INTERNATIONAL STANDARD

ISO 22381

First edition
2018-09

Security and resilience — Authenticity, integrity and trust for products and documents — Guidelines for establishing interoperability among object identification systems to deter counterfeiting and illicit trade

Reference number
ISO 22381:2018(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
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*.

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

Identification systems based on unique identifiers are no longer restricted to individuals' ID cards, car licence plates or telephone numbers. For many years, product identification has been well established in the world of things: unique identifiers are used on sales items and on their packaging, as well as on other sales and transport units. This is seen as a major step forward in consumer safety, in particular for uncovering counterfeit and illicit trade activities.

ISO 16678 outlines functional units and principles of systems based on unique identifiers. It has been established that interoperability of such systems is key to future deployment, enabled by the vast use of internet connectivity.

As object identification systems and various requirements by the public and the private sector are being created, there is urgent need to enable interoperability. The automation of processes on an interorganizational level is one of the core challenges of the digital era. By establishing interoperability, collaborating organizations strive for operational connectivity between their business processes and supporting infrastructures.

This guidelines document describes the landscape of safe, interoperable architectures. It encourages the vast deployment of object identification and authentication systems to deter counterfeits, product falsification and illicit trade, and to increase resilience against product fraud.

This allows industry and other sectors, confronted with the need to adopt object identification systems, to run multiple identification schemes in parallel.

Governments, associations, industry and other stakeholders in the battle against counterfeiting and illicit trade are encouraged to use this guidelines document. It is applicable to both simple and sophisticated object identification systems.

The guidelines aim to leave competition open to current and future solutions in object identification and authentication systems. By interoperability, the development of technologies, present and future, is maintained.

Figure 1 shows the process of planning, implementing and controlling systems' interoperability.

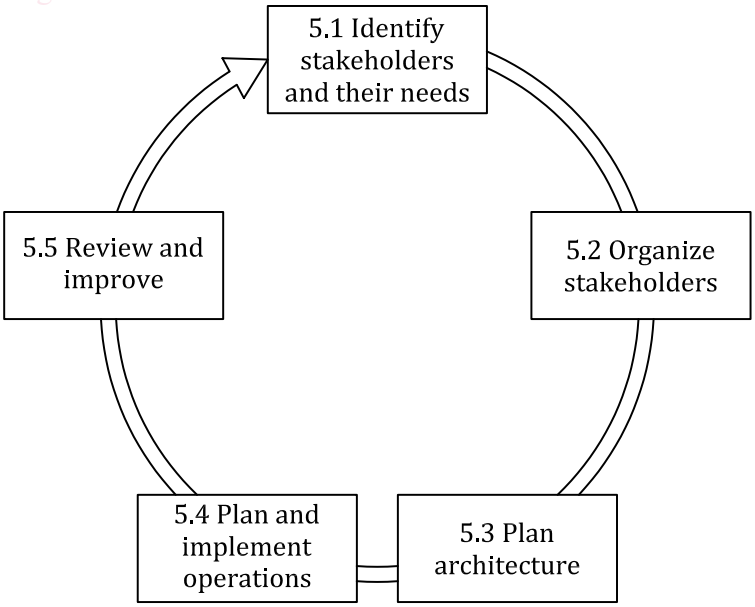

Figure 1 — Process of planning, implementing and controlling systems' interoperability

Security and resilience — Authenticity, integrity and trust for products and documents — Guidelines for establishing interoperability among object identification systems to deter counterfeiting and illicit trade

1 Scope

This document gives guidelines for establishing interoperability among independently functioning product identification and related authentication systems, as described in ISO 16678. The permanent transfer of data from one system to another is out of the scope of this document.

It also gives guidance on how to specify an environment open to existing or new methods of identification and authentication of objects, and which is accessible for legacy systems that may need to remain active.

It is applicable to any industry, stakeholder or user group requiring object identification and authentication systems. It can be used on a global scale, or in limited environments. This document supports those involved in planning and establishing interoperation.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. 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 and the following apply.

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

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

3.1
attribute
category of information that comprises the content of object identification and authentication systems

3.2
inspector
anyone who uses the object examination function with the aim of evaluating an object

[SOURCE: ISO 16678:2014, 2.1.10, modified — The notes to entry have been deleted.]

3.3
lead stakeholder
single stakeholder organizing interoperability of object identification and authentication systems (I-OPs), a group of stakeholders or a dedicated legal entity governing an I-OP

4 Abbreviated terms

AAF	attribute assignment function
ADMS	attribute data management system
I-OP	interoperability of object identification and authentication system
NFC	near field communication
OEF	object examination function
OIAS	object identification and authentication system
PUF	physically unclonable function
RFF	response formatting function
RFID	radio frequency identification device
TEP	trusted entry point
TQPF	trusted query processing function
TVF	trusted verification function
UID	unique identifier
UIDGF	UID generating function
VDS	visible digital seal

5 Planning, implementing and controlling systems' interoperability

5.1 Identify stakeholders and their needs

In each particular case, interoperability among product identification and authentication systems (I-OPs) is driven by one or several stakeholders, such as professional or private user groups, brand owners or regulating authorities.

All relevant stakeholders should be identified no matter how active their role is in creating the I-OP.

All identified stakeholders' interests, needs, objectives and capabilities should be analysed. This can be done by conducting interviews with the stakeholders and conducting literature studies as well as by using other sources, as applicable. In particular, expectations and obligations should be analysed concerning

— governance/control of OIASs,

— governance/control of particular functional blocs or subsystems thereof,

— data privacy,

— data ownership,

— access rights,

— security levels, and

— funding of I-OPs or subsystems.

Annex A provides an overview of some of the typical stakeholders and can be used as a starting point for the identification of stakeholders and their possible needs and expectations.

5.2 Organize stakeholders

5.2.1 Identify lead stakeholder

One of the identified stakeholders, or an entity representing a group of stakeholders, should take the initiative to be the lead stakeholder.

The role of lead stakeholder can change over time.

5.2.2 Define roles and responsibilities

The lead stakeholder should address the other identified stakeholders and negotiate their roles and responsibilities, such as

— whose viewpoints need to be considered,

— who can fund what, and

— who can decide what.

This should be described in an agreement among the stakeholders who are intended to become part of contractual relationships.

Depending on the business model, the lead stakeholder should implement the relevant business structures to maintain the I-OP and its funding.

5.2.3 Develop a contractual framework

The lead stakeholder should investigate the regulations and technical means that are available and feasible to develop a written contractual framework covering

— roles and responsibilities in planning, constructing and operating an I-OP,

— expected inputs and outcomes,

— categorization of types of data,

— access rights and ownership of these categories of data,

— security levels of participating functional units,

— security levels of transactions,

— new dependencies among participating systems or functional units, and

— I-OP system's review and continuous improvement.

The lead stakeholder should employ methods and measures to mitigate identified risks, such as

— contractual and reputational risk,

— liabilities,

— conformities,

— noncompliance with legal environments,

— fraud and counterfeiting, and

— system vulnerability and failures.

As a measure of mitigating fraud risks, the availability of public security technical frameworks to support the integrity of data access, transport and exchange should be considered.

As the I-OP can create new dependencies among participating systems or functional units, these should be addressed in the contractual framework.

5.2.4 Set up an onboarding and leaving process

The lead stakeholder should set up procedures for onboarding the I-OP and should establish the rules for out-phasing for when participants leave.

5.3 Plan architecture

5.3.1 General principles

The lead stakeholder should consider the following general principles in establishing the I-OP.

The I-OP creates decentralized data management environments in which participating systems continue to function independently.

The I-OP requires that UIDs remain unambiguous over all participating services, over a defined or undefined timespan.

UIDs can be depicted and stored by different print and storage formats, such as

— human readable text,

— barcodes,

— 2D codes,

— RFIDs of different standards, and

— others.

The lead stakeholder should outline which print, storage and reading techniques will be compatible with the I-OP as planned. It is considered best practice not to narrow down the choice of presentations to a degree beyond technical necessity or affordability.

The I-OP should be based on trusted functions. Trust levels should be defined for each type of participating functional unit, such as for

— the receiver of the request (TEP),

— the system that processes the request (TQPF),

— the system that verifies the UID (TVF),

— the system that answers the request (RFF), and

— the information exchanged (ADMS).

The I-OP refers to data exchange among OIASs or their functional blocs, including data

— access,

— retrieval,

— inputs, and

— outputs.