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.

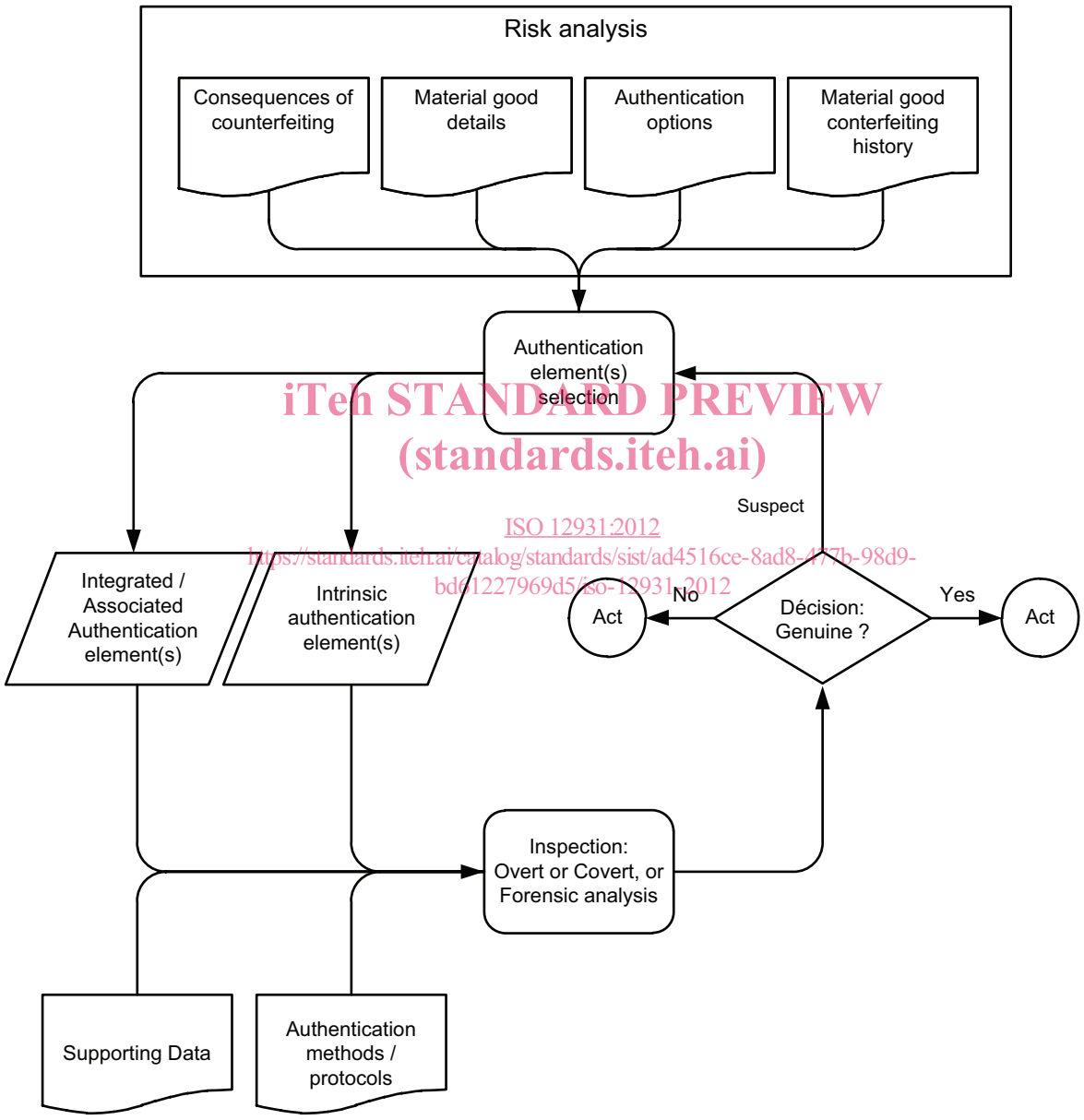

Figure 1 — Functional block diagram of a typical authentication solution

3.3 Performance requirements for authentication solutions

The aim of this International Standard is to

— establish common categorization of authentication solutions,