ISO/PC 246 N 039

2010-02-04

ISO / PC Secretariat
Your correspondent : Clément CHEVAUCHÉ
Direct line : + 33 1 41 62 82 79
Fax : + 33 1 49 17 90 00
E-mail : clement.chevauche@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.org

ISO / PC 246
Anti-counterfeiting tools

Secretariat : AFNOR

Title :	Result of the call for comments on ISO WD 12931.2 "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.

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

Result of voting

Ballot Information:	
Ballot reference:	PC246n035 - Call for comments on ISO WD 12931.2
Ballot type:	CIB
Ballot title:	Call for comments on ISO WD 12931.2 Performance criteria for authentication solutions for anti-counterfeiting in the field of material goods
Opening date:	2009-11-16
Closing date:	2010-01-31
Note:	

Member responses:	
Votes cast (12)	Austria (ASI) Canada (SCC) China (SAC) Finland (SFS) France (AFNOR) Germany (DIN) Kenya (KEBS) Korea, Republic of (KATS) Netherlands (NEN) Spain (AENOR) Switzerland (SNV) USA (ANSI)
Comments submitted (0)	
Votes not cast (5)	Egypt (EOS) Italy (UNI) Nigeria (SON) Romania (ASRO) United Kingdom (BSI)

Questions:	
Q.1	"We wish to comment ISO WD 12931.2 "Performance criteria for authentication solutions for anti-counterfeiting in the field of material goods""

Answers to Q.1: "We wish to comment ISO WD 12931.2 "Performance criteria for authentication solutions for anti-counterfeiting in the field of material goods""		
7 x	**Yes**	**Canada (SCC)** **France (AFNOR)** **Germany (DIN)** **Kenya (KEBS)** **Korea, Republic of (KATS)** **Switzerland (SNV)** **USA (ANSI)**
2 x	**No**	**China (SAC)** **Spain (AENOR)**
3 x	**Abstain**	**Austria (ASI)** **Finland (SFS)** **Netherlands (NEN)**

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
CH14			ge	Definition & standardisation: 3 layers approach, 1 common platform for public layer across channels (for OTC check), others specific to supplier.		
CH15				Reference to WHO Good Distribution Practice for Pharmaceutical Products and CEC 2001/83/EC Directive of the European Parliament and of the council reg prevention of the entry into the legal supply chain of medicinal products which are falsified in relation to their identity, history or source.		
CH17				Generic form for inspectors (customs, police, etc.). Propose pass/fail criteria. Checklist to be provided with glossary.		
CH19				General: Shorten the ISO 246 document.		
CH20				The scope of ISO 246 should include 3 aspects: 1. IP 2. safety & public health (consumers) 3. forgery & use forgeries (excise duties, etc.)		
CH21				Add a category for mass serialization and track & trace technology.		
FR1	Whole document		Ge		Replace authentication tools with authentication solutions when appropriate	
FR2	Whole document		Ed	Authenticators is not appropriated	Replace with inspector when authenticator refers to the person in charge of performing authentication, Replace with authentication element otherwise.	
FR48	Whole document		Ge	Devices may be misinterpreted	Replace devices with tools	
US1	Entire document		GE	The title of this document refers to solutions. The text of the document seems to distinguish between elements and devices/tools. The document appears to show that elements and devices/tools are distinct entities, but that they are all part of an authentication solution. However, throughout the document there does not seem to be a strict	The terms authentication solution, authentication device, authentication tool, authentication element, technical tool and authentication device, need to be defined and consistently used throughout the document. After a review and establishment of the terms, the document needs to be reviewed in its	

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
				adherence to using these terms for their narrowly defined purposes. An authentication solution seems to be the overarching scheme that is derived to allow authentication of a material good. A solution will certainly include an authentication element and may also include an authentication tool. An authentication element is something that is either attached to or integrated into the physical or chemical properties of the material good. As a practical matter, an element is part of a good. An authentication tool is a separate device that is used by an inspector (either primary or secondary inspector) that enables the inspector to "read" or interpret the element. Therefore, the device/tool does not travel as a part of the good, but is maintained by the inspector. This document must be reviewed to ensure that these terms are not used interchangeably.	entirety and the terms used consistently and appropriately.	
DE2	Foreword	3rd paragraph	Ed	Project committee PC 246 is not a technical committee (TC) which is explained only.	Include task description of a PC	
US2	Forward	Paragraph 8	Ed	"products" should be possessive "requires" should be "required"	The present document aims to integrate the performance requirements for authentication tools into the product's lifecycle in any situation when required.	
DE1	General		Te	Throughout the document the verb "must" must be exchanged by the verb "shall" according to the ISO directives.	Change accordingly	
CA1	Introduction		TE	We need to verify the number referenced as there are INTERPOL statistics, as well as from other groups such as OECD. It is not clear where this number is from and we also need to state how these numbers are measured. The difficulty in using numbers by various groups is that they are captured using different criteria regarding value. Some numbers include retail value, direct manufacturing costs etc indirect impact costs etc.	Verify number	
DE3	Introduction	1st paragraph	Ed	The statement ""…estimated up to 10% of world trade.." should be referenced including the year of the observation.	Include reference or cancel/replace statement	
DE4	Introduction	Last paragraph	Ed	Statement „…made between several products by their experienced eye" should be replaced by „…made between	Replace	

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
				several products by their experienced senses“,		
DE5	Introduction	Last paragraph	Ed	Existing phrase only refers to tools; phrase on “authentication elements” may be appropriate	Add: “Such tools typically make use of reliable authentication elements.”	
FR3	Introduction	Intellectual property infringement	Te	Geographical indications are generally recognized as one of intellectual property rights.	Add an item regarding the geographical indications: Geographical indications: indications which identify a good as originating in the territory, or a region or locality in that territory, where a given quality, reputation or other characteristic of the good is essentially attributable to its geographical origin information.	
KE1	Introduction	Paragraph 1	Ed	Change of meaning from positive to negative	The range of counterfeited products has grown tremendously over a decade...	
US3	Introduction	Paragraph 1	Ed	It would be more appropriate and enhance flow to say “has grown” rather than “has been developed.” The word “since” is not necessary, and if removed “the past” should be added.	The range of counterfeited products has grown significantly over the past decade, and is now no longer limited to luxury goods.	
US4	Introduction	Paragraph 1	Ed	Needs better subject-verb agreement	Although figures vary depending on the data source and method of calculation, counterfeit goods could constitute up to 10% of world trade….	
US5	Introduction	Paragraph 1	Te	Where does this number come from? Attempts to quantify the scope of counterfeiting and piracy vary greatly. Perhaps reference to the OECD’s Counterfeiting Report would provide the best assessment of the scope of this	Confirm and credit the source of information	
US6	Introduction	Paragraph 4	Ge	Statement needs to be inclusive of a combination of methods	Products can be authenticated by *using: experience, authentication elements, authentication devices or by a combination of these methods.*	
US7	Introduction	Last Paragraph	Ed	The words “hone in” in the third line of paragraph are not clear English	Change to “focus”	
DE6	1	6th paragraph	Te	Even though the document is not intended to apply to goods referenced, it occasionally may apply.	Change: “It does therefore not necessarily apply to for example…”	

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
DE7	1	7th paragraph	ed	"This document doesn't deal…." is colloquial	"This document does not deal…"	
US10	1. Scope	Paragraph 7	Ed	Do not use contractions in formal writing.	This document does not deal with economical….	
US8	1. Scope	1	Ge	Definiton of "product lifecycle" should be added as it is part of the scope. It would emphasize the need to ensre anti-counterfeiting strategies are aware of the vunerabilities of each stage and take the apprpriate security measures.	One suggestion: (1) "the stages in which a product goes through, includes product conception, design, manufacture, service, and disposal" – a graphic may also be helpful to illustrate the product lifecycle stages.	
US9	1. Scope	Paragraph 6	Ed	The second sentence should be reworded for better flow	Therefore, it does not apply to: goods used in the financial sector, official administrative papers, identity documents or to downloadable products.	
CH13			ge	Wording is important: Authentication	Define "authentication" which is a legal term which can be used in court.	
DE8	3		ge	Terms should be arranged alphabetically.		
FR14	3		Te	Definition missing	Add: "authentication device: physical element of authentication"	
FR4	3		Ge		Cancel all the capitals in the definitions for the terms	
FR5	3		Ge		Put all the definitions in alphabetical order	
FR6	3		Te	Add a definition for specifier	Specifier: Person or entity who defines the requirements for an authentication solution to be applied to a particular material good	
US11	3	ALL	Ge	Ease of reference	Put all of the definitions in alphabetical order.	
US12	3	3.1	Ge	Term used is typically no associated with counterfeiting of material goods	Successful or unsuccessful attempt to ~~hack~~ *circumvent* an …….	
US13	3	3.2	ed	3.2 internal attack… The US believes that the terms internal and external attack	3.1.1 internal attack… 3.1.2 external attack…	

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
				should be directly below 3.1 attack. Since the terms will fall in alphabetical order, one option could be to put the definitions as sub items to 3.1.		
US14	3	3.4	Ge	Definition is insufficient	New: The simulation, reproduction or alteration of a material good with the intent to commit a fraudulent act.	
US15	3	3.5	Ge	Expansion of definition	……who uses the anti-counterfeiting device *or other means* with the aim of authenticating the product	
US16	3	3.7	Ge	Descriptive term “professional” may not be appropriate	Any ~~professional~~ intermediaries between the rights holder ……	
US18	3		GE	Add definition	Add definition for "first line authentication"	
US19	3		GE	Add definition	Add definition for "second line authentication"	
US20	3		GE	Add definition	Add definition for "Integrated/associated authentication elements"	
US21	3		GE	Add definition	Add definition for "Intrinsic authentication elements"	
US22	3		Ge	See US Comment on 4.3.2 If “digital authenticator” is the proper term for electronic verification, then add term.	Add definition for digital authenticator "Method for retrieving data from a system using an electronic interrogator"	
CH18	3.5			Definitions are unclear. There are several different definitions for the same term in different legal documents. Please explain definition of inspectors. Propose to use definitions of WHO GDP guidelines and WCO for definitions.		
DE9	3.5	Headline	te	The term “inspector” in several applications means a person specially designated and equipped to verify product authenticity. Example: customs officers are inspectors, a consumer would be a “verifier” but not an “inspector”.	Replace “inspector” by “verifier”, add special definition for inspector	
FR7	3.5		Te		Replace anti-counterfeiting device with authentication solution	
DE10	3.8		Ed	“Element of authentication” is defined, but “authentication element” is used	Align definition and use	
DE11	3.8		Ed	“visible or invisible” does not give any information	Replace “visible or invisible” by "overt or covert"	

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	3.8		Ed		Add also Authentication element	
FR9	3.11		Ed		Replace anti-counterfeiting solution with authentication solution And Devices with tools	
FR10	3.12		Ed		a system or a set of hardware and/or software systems that makes part of the authentication solution, used to control the authentication element.	
DE12	3.15		ed	Synonyms should not be used.	Delete "fake goods"	
DE13	3.15		te	Misleading definitions need to be clarified. The wording should be active to clarify the difference between a counterfeiting product to a counterfeited product.	Change to: "counterfeiting product"	
KE2	Clause 3.15		Tech	For consistency in terminology	Replace the word good with product	
CH1	3.15 & 3.16		te	Improvement to the definition of counterfeit product	Paragraphs 3.15 & 3.16 should be combined.	
DE14	3.16	Headline	te	Misleading definitions need to be clarified. The term is at least misleading as a counterfeit product can and will be understood as counterfeit, i.e. a copy or imitation. Should be readable for non-native speakers.	Replace “counterfeit” by “counterfeited” (past perf. of “to counterfeit”)	
KE3	Clause 3.17		Gen	For brevity we propose use of the term legal person. It covers both the physical person and an institution	... a certain period of time to a legal person over the creation	
DE15	3.19	First sentence	ed	The last word “secret” must be the headline of the next clause. All clause reference numbers will shift.	Correct	
US17	3.19		Ge	A broader definition of security may be appropriate for the context of this document	One suggestion: (1) “the state of being free from danger or threat where procedures are followed or measures taken to ensure such safety” *New Oxford American Dictionary*	

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
CH2	3.20		te	Authentication features and tools are used for authenticating products but cannot prevent counterfeiting. There is no solution against counterfeiting, only measures able to reduce the risk of being counterfeited.	Do not use the word “anti-counterfeiting”. Change title of this paragraph to “authentication measures” or “verification measures”.	
DE16	3.24		te	Change accordingly to 3.25	Replace "of-the-shelf" e.g. by "non-propietary"	
DE17	3.25	Headline	te	"purpose-built" does not address the type of availability of the tool.	Replace “purpose-built” e.g. by “proprietary”	
DE18	3.28		Ed.	Replace text.	Replace: “performed independently by purely…” by “performed by purely human senses without using a technical tool”	
DE19	4.1	2nd para	Ed	Replace “avoid” by “avoided”		
DE20	4.1	1st para	Ed	Include “.”		
FR11	4.1	2nd paragraph	Te	The designer of a product can chose to alter the functionality of a product to increase the anti-counterfeiting resistance	Replace the last sentence with “Interferences of anti-counterfeiting solutions with product functionalities shall be considered."	
FR12	4.1	Last bullet	Ed		Replace with “how will the control be performed”	
US23	4.1	Paragraph 1	Ed	Missing quantifiers " Simple solution does not mean weak solution"	A simple solution does not mean a weak solution…	
US24	4.1	Paragraph 2	Ge	The paragraph needs to be rewritten for clarity	The technical, logistical, and financial criteria involved in the selection of an authentication solution will depend upon numerous factors including: 1. the characteristics of the elements of authentication 2. the verification levels and methods targeted 3. any required information system 4. security requirements 5. counterfeit resistance 6. the value of the material goods protected 7. counterfeiting risk throughout the material goods life cycle 8. integration and implementation requirements	

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
					Delete last sentence	
US25	4.1	Paragraph 3	Ed	And/or is ambiguous and should be changed to one or the other	These tools will either offer a local on-the-spot response or will call, in real-time, into a secure information system, or possibly rechannel the data, sample, or product towards a structure offering expert analysis for an off-line diagnosis.	
US26	4.1	Paragraph 3	Ed	There is no need for the final comma	The verification processes of authentication elements deployed in these solutions require the ability to read, capture and sometimes perform sampling using human sense or tools	
US27	4.1	Paragraph 4	Ed	Sentence is long, confusing, and hard to read.	Thus, there is a creation chain for authentication elements that begins with the specification of product protection (or trademark, industrial design, or model protection), runs through a verification chain that may combine the human sense, tools, or references, and ends with the way in which a right holder or licensee will use the data to match a product to its manufacturing specifications.	
US28	4.1	Paragraph 4	Te	If human actors are an integral part of performance measurement, how will this document account for human error,i.e., does a standard need to account for human error which is possible whenever humans interpret data.	This should be a discussion point at the PC246 meeting.	
US29	4.1	Paragraph 6 Second point	Ge	Need to clarify statement	Which of my *material goods are being counterfeited or have the potential to be counterfeited?*	
US30	4.1	Paragraph 6 Third point	Ge	Need to clarify statement	In what locations are we experiencing counterfeiting and how are the counterfeits being distributed?	
US31	4.1	Paragraph 6 Fourth point	Ge	Need to clarify statement	What is the manufacturing and supply chain environment?	
US32	4.1	Paragraph 6 Fifth point	Ge	Need to clarify statement	How will the authentication process be performed?	
US33	4.1		Ge	Additional question: Analysis of counterfeiting solution should include risk	Add: “What are the consequences and probability of the counterfeiting threat?”	

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
				considerations		
DE21	4.2		ed	The aim …is: Use plural because more than one aim is mentioned in the document	"The aims …are:"	
DE22	4.2	1st item	te	Change text.	"to establish a top-level classification of different …"	
DE23	4.2	2nd item	ge	Delete. Not in scope of this IS.		
DE24	4.2	3rd item	ed	“examination situations” is rather arbitrary. The performance requirements should refer to well defined “verification scenarios”.	Replace by e.g. “verification scenarios”. This might also deserve a definition in chapter 3.	
DE25	4.2	last sentence	Te	Not every security level may be desired to be defined	Replace by: The user's ability to define specific requirements for every desired level of security for their authentication solution	
FR13	4.2	2nd bullet	Te	Highlight the complementarily of different solutions	Replace with “to establish the overall performance of an authentication solution integrating different authentication elements with complementary authentication related functions”	
US34	4.2	Bullet point 1	Ed	Subject verb agreement	To establish objective descriptions of the function of different types of authentication tools	
US35	4.2	Bullet point 2	Ed	Verb agreement	To establish how different types of authentication solutions integrate with each other and with the material good they are authenticating	
US36	4.2	Bullet point 4	Ed	Remove “thus” to maintain consistency with other bullet points	To assist users and potential users of authentication tools to understand their functionality and selection criteria against their own risk analysis, which will facilitate:	
CH3	4.3		te	Semi-covert measures should be listed.	Add a line for semi-covert measures	
CH4	4.3		ed	Definitions (A) (B) (C) (D) (E) (F) already mentioned in Section 3 Definitions, page 4	Delete the definitions (A) to (F) in 4.3	
DE26	4.3		Ed	Include “.”		
DE27	4.3	table	ge	The structure of section 4.3 does not properly reflect the line of argument; the table is not properly referenced and explained in the text.	Proposed Change: • Add an introductory subsection that explains the purpose of the section, i.e. to provide a classification of authentication solutions along	

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
					the two dimensions of over/covert/forensic and of the properties of the authentication device. • This is followed by the current subsection explaining the overt/covert/forensic classification, suitably edited to remove duplicated definitions etc. • Move the current subsection providing the definitions of the device classes A-F to Chapter 3. • Add a subsection in section 4.3 that refers to these classes and provides further explanations and potentially examples. Also state that a particular solution can provide variants that fulfil several of these properties (e.g., operates both in a standalone and an on-line mode).Explain the constraints resulting from the description of overt features, which is reflected in the corresponding row of the column. • Update the table to clearly distinguish legend and classifications, and properly reference it in the text. • Consider providing suitable examples for authentication solutions for some of the classes defined by the table, to facilitate understanding of this central section of the standard.	
DE28	4.3	table	ge	The categories, though generic, might be insufficient. E.g. what about a track & trace solution based on 2d barcodes. Are these “covert” or “overt” ? The term “covert” implies “not accessible by human senses”	The workgroup should create a more precise (even if less generic and more pragmatic) set of categories.	
FR15	4.3	1 to 3	Te	Consistency of terminology	Replace “authenticator” with “authentication element”	
FR16	4.3	1	Te	Remove reference to front line and second line of defense because not used in the document.	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	

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
					retail, wholesale or other environments) where a visual check is the only one immediately possible and where this can be undertaken by people without training or equipment, such as consumers, store clerks and check-out staff.	
FR17	4.3	1	Te	Remove reference to front line and second line of defense because not used in the document. Remove “equipped” because if an equipment is needed, according to the definition, it is a covert feature.	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.	
FR18	4.3	2	Te	Remove reference to front line and second line of defense because not used in the document. Covert technology may be used stand-alone and is not necessarily related to other types of authentication elements.	Remove: “ and therefore covert authenticators are primarily intended for second line examination; that is, examination by a person with some training who is examining an item thought to be suspect. This suspicion may be a result of first-line examination or investigative intelligence. ”	
FR19	4.3	2, 2nd paragraph	Te	All the covert tools can be examined.	Remove “most”.	
FR20	4.3	2, 3rd paragraph	Te	Ensure more neutrality regarding technologies.	Covert technologies exploit all kinds of physical or chemical effects, as well as logical relationships. For example although in product authentication mostly physical effects are used, involving may include 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 fibers in or on the packaging and requiring illumination by a special light source. As an example, logical relationship can be a covert authentication element bearing an encrypted information related to any aspect of the material good itself.	
FR21	4.3	2, 4th	Te	This paragraph describes forensic solutions.	Remove this paragraph	

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
		paragraph				
FR22	4.3	2, 5th paragraph	Te	Not needed and related to a specific technology.	Remove “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. “	
FR23	4.3	2, 7th paragraph	Te	Not needed. It is not necessary to create a new category, which is contained in the “covert” type.	Remove “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?) “	
FR24	4.3	2, Last paragraph	Te	This paragraph uses terms that are not used and defined in this standard.	Replace this last paragraph with: “In opposite to the overt authentication elements which require only human interpretation, covert authentication elements require tools for being interpreted. Those tools can be stand-alone or connected to a network, can be off-the-shelf or purpose-built and the result can be either automatic or can call for human interpretation.”	
FR25	4.3	3	Te	This sentence implies ranking the solutions.	Remove “is the ultimate authentication level. Generally, it”	
FR26	4.3	3	Te	Remove reference to front line and second line of defense because not used in the document.	Remove: “Forensic features are not widely used in first-line or second-line authentication.”	
US37	4.3	Paragraph 1	Ed	First sentence is missing a period	……implementation of solutions. It is not …..	
US38	4.3	Chart	Ge	The chart does not appear to be filled out completely.	What is the purpose of the chart? 1) explanatory chart? Then fill in all the squares 2) participatory chart? Then maybe move it to the appendix and explain its use and how to complete.	
US39	4.3.1, 4.3.2, 4.3.3		Ge	It might be useful to include in these sections on the types of anti-counterfeiting solutions more in depth comments on the vulnerabilities for each type.	Add: Any one countermeasure is not foolproof and there are strengths and vulnerabilities to every solution. Countermeasures should consider all	

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
					aspects of the victim and criminal opportunities. Therefore any security program should include a layered approach (need to include definition of layered approach).	
US40	4.3.1, 4.3.2, 4.3.3		Ed	There is no spacing between paragraphs.	Counterfeiters will always try to reproduce all visible feature of the item and its packaging in their efforts to produce a realistic copy, which is why overt authenticators must be difficult to copy so their absence or imperfections will alert examiners to the fact that the item may not be genuine.	
US41	4.3.1, 4.3.2, 4.3.3		Te	From a Customs Authority perspective, the delineation of 1st line and 2nd line inspection seems to imply that the 2nd line of inspection will happen after the 1st line of inspection. However, when considering goods involved in international shipments, it is more likely that a trained customs officer (who would fall within the 2nd line of inspection) will be the first person to inspect the item rather than a 1st line inspector, such as a retail clerk or consumer. Is there a way to clarify that secondary inspectors may actually inspect a good first or that secondary inspectors may skip the first line of authentication	Overt authenticators may also be examined at the second line, by trained and equipped inspectors, to establish whether or not the authentication element is genuine. The use of the terms first line, and second line authenticators may be confused with first line and second line inspectors. Need to remove the reference to those terms. Suggested language changes: 4.3.1, fourth paragraph, first sentence: Overt authenticators may also be examined ~~at the second line, that is~~ by trained and equipped inspectors, to establish whether they are ~~themselves~~ genuine. Suggested language changes:4.3.2, last sentence,: People using these technologies may need some training and therefore covert authenticators are primarily intended for trained inspectors.~~second line examination; that is, examination by a person with some training who is examining an item thought to be suspect. This suspicion may be a result of first-line~~	

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
					~~examination or investigative intelligence.~~ Add the following language after 4.3.3: Untrained inspectors may only be knowledgeable enough to examine and provide a determination of authenticity based upon overt authentication. While trained inspectors may provide a determination of authenticity based upon the inspection of overt, covert and forensic level authenticators. The ability of an inspector to examine and make a viable determination is based upon the level of training, the knowledge available, access to tools (both simple and complex), and access to established exemplars.	
CA2	4.3.2		Te	There are many techniques used in the covert technologies field and they may not all require a reader. We need to be more general and allow for other techniques to be included.		
CH5	4.3.2		ed	Semi-covert features should be described in a separate paragraph.	Add a separate paragraph for semi-covert features. Proposed definition: “Semi-covert authentication features are not immediately obvious but can be detected without the use of special detection tools.”	
DE29	4.3.2		te	Especially in covert applications the principles of data protection have to be fulfilled.	Include sentence: "Where a covert application uses data that is or can be linked to a person, privacy principles and regulations shall be obeyed.	
DE30	4.3.2		Te	The description of possible covert techniques seems to be too narrow. To assure the intended general scope we should include also description of electronically based authenticators.	Covert technologies exploit all kinds of physical, electronical or chemical effects. Physical effects involve 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 fibers in or on the packaging and requiring illumination by a special	

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
					light source. Electronically supported authenticators use SW or/and HW based data and/or protocols securely connected to the authentic product for proof of genuineness. Used chemical compositions range 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.	
US42	4.3.2	First paragraph. Second sentence	Te	Covert technologies do not always require special readers or detectors. Need new language.	Proposed language: They can be read with a variety of means including; simple inspection tools, specialized knowledge, inspection techniques, specialized tools and proprietary readers to verify their presence and validity.	
US43	4.3.2	Paragraph 1	Ed	There seems to be a hard-return in the middle of the paragraph that separates a sentence onto two different lines.		
US44	4.3.2	Paragraph 2 First Sentence	Te	The statement is questionable in regards to: …although in product authentication mostly physical effects are used, involving radiated energy originating form one or the other part of the electromagnetic spectrum. There are a significant number of technologies used in covert product authentication that do not use the electromagnetic spectrum.	Suggested language:…..although in product authentication mostly physical effects are used, some of those technologies may involve radiated energy originating from the electromagnetic spectrum.	
US45	4.3.2	Paragraph 2	Ed	Incomplete sentence	Ultraviolet (UV) and Infrared (IR) radiations are the most commonly used, but the use of coatings, inks or fibres in or on the package that require illumination by a special light source are also common.	
US46	4.3.2	Paragraph 2	Ed	Use “that” instead of “which” because which implies a separate clause	“Chemical compositions are also used, ranging from those that react with a pen-type detector to show a visible mark, to complex organic molecules that are coded to the specific product and require a proprietary detector to check for their presence and the correct coding.	

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
US47	4.3.2	Paragraph 3	Te	The statement is ambiguous and highly questionable	Remove the sentence: The security level will essentially depend on the sophistication…….radiated energy	
US48	4.3.2	Paragraph 3	Ed	Semi-covert technologies include features like thermo chromic elements and familiar techniques such as microtext. (Duplicates?)	Semi-covert technologies include features like thermo chromic elements and familiar techniques such as microtext. ~~(Duplicates?)~~	
US49	4.3.2	Last two paragraphs	Ge	Need to break out last two paragraphs as separate subjects.	4.3.2.1 **Semi-covert** The term semi-covert authenticator……. 4.3.3 **Human sense and digital authenticators** Overt and covert authenticators…….	
US50	4.3.2	Last two paragraphs	Ge	Is “digital authenticator” the proper term for electronic verification?	Add definition for digital authenticator "Method for retrieving data from a system using an electronic interrogator"	
US51	4.3.2	Paragraph 5	Ed	Run-on sentence	Overt and covert authenticators can be further delineated into two categories: sensory authenticators and digital authenticators. Sensory authenticators are authenticators that are examined by human sense and may or may not require a specialized tool. Digital authenticators use a secure trail that requires the use of a telecommunications or computer system.	
DE31	4.3.3		ge	The document should comment on “court proof” verification independent of the nature of the applied feature.		
US52	4.3.3		Te	The description is incorrect, change to:	Forensic authentication involves the use of special tools or knowledge to validate the authentication elements. The authentication elements used are not commonly known and are revealed only to those with a legitimate “need to know”. While forensic elements may be used in the field for authentication it is more commonly used in a laboratory setting with the use of common and specialized tools for examination. The validation process may often use original exemplars for a comparative analysis. Typically forensic elements are not used in first or	

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
					second level authentication processes.	
FR27	4.4		Ed	Clarification	Replace “authentication solution” with “authentication process”	
FR28	4.4		Te	Figure	Correct the “input for” arrow	
FR29	4.4		Te		Replace “that reveals the interrelationship between the material good to be authenticated and typical components of the authentication solution. They together yield a true or false verdict or provide information that will enable to evaluate the health, safety or other form of risk posed by the possibility of fraud.” With “This figure shows how intrinsic authentication elements, i.e. features of the product itself, as well as authentication elements which are part of the authentication solution, are used iteratively to determine whether material good is genuine, suspect or fake.”	
KR1	4.4		te	It would be useful to develop a more detailed diagram for the convenience of the readers and the end-users of this standard to grasp the whole detailed pictures of the process all at once. For example, by adding ‘physical characteristics, attack resistance, integration process, field/environmental function and implementation process’ for the block of “Authentication element(s) selection.” The diagram should cover the whole page rather than just a half of the page to describe most of all the categorized items and elements for the authentication.		
US53	4.4	Parag. 1	Ed	Last sentence does not have subject-verb agreement	They together yield a true or false verdict or provide information that will enable evaluation of the health, safety or other risk posed by the possibility of fraud.	
US54	4.4	Figure	Te	Does not include risk analysis in the authentication solution selection process	Add “Risk Analysis” box to the figure as input to “Authentication Elements Selection”	
US55	4.4	Figure	Ed	Spelling, hanging phrases “Input for …”	“Counterfeiting”	

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
US56	4.4	Figure	Ge	Term is undefined to meaning in this context	Need to define “integrated/Associated Authentication Elements”	
US57	4.4	Figure	Ge	Term is undefined to meaning in this context	Need to define “Intrinsic Authentication Elements”	
DE32	5.1			Move two main classes of solutions to 4.3		
FR30	5.1		Te		The global performance of an authentication solution depends on the performance of its least performant component and on the performance of the links between them.	
FR31	5.1		Ed		Tools performance, in particular their attack resistance, should be taken into consideration with the same importance as authentication element performance.	
US58	5.1	Title	Te	5 Performance criteria specification based on risk analysis	Add to intro of 5: Risk is a function of probability and severity factors. Risk analysis is the cycle of hazard identification, risk assessment, risk management and risk communication. This section defines the performance criteria, specification factors that are used by risk analysis systems, specifically as outlined in ISO 31000.	
US59	5.1	Introduction	Te	5 Performance criteria specification based on risk analysis	When developing the criteria specifications it is important that the criteria is clearly delineated between the criteria for the authentication element and the authentication device. Often times the authentication element is subject to conditions that the authentication device will not be subject to. As an example; an authentication element for aircraft parts are subject to extreme environmental factors that the authentication device will never be expected to withstand.	
CH6	5.2	Last	ed	Not correct / Confusing	Section 5.3 will describe the criteria for the	

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
		sentence		Section 5.2 will describe the criteria for the authentication elements: section 5.3 will describe the criteria for the authentication device.	authentication elements. Sections 5.4 and 5.5 will describe the criteria for the authentication device.	
DE33	5.2	last paragraph	Ed	References of 5.2. and 5.3 do not refer to the actual document structure	Adjust appropriately	
FR32	5.2	2nd paragraph	Ed		Replace (overt, covert, forensic) With (overt, covert and forensic)	
FR33	5.2	Last paragraph	Ed		Replace Section 5.2 will describe the criteria for the authentication element; section 5.3 will describe the criteria for the authentication device With Section 5.3 will describe the criteria for the authentication element; section 5.4 will describe the criteria for the authentication device And add Section 5.5 will describe the criteria for authentication solution.	
US60	5.3.1.1	Static Characteristics	Ge	Size and thickness need to be separate elements	Size Thickness	
DE34	5.3.1.2	last paragraph	Ed	Include “.”		
FR34	5.3.1.2		Te	Liquidity	To clarify. Is it linked to viscosity, miscibility or fluidity?	
FR35	5.3.1.2		Te	The thixotropy could be a solution for authentication	Add the thixotropy	
US61	5.3.1.2	1st sentence	Te	Use should instead of shall and use modified instead of	The authentication element’s physical characteristics should not be modified by product manufacturing, or	

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
				affected.	during the storage, transportation, and integration processes.	
US62	5.3.1.2	2nd sentence	Te	What are the process requirements? Are these different than the integration process? The way the second sentence is worded now it makes it sound as though any of the process listed in the preceding sentence (manufacturing, storage, transport, integration) that alter or damage the authentication element will cause the product to be rejected. However, if the purpose of this document is to provide guidance, then this sentence should be restructured to state that process requirements should not alter or damage the authentication elements.	If process requirements alter or damage the authentication elements, they will become unusable and cause the product to be rejected during final production control. Therefore, the authentication element should be chosen to take into consideration any of the process requirements involved in the production of the product.	
DE35	5.3.1.3			Classification is not comprehensible.	Change accordingly: - mild environmental conditions (climatic features such as temperature and humidity) - harsh environmental conditions (degradation features such as chemical action and irradiation) - mechanical use typical of the product under consideration shall not affect the element`s physical characteristics during manufacturing, storage, transport, and operation in order to avoid - any kind of aging that might result in a malfunction of the authentication element over life-cycle.	
US63	5.3.1.3	Sentence 1	Ed	Ambiguous – physical characteristics of what?; use must instead of shall; use effect instead of affect.	Resistance to environment conditions during processing, storage, or in operation must not effect the physical characteristics of the authentication element.	
US64	5.3.1.3	Sentence 2	Ed	Modify existing sentence	The specifier of the authentication solution should define the conditions of usage that must be considered based upon the required risk analysis.	
DE36	5.3.1.4	title		Correct: heath	Health	

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
DE37	5.3.1.4	list	ed	"Radio waves", "radiation"	Replace by "electromagnetic radiation" and "radioactivity", (if that is the meaning)	
DE38	5.3.1.4	last paragraph	Ed	Include "."		
FR36	5.3.1.4		Te	Chemical composition	Add "And banning of some substances"	
US65	5.3.1.4	Title	Ed	Misspelling	Change" Heath" to "Health"	
US66	5.3.1.4		Ed	No period. The sentence would read better if the action portion of the sentence comes first.	The potential environmental and health impact of authentication elements must be considered, particularly in light of national, regional, and international regulations.	
FR37	5.3.1.5		Te	There are some differences regarding uniqueness intrinsic or extrinsic. Express the major difference between intrinsic and extrinsic: Intrinsic with registering, Extrinsic possible without registering for stand alone examination.	Split uniqueness into 2 possibilities: - Uniqueness intrinsic - Uniqueness extrinsic	
US67	5.3.2.1		Ge	Criteria should be practical and re-evaluated after a period of time as there are anti-counterfeiting solutions that may not be 100% copy resistant (but not easily enough) or may be easily copied after a period of time (as technologies advance and costs lower).	Suggested statement: Add a paragraph to 5.1 The performance of any authentication technology can be affected by changes in technology. These changes may make the solution obsolete or make the reproduction of the authentication technology readily available to the counterfeiter. As part of any criteria evaluation a periodic review shall be conducted to insure the implemented technology has not become obsolete or compromised by other publicly available technologies.	
US68	5.3.2.1	Third	Te	The use of the word "must" is incorrect and should be replaced by "should". If it must not be possible to create a fake that could be interpreted as genuine then there are no	To avoid simulation and emulation it ~~must~~ should not be possible to create some fake authentication element that could be interpreted as genuine by an	

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
				items that would meet this requirement.	inspector or by a device.	
DE39	5.3.2.2		Ed	The first sentence of this section is a definition and shall be moved to the respective section, if needed.	Change accordingly	
DE40	5.3.2.2		Te	Unsuccessful attacks may not affect the interdependence.	Change phrase to: interdependence must be affected by any (at least partly) successful attack undergone	
FR38	5.3.2.2	1st sentence	Te	Need to draw the attention of the customer to the function of tamper evidence.	Re write the sentence The tampering resistance is the ability of the authentication element: - to resist the removal, alteration or substitution of the element from the material good or the physical access to it, - to give evidence that access to the good has been performed or infringed.	
US69	5.3.2.2	Title	Ed	Inconsistent verb usage	5.3.2.2 Tamper resistant/Tamper evidence	
US70	5.3.2.2	1st sent	Ed	Cumbersome	A tamper resistant authentication element must be able to resist removal, alteration, or substitution as an element of the material good.	
US71	5.3.2.2	Sentences 2-5	Ed	These should be 1 paragraph. Missing punctuation. The sentences are also cumbersome and unclear.	It is crucial to develop a tangible or intangible form of interdependence between the authentication element and the material good it protects. An authentication element displays tangible interdependence if it is destroyed or displays some form of visible or recognizable alteration when an attempt is made to remove the authentication element from the material good. Intangible interdependence occurs where the authentication element has a logical association with a material good or a reference that cannot be erased or duplicated.	
US72	5.3.2.2	Fourth paragraph	Ge	Definition of “Intangible interdependence” needs clarification.	Redefine	

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
US73	5.3.2.2	Paragraph 5, 6, and 7	ed	This paragraph uses different terms for the same concept resulting in ambiguity. Furthermore, it is not clear what the parenthetical comment is referring to. Combine paragraph 5, 6, 7 to the following propsed language.	To generate tamper evidence the various forms of interdependence must be affected by any attack, which is why an attack must immediately and irreversibly change one or more characteristics of the association between the authentication element and the material good. Furthermore, any changes to these characteristics resulting from an attempted attack must be detectable during the verification protocol. To reduce the chance of a false positive, the interdependent characteristics must remain stable and resist changes in environmental conditions during the product's life cycle.	
US74	5.3.2.3	Title	Ge	Hacking resistance	Compromise resistance	
US75	5.3.2.3		Te	The last word "authenticator" is somewhat ambiguous.	It should be defined or replaced with the word "inspector" if appropriate.	
US76	5.3.2.3	2nd sentence	Ed	There should be a comma	In the event the element is hacked, detection….	
US77	5.3.2.3	2nd sentence	Ge	In the event the element is hacked detection….	In the event the element is circumvented, detection….	
FR39	5.3.2.4		Ed	Behavior is American English.	Replace with behaviour	
US78	5.3.2.4		Ed	Incorrect punctuation. Cumbersome wording	It must not be possible to capture any secret data or determine characteristics of the authentication element through analysis of its physical behaviour in any environmental circumstances.	
US79	5.3.2.5		Ed	Confusing wording. Ambiguous. Improper punctuation.	It should not be possible to intercept or listen to the communications between the authentication element and any tool required to read or verify the element. Thus, the authentication element either should not share any information with the tool or the information should be secured.	
FR40	5.3.2.6		Te	Add a reference to the composition	Add and the availability of the technology, related raw material and support in the future.	

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
CH11	5.3.3		ge	Legal suitability and enforcement aspects are not mentioned.	Add a new paragraph for legal suitability and enforcement of anti-counterfeiting by force of law. Will it be part of the ISO TC 247?	
CH12	5.3.3			Privacy aspect to be mentioned (for example: RFID in the medical industry)		
CH7	5.3.3		te	Logistical aspects are not mentioned.	Add a new paragraph for impact of measures to logistics	
FR41	5.3.3.1		Ed		Replace maintained with implemented.	
FR42	5.3.3.1		Te	Add a reference to traceability	Complete the sentence with traceability shall be insured including after repackaging.	
FR43	5.3.3.2.1		Te	Clarify "application element"	Rewrite the sentence A determination must be made to insure that the integrator can meet the production and supply requirements for the authentication element and the proceeding of its integration to the material good.	
US80	5.3.3.2.1		Ge	There is no prior reference to “application element.” This should be defined either in this section or a previous section. There is also no definition of integrator. It may not be necessary to provide a definition, but it would help with clarity to define who the integrator is.	This should be discussed at the next PC 246 meeting	
FR44	5.3.3.2.2		Ed		It must also be compatible with the process used to create the packaging or material good.	
FR45	5.3.3.2.3		Te	Complete the sentence	Any attempt to hack or tamper these machines shall be reported and if any appropriate investigation shall be decided.	
US81	5.3.3.2.3		Te	Reported to whom?	Add: Any attempt to hack or tamper these machines must be reported "to appropriate authorities"	

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
FR46	5.3.3.3		Ed		Independent audits should be conducted to prove to the responsible parties that all the integration requirements are being met and can be verified.	
FR47	5.3.3.4		Ed		Training will be required in all phases of the integration process to meet strictly the requirements of both the authentication solution provider and specifier.	
CH8	5.4		ge	The section 5.4 should be part of 5.5 because the attack resistance is one of the criteria. The numbering of the sections could be modified accordingly.	Proposal : 5.4 Criteria for the selection of authentication devices 5.4.1 Field environmental function 5.4.2 Attack resistance 5.4.3 Implementation process	
DE43	5.4	title		It is not apparent to the reader why this section does not cover environmental conditions etc. for the operation of the authentication device.	Add an introductory paragraph pointing the reader ahead to section 5.5.: “Note: Environmental and other conditions for the operation of the authentication device are covered in Section 5.5.”	
US82	5.4	Whole section	Ge	tool	Change 'tool' to 'device'	
FR49	5.4.1	Title	Te	Is "copy" appropriated for the title?		
FR50	5.4.1	1st paragraph	Te	The access to sensitive information should not be possible.	Rewrite the 1st paragraph with: The authentication device must be resistant to reverse engineering in order to recover secret or sensitive information that could lead to create/generate/manufacture an authentication element.	
FR51	5.4.1	2nd paragraph	Ed		Replace interpreted with considered.	
FR52	5.4.1		Te	Add a recommendation	Add a sentence: It can be achieved by using a calibration authentication element in order to determine if the	

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
					authentication tool is genuine and operational.	
FR53	5.4.2		Ed	Sentence is too long.	The tools must be protected and / or react to any logical attempt of deviation aimed to capture information that are processed or transferred. Particularly it should be impossible to use this information to query data bases with unauthorized tools.	
US83	5.4.2, 5.4.3		Ed	In section 5.3 on the criteria for authentication elements, the attack resistance criteria are set forth in the following order: copy resistance, tamper resistance, hacking resistance, side channel resistance, interception of communication, obsolescence. For consistency, section 5.4 should be arranged in the same manner.	section 5.4.2 should be switched with section 5.4.3.	
FR54	5.4.3		Ed		The tools must be protected and / or react to any physical attempt of deviation aimed to capture information that is processed or transferred.	
FR55	5.4.3		Te	Complete with a reporting	Any attempt to tamper these tools shall be reported and if any appropriate investigation shall be decided.	
FR56	5.4.4		Ed	Behavior is American English	Replace behavior with behaviour	
US84	5.4.4		Ed	Cumbersome wording. This section is supposed to be presenting criteria for the tool/device, but this section only refers to the element.	It must not be possible to capture any secret data or determine characteristics of the authentication device through analysis of it physical behaviour or interaction with the authentication element in any environmental circumstances.	
US85	5.4.5		Ed	The use of both “device” and “tool” in the first sentence may imply that there is a difference between a device and a tool. However, the rest of the document does not seem to make that kind of distinction. Punctuation error.	The authentication device should be protected against any unauthorized communication between the authentication element and the device and between the device and the remote components of the authentication solution. Safeguarding against the interception of communications must be considered during the authentication process and during any kind of communication needed to upload	

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
					or download information, provide updates or alarms.	
DE41	5.4.5.		Te	Not understood	Clarify	
FR57	5.4.6		Te	Complete with a reporting	Complete the sentence: "and if any appropriate investigation shall be decided."	
US86	5.4.6		Ed	Wordy and cumbersome.	If a reference database is used for authentication it must be protected against any intrusion. Any attempt or successful intrusion must be reported to appropriate authority.	
FR58	5.4.7		Te	Sentence is not enough clear.	Add at the end of the sentence: "or both inspector and tool".	
CA3	5.4.7		Ed	Database not “Data base”		
US87	5.4.7	Heading	Ed		Replace “Data base” with “Database” for consistency with remainder of the document.	
DE42	5.4.8		Te	Replace “Back end” by “Back up”		
FR59	5.4.8		Ed	Clarify the sentence	Add after back end system between brackets: (data and redundancy service)	
US88	5.4.8	Second	Te	Back end is not the appropriate word choice	Change "Back end" to "back up"	
US89	5.4.8		Ed	Not full sentences	Although security measures may be implemented, redundant databases should be considered to prevent a successful attack attempt. Furthermore, a back up system should also be considered to avoid interruption of service.	
FR60	5.4.9		Ed		Guaranteed	
FR61	5.4.9		Te	Clarify the meaning of the sentence.	This concerns either the authentication elements related information stored in databases or any equipment used to make the authentication solution work	
FR62	5.4.10		Ed	ISO 31000 has been published in November 09	Replace ISO/FDIS 31000 Risk Management with:	

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
					ISO 31000 Risk management -- Principles and guidelines	
US90	5.4.10	First	Ed	The document should use English spelling and not US.	Replace “recognized” with “recognised”.	
CH9	5.5	Title	ed	Title is confusing with 5.3 : Criteria for the selection of Authentication elements and devices	Proposal : Criteria for the selection of Authentication devices	
DE44	5.5	title		The title of this section does not properly convey its actual content.	Change the title to “Criteria for the Selection of the Authentication Solution”. This is also consistent with the titles of sections 5.3 (covering the authentication element) and 5.4 (covering the authentication device).	
US91	5.5		Te	New paragraph needs to be added to discuss Life Cycle criteria.	Suggested language: Life Cycle Criteria: In the selection of an authentication solution it is imperative that an evaluation is conducted to determine the life cycle requirements of the solution in relation to the product being protected. Multiple considerations need to be made to review the environmental factors affecting both the product and the solution. In addition an evaluation must be made to determine the life cycle capability of any authentication device used in the control process. Such considerations may include potential obsolescence of the device, technological obsolescence of the solution, company and support systems failures, and redundant authentication elements. With material goods of a short life cycle this evaluation may have minimal forecast requirements. Conversely material goods with a significant longevity and critical performance requirements this process may require extensive evaluation and unique solutions and partnerships.	
FR63	5.5.1.1		Te	Some environmental conditions could impact on the use and are not yet listed.	Add vibration, pressure, electromagnetic fields exposure	

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
US92	5.5.1.1	1st bullet	Ed	Remove periods and make dust singular	Temperature, humidity, moisture, dust	
FR64	5.5.1.2		Te	Some exposure conditions could impact on the use and are not yet listed.	Add Explosive atmosphere	
US93	5.5.1.3	Header	Ed	“aggression” is an odd word choice here and may not be the intended meaning	5.5.1.3 Factors causing deterioration during normal usage	
FR65	5.5.1.4		Ed		Complete the sentence: "in particular when intended to be used by untrained inspectors (consumers)."	
FR66	5.5.1.4	2nd sentence	Ed		Rewrite the beginning of the sentence: A tool using human senses may be adapted to authentication conditions to avoid…	
US94	5.5.1.4		Te	The last word “authenticator” is somewhat ambiguous.	Replace with “inspector”.	
US95	5.5.1.4		Te	How is it possible to adapt human senses? Perhaps this should be reworded to indicate that the process can be adapted when human senses are involved or that a device can be adapted. These criteria do not seem to fit under the concept of ergonomics – this section may be better titled “Process adaptability”	Suggested rewording: It may be beneficial to allow for a small amount of flexibility in authentication procedures to allow for adaptation of human sense or the device to the particular authentication conditions to avoid misinterpretation.	
FR67	5.5.1.4.1		Te	Clarification	Lighting conditions should not impact the reading of the authentication elements or the reading of the result if the control is done with the usage of a tool. When a tool is used, alternative solutions to reading may be used such as sound	
FR68	5.5.1.4.2		Te	Clarification	Weather or humidity conditions should not impact the reading of the authentication elements or the reading of the result if the control is done with the usage of a tool. Wiping of the authentication element with simple means before reading is acceptable	
FR69	5.5.1.4.3		Te	Clarification	If the control has to be operated under severe temperature conditions, ergonomic of the tool may be adapted to inspectors personal equipment and clothing	

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
DE45	5.5.1.5	Chapter	ge	Item “readability” is missing: do the verifier need physical / visual contact to the product item, is bulk reading possible, are there collisions when several authentication elements are present ?	Add a clause “Readability”.	
FR72	5.5.1.5		Te	Add a section related to environmental conditions (ref to 5.5.1.1).	Environmental conditions required for operating the control should be defined.	
US96	5.5.1.5		Te	It seems that section 5.5.1.5 and 5.5.1.4 could be combined because they both talk about the conditions in which an authentication is made.	**5.5.1.4 Examination conditions** The authentication process should be as intuitive as possible, in particular for untrained authenticators (consumers). *Human senses may be enhanced or a device may be adapted to accommodate authentication under all specified conditions.* ~~*that will avoid misinterpretation due to difficulties while authenticating.*~~ **5.5.1.4.1 Lighting conditions impacting the reading of an authentication element or the operating controls of the device** Under what lighting conditions will the authentication element and device be expected to function within the specification of performance. **5.5.1.4.2 Rain/Humidity/Snow** Under what humidity/moisture conditions will the authentication element and device be expected to function within the specification of performance **5.5.1.4.3** ~~**Extreme**~~ **Temperatures** ~~**requiring the device to operate in such specific conditions and the authenticators to be able to use the device (gloves...)**~~ Under what temperature conditions will the authentication element and device be expected to function within the specification of performance. **5.5.1.4.4 Wind**	

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
					Under what wind conditions will the authentication element and device be intended to function within the specification of performance. ~~**5.5.1.5 Examination condition**~~ ~~**5.5.1.5.1 Lighting**~~ **5.5.1.5~~.2~~ Life cycle** The authentication solution shall be able to provide authentication in all life cycle steps as defined by the specifier.	
FR70	5.5.1.5.1		Te	Clarification	Lighting conditions required for operating the control should be defined	
FR71	5.5.1.5.2		Ed		Replace the sentence with: The authentication solution shall be able to provide authentication in the life cycle steps requested by the specifier.	
FR73	5.5.1.6.1		Ed	Clarify the sentence	The necessary time to perform an authentication shall be stated.	
FR74	5.5.1.6.2		Te	Need to clarify differences between endurance and frequency	Suppress endurance in 5.5.1.6.2 title and replace the sentence with: The number of successive accurate authentications per unit of time, by the solution shall be stated. Add a new section for concurrent authentication: The number of concurrent authentication which can be processed simultaneously without impacting unitary performance shall be stated (this criteria is relevant only for on-line solutions).	
FR75	5.5.2		Ed	Add a clarification	The following performance criteria	

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
FR76	5.5.2.1.1		Ed	Add a clarification	Replace "devices involved" with "components of the solution"	
FR77	5.5.2.1.2		Te		The security of the supply processes of the components and data critical to the performance of the authentication solution shall be stated.	
US97	5.5.2.1.2		ED	Process should be plural	Security of all supply processes that will be used ….	
FR78	5.5.2.2.1		Te	Clarification	The solution shall comply to relevant regulations where it is used.	
US98	5.5.2.2.1		TE	Additional Language	Compliance with Regulations: The authentication solution must be compliant with all existing regulations by governmental or regulatory agencies. Special consideration needs to be made if the solution is to be implemented in international markets or used in international trade where regulations may vary by country or region. Solutions used by governmental agencies may also be subject to specific regulations, procedures or requirements.	
FR79	5.5.2.2.2		Te	Clarification	An audit procedure shall be defined and implemented for each entity, which is involved in the solution and which impacts either the performance or the security of the solution. This may concern the authentication elements, the tools and the information system (database and interfaces).	
US99	5.5.2.2.2		TE	Additional Language	Compliance audits to assure security practices and quality practices: Compliance audits for security assurance and quality should be a criterion in the selection of an authentication solution. These audits should be performed with recognized standards by organizations that are accredited by national and international bodies to perform such audits.	
FR80	5.5.2.3.1		Te	Title does not refer to the sentence	Proposed title: Start-up time	

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
					And replace set up and wake up with Set-up, wake-up	
US100	5.5.2.3.1	Title	ED	"Availability" may not be the best term for the described criteria.	Suggested titles: Mean Start Time or Device Set Up	
US101	5.5.2.3.1		ED	Suggested change in language to focus on device authentication.	The authentication *device* set up time (cold start or wake up) should be as short as possible in most applications.	
FR81	5.5.2.3.3		Te	Control actions are mandatory	Replace may with shall Control actions shall be implemented to verify the correct production both in term of quality and quantity of authentication elements and devices according to the protocols defined.	
FR82	5.5.2.3.4		Ed		Different authentication elements may be controlled without risk of interference between the control applications.	
US102	5.5.2.3.4	1st sentence	Ed	Not a complete sentence	It may be advisable to create a single tool capable of performing multiple operations or functions related to authentication.	
DE46	5.5.2.3.5	Paragr.	te	False acceptance (rate), false rejection (rate) should be defined in chapter 3	Quote appropriate definition of existent IS.	
DE47	5.5.2.3.5	2nd sentence	te	Assuming the rates are measurable and known, they will in general not be constant as a function of environmental parameters.	The specifier can specify the rates for e.g. "standard" conditions and advise the user what is likely to happen at different conditions.	
DE48	5.5.2.3.5	Paragr.	te	What are FA / FR rates for human detected authentication elements ?		
FR83	5.5.2.3.5		Te	Stability should be defined	Replace the 2nd sentence with This rate shall stay within the limits of the variation of the environmental operational conditions defined by the manufacturer.	
FR84	5.5.2.3.6		Ed		Replace degraded	

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
					with limited for performance with fallback for modes of operations	
FR85	5.5.2.3.6		Ed	MTBF: to be defined	The reliability of the components of the authentication solution should be considered to obtain the best quality of service: MTBF (Mean time between failures), calibration, and preventive maintenance issues.	
US103	5.5.2.3.6	1st sentence	Ed	And/or increases ambiguity	For tools with their own power source or tools that operate in an online mode, …..	
US104	5.5.2.3.6	2nd sentence	Ed	Poor word choice and incorrect punctuation.	This determination should consider whether there are different levels of degraded modes of operation (low battery, missing network, etc.) or an alternative protocol that may access another type of authentication element or separate backup solution.	
US105	5.5.2.3.6	Last sentence	Ed	This is not a complete sentence. It may be best to combine it with the previous sentence. Also, MTBF should be written out to clarify what this means.	The reliability, MTBF (Mean Time Between Failures), calibration, and preventive maintenance issues of the components of the authentication solution should be considered to obtain the best quality of service.	
FR86	5.5.2.3.7		Ed	Title is nor appropriated	Replace infrastructure with tool supply environment	
FR87	5.5.2.3.7		Ed	Need more explanations before the 3 bullets	The performance of tool supply environment and maintenance shall be considered, particularly in terms of:	
FR88	5.5.2.3.8		Ed		Replace the beginning of the sentence with: The reliability of the authentication result is in general impacted by the expertise of the inspector: the better trained they are, the more reliable the authentication result is.	
FR89	5.5.2.3.9		Ed		Stop the sentence just after considered.	
CH10	6		te	Authentication features are used for authenticating products but cannot prevent counterfeiting. Thus the effectiveness of	Change title to “Effectiveness Assessment”. The assessment to be performed using the criteria in	

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
				a measure cannot be measured by the amount of counterfeiting. The effectiveness of an authentication measures can be assessed but not measured.	paragraph 5.3.	
DE49	6	intro	Ed	“Effectiveness measurement” used in wrong terms	Change appropriately	
DE50	6	chapter	ge	The measurement of effectiveness is extremly difficult, if at all possible. Changes in sales numbers are subject to many parameters which change with time and region etc. For small production volumes statistics are insufficient.	What in some cases might be feasible is a “utilization rate” of an authentication system: how often has it been evaluated, how often did it spot a counterfeit ?	
FR90	6	1. the material good is already on the market	Te	Clarification	If the amount of counterfeiting is known, then an effectiveness measurement can be established based upon a reduction in the amount of known counterfeits provided the reduction in the amount of counterfeit can be effectively traced to the authentication solution.	
FR91	6	2nd paragraph	Ed		Suppress – before "this material goods…"	
FR92	6	2nd paragraph	Ed		Delete the comma after safety	
US106	6	Paragraph 1	Ge	Add sentence to end of paragraph	Add sentence: It is not intended to be all inclusive or provide measurement metrics for the diverse multitude of possible authentication solutions.	
US107	6	Paragraph 2	TE	A measurement strategy has to be defined in relation with the compliance specifications that are implemented by the specifier and with the consideration of the counterfeiting status of the material good. A material good may have a counterfeit status based upon the following categories.	A measurement strategy should be defined in relation with the compliance specifications that are implemented by the specifier and with the consideration of the counterfeiting status of the material good. A material good has a counterfeit status based upon the following categories.	
US108	6	Point 2	Ed	Punctuation errors. Also remove the bullet point from the beginning of the sentence that introduces the bullet points.	This material goods status can be the result of multiple factors: • A material good that is very difficult to counterfeit, • There is little or no value in counterfeiting the good,	

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
					• An effective solution is already in place, or • Adequate research or reporting has not been done to determine if the goods are being counterfeited.	
US109	6	Paragraph 9 – evaluation of the physical characteristics	Ed	Punctuation error	Does the solution meet each of the specified physical characteristics: dimension, tensile strength, …..	
FR93	6.1	Last paragraph	Te	False acceptance is not evaluated	Add the sentence: - number of false acceptances. This evaluation requires a specific control protocol. This protocol should include an attempt to produce false authentication elements, which pass with success the authentication control. Typically this protocol could be implemented by independent laboratory	
US110	6.1	Paragraph 1	Ed	Verb subject agreement	As in every process of manufacturing, the manufacturing of authentication solution shall comply with quality requirements.	
US111	6.1	Paragraph 3	Ed	Extra period	……true/false decision of the authenticator.	
US112	6.1	Paragraph 4, 2nd bullet	Ed	And/or, possessive punctuation	Number of false rejections on site, meaning the authentication element's characteristics or association with the material goods are not stable	
FR94	6.2	2	Ed	Degraded mode usage	Replace degraded with fall-back	
US113	6.2	4	Ge	What does "Ratio of controls" mean? Need definition		
US114	6.3	First	Ed	The document should use English spelling and not US.	Replace "organize" with "organise".	
US11	6.3	First	Ge	In case of emergency when counterfeiting detection reaches	In case of emergency when counterfeiting detection	

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
5				a defined threshold, normal authentication protocols have to be adapted or specific authentication protocols may be activated to target the counterfeiting issue and organize the appropriate reaction.	reaches a defined threshold, normal authentication protocols should be adapted or specific authentication protocols should be activated to target the counterfeiting issue and organize the appropriate reaction.	
CA4	6.4		Ed	We need to e consisten with either English spelling or American spelling throughout the document i.e. 6.4 recognize		
US116	6.4	First	Ed		Replace “provide measure metric” with “provide measurement metrics”	
US117	6.4	Second	Ed	The document should use English spelling and not US.	Replace “recognize” with “recognise”.	
CH16	7			Add WHO and EC directive for medicinal products into the bibliography section		
US118	Annex A	All Assessment Grids	Te	All of the Assessment Girds need to be reviewed.	The parameters to be assessed need to be evaluated, the terms used need to measurable or universally definable. The relevance of criticality may be an acceptable criterion but its measurement is subjective. In determining specifications it is more typically displayed as tolerances. Definitions need to be clarified and coordinated throughout the document.	
US119	Annex B	First	Te	I’m not sure the use of the word “must” is correct in the third sentence.	Replace “must” with “should”.	
US120	Annex B	All	TE	“Control means access” table needs to be reviewed.		
US121	Annex C	New Annex	TE	This proposal is an addition to the WD and not a change to the existing content. The purpose of the proposed addition is to assist and better enable end users of the performance criteria to specify requirements for an authentication solution that best satisfies their needs. The justification for this Annex is based upon the fact that not all criteria are applicable to all use cases and that value	Addition of an Annex to provide an example (or tabulation) of how to use the “ Performance Criteria for Authentication Solutions” to specify the requirements for a range of authentication solution use cases. The example envisaged will show for the most likely use cases which criteria are most likely to be applicable and which are not.	

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
				for the end user will be significantly enhanced with an example or tabulation of applicability versus the most common use cases. The provision of an example or tabulation of applicability versus use case will make the criteria less open ended.		
FR95	Bibliography		Ed	Add all the standard referred in 12931	Add: - ISO 31000 Risk management - Principles and guidelines - ISO 15408 Common Criteria (IT Systems) - ISO /IEC 27002 on Information Technology Security (IT Systems)	