ISO/PC 246 N **023**

2009-07-30

ISO / PC Secretariat
Your correspondent : Laurence DOUVILLE
Direct line : + 33 1 41 62 86 06
Fax : + 33 1 49 17 90 00
E-mail : laurence.douville@afnor.org

Support: Maxine BENACOM
Direct line : + 33 1 41 62 83 06
Fax : + 33 1 49 17 90 00
E-mail : maxine.benacom@afnor.org

The French Committee Member :

Association
Française de
Normalisation
11 rue Francis de Pressensé
93571 Saint-Denis La Plaine Cedex
France
Tél. : +33 (0)1 41 62 80 00
Fax : +33 (0)1 49 17 90 00
http://www.afnor.fr

Association reconnue
d'utilité publique
Comité membre français
du CEN et de l'ISO
Siret 775 724 818 00015
Code NAF 751 E

ISO / PC 246
Anti-counterfeiting tools

Secretariat : AFNOR

Title : **Result of the call for comments on ISO WD 12931.1 "Performance criteria for authentication tools for anti-counterfeiting in the field of material goods"**

Source : **ISO PC Secretariat**

Status : **For information and consideration at the next ISO/PC 246 meeting.**

Template for comments and secretariat observations

Date: 2009-07-30	Document: **PC246n017**

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of comment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted
AT				no expertise available		
DE1	General		te	(1) Although the document is supposed to be on a horizontal level and to give generic requirements which are technologically independent, concrete requirements and/or examples for anti-counterfeiting methods and tools are missing. Additional information giving examples for anti-counterfeiting tools should be given.	Add examples and/or more concrete requirements.	
DE2	General		te	(2) National specific privacy laws and regulations have to be obeyed by applied anti-counterfeiting mechanism. (e. g. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.; OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (Sept. 1980))	Include statement	
DE3	General		te	(3) There is text in the introduction describing processes in the development and use of anti-counterfeiting tools, but terms as "assessment of risk level" are mentioned by the way in the text (section 6). I would expect a structured process scheme, stating that e.g. a risk assessment shall take place (and before other processes).	The processes of designing, developing and using anti-counterfeiting tools should be mentioned and made mandatory.	

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.

Template for comments and secretariat observations

Date: 2009-07-30	Document: **PC246n017**

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of comment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted
DE4	General		ge	(4) Authentification tools should provide a method to check governmental or non-governmental acknowledged labels concerning product safety, health, consumer protection or environmental protection where possible.		
DE5	General		ed	(5) Terms "rights holder" and "right holder" are used synonymously by mistake.	Use "rights holder" instead of "right holder".	
NL			ge	For the Netherlands there has not been established a national mirror committee for Anti-counterfeiting tools. NEN must therefore respond ABSTAIN to the ISO document WD 12931.1.		
KR			ge	KATS would like to support the concept overall. It is agreed that it would be useful to develop a checklist regarding anti-counterfeiting tools. Meanwhile, "downloadable" products at this time should not be included in this PC level. Because it would even further delay the standardization process of this particularly selected IPR protection effort area due to digital media's very complicated and sensitive nature and issues. Also, ISO/WD 12931 needs to further clarify the performance criteria for authentication tools as it still looks somewhat vague in terms of authentication and assessment process. It seems to cover many elements for assessment of anti-counterfeiting tools' performance and effectiveness but it is not clear how those tool elements work in each stage of the authentication procedure.		

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.

Template for comments and secretariat observations

Date: 2009-07-30	Document: **PC246n017**

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of comment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted
DE6	Title		ge	(6) Any authentication feature or solution consists of several components, of which an authentication tool, in the narrow sense of the word, is only one. Performance, however, can only be assessed for a feature or solution as a whole. We thus propose to change the word "Tools" in the title of the WD to "Measures" to clarify the complete extent of the intended coverage.	Change the word "Tools" in the title to "Measures".	
US1	Foreword	Paragraph 6 Last sentence	ed	The term ”bites into” is a colloquialism and is subject to misinterpretation	Use the word “reduces”	
FR1	Foreword	7th paragraph	Ed	Consistency	Replace “requirements” With “*Criteria”*	
US2	Foreword	Paragraph 8, First sentence	ed	Word missing, “the” should be inserted “authentication tools into the products life cycle”	Insert the word “the “ as indicated.	
UK1	Foreword	8	Ge	It is not appropriate to refer to product lifecycle etc in the context of authentication tools.	Replace with: The present document aims to integrate the performance requirements for authentication tools into products’ supply and distribution chains, so that authentication is positioned as a feature of these chains.	

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.

Template for comments and secretariat observations

Date: 2009-07-30	Document: **PC246n017**

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted
FR2	Foreword	Last sentence	Te	Consistency with the content of the scope	Replace "legitimate" with "*genuine*"	
FR3	Introduction		Te	The introduction will have to be reviewed to make it consistent with the document after discussion and consensus regarding the content of the standard.	See Annex A	
UK2	Introduction	All	Ed	With the change of title to "Authentication Tools" the phrase "anti-counterfeiting" is mostly inappropriate as used throughout this section.	Replace "anti-counterfeiting" with "authentication" as necessary and appropriate.	
DE7	Intro	Para 1	ed	(7) Grammatical mistake	Change to "the range of counterfeited products has developed…"	
US3	Introduction	First Paragraph First sentence	ed	Poor wording "…..has been developed strongly since over a decade, and is new no longer limited to luxury goods."	….has been increasing rapidly for over a decade and is no longer limited to luxury goods."	
DE8	Intro	Para 1, 4th sentence	ed	(8) Clearer language needed	Change to "These counterfeit goods… regulatory requirements, and therefore generate risks for…"	
US4	Introduction	First paragraph Last sentence	gen	Additional language introduces the legal and liability issues of counterfeiting.	Additional language "……loss of earnings, job losses, brand value damage, *and increase the potential for false product claims and litigation* for the companies and distribution *supply* chain."	
US5	Introduction	Second paragraph Last Sentence	ed	Change of term for consistency and clarity, "distribution circuits" are typically related to electrical distribution.	"…… to empower and secure the distribution ~~circuits~~ *supply chain*, and help…….	
UK3	Introduction	3	Ed	See above	Delete	

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.

Template for comments and secretariat observations

Date: 2009-07-30	Document: **PC246n017**

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of comment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted
UK4	Introduction	4 and after	Ge	See attached discussion paper. Counterfeiting is more than IPR infringement.	Delete or replace as per attached paper.	
US6	Introduction, Intellectual property infringement	First paragraph, first sentence	ed	Redundant language.	"…… counterfeited in various ~~different~~ ways."	
US7	Introduction, Intellectual property infringement	Third point, "patents"	ed	The terms and phrases are not clearly understood. "…..authorized licensee for a new invention that is *inventive and industrially applicable, in many cases including a supplementary protection certificate."*	Replace with new language.	
US8	Introduction, Recognition of authenticity	First sentence in italics	ed	Typo or misspelling	Change "Nota" to "Note"	
US9	Introduction, Recognition of authenticity	First paragraph	gen	Change terms to more accurately reflect the involved entities.	"…..legal provisions designed to enable ~~professionals~~, *corporations or business entities* to release safe products……	
US10	Introduction, Recognition of authenticity	Last paragraph, Second sentence	ed	The term "hone in" is a colloquialism and is subject to misinterpretation	Replace with the word "focus".	

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.

Template for comments and secretariat observations

Date: 2009-07-30	Document: **PC246n017**

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of comment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted
FR4	Scope	4th paragraph	Ed	Clarification: the distinctive identity is the most encompassing concept from which the other items follow. Exhaustiveness: this standard has to cover issues not yet identified.	Replace "This document deals with material goods: • covered by intellectual property rights, • and/or covered by relevant national or regional regulation, • and/or with safety and public health implications, • and/or otherwise with a distinctive identity." With "*This document deals with material goods with a distinctive alleged identity and, among others:* • *covered by intellectual property rights,* • *and/or covered by relevant national or regional regulation,* • *and/or with safety and public health implications."*	
US11	Scope	Fourth paragraph	ed	The term "deals with" should be more specific. Replace with proposed language.	"This document is focused upon the authentication of material goods."	

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.

Template for comments and secretariat observations

Date: 2009-07-30	Document: **PC246n017**

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of comment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted
FR5	Scope		Te	Completeness	Add the following paragraph: *"Authentication tools covered by this standard may be used to provide pieces of evidence, for example in case of legal procedure."*	
FR6	2		Te	Useful reference	Add *"ISO/IEC 27001 Information technology -- Security techniques -- Information security management systems – Requirements"*	
UK5	3	3.1 - 3.21	Ed	It is logically wrong to establish which words or phrases in the standard require definition until the standard has been drafted. Only then can it be searched for words which require a definition.	Postpone further consideration of the Definitions in this section until the standard is drafted.	
DE9	3.1		te	(9) Improper definition.	Change accordingly: "Successful or unsuccessful attempt to imitate, produce , possible reproduce the authentic product."	
FR7	3	3.1	Ed	The definition, as it is, is too much restrictive	Delete "to be able to imitate, produce, possibly reproduce, the authentication elements"	
US12	Definitions 3.1	3.1 attack	ed	The term "hack" is inappropriate for this definition.	"….attempt to *compromise or circumvent* an anti-counterfeiting solution,…."	

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.

Template for comments and secretariat observations

Date: 2009-07-30	Document: **PC246n017**

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of comment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted
FR8	3	3.4	Te	Preciseness of the definition	Add "by copying, producing or using without authorization from the right owner"	
US13	Definitions 3.4	3.4 counterfeit	gen	The definition is very limited in scope and needs to be expanded	Additional language, "a material good from an unknown origin, that represents, or attempts to represent, the authentic product."	
US14	Definitions 3.5	3.5 Inspector	gen	Additional language to expand the definition.	Additional language, …'who uses the anti-counterfeiting device, *exemplars, individual or cumulative expertise, or other means* with the aim of ….."	
FR9	3	3.8	Ed	Clarification: the authentication is larger than a piece of information.	Change the current definition with: *"a property, object or mark associated to the product, the use, knowledge and/ or interpretation of which contribute to build evidence."*	
US15	Definitions 3.8	3.8 Authentication	ed	Additional language for clarification	Additional language, "…..help build evidence *to authenticate the material good."*	
DE10	3.9/3.13		te	(10) The document gives two different definitions for the same term "proof". Only one clear definition should be given.	Clarify/change accordingly	
FR10	3	3.9	Ed	Clarification: proof is defined in paragraph 3.13	Delete "proof" from the title	
FR11	3	3.9	Ed	Consistency	Replace "expert" with "*inspector*"	

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.

Template for comments and secretariat observations

Date: 2009-07-30	Document: **PC246n017**

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of comment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted
FR12	3	3.11	Ed	Clarification	Replace the current definition with: *"to be completed"*	
FR13	3	3.12	Ed	According the way this word is used in the standard, the definition has to be modified.	Cancel "used to build and run the anti-counterfeiting solution," Replace "product authenticity" with "*element of authentication*"	
FR14	3	3.13	Te	This definition is close to the one available in the dictionary. It has no added value in this standard	Cancel this definition	
US16	Definitions 3.14 3.16	3.14, 3.16	ge, te	Because of the legal issues around intellectual property rights(varying national laws and patent rights) I would question that all authenticate material goods carry intellectual property rights.	The definitions of "authentic product" and "counterfeit product" need to be discussed and evaluated.	
DE11	3.15		ed	(11) The wording should be active to clarify the difference between a counterfeiting product to a counterfeited product.	Change to: "counterfeiting product"	
DE12	3.15 3.16		ed	(12) Definition of "authentic product" is already given in 3.14, reference to the protection of IPRs is redundant.	Delete "covered by the protection of one or more intellectual property rights"	
DE13	3.16		ed	(13) The wording should be passive to clarify the difference between a counterfeiting product to a counterfeited product.	Change to: "counterfeited product"	

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.

Template for comments and secretariat observations

Date: 2009-07-30	Document: **PC246n017**

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of comment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted
CH	3.16			La définition du point 3.16 "counterfeit product" peut prêter à confusion dans le sens où elle définit un produit contrefait en disant qu'il s'agit d'un produit authentique couvert par la protection d'un ou plusieurs droits de propriété intellectuelle et faisant l'objet de contrefaçon ou de violation d'un brevet. Un produit contrefait ne peut jamais être un produit authentique. De plus, la notion de marchandise contrefaite/faux produit est déjà définie au point 3.15 (redondance). Definition 3.16 "counterfeit product" may be confusing when defining it by saying that it is an "authentic product covered by one or more intellectual property rights, and subjected to counterfeiting / patent infringement." A counterfeit product can never be authentic. Moreover, the notion of "counterfeit goods/fake goods" is already defined in 3.15 (redundancy).	Supprimer 3.16 Delete 3.16	
US17	Definitions 3.16	3.16	ge.	Patent infringement does not automatically result in a counterfeit product.	The definitions of “authentic product” and “counterfeit product” need to be discussed and evaluated.	
DE14	3.19		te	(14) Add paragraph after "risk". Definition of "secret" needs to be changed.	Clarify and change accordingly Change definition of 'secret' accordingly: " Data that has to be protected against disclosure to unauthorized entities."	
US18	Definitions 3.19	3.19 First definition	ge	Definition is unclear as to meaning, replace.	“A situation in which risk are mitigated in a manner that provides a level of assurance that is compatible with the threats of attack.”	

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.

Template for comments and secretariat observations

Date: 2009-07-30	Document: **PC246n017**

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of comment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted
US19	Definitions 3.19	3.19 Second definition	ge	Definition is more appropriate to the term "secret" than to the term "security"	Remove the second definition and add the definition "secret' using the second definition.	
FR15	3	3.21	Te	This definition is close to the one available in the dictionary. It has no added value in this standard	Cancel this definition	
FR16	3		Te	Definition missing	Add the following definition: " Material good : physical good, produce of nature or of a manufacturing process"	
FR17	3		Te	Definition missing	Add the following definition: " Distinctive identity : characteristics, physical or external presentation, which make a material good uniquely recognizable"	
FR18	3		Te	Definition missing	Add the following definition: " Verification protocol: sequence of steps involved in the verification of authenticity of a material good"	
UK6	4	Introduction	Ed	This requires a fundamental re-write which is beyond the scope of this comment at present. As drafted, it refers to network digital solutions only, it does not refer to what are now being called in the draft "simple" tools, but only to those being called "complex" tools.	Rethink and re-draft	

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.

Template for comments and secretariat observations

Date: 2009-07-30	Document: **PC246n017**

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of comment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted
DE15	4	1st /2nd/3rd para	te	(15) No normative text is given, therefore the text should be moved to the introduction; in fact parts of the text are already mentioned in the introduction	Move text to introduction or re- formulate so that text becomes requirement or recommendation.	
DE16	4	5th para	te	(16) This statement is part of the scope statement.	Move text to scope.	

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.

Template for comments and secretariat observations

Date: 2009-07-30	Document: **PC246n017**

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of comment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted
UK7	4.1	All		As above: this describes requirements for complex, or networked tools or systems, not simple tools.	Re-draft as: **Performance criteria for authentication tools** The aim of the performance assessment criteria for authentication tools is: • To establish objective descriptions of the function of different types of authentication tool; • To establish criteria for the assessment of the efficiency of each authentication tool within its understood functions; • To show how different types of tool provide complementary functionality; • To provide criteria for which type of tool can be used to authenticate in different examination situations; • Thus to assist users and potential users of authentication tools to understand their functionality and selection criteria against their own risk analysis, which will facilitate: • The ability to run product verifications anywhere, under all foreseeable circumstances and conditions of use; • to define specific requirements for	

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.

Template for comments and secretariat observations

Date: 2009-07-30	Document: **PC246n017**

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of comment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted
DE17	4.1		te	(17) For consumers as well as for other stakeholders it is very important that the use of anti-counterfeiting tools does not interfere with other product requirements. Especially data protection requirements shall not be interfered with; It is equally important for consumers that accessibility and usability requirements for products are met and that accessibility and usability does not decrease because of the use of anti-counterfeiting tools	Give statement on the requirement that the anti-counterfeiting tools shall not interfere with product features and requirements for products.	
FR19	4	3rd paragraph, 3rd line	Ed	Consistency	Replace "the product manufactured by the rights holder or licensee" with "*material good"*	
FR20	4.1	Title	Ed	Consistency with the title of the standard	Cancel "purpose-built"	
FR21	4.1	Title	Ed	Consistency with the title of the standard	Replace "anti-counterfeiting" with "*authentication*"	
FR22	4.1	1st bullet	Ed	Consistency	Replace "product" with "*good*"	
FR23	4.1	3rd bullet	Ed	Clarification	Replace "to enable upgrades in technological tools to be factored in" with "*to enable durability and evolutivity of the authentication tool*"	

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.

Template for comments and secretariat observations

Date: 2009-07-30	Document: **PC246n017**

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of comment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted
FR24	4.1	4th bullet	Ed	Clarification	Replace " to guarantee data security, including in terms of economic intelligence" with: "*to enable to evaluate the security of the authentication data, including in terms of economic intelligence*"	
FR25	4.1	5th bullet	Ed	Clarification	Replace: "to make it possible to define a level of reliability and robustness that is satisfactory for all the stakeholders" with: " *to enable the evaluation of a level of reliability and robustness that is satisfactory for all the stakeholders"*	
FR26	4.1	5th bullet	Te	Redondancy with 9th bullet	Cancel "and robustness"	
FR27	4.1	6th bullet	Ed	Clarification	Replace "particular" with "*unexpected*"	
FR28	4.1	7th bullet	Te	The standard doesn't only deal with industrial products	Replace "their industrial production and distribution cycles" with "*to the material goods lifecycle"*	
FR29	4.1	9th bullet	Ed	Consistency	Replace "anti-counterfeiting" with " *authentication*"	
FR30	4.1	9th bullet	Ed	Consistency	Replace "requirements" with "*criteria*"	

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.

Template for comments and secretariat observations

Date: 2009-07-30	Document: **PC246n017**

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of comment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted
FR31	4.1	9th bullet	Ed	Clarification	Replace "for every level" with "*and/or levels"*	
FR32	4.1	10th bullet	Ed	Consistency	Replace "anti-counterfeiting" with " *authentication*"	
FR33	4.1	10th bullet	Te	It is not the aim of this standard	Cancel "and deploy"	
UK8	4.2	1, 2, 3	Te	There is some feeling among IAA members that, while the definitions and descriptions of each type of tool are good, to designate them as Type 1, Type 2 etc is unhelpful. While the attempt to establish neutral, non-descriptive words is recognised, it may be that this defeats the intention of a standard for authentication tools, by obfuscating rather than clarifying meaning. The "Types" as described equate to the categories of Overt, Covert, Forensic etc which are in common use and which were defined by the CEN CPF Workshop. Perhaps adopting these words instead of Type 1, 2, 3 will improve communication between practitioners, where the use of Type 1, 2, 3 etc will confuse.	Further consideration by PC 246, with reference to the CEN CPF Workshop definitions (attached). (Note that this Workshop was disbanded by its members when 246 was established as members did not want to be divisive and welcomed ISO's initiative.)	
UK9	4.2 on			Still to be considered by IAA members after further drafting by PC 246.		

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.

Template for comments and secretariat observations

Date: 2009-07-30	Document: **PC246n017**

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of comment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted
FR34	4.2	1st paragraph 1st sentence	Te	Consistency with the decisions made during the first PC246 meeting	Replace "This typology is not intended to rank the solutions according to performance effectiveness" With "*This typology is not intended to rank the anti-counterfeiting devices according to performance effectiveness*"	
FR35	4.2	1st paragraph Last sentence	Ed	Clarification	Replace "An anti-counterfeiting solution may combine several types of anti-counterfeiting devices." With "*An anti-counterfeiting solution may consist of one or several types of anti-counterfeiting devices.*"	
FR36	4.2	Examples	Te	This standard is supposed to be solution independent. Examples may influence the reader.	Cancel examples	
FR37	4.2	4.2.1, 4.2.2, 4.2.3	Ed	All the content of 4.2 which is located after 4.2.3 seems to be part of this paragraph, which is false.	Cancel the numbering	

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.

Template for comments and secretariat observations

Date: 2009-07-30	Document: **PC246n017**

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of comment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted
FR38	4.2	2nd paragraph	Ed	Clarification	Replace the current definition for Type 1 with "*verification protocol can be performed by an informed or trained inspector, by purely human means: senses, acting, thinking, with the exclusion of any technical tool, independently of any external source of information*".	
FR39	4.2	3rd paragraph	Ed	Clarification	Replace the current definition for Type 2 with "*verification protocol is performed by an informed or trained inspector. The protocol requires a technical tool for its execution. The technical tool may be an off-the-shelf tool (C) or be built on purpose (D). The protocol may be stand-alone (A) or involve access to an external service or source of information (B). The interpretation can be made by the inspector using his human means (E) or be provided by the technical tool (F). The protocol does not require moving the product from its current location and provides a quasi-immediate answer*".	

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.

Template for comments and secretariat observations

Date: 2009-07-30	Document: **PC246n017**

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted
FR40	4.2	4th paragraph	Ed	Clarification	Replace the current definition for Type 3 with "*verification protocol is performed by an informed or trained inspector. The protocol requires moving part or all the product to an expert analyses center. The analysis center may use only off-the-shelf tools (C) or require a tool built on purpose (D). The protocol may be executable by the analyses center in a stand-alone mode (A) or involve access to external services or sources of information (B). The interpretation can be made by the inspector using his human means (E) or be provided by the technical tool (F). The protocol may take a certain amount of time to provide an answer*".	

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.

Template for comments and secretariat observations

Date: 2009-07-30	Document: **PC246n017**

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of comment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted
FR41	4.2	Table describing Inspector and element of authentication	Ed	Clarification	Move the table before the description of the types.	
FR42	4.2	table	Ed	Clarification	Replace "Tool" with "*Control means*"	
FR43	4.2	Table	Ed	Clarification	Name of the line "*Inspector*" and name of the column "*element of authentication*"	
FR44	4.2	Tools definitions	Ed	Clarification	Add *(A), (B),* … in front of the definitions	

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.

Template for comments and secretariat observations

Date: 2009-07-30	Document: **PC246n017**

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of comment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted
FR45	4.2	Standalone tool	Te	Consistency with the definitions of the types	Replace"technical tool which integrates the functions required to be able to interpret the authentication element in-the-field, off line" with "*technical tool which integrates the functions required to be able to interpret the authentication element, without connection to an external source of information*"	
FR46	4.2	Standalone tool	Ed	Consistency with the table	Replace "Technical tool" with "*control means*"	
FR47	4.2	On-line tool	Ed	Consistency with the table	Replace "Technical tool" with "c*ontrol means*"	
FR48	4.2	Off-the-shelf tool	Ed	Consistency with the table	Replace "Technical tool" with "*control means*"	
FR49	4.2	Purpose-built tool	Ed	Consistency with the table	Replace "Technical tool" with "*control means*"	

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.

Template for comments and secretariat observations

Date: 2009-07-30	Document: **PC246n017**

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of comment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted
FR50	4.2	On-line tool	Te	Clarification	Replace " technical tool which requires a real-time on-line connection to be able to locally interpret the authentication element" with "*control means which requires a real-time on-line connection to an external source of information to be able to interpret the authentication element*"	
FR51	4.2	Last sentence	Ed	Clarification	Replace "tools" with "*control means*"	
FR52	5	whole clause until 5.6 included		This comment aims to give a technologic generalization and a better understanding in the description of the performance criteria .	Replace the current clause 5 until 6.6 included with the text in annex B. The criteria are ordered by relations between entities. To do so, the chapter 5 is rewriten. The corresponding link with the previous version of the text is shown between brackets and written in underlined italic as this sentence.	
DE18	5.1	Para 3	te	(18) The mentioned CWAs have been converted into European standards, meanwhile (CWA 14167 into EN 14890-1, EN 14890-2) or are going to be converted (CWA 14169).	Check and change accordingly. Take these standards into account in Normative References or in a Bibliography	

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.

Template for comments and secretariat observations

Date: 2009-07-30	Document: **PC246n017**

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of comment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted
DE19	5.1		te	(19) The current text mandates that, should an electronic signature be part of an authentication measure, its key lengths be at least those selected for the protection of long-lasting electronic documents in the referenced CWAs/ENs. This is not appropriate, as technical constraints (e.g., available space to store the required data) might preclude using the referenced key lengths, while a shorter key length might still offer adequate protection in the particular application scenario envisaged.	Refer to the referenced CWAs/ENs as guidelines without mandating a particular key length or level of protection.	
DE20	5.5	Title	ed	(20) Grammatical mistake	Change to "Usability"	
DE21	5.5.1		te	(21) The statements need to be formulated in a normative way and give requirements and/or recommendations addressed to a stakeholder.	Change accordingly	
FR53	5.7		Te	Out of scope	Remove this paragraph	

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.

Template for comments and secretariat observations

Date: 2009-07-30	Document: **PC246n017**

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of comment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted
FR54	5.8	Title	Te	To avoid to enter in the competence field of the regulation	Replace the title with *"Ability to provide pieces of evidence"* And add *"Existence and respect of a verification protocol to check if the verification was made in the conditions proposed by the solution supplier"* And cancel the other subtitles.	
FR55	6		Te	Clarification	Replace the current paragraph with annex C	

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.

Template for comments and secretariat observations

Date: 2009-07-30	Document: **PC246n017**

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of comment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted
FR56	7		Te	Reference to national or regional standards are not relevant to an international standard.	Cancel [1] "Accord AFNOR AC Z 60-100 "Prévention et dissuasion techniques pour la lutte anti-contrefaçon (protection des droits de propriété intellectuelle) - Spécifications d'un cadre générique décrivant les dispositions d'authentification des produits, d'organisation de la traçabilité et de contrôle dédiées à la lutte anti-contrefaçon"	
DE22	Annex A		te	(22) It needs to be clarified if Annex A is normative or informative. The heading "parameters to be assessed" implies that it is normative and gives requirements.	clarify	

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.

Annex A :

Introduction

Depending on the data source and method of calculation, counterfeit goods is estimated up to 10% of world trade, and the counterfeit market has been booming in recent years.
This growth has been promoted by globalization, which accelerated the development of goods and services exchange between States, and by the development of the internet, which encouraged the rise of e-commerce. Counterfeiters take advantage of this "easy trade" environment to spread on a big scale counterfeits on the market.
Indeed, the range of counterfeited products has been developed strongly since over a decade, and is now no longer limited to luxury goods. Counterfeit ing is spreading to every economic field even if some sectors are more affected than others.
Counterfeiting is an infringement of intellectual property rights, a point that need to be kept separate from the question of product quality and the distribution of authentic products via alternative business channels.
Counterfeiting commonly concerns:

- Copyrights and rights related to copyrights: unauthorized reproduction of an original literary or artistic works or software belonging to a third party

- Patents: unauthorized production and/or marketing of a copy of a product or process covered by patent protection granted to the patent holder or to the authorized licensee for a new invention that is inventive and industrially applicable, in many cases including a supplementary protection certificate.

- Trademarks: unauthorized total or partial reproductions or imitations, without the authorization of the trademark owner or its authorized licensee, of the distinctive sign or combination of signs that a business organization attaches to a product or services to distinguish its product or services from those of others entities.

- designs or models : using or making similar or identical copies, without authorization from the owner, of the representation of a product or part of a product that confers the characteristic lines, outline , colors, shape, texture, and/or the materials of the product itself and/or its trade dress.

Products uncovered by intellectual property rights may also be subject to fraudulent practices. They cause loss of earnings, job losses and brand value damage for the companies targeted. Consumers may also be victims of these practices. Indeed counterfeit goods do not necessarily offer the same guarantees in terms of safety and/or compliance with environmental measures and regulatory requirements, generating risk for consumers and users.
That is why counterfeiting of toys, tools, automotive spare parts or electrical products is a potential threat to the safety of individuals.
Furthermore, the distribution of counterfeit medecine remains a major public health concern for States .
Awareness of the extent of this phenomenon and the dangers associated requires the adoption of appropriate measures at different levels.
Beyond the legal aspects to ensure intellectual property rights, the fight against counterfeiting requires the setting up by the business of technical devices tailored to their needs and their products. These devices become more effective when they are adapted to product lifecycles .

These devices must allow products authentication throughout the supply chain in order to facilitate recognition of genuine or forged product.
Establishing the authenticity of a product[1], in other words recognizing that the product is genuine or forged in order to demonstrate whether it is a counterfeit, consists in checking whether the product reproduces the essentials characteristics of the authentic product to help establish whether or not there has been infringement. The first step, then, required to provide solid ground on which to conduct this challenge, is to establish what these essentials characteristics are , in particular the product's origin, and then to verify whether the suspect ed product does objectively and concretely present these characteristics.
If there any doubt as to the authenticity of a product, it is the inspector's role , once they have observed the characteristics of the suspected product and/or anti-counterfeiting device, to examine whether these characteristics match those of the authentic product and/or anti-counterfeiting device. this process is ment to be an analysis essentially of technical characteristics , where time pressure is a major element for success in any effective data input and investigation procedure.
Products can be authenticated in one of two ways: either by experience, or by authentication elements.
For the professionals tasked with carrying out the verifications and who are used to handling the products, experience is the result of the match made between several products by their experienced eye. They know by experience what they need to pay attention to. However, since the counterfeits themselves get better every year, the degree of attention given and the level of expertise and experience required also need to grow. A professional who spends hours and hours examining the same kind of products undeniably acquires a mass of knowledge , acumen and sharpness of vision that will often enable them to see through the quality and origin of a part far faster than somebody else. Unfortunately, experts of this level are few and far between, and it is generally the common people that end up checking the vast majority of products submitted to inspection, a situation that makes it increasingly important to have reliable, commercially available counterfeit detection tools.

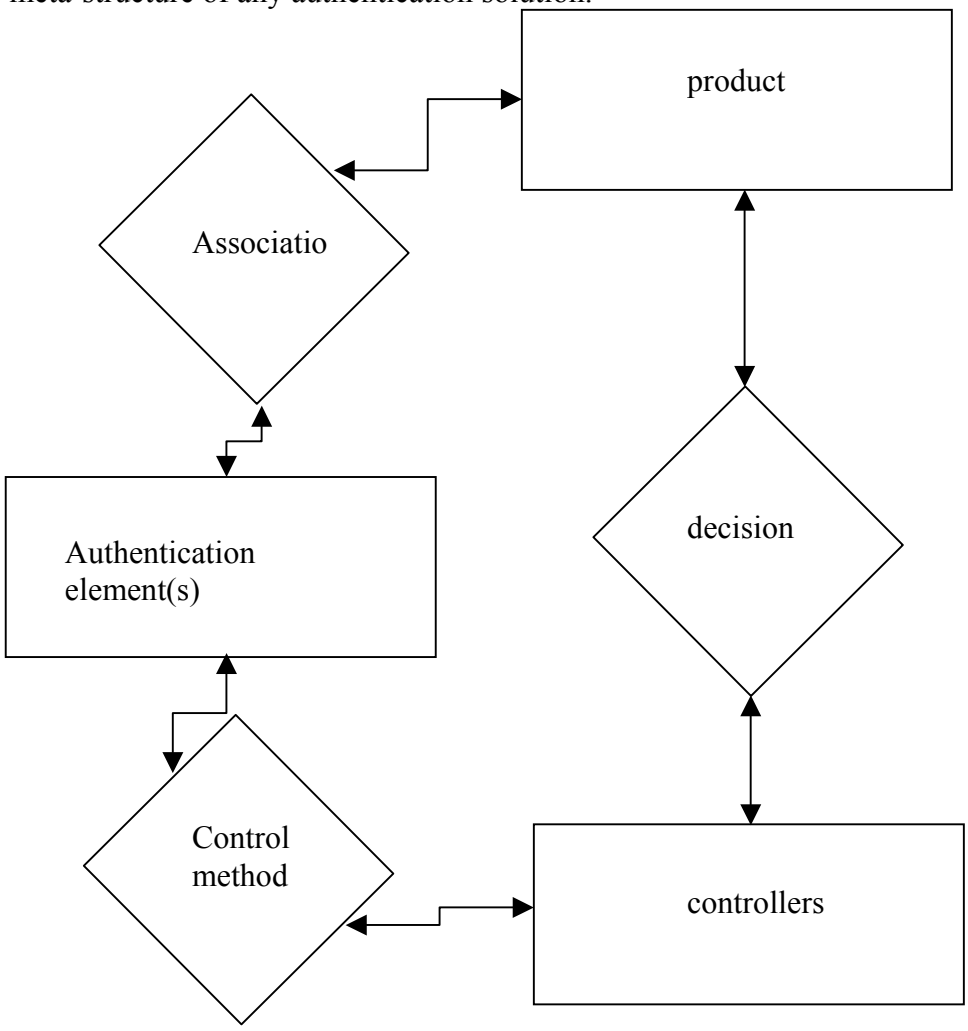
[1] Nota: this paragraph applies solely to the recognition of the authenticity of products and does not cover any counterfeit presumption stemming from independent elements such as anomalies (whether proven or suspected) in official documents, distribution circuits or shipping channels.

Annex B .

5. Performance criteria

[Corresponding to the introduction body]

The performance criteria concern the properties of the several entities constituting the authentication solution and the relations between them. Meaning entities, the product is sought to be protected, the authentication solution that will serve to authenticate the product, or controllers that will operate the act of authentication. “Relations” is a term for the physical and/or logical association that exists between the product and the authentication element(s), the method for monitoring of the controller(s) to the authentication element(s). After the results of the control, the controller(s) take a decision toward the product. This is, ultimately, the meta-structure of any authentication solution.



The standard defines the performance criteria on the nature of the association with the product, the authentication solution and the control method. It will be the right holder to define the context of implementation of elements of authentication, ie to define the product, the controllers and the type of decision.
Any single anti-counterfeiting solution may combine several authentication elements working together to build proof (nb: it would be interesting to introduce the concept of technologies stacking) These components may operate on different types and with different levels of accessibility (see 4.2) In this case,if it's relevant, the performance of each type should be considered individually . With the aim of assisting the user to choose the better adapted anti-counterfeiting solution for his needs, criteria consider both the intrinsic performance of the solutions and the performance of their use.
The main criteria is the robustness of the anti-counterfeiting solution to be defined as follows:

5.1 Robustness/Vulnerability of the anti-counterfeiting solution:
[corresponding to the 5.1 paragraph]
The robustness of a solution is measured by assessing its vulnerability. Indeed, for assessing the degree of robustness, we conduct a series of tests designed to test the weaknesses of the solution, called vulnerabilities.
The easier it is to lure the verification protocol, the more important the vulnerability of the authentication solution will be.
In order to measure the robustness of an anti-counterfeiting solution, and if this solution uses a system of information, it should be advisable to consult the Common Criteria (ISO 15408), for the relevant parts of the information system (software components and) .
5.1.1*[added paragraph]*The level of robustness is defined by the technological effort and the availability of the needed resources which was necessary to lure the verification protocol. The solution should be difficult or impossible to reproduce, either by simulation (using different methods) or by emulation (using the same processes). The characteristic « difficult » or « impossible » to reproduce should be clarified:

5.1.1.1*[added paragraph]*By requiring an ordinary level of difficulty, it is expected that the verification protocol cannot be lured with commonly available means of reproduction.

5.1.1.2 *[added paragraph]*By requiring a medium level of difficulty, it is expected that the verification protocol cannot be lured with specialized means available from industrial laboratories, as commercial benefit for example.

5.1.1.3 *[added paragraph]*By requiring a high level of difficulty, it is expected that the verification protocol cannot be lured with means, such as those available to a government agency

5.2 The association *[corresponding to the 5.1.2 paragraph and 5.4 paragraph apply to the association]*
Association means any means to guarantee the integrity of the relationship between the product and its elements of authentication. It is crucial to develop either tangible or intangible interdependence between the authentication element and the product it protects. Tangible interdependence means destruction, visible or recognizable alteration of the authentication element in case of attempted dissociation of this component and product, or product and container. Intangible interdependence means logical association between the certification element and a reference, which is a non-erasable and non-duplicable association.

5.2.1 The association must be affected by any attacks undergone (principle of reducing the risks of non-detection of an attack).

5.2.2 To do this, the association must have one or more characteristic that may change irreversibly at the first attempt of aggression.

5.2.3 The modification of these characteristics has to be detected during the verification protocol.

5.2.4 The Association must be able to resist in the environmental conditions of the product throughout its life cycle. Similarly, the sensitivity of the association should remain stable in normal environmental conditions throughout its life cycle (principle of risk reduction of false alarms).

5.3 *[added paragraph]*The performance criteria to be used for an authentication element depend on the characteristics of this authentication element that allow it to fulfill the functions of authentication expected.

5.3.1 Resistance of authentication elements *[corresponding to the 5.4 paragraph apply to the authentication elements]*
The resistance of the authentication elements to unintended alterations (climate, natural wear, handling ...) is essential in the sustainability of the performance of the solution during the period requiring the application of the verification protocol.

5.3.2 *[added paragraph]*Batch authentication element
The batch authentication element is an element which is designed to be perceived as identical by a stage in the verification protocol. The resulting series covers a range of products from the same batch

5.3.2.1 *[corresponding to the 5.1.2 paragraph apply to the batch authentication elements]*
Security of the creation of the batch authentication elements
The authentication elements cannot be produced in excess of the quantities ordered.
It is necessary to ensure the level of safety and traceability linked to the creation and / or production of authentication elements, and to human intervention in the production chain and logistics.
All information and specific means to industrially produce authentication elements should be explicit safeguards. The destruction of these information and resources can be requested at the end of production.

5.3.3 *[added paragraph]*Authentication element per unit
The authentication element is generated to be perceived as unique during a stage of the verification protocol. Each element covers a single good. These elements are identified by features discriminating against each other.

5.3.3.1 *[added paragraph]*Authentication elements per unit generated in a deterministic way
In these processes, the unique value is known before the generation of the authentication element.

5.3.3.1.1 *[corresponding to the 5.1.2 paragraph apply to the authentication elements per unit generated in a deterministic way]*The security of the establishment of the authentication elements per unit generated in a deterministic way
It is necessary to ensure the level of safety and traceability linked to the creation and / or production of authentication element, to human intervention in the production chain and logistics.
All information and specific means to industrially produce authentication elements should be explicit safeguards. The destruction of these information and resources can be requested at the end of production.

5.3.3.2 *[added paragraph]*The authentication elements per unit generated in a non-deterministic way
These elements are produced without any possible control of the man about the authentication features that result. In this case, the authentication element is the subject of a registration reference.

5.3.3.2.1 *[corresponding to the 5.1.2 paragraph apply to the authentication elements per unit generated in a non-deterministic way]*The security of the creation of the authentication elements per unit generated in a non-deterministic way
It is necessary to ensure the level of safety and traceability linked to the production and the registration of authentication elements.

5.3.3.3 *[added paragraph]*Guarantee of non-recovery on generation of the authentication elements per unit
We will have to get the statistics and mechanisms to ensure that no authentication element has been generated twice.

5.4 *[corresponding to a part of 5.6 paragraph and 5.1.3 paragraph]*The reliability of the verification protocol is the success rate of unambiguous recognition of the authentication element in the conditions defined by the supplier.

5.4.1 *[corresponding to the 5.6.1.3 paragraph]*False releases are authentication elements that were mistakenly rejected in the control

5.4.2 *[corresponding to the 5.6.1.2 paragraph]*False acceptances are authentication elements that were accepted at the control but should be refused.

5.4.2.1 *[added paragraph]*False acceptances discernment means that the verification protocol cannot distinguish the difference between two authentication elements, similar by nature but different.

5.4.2.2 *[added paragraph]*False acceptance of luring means that the verification protocol cannot distinguish the difference between the authentication element and an imitation, a copy or a clone.

5.4.3 *[corresponding to the 5.1.3.1 paragraph]*Tools inviolability
The capture devices for authentication elements must be protected and / or react to any attempt of deviation aimed to capture information that are processed or transferred, including the inability to query data bases with unauthorized tools.

5.4.3.2 *[corresponding to the 5.1.3.2 paragraph]*Normal / degraded
For capture devices having their own power source and / or operating in online mode, it must be indicated if there are different levels of degraded modes of operation (low battery, missing network ...) or an alternative protocol that may appeal to another type of authentication element.
5.4.3.3 *[corresponding to the 5.1.3.3 paragraph]*Traceability of control
Control actions can be plotted to verify the correct execution both in quality and quantity in accordance with the protocols and rules of confidentiality established with stakeholders.
5.4.3.4 *[corresponding to the 5.1.4 paragraph]*Safety of the conservation of authentication elements references
This criterion applies only in case of use of reference databases for authentication . The databases involving the references of authentication elements and verifying the authenticity of the authentication elements associated with controlled products must be protected against any intrusion. A successful intrusion must be detected and reported to the rights holder.
5.5 *[corresponding to the 5.2 paragraph]*Scalability and flexibility
The anti-counterfeiting solution must make possible to adjust the frequency and sensitivity of the controls to react to events such as the influx of goods on a geographical area, over a period, on a typology of products ...

5.6 *[corresponding to the 5.3 paragraph]*Mutualization and evolutivity of the control tools:

5.6.1 Several verification functions accessible through the same technical tool
Capability possessed by a single tool to perform verifications on different elements of authentication, with zero risk of interference between the control applications.

5.6.2 Hardware modularity

Ability to integrate hardware upgrades or additional options that will add features or improve the tool's performance levels without having to completely overhaul the tool and without weakening its security-assurance characteristics.

5.6.3 Software interoperability

Ability to integrate software upgrades or additional options that will add features or improve the tool's performance levels without having to readjust the software architecture and without weakening its security-assurance characteristics.
5.7 *[added paragraph]* Ease of integration
Authentication elements must be integrated into a production process without requiring major changes, without affecting performance. The production processes must not affect the characteristics of authentication elements.
5.8 *[corresponding to the 5.5 paragraph]*useability of the analysis tools:

5.8.1 Training
Expression of the need for training on the use of technical tools according to levels of intervention and pre-requisite. This includes training on the information sought and the tasks assigned to the stakeholder as part of the solution

5.8.2 Usage
Ease of implementation and availability

5.8.3 Autonomy
Operating time on site in normal mode, degraded mode

5.8.4 Ergonomics
criteria that evaluates the efficiency, satisfaction, well-being and ease of learning for the user while conducting the verification protocol

5.8.5Innocuousness
No negative effect on human health

5.9 *[corresponding to the 5.6 paragraph]*Reliability/solidity of the technical tools and of the control devices:

5.9.1 MTBF (Mean Time Between Failures)

The intrinsic reliability of the technical tools, resulting from formula-based calculations of the individual reliability of each of the tool's components.

5.9.2 Maintenance, preventive maintenance

Scheduling and specifying the interventions and regular checks that needs to be performed on the capture systems (such as cleaning, settings, calibration, etc.)
5.9.3 Ruggedness

Resistance to stress of all kinds (protection element against water / dust, working temperature range, impact strength, etc.)

Annex C :

6 – Effectiveness measurement of the anti-counterfeiting solution

Performance of anti-counterfeiting solutions is also linked to the fact that they are properly implemented and used. Effectiveness measurement is the only way to check that a solution is complying with the right owner objectives and the announced performances. Measurement protocols have to be defined. However, measurement protocols will depend of the controlling protocols that are defined and implemented by the right owner as effectiveness measurement is first the traceability of the different steps of production, association and control of the authentication elements.

Defining a standard and unique effectiveness measurements protocol as well as control protocols themselves is not feasible. Therefore this chapter will describe the key points to consider by right owners to define their own measurement protocols.

The measurement of effectiveness can be done:

- in the creation, and processing of authentication elements
- in the normal verification/authentication process
- in case of specific verification/control process as a reaction to attacks or to detection of abnormal rate of fake products/goods

6.1
As every process of manufacturing, manufacturing of authentication elements have to comply with quality requirements. This can be linked to the quality manual of the authentication solution providers, including its subcontractors and suppliers if any, Quality audits is usual in all sectors of industry.
This means that all the processes from authentication element creation to the shipment of the protected authentic products/goods which lack of robustness may impact the global effectiveness of the anti-counterfeiting solution have to be described and audited.

When required, and especially when IT are involved, security audit may also be required

Quality of the authentication elements have to be considered. Discrepancy of tolerances are variations in quality of the production or association of the authentication elements that will impact the true/false response as the larger the variation of production parameters, the larger the window of tolerance of the tool will be, increasing the risk of non detecting fake products/goods.

Dynamic control of the production of authentication elements will assure the reliability of the on site controls as it will guarantee the quality.

Effectiveness measurements can made with the traceability of:
nb of rejections (unauthentifiable products) in final production control
nb of rejections (unauthentifiable products) on site

6.2
Traceability of the normal control protocols may concern:

- the inspector

- the tool
- the connections and data exchanges if required
- the results

Inspector:
- identification
- authentication
- definition and revocation of rights

Tool:
- maintenance, calibration
- tampering
- downloads
- destruction

Connection and exchanges:
- successful and denied logins
- service level agreement

Results:
- ratio of controls
- nb of true/false detection
- nb of authentication elements non interpretable (« don't know »)

6.3
In case of emergency (abnormal counterfeiting rate detected) control protocols may be adapted or specific control protocols can be activated.
Measurement of effectiveness is then the key element to check the efficiency of the emergency control protocols

6.4
Obsolescence monitoring
Considering the evolution of technology, robustness of the authentication solution may decrease over time. Therefore, the right owner should regularly assess whether the solution deployed is still robust enough.

WORKSHOP CPF N07-012

Secretariat : UNINFO	Date: 2008-03-28

CEN/ISSS Workshop on Anti-counterfeiting: Protocols for Detection of Counterfeits (WS/CPF)

TITLE **draft proposed outline CWA**

SOURCE **WS chair**

ACTION **to be discussed**

CEN/ISSS	European Committee for Standardization/Information Society Standardization System	
Secretariat	UNINFO	Massimo Actis Dato
Massimo Actis Dato	☎ : + 39 011 50 10 27 🖷 : + 39 011 50 18 37	🖃 : dato@uninfo.polito.it
	☎ : + 39 011 50 10 27 🖷 : + 39 011 50 18 37	🖃 : sirocchi@uninfo.polito.it

Counterfeit:

A counterfeit is an item, manufactured or otherwise, which in its physical characteristics, naming, packaging or other identification copies the identity of another item with the deliberate intent to defraud. Usually a counterfeit claims to be an authentic, brand-name product or component but is in fact produced without the authority of the designer or manufacturer of the authentic item and is often made from inferior materials.

Thus a counterfeit may be the product of a mass production operation or a single operator. It may be a product that is an accurate copy of the copied item, or it may only bear a superficial resemblance to the copied item, but in either case it will be sold as or described as, verbally or in writing, the copied item. In many cases the packaging of the counterfeit will deliberately resemble or copy the packaging of the authentic item. In some cases this will also include unauthorised brand extensions or product variants where the name, logo or branding of a company or brand is applied to items outside the authentic item's product range.

An item is not a counterfeit if it does not claim to be another product. Thus products which are packaged and named in such a way as to emulate an established or authentic product through similar naming or packaging are not necessarily counterfeits, although they may be subject to action by the owners or producers of the authentic product for mis-use of "trade dress" - ie the look and feel of the authentic product and its packaging.

Today, it is very common for branded or other authentic products to be manufactured by third-party sub-contractors which are supplied with designs, drawings, access to component suppliers, and/or labels and authenticating features by the contracting owner. Normally such arrangements will specify the number of items the sub-contractor is entitled to make. If the sub-contractor produces more than this entitlement and then goes on to sell these additional items, this over-production is likely to be a breach of the contract with the contracting owner, but the items thus produced are not necessarily counterfeit. They will be counterfeit, however, if they use components, packaging or other materials which are not supplied by the authorised supplier, are inferior to or do not match those specified by the contractor, while claiming to be the same as the authorised item.

An item which is re-packaged or otherwise distributed outside the terms of the original distribution or supply contract with the owner or supplier of the authentic product is not counterfeit, but is parallel trade or diversion. In the EU such parallel trade is legitimate (although the European Commission is considering proposals to change this as it applies to medicines and medical products). However, diversion of items away from the supposed customer or market may be a breach of contract, and such diversion does often facilitate the introduction of counterfeits into diverted shipments.

Note: this definition deliberately avoids reference to *intellectual property rights* which is a legal construct that includes patents, trademarks, designs and copyrights. In most legal jurisdictions these have to be formally registered in order to be protected (with the exception of copyright). Therefore if *counterfeit* is

defined in relation to IPR, there cannot be a counterfeit if the IPR has not been registered, whereas the reality is that an item can be counterfeited even if the IPR has not been registered in the jurisdiction where the counterfeit is made or on sale.

However, there are occasions when it will be necessary to take a legalistic view of counterfeits, in which case the definition in the European Union Customs Regulation 1383/2003 should be referred to.

Authentication

Authentication Authentication is the act of establishing or confirming an item is what it claims to be. Authenticating an item means confirming its nature and composition as well as its provenance (but see also Tracking Technology below). Authentication is thus central to the detection of counterfeit goods.

Authentication of an item is carried out by an examination of

- the *item*,
- all the components of the item
- the packaging used on the item (if any)
- *authenticators* that are placed on or in the item or its packaging with the specific intent of giving an indication that the item is authentic.

If anyone of the above items is counterfeited, the product should be considered counterfeited.

Authenticators could include but not necessarily be limited to special seals, marks, labels, or additives designed explicitly not to be copied and therefore designed to be authenticated. (to expand)

These examinations may be undertaken by people who are trained, equipped and focused on carrying out such examinations, or they may be undertaken by members of the public, in their role as buyers and consumers. Additionally, the examination may be undertaken in a controlled environment with time for detailed examination, or it may be undertaken in an environment where time, the physical environment and situational pressures make it important to reach a quick decision, although this decision may not be ultimately definitive (see definitions of examination hierarchy below).
Because of this variety of examiners and examining situation, authenticators are designed to meet different operational requirements, and are therefore categorised in to *authentication layers*.

Authentication Layers, including Secure Trail;

Layer	Function	Examination Method	Tools
Overt	Rapid check for a first-level test that an item is or is not genuine.	Human senses, often sight, unassisted	None
Covert	Non-invasive check of suspect item to determine to a high degree of probability whether it is genuine or not, and thus facilitate impounding/arrest decisions.	Tool to render the covert feature visible to human sight; and/or a machine reader to display secure trail data contained in the covert feature.	Usually handheld reader, which may require electrical power, often proprietary or at least specific to the covert feature; may instead be installed on warehouse/distribution centre conveyor or retail sales point.
Forensic	Analysis to provide evidential-quality proof that an item is counterfeit.	Laboratory analysis equipment, sometimes available in portable kit.	Laboratory analysis equipment
Secure Tracking	To provide data about the item, such as manufacturing and distribution information.	Remote database *or* read/write device on product.	Handheld or conveyor or retailer installation of reader/decoder.

AUTHENTICATION LAYERS

Authentication depends upon one or more authentication layers legally called corroborative evidences.

There are three kinds of authentication layer, which may be used discretely or in combination:

- Overt authentication
- Covert authentication

- Forensic authentication

Overt authentication

Overt authentication can be directly performed by an observer such as a member of the public or untrained inspectors and does not require any additional reader or equipment to allow a feature to be verified as genuine.

Overt authenticators are apparent to the human senses, most often sight but touch is also used as a characteristic. Overt authenticators are often therefore employed as a *front line* feature (that is, they are intended for examination in the *front line* of retail, wholesale or other environments) where a visual check is the only one immediately possible and this can be undertaken by people without training or equipment, such as consumers, store clerks and check-out staff.

Overt authenticators must be difficult to copy accurately so that their absence or their imperfections will alert examiners to the fact that an item may not be genuine, because counterfeiters will always try to reproduce all visible features on the item and its packaging in their effort to produce a realistic copy. The absence of an overt authenticator, or the presence of a crude copy, therefore, is an indication that the item is probably not genuine.

Overt authenticators may also be examined at the *second line*, that is by trained and equipped inspectors, to establish whether they are themselves genuine. In this case the examiner will have knowledge of the genuine authenticator, preferably with one available as a reference item, and will know and be able to look for the intricate or hidden features that are most often not reproduced in a copy.

The most widely used overt authenticators include optically variable inks, intaglio[1] printed marks, optical devices such as holograms and angle-dependent latent images, and watermarks. Rights holders also use product design features as overt identifiers, such as perforations, shapes, colours, cuts and images, as front line inspection features.

Covert authentication

Covert authenticators are not instantly recognisable to the human senses. They require special readers or detectors to verify their presence and validity, either revealing themselves to the human senses (usually vision) or to the detector. People using these technologies may need some training and therefore covert authenticators are primarily intended for *second line* examination; that is, examination by a person with some training

[1] Intaglio printing is a process that uses deep grooves in the printing plate and high pressure ink application to create raised patterns on the printed item, which can be felt by touch.

who is examining an item thought to be suspect. This suspicion may be a result of first-line examination or investigative intelligence.
Most covert systems are designed so that they can be used in the field, though ease of verification and time taken for authentication may vary.

Covert technologies exploit all kinds of physical or chemical effects, although in product authentication mostly physical effects are used, involving radiated energy originating from one or the other part of the electromagnetic spectrum. Ultraviolet (UV) and Infrared (IR) radiations are the most commonly used, through the use of coatings, inks or fibres in or on the packaging and requiring illumination by a special light source.

Chemical compositions are also used, ranging from those which react with a pen-type detector to show a visible mark, to complex organic molecules which are coded to the specific product and which require a proprietary detector to both check their presence and check that the code is correct.
The security level will essentially depend on the sophistication of the signature to be detected by the radiated energy. The need for security (often associated with commercial availability) is to be balanced with cost and ease of use.
Covert authenticators are an important part of an examiner's decision process to determine whether the item is *probably* counterfeit and should therefore be confiscated or impounded.

*The term **semi-covert** authenticator is also sometimes used to refer to authentication features that are not immediately obvious but do not require the use of any specialist detectors. These features are often verified using a person's senses or by physically moving the object. Semi-covert technologies include features like thermo chromic elements and familiar techniques such as microtext. (Duplicates?)*

Overt and covert authenticators which are examined by one or more human sense, whether a tool to reveal the authenticator is required or not, are termed *sensory authenticators*, to differentiate them from authentication through the secure trail (see below) which requires use of a telecommunications and/or computer system, which are therefore termed *digital authenticators*.

Forensic authentication

Forensic authentication is the ultimate authentication level. Generally, it involves either analyzing the product itself or detecting and analyzing trace elements, known as *taggants*, previously added in the product or its packaging. Forensic features are not widely used in first-line or second-line authentication. They are usually employed by trained investigators, either within a manufacturer's laboratory or a public criminal forensic laboratory, who will examine a product has been identified as potentially fake, as the analysis of most forensic features requires the expertise of a forensic sciences laboratory.

ANTI-TAMPERING DEVICES

These are not authentication layers as such but can be used to support product authentication in situations where, for example, the content of a package might have been replaced. Sleeves, seals, films, tapes, foils, caps, closures and labels have been developed that secure containers and packaging and ensure that the contents cannot be tampered with, replaced or diluted. These devices will make tampering attempts obvious, were they successful or not.

A tamper-evident feature that is intact assures the buyer or verifier that the container has not been tampered with and that the product is likely to be authentic. Anti-tampering features increase consumer confidence in a product's integrity. Anti-tampering technologies have traditionally been used for drinks (shrink sleeves and tamper-proof caps and closures) and in the pharmaceutical industry (blister packs), though there is now increasing use of this approach in other areas, including cosmetics and the food sector.

Unique Product Identifier
The issue on to an item of a unique product identifying code, stored on a central database, enables that item to be tracked through the distribution chain. This means that at any point in the chain it should be possible to establish where the product originated, where it has been (and perhaps who has handled it) and whether it is in the right place at the time of examination. This will help to establish whether the product or a group of products is suspect as a counterfeit, so that the authenticator/s can then be examined to determine whether the item is or is not genuine.
There are currently two categories of system used to establish the secure trail: *static* and *dynamic*. A **static system** applies a code to the product at the point of manufacture, that code normally containing information on the product itself, its origin and destination, and this code will remain in the same state through the distribution chain. Examples include barcodes and 2D data matrices. **Dynamic systems** similarly apply a code to the product, but as well as being readable, it is in a form that can be written to, allowing the addition of information about the item's route through the distribution chain and who has handled it. The primary example of a dynamic secure trail technology is *radio frequency identification* (RFID).
A tracking feature which provides the secure trail primarily provides:

- increased efficiency within the supply chain
- compliance with ever more stringent regulations
- more effective product recalls
- provide evidence that a product was illegally produced, traded or distributed

By analysing tracking information, conclusions can be drawn as to a product's likely authenticity. On the other hand, a data storage element on a package that identifies the manufacturer or distribution route does not automatically prove that the product inside is genuine. Data storage elements such as standard barcodes or standard RFID can easily

be corrupted, destroyed or copied. Also, criminals may open legitimate packages and replace genuine products with counterfeits. For this reason, secure tracking technologies have been developed which combine authentication and tracking layers.

SECURE TRAIL TECHNOLOGIES
Combined authentication layers

Most rights holders and stakeholders in a security solution have a number of requirements that can be better supported by the application of the right combination of overt, covert, anti-tamper and forensic technologies. Quite often, for example, overt features are combined with less visible, covert, features that enable trained inspectors to authenticate the product with even greater certainty.

Hierarchy of examiners

Level	Examiner	Definition	Equipment Expectation	Training Expectation
1	**Consumer**	**Product purchaser**	**No tools.**	**None, but tactility, taste and vision for familiar items, and any awareness instilled by advertising or educational campaigns.**
2	**Retailer**	**Seller of product to consumer:**	**Standard bar-code reader installed; credit card reader installed;** **might install or store by checkout:** • **device to show the semi-overt element** • **track and trace and/or pedigree reader**	**Possible short training/demonstration by brand owner's sales or other representative, plus touch and vision with products handled every day.**
3	**Specialist**	**IPR-owner**	**Equipped with**	**Trained by supplier and**

Level	Examiner	Definition	Equipment Expectation	Training Expectation
		staff **Government inspector (eg DRA, Aviation)**	**required portable equipment** **If Agency issues or specifies authentication – equipped as required; otherwise may carry basic inspection equipment**	**IPR owner** **Trained by supplier and govt agency**
3	**Law Enforcement Agency**	**Customs, police, consumer protection (ie tasked but not specialist**	**May have basic inspection equipment, access to secure IPR database and contact phone numbers**	**Trained within their overall enforcement officer training and with in-service courses.**
4	**Forensic scientist**	**IPR-owner or public sector laboratory**	**Bench analytical equipment**	**High level specialist analytical training**
5	**Judiciary**	**Prosecutors, judges and juries**	**None**	**None**