INTERNATIONAL STANDARD

ISO 22383

First edition
2020-09

Security and resilience — Authenticity, integrity and trust for products and documents — Guidelines for the selection and performance evaluation of authentication solutions for material goods

Reference number
ISO 22383:2020(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: 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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 292, *Security and resilience*.

This second edition cancels and replaces the first edition (ISO 12931:2012), which has been technically revised. The main changes compared with the previous edition are as follows:

— it has a new ISO number and title, and is now included in the ISO 22300 family of standards;

— its terminology mirrors ISO 22300;

— relevant standards published since the first edition have been added as references.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

Since the issuance of the first edition of this document in 2012, the quantity and range of material goods counterfeited or otherwise subject to product fraud continues to expand, and now affects many consumer goods and spare parts.

The sale of counterfeit goods, as well as falsified, illegally copied or illicitly traded products, 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 companies and targeted rights holders as well as tax losses for governments. Counterfeiting increases the potential for false material goods claims and litigation for companies and distribution supply chains. 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 and other types of product fraud, rights owners, institutions and governmental regulators are increasingly demanding and implementing authentication solutions geared to specific 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 promote greater confidence among consumers, support the security of the supply chain, and help public authorities devise and implement preventive, deterrent and law enforcement policies. In addition, the growth of global trade and the reduction of physical controls at borders has increased the risk of more counterfeited products in circulation. This document will contribute to further strengthen such controls by enabling faster and more reliable evidence of the authenticity and integrity of material goods.

Product fraud includes, but is not limited to, counterfeiting, adulteration, tampering, substitution and simulation.

Product fraud impact can include, but is not limited to:

— deception of the consumer;

— deception of the purchaser of new goods or replacement parts;

— infringement of intellectual property rights;

— violation of national, regional or international laws;

— false claims regarding:

  — intellectual property rights;

  — details of manufacture;

  — trade and origin details;

  — identification codes and/or authentication elements.

The problem of product fraud is aggravated by the following factors:

— the market is increasingly global;

— the material goods and their supply chains are more complex;

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

Counterfeiting needs to be kept separate from diversion.

It can be difficult for an inspector, be it a dedicated professional or any citizen or consumer, to recognize the characteristics of a 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 into the market in fair competition. Buyers do not necessarily pay all the attention needed to the material goods they are examining, particularly due to 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 whether the item is genuine or a counterfeit good.

Establishing the authenticity and integrity of a material good, in other words recognizing whether it is genuine or fake or otherwise subject to fraudulent activities, requires checking whether it reproduces the essential characteristics of the authentic material good, to help establish whether or not there has been an infringement.

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 verify 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 document has been drafted to pinpoint the objectives and boundaries required for industry-wide and services-wide application. It sets out the performance criteria for purpose-built authentication solutions.

These solutions are designed to provide reliable evidence, making it easier to assess whether material goods are authentic and have not been counterfeited, altered, mimicked, replaced, refilled, tampered or subject to other types of product fraud.

This document integrates the performance requirements for authentication solutions. The material good's life cycle needs to be considered. Whereas authentication of fast-moving consumer goods often concentrates on packaging, authentication solutions of material goods with longer life cycles instead aim at the material good itself, throughout its life cycle.

This document is part of a wider framework of related standards. It was not drafted or designed to define any exclusive means of authentication.

Experience shows that advancements in technologies are exploited by counterfeiters to make counterfeited products less detectable. At the same time, new authentication technologies (e.g. material, digital and combined) can give law enforcement inspectors, legitimate economic operators and consumers better means to detect counterfeits and act accordingly. This document is applicable irrespective of the authentication technology used and recommends ways to stay ahead of fraudsters.

This document therefore includes:

— a common categorization of authentication solutions;

— an understanding of how an authentication solution can constitute a more robust solution when layered, and therefore it promotes the use of individual authentication elements in combination;

— the role of tamper resistance and tamper evidence as part of an authentication solution;

— criteria for the types of solution that can be used to authenticate in different verification scenarios;

— methods to enable material good verifications in all intended locations, circumstances and conditions of use;

— requirements and evaluation criteria on security for the authentication solutions.

The main topics of this document can be represented as a Plan-Do-Check-Act (PDCA) cycle, see Figure 1.

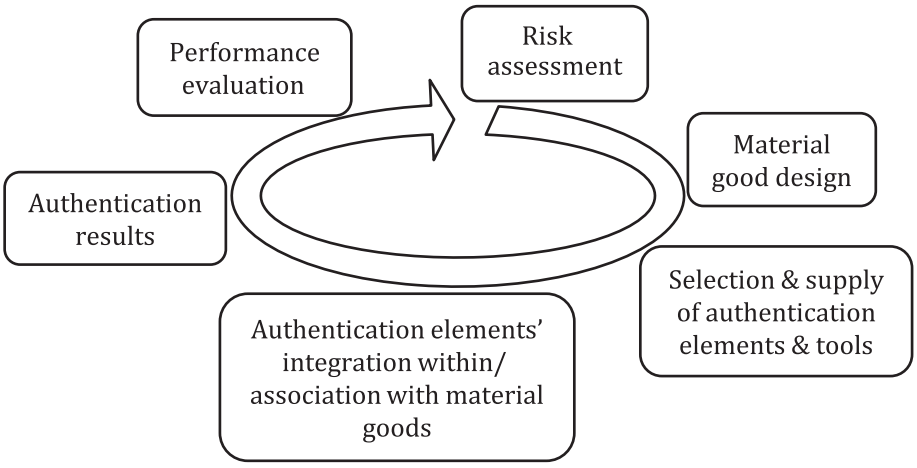

Figure 1 — Sequence of the main topics

Security and resilience — Authenticity, integrity and trust for products and documents — Guidelines for the selection and performance evaluation of authentication solutions for material goods

1 Scope

This document gives guidelines for performance criteria and an evaluation methodology for authentication solutions that aim to unambiguously establish material good authenticity and integrity throughout an entire material good's life cycle. It focuses on the authentication of a material good and, if appropriate, its components, parts and related data:

— covered by intellectual property rights;

— covered by relevant international, regional or national regulations;

— with counterfeiting-related implications;

— otherwise with a distinctive identity.

This document is applicable to all types and sizes of organizations that require the ability to validate the authenticity and integrity of material goods. It will help organizations to determine the categories of authentication elements they need in order to combat counterfeiting-related risks, and the criteria for selecting authentication elements, after having undertaken a counterfeiting risk assessment.

Authentication solutions can be used in areas such as anti-counterfeiting, prevention of product fraud and prevention of diversion.

This document does not specify economic criteria aiming to correlate performance and costs of the authentication solutions.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies:

ISO 22300, *Security and resilience — Vocabulary*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 22300 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

3.1
attack
successful or unsuccessful attempt(s) to circumvent an authentication solution, including attempts to imitate, produce or reproduce the authentication elements

3.2
covert authentication element
authentication element that is hidden from the human senses until the use of a tool by an informed person reveals it to their senses or else allows an automated interpretation of the element

[SOURCE: ISO 22300:2018, 3.58, modified — The definition has been rephrased.]

3.3
integrity
property of safeguarding the accuracy and completeness of assets

Note 1 to entry: Assets relate to material goods and its primary packaging.

Note 2 to entry: Integrity also concerns the associated data, information or the elements and means for their processing.

[SOURCE: ISO 22300:2018, 3.123, modified — Notes 1 and 2 to entry have been added.]

3.4
raw material
any element, constituent or part of a material good

3.5
rights holder
physical person or legal entity either holding or authorized to use one or more intellectual property rights

[SOURCE: ISO 22300:2018, 3.198, modified — "physical person or" has been added.]

3.6
security
state of being free from danger or threats where procedures are followed or after taking appropriate measures

[SOURCE: ISO 22300:2018, 3.223, modified — "where procedures are followed or after taking appropriate measures" has been added.]

3.7
simulation
imitative representation of the functioning of one system or process by means of the functioning of another

3.8
specifier
person or entity who defines the requirements for an authentication solution to be applied to a particular material good

[SOURCE: ISO 22300:2018, 3.246, modified — "person or" has been added.]

3.9
tamper evidence
ability of the authentication solution or the authentication element to show that the material good has been compromised

[SOURCE: ISO 22300:2018, 3.254, modified — "the authentication solution or" has been added.]

3.10
track and trace
means of identifying every individual material good or lot(s) or batch in order to know where it is at a given time (track) and where it has been (trace) in the supply chain

[SOURCE: ISO 22300:2018, 3.264, modified — "where it is at a given time (track) and where it has been (trace)" has replaced "where it has been (track) and where it is (trace)".]

3.11
verification
confirmation, through the provision of evidence, that specified requirements have been fulfilled

Note 1 to entry: Verification can include checking that a unique identifier exists and is valid within an object identification system.

4 Principles

4.1 General

The organization should select the most appropriate authentication elements to form an authentication solution for a material good, based on a risk assessment and on the context of implementation and usage.

When selecting an authentication solution, the organization should consider the technical, logistical and financial criteria, which will depend on numerous factors including:

— the characteristics of the authentication element(s);

— verification methods;

— any required information system;

— security requirements;

— counterfeit resistance;

— resilience against tampering;

— value of the material goods intended to be protected;

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

— integration and implementation requirements;

— the role of packaging;

— evidence of forged, counterfeited or copied features.

The organization should not select an authentication solution that affects or alters, in an uncontrolled way, the intended functionality and the integrity of the material goods.

NOTE Authentication elements can be part of the functionality of a product, for example, in the security-by-design approach whereby the security is embedded at the stage of product conception.

The organization should be aware of applicable laws and regulations especially on privacy and safety.

In order to establish an authentication solution for a material good, a creation process must be followed by an inspection process. The creation process consists of defining, generating and manufacturing the authentication elements and integrating them with the material good or its packaging. The inspection process includes verifying the authentication elements along the distribution chain by trained people using human senses, tools or references. Those two processes are linked in the PDCA cycle and the actors involved form an integral part of the authentication solution.

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 re-channel the data, sample or material good towards a structure offering expert analysis for an off-line diagnosis.

The level of performance of an authentication solution should 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 and threats?

— What is the likelihood and what are the consequences of the counterfeiting risks on my products, organization and business?

— Which of my material goods (or its raw materials) 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 material good manufacturing and supply chain environment and risks of counterfeiting?

— What is the raw materials' manufacturing and supply chain environment and risks of counterfeiting?

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

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

4.2 Security-by-design process for authentication solutions

The organization should follow the process diagram given in Figure 2 when designing its authentication solution. This process includes a proper analysis of the risks associated with the characteristics of a material good, including its raw materials, the options for its authentication, and the consequences and history of counterfeiting acts such as adulteration, tampering, substitution/refill, simulation, cloning or diversion.