INTERNATIONAL STANDARD

**ISO 13491-2**

Third edition
2016-03-15

# 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 13491-2:2016(E)

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

# 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 on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is ISO/TC 68, *Financial services*, Subcommittee SC 2, *Security*.

This third edition cancels and replaces the second edition (ISO 13491-2:2005), which has been technically revised.

ISO 13491 consists of the following parts, under the general title *Financial Services — Secure cryptographic devices (retail)*:

— *Part 1: Concepts, requirements and evaluation methods,*

— *Part 2: Security compliance checklists for devices user in financial transactions*

# Introduction

This part of ISO 13491 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, etc.) 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 may be tampered with, or otherwise, compromised to disclose or modify such data.

It is to be ensured that the risk of financial loss is 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 part of ISO 13491 provides the security compliance checklists for evaluating SCDs used in financial services systems in accordance with ISO 13491-1. Other evaluation frameworks exist and may be appropriate for formal security evaluations, e.g. ISO/IEC 15408-1, ISO/IEC 15408-2, ISO/IEC 15408-3, and ISO/IEC 19790, and are outside the scope of this part of ISO 13491.

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.

**INTERNATIONAL STANDARD** **ISO 13491-2:2016(E)**

# Financial services — Secure cryptographic devices (retail) —

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

## 1 Scope

This part of ISO 13491 specifies checklists to be used to evaluate secure cryptographic devices (SCDs) incorporating cryptographic processes as specified in H.5, ISO 9564-2, ISO 16609, ISO 11568-1, ISO 11568-2, and ISO 11568-4 in the financial services environment. IC payment cards are subject to the requirements identified in this part of ISO 13491 up until the time of issue after which they are to be regarded as a “personal” device and outside of the scope of this part of ISO 13491.

This part of ISO 13491 does not address issues arising from the denial of service of an SCD.

In the checklists given in Annexes A to H, the term “not feasible” is intended to convey the notion that although a particular attack might be technically possible, it would not be economically viable since carrying out the attack would cost more than any benefits obtained from a successful attack. In addition to attacks for purely economic gain, malicious attacks directed toward loss of reputation need to be considered.

## 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 11568-1, *Banking — Key management (retail) — Part 1: Principles*

ISO 11568-2, *Financial services — Key management (retail) — Part 2: Symmetric ciphers, their key management and life cycle*

ISO 11568-4, *Banking — Key management (retail) — Part 4: Asymmetric cryptosystems — Key management and life cycle*

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.

**3.1**
**auditor**
one who has the appropriate skills to check, assess, review, and evaluate compliance with an informal evaluation on behalf of the sponsor or audit review body

**3.2**
**data integrity**
property 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 SCD (using specialist skills and tools) in accordance with ISO 13491

**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, as specified in this part of ISO 13491

**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

## 4 Use of security compliance checklists

### 4.1 General

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

a) approve evaluating agencies for use by suppliers to or participants in the system, and

b) set up an audit review body to review the completed audit checklists.

Annexes A to H provide checklists defining the minimum evaluation to be performed to assess the acceptability of cryptographic equipment. Additional tests may be performed to reflect the state-of-the-art at the time of the evaluation.

The evaluation may be either "informal", "semi-formal", or "strict semi-formal" as specified in ISO 13491-1. Should a "formal" evaluation be chosen, these audit checklists shall not be used as presented here, but shall rather be used as input to assist in the preparation of the "formal claims" that such an evaluation requires.

NOTE These formal claims, as they inherently include other criteria, are themselves outside of the scope of this part of ISO 13491.

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, e.g. a device intended for use in a public location could 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 part of ISO 13491 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.

The four evaluation methods specified in ISO 13491-1 are described in 4.2, 4.3, 4.4, and 4.5.

## 4.2 Informal evaluation

As part of an informal evaluation, an independent auditor shall complete the appropriate checklist(s) for the device being evaluated.

## 4.3 Semi-formal evaluation

In the semi-formal method, the sponsor, who may be the manufacturer, shall submit a device to an evaluation agency for testing against the appropriate checklist(s).

## 4.4 Strict semi-formal evaluation

In the strict semi-formal method, the sponsor, who may be the manufacturer, shall submit a device to an evaluation agency for testing against the appropriate checklist(s) determined by an approval authority.

## 4.5 Formal evaluation

In the formal method, the manufacturer or sponsor shall submit a device to an accredited evaluation agency for testing against the formal claims where the appropriate checklist(s) were used as input.

# 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 are required to 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 and the criteria given 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) the following:

- chemical attacks (solvents);
- scanning attacks (scanning electron microscope);
- mechanical attacks (drilling, cutting, probing, etc.);
- thermal attacks (high and low temperature extremes);
- radiation attacks (X-rays);
- information leakage through covert (side) channels (power supply, timing, etc.);
- failure attacks;

and has concluded the following:

**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 electro-magnetic emissions from the device with or without the cooperation of the device operator). | | | |
| **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 complies with ISO 18031. | | | |
| **A8** | If the device generates random numbers or pseudo random numbers, it is not feasible to influence the output of those numbers, e.g. by varying environmental conditions of the device such as resetting or reinitializing the device, or manipulating the power supply/electro-magnetic injection. | | | |

### A.2.1.3 Tamper-evident characteristics

The evaluating agency has concluded the following:

**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<br>— make any additions, substitutions, or modifications (e.g. the installation of a bug) to the hardware or software of the device, or<br>— determine or modify any sensitive information (e.g. PINs, access codes, and cryptographic keys)<br>and then subsequently, return the device without requiring specialized skills and equipment not generally available and<br>a) without damaging the device so severely that the damage would have a high probability of detection, or<br>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 evaluating agency has concluded the following:

**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 evaluating agency has concluded the following:

**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. | | | |

**Table A.4** *(continued)*

| No. | Security compliance statement | True | False | N/A |
|---|---|---|---|---|
| **A15** | Any tamper detection/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.<br>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 not readily available at the device site nor can be feasibly transported to the device site.<br>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 h of unlimited, undisturbed access to the target device. | | | |

### A.2.2 Logical security characteristics

The evaluating agency has concluded the following:

**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 comply with ISO 11568-1, ISO 11568-2, and ISO 11568-4. | | | |
| **A22** | The device key management complies with ISO 11568-1, ISO 11568-2, and ISO 11568-4 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. | | | |