BS ISO 16678:2014

BSI Standards Publication

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

bsi.

...making excellence a habit.™

**National foreword**

This British Standard is the UK implementation of ISO 16678:2014.

The UK participation in its preparation was entrusted to Technical Committee SSM/1/2, Security Management.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.



ISBN 978 0 580 75436 4

ICS 13.310

**Compliance with a British Standard cannot confer immunity from legal obligations.**

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 July 2014.

**Amendments issued since publication**

| Date | Text affected |
|---|---|

BS ISO 16678:2014

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)

**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.

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.

INTERNATIONAL STANDARD ISO 16678:2014(E)

# 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.

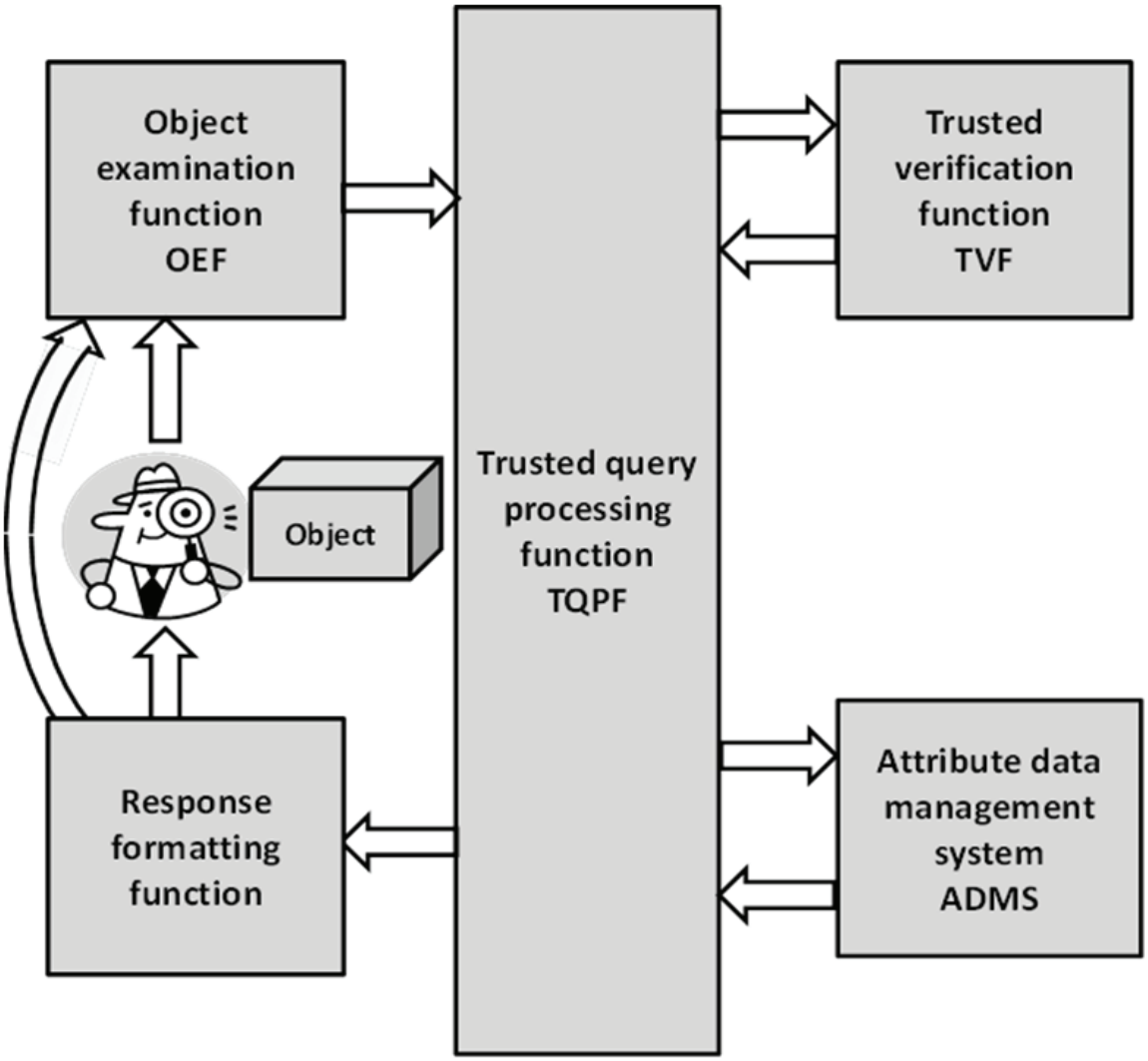



**Figure 1 — Object inspection model**

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.

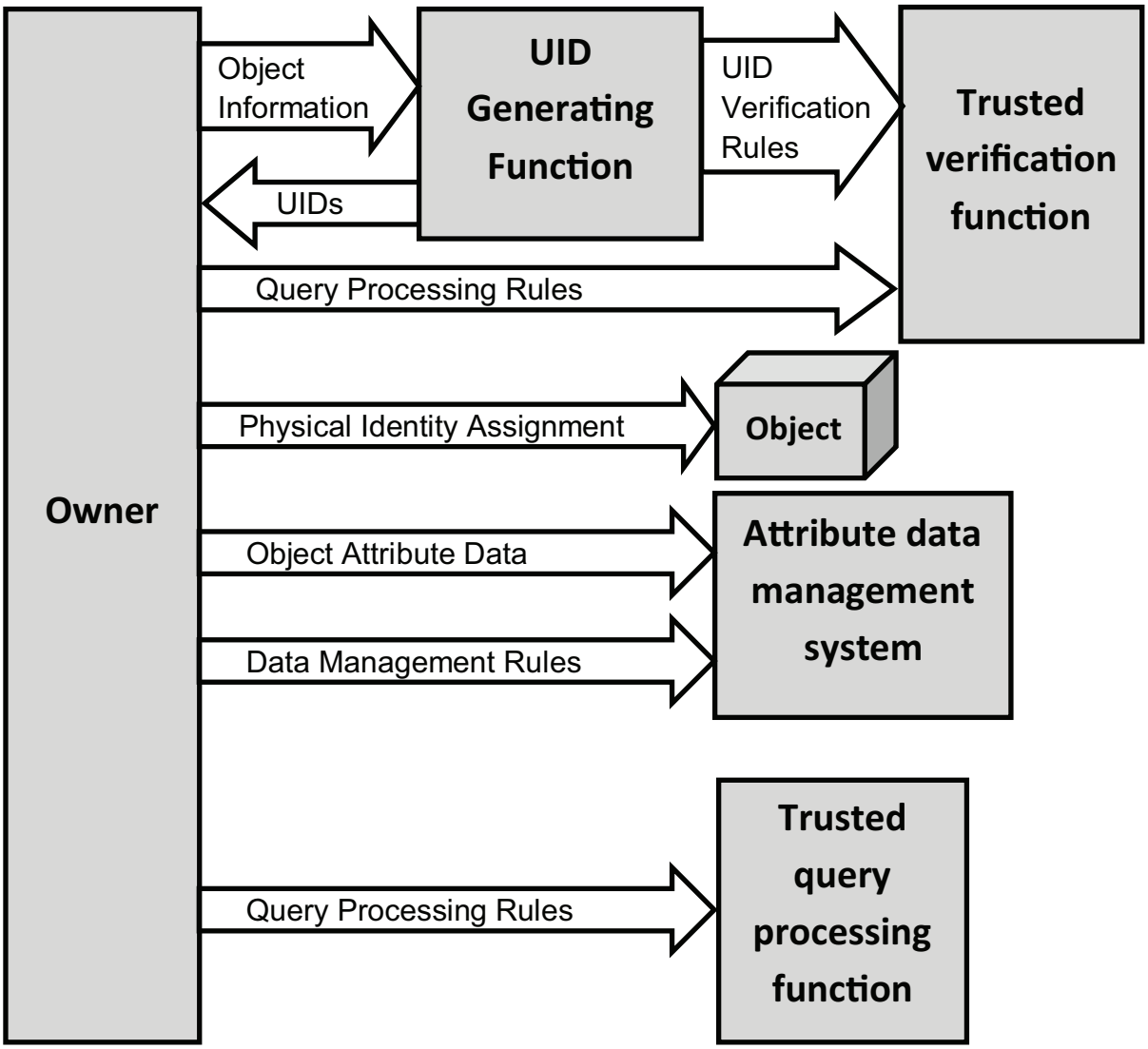



**Figure 2 — Setup and configuration**

### 3.3.1 Owner responsibilities

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.

### 3.3.2 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.

### 3.3.3 Object information

Subset of object attribute data or pointer (reference) to object attribute data.

### 3.3.4 UID verification rules

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

### 3.3.5 Physical identity assignment

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

### 3.3.6 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.

### 3.3.7 Data management rules

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

— access rights:
  — requirements to gain privilege to an access level;
  — assigns attributes to access levels;
  — the protection levels of the attribute data.
— user (inspector) roles, and
— standard query responses:
  — business rules for data disclosure;
  — responses to queries. For example, What to say when UID is invalid;
  — privileged versus un-privileged response.

### 3.3.8 Query processing rules

The rules that enable a function to

— route a query or response to the appropriate function,
— verify a request is authorized or allowed, and
— verify communication is authorized or allowed.

## 4 Key principals

### 4.1 Availability and timely response

Availability and response times should meet the inspector's expectations.

Response times should include the time needed to verify credentials. It is recommended that availability and response times be addressed in a service level agreement.

### 4.2 One authoritative source

Only one authoritative source should correspond to the object to be identified. Multiple sources could confuse inspector, furthermore, malicious service provider can copy the source, manipulate it, and

publish as one of the authoritative sources to inspector. There can be service providers who have custodian privileges, but it should always be clear who the authoritative source is and why custodian copies of the data can be trusted.

### 4.3 Data management

Master data and transactional data should be kept up-to-date. The data should be managed in line with the expected life cycle of the object. Consideration should be also given to how regulatory requirements can change in the future, long term object identification needs driven by maintenance, warranty, and investigations needing authentication. See Annex B for key concepts on master data management and transactional data management.

### 4.4 Need to know

To create an effective system, any knowledge about the presence of the features, the nature of the feature, and the processes and architecture of the system should be protected and only shared on a need-to-know basis.

### 4.5 Data protection

The system contains business critical data and should use best practices to protect data. Through designing and organizing the security both technically and operationally, appropriate means should be taken for protecting confidentiality, integrity, and availability of information that are maintained in a system.

### 4.6 Privacy

Any Personal Identifiable Information (PII) should be protected following local and jurisdictional regulations, and where there are no regulations, industrial best practises should be used.

### 4.7 Regulatory compliance

Different industries and countries are regulated with different directives that cannot be considered in this guideline. Any interoperable system shall be adapted to respect the specific regulatory requirements.

### 4.8 Vetting

Owners should ensure the implementations of TVF and ADMS are trustworthy. They should consider the audit results and credentials of providers as part of a provider selection process. Owners should ensure the credentials are available and up-to-date.

Whoever selects that TQPF should ensure the implementation is trustworthy and credentials are up-to-date.

Service providers should perform background checks on customers requesting contractual use of their services to deter malicious actors from pretending to be owners.

Vetting is bidirectional and trust is increased when all parties are credentialed.

### 4.9 Interoperability

Interoperability is the ability of two or more systems or services that exchange structured information (syntactic interoperability) and to automatically interpret it (semantic interoperability) and use the information that has been exchanged accurately and meaningfully in order to produce useable results.

Principle of the interoperability includes

— define target user group:

  — define minimum information user needs;

  — define style sheet as necessary;

  — agree on how to handle access rights.

— data handling:

  — agree on data ownership;

  — agree on data protection and usage restrictions.

— define data interfaces:

  — identify useful existing standards for data exchange.

— define service level agreement to ensure the response.

NOTE This International Standard is intended to improve semantic interoperability. Some syntactic alignment might be necessary for the routing process.

### 4.10 UID generation

UID should be generated such that they are unique within the domain the service operates.

## 5 Guidance

### 5.1 Introduction

The specific implementation details of actual systems vary broadly, however, there are common functions between these systems that enable interoperability. It helps to describe systems from a functional perspective to show the common operations. 5.2 and 5.3 focus on what systems have in common.

The guidance presented here strongly considers the common frauds listed in 5.4. Implementation details have impact on how effectively a service can detect each specific fraud listed. The guidance attempts to illustrate which implementation approaches are most effective for each common fraud. The guidance that follows in 5.4 outlines the advantages and disadvantages of popular or common implementation approaches to help an interested party choose the most appropriate approach based upon their situation.

### 5.2 Determination of trusted services

#### 5.2.1 General

An inspector needs to find or determine which TQPF can be involved with an object. That inspector should also decide a level of trust to associate with the involved TQPF. When selecting or developing object examination function, consideration should be given to the challenges a new or first time inspector faces in finding the TQPF.

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

#### 5.2.2 Trust in the TQPF

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 need to 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 (1) or just a few TQPF's 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.

#### 5.2.3 Use of prefix or postfix

Interoperability can be improved by using a standardized Data Identifier (DI) or Application Identifier (AI) as a prefix or postfix to assist the TQPF route the query to the correct TVF. The Bibliography lists several existing standards that define AI and DI.

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.

#### 5.2.4 Object examination techniques

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 object examination functions degrade as UID are lost or destroyed. Redundant and error-correcting elements can improve performance in such circumstances.

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

### 5.3 Management of object identification data and attributes

#### 5.3.1 Introduction

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.

#### 5.3.2 Verify the service entry point (TQPF)

Interested parties are advised to carefully consider the possibility that the service entry point might 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. Credential that attests 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.

### 5.3.3 Maintenance and management

The owner should 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 might need updating.

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

### 5.3.4 Privilege levels and user roles

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 might contain only publicly available information.

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

### 5.3.5 Access control

Industry practices for granting access rights are varied for many reasons, such as regulatory mandates, communication network constraints, equipment cost, and so forth. A few common access methods include

— user name and password challenge,

— digital certificates, and

— unique 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.

### 5.3.6 Ownership of transactional data

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.

### 5.3.7 Use of transactional data

UID codes without 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. Also 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.

### 5.3.8 Governmental or inter-governmental agencies or competent authorities

Governments or inter-governmental 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 need to 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 might be restrictions on cross-border access to data and services.

## 5.4 Common frauds

### 5.4.1 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, and

— 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, and

— 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, and

— physical uncountable functions or markings.

Adjacent physical security layer options include but are not limited to

— security papers, and

— inks, taggants, optically variable devices and other authentication features.

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

### 5.4.2 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

— supply chain,

— scrap, reclaim or reuse, and

— warranty replacement programs.

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

— tamper evident sealing technologies,

— white list of authorized sources,

— track and trace of UID code, inspectors, and inspections, and

— deactivating of UID codes.

### 5.4.3 Feature deception

While it seems obvious that the absence of an expected UID code indicates fraud, this is only true when the inspector know 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 owner or other experts, and

— public training and announcements.

### 5.4.4 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 re-routing fraud. Malicious service attacks include

— rerouting, sniffing, spoofing, redirecting, and

— 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,

— digital certificate,

— periodic check that root of trust is still valid,

— white list, and

— use trusted website 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.

### 5.4.5 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 were based on a need-to-know.

### 5.4.6 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, misconduct,

— malicious behaviour,

— inadequate security policy and training, and

— inside steals active UID codes.

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

— adequate security policies,

— avoid multiple authoritative sources of the same ID numbers, and

— activate UID codes only as they are properly used.

# Annex A
(informative)

# Digital certificate (for inspectors)

## A.1 Introduction

This annex shows one possible implementation of using X.509 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 could be used by all TQPF.

We want 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)

Use of digital certificate to achieve access control to ADMS is one of best practices, but then 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 attribute data management system. Higher trustworthiness can be achieved by using white list. White list is a list of trusted inspectors, managed and defined by the authoritative source.

## A.4 Trustworthiness of digital certificate

In order to ensure the trustworthiness of digital certificate, digital certificate issued by the CA accredited/certified body according to the following standards should be used.

— ETSI/TS 102 042;

— ETSI/TS 101 456;

— WebTrust for CA.

## A.5 Common field of digital certificate

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

Example of the common profile 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<br>– All capital letter | Administrator | JP |
| State name | Printable String (128) | – Name of state, province, etc.<br>– A head character is a capital letter | Administrator | Tokyo |
| Locality name | Printable String (128) | – Name of city, etc.<br>– A head character is a capital letter<br>– 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<br>– In order to distinguish in automatic verification, it shall attach the prefix "OU1-"[b] | Administrator | OU1-G2–1.2.392.200063.80.1.1 |
| OrganizationUnitName2 | Printable String (64) | – Identifier, which RA or LRA manages<br>– In order to distinguish in automatic verification, it shall attach the prefix "OU2-"[c] | RA or LRA | OU2–007 |
| Common name | Printable String (64) | – Subject's name (real name, section name, role or ID)<br>– 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 Mngr.) |

[a] It shall use the name which is registered in QGIS or QIIS.

[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 could not be recorded on the certificate.

[c] It can be used as a pointer to the secret attribute information (section name, etc.), which could not 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 could be inhibitors to sharing information with competent authorities due to contractual restrictions and legal ramifications.

## B.2 Master data

Master data are defined as 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, weight, 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 lifecycle management.

## B.3 Transactional data

Transactional data are dynamic, supply chain event-driven data, which can also be defined as 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 Introduction

This Annex shows a few implementations of object identification systems and how different implementations still follow the generic model offered by this standard.

The function blocks instances can vary. The blocks show in each example were 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) – i.e. product and packaging traits,

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

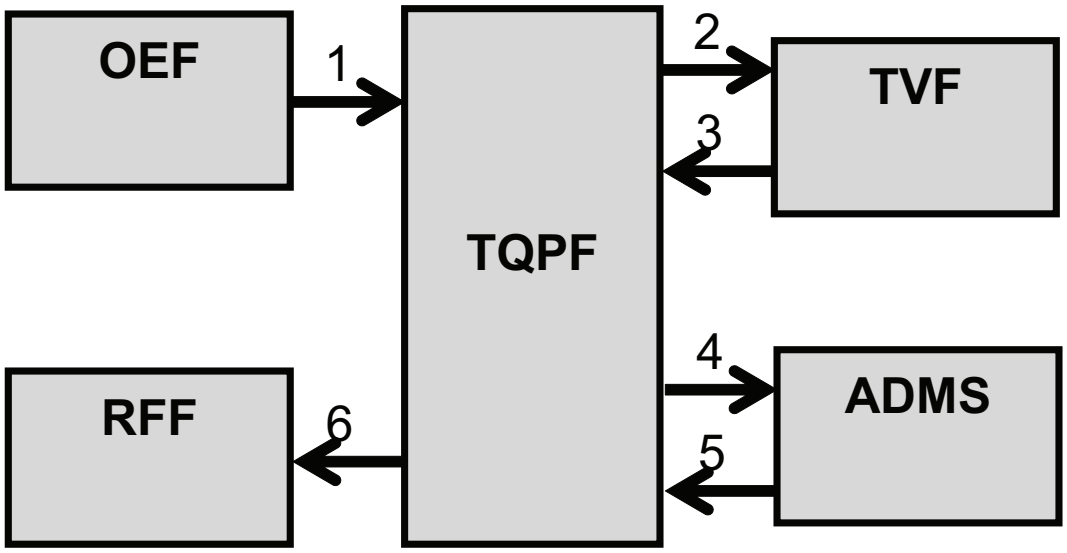
— descriptive for a lot of objects – i.e. shipment information, information on buyers and sellers of a lot of objects, and

— descriptive for a single item – i.e. 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, we expect many instances of each class UID to exist, but only one object UID is expected. Finding two identical class UID is not unusual whereas finding two identical object UID tells us something is wrong. However, object UID typically have higher implementation and maintenance overhead than class UID.

## 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.




**Key**

A typical query is as follows:

1 OEF extracts UID from object and sends query to TQPF.

2 TQPF evaluates inspector's credentials against the rules and routes conforming queries to TVF.

3 TVF checks validity of UID. If UID is valid and inspector credentials are acceptable, TVF returns a pointer for attribute data.

4 TQPF routes accepted queries (plus attribute pointer) to ADMS. Queries rejected by TVF by-pass the ADMS are routed directly to RFF for presentation to inspector.

5 ADMS evaluates inspector's credentials against access rules and replies to conforming queries with attribute data.

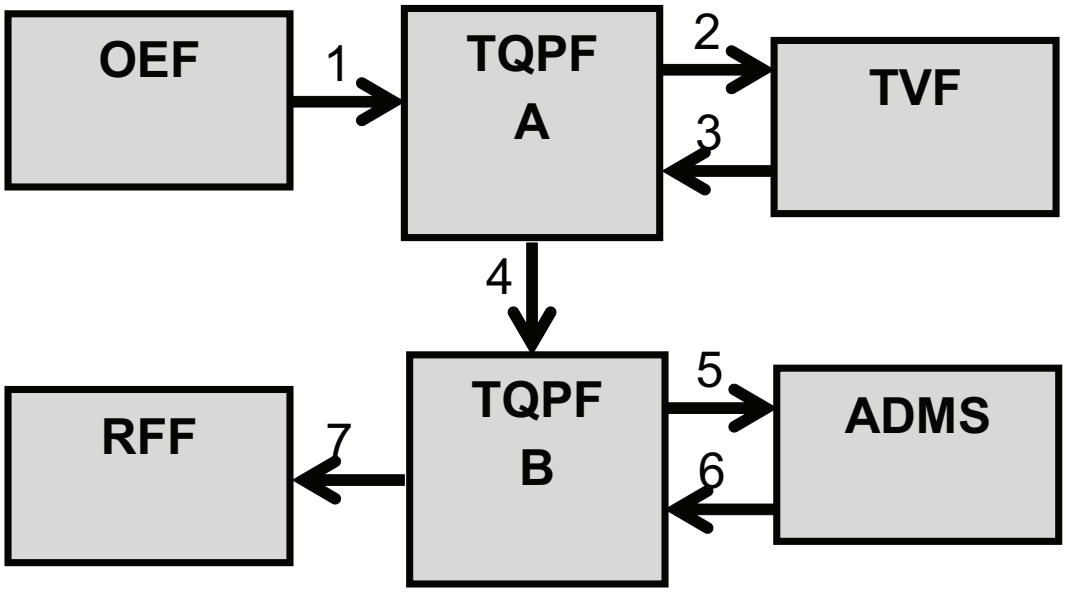
6 TQPF routes reply to RFF for presentation to inspector.

NOTE Counterfeits are detected when attributes reported to the inspector do not match attributes of the object.

**Figure C.1 — Class UID, no authentication function**

## C.4 Instance UID, no authentication function example

This implementation uses instance UIDs, where each object carries a different UID. Each UID points to attributes of one object. Other objects might or might not have identical attributes. It can be that only the UIDs themselves are unique within the class of object and all objects in the class have identical attribute and would be indistinguishable with a UID.




**Key**

A typical query is as follows:

1 OEF extracts UID from object and sends query to TQPF.

2 TQPF evaluates inspector's credentials against the rules and routes conforming queries to TVF.

3 TVF checks validity of UID. If UID is valid and inspector credentials are acceptable, TVF returns a pointer for attribute data.

4 TQPF routes accepted queries (plus attribute pointer) to second and independent TQPF (This example illustrates that functions can be split. In this case, TQPF-A knows locations of TVF functions while TQPF-B knows locations of ADMS.).

5 The second TQPF routes the query to the ADMS. Queries rejected by TVF by-pass the ADMS are routed directly to RFF for presentation to inspector.

6 ADMS evaluates inspector's credentials against access rules and replies to conforming queries with attribute data.

7 TQPF routes reply to RFF for presentation to inspector.

NOTE 1 Counterfeits are detected when attributes reported to the inspector do not match attributes of the object.

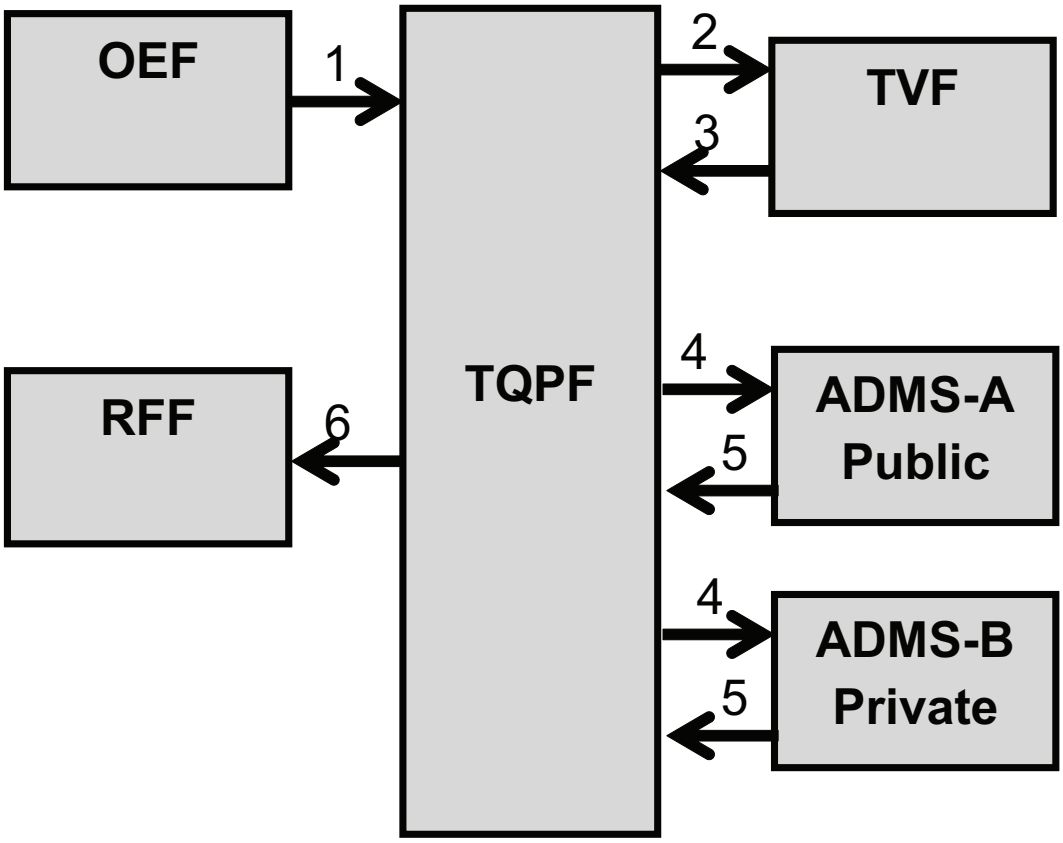
NOTE 2 Counterfeits can be detected when an instance specific UID is queried too many times.

NOTE 3 Counterfeits can be detected when an instance specific UID claims to be at two or more locations at the same time.

**Figure C.2 — Instance UID, no authentication function**

## C.5 Class UID, with authentication function example

This implementation uses class UID where public master data are stored in ADMS-A and confidential master data are stored in ADMS-B. During set-up, the owner loaded descriptive attributes that apply to every object in the class into the ADMS. Each UID points to one set of object attributes in the ADMS'es. Only inspectors providing a credential accepted by the rules loaded in ADMS-B will receive responses containing confidential (private) master data.




**Key**

A typical query is as follows:

1 OEF extracts UID from object and sends query to TQPF.

2 TQPF evaluates inspector's credentials against the rules and routes conforming queries to TVF.

3 TVF checks validity of UID. If UID is valid and inspector credentials are acceptable, TVF returns a pointer for attribute data.

4 TQPF routes accepted queries (plus attribute pointer) to ADMS-A, B; queries rejected by TVF by-pass the ADMS are routed directly to RFF for presentation to inspector.

5 Each ADMS-A, B evaluates inspector's credentials against access rules and replies to conforming queries with attribute data.

6 TQPF routes reply to RFF for presentation to inspector.

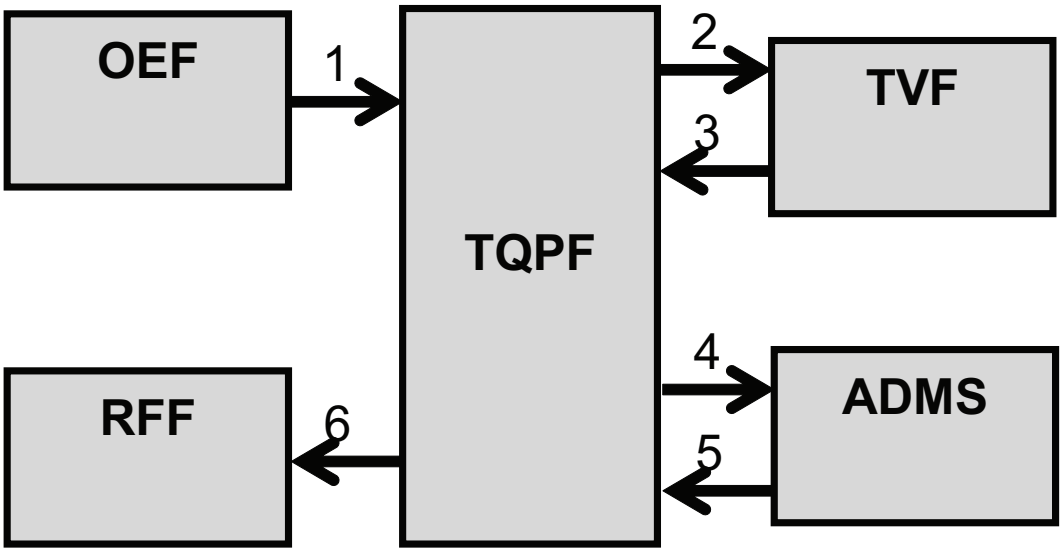
NOTE 1 Counterfeits are detected when attributes reported to the inspector do not match attributes of the object.

NOTE 2 Counterfeits are detected when the TVF performs a verification on the authentication element.

**Figure C.3 — Class UID, with authentication function**

## C.6 Instance UID, with authentication function example

This implementation uses instance UIDs, where each object carries a different UID. Each UID points to attributes of one object. Other objects might or might not have identical attributes. It can be that only the UIDs themselves are unique within the class of object and all objects in the class have identical attribute and would be indistinguishable with a UID.




**Key**

A typical query is as follows:

1 OEF extracts UID from object and sends query to TQPF.

2 TQPF evaluates inspector's credentials against the rules and routes conforming queries to TVF.

3 TVF checks validity of UID. If UID is valid and inspector credentials are acceptable, TVF returns a pointer for attribute data.

4 TQPF routes accepted queries (plus attribute pointer) to ADMS. Queries rejected by TVF by-pass the ADMS are routed directly to RFF for presentation to inspector.

5 ADMS evaluates inspector's credentials against access rules and replies to conforming queries with attribute data.

6 TQPF routes reply to RFF for presentation to inspector.

NOTE 1 Counterfeits are detected when attributes reported to the inspector do not match attributes of the object.

NOTE 2 Counterfeits can be detected when an instance specific UID is queried too many times.

NOTE 3 Counterfeits can be detected when an instance specific UID claims to be at two or more locations at the same time.

NOTE 4 Counterfeits are detected when the TVF performs verification on the authentication element.

**Figure C.4 — Instance UID, with authentication function**

# Bibliography

[1] ISO 3166-1, *Codes for the representation of names of countries and their subdivisions — Part 1: Country codes*

[2] ISO 3166-2, *Codes for the representation of names of countries and their subdivisions — Part 2: Country subdivision code*

[3] ISO 12931, *Performance criteria for authentication solutions used to combat counterfeiting of material goods*

[4] ISO 16022, *Information technology — Automatic identification and data capture techniques — Data Matrix bar code symbology specification*

[5] ISO/IEC 9594-8, *Information technology — Open Systems Interconnection — The Directory — Part 8: Public-key and attribute certificate frameworks*

[6] ISO/IEC 15418, *Information technology — Automatic identification and data capture techniques — GS1 Application Identifiers and ASC MH10 Data Identifiers and maintenance*

[7] ISO/IEC 15459 (all parts), *Information technology — Unique identifiers*

[8] ITU-T Recommendation X. 509 (03/00), Information Technology — Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks

[9] ETSI/TS 101456, *Electronic Signatures and Infrastructures (ESI); Policy requirement for certification authorities issuing qualified certificates*

[10] ETSI/TS 102042, *Electronic Signatures and Infrastructures (ESI); Policy requirement for certification authorities issuing public key certificates*

[11] ANSI MH 10.8.2, *Data Identifier and Application Identifier Standard*

[12] SEMI G83-0301, Specification for Bar Code Marking of Product Packages

[13] SEMI T15-0705, General Specification of Jig ID: Concept

[14] SEMI T19-0311, Specification for Device Marking

[15] SEMI T20-0710, Specification for Authentication of Semiconductors and Related Products

[16] SEMI T20.1-1109, Specification for Object Labelling to Authenticate Semiconductors and Related Products in an Open Market

[17] SEMI T20.2-1109, Guide for Qualifications of Authentication Service Bodies for Detecting and Preventing Counterfeiting of Semiconductors and Related Products

[18] SEMI T20.3-0710, Specification for Service Communication for Authentication of Semiconductors and Related Products

[19] SEMI T21-0212, Specification for Organization Identification by Digital Certificate Issued from Certificate Service Body (CSB) for Anti-Counterfeiting Traceability in Components Supply Chain

[20] SEMI T22-0212, Specification for Traceability by Self Authentication Service Body and Authentication Service Body

[21] Web Trust for CA — CA criteria designated from many browsers

[22] NIST Special Publication 800-63-1, Electronic Authentication Guideline

**ICS 13.310**
Price based on 24 pages

*This page deliberately left blank*

# British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

## About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

## Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

## Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

## Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

**PLUS** is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email bsmusales@bsigroup.com.

**BSI Group Headquarters**

389 Chiswick High Road London W4 4AL UK

## Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

## Copyright



## Useful Contacts:

**Customer Services**
**Tel:** +44 845 086 9001
**Email (orders):** orders@bsigroup.com
**Email (enquiries):** cservices@bsigroup.com

**Subscriptions**
**Tel:** +44 845 086 9001
**Email:** subscriptions@bsigroup.com

**Knowledge Centre**
**Tel:** +44 20 8996 7004
**Email:** knowledgecentre@bsigroup.com

**Copyright & Licensing**
**Tel:** +44 20 8996 7070
**Email:** copyright@bsigroup.com

bsi.

...making excellence a habit.™