ISO/PC 246 N **009**

2009-02-03

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 : **Comments received regarding the NWIP and the WD ISO 12931 "Performance requirements for purpose-built anti-counterfeiting tools"**

Source : **ISO PC Secretariat**

Status : **For information and consideration during the ISO PC 246 plenary meeting**

Comment received during the call for comments on
ISO WD 12931 "Performance requirements for purpose-built anti-counterfeiting tools"

Template for comments and secretariat observations

Date: 2009-01-23	Document: **ISO PC 246 N005**

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	all		ge	After an analysis of this working draft ISO/PC 246 N005 that we globally approve (subject to discussions during the upcoming PC 246 plenary meeting), we have reserves about the restrictive approach on Intellectual Property infringement. The worldwide counterfeiting situation does not just concern IPR and its protection. Development of counterfeiting-crime in consumer goods affects also safety and public health. Recognition of authenticity should be in priority to protect consumers before right holders.	In this context, we propose to extend the debate about counterfeiting (IPR) and counterfeiting-crime (affecting consumers).	

Comments received during the ISO/TMB ballot on NWIP
"Performance requirements for purpose-built anti-counterfeiting tools"

Austria (ON)
ABSTAINS from voting because no expertise available.

Bahrain (BSMD)
Related documents
Article 268 of the Bahrain Penal Code of 1976 provides "A punishment of imprisonment for a period not exceeding 5 years shall be inflicted upon any person who manufactures equipment, tools, or items or such other things intended for imitating, forging or counterfeiting of the lawful currency, whether coins or notes or obtains with the intent of using them for ths purposes.
A prison sentence shall be inflicted upon any person who knowingly keeps such equipemtn, tools or items in his possession. "

Canada (SCC)
3. Canada is in favour of the concept, however, the proposal is not sufficiently mature to accept. Recommendations to consider for a revised proposal include:
The scope notes that "downloadable" products fall outside the scope of the document and would therefore be limited to hard goods. Given the explosion of counterfeit digital media and the increasing electronic distribution in place of physical media, this proposal does not address perhaps the most significant emerging risk. Counterfeiting will also need to be addressed by border controls, certification bodies, manufacturers, distributors, local, national and international regulators and others as this issue has many touch points.
The proposal mixes good performance with good practice, whereas, there is value in a guide to how to mitigate the risk of counterfeiting in a supply chain and also in parallel to a supplier. With respect to the tools used for anti-counterfeiting the proposal does not seem, given the range of counterfeiting, that it would be possible to set up valid and deliverable performance requirements for these.
A standard of this type needs to include the practical aspects of how it can be implemented. Small businesses may have difficulties with the implementation of such standards without significantly increasing the cost of production.
4. Should this, or an improved proposal be accepted, SCC will appoint Mr. Doug Geralde to the Project Committee.

China (SAC)
3.
(1) The title "Performance requirements for purpose-built anti-counterfeiting tools" should be changed. Because not only anti-counterfeiting tools but also anti-counterfeiting solutions related systems have been included in the content of NWI proposal. It also describe various factors in the authentication element creation chain and verification chain. So its scope is not limited within the tools performance. The title can be "Assessment requirements for purpose-built anti-counterfeiting solutions / chain", as suggested.
(2)The NWI project team should build liaison relationship with ISO TC184/SC4, since it will deal with product lifecycle and data management and integration.
(3) In 4.2, there should be a anti-counterfeiting framework and define the authentication element creation chain and verification chain which have been used in the content of this NWI. The content of Per-Type breakdown should be rewritten. It should be based on a framework of anti-counterfeiting.
4. Mr. Junfeng ZHAN

Finland (SFS)
3. Although supporting the initiave, we have concerns on how the resulting standard might be utilized. The scope should be carefully studied; a single solution might not be useful for all product areas and all industrial sectors.
4. susanna.vahtila@sfs.fi

France (AFNOR)
4. Jean-Michel LOUBRY

Germany (DIN)
DIN agrees that it would be useful to develop a checklist with regards to anticounterfeiting methods and tools. DIN is neutral regarding whether or not a Project Committee needs to be established for that purpose, or whether the work could be done by ISO TC 184.
However, DIN disagrees to the development of a standard "Performance requirements for purpose-built anti-counterfeiting tools":
Anti-counterfeiting tools that have been developed for the protection of a certain product or a certain industry are by nature likely to be unique (e.g. use of unique serial numbers in the JTC 1 SC 31 context) or at least very specific.
Anti-counterfeiting tools that are developed by a company and which conform to the performance requirements of a potential standard are very likely to be subject to an IP policy in order to allow the developer to keep ahead of his competitors. This will hamper the use of a potential standard.
Generally speaking, such anti-counterfeiting tools will need to be permanently improved in order to keep pace in the technology race between the industry and the people who counterfeit their products, and a list of performance requirements that has been standardized once and for all will soon be outdated.
Consequently, DIN is in favour of the development of a Technical Report containing mainly a checklist with regards to anticounterfeiting methods and tools.

Italy (UNI)
4 - Participation
Names and contact information of nominated experts:
Mr Marco Fossi
Mr Roberto Sordini
Mr Enrico Marchetti
Mr Marco Tappainer
and for information, UNI contact person:
Mr Gianluca Salerio

Japan (JISC)
3. JISC disagrees with this proposal, and has the following comments.
(1) There is no demand for this standardization.
Both vendors and users of purpose-built anti-counterfeiting tools in Japan do not recognize the necessity of the proposed standard, and they estimate that the attached draft will not be useful as an anti-counterfeiting tool. According to their perception, the performance requirements for purpose-built anti-counterfeiting tools depend on the particular products and markets, and they do not require general principles of the performance requirement. Thus, JISC cannot identify any demand for this standardization at this point.
(2) It is not feasible for standardization.
According to Japanese stakeholders who fight counterfeiting, since vendors and users of purpose-built anti-counterfeiting tools share secrets regarding purpose-built anti-counterfeiting tools, including the performance requirements for them under their mutual agreements, it would be very difficult to accomplish the proposed standardization because there are many obstacles to information exchange. They are concerned that the proposed standard will be neither useful nor globally relevant. Thus, JISC believes this standardization is not feasible.
(3)This standardization may cause unexpected problems.
In consultations with Japanese stakeholders, they point out that, although the proposed standard might help those who fight counterfeiting, at the same time it could also assist those who make counterfeit goods. In other words, the proposed standard may benefit counterfeiters. Therefore, JISC cannot see that the proposal will contribute to the public benefit.

Netherlands (NEN)
Mr Jelte Dijkstra from NEN

New Zealand (SNZ)

Although New Zealand will not be an active partcipant on this committee, New Zealand is likely to request observer status for the work of this PC.

Spain (AENOR)
2. CEN/ISSS Workshop on 'Anti-counterfeiting: Protocols for Detection of Counterfeits' - WS/CPF
4. Ms. Paloma GARCÍA

Switzerland (SNV)
4. Pierre Delval,

United Kingdom (BSI)
Anti-counterfeiting is a broad subject, and there are many potential areas for standardization. The AFNOR proposal could be a useful contribution to the work on anti-counterfeiting. There is also existing work in CEN Workshop Agreements on protocols for the detection of counterfeits. These two initiatives are potentially complementary.
It is essential that this proposal is not developed in isolation within an ISO Project Committee. We would like to see the development of a framework for anti-counterfeiting standards. Performance requirements for anti-counterfeiting tools should be one element of this framework and it would be more appropriate for this work to be performed in a TC. Such a TC could ultimately cover:
• Protocols for the detection of counterfeits;
• Definitions of the types of anti-counterfeiting authenticators;
• The role of a secure trail (or track and trace) in authentication of goods;
• Definitions of the layers of anti-counterfeiting and the layers of examination, defining, for example, expectations on consumers, law enforcement officers etc;
• Performance measures, including robustness, for anti-counterfeiting tools;
• Requirements for the security of the premises and procedures for the manufacture of anti-counterfeiting tools;
Our continued view is that there is a wider standardization need around anti-counterfeiting than that outlined in this proposal. Therefore the UK is against this NWIP.

USA (ANSI)
ANSI Position and Comments on AFNOR NWIP on Performance requirements for purpose-build anti-counterfeiting tools
ANSI votes negative on the subject AFNOR NWIP. Please do not register ANSI as a P or O member of this committee at this time should this proposal be approved.
General Comments
The scope of the project is broad and somewhat ambiguous, lending itself to different interpretations. It can be read as a specification of the performance requirements for instruments (tools) that are used to read hidden authentication messages or detect the presence of authentication materials. Alternatively, it can be viewed as an attempt to write a comprehensive requirements definition document for anti-counterfeiting solutions in general including those aimed at prevention as well as correction of the problem. The scope therefore requires further clarification.
While the proposal notes over 300 devices, the types of tools typically found in the brand protection authentication market include: barcode readers, magnifiers, magnetic stripe readers, and taggent detection devices. Some simple devices such as magnifiers, authentication pens, and ultraviolet lights, would fall outside of the scope of this particular proposal in that they may not be purpose built or don't typically collect or exchange data.
The proposal does not address the following issues:
1) The means as to how the tools are to be evaluated; it only establishes an objective level.
2) The authentication technologies' effectiveness, suitability or characteristics.
3) The applicability and/or use of the machines in the general populace.

Key questions that we believe need to be addressed are as follows:
1) What are the prominent issues in regards to the current anti-counterfeiting tools?
   (1) Interoperability
   (2) Unreliability/mechanical failure
   (3) Security of data and/or tool technology

(4) Efficiency to detect
(5) Data collection and dissemination
(6) User training

2) Is the anti-counterfeiting tools industry aware of the issues?
3) Who is the primary target audience for this standard?
(1) The anti-counterfeiting tools industry
(2) The anti-counterfeiting technology users
4) Has either of the audiences expressed a need for such a standard?
5) Why does the standard exclude "candidate technologies like RFID, optical devices, DNA, etc."?

Conclusion: This is a technical standard focused upon "anti-counterfeiting tools", in effect the readers and detection devices used in the brand protection market. While in general agreement with such a standard; the need for this type of standard has not been commonly expressed by the industry in North America.

Additional General Comments

The Justification and Need

We recognize that this new work item proposal is specifically focused upon purpose built anti-counterfeiting tools, but may involve entire security systems. These tools are generally or commonly recognized as "readers" and include the ability to capture information related to barcodes, character recognition, taggents, reflectivity, DNA, nanoparticles, and other technologies. As acknowledged in the proposal there are over 300 devices or systems available for authentication. Many of these devices are proprietary to a specific technology and would raise the question of the desirability of interoperability, modularity and performance to a generic standard. It thus poses the question:

"Is there a general recognition among the technology developers or Brand Protection market, of the need for a generic standard that will attempt to develop performance requirements and evaluations, and that may not be specific to the technology or intended working environment?"

While those in the security technology segment recognize the issues of fraud, there is no recognition in the "Purpose and Justification" of the proposal that the technology providers or Brand Protection market desires or requires such a standard.

Broad Scope

The broad scope of this proposal creates a very complex issue of developing a meaningful, useful and trusted standard. Among the proposed issues are:

- reliability and robustness of tools
- integration and processing
- data acquisition, data processing and storage
- adequacy with product authentication function
- guidelines for data model in security target for a possible application of Common Criteria
- extensibility capabilities requirements systems/sub systems to anticipate new additional functions
- modularity of functions in view to facilitate integration of tools
- capability to facilitate controls in any circumstance, location, condition of usage, without generating specific constraints
- design requirement to authorize and monitor data access
- typology of the actors concerned by the control process
- types of data to be shared with the actors
- scalability of tools: availability to adapt the dynamics of controls depending on threat
- to bring a high level of reliability to all interested actors
- efficiency to detect a counterfeit product
- specific requirements for security, including tracking process
- data security requirements

If one begins to think through the scope of work involved in this proposal, it begins to become apparent that many of the individual issues may support the creation or implementation of individual standards. Those supporting standards, if not in existence, would then need to be developed, consensus reviewed, and approved prior to the establishment of performance requirements. It would appear that this proposal needs to be more closely defined and limited in scope to achieve a workable result. A more stepped approach of building supporting standards and

practices used in the performance requirements would appear to be a more constructive method of development.

Methodology

The working draft provides an example of the Assessment Grid that will be used for performance Assessment. It outlines the Assessment criteria, Objectives targeted, and Parameters to be assessed. The area of "Parameters to be accessed" does not discuss the methodologies that will be used to evaluate that criterion. For an example; Assessment criteria 1 uses the following terminology to describe Parameters to be addressed, "level of difficulty of the technical device be reproduced by the person skilled in the art". What methodology is used to determine objective "Level of difficulty…", or the skill of the "person skilled in the art". These appear to be very subjective assessment criteria and open to interpretation and critical comment. A subjective performance requirement process leads to a variability of results that are not consistent to the intent of the evaluation. In an area of business competitiveness, subjective assessment systems are open to abuse and distrust.

The methodologies used in the performance requirements assessment must be able to support measurable, objective results.

Conclusion

While the North American security assurance industry is supportive of effective security focused standards, the question of need, scope and methodology of this work proposal raises questions that need to be addressed. Without a re-evaluation of the areas of concern outlined above, acceptance and use of this proposal will be difficult to achieve.

Further Comments

The concept of allowing customers to have an objective assessment of an "anti-counterfeiting" tool would be extremely helpful to customers when choosing a solution to use. However, details of the criteria, metrics and how the assessments will be made (as well as what entities would be allowed to certify the assessment) must be discussed and agreed upon in order to realize the goals specified in the document. For example, while the concept of "measurable" levels of performance would be very useful to the customers and users, the proposed document needs to include how the various performance criteria can be measured. The Appendix table indicates a start in defining important requirements or features and potential parameters, but does not necessarily provide an objective means for assessing the quality of an anti-counterfeiting tool implementation.

Specific Comments

Text	Location	Issue	Suggestions/Questions
"measurable levels of performance to be achieved"	p. 1 Section I Scope	Not all of the criteria specified in the appendix or defined in the document appear to have a clear method of objectively measuring the degree to which a functionality/requirement is achieved.	Examine each functional and non-functional criteria to determine if objective metrics can be used to assess the tool. Perhaps the document can also distinguish between functional and non-functional requirements. Define objective metrics for the functional and non-functional features. Creating a data model of the measurable criteria to describe the pertinent data or framework needed to assess the anti-counterfeiting tool. The model should also capture what is required for different levels of certification/compliance.
"product life cycle"	4 and 4.1	Need a clear definition of product lifecycle.	Include a definition; and define what features would ensure interoperability, reliability, etc. throughout the product lifecycle. Will there be a way to specify requirement to maintain certain authentication features (elements) throughout the product life cycle? Would there be different requirements at different stages of the lifecycle?

Text	Location	Issue	Suggestions/Questions
"Access to tools"	4.2.3 2nd table and 5.7	Roles may not be specific to be actual access roles. For example, "supervisory agents" – there may be a need to define finer granularities of access levels within that category depending on what supervisory agents they are.	Either define the roles: "end user", "supervisory authority" … etc. OR allow industry to define the roles as needed and put the table in an appendix as an example.
"Performance"	In the title, and throughout the document	The word "Performance" in software can be misconstrued. It is often used to refer to speed, and might be better replaced with "requirements" or "objectives".	1. Change title to "Requirements for anti-counterfeiting tools" or "Criteria specification for anti-counterfeiting tools" 2. Change first sentence of the scope (pg. 1) to: "…specification of objectives to anti-counterfeiting tools."
"Common Criteria"	5.1	"Advisable to consult the Common Criteria …"	How will robustness be measured? If the Common Criteria is not required, is there a subset of security standards that must be used to measure robustness in order to ensure a level of security the customer can trust and/or verify?
"Harmlessness"	5.5.5	It would be more informative to the customer to know possible health risks than to know whether there is an absence of (*known*) negative effects on human health.	A possible metric would be to enumerate known risks on human health.