ISO/PRF 22378:2022(E)

Date: 2022-~~09-20~~10-21

ISO/TC 292

Secretariat: SIS

Security and resilience — Authenticity, integrity and trust for products and documents — Guidelines for interoperable object identification and related authentication systems to deter counterfeiting and illicit trade

Sécurité et résilience — Authenticité, intégrité et confiance pour les produits et les documents — Lignes directrices pour l'identification interopérable d'objets et systèmes d'authentification associés destinés à décourager la contrefaçon et le commerce illicite

ISO Copyright Office
CP 401 • CH-1214 Vernier, Geneva
Phone: + 41 22 749 01 11
Email: copyright@iso.org
Website: 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 ~~should~~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~~first edition of ISO 22378 cancels and replaces the first edition ~~(~~ISO 16678:2014~~)~~, which has been technically revised.

The main changes are as follows:

— ~~th etitle~~the title and number ~~has~~have been updated to follow the same structure as all other documents developed by ISO/TC 292~~;~~.

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

This document is based on three foundational assumptions:

- detecting counterfeit objects is a complex and often difficult task;
- accurate identity information about the object in question simplifies the counterfeit detection process;
- 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 inspectors when 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. This document will make it easier for inspectors to access identity information and ~~help them to detect counterfeits and~~ granting inspectors access to reliable identity information helps facilitate the detection of counterfeits.

This 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.

This document contains:

- terms and definitions;
- an overview on how object information is used to detect counterfeits;
- principles, concepts and values;
- recommendations on how to improve interoperability of systems capable of providing object information to inspectors;
- specific examples that illustrate some of the concepts presented.

This document enables reliable and safe object identification to deter the introduction of illegal objects to the market.

It includes a framework with the objective to increase trust by making object identification solutions interoperable. For example, the framework describes method and solutions for how to:

- detect some counterfeits without authenticating products;
- evaluate an authentication element;
- formally prove that a remote description of an object can be trusted.

This is document is part of a family of standards which includes ISO 22380, ISO 22381, ISO 22382, ISO 22383, ISO 22384.

One goal of this document 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 should also include solutions which simply detect some counterfeits without authenticating products. Likewise, the framework should also include a solution which only evaluates an authentication element.

Assuming that the object identification systems themselves can also be counterfeited and copied, This document establishes a method to formally prove that a remote description of an object can be trusted. 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 use-cases 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.

This document is complemented by ISO 22381:2018, which guides the establishment and set-up of interoperability.

Security and resilience — Authenticity, integrity and trust for products and documents — Guidelines for interoperable object identification and related authentication systems to deter counterfeiting and illicit trade

1 Scope

This document establishes a framework for identification and authentication systems. It provides recommendations and best practice that include:

- management and verification of identifiers;
- physical representation of identifiers;
- participants' due diligence;
- vetting of all participants within the system;
- relationship between the unique identifier (UID) 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).

The model described in this document is intended to determine the common functions of different systems.

This document describes processes, functions and functional units of a generic model. It does not specify any specific technical solutions.

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 document.

NOTE This document does not refer to industry-specific requirements such as GS1 Global Trade Item Number (GTIN).

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 apply.

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

- ISO Online browsing platform: available at https://www.iso.org/obp
- IEC Electropedia: available at https://www.electropedia.org/

4 Abbreviated terms

ADMS	attribute data management system
AI	application identifier (see ANSI MH 10.8.2[~~15~~8])
CA	Certification Authority
DI	data identifier (see ANSI MH 10.8.2[~~15~~8])
IP	Internet Protocol
OEF	object examination function
RFF	response formatting function
TQPF	trusted query processing function
TVF	trusted verification function
UID	unique identifier
SLA	service level agreement

5 Overview

5.1 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;
- lowering the cost of:
  - training;
  - equipment;
  - development;
  - deployment;
  - inspection time.

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

All participants should perform their roles with due diligence considering the following:

- 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.

5.2 Object identification systems — Operating process

5.2.1 General

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

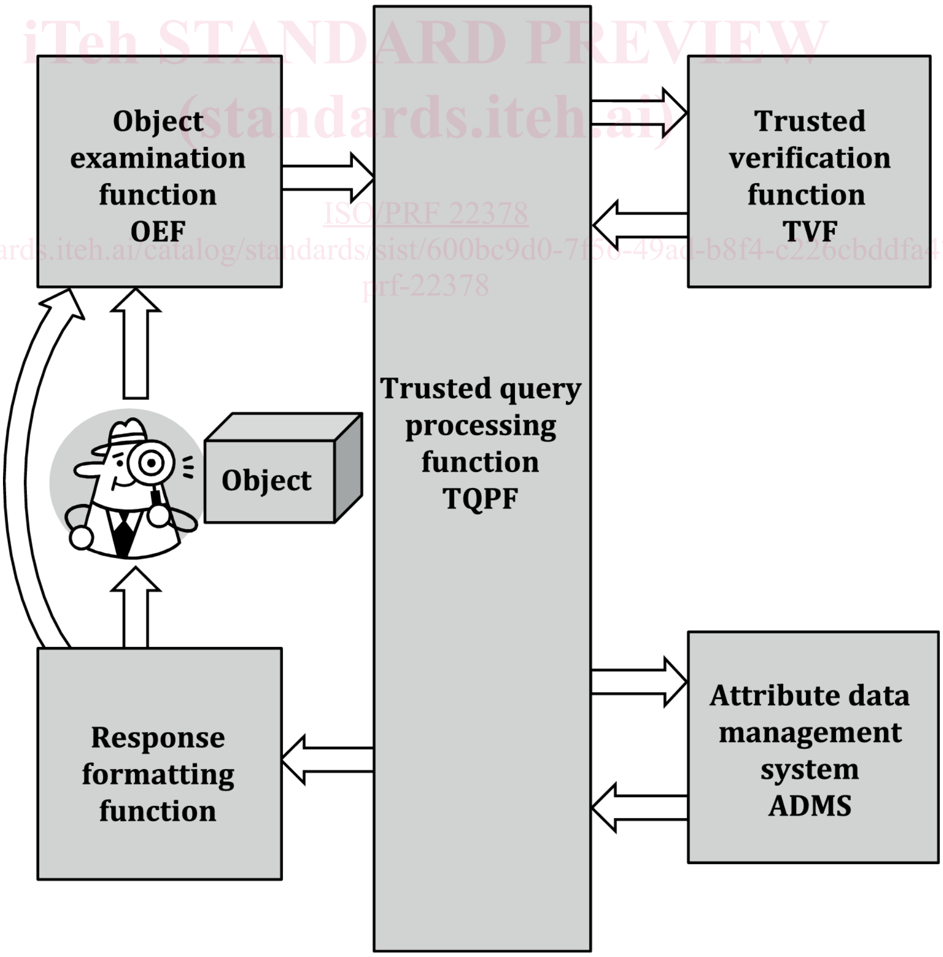
Object examination function OEF
Trusted verification function TVF
Trusted query processing function TQPF
Object
Attribute data management system ADMS
Response formatting function

Figure 1 — Object identification model

The model makes no assumptions on specific implementation of the functions.

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 given in Annex C.

5.2.2 Object examination function

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 TQPF(s) are likely to know of this UID. The function forms a query that can consist of only a UID, a combination of UID with the inspector's credentials, or other physical attribute data including intrinsic authentication elements that can uniquely identify an object such as a digital image. The OEF ends 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.

5.2.3 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.

EXAMPLE 1 A TQPF routes a query formed by an OEF to the appropriate TVF.

EXAMPLE 2 A TQPF combines the verification or authentication response from a TVF with any credentials from an inspector to form a query into an ADMS.

5.2.4 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 (e.g. "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.

5.2.5 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, TVF 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.