INTERNATIONAL STANDARD

ISO 13491-1

Third edition
2016-03-15

Financial services — Secure cryptographic devices (retail) —

Part 1: Concepts, requirements and evaluation methods

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

Partie 1: Concepts, exigences et méthodes d'évaluation

Reference number
ISO 13491-1:2016(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

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 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 13491-1:2007), 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 used in financial transactions*

Introduction

ISO 13491 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 information used in a retail financial services environment.

This part of ISO 13491 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, and

— 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 opportunity for a breach of SCD security. This aims for a high probability of detection of any unauthorized access to sensitive or confidential data should device characteristics fail to prevent or detect the security compromise.

Financial services — Secure cryptographic devices (retail) —

Part 1: Concepts, requirements and evaluation methods

1 Scope

This part of ISO 13491 specifies the security characteristics for secure cryptographic devices (SCDs) based on the cryptographic processes defined in ISO 9564, ISO 16609, and ISO 11568.

This part of ISO 13491 has two primary purposes:

- to state the security characteristics concerning both the operational characteristics of SCDs and the management of such devices throughout all stages of their life cycle;
- to provide guidance for methodologies to verify compliance with those requirements. This information is contained in Annex A.

ISO 13491-2 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, ISO 11568-1, ISO 11568-2, ISO 11568-3, ISO 11568-4, ISO 11568-5, and ISO 11568-6 in the financial services environment.

Annex A provides an informative illustration of the concepts of security levels described in this part of ISO 13491 as being applicable to SCDs.

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

Specific requirements for the security characteristics and management of specific types of SCD functionality used in the retail financial services environment are contained in ISO 13491-2.

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*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1
accreditation authority
authority responsible for the accreditation of evaluation agencies and supervision of their work in order to guarantee the reproducibility of the evaluation results

3.2
accredited evaluation agency
body accredited in accordance with a set of rules and accepted by the approval authority for the purpose of evaluation

Note 1 to entry: An example of a set of rules is ISO/IEC 17025.

3.3
approval authority
authority responsible for the approval of devices and for issuance of the *approval letter* (3.4)

3.4
approval letter
output of the *approval authority* (3.3) based on the results from an *evaluation review body* (3.20)

3.5
assessment checklist
list of claims, organized by device type, and contained in ISO 13491-2

3.6
assessment report
output of the *assessment review body* (3.7), based on the results from an *assessor* (3.8)

3.7
assessment review body
group with responsibility for reviewing and making judgements on the results from the *assessor* (3.8)

3.8
assessor
person who checks, assesses, reviews, and evaluates compliance with an informal evaluation on behalf of the *sponsor* (3.33) or *assessment review body* (3.7)

3.9
attack
attempt by an adversary on the device to obtain or modify *sensitive information* (3.30) or a service they are not authorized to obtain or modify

3.10
evaluation certificate
output of the accreditation authority based on the results from an *accredited evaluation agency* (3.2)

3.11
controller
entity responsible for the secure management of an *SCD* (3.28)

3.12
deliverables
documents, equipment, and any other items or information needed by the evaluators to perform an evaluation of the *SCD* (3.28)

3.13
device compromise
successful defeat of the physical or logical protections provided by the *SCD* (3.28), resulting in the potential disclosure of *sensitive information* (3.30) or unauthorized use of the SCD

3.14
device security
security of the *SCD* (3.28) related to its characteristics only, without reference to a specific *operational environment* (3.26)

3.15
device management
processes, including procedures, controlling the access to and use of the device which may vary depending on the deployed environment

3.16
dual control
process of utilizing two or more separate entities (usually persons) operating in concert to protect *sensitive functions* (3.31) or information whereby no single entity is able to access or utilize the materials

EXAMPLE A cryptographic key is an example of the type of material protected by dual control.

3.17
environment-dependent security
security of an *SCD* (3.28) as part of an *operational environment* (3.26)

3.18
evaluation agency
organization trusted by the design, manufacturing, and sponsoring entities which evaluates the *SCD* (3.28) (using specialist skills and tools) in accordance with ISO 13491

3.19
evaluation report
output of the *evaluation review body* (3.20), based on the results from an *evaluation agency* (3.18) or auditor

3.20
evaluation review body
group with responsibility for reviewing, and making judgements on, the results of the *evaluation agency* (3.18)

3.21
financial key
cryptographic key used to protect financial transaction data between the PED and the entity processing the transaction, e.g. the entity's public key used for mutual authentication with the PED, the initial DUKPT keys, Terminal Master Keys, and PIN encryption keys

3.22
formal claim
statement about the characteristics and functions of an *SCD* (3.28)

3.23
hardware security module
HSM
SCD (3.28) that provides a set of secure cryptographic services, e.g. key generation, cryptogram creation, PIN translation, and certificate signing

3.24
key loading device
KLD
SCD (3.28) that loads keys into other SCDs

3.25
logical security
ability of a device to withstand *attacks* (3.9) through its functional interface

3.26
operational environment
environment in which the *SCD* (3.28) 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

3.27
physical security
ability of a device to withstand *attacks* (3.9) against its physical construction, including physical characteristics such as electromagnetic emissions and power fluctuations, the analysis of which can lead to side channel attacks

3.28
secure cryptographic device
SCD
device that provides physically and logically protected cryptographic services and storage (e.g. PIN entry device (PED) or *HSM* (3.23)), and which may be integrated into a larger system, such as an automated teller machine (ATM) or point of sale (POS) terminal

3.29
security scheme
configuration that supports the secure status of the device

3.30
sensitive data
sensitive information
data, status information, cryptographic keys, PINs, etc., which need to be protected against unauthorized disclosure, alteration, or destruction

3.31
sensitive function
those functions which are accessible when the device is in a *sensitive state* (3.32)

3.32
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* (3.16)

3.33
sponsor
entity that submits the *SCD* (3.28) for evaluation

Note 1 to entry: Sponsor in this context does not refer to the “sponsor” of a transaction.

3.34
tamper evident characteristic
characteristic that provides evidence that an *attack* (3.9) has been attempted

3.35
tamper resistant characteristic
characteristic that provides passive physical protection against an *attack* (3.9)

3.36
tamper responsive characteristic
characteristic that provides an active response to the detection of an *attack* (3.9)

4 Abbreviated terms

ATM	automated teller machine
MAC	message authentication code
PIN	personal identification number
POS	point of sale
SCD	secure cryptographic device

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 MAC-ing 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 the above 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 information;
- unauthorized use or modification of cryptographic services.

A secure cryptographic device (SCD) is a physically and logically secure hardware device providing a defined set of cryptographic functions, access controls, and secure key storage. SCDs are employed to protect against these threats. The requirements of this part of ISO 13491 pertain to the SCD and not the system in which the SCD may be integrated. However, it is important to analyse the interfaces between the SCD and the remainder of the system to ensure that the SCD may 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 may 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. Evaluation methods are given in Annex A.

5.2 Attack scenarios

5.2.1 General

SCDs are subject to the following five primary classes of attack, which may be used in combination:

— penetration;

— monitoring;

— manipulation;

— modification;

— substitution.

These attack scenarios do not form an exhaustive list, but are an indication of the main areas of concern and are described below.

NOTE The Internet has enabled new classes of attackers who share information enabling the dissemination of exploits to be both wide reaching and rapid and to market attacks developed against particular SCDs (particularly point of sale devices). These later attackers expend considerable time, effort, and expertise to develop an attack which is packaged and then sold to other attackers.

5.2.2 Penetration

Penetration is an attack which involves the physical perforation or unauthorized opening of the device to ascertain sensitive data contained within it, e.g. cryptographic keys.

5.2.3 Monitoring

Monitoring is an attack which may involve the monitoring of electromagnetic (EM) radiation, power consumption differentials, timing differentials, and other side channel attacks, etc. for the purposes of discovering sensitive information contained within the device. Alternatively, it may involve the visual, aural, or electronic monitoring of sensitive data being entered into the device.

5.2.4 Manipulation

Manipulation involves the unauthorized sending to the device of a sequence of inputs, varying the external inputs to the device (such as power or clock signals), or subjecting the device to other environmental stresses so as to cause the disclosure of sensitive information or to obtain a service in an unauthorized manner. An example of this would be causing the device to enter its “test mode” in order that sensitive information could be disclosed or the device integrity manipulated.

5.2.5 Modification

Modification is the unauthorized alteration of the logical or physical characteristics of the device, e.g. inserting or overlaying a PIN-disclosing “bug” in, or on, a PIN pad between the point of PIN entry and the point of PIN encryption. The purpose of modification is to alter the device rather than to immediately disclose information contained within the device. Following modification, the device shall be made (or shall remain) operational in order for the attack to be successful. The unauthorized replacement of a cryptographic key contained within a device is a form of modification.

5.2.6 Substitution

Substitution is the unauthorized replacement of one device with another. The replacement device might be a look-alike “counterfeit” or emulating device having all or some of the correct logical characteristics plus some unauthorized functions such as a PIN-disclosing bug.

The replacement device might also be a once-legitimate device that has been subject to unauthorized modifications and then substituted for another legitimate device.

Substitution may include removal of the device in order to perform a penetration or modification attack in an environment better suited to such attacks. Substitution can be seen as a special case of modification in which the adversary does not actually modify the target device, but instead replaces it with a modified substitute.

5.3 Defence measures

5.3.1 General

To defend against the attack scenarios discussed above, the following three factors work together to provide the security required:

- device characteristics;
- device management;
- environment.

While in some cases, a single factor, e.g. device characteristics, may be dominant, the normal situation is that all factors are necessary to achieve the desired result.

5.3.2 Device characteristics

SCDs are designed and implemented with logical and physical security so as to deter attack scenarios such as those described in 5.2.

Physical security characteristics can be subdivided into the following three classes:

- tamper evidence characteristics;
- tamper resistance characteristics;
- tamper response characteristics.

SCDs shall require a combination of all three of these classes of characteristics. Other physical security characteristics may be required to defend against other passive attacks, such as monitoring. Physical security characteristics may also help defend against modification or substitution.

The intent of tamper evidence is to provide evidence that an attack has been attempted and may or may not have resulted in the unauthorized disclosure, use, or modification of the sensitive information. The disclosure of an attempted attack could be in the form of physical evidence, such as damage to the external casing. The evidence could also be that the device is no longer in its expected location. Tamper evidence provides an indication that the device may have been penetrated or modified.

The intent of tamper resistance is to block attacks by employing passive barriers or logical design features. Barriers are usually single purpose and are designed to block a particular threat, such as a penetration attack. The logical protection measures are designed typically to prevent the leakage of sensitive information or to prevent the illicit modification of system or application software. Tamper resistance provides a barrier of protection, the circumvention of which may lead to tamper evidence and result in tamper responsiveness. In this context, “tampering” is understood to also cover purely passive attacks, e.g. EM radiation monitoring

The intent of tamper response is to employ active mechanisms against attacks. When the active protection mechanisms are triggered, the protected information is either erased or rendered unusable.

The implementation of the various security characteristics is dependent on the designer’s knowledge and experience of known attacks against the particular implementation. For that reason, attacks are usually directed to discovering which, if any, of the known threats the implementer failed to address.