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

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]

2.1.3
authentication function
the function performing authentication

2.1.4
authoritative source
the official origination of an attribute which is also responsible for maintaining that attribute

2.1.5
custodian copy
a duplicate that is subordinate to the authoritative source

2.1.6
entity
something that has separate and distinct existence and that can be identified within context

Note 1 to entry: An entity can be human, organization, a physical object, class of objects, or intangible object.

[SOURCE: ISO/IEC 29115]

2.1.7
identification
process of recognizing the attributes that identify the object

[SOURCE: ISO/IEC 29115]

2.1.8
identifier
a specified set of attributes assigned to an entity for the purpose of identification

2.1.9
identity
set of attributes that are related to an entity

Note 1 to entry: An identity can have unique attributes that enable an object to be distinguished from all others.

Note 2 to entry: Identity can be viewed in terms of human, organization, and objects (physical and intangible).

2.1.10
inspector
anyone who uses the object examination function with the aim of evaluating an object

Note 1 to entry: Any participant within the system can act as an inspector.

Note 2 to entry: Inspectors can have different levels of qualification and training.

Note 3 to entry: The inspector could be an automated system.

2.1.11
inspector access history
access logs detailing when unique identifier codes (UID) were checked, optionally by which (privileged) inspector, and optionally from what specific location

Note 1 to entry: Time stamps are often used.

2.1.12
interoperability
ability of single entry point to route queries for objects carrying UIDs to the responsible authoritative source for trusted verification function (TVF)

Note 1 to entry: Ability of multiple authentication systems to deliver similar responses to user groups.

2.1.13
object
any single and distinct entity that can be identified

2.1.14
object examination function
OEF
process of finding or determining the UID or other attributes intended to authenticate

Note 1 to entry: In this process, other attributes can assist in the evaluation of the UID.

2.1.15
owner
entity that legally controls the licensing and user rights and distribution of the object associated with the UID

2.1.16
participant
solution providers for interoperable object identification and related authentication systems and its user groups including but not limited to rights holders, customs officers, distributors, and consumers

2.1.17
semantic interoperability
the ability of two or more systems or services to automatically interpret and use information that has been exchanged accurately

2.1.18
syntactic interoperability
the ability of two or more systems or services to exchange structured information

2.1.19
trusted query processing function
TQPF
function which provides a gateway to trusted verification function (TVF) and attribute management data system (ADMS)

Note 1 to entry: This includes software running locally on a hand-held device.

2.1.20
trusted verification function
TVF
function which verifies whether a UID received is valid or not and, manages response according to rules and access privileges

2.1.21
unique Identifier
UID
a code that represents a single and specific set of attributes that are related to an object or class of objects during its life within a particular domain and scope of an object identification system

2.1.22
verification
a check that a UID exists and is valid within an object identification system

Note 1 to entry: Verification can detect some types of fraud, but by itself does not prove an entity is authentic.

2.2 Abbreviations and acronyms

ADMS	Attribute Data Management System
AI	Application Identifier (see MH10.8.2)
CA	Certification Authority
DI	Data Identifier (see MH10.8.2)
OEF	Object Examination Function
RFF	Response Formatting Function
TQPF	Trusted Query Processing Function
TVF	Trusted Verification Function
UID	Unique Identifier

3 Overview

3.1 General

The advantage of interoperability of these systems is to enhance detection of counterfeiting and fraud by

- increasing use by specific user groups,
- increasing the number of inspected objects,
- increasing access to the authoritative sources, and
- lowering cost:
  - training;
  - equipment;
  - development;
  - deployment;
  - inspection time.

Once interoperability is achieved and these systems are widely deployed, an inspector would use an identifier to make inquiries about an object to guide disposition decisions regarding the object. The inspector would have credible evidence that the information provided in response to the inquiry is accurate and trustworthy.

All participants are advised to perform their roles with due diligence.

- Auditing and vetting of the service providers should be considered to ensure they are acting in good faith and are not threat agents operating from behind a deceptive “store front”.
- Auditing and vetting of the manufacturers should be considered to ensure they are following documented processes and feed accurate information into the systems.
- The interested parties with a need-to-know should obtain appropriate credentials to process inquiries, so that the rights holder can release information in a socially responsible manner.

3.2 Object identification systems (in operation)

3.2.1 General

Object identification systems typically consist of functional units as depicted in the model (Figure 1) below.

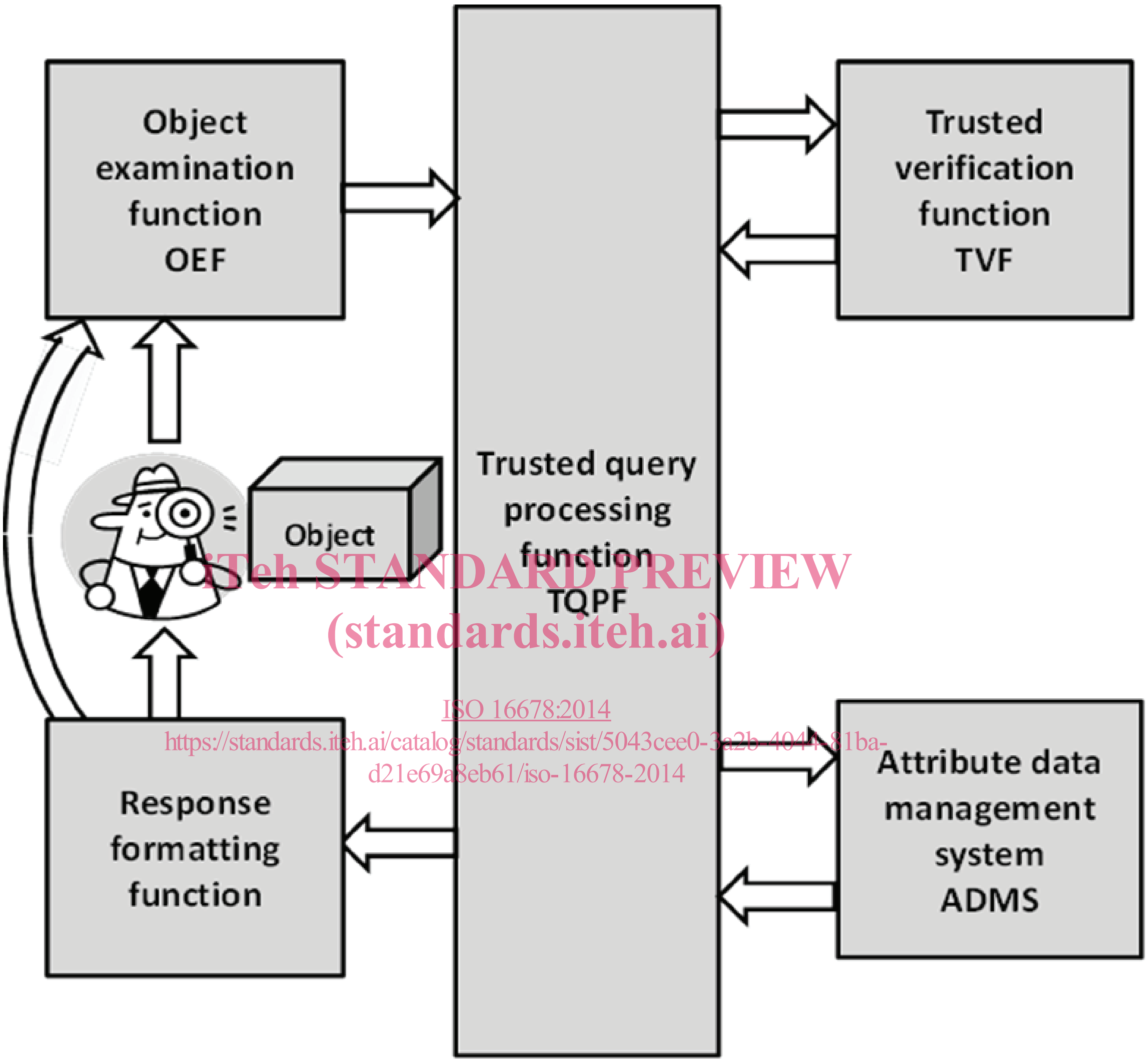
Object examination function OEF
Trusted verification function TVF
Object
Trusted query processing function TQPF
Response formatting function
Attribute data management system ADMS

Figure 1 — Object inspection model

The model makes no assumptions on how functions are implemented. Multiple instances of a function can exist across the system. Different functions can be combined into a single service.

Illustrative examples implementing this model are found in Annex C.

3.2.2 Object examination function (OEF)

The inspector examines an object of interest (such as a material good) to determine if the object has a UID. If a UID is found, further examination can be required to determine which Trusted Query Processing Function(s) are likely to know of this UID. The function forms a query that might consist of only a UID, a combination of UID with the inspector’s credentials, or other physical attribute data including intrinsic authentication elements that might uniquely identify an object such as a digital image. The object examination function concludes when a query is submitted to one or more TQPF. When the process is iterated, the OEF can evaluate the response of a previous query.

3.2.3 Trusted query processing function

A TQPF routes information between the other functions according to defined rules. The TQPF can examine credentials from requesting parties according to defined rules. The TQPF can be distributed across multiple services.

For example, a TQPF can route a query formed by an OEF to the appropriate TVF; or a TQPF can combine the verification or authentication response from a TVF with any credentials from an inspector to form a query into an ADMS.

3.2.4 Trusted verification function

The TVF verifies whether the UID exists within the domain. The TVF should check the credentials of the requesting TQPF. The TVF should enforce access privileges based on defined rules. It can respond to the source of the query or through one or more other TQPF. The response would typically include verification information about the UID (is the UID valid or not?) TVF can also generate alerts to interested parties. TVF should protect sensitive data from unauthorized access.

The TVF can execute an authenticating procedure or algorithm against the information (data) received.

3.2.5 Attribute data management system

An ADMS is the authoritative source of object master data. There should be only one master data record for each object attribute. If multiple instances of attribute data records exist, only one should be “master” and all others “subordinate”. Different object attributes can reside in different databases. Multiple databases can exist in federated environment.

An ADMS receives a response (via a TQPF) from a TVF. The ADMS verifies credentials of both the requesting TQPF and the credentials of the inspector. Access privileges should be based on credentials and rules. The ADMS responds with data selected corresponding to the request and filtered by rules. The response can resolve all the inspector’s questions or can include information on how to proceed. If a response contains further instructions, an inspector decides if further action should be taken by initiating a new query.

Attributes in an ADMS can include information details on how to authenticate objects or proceed with further examination.

The ADMS should protect sensitive data from unauthorized access.

3.2.6 Response formatting function

This function converts ADMS responses into a defined format.

In some cases, the inspection process can be iterated based on the results given by the ADMS or depending on the architecture of the system.

3.3 Object identification systems (setup)

The rules, data, and data relationships need to be defined before these systems can operate.

Figure 2 shows how the example model could be configured.