ISO/PC 246 N **005**

2008-11-14

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 : **Call for comments on the ISO WD "Performance requirements for purpose-built anti-counterfeiting tools"**

Source : **ISO PC Secretariat**

Status : **The members are invited to comment the attached draft.**

Please use the ISO template for comments, and download it on the ISO electronic balloting portal / Committee internal balloting, no later than the 30th of January 2009.

Date: 2008-06-19

ISO/WD

Performance requirements for purpose-built anti-counterfeiting tools

Exigences de performance pour des dispositifs techniques dédiés à la lutte contre la contrefaçon

Warning

This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Document type: International Standard
Document subtype:
Document stage: (20) Preparatory
Document language: E

M:\dms\dtec\xdom446\2008-06-19\Projet V5.1 VE.doc STD Version 2.2

Contents

Page

Foreword v

Introduction vii
Intellectual property infringement vii
Recognition of authenticity vii

1 Scope 1

2 Normative references 2

3 Definitions 2
3.1 attack 2
3.2 internal attack 2
3.3 external attack 2
3.4 counterfeit 2
3.5 inspector 2
3.6 capture system 2
3.7 distributors and service providers 2
3.8 element of authentication 2
3.9 proof/evidence 2
3.10 integrity 3
3.11 interoperability 3
3.12 technical tool 3
3.13 proof 3
3.14 authentic product 3
3.15 counterfeit goods/fake goods 3
3.16 counterfeit product 3
3.17 Intellectual property rights 3
3.18 robustness 3
3.19 security 3
3.20 anti-counterfeiting solution 4
3.21 rights owner / rights holder 4

4 General principles 5
4.1 Performance requirements for purpose-built anti-counterfeiting tools 5
4.2 Per-type breakdown of anti-counterfeiting solutions 6
4.2.1 Type 1 6
4.2.2 Type 2 6
4.2.3 Type 3 6

5 Assessment criteria 7
5.1 Robustness of the anti-counterfeiting solution: 8
5.1.1 Security in the creation of elements of authentication 8
5.1.2 Security in the matching of the elements of authentication with the products 8
5.1.3 Security in the verification of elements of authentication 8
5.1.4 Security of reference base of authentication elements storage 9
5.2 Adaptability and flexibility 9
5.3 Interoperability and upgrade capability of the control tools : 9
5.3.1 Several verification functions accessible through the same technical tool 9
5.3.2 Hardware modularity 9
5.3.3 Software interoperability 9
5.4 Resistance of the elements of authentication 9
5.4.1 Operational resistance 9
5.4.2 Transferability 10
5.5 Useability of the analysis tools: 10

5.5.1 Training 10
5.5.2 Usage 10
5.5.3 Endurance 10
5.5.4 Usability engineering 10
5.5.5 Harmlessness 10
5.6 Reliability/solidity of the technical tools and of the control devices: 10
5.6.1 Control systems reliability (true/false) 10
5.6.2 MTBF (Mean Time Between Failures) 10
5.6.3 Maintenance, preventive maintenance 10
5.6.4 Ruggedness 11
5.7 Access rights for the various actors in the verification chain: 11
5.7.1 End user 11
5.7.2 Operators of the distribution and supplying networks 11
5.7.3 Supervisory administrative authorities 11
5.7.4 Supervisory agents given clearance by the copyright holder or its licensees 11
5.8 Ability to provide elements for the proof of counterfeiting 11
5.8.1 Recorded evidence of the verification 11
5.8.2 Tamper-proofing the recorded evidence of verification 11
6 Effectiveness measurement of the anti-counterfeiting solution 12
7 Bibliography 13
Annex A 14

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

ISO was prepared by ….

Counterfeiting is a fast-expanding phenomenon targeting every sector of business. The increasing volumes of products being counterfeited generates consumer health and welfare risks, introduces distortion of competition, violates the interests and intellectual property rights of legitimate producers, fuels unemployment, undermines fair trade and bites into tax revenues.

The present document has been drafted by the actors involved in response to a call to pinpoint the objectives and boundaries required for industry-wide and services-wide application. This document sets out the performance requirements for purpose-built anti-counterfeiting tools. These anti-counterfeiting tools are designed to provide reliable evidence making it easier to assess whether products are authentic or counterfeit.

The present document aims to integrate the performance requirements for anti-counterfeiting tools into products lifecycle, particularly from their design and their manufacturing and in any situation requiring the authentication of the product. Anti-counterfeiting is thus positioned as a feature of the product and services lifecycle.

The present document is part of a wider framework wherein the proof that a product is authentic or counterfeit can be obtained by any means whatsoever, and it was not drafted or designed to define a sole means of establishing proof for the relevant authorities.

It application, based on voluntary cooperation, shall make it possible to:

pool the experience built up on anti-counterfeiting issues by business and the governing authorities,

determine the level of reliability offered by various anti-counterfeiting tools according to their levels of performance,

to create the conditions for a better assessment of the anti-counterfeiting tools used, in compliance with the rules on fair competition.

In this document, as special case, we are going also to take into consideration the following issues, in terms of performance requirements of protection systems against counterfeiting which are, a.o. under the scope of ISO/TC 184.

• Data acquisition, data processing and data storage

  o Adequacy with product authentication function

• Interoperability for systems and sub-systems dedicated to protection against counterfeiting

  o Extensibility capabilities requirements for systems/sub systems to anticipate new additional functions for covering further needs issued from anti-counterfeiting fight

  o Modularity of functions in view to facilitate integration of tools

• Capability to facilitate controls in any circumstances, in any locations, and in any conditions of usage, without generating specific constraints

• Design requirement to authorize and monitor data access to different actors concerned:

  o Types of data to be shared with the actors of the control at different step of the control process

  o Scalability of tools: availability to adapt the dynamic of controls depending of threat

• Specific requirements for security, including tracking process

  o This section will refer as much as possible to existing international security standards

  o Data security requirements to ensure non dissemination of confidential information related to the user

The present document is in no way designed to create a framework targeted towards stemming the sales of products distributed through alternative business channels, nor is it intended to introduce the legal and technical basis for a new offence founded on the counterfeiting of a label system that may have been given approval from the public authorities.

Since said tools are designed to be deployed and used by the intellectual property holders, authorized licensees as well as the administrative authorities, they are led to be integrated into anti-counterfeiting systems and therefore need to be designed with harmonisation and interoperability in mind.

Introduction

The range of counterfeited products has been developed strongly since over a decade, and is now no longer limited to luxury goods. Although figures vary depending on the data source and method of calculation, counterfeit goods is estimated up to 10% of world trade, and the counterfeit market has been booming in recent years. Counterfeit goods trafficking is progressively spanning out to target more general consumer goods. These counterfeit goods do not necessarily offer the same guarantees in terms of safety and/or compliance with environmental measures and regulatory requirements, generating risk for consumers, users and the distribution chain. They cause loss of earnings, job losses and brand value damage for the companies targeted.

In order to prevent counterfeiting from plaguing their business, companies are increasingly using technological devices geared to their individual needs. It is important to specify the performance requirements for the devices designed to fight against counterfeiting at both national and international level, to nurture greater confidence among consumers, to empower and secure the distribution circuits, and to help the public authorities deploy preventive and punitive measures.

Technology-enabled anti-counterfeiting systems become more effective when they are geared to product lifecycles.

Counterfeiting is an infringement of intellectual property rights, a point that needs to be kept separate from the question of product quality and the distribution of authentic products via alternative business channels.

Intellectual property infringement

The products protected by intellectual property rights can be counterfeited in various different ways: Counterfeiting commonly concerns:

— copyright and rights related to copyrights: unauthorised reproduction of an original literary or artistic works or software belonging to a third party;

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

— trademarks: unauthorised total or partial reproductions or imitations, without the authorisation of the trademark owner or its authorized licensee, of the distinctive sign or combination of signs that a business organisation attaches to a product or services to distinguish its product or services from those of other entities;

— industrial designs : using or making similar or identical copies, without authorisation from the owner, of the representation of a product or part of a product that confers the characteristic lines, contours, colours, shape, texture and/or the materials of the product itself and/or its trade dress.

Recognition of authenticity

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

Counterfeiting seeks to bypass the legal provisions designed to enable professionals to release safe products onto the market in fair competition. Buyers do not necessarily pay all necessary attention to the products they are examining, particularly because of: trust, lack of time, the temptation of attractive prices, or simply because they are unfamiliar with the product itself or possibly the anti-counterfeiting device.

Establishing the authenticity of a product, in other words recognizing that the product is 'genuine or forged' in order to demonstrate whether it is a counterfeit, consists in checking whether the product reproduces the essential characteristics of the authentic product to help establish whether or not there has been infringement. The first step, then, required to provide solid ground on which to conduct this challenge, is to establish what these essential characteristics are, in particular the product's origin, and then to verify whether the suspect product being challenged does objectively and concretely present these characteristics.

If there is any doubt as to the authenticity of a product, it is the inspector's role, once they have observed the characteristics of the suspect product and/or anti-counterfeiting device, to examine whether these characteristics match those of the authentic product and/or anti-counterfeiting device. The process involved is an essentially technical analysis, where time pressure is a major element for success in any effective data input and investigation procedure.

Products can be authenticated in one of two ways: either by experience, or by authentication elements.

For the professionals tasked with carrying out the verifications and who are used to handling the products, experience is the result of the match made between several products by their experienced eye. They know by experience what they need to hone in on. However, since the counterfeits themselves get better every year, the degree of attention given and the level of expertise and experience required also need to grow. A professional who spends hours and hours examining the same kinds of products undeniably acquires a mass of knowledge, acumen and sharpness of vision that will often enable them to see through the quality and origin of a part far faster than somebody else. Unfortunately, experts of this level are few and far between, and it is generally the "all-rounders" that end up checking the vast majority of products submitted to inspection, a situation that makes it increasingly important to have reliable, commercially available counterfeit detection tools.

Performance requirements for purpose-built anti-counterfeiting tools

1 Scope

The present document concerns the performance of anti-counterfeiting tools. It is therefore intended to establish a standard of objectives and not a standard of means. The term standard of objectives is understood as a document setting out measurable levels of performance to be achieved, but which does not necessarily specify one or more individual technical solutions for achieving these performance levels.

In its current state, the purpose of the present document is to specify performance requirements for authentication and verification tools purpose-built for protecting against counterfeiting.

This document specifies performance requirements for an authentication solution deployed to help demonstrate product authenticity.

The present document is intended for any kind of business organisation liable to be targeted by counterfeiting, for whom it offers a set of individually-geared measures designed to enable them to make an informed choice between the range of tools used to establish the authenticity of a product.

The performance criteria for anti-counterfeiting tools shall be studied by the businesses in relation to their organisation, their technical resources and their product targets.

This document defines these criteria, making it possible to build and use a scale of quality level, and goes on to specify the performance requirements for an authentication solution deployed to help demonstrate product authenticity.

The scope of this document covers the performance of technical anti-counterfeiting tools. It deals exclusively with the products protected by the following intellectual property rights:

— Copyright and rights related to copyrights

— patent inventions and supplementary protection certificate;

— trademarks;

— industrial designs;

The scope of this document covers the performance of technical anti-counterfeiting devices, which are complementary means of recognition of the products protected by an intellectual property right.

This document applies to manufactured products. It does not apply to products used in the banking and finances sector, nor to official administrative papers, nor to downloadable products sold online.

2 Normative references

To be completed:

ISO/CEI 15408: *Common Criteria for Information Technology Security Evaluation, version 3.1 dated September 2006 (and versions 2.1, 2.2, and 2.3)*

3 Definitions

For the purpose of this document, the following terms and definitions apply:

3.1 attack

successful or unsuccessful attempt to hack an anti-counterfeiting solution, to be able to imitate, produce, possibly reproduce, the authentication elements.

3.2 internal attack

attack perpetrated by persons or entities directly or indirectly linked with the right holder (staff of the right holder, subcontractor, supplier …)

3.3 external attack

attack perpetrated by persons or entities that are not directly or indirectly linked with the right holder

3.4 counterfeit

infringement of intellectual property rights

3.5 inspector

any natural person, from the consumer to the expert, who uses the anti-counterfeiting device with the aim of authenticating the product

3.6 capture system

human and/or technical means for reading, capturing or sampling an element of authentication

3.7 distributors and service providers

any professional intermediaries between the rights owner and the end-user

3.8 element of authentication

a visible or invisible piece of information associated with a product that can be used or deployed to help build evidence

3.9 proof/evidence

the result of an expert appraisal that is used as the grounds for an enquiry and/or an administrative and/or legal decision

3.10 integrity

the property of the unimpaired condition of the element of authentication, the associated data, the information or the elements and the means for processing them

3.11 interoperability

degree to which an anti-counterfeiting solution is able to work together with other different technical devices

3.12 technical tool

a system or a set of hardware and/or software-based systems used to build and run the anti-counterfeiting solution, used to perform the control of the product authenticity.

3.13 proof

something which demonstrates/establishes that something or some action is true

3.14 authentic product

a product produced under the control of the holder of intellectual property rights

3.15 counterfeit goods/fake goods

product imitating or copying an authentic product covered by the protection of one or more intellectual property rights

3.16 counterfeit product

authentic product covered by the protection of one or more intellectual property rights and subjected to counterfeiting/patent infringement

3.17 Intellectual property rights

exclusive rights given for a certain period of time to a physical person or legal entity over the creation of their minds and customarily divided into two main areas: 1 – copyright and rights related to copyright, 2 – industrial property

3.18 robustness

the ability of a system to resist to virtual or physical, internal or external attacks

Note: particularly, in the context of this document, it is the ability to resist attempted imitation, copy, intrusion or bypassing

3.19 security

situation presumed as being not at risk secret

information that is unknown to unauthorised people, and which plays a role in creating or interpreting authentication element

3.20 anti-counterfeiting solution

a set of devices, tools, authentication elements and procedures used to contribute to the recognition of the authentic products and to the detection of products being counterfeited within the framework of anti-counterfeiting.

3.21 rights owner / rights holder

a physical person or legal entity either holding or authorised to use one or more intellectual property rights

4 General principles

Anti-counterfeiting solutions can come in a range of formats, given that the technical, logistical and financial criteria involved will depend on the intrinsic, integrated or attached characteristics of the element(s) of authentication, the verification levels and methods targeted, the information systems distributed and/or secured, how strongly the solution can resist against counterfeiting, the value of the products intended to be protected, and the counterfeiting-related risks that weigh throughout the product's lifecycle (The product life cycle is divided into defined periods called phases in which activities that belong together are grouped, e.g. product concept, design, production, service, dismantling etc..

The verification processes of authentication elements deployed in these solutions require the ability to read, capture and sometimes perform sampling, using purpose-built tools. 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 and/or sample and/or product towards a structure offering expert analysis for an off-line diagnosis.

This means that there is an authentication element creation chain that starts at the specification of product protection (or trademark protection or industrial design or model protection) and runs through to how this data matches the product manufactured by the rights holder or licensee, as well as a verification chain combining the tools and/or references used in the information system. There are also human actors involved in this chain – essentially people that are present, trained and organised – and who therefore form an integral part of performance measurement of the anti-counterfeiting solutions.

The level of performance of an anti-counterfeiting solution shall therefore be assessed as a whole, including all the components and interfaces involved.

This document doesn’t deal with economical criteria aiming to correlate performance and costs of the anti-counterfeiting solutions.

4.1 Performance requirements for purpose-built anti-counterfeiting tools

The aim of the performance assessment criteria for purpose-built anti-counterfeiting tools is:

- to offer a level of data acquisition, processing, release and storage making it possible to authenticate the product;
- to make it possible to define the system's level of interoperability throughout the product lifecycle;
- to enable upgrades in technological tools to be factored in;
- to guarantee data security, including in terms of economic intelligence;
- to make it possible to define a level of reliability and robustness that is satisfactory for all the stakeholders;
- to facilitate the verification process without generating particular constraints;
- to ensure that the stakeholders are given widespread access to tools geared to their industrial production and distribution cycles;
- to run product verifications anywhere, under all foreseeable circumstances and conditions of use;
- to define specific requirements for every level of security of the anti-counterfeiting tools;
- to help define and deploy a system for assessing the operational effectiveness of the anti-counterfeiting solutions.

4.2 Per-type breakdown of anti-counterfeiting solutions

This typology is not intended to rank the solutions according to performance effectiveness, but to provide a presentation table for solution users and anti-counterfeiting device suppliers, according to the tools needed for the implementation of the solutions. An anti-counterfeiting solution may combine several types of anti-counterfeiting devices.

4.2.1 Type 1

Verifiable independently by purely human input

4.2.2 Type 2

Requires a technical tool

4.2.3 Type 3

Requires valuation by an analyses centre

Tool	Standalone (A) / On-line connection (B)	Off-the-shelf (C) /Purpose-built (D)	Human (E) /Automated (F) interpretation
Element of authentication			
Type 1 Verifiable independently by purely human input	NA	NA	human
Type 2 Requires a technical tool			
Type 3 Requires valuation by an analyses centre			

Standalone tool: technical tool which integrates the functions required to be able to interpret the authentication element in-the-field, off line.

On-line tool: technical tool which requires a real-time on-line connection to be able to locally interpret the authentication element

Off-the-shelf tool: technical tool which can be purchased through open sales networks

Purpose-built tool: technical tool which is offered exclusively by the supplier of the authentication solution

Human interpretation: authenticityis evaluated by the inspector

Automated interpretation: authenticity is evaluated automatically by one or more components of the authentication solution

Examples to be provided

Access to the tools

	End user	Distribution and supplying networks	Supervisory authority	Personnel given clearance by the right holder	Certified laboratory
Type 1 Verifiable independently by purely human input					
Type 2 Requires a technical tool					
Type 3 Requires valuation by an analyses centre					

Access to the tools is defined according to the authentication elements chosen.

5 Assessment criteria

Any single anti-counterfeiting solution may combine several authentication elements working together to build proof. These components may operate on different types and with different levels of accessibility (see 5.2). In this case, the performance of each type should be considered individually, where relevant.

With the aim of assisting the user to chose the better adapted anti-counterfeiting solution for his needs, criteria consider both the intrinsic performance of the solutions and the performance of their use.

5.1 Robustness of the anti-counterfeiting solution:

Robustness of the technical device will be all the more high since its copying appears difficult for the person skilled in the art.

In order to estimate the robustness of the anti-counterfeiting solution, it should be advisable to consult the Common Criteria (ISO 15408), for the relevant parts of the solution (software components and datas).

If the solution includes an electronic signature, the applicable level of protection is at least the same as the one referenced by the community regulations (CWA 14167, CWA 14169)

5.1.1 Security in the creation of elements of authentication

The processes designed to create and to produce the element of authentication draw on functions that integrate secret elements to which access shall be stringently protected. This makes it important to guarantee the level of security and of traceability in relation to human interventions, tamper-proof processes, and sealed-down inter-application communications. In particular, if the processes are shared in order to generate secrets for different targets (products, manufacturers, etc.), then the partitioning and diversification in how the elements are transmitted shall guarantee total inter-process independence and not open up any loopholes.

5.1.2 Security in the matching of the elements of authentication with the products

The processes designed to match the elements of authentication with the products shall be secured in order to prevent any upstream or downstream subversion. This includes all downstream processes generating elements of authentication, right up to the match-up itself: transfer/transport, integration into the production processes, and so on.

It is crucial to develop either tangible or intangible interdependence between the authentication element and the product it protects.

Tangible interdependence means, on one hand, that the association between the anti-counterfeiting tool and the product it protects is made physically resistant, and on the other hand, that the element of authentication is destroyed if an attempt is made to sever this association.

Intangible interdependence means a logical association between the element of authentication and some kind of master reference, an association between the element and the product, or between the product and the container that cannot be destroyed nor reproduced.

5.1.3 Security in the verification of elements of authentication

The processes and tools designed to verify the elements of authentication shall be made impenetrable to any internal or external attack intended to capture secret data or the processes that allow to produce, possibly reproduce, the authentication elements.

5.1.3.1 Tamper-proofing of the tools

The devices designed to capture the elements of authentication shall be protected and/or respond to any attempted subversion aiming to capture the data processing or data transfers performed. This includes making it impossible to query reference databases using unauthorised tools.

5.1.3.2 Normal mode/fallback mode

For capture devices fitted with power sources making them able to operate in standalone mode and/or in on-line mode, indications shall be given as to whether the systems features a fallback mode (for low battery, network down, etc.) or an alternative protocol, possibly requiring another type of authentication element.

5.1.3.3 Traceability of inspections

Inspections should be tracked in order to check that they are being executed in a quantitatively and qualitatively appropriate manner, in accordance with the protocols and the confidentiality rules defined by the stakeholders.

5.1.4 Security of reference base of authentication elements storage

This criteria only applies in case of use of database of authentication references.

The databases containing the references of the authentication elements and allowing to check the authentic character of the authentication elements linked with the checked products have to be protected against any interference. A successful interference shall be detected and signalled to the right holder.

5.2 Adaptability and flexibility

The anti-counterfeiting solution shall permit an adaptation of the frequency and of the intensity of the controls in order to respond to irregular events, such as a glut of suspect goods hitting a geographical market, for a given period, for a given class of products, etc.

5.3 Interoperability and upgrade capability of the control tools :

5.3.1 Several verification functions accessible through the same technical tool

Capability possessed by a single tool to perform verifications on different elements of authentication, with zero risk of interference between the control applications.

5.3.2 Hardware modularity

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

5.3.3 Software interoperability

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

5.4 Resistance of the elements of authentication

How the authentication element resists to involuntary alterations (environmental climate, natural wear and tear, repeated handling) is a key factor in the sustainability of the solution's performance levels. Any involuntary alteration rendering the authentifier inoperable would prevent authentication and may – possibly wrongfully – lead to suspected counterfeiting

5.4.1 Operational resistance

The authentication elements shall not be affected by the product environment during the whole period requiring authentication controls.

5.4.2 Transferability

The elements of authentication shall be capable of being integrated into a production process without requiring wholesale changes and without impairing performance levels. The production processes shall not alter the characteristics of the authentication element.

5.5 Useability of the analysis tools:

5.5.1 Training

Expression of the need for training on using the technical tools according to input level and pre-requisite skills. This includes training on the data targeted and the missions assigned to users tasked with deploying the solution

5.5.2 Usage

Deployability and up-time

5.5.3 Endurance

On-site operational time range in normal mode and/or in fallback mode

5.5.4 Usability engineering

User-friendliness, with no confusing ambiguities

5.5.5 Harmlessness

Absence of negative effects on human health

5.6 Reliability/solidity of the technical tools and of the control devices:

5.6.1 Control systems reliability (true/false)

5.6.1.1 Absence of misleading interpretation

5.6.1.2 Rejecting shams

The capture system shall be able to detect imitation authentifiers

5.6.1.3 False positives

The sensitivity of the capture system to variations in the processes of creating authentication elements.

5.6.2 MTBF (Mean Time Between Failures)

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

5.6.3 Maintenance, preventive maintenance

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

5.6.4 Ruggedness

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

5.7 Access rights for the various actors in the verification chain:

Who is the tool intended for? How are the user rights managed?

5.7.1 End user

5.7.2 Operators of the distribution and supplying networks

5.7.3 Supervisory administrative authorities

5.7.4 Supervisory agents given clearance by the copyright holder or its licensees

5.8 Ability to provide elements for the proof of counterfeiting

5.8.1 Recorded evidence of the verification

5.8.1.1 filed with the copyright holder or its licensees

5.8.1.2 filed with the legal and administrative authorities

5.8.2 Tamper-proofing the recorded evidence of verification

6 Effectiveness measurement of the anti-counterfeiting solution

This is a measurement that can be made on all the aforementioned criteria or just a selection.

It is the risk level as assessed by the rights holder or its licensees and the performance level of the anti-counterfeiting measures deployed that will determine the protocols capable of assuring that the system is effective against internal and external attacks (hacking, disclosure of confidential information, corruption of authentication elements etc.).

The protocols defined in this section are typical protocols that each rights owner or its licensees can adapt to their own market environment and procurement and distribution circuits, or possibly even to their own products.

Certain protocol parameters shall be made resettable so that an on-the-spot reaction can be employed in response to any attempted breach.

These protocols shall deal with both preventive and corrective effectiveness measurements.

The protocols which should specify the effectiveness of a solution are, according to the solution:

- The actors given access to different levels and conditions of access
    - Actors in the authentication element creation chain
    - Actors in the chain of supply of authentication information and elements
    - Actors in the verification chain
- Measurement parameters as part of preventive action
    - Traceability of the interference attempts in the databases linked to authentication elements
    - Quality control on the evidence of elements of authentication recorded
    - Frequency of in-field verifications
    - Verification control sites
    - True-false capture rates (from the field)
- Measurement parameters as part of corrective action
    - Verification rates
    - Number of failures of the system pointed out to the users

7 Bibliography

[1] Accord AFNOR AC Z 60-100 "Prévention et dissuasion techniques pour la lutte anti-contrefaçon (protection des droits de propriété intellectuelle) - Spécifications d'un cadre générique décrivant les dispositions d'authentification des produits, d'organisation de la traçabilité et de contrôle dédiées à la lutte anti-contrefaçon"

[2] TRIP'S Trade related aspects of intellectual property rights

[3] Security standards for Information systems

Annex A

Assessment grid

This annex presents the grid for assessing anti-counterfeiting solutions according to the criteria defined in section 6.

It specifies the parameters to be analysed and the results targeted.

To be completed

Assessment criteria	Objectives targeted	Parameters to be assessed	Assessment
1- Robustness of the anti-counterfeiting solution	To ensure that the solution can resist to external or internal attacks	Level of difficulty of the technical device to be reproduced by the person skilled in the art	
1.1- security of elements of authentication generated	To ensure that secrets used to create elements of authentication can never be divulged	Security means and security measures employed Management of secrecy-related elements (keys, certificates, etc.) Personnel given clearance: training, traceability	
1.2- security in the matching of elements of authentication with the products	To ensure the robustness of all the links between the generation of elements of authentication and their match-up with the products	Security means and security measures deployed for routing elements of authentication The material or immaterial match-up process	
1.3- security of verifications run on elements of authentication	To ensure the robustness of the tools and processes used for the elements of authentication capture and verification		
1.3.1- tamper-proofing of the technical tools	To ensure that it is impossible to intercept the elements of authentication as it is being processed or transferred to reference databases	Physical tamper-proofing (intrusion detection, etc.) Security means and security measures employed in elements of authentication transfers to the reference databases and for the	

		replies	
1.3.2- normal mode/fallback mode	Make sure of the operating conditions for tools in fallback mode	Operation when battery power is low Operation when there is no on-line connection	
1.3.3- traceability of the inspections	Make sure that any use of the technical tools should be recorded	Records of use and management of the tracks	
1.4- security of reference base storage	To ensure the robustness of the reference base storages used for verification of the elements of authentication	common criteria or further references according to the anti-counterfeiting solution chosen	
2- Adaptabilityand flexibility	To make sure that the solution can react to specific events and can put up with an one-off or permanent increase of load.	Dynamic reactivity parameters Adaptability parameters Typical and atypical treatment ability Traffic timetable	
3- Interoperability and upgrade capability of the verification tools	To ensure that the solution has extensibility		

3.1- several verification functions accessible with a single technical tool	To ensure that the verification applications don't interfere with each other	Verification functions, physical and logical, implemented Security means and security measures deployed	
3.2- hardware modularity	Assurance that upgrading the hardware will not impact negatively on technical tool performance and can be carried out with zero security vulnerability	Hardware extensibility (connections, formats, etc.) Compatibility imperatives between various equipments	
3.3- software interoperability	Assurance that software upgrades will not impact negatively on technical tool performance and can be carried out with zero security vulnerability	Type of operating system Security means and security measures deployed to handle new software Validation procedure	
4- Resistance of the elements of authentication	To ensure that the elements of authentication are capable of resisting challenges throughout every phase in their lifecycle		
4.1- operational resistance	Assurance that the elements of authentication are capable of resisting involuntary functional or natural environmental stress.	Temperature range Impact strength, vibration resistance, life.	
4.2- easiness to be integrated	To ensure that the elements of authentication remain unaltered by the production process and that they can be seamlessly integrated into the	Description of the methods system for matching authentication element with the products: processes modified, any additional constraints, etc.	

	production processes		
5- Useability of the technical tools	To ensure that the technical tools can easily deployed and used by the actors in the verification chain		
5.1- training	To define the needs in terms of pre-requisite skills or training required to implement the technical tools	Description of the training necessary for each level of intervention	
5.2- usage	To characterise deployability	Description of how the technical tool is to be deployed: storage conditions, installation, commissioning, etc.	
5.3- endurance	To specify the on-site operational time range in normal mode and/or in fallback mode	Autonomy in normal operation and in standby mode Autonomy in fallback mode	
5.4- usability engineering	To characterise on-site useability during the different verification phases	Site-wide useability under any circumstances: manual actions (keypad), angle-of-view, readability, audio, etc.	
5.5- Harmlessness	To ensure of the absence of negative known effects on human health	Respect of health and safety standards	
6- Reliability/solidity of the technical tools and verification systems	To ensure the operational performance of the data capture, technical tools and verification systems		
6.1- verification systems reliability	To characterise performance in terms of the distinguishing 'genuine from forged' authentication elements		

6.1.1- Absence of misleading interpretation	To characterize the ability to provide results preventing the possibility of misleading interpretations	Presentation of the results of verification of authentication elements	
6.1.1- rejecting shams	To characterise the ability of the capture tools to reject imitation authentication element	Read rates for nonconform elements	
6.1.2- false positives	To characterise the ability of the capture tools to handle production-related variations and tolerances in elements of authentication	Refusals rate for elements within the tolerance ranges Acceptance rates for elements outside the tolerance range	
6.2- MTBF	To specify the forecasted reliability performance of the capture tools	Formula-based calculations	
6.3- maintenance / preventive maintenance	To specify the conditions of regular and preventive maintenance required to ensure that the technical tools continue to work properly	Frequency schedule Types of maintenance operation	
6.4- ruggedness	To specify the environmental resistance characteristics or the usage conditions for the technical tools	Protection element Temperature range Resistance to impacts, falls	
7- Access rights for the various actors in the verification chain	To define the profiles of the actors in the verification chain who are cleared to access the technical tools. To define usage rights	Listing of potential users and conditions for use, management of the rights	
8- Ability to provide elements for the proof of counterfeiting	To specify the elements resulting from verification actions in the event of negative authentication		

8.1- recorded evidence of the verification	To specify the evidence generated for the right holder or its licensees and for the legal and administrative authorities	Result generated by the anti-counterfeiting solution: format, etc.	
8.2- tamper-proofing	To ensure that evidence resulting from the verifications is tamper-proof	Security measure to guarantee the integrity of the result	