INTERNATIONAL STANDARD

ISO 16678

First edition
2014-07-01

Guidelines for interoperable object identification and related authentication systems to deter counterfeiting and illicit trade

Lignes directrices pour l'identification interopérable d'objets et systèmes d'authentification associés destinés à décourager la contrefaçon et le commerce illicite

Reference number
ISO 16678:2014(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.

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 on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is ISO/TC 247, *Fraud Countermeasures and Controls*.

Introduction

This International Standard makes three foundational assumptions. First, detecting counterfeit objects is a complex and often difficult task; second, accurate identity information about the object in question simplifies the counterfeit detection process; and third, accurate identity information is often difficult and hard to find.

The main objective of this International Standard is to simplify access and delivery of accurate identity information to trusted agents (inspectors) in the process of authenticating objects.

To accomplish this objective, the document provides guidance intended to make object identity information easier to find and use. Identity data and information can be found in many places, including verification and authentication systems. Granting inspectors access to identity information helps them detect counterfeits. Helping inspectors find the identity information helps them detect counterfeits. This leads us to the conclusion that:

> Improving interoperability of object identification and related authentication systems should make these systems easier for inspectors to use. Improving ease-of-use should increase inspector utilization of the multitude of systems containing accurate information, thus, increasing detection of counterfeits and reducing the losses caused by counterfeiting.

This International Standard focuses attention on routing requests for object information to the appropriate authoritative service and then routing responses back to inspectors.

Object identification systems commonly use Unique Identifiers (UID) to reference or access object information. UID can be assigned to a class of objects or can be assigned to distinct object. In either case, the UID can enhance detection of counterfeiting and fraud, although UIDs assigned to single instances can be more efficient. The International Standard is organized into six (6) major sections:

- **Scope:** Declares the limits of this International Standard as providing only guidance and advice. There are no requirements in this International Standard.
- **Terms:** Defines the contextual meaning of important terms as used in this International Standard such as “trusted agent”, “inspector”, and “semantic interoperability”.
- **Overview:** An outline of how object information is used to detect counterfeits.
- **Key Principals:** The concepts and values that have influenced the guidance.
- **Guidance:** Recommendations that should improve interoperability of systems capable of providing object information to inspectors.
- **Informative Annexes:** Specific examples that illustrate some of the concepts presented in this International Standard.

Desired Outcomes

The more validation or authentication solutions are used, the more effective they become at detecting and deterring frauds such as counterfeiting and illegal diversion. This International Standard intends to enable reliable and safe object identification to deter introduction of illegal objects to the market.

One goal of this International Standard is to describe a framework in which disparate object identification solutions are interoperable and trust is increased, and therefore will be used more frequently. The framework shall also include solutions which simply detect some counterfeits without authenticating products. Likewise, the framework shall also include a solution which only evaluates an authentication element.

Since we also anticipate that the object identification systems themselves will also be counterfeited and copied, this International Standard establishes a method to formally prove that a remote description of an object can be trusted. Consideration is given to prevent interference between different independent implementations of such systems and to allow an unambiguous unique identification reference to service multiple uses and applications.

The theory supporting the design of the system is that a lack of trust and lack of interoperability introduces ‘friction’ for users. By reducing this friction, there will be greater awareness and usage, and therefore greater detection and deterrence of fraud.

Guidelines for interoperable object identification and related authentication systems to deter counterfeiting and illicit trade

1 Scope

This International Standard describes framework for identification and authentication systems. It provides recommendations and best practice guidance that include

- consequences and guidance of
  - management and verification of identifiers,
  - physical expression of identifiers, and
  - participants' due diligence.
- vetting of all participants within the system,
- relationship between the unique identifier and possible authentication elements related to it,
- questions that deal with the identification of the inspector and any authorized access to privileged information about the object, and
- inspector access history (logs).

Accordingly, this International Standard establishes a framework and outlines functional units used to achieve trustworthiness and interoperability of such systems.

This International Standard does not specify any specific technical solutions, but instead describes processes, functions, and functional units using a generic model to illustrate what solutions have in common.

Object identification systems can incorporate other functions and features such as supply chain traceability, quality traceability, marketing activities, and others, but these aspects are out of scope of this International Standard.

NOTE This International Standard does not refer to industry specific requirements such as Global Trade Item Number.

2 Terms, definitions, abbreviations, and acronyms

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

2.1 Terms and definitions

2.1.1
attribute data management system
ADMS
the system that stores, manages, and controls access of data pertaining to objects

2.1.2
authentication
process of corroborating an entity or attributes with a specified or understood level of assurance

[SOURCE: ISO/IEC 29115]