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.

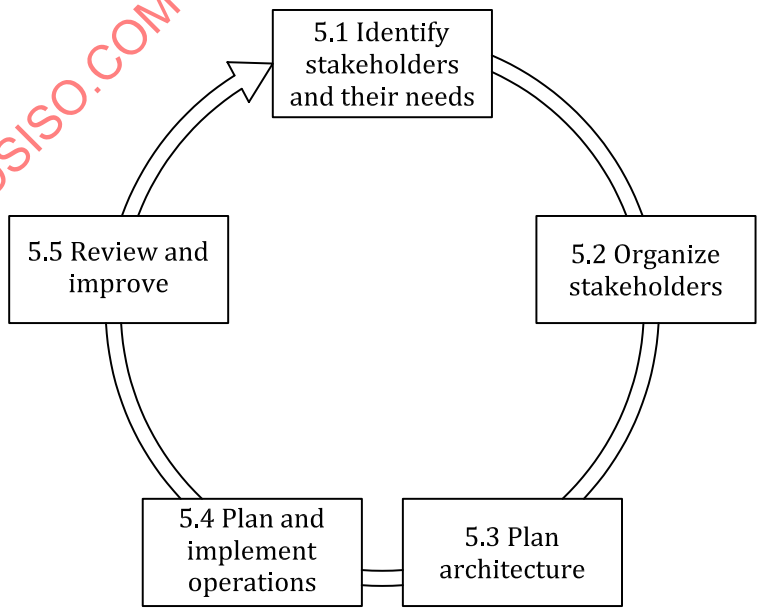

Figure 1 — Process of planning, implementing and controlling systems' interoperability

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.

Some OIASs use UIDs which themselves represent a group of subordinate UIDs. For example, the UID of a shipping box could be related to all UIDs of the items inside, often referred to as aggregated UIDs.

Data exchange can be achieved by

— routing and linking,

— data input, output and exchange, and

— data access and retrieval.

In case of routing and linking, information, which is not predefined or pre-structured, could be accessed, such as web pages coming as a response from a particular OIAS.

An I-OP can be established among, but is not limited to, systems focusing on

— object verification and authentication,

— supply chain traceability,

— life cycle traceability, or

— others and combinations of systems.

Participating OIASs or participating functional units of an OAIS can provide one, several or all of the above:

— OIASs with diverse focus points that can be connected via the I-OP;

— one OIAS or one functional bloc of OIAS that can connect to several I-OP frameworks simultaneously;

— one UID that can be used by different OIASs and I-OP frameworks.

Consideration should be given to different levels of quality and complexity of identification and authentication measures without bringing them down to the lowest common denominator.

This guidance is intended to also support pre-existing systems that need to be accessed and continuously used. This particularly applies for items that require identification during the entire life cycle, whereas technologies used for an I-OP can evolve further during that life cycle.

5.3.2 Identify participating OIASs and functional blocs to form the constituents of the I-OP

The I-OP designates interoperability among OIASs, as they are independently functioning, or among functional blocs of an OIAS.

These functional blocs (some of which are described in ISO 16678:2014) can comprise, but are not limited to

— AAF,

— ADMS,

— I-OP,

— OEF,

— RFF,

— TEP,

— TQPF,

— TVF,

— UID, and

— UIDGF.

The lead stakeholder should

— analyse which of these functional blocs are available or should be created,

— understand which stakeholders are controlling these functions, and

— confirm that this is in line with the contractual framework as established.

5.3.3 Study types and ownership of attributes to be handled

The lead stakeholder, when planning an I-OP, should study the types of attributes involved.

These can be

— attributes of origin (e.g. production batch, production date, manufacturer, expiry date, product name),

— attributes added intentionally by supply chain participants, to add trace or track information, and

— attributes created in the process of verification, and which could be unintentional (e.g. IP address, date, location of verification).

The choice of architecture should reflect stakeholder expectations and legal obligations towards these attributes, their confidentiality and ownership.

It should be decided if the interoperable architecture should be delimited to predefined categories of information, or whether participating services should share information that is non-structured and not predefined.

NOTE An expiration date is an example of a predefined semantic and syntactic content. A response web page from a participating OIAS displaying brand specific information is an example of a predefined content and layout.

Depending on the purpose of the I-OP, it should be clarified

— how much information will be shared, and

— how much this sharing will be structured.

After this has been defined, consideration should be given to attribute data

— ownership,

— right to add or change,

— obligation to add or change,

— availability and access rights, and

— security profiles in all aspects of creating, handling and accessing these data.

Use cases for the exchange of structured and unstructured information, advantages and drawbacks are given in Annex C.

5.3.4 Specify TEPs for secure I-OP access

The lead stakeholder in the I-OP should explore technically and economically feasible solutions to specify TEPs for the intended user groups.

OIASs are used as a means to deter counterfeiting and illicit trade. However, they are exposed to potential fraud, such as the occurrence of parallel systems. Such fraudulent systems could link to illegitimate websites, possibly unnoticed by the user.

By establishing the I-OP, this risk can be reduced by the establishment of TEPs. The goal of TEPs is to reduce or eliminate the risk of users being fooled by a multiplicity of entry points. The lead stakeholder should define security mechanisms within the I-OP, which should be maintained for the TEPs.

TEPs could be organized or operated by

— a trustworthy TEP provider,

— by the involvement of a trusted third party as a provider, or

— by the implementation of encryption techniques, VDSs or other mechanisms to raise trust.

Since a single UID can be used by multiple OIASs for different purposes, the lead stakeholder should take care that the TEP is able to resolve any ambiguity of multiple UIDs.

The use of trust signs is recommended. They can be visible to human eyes or be designed for electronic recognition.

Trust signs for electronic recognition could be employed as means against code-cloning or against code-generation by unauthorized sources.

If trust signs for electronic recognition are considered to be part of an I-OP, the lead stakeholder should check the TEP's ability to use these functionalities, particularly in a heterogeneous environment of UIDs with and without trust signs.

When using visible trust signs, it should be determined if they will guide users or if such trust signs could, in fact, fool users. When visible trust signs are used, their use should be promoted through independent communication channels.

5.3.5 Specify access rules for users

The lead stakeholder should

— determine how to define and apply user access rules supported by functional blocs, such as TEP, TQPF, TVF, ADMS and RFF, and

— consider responsibilities towards data privacy, as well as practical feasibility, depending on the I-OP architecture chosen (see 5.3.8) when taking an informed decision.

5.3.6 Define and improve trust levels

The lead stakeholder should

— establish trust levels that are appropriate to the targeted purposes of the I-OP and consistent with the contractual framework,

— define (minimum) trust levels,

— consider the role, availability and feasibility of encryption techniques, electronic signatures, VDSs and comparable technologies,

— employ technologies that are defined by their efficiency without being prescriptive, leaving them open to future technological development, and

— determine opportunities to raise trust levels in the I-OP by security mechanisms, thereby reducing opportunities for unwanted or illicit data harvesting, be it attributes of origin, tracing and tracking information, or metadata created by verification queries.

Security measures can be supported by third parties. As with the other parties participating in the I-OP, third parties may be public or private, and may be subject to audits.

In I-OPs, trustworthiness of participating OIASs and their functional blocs can be heterogeneous. In such an I-OP architecture, the lead stakeholder should outline a classification of trust levels and prepare a communication strategy for users to assist them in deciding on a trust level of information retrieved or assigned.

5.3.7 Outline or delimit the usage of participating OIASs and their functional units

In its core functionality, to combat, for example, counterfeiting and product falsification, trusted authentication and identification services (OIASs) provide evidence about the identity and provenience of a product.

Many systems go beyond this, taking advantage of the multi-use capacity of UIDs. They can offer functions such as supply chain traceability, consumer communication and more.

Some OIASs are interwoven with authentication. For example, upon verifying a UID, it can be required to check an authentication feature in a second step. It can also be vice versa: the authentication feature needs to be checked first.

Such combinations of authentication by a feature and identification by a UID can also be subject of an interoperation function. In this case, the device for verification itself can, but does not have to, become part of interoperation.

It should be considered good practice not to eliminate such combined authentication elements for identification and authentication when an I-OP is established, thus to neither lower the security level nor lower the multi-use capacity of the OIAS.

5.3.8 Draft an I-OP architecture

An I-OP could be established in different ways and on different system levels, the lowest common denominator being TEPs, which link to several independent OIASs by their functional blocs.

I-OP architectures could aim at simplifying the usage and access for particular user groups, making it easier and more secure by establishing TEPs (see Annex B).

I-OP architectures could also manage the exchange of or access to attribute data, which are under diverse ownerships, or which changes custodianship, as items and their UIDs travel through the supply chain.

I-OP architectures could include multi-usage of UIDs.

I-OP architectures also could include interoperation of OIASs of different focus and trust levels.

5.3.9 Return information back to the source

The lead stakeholder should be aware of what is in and out of scope when planning interoperability (I-OP) of unique code systems to deter counterfeiting and illicit trade (OIAS).

A prerequisite for establishing an I-OP is the existence or creation of systems and functional blocs working independently.

If there were no information exchange, but one-directional data forwarding to an ultimate RFF, this could deprive the source, such as an ADMS of participating OIASs, from information necessary to analyse the root causes of fraud, such as product falsification, counterfeiting and illicit trade.

The lead stakeholder should aim to feed back the results of an I-OP in object identification and authentication to the relevant sources of the information shared.

5.4 Plan and implement operations

5.4.1 Define data exchange formats

Where standardized interfaces and exchange formats exist, these should be preferably considered, together with other criteria, such as performance, security or cost.

Special consideration should be given to publicly available formats and security mechanisms related to digital trust in electronic transactions.

5.4.2 Establish trust into the service behind a particular UID

The lead stakeholder should set up strategies and rules regarding how participating OIASs and their functional blocs can be unambiguously addressed.

Thus, UIDs need to contain or need to be obviously related to identifiers.

Identification of the TVF can be achieved by amendments to the UID, such as

— a data identifier (DI),

— an application identifier (AI),

— a unique address (URL, IP address),

— a product name or code, by which the service can be found in an intermediate step,

— a sign to designate the TEP, machine readable or as a visual appearance, or both, and

— other means of identifying the service to be established in the future.

5.4.3 Delimit data inputs and outputs

For operation of an I-OP, expected inputs into participating OIASs and outputs from them or their functional units should be planned.

Inputs could include, for example

— trace information: collecting locations, time-stamps, organizations,

— track information: collecting information of an item's next destination,

— verifications, (e.g. counting the frequency of verifications), and

— statistical material that is collected as users access the system, such as IP addresses or geo-localization.

Typical outputs could include information such as

— whether a particular OID exists,

— whether it has been assigned to the particular object, where it is present,

— whether there a recall on the product,

— other information related to the product (e.g. various user group specific attributes),

— tracking and tracing information for a particular product: where has it been sent to, where has it been, where it is now, etc., and

— statistical and other information related to an item and its UID.

When planning the architecture of interoperation, it should be defined whether inputs or outputs or both are being addressed.

Communication options should be outlined on an IT technical level.

Interfaces should include the handling of failure and denial, to enable and support automated processes and the creation of statistics, and for continuous improvement measurement.

5.4.4 Define storage and custodianship of data inputs and outputs

The lead stakeholder should define for an I-OP, including data inputs, where the various categories of attribute data should be stored and made accessible.

In particular, transactional data and their hosting should be clearly defined. Such attributes could be input into the same system that hosts the attributes of origin, or they could be hosted in third parties' and other systems.

5.4.5 Define operational responsibilities

The lead stakeholder should lay out operational guidelines and should establish a sound platform of communication among participating functional blocs and legal entities.

Each participating organization should

— define which of its functions or departments is involved in running the participating OIASs or functional units,

— identify the responsible persons, and

— keep all the functions that are authorized by rights owners (e.g. brand owners, public or governmental agencies) available for the I-OP system.

5.4.6 Prepare for systems failures

The participating organizations should establish a protocol for stakeholders to communicate, particularly in the case of failure. The protocol should include information for right holders about any incidents and alerts, be they real or caused by technical defects.

5.4.7 Negotiate alarm responses of common interest

In an I-OP, denials and failures can be caused by various participating functions or communication issues. These can be due to technical malfunctions; however, they can be an indicator of serious technical or malicious events also and should alert the inspector. Such events can lead to alarms, be it in automated check procedures and the data produced in consequence, or be it in checking by users, creating uncertainty and mistrust. When planning and implementing the I-OP, the lead stakeholder should

— identify an appropriate way to handle and communicate denials and systems failures, and

— define operational procedures.

The lead stakeholder should ensure that the operational procedures cover

— possible reaction procedures in case of incidents,

— responses to users in case of system failure or denial, while considering the minimal damage to the reputation of participants, and

— instructions for careful wording for failures and alarms, subject to legal advice, including disclaimers.

5.4.8 Run pilots

It is advised to run step-by-step pilots to reaffirm architectures as agreed.

In particular, the lead stakeholder should

— involve all systems and functional units as planned,

— involve representatives of all stakeholders as identified,

— challenge the technology employed, the IT-interfaces, communication and robustness, and

— test the overall practicality of the I-OP as planned.

5.5 Review and improve

5.5.1 General

The lead stakeholder should review and continually improve the I-OP.

5.5.2 Revisit stakeholders' expectations

The lead stakeholder should

— evaluate, monitor and confirm that the targets set in the contractual framework are met,

— revisit stakeholders' needs and expectations and assess how they are covered by the I-OP implementation, and

— monitor indicators and challenge measurable goals where applicable.

5.5.3 Review operations

The lead stakeholder should

— review the contracts and rules set up for operations,

— confirm their suitability, and

— monitor the parameters set up for operations (e.g. response times, service levels, availability and failure rates).

5.5.4 Review security

The lead stakeholder should review the security and integrity of the I-OP and check, on a regular basis, against the requirements defined in the operational guidelines.

The integrity of data, their accessibility and ownership, and possibly unauthorized access or use should be challenged, in particular regarding

— attributes of origin,

— attributes of transaction, and

— data created by using the system.

There is a risk of obsolescence for security measures. Therefore, as part of the review, it should be checked that security measures are up-to-date.

5.5.5 Review technology

The lead stakeholder should

— re-evaluate the I-OP and its technical constituents to determine whether newer, more secure, more cost-efficient or otherwise better versions are available,

— evaluate and test the organizational and financial impacts of switching technology, and

— implement changes to alternative technologies in an I-OP environment only following a validation process.

Annex A
(informative)

Typical stakeholder interests in an I-OP

Table A.1 can be used as a starting point for the identification of stakeholders and their possible interests, as suggested in 5.1.

Table A.1 — Typical stakeholder interests in an I-OP

Stakeholder interests	Service providers	Regulators	Industry associations	Brand owners	Supply chain participants	Users
Being future proof Many stakeholders want OIASs to be future proofed. Therefore, they do not want to be bound to a single service provider, for reasons such as — being open to new developments and technologies, — being open to negotiate among several service providers, — being able upscale the usage, and — mitigating the risk of service providers going out of business. To be future proof, stakeholders often want to be able to include legacy systems in interoperation.	X	X	X	X		
I-OPs among reliable parties Stakeholders, such as brand owners, can run an interoperable scheme under their own control. If brand owners connect to an external interoperable framework, they want to be certain about the reliability of the third party providing interoperation. Brand owners also aim for a situation where they can be certain that only legitimate service providers of TQPFs will be able to interoperate, as well as legitimate users.				X		

Table A.1 *(continued)*

Stakeholder interests	Service providers	Regulators	Industry associations	Brand owners	Supply chain participants	Users
Multiple use of codes Brand owners often want to use one and the same UID in multiple ways and for multiple purposes. For example, one UID could be stored in different databases and could be connected to different services and I-OP schemes independently. Such a UID, used in multiple ways, could be able to fulfil different private or public tasks simultaneously, in different countries and markets. This adds flexibility and allows for cost sharing to several functions and purposes, with regards to creation, storage and print of the UID.				X		
Control of data Brand owners strive to retain control over data provided and retrieved. Such data can be product attribute data, batch information, data generated by track and trace functions, data derived from users and others.				X	X	
Common language When an I-OP is set up, a common language and terminology is needed, which describes functional blocs, typical transactions and typical use cases in architecture. The definition of these elements facilitates the establishment of interoperable product identification within an industry or segment. It helps to define the scope of interoperation and to select the architecture that best fits.			X			
Applicability to different life cycle models There are structural differences in operation for products that are used and consumed once versus products that have a longer life cycle, including re-use. Industry, therefore, wants to be able to address all of these products, and to make interoperable object identification and authentication systems applicable for all industries.			X			

Table A.1 *(continued)*

Stakeholder interests	Service providers	Regulators	Industry associations	Brand owners	Supply chain participants	Users
Benefiting from and participating in private initiatives Regulators can decrease the capital costs of excise bands or direct marking by leaving ownership/maintenance of OIASs with brand owners. Comprehensive and timely information can be made available for field inspectors interested in the legitimacy of product in the market, if an I-OP among private and public verification systems is established.		X	X			
Supplement to anti-counterfeiting regulations Authorities want to have a standard that can be adopted for national and international rules and trading regulations, for example to combat counterfeiting and illicit trade. The standard can be used as a supplement to national or international guidelines and regulations.		X	X			
Quick implementation of OIASs Interoperation of OIASs, as compared with larger and more encompassing governmental integrated systems, facilitates quicker implementation, if regulation is established for traceability or track and trace. It reduces switching costs or proprietary technology lock-in with a provider after a proprietary traceability solution is deployed. Interoperation should lead to faster and wider adoption of OIASs by governments and the industry.	X	X	X			
Interoperation among governmental implementations Governments running their own systems (e.g. for excise stamps) on their own behalf, want to retain ownership over ADM and sometimes also over code generation. By establishing interoperation among national entities, these traits of independence can be maintained, while creating means to detect and eliminate undeclared products, and to fight false declarations, etc., thanks to reliable data that can be cross-checked between administrations.		X				

Table A.1 *(continued)*

Stakeholder interests	Service providers	Regulators	Industry associations	Brand owners	Supply chain participants	Users
Open future development and competition An I-OP should work for any object identification and authentication system. A multiplicity of solutions should work. Interoperation should leave the market open for new technology, and to any new method of identification and/or authentication. OIAS providers do not want to give up individual identification technologies and systems for one common system, which is likely to be less open to future improvement.	X					
Standardized data exchange formats Service providers are interested in the definition of basic sets of data, which are relevant in object identification and related authentication systems. The use of standardized data exchange formats should be the prerequisite or result of establishing interoperation. Types of data exchange and interfaces should be defined, including human readable text, automatically readable printed codes and PUFs or RFID/NFC.	X					
Definition of functional blocs and interfaces Functional blocs, as defined in ISO 16678, are the basis to define architectures and interfaces. This provides a future proof frame for the development of services. It enables efficient communication when new I-OP frameworks are being set up, which include several service providers.	X	X	X			
Clarity on legal obligations and liabilities Legal requirements can be different in various legal domains. To ensure they comply with them, service providers need a clear description of the architecture (data format, purpose of the service) to take the responsibility in involved legal environments. Liabilities should be defined when interoperation takes place.	X	X	X			