INTERNATIONAL STANDARD

ISO 13491-2

Second edition
2005-06-15

Banking — Secure cryptographic devices (retail) —

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

Banque — 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 13491-2:2005(E)

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web 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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

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.

ISO 13491-2 was prepared by Technical Committee ISO/TC 68, *Financial services*, Subcommittee SC 2, *Security management and general banking operations*.

This second edition cancels and replaces the first edition (ISO 13491-2:2000) which has been technically revised.

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

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

— *Part 2: Security compliance checklists for devices used 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 must 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. parts 1 to 3 of ISO/IEC 15408 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.

Banking — 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 parts 1 and 2 of ISO 9564, ISO 16609 and parts 1 to 6 of ISO 11568, 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 document.

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 referenced documents are indispensable for the application 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 9564-1:2002, *Banking — Personal Identification Number (PIN) management and security — Part 1: Basic principles and requirements for online PIN handling in ATM and POS systems*

ISO 9564-2, *Banking — Personal Identification Number management and security — Part 2: Approved algorithms for PIN encipherment*

ISO 11568 (all parts), *Banking — Key management (retail)*

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

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

ISO 18031, *Information technology — Random number 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 A cryptographic key is an example of the type of material to be accessed or utilized.

3.4
exclusive or
bit-by-bit modulo two addition of binary vectors of equal length

3.5
security compliance checklist
list of auditable claims, organized by device type, as specified in this document

3.6
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 by the sponsor who wishes to assess the acceptability of cryptographic equipment upon which the security of the system depends. It is the responsibility of any sponsor 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” or “semi-formal”, as specified in ISO 13491-1, depending upon the nature of the evaluating agencies approved by the sponsor. Should the sponsor decide on a “formal” evaluation, 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 themselves are 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 must 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 assured environment. However, these audit checklists may be used with categorizations of the environment other than those suggested in Annex H.

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

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 manufacturer or sponsor shall submit a device to an evaluation agency for testing against the appropriate checklist(s).

4.4 Formal evaluation

In the formal method, the manufacturer or sponsor shall submit a device to an accredited evaluation authority 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 in A.2.1.3 for tamper-evident characteristics. Many devices shall additionally meet either the criteria given in A.2.1.4 for tamper-resistant characteristics or the criteria given in A.2.1.5 for tamper-responsive characteristics. However some devices need meet only the criteria for general security characteristics and tamper-evident characteristics. Such devices meet the following requirements:

a) the device retains no secret key that has ever been used to encipher any secret data, nor does it retain any information from which such a key could feasibly be determined, even with knowledge of any data that have ever been available in plaintext form;

b) the device is managed in such a way that there is a high probability of noting and reporting on a timely basis either the extended absence of the device from its authorized location, or any obvious damage to the device;

c) means exist at all facilities capable of direct cryptographic communication with the device to not process any enciphered data received from the device after it has been reported absent or damaged.

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 that:

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), when the device is operating in its intended environment.			
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.			
A5A	The design of the device is such that it is not practical to construct a duplicate device from commercially available components; e.g. the casing used to house the device's electronic components is not commonly available.			

A.2.1.3 Tamper-evident characteristics

The evaluating agency has concluded that:

No.	Security compliance statement	True	False	N/A
A6	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 re-install 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 evaluating agency has concluded that:

No.	Security compliance statement	True	False	N/A
A7	The device is protected against penetration by employing physical protection to such a degree that penetration is not feasible.			
A8	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 that:

No.	Security compliance statement	True	False	N/A
A9	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.			
A10	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.			
A11	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.			
A12	Any tamper detection/key erasure mechanisms function even in the absence of applied power.			
A13	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. NOTE 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.			
A14	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. NOTE 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 **twelve hours** of unlimited, undisturbed access to the target device.			