DRAFT INTERNATIONAL STANDARD ISO/DIS 16678

ISO/TC **247** Secretariat: **ANSI**

Voting begins on **2013-05-25** Voting terminates on **2013-08-25**

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION • МЕЖДУНАРОДНАЯ ОРГАНИЗАЦИЯ ПО СТАНДАРТИЗАЦИИ • ORGANISATION INTERNATIONALE DE NORMALISATION

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

ICS 13.310

To expedite distribution, this document is circulated as received from the committee secretariat. ISO Central Secretariat work of editing and text composition will be undertaken at publication stage.

Pour accélérer la distribution, le présent document est distribué tel qu'il est parvenu du secrétariat du comité. Le travail de rédaction et de composition de texte sera effectué au Secrétariat central de l'ISO au stade de publication.

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENT AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

COPYRIGHT PROTECTED DOCUMENT

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 16678 was prepared by Technical Committee ISO/TC 247, *Fraud Countermeasures and Controls*.

Introduction

This document 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 document 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.

The document 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 document is organized into six (6) major sections:

Scope: Declares the limits of this document as providing only guidance and advice. There are no requirements in this document.

Terms: Defines the contextual meaning of important terms as used in this document 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 document.

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 standard intends to enable reliable, safe object identification to deter introduction of illegal objects to the market.

One goal of this Guideline 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 must also include solutions which simply detect some counterfeits without authenticating products. Likewise, the framework must 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 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 guideline 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;
  - 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;
- Inspector Access History (logs).

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

This guideline 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 may 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 guideline.

NOTE This guideline does not refer to industry specific requirements such as Global Trade Item Numbers (EAN).

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

[SOURCE: ISO/IEC 29115]

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

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 may 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 virtual.

2.1.10
inspector
anyone who uses the object identification system with the aim of evaluating an object

Note 1 entry: Any participant within these systems may act as an inspector.

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

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

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 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
the process of finding or determining the UID of an object

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 entry: This includes software running locally on a handheld 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 entity during its life within a particular domain and scope of an object identification system

Note 1 entry: Entity can be a specific item or a class of identical items.

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

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