INTERNATIONAL STANDARD

ISO 13491-2

First edition
2000-11-01

Banking — Secure cryptographic devices (retail) —

Part 2: Security compliance checklists for devices used in magnetic stripe card systems

Banque — Dispositifs cryptographiques de sécurité (services aux particuliers) —

Partie 2: Listes de contrôle de conformité de sécurité pour les dispositifs utilisés dans les systèmes de cartes à bande magnétique

Reference number
ISO 13491-2:2000(E)

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.ch
Web www.iso.ch

Printed in Switzerland

Contents

Foreword ... iv
Introduction ... v
1 Scope ... 1
2 Normative references ... 1
3 Terms and definitions ... 2
4 Use of security compliance checklists ... 3
4.1 General ... 3
4.2 Informal evaluation ... 4
4.3 Semi-formal evaluation ... 4
4.4 Formal evaluation ... 4
5 Summary ... 4
Annex A (normative) Physical, logical and device management characteristics common to all secure cryptographic devices ... 5
Annex B (normative) Devices with PIN entry functionality ... 12
Annex C (normative) Devices with PIN management functionality ... 15
Annex D (normative) Devices with message authentication functionality ... 17
Annex E (normative) Devices with key generation functionality ... 19
Annex F (normative) Devices with key transfer and loading functionality ... 22
Annex G (normative) Devices with digital signature functionality ... 26
Annex H (informative) Categorization of environments ... 28

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 3.

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 part of ISO 13491 may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

International Standard ISO 13491-2 was prepared by Technical Committee ISO/TC 68, *Banking, securities and other financial services*, Subcommittee SC 6, *Retail financial services*.

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 magnetic stripe card systems*

Annexes A to G form a normative part of this part of ISO 13491. Annex H is for information only.

Introduction

This International Standard 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 banking environment.

The security of retail electronic banking 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, communications lines can be “tapped” and authorized data or control inputs into 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 banking (e.g. PIN pads, ATMs, 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 magnetic stripe systems in accordance with ISO 13491-1.

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 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 magnetic stripe card systems

1 Scope

This part of ISO 13491 specifies checklists to be used to evaluate secure cryptographic devices (SCDs) incorporating cryptographic processes, as specified in ISO 9564, ISO 9807 and ISO 11568, in a magnetic stripe card environment. It does not specify checklists for SCDs used in an integrated circuit card (ICC) environment.

This part of ISO 13491 does not address issues arising from the denial of service of a 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 prudent, 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 normative documents contain provisions which, through reference in this text, constitute provisions of this part of ISO 13491. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. However, parties to agreements based on this part of ISO 13491 are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. For undated references, the latest edition of the normative document referred to applies. Members of ISO and IEC maintain registers of currently valid International Standards.

ISO 7498-2, *Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture*.

ISO 8908, *Banking and related financial services — Vocabulary and data elements*.

ISO 9564-1, *Banking — Personal Identification Number management and security — Part 1: PIN protection principles and techniques*.

ISO 9564-2, *Banking — Personal Identification Number management and security — Part 2: Approved algorithm(s) for PIN encipherment*.

ISO 9807, *Banking and related financial services — Requirements for message authentication (retail).*

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

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

3 Terms and definitions

For the purposes of this part of ISO 13491, the terms and definitions given in ISO 13491-1 and ISO 8908 and the following apply.

3.1
accredited evaluation authority
body accredited in accordance with a set of rules (e.g. EN 45000 or ISO Guide 25) and accepted by the accreditation authority for the purpose of evaluation

3.2
attack
attempt by an adversary on the device to obtain or modify sensitive information or a service he/she is not authorized to obtain or modify

3.3
audit report
output of the audit review body based on the results from an auditor

3.4
audit review body
group with responsibility for reviewing and making judgements on the results from the auditor

3.5
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

3.6
device security
security of the SCD related to its characteristics only, without reference to a specific operational environment

3.7
evaluation agency
organization trusted by the design, manufacturing and sponsoring authorities which evaluates the SCD (using specialist skills and tools) in accordance with ISO 13491-2

3.8
evaluation report
output of the evaluation review body based on the results from an evaluation agency or auditor

3.9
evaluation review body
group with responsibility for reviewing, and making judgements on, the results of the evaluation agency

3.10
formal claims
statements about the characteristics and functions of a secure cryptographic device

3.11
logical security
ability of a device to withstand attacks through its functional interface

3.12
operational environment
environment in which the SCD is operated, i.e. the application system of which it is part, the location where it is placed, the persons operating and using it, the entities communicating with it

3.13
physical security
ability of a device to withstand attacks against its physical construction

3.14
secure cryptographic device
SCD
physically and logically protected hardware device that provides a set of secure cryptographic services

3.15
secure operator interface
interface which allows the protective mechanisms of the device to be disabled by using a data entry mechanism and which can only be accessed when the device is in a sensitive state

3.16
security compliance checklist
list of auditable claims, organized by device type, as specified in ISO 13491-2

3.17
sensitive data
sensitive information
data which must be protected against unauthorized disclosure, alteration or destruction, especially plaintext PINs and cryptographic keys, and which includes design characteristics, status information, etc.

3.18
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

3.19

software
programs and/or data that will be used within the SCD or downloaded for use by the SCD

3.20
sponsor
sponsoring authority
individual, company or organization that requires the SCD to undergo evaluation

3.21
tamper-evident characteristic
characteristic that provides evidence that an attack has been attempted

3.22
tamper-resistant characteristic
characteristic that provides passive physical protection against an attack

3.23
tamper-responsive characteristic
characteristic that provides an active response to the detection of an attack preventing its success

4 Use of security compliance checklists

4.1 General

These checklists shall be used by the evaluation sponsor that 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 give 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 check lists, the environment in which the device is located must be considered. For example, 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 International Standard 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. Then 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 check lists 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

5 Summary

The security compliance checklist is used in the evaluation method to determine compliance with the requirements of standards listed in the references of this International Standard where the estimated risk is seen as low. It is recommended for use whenever the security compliance statements are facts that can be verified without the need for specialized knowledge or skills. In general, compliance with functional requirements can be performed by means of security compliance checklists.

In the context of this part of ISO 13491, international acceptance means the level of assurance required for a device, as agreed by the participants in an international organization.

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 which 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 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 has 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 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 into 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 to 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.			

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: 1) without damaging the device so severely that the damage would have a high probability of detection, or 2) requiring 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.			