INTERNATIONAL STANDARD

ISO 13491-1

First edition
1998-06-15

Banking — Secure cryptographic devices (retail) —

Part 1:
Concepts, requirements and evaluation methods

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

Partie 1: Concepts, prescriptions et méthodes d'évaluation

Contents

International Organization for Standardization
Case postale 56 • CH-1211 Genève 20 • Switzerland
Internet iso@iso.ch

Printed in Switzerland

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.

International Standard ISO 11568 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 check-lists for devices used in magnetic stripe card systems

Annex A of this part of ISO 13491 is for information only.

Introduction

ISO 13491 describes both the physical and logical characteristics and the management of the secure cryptographic devices (SCD's) used to protect messages, cryptographic keys and other sensitive information used in a retail banking environment, where a SCD is a physically and logically protected hardware device that provides a secure set of cryptographic services.

The security of retail electronic banking 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. While certain cryptographic equipment (e.g. host security modules) remain concentrated in the relatively high security of processing centers, a large proportion of cryptographic devices used in retail banking (e.g. PIN pads, ATM's, etc) now reside in non-secure environments. Therefore when Personal Identification Numbers (PIN's), Message Authentication Codes (MAC's), Cryptographic Keys and other sensitive data are processed in these devices, there is a risk that these 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 characteristics and are properly managed.

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

1 Scope

This part of ISO 13491 specifies the requirements for Secure Cryptographic Devices which incorporate the cryptographic processes defined in ISO 9564, ISO 9807 and ISO 11568.

This part of ISO 13491 has two primary purposes:

1. to state the requirements concerning both the operational characteristics of SCD's and the management of such devices throughout all stages of their life cycle,

2. to standardize the methodology for verifying compliance with those requirements.

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 management procedures and secure cryptographic characteristics. These management procedures implement preventive measures to reduce the opportunity for a breach of cryptographic device security. These aim for a high probability of detection of any illicit access to sensitive or confidential data should device characteristics fail to prevent or detect the security compromise.

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

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

Specific requirements for the characteristics and management of specific types of SCD functionality used in the retail banking environment are contained in another part of ISO 13491.

2 Normative references

The following standards contain provisions which, through references in this text, constitute provisions of this part of ISO 13491. At the time of publication, the editions indicated were valid. All standards are subject to revision and parties to agreements based upon this part of ISO 13491 should apply the most recent edition of the standards indicated below. Members of IEC and ISO maintain registers of currently valid International Standards.

ISO 7498-2:1989, *Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security architecture*.

ISO 8908:1993, *Banking and related financial services — Vocabulary and data elements*.

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

ISO 9807:1991, *Banking and related financial services — Requirements for message authentication (retail)*.

ISO 10202 (all parts), *Financial transaction cards — Security architecture of financial transaction systems using integrated circuit cards*.

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

ISO 13491-2:—[2)], *Banking — Secure cryptographic devices (retail) — Part 2: Security compliance checklists for devices using magnetic stripe cards*.

1) To be published. (Revision of ISO 9564-1:1991)

2) To be published.

3 Terms and definitions

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

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

3.2 accredited evaluation authority: a body accredited in accordance to a set of rules, e.g. EN 45000 or ISO Guide 25, and accepted by the accreditation authority for the purpose of evaluation.

3.3 attack: an attempt by an adversary on the device to obtain or modify sensitive information or a service he is not authorized to obtain or modify.

3.4 audit check-list: a list of auditable claims, organized by device type, and contained in another part of ISO 13491.

3.5 audit report: the output of the Audit Review Body based on the results from an auditor

3.6 audit review body: a group with responsibility for reviewing and making judgements on the results from the auditor.

3.7 auditor: one who checks, assesses, reviews and evaluates compliance with an informal evaluation on behalf of the Sponsor or Audit Review Body.

3.8 certification report: the output of the evaluation review body based on the results from an accredited evaluation authority.

3.9 controller: Entity responsible for the secure management of an SCD

3.10 deliverables: documents, equipment and any other items or information needed by the evaluators to perform an evaluation of the Secure Cryptographic Device.

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

3.12 environment-dependent security: security of an SCD as part of an operational environment.

3.13 evaluation agency: an organization trusted by the design, manufacturing and sponsoring authorities which evaluates the SCD (using specialist skills and tools) in accordance with this part of ISO 13491.

3.14 evaluation report: the output of the evaluation review body based on the results from an evaluation agency or auditor.

3.15 evaluation review body: a group with responsibility for reviewing, and making judgements on, the results of the evaluation agency.

3.16 formal claims: statements about the characteristics and functions of a Secure Cryptographic Device.

3.17 logical security: the ability of a device to withstand attacks through its functional interface.

3.18 operational environment: the 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.

3.19 physical security: the ability of a device to withstand attacks against its physical construction.

3.20 secure cryptographic device: SCD: a physically and logically protected hardware device that provides a secure set of cryptographic services.

3.21 SCD interface: the interface of the SCD through which the SCD interacts with the operational environment (e.g. command, control panels, lock, etc.).

3.22 sensitive data; sensitive information: data, design characteristics, status information, cryptographic keys etc, which must be protected against unauthorized disclosure, alteration, or destruction.

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

3.24 sponsoring authority; sponsor: the individual, company or organization that requires the SCD to undergo evaluation.

3.25 tamper evident characteristic: A characteristic that provides evidence that an attack has been attempted.

3.26 tamper resistant characteristic: A characteristic that provides passive physical protection against an attack.

3.27 tamper responsive characteristic: A characteristic that provides an active response to the detection of an attack, thereby preventing its success.

4 Secure cryptographic device concepts

Cryptographic devices are used in retail banking to help ensuring:

- the integrity of sensitive data, eg transaction details
- the confidentiality of secret information, eg customer PINs
- the confidentiality of cryptographic keys used to achieve these objectives.

To ensure the above objectives, the following threats must be countered:

- Disclosure of sensitive information stored or entered into the device
- Modification of sensitive information
- Unauthorized use of a device
- Unauthorized access to service.

Since absolute security is not practically achievable, it is not realistic to describe a 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 a security device as possessing a degree of tamper resistance, where an acceptable degree is one that is deemed adequate to deter any attack envisioned as feasible during the operational life of the device, taking into account the equipment, skills and other costs to the adversary to mount a successful attack and the financial benefits that the adversary could realize from such an attack.

Security of retail systems considers physical and logical aspects of device security, 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 have 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. Standardized methods of evaluation are given in clause 7.

4.1 Attack scenarios

The attack scenarios described are not intended to be an inclusive list but are an indication of the main areas of concern. SCDs are subject to five primary classes of attack:

- penetration
- monitoring
- manipulation
- modification
- substitution.

These attacks are described below.

4.1.1 Penetration

Penetration is an active attack which involves the physical perforation or unauthorized opening of the device to ascertain sensitive data contained within it, for example, cryptographic keys. Therefore, penetration is an attack on the physical characteristics of the device.

4.1.2 Monitoring

Monitoring is a passive attack which may involve the monitoring of electromagnetic radiation for the purposes of discovering sensitive information contained within the device; or visually, aurally, or electronically monitoring secret data being entered into the device. Therefore, monitoring is an attack on the physical characteristics of the device.

4.1.3 Manipulation

Manipulation is the unauthorized sending to the device of a sequence of inputs so as to cause the disclosure of sensitive information or to obtain a service in an unauthorized manner, for

example, causing the device to enter its "test mode" in order that sensitive information could be disclosed or the device integrity manipulated. Manipulation is an attack on the logical characteristics of the device.

4.1.4 Modification

Modification is the unauthorized modification or alteration of the logical or physical characteristics of the device, for example, inserting a PIN-disclosing "bug" in a PIN pad between the point of PIN entry and the point of PIN encryption. Note that modification may involve penetration but for the purpose of altering the device rather than disclosing information contained within the device. The unauthorized replacement of a cryptographic key contained within a device is a form of modification. Modification is an attack on either the physical or logical characteristics of the device.

4.1.5 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 be a once-legitimate device that had been subject to unauthorized modifications and then substituted for another legitimate device. Removal is a form of substitution which may be carried out in order to perform a penetration or modification attack in an environment better suited to such attacks, or as a first step in a substitution attack, the device may be taken out of its operating environment. 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. Substitution is an attack on the physical and logical characteristics of the device.

4.2 Defence Measures

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

- Device Characteristics
- Device Management
- Environment.

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

4.2.1 Device Characteristics

Cryptographic devices are designed and implemented with logical and physical security so as to deter the attack scenarios described in 4.1, as indicated by the results of the risk assessment of the application and the environment.

The main objective of physical security device characteristics is to defend against attacks using penetration. Such characteristics can be subdivided into three classes;

- Tamper Evidence Characteristics
- Tamper Resistance Characteristics
- Tamper Response Characteristics.

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 packaging. The evidence could also be that the device is no longer in its expected location.

The intent of Tamper Resistance is to block attacks against the information to be protected from unauthorized disclosure, use, or modification by employing passive barriers. Defences or blocks are usually single purpose and are designed to block a particular threat. The implementation of tamper resistant designs is very dependent on the designer's knowledge and experience of known attacks against the particular implementation. For that reason, attacks against tamper resistance implementations are usually directed to discovering which, if any, of the known threats, the implementor failed to address. The attacker will also attempt to discover new attacks that are likely to be unknown by the implementor. Evaluation of a tamper resistant design is difficult and not conclusive in that the evaluation normally only proves that the design successfully blocks the known attacks for which it was designed, but does not or cannot evaluate resistance to unknown attacks.

The intent of Tamper Response is to employ active barriers against attacks aimed at unauthorized disclosure, use or modification of the protected information. The active barriers are intended to alter the protected information into an unusable form. Deployment of the tamper response is initiated by some pre-defined condition or by the discovery of an attack against the information.

Physical implementations are usually a combination of the three classes of characteristics. Other physical security characteristics may be required to defend against monitoring. Physical security characteristics may also help defend against modification or substitution.

4.2.2 Device Management

Device management refers to the external controls placed on the device during its life cycle and by its environments. These controls include external key management methods, security practices and operational procedures. The security level may change during the device life cycle. A primary objective of device management is to ensure that device characteristics are not subject to unauthorized alteration during the life of the device.

4.2.3 Environment

The objective of environment security is to control access to the SCD and its services, thus preventing or at least detecting attacks on the SCD. Throughout its life cycle, a SCD will reside in a variety of environments. These environments may be characterized as ranging from highly controlled to minimally controlled. A highly controlled environment is one that includes constant surveillance by trusted individuals, while a minimally controlled environment may not include any special environmental security supplements. If the security of an SCD is dependent on some function of a controlled environment, it must be satisfactorily proven that the controlled environment actually provides this function.

5 Requirements for device characteristics

5.1 Introduction

The device characteristics of a Secure Cryptographic Device may be categorized as either physical or logical.

- Physical characteristics are the way the device is constructed.

- Logical characteristics are the way that inputs are processed to produce device outputs.

The SCD needs to have characteristics that ensure that in the normal operating environment the device or its interface does not endanger any data that is entering or leaving the device, or stored or processed in the device.

Where the SCD is operated in a controlled environment, the requirements for device characteristics may be eased to the extent that the protection is provided by the controlled environment and the management of the device.

5.2 Physical Security Requirements for SCDs

5.2.1 General

An SCD **shall** be so designed that any failure of a component in the device or use of that component outside of the device specification **shall** not cause the disclosure or undetected modification of sensitive data.

An SCD **shall** be so designed and constructed that any unauthorized access to or modification of sensitive data (including device software) that are input, stored, or processed in it **shall** necessitate physical penetration of the device.

NOTE It is recommended that an SCD should be so designed and constructed that any additions of external devices that intercept or substitute data input to or output from the SCD for the purpose of masquerade, will have a high probability of being detected and/or recognized as not being part of a correct device.

When an SCD is designed to permit access to internal areas, eg. for service or maintenance, it **shall** have a mechanism so that such access causes immediate erasure of all cryptographic keys and other sensitive data, if compromise cannot otherwise be prevented.

The SCD and its data entry functions **shall** be so shielded from direct and indirect monitoring that when it is operating in its intended environment and in its intended manner, no feasible attack will result in compromise of any secret or sensitive data.

If there is an appreciable risk of modification or substitution that will not be countered by the logical security of the SCD, or its management and environment, the physical design **shall** be such