INTERNATIONAL STANDARD

ISO 13491-2

Fifth edition
2023-01

Financial services — Secure cryptographic devices (retail) —

Part 2: Security compliance checklists for devices used in financial transactions

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

Partie 2: Listes de contrôle de conformité de sécurité pour les dispositifs utilisés dans les transactions financières

Reference number
ISO 13491-2:2023(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 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 68, *Financial services*, Subcommittee SC 2, *Financial services, security*.

This fifth edition cancels and replaces the fourth edition (ISO 13491-2:2017), which has been technically revised.

The main changes are as follows:

— an additional subclause, H.5, is added to Annex H and the entire Annex H is reordered for clarity;

— editorially revised.

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

This document specifies both the physical and logical characteristics and the management of the secure cryptographic devices (SCDs) used to protect messages, cryptographic keys and other sensitive information used in a retail financial services environment.

The security of retail financial services is largely dependent upon the security of these cryptographic devices.

Security requirements are based upon the premise that computer files can be accessed and manipulated, communication lines can be "tapped" and authorized data or control inputs in a system device can be replaced with unauthorized inputs. While certain cryptographic devices (e.g., host security modules) reside in relatively high-security processing centres, a large proportion of cryptographic devices used in retail financial services (e.g., PIN entry devices) now reside in non-secure environments. Therefore, when PINs, MACs, cryptographic keys and other sensitive data are processed in these devices, there is a risk that the devices can be tampered with or otherwise compromised to disclose or modify such data.

The risk of financial loss can be reduced through the appropriate use of cryptographic devices that have proper physical and logical security characteristics and are properly managed. To ensure that SCDs have the proper physical and logical security, they require evaluation.

This document provides the security compliance checklists for evaluating SCDs used in financial services systems in accordance with ISO 13491-1. Other evaluation frameworks exist and can be appropriate for formal security evaluations (e.g., ISO/IEC 15408-1, ISO/IEC 15408-2, ISO/IEC 15408-3 and ISO/IEC 19790) but are outside the scope of this document.

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) have not been subject to disclosure or change.

Absolute security is not practically achievable. Cryptographic security depends upon each life cycle phase of the SCD and the complementary combination of appropriate device management procedures and secure cryptographic characteristics. These management procedures implement preventive measures to reduce the opportunity for a breach of cryptographic device security. These measures aim for a high probability of detection of any illicit access to sensitive or confidential data in the event that device characteristics fail to prevent or detect the security compromise.

Financial services — Secure cryptographic devices (retail) —

Part 2: Security compliance checklists for devices used in financial transactions

1 Scope

This document specifies checklists to be used to evaluate secure cryptographic devices (SCDs) incorporating cryptographic processes as specified in ISO 9564-1, ISO 9564-2, ISO 16609, and ISO 11568 in the financial services environment. Integrated circuit (IC) payment cards are subject to the requirements identified in this document up until the time of issue, after which they are to be regarded as a "personal" device and outside of the scope of 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 9564-1, *Financial services — Personal Identification Number (PIN) management and security — Part 1: Basic principles and requirements for PINs in card-based systems*

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

ISO 13491-1, *Financial services — Secure cryptographic devices (retail) — Part 1: Concepts, requirements and evaluation methods*

ISO 16609, *Financial services — Requirements for message authentication using symmetric techniques*

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

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 13491-1 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
auditor
person or organization approved as an auditor by an approval authority

[SOURCE: ISO 9000:2015, 3.13.15]

3.2
data integrity
assurance that data has not been altered or destroyed in an unauthorized manner

3.3
dual control
process of utilizing two or more entities (usually persons) operating in concert to protect sensitive functions or information whereby no single entity is able to access or use the materials

Note 1 to entry: A cryptographic key is an example of the type of material to be accessed or utilized.

3.4
evaluation agency
organization trusted by the design, manufacturing, and sponsoring entities which evaluates the secure cryptographic device (using specialist skills and tools)

Note 1 to entry: Evaluation is in accordance with ISO 13491-1.

3.5
exclusive-or
bit-by-bit modulo two addition of binary vectors of equal length

3.6
security compliance checklist
list of auditable claims, organized by device type

Note 1 to entry: Checklist is as specified in this document.

3.7
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 or multiple control

3.8
sponsor
person or organization that requests a test

[SOURCE: ISO 20088-3:2018, 3.5]

4 Use of security compliance checklists

These checklists shall be used to assess the acceptability of cryptographic equipment upon which the security of the system depends. It is the responsibility of any sponsor, approval authority or accreditation authority, depending on the evaluation method chosen, that adopts some or all of these checklists to:

— approve evaluating agencies for use by suppliers to or participants in the system;

— set up an audit review body to review the completed audit checklists.

Annex A to Annex H, which provide checklists defining the minimum evaluation to be performed to assess the acceptability of cryptographic equipment, shall be applied. Additional tests may be performed to reflect the state of the art at the time of the evaluation.

A cryptographic device achieves security both through its inherent characteristics and the characteristics of the environment in which the device is located. When completing these audit checklists, the environment in which the device is located shall be considered, for example a device intended for use in a public location can require greater inherent security than the equivalent device operating in a controlled environment. So that an evaluating agency need not investigate the specific environment where an evaluated device may reside, this document provides a suggested categorization of environments in Annex H. Thus, an evaluating agency may be asked to evaluate a given device for operation in a specific environment. Such a device can be deployed in a given facility only if this facility itself has been audited to ensure that it provides the ensured environment. However, these audit checklists may be used with categorizations of the environment other than those suggested in Annex H.

Annex A
(normative)

Physical, logical and device-management characteristics common to all secure cryptographic devices

A.1 General

This annex is intended for use with all evaluations and shall be completed prior to any device-specific security compliance checklists.

The following statements in this security compliance checklist shall be specified by the auditor as "true (T)", "false (F)" or "not applicable (N/A)". A "false" indication does not necessarily indicate unacceptable practice but shall be explained in writing. Those statements that are indicated as "N/A" shall also be explained in writing.

A.2 Device characteristics

A.2.1 Physical security characteristics

A.2.1.1 General

All devices shall meet the criteria given in A.2.1.2 for general security characteristics, in A.2.1.5 for tamper-responsive characteristics and in A.2.1.3 for tamper-evident characteristics. Other devices shall additionally meet the criteria given in A.2.1.4 for tamper-resistant characteristics.

A.2.1.2 General security characteristics

An evaluation agency has evaluated the device bearing in mind susceptibility to physical and logical attack techniques known at the time of the evaluation, such as (but not limited to):

— chemical attacks (solvents);

— scanning attacks (scanning electron microscope);

— mechanical attacks (e.g. drilling, cutting, probing);

— thermal attacks (high and low temperature extremes);

— radiation attacks (X-rays);

— information leakage through covert (side) channels (e.g. power supply, timing);

— failure attacks.

The conclusions are given in Table A.1.

Table A.1 — General security characteristics

No.	Security compliance statement	True	False	N/A
A1	It is not feasible to determine a PIN, a key or other secret information by monitoring (e.g., the electromagnetic emissions from the device with or without the cooperation of the device operator).			

Table A.1 *(continued)*

No.	Security compliance statement	True	False	N/A
A2	Any ventilation and other openings in the module are positioned and protected so that it is not feasible to use such an opening to probe any component of the module such that plaintext PINs, access codes or cryptographic keys might be disclosed or to disable any of the protection mechanisms of the device.			
A3	All sensitive data and cryptographic keys, including residues, are stored in the security module.			
A4	All transfer mechanisms within the device are implemented in such a way that it is not feasible to monitor the device to obtain unauthorized disclosure of any such information.			
A5	Any access entry point into the device's internal circuitry is locked in the closed position when the device is operative, by means of one or more pick-resistant locks or similar security mechanisms.			
A6	The design of the device is such that a duplicate device cannot be constructed from components which are available through retail commercial channels.			
A7	If the device generates random numbers or pseudo-random numbers, then the generation of those numbers conforms to ISO/IEC 18031.			
A8	If the device generates random numbers or pseudo-random numbers, it is not feasible to influence the output of those numbers, for example by varying environmental conditions of the device, such as resetting or reinitializing the device or manipulating the power supply or electromagnetic injection.			

A.2.1.3 Tamper-evident characteristics

The conclusions of the evaluating agency are given in Table A.2.

Table A.2 — Tamper-evident characteristics

No.	Security compliance statement	True	False	N/A
A9	The device is designed and constructed so that it is not feasible to penetrate the device in order to: — make any additions, substitutions or modifications (e.g., the installation of a bug) to the hardware or software of the device; or — determine or modify any sensitive information (e.g., PINs, access codes, and cryptographic keys); and then subsequently return the device without requiring specialized skills and equipment not generally available and: a) without damaging the device so severely that the damage would have a high probability of detection; or b) requiring that the device be absent from its intended location for a sufficiently long time that its absence or reappearance would have a high probability of being detected.			

A.2.1.4 Tamper-resistant characteristics

The conclusions of the evaluating agency are given in Table A.3.

Table A.3 — Tamper-resistant characteristics

No.	Security compliance statement	True	False	N/A
A10	The device is protected against penetration by employing physical protection to such a degree that penetration is not feasible.			
A11	Even after having gained unlimited, undisturbed access to the device, discovery of secret information in the target device is not feasible.			

A.2.1.5 Tamper-responsive characteristics

The conclusions of the evaluating agency are given in Table A.4.

Table A.4 — Tamper-responsive characteristics

No.	Security compliance statement	True	False	N/A
A12	The device is protected against penetration by including features that detect any feasible attempts to tamper with the device and cause immediate erasure of all cryptographic keys and sensitive data when such an attempt is detected.			
A13	Removal of the case or the opening, whether authorized or unauthorized, of any access entry to the device's internal components causes the automatic and immediate erasure of the cryptographic keys stored within the device.			
A14	There is a defined method for ensuring that secret data or any cryptographic key that has been used to encrypt secret data is erased from the unit when permanently removing the unit from service (decommissioning). There is also a defined method for ensuring, when permanently decommissioned, that any cryptographic key contained in the unit that might be usable in the future is either erased from the unit or is invalidated at all facilities with which the unit is capable of performing cryptographically protected communications.			
A15	Any tamper detection or key erasure mechanisms function even in the absence of applied power.			
A16	If the device has no mechanism for detection of removal from its operational environment, then defeating the tamper detection mechanisms or discovery of secret information in the target device is not feasible, even when removed from its operational environment. Compromise of the device requires equipment and skill sets that are not readily available. As a possible example, discovery of such information requires a significant time, such as one month of preparation, including analysis of other devices and at least one week of effort to compromise the device after having gained unlimited, undisturbed access to the target device.			
A17	If the device has a mechanism for detection of removal from its operational environment, then defeating the tamper- detection mechanisms or discovery of secret information in the target device is not feasible. Compromise of the device shall require skill sets that are not readily available and equipment that is neither readily available at the device site nor can be feasibly transported to the device site. As a possible example, discovery of such information requires a significant time, such as one month of preparation, including analysis of other devices and at least 12 hours of unlimited, undisturbed access to the target device.			

A.2.2 Logical security characteristics

The conclusions of the evaluating agency are given in Table A.5.

Table A.5 — Logical security characteristics

No.	Security compliance statement	True	False	N/A
A18	The device includes self-test capabilities capable of manual or automatic initiation to ensure that its basic functions are operating properly.			
A19	The device only performs its designed functions.			
A20	It is not feasible to determine a key or other secret information by the use of diagnostic or special test modes.			
A21	The cryptographic algorithms, modes of operation and lengths of cryptographic keys used by the device conform to ISO 11568.			
A22	The device key management conforms to ISO 11568 using each key for only one cryptographic purpose (although a variant of a key may be used for a different purpose).			
A23	The functionality implemented within the device is such that there is no feasible way in which plaintext secret information (e.g., PINs or cryptographic keys) or secret information enciphered under other than the legitimate key can be obtained from the device, except in an authorized manner (e.g., PIN mailers).			
A24	If the device is composed of several components, it is not possible to move a secret cryptographic key within the device from a component of higher security to a component providing lower security.			
A25	The loading of keys is performed when: — the device is in a sensitive state; or — the action of loading a key puts the device into a mode that activates all the tamper-protection mechanisms within the device.			
A26	The following operator functions that may influence the security of a device are only permitted when the device is in a sensitive state, i.e., under dual or multiple control: — disabling or enabling of device functions; — change of passwords or data that enable the device to enter the sensitive state.			
A27	The secure operator interface is so designed that entry of more than one password (or some equivalent mechanism for dual or multiple control) is required in order to enter this sensitive state.			
A28	The secure operator interface is so designed that it is highly unlikely that the device can inadvertently be left in the sensitive state.			
A29	If sensitive state is established with multiple limits (e.g., on the number of function calls and a time limit), the device returns to normal state when the first of these limits is reached.			
A30	Where passwords or other plaintext data are used to control transition to a sensitive state, then these are protected in the same manner as other secret or sensitive information.			
A31	If cryptographic keys are lost for any reason (e.g., long-term absence of applied power), the device will enter a non- operational state.			

Table A.5 *(continued)*

No.	Security compliance statement	True	False	N/A
A32	The only function calls and sensitive operator functions that exist in the device are functions approved by the sponsor or the system in which the device is to operate.			
A33	Keys are never translated from encipherment under one variant to encipherment under another variant of the same key.			

A.3 Device management

A.3.1 General consideration

For each life cycle stage, the entity responsible for completing the audit checklist for that stage has provided assurance for the statements given in Table A.6.

Table A.6 — General consideration

No.	Security compliance statement	True	False	N/A
A34	For audit and control purposes, the identity of the device (e.g., its serial number) can be determined either by external tamper-evident marking or labelling or by a command that causes the device to return its identity via the interface or via the display.			
A35	When the device is in a life cycle stage such that it contains cryptographic keys, the identity of these keys can be easily determined from the identity of the device [so that the key(s) can be invalidated if the device is reported lost or stolen].			
A36	Any physical keys used to unlock or operate the device are carefully controlled and available only to authorized persons.			
A37	If a device contains a secret cryptographic key and there is an attack on a device, or a device is stolen, then procedures are in place to notify the party responsible for the security of the device immediately after detection.			
A38	If a device does not yet contain a secret cryptographic key and there is an attack on a device, or a device is stolen, then procedures are in place to prevent the substitution of the attacked or stolen device for a legitimate device that does not yet contain a secret cryptographic key.			
A39	If no sensitive state exists in the device, the loading of plaintext keys is performed under dual control.			

A.3.2 Device protection by manufacturer

The device manufacturer or an independent auditor has provided assurance, acceptable to the audit review body, for the statements given in Table A.7

Table A.7 — Device protection by manufacturer

No.	Security compliance statement	True	False	N/A
A40	The hardware and software design of the device has been evaluated to ensure that the functional capabilities provided with the device are all legitimate, documented functions and that no unauthorized function (e.g., a "Trojan horse") resides in the device.			