



BSI Standards Publication

**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**

National foreword

This British Standard is the UK implementation of ISO 22381:2018.

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

© The British Standards Institution 2018
Published by BSI Standards Limited 2018

ISBN 978 0 580 98803 5

ICS 03.100.01

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 October 2018.

Amendments/corrigenda issued since publication

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

INTERNATIONAL STANDARD

ISO
22381

First edition
2018-09-30

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)
Documents
Document Sharing Hub
© ISO 2018



COPYRIGHT PROTECTED DOCUMENT

© ISO 2018, Published in Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

Page

Foreword	iv
Introduction	v
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Abbreviated terms	2
5 Planning, implementing and controlling systems' interoperability	2
5.1 Identify stakeholders and their needs	2
5.2 Organize stakeholders	3
5.2.1 Identify lead stakeholder	3
5.2.2 Define roles and responsibilities	3
5.2.3 Develop a contractual framework	3
5.2.4 Set up an onboarding and leaving process	4
5.3 Plan architecture	4
5.3.1 General principles	4
5.3.2 Identify participating OIAs and functional blocs to form the constituents of the I-OP	5
5.3.3 Study types and ownership of attributes to be handled	6
5.3.4 Specify TEPs for secure I-OP access	6
5.3.5 Specify access rules for users	7
5.3.6 Define and improve trust levels	7
5.3.7 Outline or delimit the usage of participating OIAs and their functional units	8
5.3.8 Draft an I-OP architecture	8
5.3.9 Return information back to the source	8
5.4 Plan and implement operations	9
5.4.1 Define data exchange formats	9
5.4.2 Establish trust into the service behind a particular UID	9
5.4.3 Delimit data inputs and outputs	9
5.4.4 Define storage and custodianship of data inputs and outputs	10
5.4.5 Define operational responsibilities	10
5.4.6 Prepare for systems failures	10
5.4.7 Negotiate alarm responses of common interest	10
5.4.8 Run pilots	11
5.5 Review and improve	11
5.5.1 General	11
5.5.2 Revisit stakeholders' expectations	11
5.5.3 Review operations	11
5.5.4 Review security	11
5.5.5 Review technology	12
Annex A (informative) Typical stakeholder interests in an I-OP	13
Annex B (informative) The role of trusted entry points for user groups	18
Annex C (informative) Types of information exchanged in I-OP architectures	19
Bibliography	20

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.

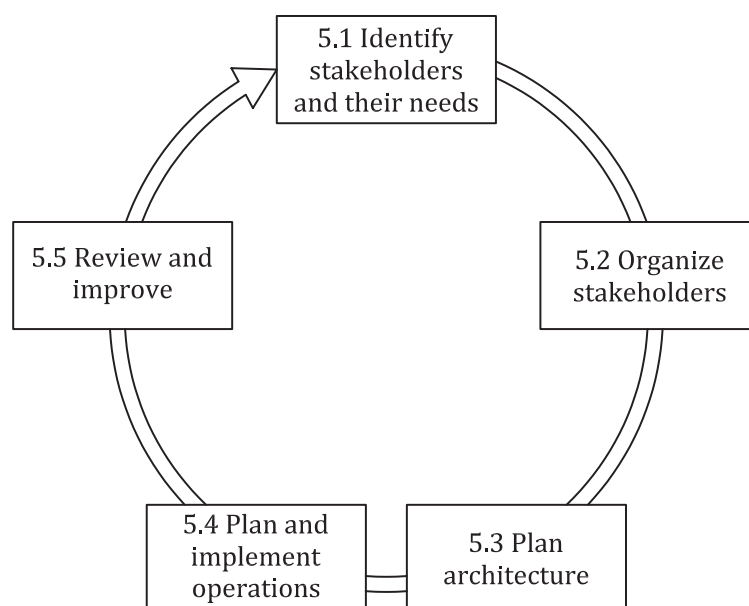


Figure 1 — Process of planning, implementing and controlling systems' interoperability

This page deliberately left blank

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