepted
UK 29	6.4.3	Bullet 4	Ed	'Last but not least' is informal language.	Remove phrase.	Accepted
UK 30	6.4.3.	Bullet 4, line 3.	Ed	There are problems with position and style of calls <i>generate</i> , <i>replicate</i> and their arguments $P(k)$	Fix. Add a closing bracket after '(generate $k$ $P(k)$ '	Accepted
UK 31	6.5.2	Bullets 1-3	Ed	Semicolons are missing at the end of bullets 1-2, and a full stop is missing at the end of bullet 3.	Fix.	Accepted

<sup>1</sup> **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 \*\*)

<sup>2</sup> **Type of comment:** **ge** = general **te** = technical **ed** = editorial

**NOTE** Columns 1, 2, 4, 5 are compulsory.

**Attachment 2 to SC 27 N6988**  
**[UK] comments on ISO/IEC 2<sup>nd</sup> WD 29128**

Date: 2008-09-26	Document: <b>SC27 N6649</b>
------------------	-----------------------------

1	2	(3)	4	5	(6)	(7)
<b>NB<sup>1</sup></b>	<b>Clause No./ Subclause No./ Annex</b> (e.g. 3.1)	<b>Paragraph/ Figure/Table/Note</b> (e.g. Table 1)	<b>Type of comment<sup>2</sup></b>	<b>Comment (justification for change) by the NB</b>	<b>Proposed change by the NB</b>	<b>Resolution on each comment</b>
UK 32	6.5.2	Para starting with 'The temporal property....', line 3	Ed	' <i>honest</i> ' should not be italic.	Fix.	Accepted
UK 33	7.1	Table 1, slot in row 3 and col 2	Ed	A full stop is missing at the end of the sentence.	Fix.	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 comment <sup>2</sup>	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
UK 34	7.3		Te	As (a) and (d) are currently worded, only tool-based evidence can be used to achieve PAL2. This implies that mathematical proofs are of no value unless they are machine-generated. This is unsound; underlying all mechanical tools eventually there is a paper-and-pen human proof of the tool's correctness. In addition, although manually generated proofs may be more difficult to independently verify (and more subject to verification error), they should be treated as a valid alternative.	Please reconsider classification scheme and either change or justify.	Accepted.  As described in the last Notes in Clause 5 in current draft, "At least in theory, protocol verification may be carried out by hand proofs, using paper and pencil. However, given the substantial amount of detail typically involved in security protocol verification, especially for the high Protocol Assurance Levels confidence in the results is substantially increased by using mechanized tools such as model checkers and theorem provers. Thus, proofs only with paper-and-pencil are treated as lowest assurance level (i.e. PAL1) in this standard."  Another possible way is to put paper-and-pencil proof to a level between PAL1 and PAL2. Protocols whose all necessary statements are given mathematically, and whose security properties are proven in mathematically rigorous way, then the protocol may be better to be classified higher than PAL1.  <i>Paper and pencil proof will have a new level such as PAL1.5 or PAL B or something. Partial ordering may be better.</i>

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.

**Attachment 2 to SC 27 N6988**  
**[UK] comments on ISO/IEC 2<sup>nd</sup> WD 29128**

Date: 2008-09-26	Document: <b>SC27 N6649</b>
------------------	-----------------------------

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
UK 35	7.2		Te	In Section 7.2, it appears that the protocol assurance levels are largely dependent upon whether a protocol is specified in a semiformal language or a formal language. But no formal definition of a formal language or a semiformal language is provided.	Please define all terms.	Accepted.
UK 36	7.5	Last para, line 5.	Ed	'adversary' should be plural.	Replace this with 'adversaries'.	Accepted.
UK 37	Bibliography	All references	Ed	The format of the authors' names of all references should be more consistent. For example:  ff. Reference 1: authors names are Yannick Chevalier and other, but in references 3: reference names are abbreviated D. Dolev and A. Yao. Similarly in references 4, 9, 10, 11, and 12.  gg. Where there are more than 3 authors, sometimes all are listed (e.g. Reference 8) sometimes "et al" is used (e.g. Reference 11).	Fix.	Accepted. (cf. ISO 690)
UK 38	Bibliography	References 7-8	Ed	Please remove double quotes around titles of these references to make them consistent with others.	Please remove double quotes.	Accepted.
UK 39	Bibliography	References 5, 7, 8 and 10	Ed	Missing page numbers.	Please add page numbers.	Accepted.
UK 40	Bibliography	Reference 12	Ed	'Prod.' should be replaced by 'Proceedings' to be consistent with reference 8.	Fix.	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.