International Standard

ISO 13491-1

Financial services — Secure cryptographic devices (retail) —

Part 1: Concepts and requirements

Services financiers — Dispositifs cryptographiques de sécurité (services aux particuliers) —

Partie 1: Concepts et exigences

Fourth edition
2024-07

Reference number
ISO 13491-1:2024(en)

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 268, *Financial services*, Subcommittee SC 2, *Financial Services, security*.

This fourth edition cancels and replaces the third edition (ISO 13491-1:2016), which has been technically revised.

The main changes are as follows:

— revision for classes of secure cryptographic devices (SCDs);

— updated life cycle guidance.

A list of all parts in the ISO 13491 series can be found on the ISO website.

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

The ISO 13491 series describes both the physical and logical characteristics and the management of the secure cryptographic devices (SCDs) used to protect messages, cryptographic keys and other sensitive data used in a retail financial services environment.

This document contains the security requirements for SCDs. ISO 13491-2 is a tool for measuring compliance against these requirements. It provides a checklist of:

- characteristics that a device has to possess;
- how devices have to be managed;
- characteristics of the operational environments.

The security of retail electronic payment systems is largely dependent upon the security of these cryptographic devices. This security is based upon the premise that computer files can be accessed and manipulated, communications lines can be tapped and authorized data or control inputs into system equipment can be replaced with unauthorized inputs. When personal identification numbers (PINs), message authentication codes (MACs), cryptographic keys and other sensitive data are processed, there is a risk of tampering or other compromise to disclose or modify such data. The risk of financial loss is reduced through the appropriate use of cryptographic devices that have proper characteristics and are properly managed.

Appropriate device characteristics are necessary to ensure that the device has the proper operational capabilities and provides adequate protection for the data it contains. Appropriate device management is necessary to ensure that the device is legitimate, that it has not been modified in an unauthorized manner (e.g. by bugging) and that any sensitive data placed within the device (e.g. cryptographic keys) has not been subject to disclosure or change.

Absolute security is not achievable in practical terms. Cryptographic security depends upon each life cycle phase of the SCD and the complementary combination of appropriate management procedures and secure cryptographic characteristics. These management procedures implement preventive measures to reduce the opportunities for breaches of SCD security. The aim is for a high probability of detection of any unauthorized access to sensitive or confidential data in cases where device characteristics fail to prevent or detect the security compromise.

Financial services — Secure cryptographic devices (retail) —

Part 1: **Concepts and requirements**

1 Scope

This document specifies the security characteristics for secure cryptographic devices (SCDs) based on the cryptographic processes defined in the ISO 9564 series, ISO 16609 and ISO 11568.

This document states the security characteristics concerning both the operational characteristics of SCDs and the management of such devices throughout all stages of their life cycle.

This document does not address issues arising from the denial of service of an SCD.

This document does not address software services that use multi-party computation (MPC) to achieve some security objectives and, relying on these, offer cryptographic services.

NOTE These are sometimes called “soft” or software hardware security modules (HSMs) in common language, which is misleading and does not correspond to the definition of HSM in this document.

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 11568, *Financial services — Key management (retail)*

ISO 13491-2:2023, *Financial services — Secure cryptographic devices (retail) — Part 2: Security compliance checklists for devices used in financial transactions*

ISO/IEC 18031, *Information technology — Security techniques — Random bit generation*

NIST SP 800-90A, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*

NIST SP 800-90B, *Recommendation for the Entropy Sources Used for Random Bit Generation*

3 Terms and definitions

For the purposes of this document, the following terms and definitions 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
audit
evaluates compliance with an evaluation on behalf of an evaluation agency

3.2
auditor
person who conducts an *audit* (3.1)

3.3
attack
attempt by an adversary on the device to obtain or modify *sensitive data* (3.20) or a service they are not authorized to obtain or modify

3.4
controller
entity responsible for the secure management of a *secure cryptographic device (SCD)* (3.18)

3.5
derived unique key per transaction
DUKPT
key management method that uses a unique key for each transaction and prevents the disclosure of any past key used by the transaction originating *secure cryptographic device (SCD)* (3.18)

[SOURCE: ISO 11568:2023, 3.35]

3.6
device compromise
successful defeat of the physical or logical protections provided by the *secure cryptographic device (SCD)* (3.18), resulting in the potential disclosure of *sensitive data* (3.20) or unauthorized use of the SCD

3.7
device security
security of the *secure cryptographic device (SCD)* (3.18) related to its characteristics only, without reference to a specific *operational environment* (3.15)

3.8
device management
processes, including procedures, controlling the access to and use of the device

Note 1 to entry: These processes can vary depending on the deployed environment.

3.9
dual control
process of utilizing two or more separate individuals operating in concert to protect *sensitive functions* (3.21) or *sensitive information* (3.20) whereby no single individual is able to use the function or access all the information alone

Note 1 to entry: A cryptographic key is an example of the type of material protected by dual control.

[SOURCE: ISO 11568:2023, 3.39, modified — Note 2 to entry deleted.]

3.10
financial key
cryptographic key used to protect financial transaction data

EXAMPLE Entity’s public key used for mutual authentication with the payment terminal, initial derived unique key per transaction (DUKPT) key, terminal master key, personal identification number (PIN) encryption key.

3.11
hardware management device
HMD
non-*secure cryptographic device (SCD)* (3.18), typically a dedicated integrated circuit card (ICC), with security features similar to an SCD but lacking *tamper-response characteristics* (3.25), which provides a set of cryptographic services in support of the management of SCDs

Note 1 to entry: HMDs are subject to additional environment controls (see 5.2) due to their limited security features.

Note 2 to entry: Cryptographic services can include key generation, secure storage of key shares and key components, cryptogram creation and signature generation.

3.12
hardware security module
HSM
secure cryptographic device (SCD) (3.18) that provides a set of secure cryptographic services

Note 1 to entry: Secure cryptographic services can include key generation, cryptogram creation, personal identification number (PIN) translation and certificate signing.

3.13
key loading device
KLD
secure cryptographic device (SCD) (3.18) that loads keys into other SCDs

3.14
logical security
ability of a device to withstand *attacks* (3.3) through its functional interface

3.15
operational environment
environment in which the *secure cryptographic device (SCD)* (3.18) is operated, i.e. the system of which it is part, the location where it is placed, the persons operating and using it and the entities communicating with it

3.16
physical security
ability of a device to withstand *attacks* (3.3) against its physical construction, including exploitation of physical characteristics such as electromagnetic emissions and power fluctuations, the analysis of which can lead to side-channel attacks

3.17
public key infrastructure
PKI
structure of hardware, software, people, processes and policies that employs digital signature technology to facilitate a verifiable association between the public component of an asymmetric public key pair with a specific subscriber that possesses the corresponding private key

Note 1 to entry: The public key may be provided for digital signature verification, authentication of the subject in communication dialogues, and/or for message encryption key exchange or negotiation

[SOURCE: ISO 21188:2018, 3.48]

3.18
secure cryptographic device
SCD
device that provides physically and logically protected cryptographic services and storage, and which can be integrated into a larger system, such as an automated teller machine (ATM) or point-of-sale terminal

EXAMPLE Personal identification number (PIN) entry device (PED), *hardware security module (HSM)* (3.12).

3.19
security scheme
configuration that supports the secure status of the device

3.20
sensitive data
sensitive information
data which need to be protected against unauthorized disclosure, alteration or destruction

EXAMPLE Status information, cryptographic key, personal identification number (PIN).

3.21
sensitive function
function which is accessible when the device is in a *sensitive state* (3.22)

3.22
sensitive state
device condition that provides access to the secure operator interface, such that it can only be entered when the device is under *dual control* (3.9)

3.23
tamper-evident characteristic
characteristic that provides evidence that an *attack* (3.3) has been attempted

3.24
tamper-resistant characteristic
characteristic that provides passive physical protection against an *attack* (3.3)

3.25
tamper-response characteristic
characteristic that provides an active response to the detection of an *attack* (3.3)

4 Abbreviated terms

API	application programming interface
ATM	automated teller machine
DUKPT	derived unique key per transaction
EPP	encrypting PIN pad
HMD	hardware management device
HSM	hardware security module
KLD	key loading device
MAC	message authentication code
MPC	multi-party computation
PED	PIN entry device
PIN	personal identification number
PKI	public key infrastructure
POS	point of sale
SCD	secure cryptographic device
SCR	secure card reader
SCRP	SCR with PIN function

5 Secure cryptographic device concepts

5.1 General

Cryptography is used in retail financial services to help ensure the following objectives:

a) the integrity and authenticity of sensitive data (e.g. by using a MAC over transaction details);

b) the confidentiality of secret information (e.g. by encrypting customer PINs);

c) the confidentiality, integrity and authenticity of cryptographic keys;

d) the security of other sensitive operations (e.g. PIN verification).

To ensure that these objectives are met, the following threats to the security of the cryptographic processing shall be countered:

- unauthorized use, disclosure or modification of cryptographic keys and other sensitive data;
- unauthorized use or modification of cryptographic services.

A secure cryptographic device provides a defined set of cryptographic functions, access controls and secure key storage. SCDs are employed to protect against these threats. The requirements of this document pertain to the SCD and not the system in which the SCD might be integrated. However, it is important to analyse the interfaces between the SCD and the remainder of the system to ensure that the SCD will not be compromised.

Since absolute security is not achievable in practical terms, it is not realistic to describe an SCD as being “tamper proof” or “physically secure”. With enough cost, effort and skill, virtually any security scheme can be defeated. Furthermore, as technology continues to evolve, new techniques might be developed to attack a security scheme that was previously believed to be immune to feasible attack. Therefore, it is more realistic to categorize an SCD as possessing a degree of tamper protection where an acceptable degree is one that is deemed adequate to deter any attack envisaged as feasible during the operational life of the device, taking into account the equipment, skills and other costs to the adversary in mounting a successful attack and the financial benefits that the adversary could realize from such an attack.

Security of retail payment systems includes the physical and logical aspects of device security, the security of the operational environment and management of the device. These factors establish jointly the security of the devices and the applications in which they are used. The security needs are derived from an assessment of the risks arising from the intended applications.

The required security characteristics will depend on the intended application and operational environment and on the attack types that need to be considered. A risk assessment should be made as an aid to selecting the most appropriate method of evaluating the security of the device. The results are then assessed in order to accept the devices for a certain application and environment.

5.2 Hardware management devices

Some key management activities necessitate the use of non-SCD devices where their form factors have inherent limitations preventing them from meeting some SCD security requirements, especially tamper-responsiveness. These limitations have associated security risks which shall be addressed by restricted usage and additional controls. These devices are hardware management devices (HMDs).

Examples of HMDs include, but are not limited to:

a) smart cards used for component or share transport or storage;

b) smart cards containing public or private key pair(s) used to facilitate management of HSMs;

c) devices used to authorize or enable key management functions.

HMDs shall only be used in cases where the compromise of a single HMD would not compromise keys or secrets not held within that HMD.