INTERNATIONAL STANDARD

ISO 12931

First edition
2012-06-01

Performance criteria for authentication solutions used to combat counterfeiting of material goods

Critères de performance des solutions d'authentification utilisées pour combattre la contrefaçon des biens matériels

Reference number
ISO 12931:2012(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

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 12931 was prepared by Project committee ISO/TC 246, *Anti-counterfeiting tools*.

Introduction

The quantity and range of counterfeited material goods has been expanding rapidly over a decade, and is now no longer limited to luxury goods. The sale of counterfeit goods is prevalent in many developing countries and is becoming more common in the developed world. Individual manufacturers and rights holders are experiencing an increase in the number of counterfeiting attacks on their material goods. The internet is compounding the problem. These counterfeit goods do not necessarily offer the same guarantees in terms of safety and compliance with environmental measures and regulatory requirements, generating risk for consumers, patients, users and the distribution chain. They cause loss of earnings, job losses, and brand value damage for the companies and rights holders targeted as well as tax losses for governments. Counterfeiting increases the potential for false material good claims and litigation for the companies and distribution supply chain. Counterfeiting of material goods has become one of the major activities of organized crime, both within domestic markets and international trade and smuggling.

In order to prevent counterfeiting from plaguing their business, companies are increasingly using authentication solutions geared to their individual needs. It is important to specify the performance requirements for the solutions designed to support the fight against counterfeiting at both national and international levels. This will nurture greater confidence among consumers, support the security of the supply chain, and help the public authorities devise and implement preventive, deterrent and punitive policies.

Counterfeiting can include but is not limited to

— deceipt of the consumer,

— deceipt of the purchasers of new goods or replacement parts,

— infringement of intellectual property rights, and

— violation of national, regional or international laws.

Counterfeiting can include false claims regarding

— intellectual property rights,

— details of manufacture, and

— trade dress.

Counterfeiting needs to be kept separate from diversion.

The problem of counterfeiting is aggravated by the following factors:

— the market is increasingly global and the material goods are more complex;

— the global movement of material goods is increasing, and may use non-traditional channels.

Therefore it is more difficult for an inspector to recognize the characteristics of any given authentic material good.

Counterfeiting seeks to bypass legal provisions, including guarantees of conformity and quality, designed to enable professionals to release safe material goods onto the market in fair competition. Buyers do not necessarily pay all necessary attention to the material goods they are examining, particularly because of trust, lack of time, the temptation of attractive prices, or simply because they are unfamiliar with the material good itself. The authentication element provides a specific and more reliable method of determining if the item is genuine or a counterfeit good.

Establishing the authenticity of material goods, in other words recognizing whether it is genuine or fake, consists in checking whether the material good reproduces the essential characteristics of the authentic material good 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 material good's origin, and then to verify whether the suspect material good being challenged does objectively and concretely present these characteristics.

If there is any doubt as to the authenticity of a material good, it is the inspectors' role, once they have observed the characteristics of the suspect material good and/or authentication element, to examine whether these characteristics match those of the authentic material good and/or authentication element. The process involved is an essentially technical analysis using experience, authentication elements, authentication tools or a combination of these methods.

This International Standard has been drafted to pinpoint the objectives and boundaries required for industry-wide and services-wide application. This International Standard sets out the performance criteria for purpose-built authentication solutions. These authentication solutions are designed to provide reliable evidence making it easier to assess whether material goods are authentic or counterfeit.

This International Standard aims to integrate the performance requirements for authentication solutions into the material good's life cycle in any situation when required. Authentication is thus positioned as a feature of the material good and services life cycle against counterfeiting.

This International Standard is proposed to be part of a wider framework in related standards in the anti-counterfeiting field wherein the proof that a material good is authentic or counterfeit can be obtained by any means whatsoever, and it was not drafted or designed to define a sole means of authentication.

Performance criteria for authentication solutions used to combat counterfeiting of material goods

1 Scope

This International Standard specifies performance criteria and evaluation methodology for authentication solutions used to establish material good authenticity throughout the entire material good life cycle. It does not specify how technical solutions achieve these performance criteria.

This International Standard is intended for all types and sizes of organizations that require the ability to validate the authenticity of material goods. It is intended to guide such organizations in the determination of the categories of authentication elements they need to combat those risks, and the criteria for selection of authentication elements that provide those categories, having undertaken a counterfeiting risk analysis. Such authentication elements can be part of the material good itself and/or its packaging. The criteria applies to the material good and/or its packaging.

The performance criteria is considered by organizations in relation to their specific situation.

This International Standard is focused upon the authentication of material goods

— covered by intellectual property rights,

— covered by relevant national or regional regulation,

— with safety and public health implications,

— otherwise with a distinctive identity.

This International Standard focuses on material goods and is not intended to apply to, for example, goods used in the financial sector, official administrative papers, identity documents or to downloadable products.

This International Standard does not apply to technologies or systems designed for the tracking and tracing of material goods. Track and trace on its own is not an authentication solution and is therefore outside the scope of this International Standard.

This International Standard does not deal with economical criteria aiming to correlate performance and costs of the authentication solutions.

Some industries and services may have special regulatory requirements which would require additional functionality to supersede part(s) of this International Standard.

This International Standard is intended to contribute to an organization's understanding of its authentication needs, possible strategies, and challenges. It is intended to give the organization a set of criteria to analyse, specify and implement its authentication solutions.

The organization will determine the level of security assurance required for the selected authentication solution. The authentication solution provider is expected to comply with the risk and security requirements of the organization.

This International Standard is not intended to constrain the organization's choice of authentication technologies.

2 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

2.1
attack
successful or unsuccessful attempt(s) to circumvent an authentication solution, including attempts to imitate, produce or reproduce the authentication elements

2.1.1
internal attack
attack perpetrated by persons or entities directly or indirectly linked with the legitimate manufacturer, originator of the good or rights holder (staff of the rights holder, subcontractor, supplier, etc.)

2.1.2
external attack
attack perpetrated by persons or entities that are not directly or indirectly linked with the legitimate manufacturer, originator of the good or rights holder

2.2
authentic material good
material good produced under the control of the legitimate manufacturer, originator of the good or holder of intellectual property rights

2.3
authentication
act of establishing whether a material good is genuine or not

2.3.1
authentication element
tangible object, visual feature or information associated with a material good or its packaging that is used as part of an authentication solution

2.3.1.1
overt authentication element
authentication element which is detectable and verifiable by one or more of the human senses without resource to a tool (other than everyday tools which correct imperfect human senses, such as spectacles or hearing aids)

2.3.1.2
covert authentication element
authentication element which is hidden from the human senses until the use of a tool by an informed person reveals it to their senses or else allows automated interpretation of the element

2.3.2
authentication tool
set of hardware and/or software system(s) that is part of an anticounterfeiting solution and is used to control of the authentication element

2.3.2.1
stand-alone authentication tool
authentication tool which either is used to reveal a covert authentication element to the human senses for human verification, or which integrates the functions required to be able to verify the authentication element independently

2.3.2.2
on-line authentication tool
authentication tool which requires a real-time on-line connection to be able to locally interpret the authentication element

2.3.2.3
off-the-shelf authentication tool
authentication tool which can be purchased through open sales networks

2.3.2.4
purpose-built authentication tool
authentication tool dedicated to a specific authentication solution

2.3.3
authentication solution
complete set of means and procedures that allows the authentication of a material good to be performed

2.4
automated interpretation
authenticity is evaluated automatically by one or more components of the authentication solution

2.5
counterfeit, verb
to simulate, reproduce or modify a material good or its packaging without authorization

2.6
counterfeit good
material good imitating or copying an authentic material good

2.7
false acceptance rate
proportion of authentications wrongly declared true

2.8
false rejection rate
proportion of authentications wrongly declared false

2.9
forensic analysis
scientific methodology for authenticating material goods by confirming an authentication element or an intrinsic attribute through the use of specialised equipment by a skilled expert with special knowledge

2.10
human interpretation
authenticity as evaluated by the inspector

2.11
inspector
anyone who uses the authentication solution with the aim of authenticating a material good

2.12
integrated authentication element
authentication element that is added to the material good

2.13
integrity
the property of the unimpaired condition of the authentication element, the associated data, the information or the elements and the means for processing them

2.14
interoperability
degree to which an authentication solution is able to work together with other different tools

2.15
intrinsic authentication element
authentication element which is inherent to the material good

2.16
likelihood
chance of something happening

NOTE 1 to entry: In risk management terminology, the word “likelihood” is used to refer to the chance of something happening, whether defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically (such as a probability or a frequency over a given time period).

NOTE 2 to entry: The English term “likelihood” does not have a direct equivalent in some languages; instead, the equivalent of the term “probability” is often used. However, in English, “probability” is often narrowly interpreted as a mathematical term. Therefore, in risk management terminology, “likelihood” is used with the intent that it should have the same broad interpretation as the term “probability” has in many languages other than English.

[SOURCE: ISO Guide 73:2009, 3.6.1.1]

2.17
material good
manufactured, grown product or one secured from nature

2.18
material good life cycle
stages in the life of a material good including conception, design, manufacture, storage, service, resell and disposal

2.19
rights holder
physical person or legal entity either holding or authorised to use one or more intellectual property rights

2.20
risk analysis
process to comprehend the nature of risk and to determine the level of risk

NOTE 1 to entry: Risk analysis provides the basis for risk evaluation and decisions about risk treatment.

NOTE 2 to entry: Risk analysis includes risk estimation.

[SOURCE: ISO Guide 73:2009, 3.6.1]

2.21
robustness
ability of a system to resist to virtual or physical, internal or external attacks

NOTE 1 to entry: Particularly, in the context of this International Standard, it is the ability to resist attempted imitation, copy, intrusion or bypassing.

2.22
security
state of being free from danger or threats where procedures are followed or after taking appropriate measures

2.23
secret
data and/or knowledge that are protected against disclosure to unauthorised entities

2.24
specifier
person or entity who defines the requirements for an authentication solution to be applied to a particular material good

2.25
tamper evidence
ability of the authentication element to show that the material good has been compromised

2.26
track and trace
means of identifying every individual material good or lot(s) or batch in order to know where it has been (track) and where it is (trace) in the supply chain

3 General principles

3.1 Introduction

Authentication solutions come in a wide range of formats, from simple solutions to complex ones involving information technology architectures. A simple solution does not mean a weak solution as the most appropriate authentication solution for a material good will depend of the context of implementation and usage.

The technical, logistical and financial criteria involved in the selection of an authentication solution will depend upon numerous factors including

— characteristics of the authentication element(s),

— the verification levels and methods targeted,

— any required information system,

— security requirements,

— counterfeit resistance,

— the value of the material goods intended to be protected,

— counterfeiting risks throughout the material good's life cycle,

— integration and implementation requirements,

— role of packaging.

Authentication solutions should not affect the functionality and the integrity of the material goods.

A proper application of this International Standard relies on the observation of national, regional and international laws and regulations especially on privacy and safety.

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

Thus, in relation with the specification of the material good protection, an authentication solution is the result of a creation process followed by a verification process. The creation process consists of defining, generating and manufacturing the authentication elements and integrating them with the material good or its packaging. The verification process consists of checking the authentication elements along the distribution chain by trained people using human senses, tools or references. Those two processes are linked in a Plan-Do-Check-Act (PDCA) model and the actors involved form an integral part of the authentication solution.

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

As a strategy analysis, the main questions to be addressed by the rights owners are as follows.

— What are the counterfeiting issues, the consequences and likelihood of the counterfeiting threat?

— Which of my material goods are being counterfeited or have the potential to be counterfeited?

— In which locations are we experiencing counterfeiting and how are the counterfeits being distributed?

— What is the manufacturing and supply chain environment?

— How and by whom will the authentication process be performed?

— What is the impact of human error on the solution (process and authentication)?

3.2 Authentication process

The typical authentication solution is shown in Figure 1 and 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 detect the authenticity of the material good.

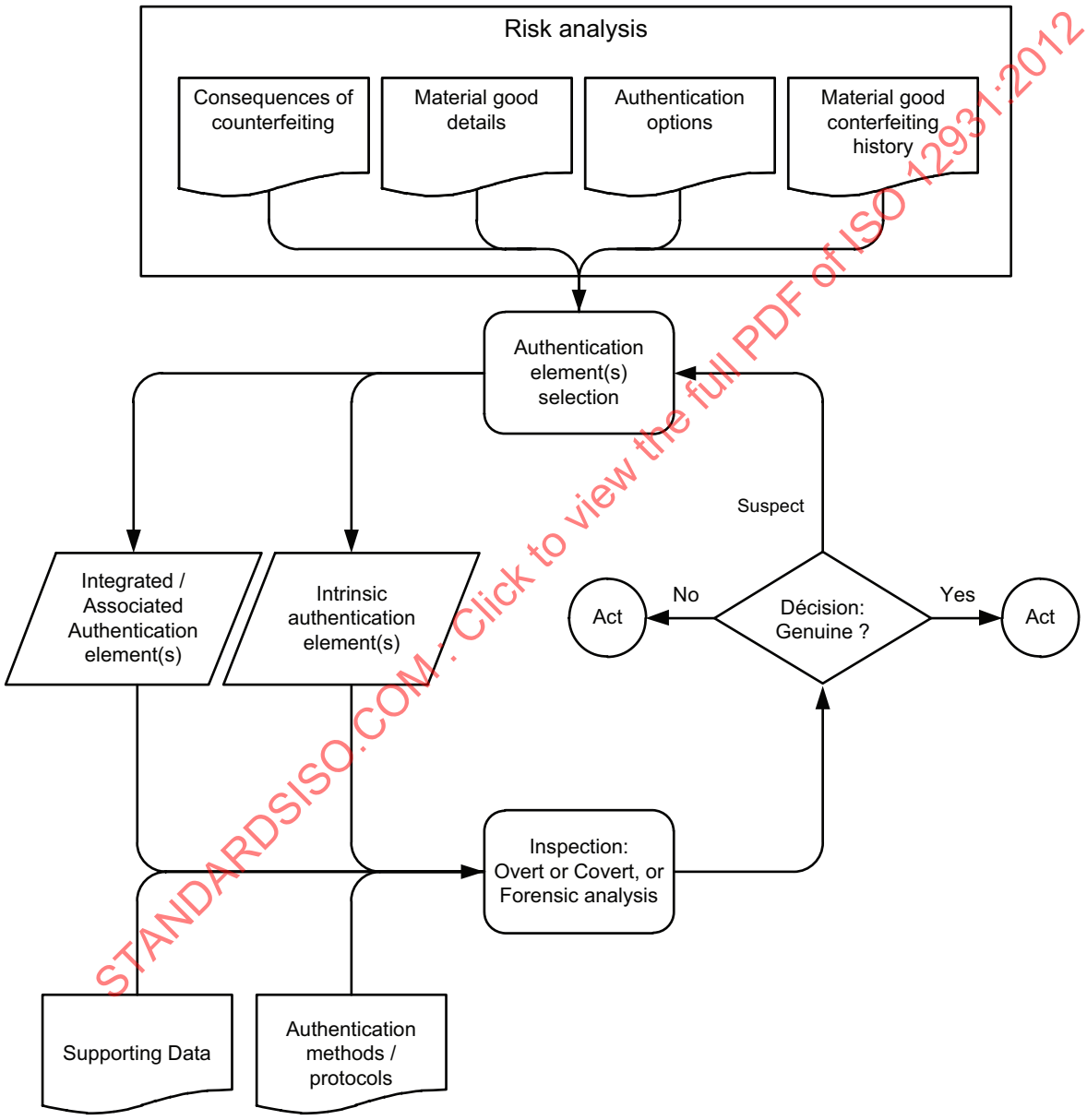

Figure 1 — Functional block diagram of a typical authentication solution

3.3 Performance requirements for authentication solutions

The aim of this International Standard is to

— establish common categorization of authentication solutions,

— establish an understanding how an authentication solution may constitute a more robust solution when layered and therefore individual authentication elements should be used in combination, and

— provide criteria for which type of solution can be used to authenticate in different verification scenarios.

Thus to assist users and potential users of authentication solutions to understand their functionality and selection criteria against their own risk analysis, which will facilitate the user's ability to

— run material good verifications anywhere, under all foreseeable circumstances and conditions of use, and

— define specific requirements for every desired level of security for their authentication solution.

3.4 Categorization of authentication solutions

This categorization is intended to provide a guideline for users and suppliers of authentication solutions that allow solutions to be compared or selected according to their characteristics. It is not intended to rank the solutions according to performance effectiveness. The environment of the examination helps to determine the choice of authentication solution(s).

The characteristics used in this categorization are based on the following considerations.

3.4.1 Provision of knowledge

Any authentication solution will require some knowledge to be provided to the inspector. Without the knowledge that a certain authentication solution has been applied to the material good in question, an inspector cannot inspect the associated authentication element. Without knowledge of the appropriate inspection procedure, he cannot adequately perform the authentication. The knowledge required can be subdivided into general knowledge (e.g., how a class of authentication elements appears to the inspector) and material good-specific knowledge (e.g., which particular authentication element has been applied to the material good being inspected). However, the right holder may control the intended audience of this knowledge, in particular of material good-specific knowledge. The following distinction is used for the categorization.

3.4.1.1 General audience

Knowledge about the authentication solution employed is made public, e.g., via advertisements, websites, or marketing materials.

3.4.1.2 Restricted audience

Knowledge about the authentication solution employed is made available only to a restricted group of people that have a need to know; this will usually include all those people who are professionally required to inspect the material good, and thus exclude those in the general audience. This approach is limited by the potential risk that the knowledge will leak from the intended audience and may ultimately become public knowledge; on the other hand, the security of an authentication solution can be substantially increased by restricting the availability of knowledge.

3.4.2 Inspection method

The process of inspection of an authentication element invariably involves some form of physical observation. The following distinction in this regard is used for the categorization.

3.4.2.1 Human senses

The inspection method makes use of the human senses.

3.4.2.2 Authentication tool

An authentication tool is employed to perform the required inspection and to display the result in some appropriate way for presentation to the inspector. The tool employed may either be field available tool or require the use of a laboratory equipment or similar environment.

Using these characteristics, the following set of basic categories can be established, as shown in Table 1 and further detailed below.

Table 1 — Characteristics of categories for authentication solutions

	Human senses	Authentication tool		Forensic analysis
		Off the shelf	Purpose built	
General audience	OVERT	COVERT[a]	—	—
Restricted audience	OVERT	COVERT	COVERT	COVERT
[a] See 3.4.4.2.				

Track and Trace technology when used alone is not considered to be an authentication solution and as such is not covered by this International Standard.

Annex B provides the specifier a tool with which to define the audience.

3.4.3 Categorization of authentication tools

When an authentication solution uses an authentication tool to inspect the authentication element, the technical tool can further be characterized by the following categories.

3.4.3.1 Mode of operation

Depending on how the authentication tool operates, two categories for its mode of operation can be distinguished.

3.4.3.1.1 Stand-alone

The authentication tool can operate and perform the inspection of the authentication element in complete autonomy (except for a source of electrical power where required).

3.4.3.1.2 Online

The authentication tool requires the use of a network connection to operate. The connection may be required, for instance, to send or receive data required to perform the inspection, or to request authorization to perform inspection of the authentication element.

3.4.3.2 Availability

Depending on how an authentication tool can be procured, two categories for its availability can be distinguished.

3.4.3.2.1 Commercial off-the-shelf

The authentication tool can be procured as a standard commercial item, often from more than one source.

3.4.3.2.2 Purpose-built

The authentication tool has been especially designed for authenticating one or several authentication elements; often, it is available only from a single source.

3.4.4 Categorization of authentication elements

3.4.4.1 Overt category

Overt authentication can be directly performed by an informed inspector and does not require any additional equipment to allow a feature to be verified as genuine.

Overt authentication elements are apparent to the human senses, most often sight, but touch is also used. Overt authentication elements are often therefore employed where a visual check is the only one immediately possible and this can be undertaken by informed inspectors, such as consumers, store clerks and check-out staff.

Ideally the inspector will have a genuine authentication element as a reference comparison.

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

3.4.4.2 Covert category

Covert authentication elements are not instantly recognizable or interpretable by the human senses. They require authentication tools and/or specialized knowledge to verify their presence and validity, either revealing themselves to the human senses (usually vision) or to the authentication tool. These tools can be stand-alone or require a connection to a network, they can be off-the-shelf or purpose-built. The result presented by an authentication tool might make a determination of the authentication element's authenticity, or the decision might be left to the inspector. Inspectors analysing these authentication elements may need some training.

Covert technologies exploit all kinds of physical, chemical or biological effects, as well as logical relationships. Electronically supported authentication elements use software or/and hardware based data and/or protocols securely related to the genuine material good for proof of authenticity.

Covert authentication solutions may be designed so that authentication can be performed in the field.

Particularly, where a covert application uses data that is or can be linked to a person, privacy principles and regulations shall be obeyed.

With the evolution of technology, a general audience will have the capacity to authenticate a covert authentication element, subject to specific conditions as determined by the authentication solution specifier.

3.4.5 Forensic analysis

Forensic analysis involves the use of knowledge and dedicated scientific methods to validate the authentication elements or intrinsic attributes of a material good. While forensic analysis 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.

To be acceptable by a legal authority, forensic evidence may need to be established by a trusted third party.

4 Performance criteria specification based on risk analysis

4.1 Introduction

This clause establishes the performance criteria for the selection of an authentication solution. Based upon these criteria the authentication solution specifier may determine what class or combination of categories of solutions meets the needs and requirements of the user.

The global performance of an authentication solution depends on the performance of each component and on the performance of the links between them. Tools performance, in particular their attack resistance shall be taken into consideration with the same importance as authentication element performance.

Risk is a function of consequences and likelihood of events. Risk assessment is an overall process of risk identification, risk analysis and risk evaluation (see ISO 31000). This clause defines the performance criteria, specification factors that are used by risk analysis systems.

The performance of any authentication element 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 ensure the implemented technology has not become obsolete or compromised by technological developments.

4.2 Performance criteria categories

This subclause defines the performance criteria of authentication solutions in the following different categories:

— physical characteristics;

— attack resistance;

— integration process;

— field/environmental function;

— implementation process.

A specifier may choose to adopt an authentication solution that combines several authentication elements working together to build proof. These elements may be of different types (overt, covert and forensic) and with different levels of accessibility. Regarding all the criteria, the more robust the solution and the greater the expertise of the inspector, the more reliable the result of the authentication process.

While the categories of criteria may be the same for different solutions, the use of different methodologies to authenticate is required. In recognition of this difference the criteria is separated into three clauses. Subclause 4.3 will describe the criteria for the authentication element; 4.4 will describe the criteria for the authentication tool; 4.5 will describe the criteria for authentication solution.

Annex A provides the specifier the grid with which to select the criteria.

4.3 Criteria for the selection of authentication elements

4.3.1 Physical characteristics

This performance criteria is linked to the physical characteristics of the authentication elements.

The readability of the authentication elements (either human or machine readable) is a key issue. Multiple factors shall be taken into consideration including: the characteristics of the material good, the user/inspector, the authentication environment and the authentication durability. All of these factors may be affected by the physical characteristics of the authentication elements. Among the physical characteristics, the following should be considered.

4.3.1.1 Static characteristics

— Size

— Thickness

— Weight

These characteristics have to be considered according to the material good: available space, compatibility, potential interference with material good features or process (see integration process characteristics, 4.3.3).

4.3.1.2 Dynamic characteristics

Authentication element's physical characteristics shall not be detrimentally affected by material good manufacturing, or during the storage, transport and integration processes.

This includes characteristics such as

— flexibility,

— viscosity,

— tear,

— tensile strength.

Therefore, the authentication element shall be chosen to take into consideration any of the process requirements involved in the production of the material good.

If process requirements alter or damage the authentication elements, they will become unusable and cause the material good 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 material good.

4.3.1.3 Durability characteristics

The following environmental conditions during subsequent processing, storage, or operation shall not affect the physical characteristics of the authentication element used for authentication in an adverse manner that might result in a malfunction of the authentication element over life cycle:

— mild environmental conditions (Climatic features such as temperature and humidity);

— harsh environmental conditions (Degradation features such as chemical action and radiation);

— mechanical use typical of the material good under consideration; and

— aging that may result in a malfunction of the authentication element over the life cycle of the material good.

The specifier of the authentication solution shall define the conditions of usage based upon the required risk analysis. In addition, the life cycle of the material good may have a significant impact in determining the durability of the authentication capability.

4.3.1.4 Health and Environmental Impact Characteristics

— Electromagnetic radiation

— Radioactivity

— Chemical composition and banning of some substances

— Migration of substances

— Recyclability

The potential environmental and health impact of authentication elements shall be considered, particularly in light of national, regional, international regulations.

4.3.1.5 Feature-linked physical characteristics

— Visibility

— Machine readable

— Tamper evidence

— Uniqueness (one-to-one, one-to-many)

A feature can be recognized as unique in two manners, one-to-one or one-to-many. A unique feature that authenticates a single item and is unique only to that item is recognized as one–to-one. A unique feature applied to several items is recognized as one-to-many.

4.3.2 Attack resistance

This performance criteria is linked to the attack resistance of the authentication elements.

The attack resistance of an authentication element is defined as the degree to which an authentication element is able to withstand the acts outlined in 4.3.2.1 to 4.3.2.7.

4.3.2.1 Reverse engineering and copy resistance

The element shall be resistant to reverse engineering. It shall be extremely unlikely to acquire enough information to be able to successfully create/generate/manufacture an authentication element and to use this element to circumvent the material good protection.

It shall require an extraordinary level of effort to accurately copy authentication elements. If an authentication element were to be copied, the authentication element should contain copy evident features apparent in the authentication process.

To avoid simulation and emulation it should not be possible to create some fake authentication element that could be interpreted as genuine by an inspector or by a tool.

4.3.2.2 Tamper resistance/Tamper evidence

The tamper resistance is the ability of the authentication element to resist the removal, alteration or substitution of the element from the material good or tis packaging.

A tangible or intangible form of interdependence between the authentication element and the material good it protects shall be developed. 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.

To generate tamper evidence the various forms of interdependence shall be affected by any (at least partly) serious attack, which is why an attack should 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 should be detectable during the verification protocol. To reduce the chance of a false positive, the interdependent characteristics should remain stable and resist changes in environmental conditions during the material good's life cycle.

4.3.2.3 Alteration resistance

The authentication element should withstand modification of its characteristics or the modification of the information contained within the element. In the event the element is circumvented, detection of the attempt should be evident to the inspector.

4.3.2.4 Side channel resistance

It should not be possible to capture any secret information or determine characteristics of the authentication element through analysis of its physical behaviour in any environmental circumstances,

4.3.2.5 Interception of communication

It shall not be possible to gain attack-sensitive information by intercepting the communication between the authentication element and any tool required to read or verify the element. Thus, the authentication element either shall not communicate any attack-sensitive information with the tool or the information exchange shall be secured.

4.3.2.6 Obsolescence

An evaluation shall be conducted to determine the potential longevity of the authentication element, the degree the element will remain an effective solution, and the availability of the technology and support in the future.

4.3.2.7 Not uncontrolled reuse

It shall not be possible to reuse the authentication element without authorization.

4.3.3 Integration process

The performance criteria are linked to the integration process of the authentication elements with the material good to be protected.

4.3.3.1 Security

— Security policy

During the integration process recognized security process and controls shall be implemented.

— Supply chain security

An evaluation of supply chain components shall be performed to ensure compliance with all security policies and procedures.

4.3.3.2 Manufacturing

4.3.3.2.1 Availability

A determination shall be made to ensure that the integrator can meet the production and supply requirements for the authentication element and its integration to the material good or its packaging.

4.3.3.2.2 Compatibility

— Material good/packaging

— Process

— Logistics

The authentication element shall be compatible with the material good or its packaging. The impact of the authentication element on the manufacturing and distribution processes shall be evaluated.

In the selection of authentication technologies the possibilities of bulk reading requirements and their potential conflicts shall be taken into consideration.

4.3.3.2.3 Integrity

The machines involved in the manufacturing shall be secured so that no access to secure information is possible. Any attempt to hack or tamper these machines shall be reported to appropriate authorities.

4.3.3.3 Compliance

Independent audits should be conducted to ensure the responsible parties that all of the integration requirements are being met and can be verified.

4.3.3.4 Training

Training for all involved parties shall be considered in all phases of the integration process to meet the requirements of the authentication solution provider and the authentication solution specifier.

4.4 Attack resistance criteria for the selection of authentication tools

4.4.1 General

The attack resistance of an authentication tool is defined as the degree to which an authentication tool is able to provide the properties outlined in 4.4.2 to 4.4.11.

NOTE Environmental and other conditions for the operation of the authentication tool are covered in 4.5.

4.4.2 Secret recovery, simulation and emulation

The authentication tool shall be resistant to attacks which can be used to recover secret or sensitive information that could lead to the ability to create/generate/manufacture an authentication element.

To avoid simulation and emulation it shall not be possible to create a fake authentication tool that could be considered as genuine by an inspector. This goal can be achieved by using a calibration method in order to check if the authentication tool is genuine and operational.

4.4.3 Tamper resistance/Tamper evidence

The tools shall be protected and/or react to any physical attempt of deviation aimed to capture information that is processed or transferred. Any detected attempt to tamper with these tools shall be reported to the appropriate authorities.

4.4.4 Alteration resistance

The tools shall be protected and/or react to any logical attempt of deviation aimed to capture information that are processed or transferred. Particularly it shall not be possible to use this information to successfully query databases with unauthorised tools.

4.4.5 Side channel resistance

It shall not be possible to capture any confidential data or characteristics of the authentication tool through analysis of its physical behaviour or interaction with the authentication element in any environmental circumstances.

4.4.6 Interception of communication

The authentication tool should be protected against any unauthorised communication between the authentication element and the tool and between the tool and the remote components of the authentication solution.

Securing all communication shall be considered during the authentication process, and during any kind of communication needed to upload or download information, provide updates or alarms.

4.4.7 System security

If a reference database is used for authentication it shall be protected against any intrusion. Attempts, and in worst case successful intrusion, shall be reported to the appropriate authorities.

4.4.8 Security of database access

Any access to a database used for the authentication process shall be protected by authentication of the inspector or both inspector and tool.

4.4.9 Redundancy/Back up

Although security measures may be implemented, redundant databases should be considered to prevent a successful attack attempt. Furthermore, a back up system (data and redundancy service) should also be considered to avoid interruption of service.

4.4.10 Obsolescence

The obsolescence of tools shall be managed so that the introduction of new tools in an authentication solution may be possible while maintaining the level of security of the solution

The obsolescence of IT equipment shall be managed so that backward compatibility and level of security are guaranteed for a period of time to be specified by the right holder. This concerns either the information related to authentication elements stored in databases or any equipment used to make the authentication solution work.

4.4.11 Assessing of vulnerability and resistance of authentication tools

The attack resistance of a solution is determined by assessing its vulnerability and resistance to the types of attacks (threats) identified above and based upon the risk analysis on the material good (see ISO 31000, ISO 15408, ISO/IEC 27002).

4.5 Criteria for the selection of authentication solutions

4.5.1 General

This set of criteria is related to the conditions where the authentication process is performed.

4.5.2 Field environmental function

This performance criteria is linked to the function of the authentication solution in the field, it is a consideration of operating conditions.

4.5.2.1 Required resources

The authentication solution may require various resources for its operation. Among those to be considered are provisions of

— power,

— communications,

— facilities.

4.5.2.2 Environmental conditions

The environmental conditions outlined in 4.5.2.2.1 to 4.5.2.2.6 shall be considered.

4.5.2.2.1 Temperature

Hot, moderate, cold

4.5.2.2.2 Humidity

Dry, moisture, wet

4.5.2.2.3 Dirt

Clean, dusty, muddy

4.5.2.2.4 Electromagnetic radiation

4.5.2.2.5 Electrostatic and magnetic fields

4.5.2.2.6 Air pressure

4.5.2.3 Hazardous conditions exposure

— Chemical, radioactive

— Explosive atmosphere

4.5.2.4 Factors causing deterioration during normal usage

— Abrasion

— Dirt

4.5.2.5 Ergonomics

The authentication process should be as intuitive as possible, in particular when intended to be used by untrained inspectors. Human senses may be enhanced or a tool may be adapted to accommodate authentication under all specified conditions.

4.5.2.5.1 Lighting conditions

A determination of the lighting conditions under which the authentication element and tool are expected to function shall be made. Lighting conditions should not inhibit the reading of the authentication elements or the reading of the result if the control is done with the usage of a tool.

4.5.2.5.2 Rain/Humidity/Snow

A determination of the rain/humidity/snow conditions under which the authentication element and tool are expected to function shall be made. Weather or humidity conditions should not inhibit the reading of the authentication elements or the reading of the result if the control is done with the usage of a tool.

4.5.2.5.3 Temperature

A determination of the temperature conditions under which the authentication element and tool are expected to function shall be made. If the control has to be operated under severe temperature conditions, ergonomic of the tool may be adapted to inspectors' personal equipment and clothing.

4.5.2.5.4 Wind

A determination of the wind conditions under which the authentication element and tool are expected to function shall be made. Wind should not inhibit the application of the authentication solution, the usage of a respective tool and/or the analysis of the investigation results.

4.5.2.6 Authentication parameters

4.5.2.6.1 Authentication cycle time

The necessary time to process an authentication shall be stated.

4.5.2.6.2 Frequency

The number of successive accurate authentications per unit of time by the solution shall be stated.

4.5.2.6.3 Concurrent authentication

The dependency of response time on the number of concurrent authentications shall be stated (this criterion is relevant only for online solutions).

4.5.2.6.4 Response time

The necessary time to get an authentication result shall be stated.

4.5.3 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 material good being protected. Multiple considerations need to be made to review the environmental factors affecting both the material good and the solution. In addition an evaluation shall be made to determine the life cycle capability of any authentication tool used in the control process. Such considerations may include potential obsolescence of the tool, technological obsolescence of the solution, company and support systems failures, redundant authentication elements and their positioning on the material good or its packaging.

With material goods of a short life cycle this evaluation may have minimal forecast requirements. Conversely, material goods with a significant longevity and/or critical performance requirements may require extensive evaluation and unique solutions and partnerships to guarantee the security of data during the life cycle.

4.5.4 Implementation process

The following performance criteria are linked to the implementation process of the authentication solution.

4.5.4.1 Security policy

The overall security policy for the authentication solution shall be clearly established. This concerns all the components of the solution involved, the links between them and the processes.

It also includes the security of the supply chain and involved information technologies.

The security policy shall be in accordance with relevant international or national standards and resolutions, or recognized industry practices.

4.5.4.2 Compliance

4.5.4.2.1 Compliance with regulations

The authentication solution shall be compliant with all existing regulations by governmental or regulatory agencies. Special consideration shall 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 and privacy regulations which have to be taken in account.

4.5.4.2.2 Compliance audit to ensure security practices and quality procedures

Security assurance and quality procedures, audited for compliance, shall be a criterion in the selection of an authentication solution. The audits should be performed according to relevant international or national standards, or recognized industry practices, by approved auditors or other authorities.

4.5.4.3 Operation

4.5.4.3.1 Start time

The authentication solution start up time (cold start or wake up) shall meet requirements of the solution specifications.

4.5.4.3.2 Process adaptability

It should be possible to adapt the authentication protocol to accommodate an increased volume of authentication.

4.5.4.3.3 Upgrade capability

The authentication solution should be upgradable without compromising the effectiveness of authentication solution.

4.5.4.3.4 Accountability and quality control

Procedures shall be implemented to verify the production of authentication elements in terms of quality and quantity of authentication elements and tools according to the solution specifications.

4.5.4.3.5 Multiuse capability

It may be advantageous to create a single tool capable of performing multiple authentication operations or functions. If a tool is used for verification of different material goods at the same time, the verification of one material good shall not interfere with the verification of the other material goods.

4.5.4.3.6 Sensibility of results

The acceptable rates of false acceptance and false rejection shall be defined by the specifier. These rates shall stay within the limits of the variation of the environmental operational conditions defined by the manufacturer.

4.5.4.3.7 Normal/fallback modes

For tools with their own power source or tools that operate in online mode, it shall be determined if a mode of operation with reduced functionality is acceptable. This determination should consider whether there are different levels of such modes of operation (low battery, missing network, etc.) or an alternative protocol that may access another type of authentication element, or separate backup solution. See 4.5.2.6, Authentication parameters. The reliability, mean time between failures, calibration and preventive maintenance of the components of the authentication solution should be considered to obtain the best quality of service.

4.5.4.3.8 Tool supply environment

The performance of tool supply environment and maintenance shall be considered, particularly in terms of

— availability,

— repair centre, and

— security related to tool supply chain.

4.5.4.3.9 Training

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. According to the access level defined, training is adapted.

The solution may describe the necessary training policy for each level of inspectors. Regular training updates may be required.

4.5.4.3.10 Health and Environmental

The potential impact of the solution on human health and environment should be considered.

5 Effectiveness assessment of the authentication solution

5.1 General

The performance of an authentication solution depends upon a proper risk analysis and criteria analysis that establishes a set of compliance specifications. Effectiveness assessment is a means to evaluate that a solution is complying with the established standards and if the solution is providing a measurable result. In addition to the overall solution effectiveness assessment should be established based on the specification for each of the criteria categories. Authentication solutions are a key means for detecting counterfeits and therefore support investigation and enforcement against counterfeiting and provide increased corroborative evidence. They also may deter counterfeiting by making it technically or financially unattractive to the counterfeiter.

It is not intended to be all inclusive or provide assessment metrics for the diverse multitude of possible authentication solutions.

5.1.1 Authentication solution effectiveness assessment

An assessment 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:

a) The material good is already on the market and is counterfeited

In this condition a material good is being counterfeited and the amount of counterfeiting may be known or unknown to the material good supplier. If the level of counterfeiting is known, then an effectiveness assessment 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. If the level of counterfeiting is unknown then an estimate of this amount needs to be established by research and/or statistical analysis. Based upon that analysis, estimation can be made of the effectiveness of the solution.

b) The material good is already on the market and no fake is detected

This material good's 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 of the good;

— an effective solution is already in place; or

— adequate research or reporting has not been done to determine if the goods are being counterfeited.

A risk analysis should be conducted to determine the threat of counterfeiting, and if there are financial, legal, social, health, safety or regulatory issues that shall be considered to determine if an authentication solution is necessary for the material good. The ability to create an effectiveness assessment for a solution that is used as a protective means or that no counterfeits are being detected is a difficult task that will require evaluation based upon the above factors.

c) The material good is not yet on the market

Prior to the introduction of a material good to the market a risk analysis should be performed to determine the likelihood of counterfeiting, and if there are financial, legal, social, health, safety or regulatory issues that require the implementation of an authentication solution. Effectiveness assessments of the solution can be derived based upon the above two categories.

When the material good is already on the market, the variation of the sales curve could reflect an evolution of the counterfeiting situation. But the response to counterfeiting issues needs more indicators to be efficient, adding that external (non technical) actions could have caused the variation.

Defining a standard that would encompass all of the unique effectiveness assessments protocols as well as authentication protocols themselves is not feasible. This subclause describes the key points to consider by authentication solution specifiers to define their own effectiveness assessment protocols.

Effectiveness assessment is the evaluation of the selected solution to meet the requirements of the selection criteria, that is, how well the selected solution meets each of the following categories of criteria:

— Physical characteristics

— Attack resistance

— Integration process

— Field/Environmental function

— Implementation process

The assessment of effectiveness can be done by the following evaluations.

— Evaluation of the physical characteristics

Does the solution meet each of the specified physical characteristics: dimension, tensile strength, dimensional stability, flexibility, etc. Are these characteristics measurable and definable in a specification? Can they be maintained consistently to meet quality assurance levels?

— Evaluation of the attack resistance

Does the solution meet the specified attack resistance criteria: copying, hacking, tampering, etc. Are these characteristics measurable and definable by specification? Can they be maintained consistently to meet quality assurance levels?

— Evaluation of the integration process

Based upon all of the physical characteristics is the integration process capable of successful integration of the solution? Are these characteristics measurable and definable by specification? Can they be maintained consistently to meet quality assurance levels?

— Evaluation of the field/environmental function

Does the solution meet the field/environmental function criteria: environmental conditions, hazardous conditions, etc. Are these characteristics measurable and definable by specification? Can they be maintained consistently to meet quality assurance levels?

— Evaluation of the implementation process

Based upon the all of the characteristics, is the implementation process capable of successful implementation of the solution? Are these characteristics measurable and definable by specification? Can they be maintained consistently to maintain the level of authentication required by the specifier?

The effectiveness assessment of the solution can be determined based upon an overall evaluation of the criteria selection process, the counterfeit environment of the material good, and the expectations of the risk analysis.

5.2 Effectiveness assessment in manufacturing of authentication elements

As in every process of manufacturing, the manufacturing of authentication solution shall comply with quality requirements. This can be linked to the quality manual of the authentication solution providers, including its subcontractors and suppliers if any. Quality audits are customary in all sectors of industry.

For authentication solutions, security issues have to be also addressed. This means that all the processes from authentication element creation to the shipment of the protected authentic material goods shall be considered. Those processes, which lack security assurance protocols and procedures, can impact the global effectiveness of the authentication solution. Security assurance procedures therefore shall be described and audited.

Discrepancy of tolerances and variations in quality of the production or of the integration of the authentication elements to the material goods will impact the true/false decision of the inspector.

Effectiveness assessments can be made with an evaluation of the

— number of false rejections in final control of production, meaning that the authentication elements are out of tolerance, or an anomaly in the process makes the authentication element unreadable,

— number of false rejections on site, meaning that the authentication element's characteristics or association with the material goods are not stable, and

— 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.

5.3 Effectiveness measurement in the normal verification/authentication situation

Evaluation in the normal control situations may concern

a) the inspector(s)

   1) identification/authentication access rights

   2) training

b) the tool

   1) authentication activity

   2) reduced functionality

   3) maintenance, calibration

   4) downloads

   5) tampering

c) the connections and data exchanges (if required)

   1) successful and denied logins

   2) quality of service

d) the results

   1) sampling rates

   2) number of true/false detections

   3) number of authentication elements non interpretable ("don't know")

Depending on the type of authentication solution implemented, these indicators could be issued through automated data collection or through declaration from the inspectors.

5.4 Effectiveness assessment in the emergency verification/authentication situation

In case of emergency when counterfeiting detection 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.

Assessment of effectiveness is then the key element to check the efficiency of the reaction.

5.5 Summary of effectiveness assessments

Effectiveness assessment of the authentication solution is dependent upon the solution specifier's requirements and therefore unique to each set of specifications. This clause provides the user of this International Standard some general guidance on how the effectiveness of solutions might be measured. It is not intended to be all inclusive or provide assessment metric for the diverse multitude of possible authentication solutions.

It is important to recognize the effectiveness assessment of the solution is a difficult task and involves an evaluation of the multiple criteria elements of the selection process as outlined in this International Standard. The assessment metric may be as simple as a yes or no answer, or as complex as any design specification for an engineered device. In many cases the assessment metric will simply be: does the solution or authentication element do what it is intended to do during the authentication process?

It is not an effective measure of the solution to measure only the perceived effectiveness of the authentication element. All of the processes should be evaluated. A perceived highly effective authentication element may fail the authentication process if it has not been evaluated against the specifications derived from criteria described within this International Standard.