INTERNATIONAL STANDARD

ISO 22388

First edition
2023-11

Security and resilience — Authenticity, integrity and trust for products and documents — Guidelines for securing physical documents

Sécurité et résilience — Authenticité, intégrité et confiance pour les produits et les documents — Lignes directrices visant à sécuriser les documents physiques

Reference number
ISO 22388:2023(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO document 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).

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents. ISO shall not be held responsible for identifying any or all such patent rights.

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

Documents perform key functions in economic, legal and social transactions, including but not limited to financial interactions, ownership titles, title transfers, transportation, identity verification, customs transactions, academic records, professional licences and gun permits. These roles make them a target for counterfeiting, alteration and other forms of fraud, thereby potentially reducing the reliability of such transactions and creating economic, human and social hazards.

This document is intended to support the review of physical documents used in all kinds of usage contexts and to enable evaluation of physical document designation. Such evaluation also involves assessment to determine risk levels from the most common forms of attack, with consideration of the type and number of security features to be incorporated into documents for authentication. Based on such review and evaluation, these guidelines are expected to serve as guidelines for securing all designated security documents (SDs).

It is important to consider the usage of physical documents for threat and risk assessment and for determining their classification. Common documents can carry a high level of risk when used for critical functions. These guidelines assist in performing risk assessment for various document categories, but they are not intended to identify all potential uses of the documents.

This document is intended to support users and producers in determining security recommendations for documents produced or procured, to establish a relative classification of their documents and to enhance the reliability of transactions supported by such documents.

It should be acknowledged that these guidelines provide guidance on common risks, threats and mitigation treatments at the time of publication. As the security risks to physical documents are constantly changing, so are the mitigating security technologies. Therefore, it is important that users of these guidelines recognize that the risk and mitigation rates are relative and can change based upon a change in risk and the evolution of security technologies to mitigate that risk. It is recommended that the user of these guidelines understands the concepts used in developing a security risk assessment and performs an evaluation of any appropriate newly developed security technologies to establish the most effective solution.

Examples of risks that are not addressed in this document:

— technical risks arising, for example, when applicable security tools are applied improperly;

— management risks relating to document examination from inadequate or no supervision, or lack of training of personnel assigned to examine documents;

— organizational risks, including illegal collection of data from examined documents or insiders who deliberately overlook counterfeit documents in exchange for economic gain or as a part of a criminal enterprise [e.g. security staff allowing under-age entry based on counterfeit identification (ID), internal fraud at licensing agencies where personnel consciously overlook counterfeit ID to issue valid ID];

— external risks meaning impacts outside the control of affected organizations (e.g. power outages or short-term equipment failure);

— compliance risks occurring when a company fails to comply with mandated laws or regulations, which can result in fines or legal actions.

This document has been developed on the basis of concepts and methodologies adapted from Reference [7].

Security and resilience — Authenticity, integrity and trust for products and documents — Guidelines for securing physical documents

1 Scope

This document gives guidance on how to secure physical documents for specifying entities of physical documents. It establishes a procedure for security design, which includes:

— risk assessment;

— determination of document classes;

— introduction of security features;

— security evaluation;

— document risk mitigation.

This document is applicable to secure physical documents that are used for important actions such as validating value transactions, providing access, demonstrating compliance and securing products.

This document does not apply to banknotes, machine-readable travel documents, driving licences, postage stamps, tax stamps, health cards or national identity cards covered by existing standards and regulations.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 22300, *Security and resilience — Vocabulary*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 22300 and the following apply.

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

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

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

3.1
document fraud
wrongful or criminal deception that utilizes *security documents* (3.4) for financial or personal gain

Note 1 to entry: Fraud means wrongful or criminal deception intended to result in financial or personal gain that creates social or economic harm.

Note 2 to entry: Fraud includes false use that does not necessarily involve the recreation of documents (e.g. an impostor, using someone else's ID for impersonation).

Note 3 to entry: Fraud related to digitally transmitted electronic media should be considered separately.

3.2
risk communication
exchange or sharing of information about risk between an issuer and other interested parties

Note 1 to entry: The information can relate to the existence, nature, form, probability, severity, acceptability, treatment or other aspects of risk.

[SOURCE: ISO 22300:2021, 3.1.220, modified — Definition revised.]

3.3
forensic
<physical document> application of scientific methodologies for authenticating documents by confirming a *security feature* (3.6) or an intrinsic attribute through the use of specialized equipment by a skilled expert with special knowledge

3.4
security document
SD
document protected by a combination of features selected to mitigate the risk of counterfeit

3.5
specifying entity
person or organization who defines the requirements for authentication solution to be applied to a particular *security document* (3.4)

3.6
security feature
feature of a document that is linked to a specific method of verification and thus helps ensure the document's integrity and/or authenticity as a properly issued document, including that it has not been tampered with

[SOURCE: ISO/IEC 18013-1:2018, 3.27]

3.7
blank document
document ready to personalize after uniformed background printing on the substrate

Note 1 to entry: Background printing often includes *security features* (3.6).

4 Document security principles

4.1 User's category

In relation to the document authentication, potential users are categorized as follows:

— General: SD holders and third-party related users performing document processing.

— Specific: counter staff, document checkers and others providing prescribed services, with true-false check, based on issuer-defined document functions.

— Authorities and experts: parties setting SD specifications, staff at official investigative and analytical organizations with verification expertise, and other inspectors with deep knowledge of security specifications.

The specifying entity should specify document security considering the user resources shown in Table 1. See also Table D.1.

Table 1 — Users and resources

Users	Resources		
	Time available for inspection[a]	Expertise or training	Access to inspection tools
General	Limited	Limited or none	Limited or none
Specific	Medium	Medium	Medium
Authorities and experts	Extensive	Extensive	Extensive

[a] For a correct inspection, the inspection time required should match the user availability.

4.2 Document stages

The specifying entity should use the following stages when describing the life cycle of an SD, see also Figure 1:

— Security design, which is the incorporation of security measures against various types of document fraud that threaten each process in the document life cycle. This process includes review and improvement of document security.

— Blank document production, which includes the implementation of specifications related to design and the overall manufacturing process, including the acquisition of raw materials, production, quality checking, testing, storage and, operationally, transportation to a personalization entity.

— Personalization, which incorporates the integration of variable content such as monetary values, personal qualification information and credentials for certification elements on blank documents as required by the issuer.

— Issuance, which is the act of delivering an SD to a validated entity.

NOTE Delivery involves the secure transportation of the SDs to the intended entity.

— Service lifetime, which is the length of time the document maintains its document function, including its security effectiveness.

— Revocation, which is the intentional discontinuation and disposal of SDs by an authorized entity. Documents are subjected to physical processes, such as stringent disposal to prevent reuse, printing, perforation and other acts, thereby ensuring discontinuation.

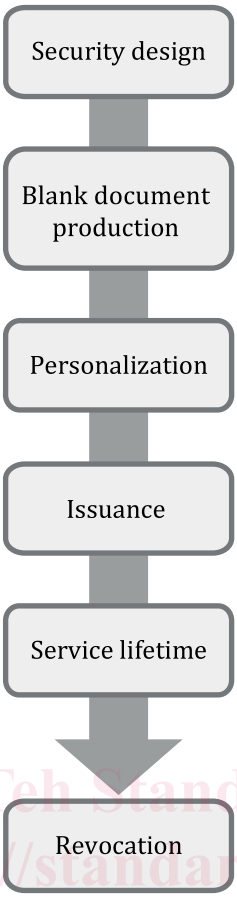

Figure 1 — Document linear progression stages

4.3 Elements to be protected

The specifying entity should protect the following from various threats:

— SDs (during all life cycles): SDs should be highly resistant to counterfeiting and should be verifiable. Official copies of SDs produced by photocopying or other means should be clearly marked as such.

— Manufacturing processes, including production, personalization and issuing processes.

— Integrity of recorded information: information recorded on SDs and related security features should remain in the original state provided by the issuer supported by the appropriate anti-counterfeiting or tampering features, which requires physical and chemical resistance. The counter measures should enable detection of fraudulent alterations such as data deletion, modification and overwriting.

Personalization impacts privacy; accordingly, designers and developers should apply the requirements of ISO 31700-1. Privacy protection is a matter of regulation in many jurisdictions.

4.4 Considerations for security manufacturing

The specifying entity should consider the following when designing and manufacturing SDs and in the setting of security features:

— Materials: composition, formulation and manufacture of raw materials used for security features should be securely controlled and materials should not be readily available to those attempting to fraud.

— Manufacturing machinery: devices used to provide and produce security features should be securely controlled and should not be readily available.

— Production methods: methods for the production of security features should be securely controlled.

NOTE 1 ISO 14298 provides guidance on the specifying entity for the management of security processes such as manufacture, storage, distribution and accountability.

— Principles: the principles, mechanisms and specifications of security features should be maintained in a secure and confidential manner.

— Quality stability: variances in quality among SDs at the time of security feature implementation and production should be minimized to prevent false counterfeit identification.

— Durability: SD authentication should be possible regardless of changes in appearance through use and aging (including individual differences present at the time of production).

NOTE 2 Securely controlled means materials and processes are controlled under accepted security practices such as ISO 14298 and Reference [8], or equivalent accepted security industry practices.

5 Document security design

5.1 General

The specifying entity should follow the security design procedure outlined in Figure 2 to manage risk associated with misuse or fraud aligned to ISO 31000 when developing the specification for SDs.

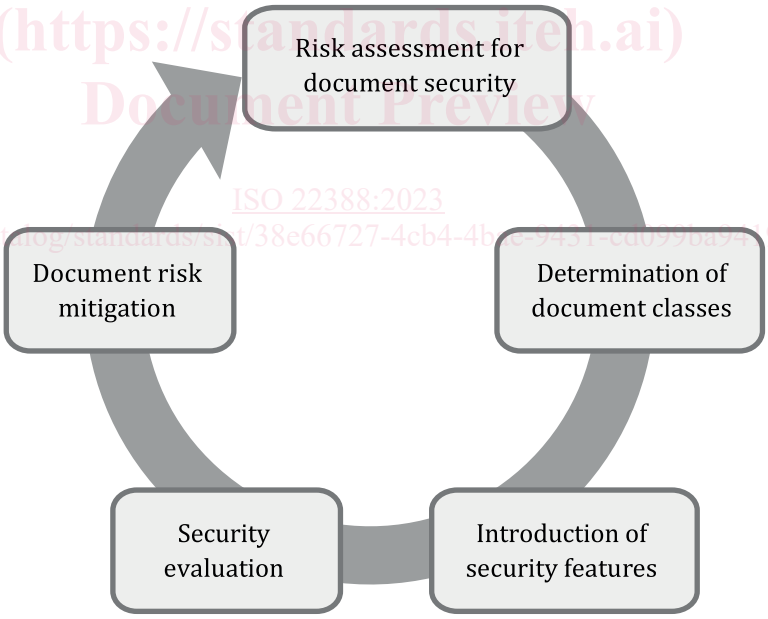

Figure 2 — Security design procedures

5.2 Risk assessment for document security

5.2.1 Estimation of risk

The specifying entity may perform a risk assessment on a document when an initial review indicates the possibility of fraud or misuse and the potential impacts if sources of risk are not mitigated. Where possible, the risk assessment methodology should draw on quantitative data and, where there are

degrees of uncertainty, recognize qualitative estimation as a guide for the assessment and be performed in consideration of:

— four modes of document fraud;

— intention and capability of known or potential threat actors;

— specific risk factors derived from document purpose, use, distribution and validity period.

NOTE An example of risk rate estimation for a general SD is provided in Annex A.

5.2.2 Four attack enablers of document fraud

Document fraud is generally divided into the following four modes of attack:

— Cloning: reproduction of original including security features employing the same base components and manufacturing techniques as the original. In this scenario, a party unauthorized to issue the document uses materials equivalent to or similar to the genuine versions, imitates the internal structure and creates a counterfeit with an appearance and characteristics similar to the original. Cloning is usually based on reverse engineering.

— Facsimile: an unauthorized reproduction of the original, including security features made with base components and manufacturing techniques different from those of the original version, but with an appearance being able to mislead the inspector. The internal structure and characteristics are not necessarily similar to those of the original.

— Alteration: changes made to a legitimate item, including deletion and insertion, replacement of genuine content and illegal rewriting of printed information or patterns.

— Theft or public acquisition (PA): the ability to readily obtain original security features by illicit or legitimate means.

NOTE Theft or PA is a protective security measure for physical handling control of the environment, which is not a characteristic of the document but rather an enabler of fraud.

5.2.3 Types of threat

One or more threats occur when a threat actor chooses to attack the document to gain advantage or reward. The success of such an attack is predicated on the threat actor having the intent and capability to cause harm. A potential attack can come from individuals or organized groups of varying size and can include:

— issue-motivated activist organizations;

— politically motivated groups or states;

— criminal organizations;

— opportunists or individuals seeking gain;

— insiders.

A threat actor's intent (motives and objectives) can be multiple or overlap (e.g. a terrorist group seeking both political or national advantage and conducting fraud to finance their operations). Intent can be driven by a range of motivations, including:

— revenge;

— financial gain;

— political advantage;

— reputation of threat actor or victim.