INTERNATIONAL STANDARD

ISO 22378

First edition
2022-12

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

Reference number
ISO 22378:2022(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 first edition cancels and replaces ISO 16678:2014, which has been technically revised.

The main changes are as follows:

- the title and number 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 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[8])
CA	Certification Authority
DI	data identifier (see ANSI MH 10.8.2[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.

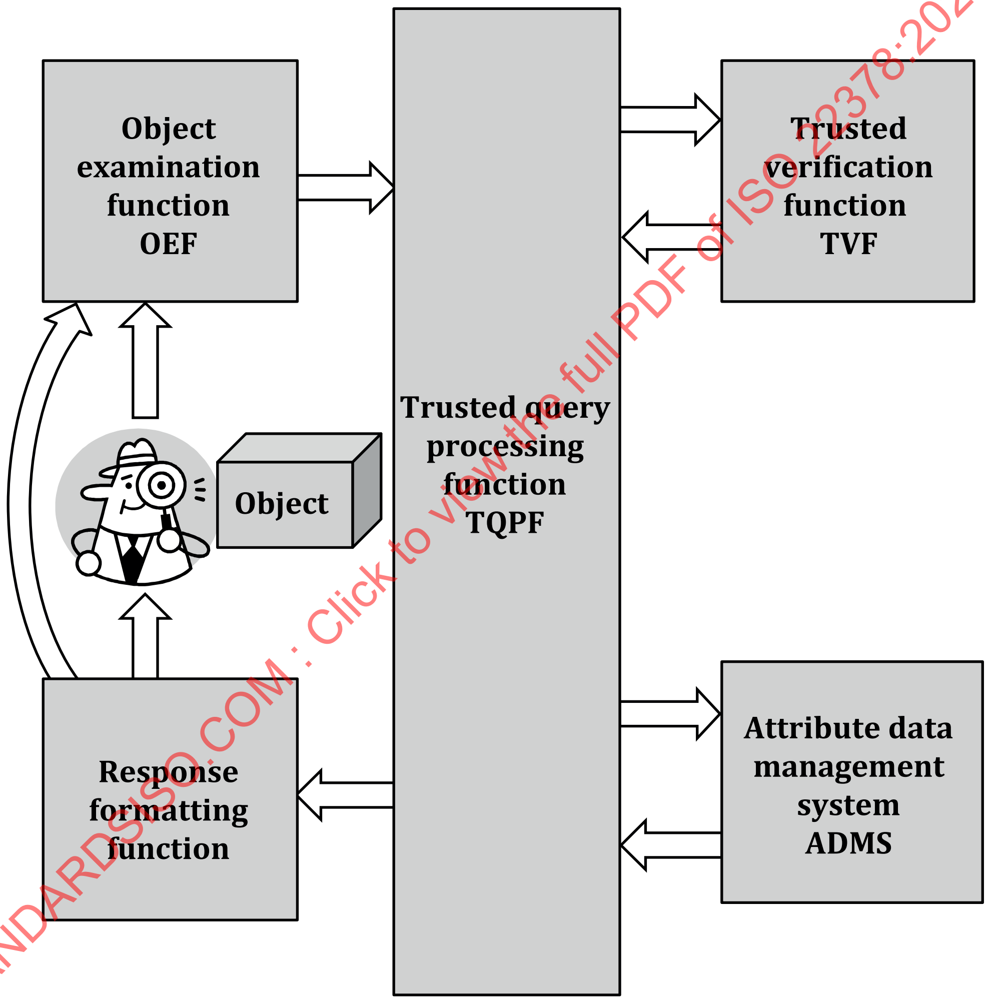
Object examination function OEF
Trusted query processing function TQPF
Trusted verification function TVF
Object
Response formatting function
Attribute data management system ADMS

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.

5.2.6 Response formatting function

This function converts ADMS responses into a defined format and communicates them to the inspector. This is the end of the process.

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.

5.3 Object identification systems — Set-up of trusted framework

5.3.1 General

The identification and authentication system should operate in accordance with the following definitions, rules, data and data relationships.

Figure 2 shows how the example model can be configured.

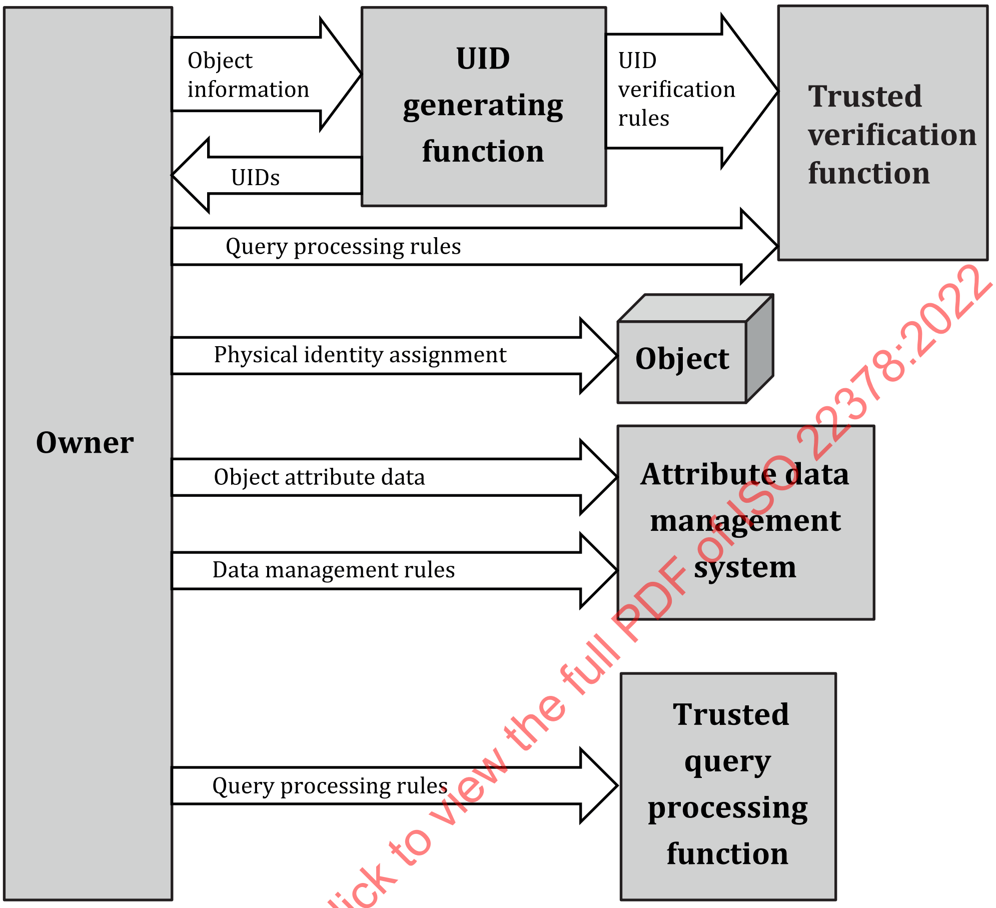

Figure 2 — Set-up and configuration

5.3.2 Owner

Owners determine all of the detail on whom, how, where and when access rights to attribute data are granted. Owners choose the service providers that implement the functional block and provide the access and business rules to the various providers.

5.3.3 UID-generating function

The UID-generating function should ensure UIDs are unique within the domain the service operates. UID can be generated following a specific format or function that can include object specific attribute data.

The function also generates or produces the verification rules that TVF use when considering a specific UID during a query.

5.3.4 Object information

Object information should be a subset of object attribute data or pointer (reference) to object attribute data.

5.3.5 UID verification rules

The algorithms and procedures that allow a TVF to determine if a UID is valid within the domain. They can include algorithms and processes that allow authentication. They can also include a list of generated UIDs.

5.3.6 Physical identity assignment

In creating the link between a UID and an object, assignment can be accomplished by enrolment of an intrinsic UID.

5.3.7 Object attribute data

Object attribute data refers to the attributes sufficient to identify an object or class of objects. Owner can include additional attributes at their discretion.

5.3.8 Data management rules

The policies regarding protection and disclosure of attribute data include, but are not limited to:

- access rights, including:
  - requirements to gain privilege to an access level;
  - assigns attributes to access levels;
  - the protection levels of the attribute data;
- user (inspector) roles;
- standard query responses, including:
  - business rules for data disclosure;
  - responses to queries in all situation including invalid UID cases ;
  - privileged versus unprivileged response.

5.3.9 Query processing rules

The query processing rules enable a function to:

- route a query or response to the appropriate function;
- verify a request is authorized or allowed;
- verify communication is authorized or allowed.

6 Key principals

6.1 General

This clause provides key principles on how to design the identification and authentication system.

6.2 Availability and timely response

The identification and authentication system should be designed so that:

- availability and response times meet the inspector's expectations;

- response times are long enough to verify credentials.

This may be addressed and specified by a service level agreement (SLA).

6.3 One authoritative source

The identification and authentication system should be designed so that only one authoritative source corresponds to the object to be identified.

Allowing multiple sources can confuse the inspector. It can also be possible for malicious service providers to copy the source, manipulate it and publish as one of the authoritative sources to the inspector.

The identification and authentication system can allow custodian privileges to service providers, but it should always be clear who the authoritative source is and why custodian copies of the data can be trusted.

6.4 Data management

The identification and authentication system should be designed so that:

- master data and transactional data are kept up to date;
- all data are managed in line with the expected life cycle of the object;
- it is possible to adapt to future changes in regulatory requirements;
- long-term object identification is driven by maintenance warranty, and investigations needing authentication.

NOTE Annex B gives further information on key concepts on master data management and transactional data management.

6.5 Need to know

The identification and authentication system should be designed so that any knowledge about the following aspects is protected and only shared on a need-to-know basis:

- the presence of the features;
- the nature of the feature;
- the processes and architecture of the system.

6.6 Data protection

The identification and authentication system should be designed so that it uses best practices to protect data about business critical. This includes designing and organizing the security both technically and operationally, where appropriate means are taken for protecting confidentiality, integrity and availability of information that are maintained in the system.

6.7 Privacy

The identification and authentication system should be designed so that any personal identifiable information (PII) are protected, taking into account local and jurisdictional regulations, as well as industrial best practices.

6.8 Regulatory compliance

The identification and authentication system may be designed so it can be adapted with respect to applicable regulatory requirements.

NOTE Applicable regulations can be different in different industries and countries.

6.9 Vetting

The identification and authentication system should be designed so that:

- all participating/involved parties are vetted and credentialed;
- the owner ensures that the implementations of TVF and ADMS are trustworthy, the audit results and credentials of providers are considered as part of a provider selection process, and credentials are available and up to date;
- the person who selects the TQPF ensures the implementation is trustworthy and credentials are up to date;
- the service provider performs background checks on customers requesting contractual use of their services to deter malicious actors from pretending to be owners.

6.10 Interoperability aspects

Two or more systems or services should support the ability to exchange structured information (syntactic interoperability), to automatically interpret it (semantic interoperability) and to accurately use the information.

The identification and authentication system should be designed so that interoperability is achieved by defining and agreeing on:

- the target user group;
- the minimum information user needs;
- access rights;
- standards for data exchange to follow, including data handling, data ownership, data protection and usage restrictions, and data interfaces;
- the style sheet, as necessary;
- SLAs.

NOTE 1 This document only covers semantic interoperability. Some syntactic alignment can be necessary for the routing process.

NOTE 2 ISO 22381 gives further information on the process of how to establish interoperability by organizing participants involved, planning an architecture, and implementing and operating interoperation.

6.11 UID generation

The identification and authentication system should be designed so that each UID is generated to be unique within the domain in which the service operates.

7 Plan and implementation

7.1 General

This clause includes the following:

- 7.2 describes how to determine trusted services by TQPF;
- 7.3 focuses on how to manage object identification data and attributes, and describes in particular what systems have in common;
- 7.4 gives an overview of common frauds, and outlines the advantages and disadvantages of various implementation approaches to help an interested party choose the most appropriate solution based upon their situation.

7.2 Determination of trusted services

7.2.1 General

The identification and authentication system should be designed so that the inspector can easily find or determine which TQPF is involved with an object. The inspector should be able to decide a level of trust to associate with the involved TQPF.

It is important to make the TQPF easy to find. Anything that makes the correct or authoritative TQPF more visible should be considered.

7.2.2 Trust in the TQPF

The identification and authentication system should be designed so that the TQPF, which acts as a portal for inspectors, should be referenced or endorsed by independent and well-known authorities.

Consideration should be given to detect and recover from attacks on the TQPF portals. For example, malicious agents are known to execute denial of service attacks on portals. Attacks occur in many forms and countermeasures should be appropriate for the specific attack.

Limiting the number of established services can assist the users with detecting deceptive services and threat agents. Consolidating users onto only one or just a few TQPFs can allow someone in the group to recognize and report suspicious actions and behaviours. The sudden appearance of a new service can draw more scrutiny.

7.2.3 Use of prefix or postfix

The identification and authentication system should be designed so that interoperability can be improved by using a standardized data identifier (DI) or an application identifier (AI) as a prefix or postfix to assist the TQPF route the query to the correct TVF.

In the absence of AI, DI or other hints for locating the service, the approach is to examine the object for trademarked logos or other evidence that identifies the manufacturer of the object. Inspectors can contact the manufacturer for assistance in locating the TQPF.

7.2.4 Object examination techniques

The identification and authentication system should be designed so that guidance is not needed when all data and identity elements are present in a system where all the participants are following the agreements and rules. In non-ideal systems, consideration should be given to how OEFs degrade as UIDs are lost or destroyed. Redundant and error-correcting elements can improve performance in such circumstances.

Consideration should be given to how OEFs behave when rules and agreements are violated. Trust and confidence can erode quickly and defensive behaviours can emerge.

7.3 Management of object identification data and attributes

7.3.1 General

The identification and authentication system should be designed so that an inspector with sufficient credentials can initiate a query with a TQPF that results in a response from an ADMS. If the access rules allow it, the ADMS response can contain object identification data or other object attributes.

NOTE Inspectors without credentials such as consumers can find only publicly available or limited information in the response.

7.3.2 Verify the service entry point (TQPF)

The identification and authentication system should be designed so that interested parties are advised to carefully consider the possibility that the service entry point can be hosted by malicious agents with the intent to commit fraud. The interested party should consider a number of questions before trusting or believing data provided from a service. A few possible example questions are:

- Is the service provider credible?
- Is the object data coming from the trusted source?

Independent audits can resolve concerns regarding the credibility of a service. Credentials that attest to the audit results can be issued. The service can choose to make these credentials available to interested parties to improve trust.

Inspectors can request credentials from the services they use and should check that any credentials provided are current and rooted to a trustworthy authority.

7.3.3 Maintenance and management

The identification and authentication system should be designed so that the owner can ensure that data are accurate and up to date. For example, if an attribute that describes objects in a class changes, the corresponding information in the ADMS can need updating.

The owner should ensure that functions enforcing access rights have up-to-date rules and authorized user information.

7.3.4 Privilege levels and user roles

The identification and authentication system should be designed so that access to confidential object identification data can be dependent on privilege level. For example, replies containing highly valued and confidential object data can be routed only to inspectors with very high-level credentials, whereas replies routed to inspectors without credentials can contain only publicly available information.

There can be as many access privilege levels as the data owner decides to create.

7.3.5 Access control

The identification and authentication system should be designed so that industry practices for granting access rights are varied for many reasons, such as regulatory mandates, communication network constraints, equipment cost, etc. A few common access methods include:

- user name and password challenge;
- digital certificates;

- unique Internet Protocol (IP) address access control.

Best practices for access control should be considered. There should be a means to verify an inspector's identity and organization affiliation before access to confidential information is granted. Ease-of-use can be facilitated when single sign-on mechanisms are used. Access control utilizing a digital certificate should be considered for highly confidential data. An example of digital certificates for inspectors is given in Annex A.

7.3.6 Ownership of transactional data

The identification and authentication system should be designed so that transaction event data and logs can be generated as TQPF and TVF systems operate. All affected parties should understand who owns and manages the transactional data and who has rights to access and use this data. Formal contractual agreements should be established to prevent misunderstandings.

7.3.7 Use of transactional data

The identification and authentication system should be designed so that UID codes without a related authentication function cannot be used to determine whether or not an object is genuine. However, analysis of event logs can detect some systematic attacks and help isolate counterfeit objects.

For example, an event log that contains location information can detect a single object UID claiming to be in two places at once. In addition, for UID systems that establish an instance-specific code for each instance of an object, special attention should be given when a code is queried too many times as this can indicate that counterfeit objects exist.

7.3.8 Governmental or intergovernmental agencies or competent authorities

The identification and authentication system should be designed so that governments or intergovernmental agencies can establish requirements to ensure the safety of the public. These requirements can change from country to country or by geographic region. These requirements are usually monitored or supervised by a competent authority or agency established by governments with jurisdictional authority over the geographic region. These agencies can be empowered by government mandates that require access to confidential information about products and any information used to authenticate products to ensure they are authorized for the destination market and safe for the consumer.

Owners should be aware of specific regulatory requirements which can require them to provide data about their products to the above agencies in the markets where their products are distributed or sold. Similarly, owners should be aware that in some jurisdictions, there can be restrictions on cross-border access to data and services.

7.4 Common frauds

7.4.1 Duplicate UID codes

The techniques used to detect duplication of UID codes differ between class identifiers and identifiers intended for use on single instance of the object. When UID codes are copied, re-originated, guessed or reused, duplicates or "clones" occur across the system. Systems and services should be designed to detect and report duplicate UID codes. Indications of duplicated UID codes for both types (class and instance) can include, but are not limited to:

- queries coming from unauthorized locations or unauthorized inspectors;
- the object does not match the description reported by the ADMS.

Indication of duplicated single instance UID code for an object can also include, but are not limited to:

- queries coming from different locations at the same time;

- more queries than expected occurring for a single UID code.

In order to mitigate the risk of duplicated UID codes, an authentication element should be used.

An intrinsic physical security layer can be incorporated into a UID code. Intrinsic physical security layer options include, but are not limited to:

- security inks, taggants, optically variable devices and other authentication features;
- embedded secret keys;
- encrypted information related to secure element;
- physical unclonable functions or markings.

Adjacent physical security layer options include, but are not limited to:

- security papers;
- inks, taggants, optically variable devices and other authentication features.

In complement to the above, brand specific features, stitching, designs and colours can be used.

7.4.2 Substitution

Fraud occurs when a valid UID becomes attached to a counterfeit object by substitution of the object. Bad actors use multiple methods in committing this fraud by targeting:

- the supply chain;
- scrap, reclaim or reuse;
- warranty replacement programmes.

Methods to mitigate the risk of substitution can include, but are not limited to:

- tamper-evident-sealing technologies;
- an allow list of authorized sources;
- track and trace of UID code, inspectors and inspections;
- deactivating of UID codes.

7.4.3 Feature deception

While it seems obvious that the absence of an expected UID code indicates fraud, this is only true when the inspector knows that a UID code should be present. Many authentic products exist that do not use any form of UID, so the absence of any UID does not automatically mean fraud has occurred. Feature deception fraud occurs when the set of identity features is incorrect, for example:

- the expected UID is missing;
- the UID is incorrect;
- more UID are present than expected;
- the type of physical security is incorrect;
- the number of physical security layers is incorrect.

Methods to mitigate the risk of false features deceiving inspectors can include, but are not limited to

- inspector training;

- communication with the owner or other experts;
- public training and announcements.

7.4.4 Malicious services

Bad actors will attempt to route inspectors to malicious services. Most of the methods used to trick inspectors are easily detected, but new or untrained inspectors are at higher risk of a rerouting fraud. Malicious service attacks include:

- rerouting, sniffing, spoofing and redirecting;
- man-in-the-middle attack.

Methods to mitigate the risk of malicious services can include, but are not limited to:

- encrypted communication channels between functional units;
- a digital certificate;
- a periodic check that the root of trust is still valid;
- an allow list;
- the use of trusted websites as a possible entry point, for example:
  - owner's website;
  - industry sector website;
  - trusted third-party services.

Owners should ensure that systems and services are audited and that credentials or other assurances are available for inspectors to reference. Owners should ensure that inspector-oriented training materials are developed and maintained.

Inspectors can check for credentials when encountering any system or service for the first time, and periodically re-check that credentials remain current for all systems and services used.

7.4.5 Malicious inspector

There should be means to detect malicious query patterns. Example means include, but are not limited to, access logs and procedures that frequently verify access was based on a need-to-know.

7.4.6 Insider attacks

A bad actor on the inside can corrupt a good service provider or brand owner into a malicious one. Valid ID numbers can become available to bad actors due to:

- security leaks;
- unintentional mistakes and misconduct;
- malicious behaviour;
- inadequate security policy and training;
- an insider stealing active UID codes.

Methods to mitigate the risk of insider attacks can include, but are not limited to:

- adequate security policies;

- avoiding multiple authoritative sources of the same ID numbers;
- activating UID codes only as they are properly used.

Annex A
(informative)

Digital certificate (for inspectors)

A.1 General

This annex shows one possible implementation of using X.509 (see ISO/IEC 9594-8) certificates to transmit inspector credentials to the functions of an object identity system. In this specific example, interoperability is improved by using a common and existing standard (X.509) as the mechanism to deliver information across the internet. This is achieved by using OU1 and OU2.

One owner will initiate the generation of a certificate for the inspector. This certificate can be used by all TQPFs.

The aim is to establish secure and trusted communication between the functions. X.509 is one method to accomplish this when using publically available networks.

A.2 Example and definitions of digital certificates (for inspectors)

The use of a digital certificate to achieve access control to ADMS is one of the best practices, but the brand owner should consider the trustworthiness of both inspector and digital certificate itself.

A.3 Trustworthiness of inspector

It is important that the brand owner considers the trustworthiness of the inspector who receives the digital certificate in order to access high confidential data in an ADMS. Credibility can be increased by using an allow list inspector maintained by a trusted source.

A.4 Trustworthiness of digital certificate

In order to ensure the trustworthiness of a digital certificate, a digital certificate issued in accordance with the following standards should be used.

- ETSI/TS 102 042[10];
- ETSI/TS 101 456[9];
- WebTrust for CA[12].

A.5 Common field of digital certificate

Common profiles of digital certificates can be necessary in order to achieve the interoperability between systems.

An example of the common profile of the X.509 (see ISO/IEC 9594-8) certificate is shown in Table A.1.

Table A.1 — Mandatory fields (basic certificate fields)

Certificate fields	Data type (number of characters)	Definition	Authority	Example
Subject				
Country name	Printable String (2)	— The two character country code in alpha-2 of ISO 3166-1 — All capital letter	Administrator	JP
State name	Printable String (128)	— Name of state, province, etc. — A head character is a capital letter	Administrator	Tokyo
Locality name	Printable String (128)	— Name of city, etc. — A head character is a capital letter — A delimiter is a hyphen	Administrator	Minato-ku
Organization name	Printable String (64)	— Name of organization[a]	Administrator	JIPDEC
OrganizationUnitName1	Printable String (64)	— Identifier, which administrator manages — In order to distinguish in automatic verification, it attaches the prefix “OU1-”[b]	Administrator	OU1-G2–1.2.392.200063.80.1.1
OrganizationUnitName2	Printable String (64)	— Identifier, which a registration authority (RA) or local registration authority (LRA) manages — In order to distinguish in automatic verification, it attaches the prefix “OU2-”[c]	RA or LRA	OU2–007

[a] It uses the name which is registered in the QGIS (Qualified Government Information Source) or QIIS (Qualified Independent Information Source) or QTIS (Qualified Tax Information Source).

[b] It can be used as a pointer to the open attribute information (the company name, etc.), which cannot be written with the alphabet), which cannot be recorded on the certificate.

[c] It can be used as a pointer to the secret attribute information (section name, etc.), which cannot be recorded on the certificate.

Table A.1 *(continued)*

Certificate fields	Data type (number of characters)	Definition	Authority	Example
Common name	Printable String (64)	— Subject's name (real name, section name, role or ID) — In order to distinguish in automatic verification, it can attach the prefix "BN-" (business name which used as a formal common name in the organization, such as a real name and maiden name), "BO-" (organization/role), or "ID-"	RA or LRA	Smith Betty (Supply Manager)

[a] It uses the name which is registered in the QGIS (Qualified Government Information Source) or QIIS (Qualified Independent Information Source) or QTIS (Qualified Tax Information Source).

[b] It can be used as a pointer to the open attribute information (the company name, etc.), which cannot be written with the alphabet), which cannot be recorded on the certificate.

[c] It can be used as a pointer to the secret attribute information (section name, etc.), which cannot be recorded on the certificate.

Annex B
(informative)

Master data management

B.1 Master data versus transactional data

Master data and transactional data are two distinct data sets. Both have an impact on traceability as well as product safety, recall and anti-counterfeit measures. Aspects of the data sets are defined as either public data or confidential data, and this has implications for authorized access to object information when a counterfeit issue arises.

Access to object master data requires certain levels of access authentication normally controlled by the brand owner or IP rights holder. As supply chains are generally multi-party, contractual agreements between actors can be inhibitors to sharing information with competent authorities due to contractual restrictions and legal ramifications.

B.2 Master data

Master data should have static product data, which is somewhat permanent in nature and typically does not change often during the life cycle of an object. It includes data that can be considered public, such as the object identification number on consumer level packaging, as well as the brand name, product description, mass and dimensions, etc. Master data can also contain business confidential information, such as design specifications, bill of materials, component sources, authentication attributes and others.

Processes commonly used in master data management include item master creation, object codification, data classification, source identification, data collection, data transformation, normalization, rule administration, error detection and correction, data consolidation, data storage, data distribution, data synchronization, taxonomy services, schema mapping, data enrichment, data governance and object data life cycle management.

B.3 Transactional data

Transactional data are dynamic, supply chain event-driven data, which should have public and confidential data. Transactional data are created in information systems as an object moves along the supply chain. Transactional data can be captured and logged, and should be managed by contractual agreement.

Annex C
(informative)

Illustrative implementation examples

C.1 General

This annex provides a few implementations of object identification systems and how different implementations still follow the generic model offered by this document.

The function blocks instances can vary. The blocks shown in each example have been shifted and mixed to illustrate how broadly implementations can vary.

C.2 Class UID versus object UID

In all example implementations found in this annex, the UID helps an inspector find information that describes an object.

For “class UIDs”, this descriptive information refers to attributes common to all objects of that class, such as contents and traits of the products and their packaging. This data are sometimes referred to as “master data”.

Information for “object UIDs” often includes several levels of attribute detail. Object UID information can be:

— descriptive for the whole class of objects (master data: same information as given for class UIDs), e.g. product and packaging traits;

— descriptive for a production batch of objects, e.g. production batch number, expiration date, batch recall information;

— descriptive for a lot of objects, e.g. shipment information, information on buyers and sellers of a lot of objects;

— descriptive for a single item, e.g. the serial number of an individual product and/or its components.

Many factors should be considered when selecting an implementation based on class UIDs versus one based on object UIDs. Object-specific information can be more efficient than class-specific information at detecting counterfeit objects. For example, many instances of each class UID are expected to exist, but only one object UID is expected. Finding two identical class UID is not unusual whereas finding two identical object UID indicates that something is wrong. However, object UIDs typically have higher implementation and maintenance overheads than class UIDs.

C.3 Class UID, no authentication function example

Objects in this example implementation use only class UID. During set-up, for each UID, the owner loads attributes that describe the objects in each class into the ADMS. Each UID points to one set of object attributes in the ADMS. Figure C.1 shows an example of the class UID, no authentication function.