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

Reference number
ISO 13491-1:1998(E)

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

that there will be a high degree of probability of detection of any modification or substitution.

5.2.2 Tamper Evidence Requirement

A device that claims Tamper Evidence characteristics **shall** be designed and constructed as follows.

Substitution:

To protect against substitution with a forged or compromised device, a device is designed so that it is not practical for an attacker to construct a duplicate from commercially available components that can reasonably be mistaken for a genuine device.

Penetration:

To ensure that penetration of an SCD is detected, the device **shall** be so designed and constructed that any successful penetration **shall** require that the device be subject to physical damage or prolonged absence from its authorized location such that the device cannot be placed back into service without a high probability of detection by a knowledgeable observer.

5.2.3 Tamper Resistance Requirements

Penetration:

An SCD **shall** be protected against penetration by being Tamper Resistant to such a degree that its passive resistance is sufficient to make penetration infeasible both in its intended environment and when taken to a specialized facility where it would be subjected to penetration attempts by specialized equipment.

Modification:

The unauthorized modification of any key or other sensitive data stored within an SCD, or the placing within the device of a tap e.g. active, passive, radio etc, to record such sensitive data, **shall** not be possible unless the device be taken to a specialized facility and at this facility be subject to damage such that the device is rendered inoperable.

Monitoring:

Monitoring **shall** be countered by using tamper resistant device characteristics. The passive physical barriers **shall** include the following:

- shielding against electromagnetic emissions in all frequencies in which sensitive information could be feasibly disclosed by monitoring the device;

- privacy shielding such that during normal operation, keys pressed will not be easily observable to other persons. (For example, the device could be designed and installed so that the device can be picked up and shielded from monitoring by the user's own body.)

Where parts of the device cannot be appropriately protected from monitoring, these parts of the device **shall** not store, transmit or process sensitive data.

The device **shall** be designed and constructed in such a way that any unauthorized additions to the device, intended to monitor it for sensitive data, **shall** have a high probability of being detected before such monitoring can occur.

Removal:

If protection against removal is required, the device **shall** be secured in such a manner that it is not economically feasible to remove the device from its intended place of operation.

5.2.4 Tamper Response Requirements

Where an SCD employs a Tamper Responsive mechanism, the integrity of the mechanism **shall** be ensured by employing Tamper Responsive characteristics and/or Tamper Resistant characteristics.

Penetration:

A device that claims Tamper Responsive characteristics **shall** be designed and constructed to ensure that penetration of the device results in the immediate and automatic erasure of all keys and other sensitive data and all useful residues of sensitive data.

Modification:

A device that claims Tamper Responsive characteristics **shall** be designed to detect any unauthorized modification and **shall** cause the immediate and automatic erasure of all keys and other sensitive data and all useful residues of such sensitive data.

Removal:

Removal of the device can be the first step to an attack when taken out of its operating environment. Therefore if the security of the device depends on the operating environment, the unauthorized movement of the device **shall** cause the immediate and automatic erasure of all keys and other sensitive data and all useful residues of such sensitive data.

5.3 Logical Security Requirements for SCDs

Where a requirement for dual or multiple control is stated below, the requirement for logical security device characteristics is that the device **shall** provide facilities that support the secure implementation of dual or multiple control.

5.3.1 Assurance of genuine devices

If the provision of a genuine, uncompromised device is not assured by the device management and the device characteristics, then the device **shall** be delivered with sensitive information that enables the user to ascertain that the device is genuine and not compromised.

NOTE One example of such information is a secret symmetric key, without which the device will not operate correctly. Another example is an asymmetric key pair, with the public key of the device signed by the private key of the supplier.

5.3.2 Design of functions

The function set of an SCD **shall** be so designed that no single function, nor any combination of functions, can result in disclosure of sensitive data, except as explicitly allowed by the security scheme used.

Logical protection must be sufficient so as not to permit the compromise of sensitive data, even when only legitimate functions are used. Therefore protection against exhaustive searches is needed. When the environment does not provide this protection, it must be provided by device characteristics.

NOTE The following methods are examples of how this can be achieved:

- internal monitoring of statistics, e.g. so that only some given fraction of incorrect PIN verifications are permitted,
- imposing a minimum time interval between sensitive function calls.

5.3.3 Use of cryptographic keys

An SCD **shall** enforce a key separation scheme such that no key can be used for any but its single intended purpose (see ISO 11568-2 and ISO 11568-4).

The key generation methods of an SCD **shall** comply with ISO 11568-3 or ISO 11568-5.

An SCD **shall** implement one or more key management schemes that comply with the principles outlined in ISO 11568-1.

5.3.4 Sensitive Device States

If an SCD can be put into a 'sensitive state', i.e. a state that allows functions that are normally not permitted (e.g. manual loading of cryptographic keys), then such a transition **shall** require multiple control via a secure operator interface. Activation of a Tamper Responsive mechanism **shall not** put the SCD into a sensitive state.

If passwords or other plaintext data are used to control transition to a sensitive state, then the input of such passwords **shall** be protected in the same manner as other sensitive data.

To minimize the risks of unauthorized use of sensitive functions, the sensitive state **shall** be established with limits on the number of function calls (where appropriate) and a time limit. After the first of these limits is reached, the device **shall** return to its normal state.

5.3.5 Multiple Cryptographic Relationships

The selection of cryptographic key sets for encipherment of sensitive data (eg PINs) **shall** be controlled only by a Controller responsible for the secure management of the SCD. Where multiple cryptographic relationships are to be maintained in a device (eg a Multi-Acquirer PIN Pad), then there **shall** be one entity, the Controller. In this situation, the source and path of data used to select a cryptographic key set **shall** be physically or logically protected.

5.3.6 SCD Software Authentication

A specific technique for authentication of the software must be included. Such a technique **shall** ensure that only software produced by the supplier, owner or a third party approved by the Controller can be loaded and installed in the SCD.

NOTE The technique may involve either generating a cryptographic check value for the software or enciphering the software.

5.3.7 Minimally Tamper Resistant Devices with Tamper Evidence Characteristics

In some applications and environments, risk assessment may result in minimal requirements for physical security. Penetration of an SCD **shall not** permit the determination of any key or other sensitive data used by the device for any previous transaction, given the knowledge of all data stored within the device as well as any relevant data that has ever existed outside the device, except within an SCD.

One means of accomplishing this is through the use of a derived, or non-reversible, unique key per transaction key management scheme. Where devices employ a derived or non-reversible unique key per transaction key management scheme and where all information from which these keys might be determined is erased from the device at the completion of the transaction, the potential damage of a breach of security is reduced. Therefore requirements for tamper resistance or tamper response characteristics may be reduced.

Any compromise of an SCD **shall not** result in the compromise of another such device.

Therefore, the secret keys used by one SCD **shall not**, except by chance, be equal to any keys used by any other SCD.

The logical security features of the SCD **shall** ensure that any working keys stored within a device are not themselves directly loaded into the device. Rather, the working keys are created within the device by non-reversibly transforming the keying material which is directly loaded into the device. The directly loaded keying material **shall not** be stored within the device. This will ensure that compromised working keys cannot be used in other SCD's.

6 Requirements for device management

The security of a cryptographic device depends not only upon the characteristics of the device, but also upon the characteristics of the environment in which the device is located. Device management may therefore be viewed as requirements imposed on the device's environment. The device **shall** be subject to appropriate auditing and controls that are applied at each phase of the device's life cycle. If this were not done, the device might be subject, in one phase of its life cycle, to the attack scenarios identified earlier. Such attacks could jeopardize its security when it is placed into operational use.

Whether detection of a compromise is sufficient or whether prevention of the compromise is necessary, and the means that can be used to implement prevention or detection, depend upon where the device is in its life cycle.

6.1 Life-Cycle Phases

A life-cycle phase is a result of a change in either the environment and/or the state of the device. Different cryptographic devices can have substantially different life cycles. Table 1 presents a generalized device life cycle, indicating the possible phases in the life of a cryptographic device and the events that cause a transition from one phase to the next. It is important to distinguish between these phases because the protection requirements for the device, as well as the means of providing protection, may change as the device moves from one life cycle phase to another.

For the purpose of this part of ISO 13491, the phases of the Life-Cycle are defined as follows:

- Manufacturing; The design, construction, repair, upgrade and testing of a device so that it incorporates the intended functional and physical characteristics of that device.

- Post-Manufacturing; The post-manufacturing phase consists of the transport and storage of the device up to and including initial key loading.

- Pre-Use; The phase in the device life cycle in which the device contains a key but has not yet been placed into operational use.

- Use; A device can be regarded as being in an operational use state when it has been installed for its intended purpose at its intended location.

- Post-Use; The phase in the life of a device when it is removed from service. The removal may be temporary, for example to move the device to another operational location or to repair the device. It may be permanent, if the device is removed from service without the intent to subsequently re-use it.

Table 1 — Device Life-Cycle Phases

Life Cycle Phase	Transition Event (to the next phase)
Manufacturing	Completion
Post-Manufacturing	Initial Key Loading
Pre-Use	Installation
Use	Removal
Post-Use	Re-installation Repair, upgrade Destruction

6.2 Life Cycle Protection Requirements

At most phases in the device life cycle it is generally not necessary to prevent a security compromise, but only to detect it. This is because the device does not contain any keys or other sensitive material that is or has been used. Thus if a device is compromised before it is placed into operational use and the compromise is detected, the device can be discarded or repaired to remove the effects of the compromise.

The security of the device **shall not** depend only upon the secrecy of the design details. However, where such secrecy contributes to the security of the device, compromise prevention is required throughout all life-cycle phases. When secrecy of the design features is not required, the general requirements for each phase are:

6.2.1 Manufacturing and Post-Manufacturing

During the manufacturing and post-manufacturing phases, there is no cryptographic key within the device. Until an initial key has been loaded, it is necessary to detect a compromise but not to prevent it. If a compromise is detected, it is only necessary to ensure that the device is not placed in service until all effects of the compromise have been eliminated from it.

Prior to initial key loading, the only protection provided by the characteristics of the device itself is the physical difficulty of opening the device or of obtaining a counterfeit version to substitute for the device. Subsequent to initial key loading, the key-erasure mechanisms of the device can provide substantial additional protection, if provided.

6.2.2 Pre-Use

During the pre-use phase, the device contains at least one initial key. Prevention of device compromise **shall** be required if:

- the initial key may be, or had been in use (in other devices, other than by chance) to encipher secret data;

NOTE ISO 11568-3, subclause 4.5 requires that:

> "Any key shall exist in a minimum number of locations consistent with effective system operation. Any key that exists in a transaction originating device shall not exist in any other such device".

Thus a device conforming to ISO 11568 needs only compromise detection, not compromise prevention, prior to actual use.

or

- the compromised key cannot be blocked at all cryptographic devices capable of cryptographic communication with the compromised device, before the first unauthorized use of the key after its compromise.

The high probability of detection of device compromise **shall** be required, except as listed above.

NOTE When a cryptographic device requires only compromise detection prior to use, the presence of an initial key in the device can serve as an effective means of detection, provided the device has characteristics which cause the automatic and immediate erasure of this key in the event of tampering. When the device is placed in service, the absence of a correct initial key becomes apparent on the first attempt to use the device. The device is immediately taken out of service and is considered suspect. Therefore such a device requires less stringent device management subsequent to initial key loading than prior to it.

6.2.3 Use

When in operational use, a cryptographic device **shall** require compromise prevention if:

- it contains any key that has been used by this or any other device, or it contains

information from which such a key could be obtained,

or

- detection of a compromise cannot occur before the device can be re-installed.

The high probability of detection of device compromise **shall** be required, except as listed above.

NOTE To minimize requirements for compromise prevention, a device should implement a "unique key per transaction" technique such that the disclosure of all data contained within the device would not provide any information that could disclose any key that the device has used.

Device management **shall** prevent or detect the unauthorized functional alteration of the device, for example the unauthorized modification of the device's software. Therefore where a download feature is available, a specific technique for authentication of the software and/or data **shall** be included. Such a technique will ensure that only items intended for download and that have been authenticated and/or enciphered by the controller or his agent can be loaded and installed in the device.

For some types of cryptographic devices, device management may be required to prevent misuse (e.g. manipulation) of the device. For example, if a device performs PIN verification, device management may be required to prevent unauthorized calls to the device to determine PINs by exhaustive trial-and-error.

6.2.4 Post-Use

During the post-use phase, a cryptographic device **shall** require compromise prevention if:

- the cryptographic keys or other sensitive data are still stored in a cryptographic device which required compromise prevention in the use cycle.

6.3 Life Cycle Protection Methods

Each of the five life-cycle phases has unique characteristics.

6.3.1 Manufacturing

During the manufacturing process, the manufacturer **shall** implement auditing and control procedures so that the manufactured devices have the intended physical and functional characteristics, and only these characteristics. Any unauthorized alteration of the device's physical protection mechanisms, or any unauthorized additions or deletions to the device's functionality, **shall** have a high probability of being prevented or detected. The replacement of the device with a counterfeit substitute **shall** also have a high probability of being prevented or detected, for example by dual control over the device.

6.3.2 Post-Manufacturing

During this phase, auditing and control procedures **shall** be implemented which have a high probability of preventing or detecting the unauthorized alteration of the device or the replacement of the device with a counterfeit substitute.

Devices that use symmetric ciphers exclusively are loaded with one or more secret key(s) that are generated externally and transferred into the device. Devices that use asymmetric ciphers may themselves generate and retain the secret key and disclose (to the key loading process) only the corresponding public key. Whichever method of key generation is used, key loading **shall** be performed in such a way that the secret key cannot be determined by any one person.

Immediately prior to initial key loading there **shall** be assurance that the device has not been subject to unauthorized modification or substitution. This may be accomplished by:

- Testing and/or inspection of the device

- Careful auditing and control of the device since manufacturing, or since the most recent testing and/or inspection of the device

- Confirmation of the existence within the device of a secret device-unique key or data installed by the manufacturer for the sole purposes of confirming the legitimacy of the device.

Device management **shall** provide detection of theft or unauthorized removal of the device.

NOTE ISO 11568 requires that initial key loading shall take place in a secure facility.

6.3.3 Pre-Use

Auditing and controls **shall** be implemented to detect and, where required, prevent any tampering that might disclose the device's sensitive key(s), or any unauthorized modification to the device. For those devices with an automatic key-erasure

mechanism, this mechanism itself may provide a means of detection. Any attempt to obtain access to the device for purposes of key determination or unauthorized modification should result in key erasure, an effect that **shall** be detected when operational use is first attempted.

NOTE The replacement of a device with a counterfeit substitute is not normally possible unless the device's key is first compromised. The substitute device would not otherwise contain the correct key(s), a fact that would be detected when it is first placed into operational use.

Even though a device has key-erasure mechanisms, some degree of auditing and external control is still required. This is necessary to ensure that the device is not available to adversaries for a sufficiently long time that they might successfully compromise these mechanisms and determine the key(s), or bypass the mechanisms, make unauthorized modifications to the device and then return the device.

If a particular cryptographic device is subject to fraud that might occur if the device is installed in an unauthorized location or by unauthorized personnel or is left unguarded for long periods, then the device may require the entry of an "unlocking code" before it permits operational use.

Device management **shall** provide detection of theft or unauthorized removal of the device.

6.3.4 Use

The combination of device characteristics plus device management **shall** have a high probability of preventing a successful attack on the device.

If a cryptographic device is operated in a minimally-controlled environment, security of the device depends primarily upon its characteristics and only secondarily upon its management.

It should not be possible to compromise a properly designed device without removing it from its operational location. Device management should provide detection of theft or unauthorized removal by means such as the following:

- Reporting procedures so that device users report missing devices in a timely manner as specified by the device controller or his agent.

- Electronic interrogation procedures by which a device is periodically interrogated by a host computer system, and confirms its operational status to this system by returning a cryptographically-authenticated response.

- Auditing and control procedures to confirm that all devices of a given set are in their intended operational locations.

Malfunction of the device can occur at any time. Such an event may require the removal of the device from service to enter the "post-use" phase of the device life cycle. If keys are erased from the failed device after its removal from service, then replacement keys **shall** not be installed in the repaired device until it can be ensured that the physical or functional characteristics of the device have not been altered. If a cryptographic device outputs alarms that indicate a malfunction has occurred that might jeopardize the device's security, then the device **shall** immediately be removed from service.

6.3.5 Post-Use

If a device enters the post-use phase and it is intended to re-use the device in the same organization, it may be stored until such re-use with the key still present, provided it is given the same type of protection (compromise prevention or compromise detection) that the device required while in use.

Any device intended for possible re-use requires at least compromise detection in post-use.

If a device enters the post-use phase for repair, and if key compromise during repair can be neither prevented nor detected then all keys **shall** be erased. Special care **shall** be taken to ensure that the repair process does not result in unauthorized physical or functional modifications to the device.

If the device's keys are erased before it is stored for repair and/or possible re-use, new keys may be loaded into the device only when it can be assured that the device has not been subject to unauthorized physical or functional modification.

NOTE ISO 11568 requires that the key replacement shall take place in a secure facility.

When a device is removed from service with the intent not to restore the device to service within the organization, the device **shall** have the same type of protection required during operational use until its keys are erased or destroyed. At this point, the device can be transferred to another organization to enter the pre-use life cycle.

or

the device must be physically damaged such that the device cannot be restored to service. This technique **shall** be selected if it cannot otherwise be ensured that the device will not, accidentally or deliberately, be reloaded with keys and restored to service or used as a counterfeit substitute. The device can then be disposed of by any means.

If the device's keys cannot be erased or destroyed, the device **shall** be physically destroyed such that there is no possibility of the keys or other sensitive data being compromised.

6.4 Accountability

At each phase of the device life cycle, a party (one person or a group of persons) **shall** be accountable for the device. The accountable party **shall** understand and implement the requirements of this part of ISO 13491 for the appropriate life-cycle phases.

NOTE Accountability for the management of the physical device and the management of the logical security of the device may rest with different people in different organizations.

The responsibilities of each party that participates in device management should be clearly specified in writing by the organization that is responsible for overall security. An audit check list **shall** be prepared so that compliance with these requirements can be evaluated.

Independent auditors may be either internal or external to the organization and using the audit check lists, should periodically confirm that all device management requirements are being met by the organization in question and that the accountable person/people are performing their functions properly.

For each life-cycle phase, accountable records **shall** be maintained that indicate the location and status of each device. The accountable person should be identified by these records. When devices are transferred to another organization, another person becomes accountable for the devices. Therefore the records at both the originating and receiving organization should identify the devices and indicate the date of the transfer, the organization to/from which the transfer was made, the method of transit, and the means used to protect the devices while in transit (e.g. secure courier, counterfeit-resistant tamper-evident packaging). There should be some means of confirming that accountability has been accepted by the receiving organization and the name of the person who is now accountable for the transferred devices should be included in the records of the transferring organization.

6.5 Device Management Principles of Audit and Control

Audit and control are an essential part of device management. Table 2 summarizes some general principles relating to audit and control procedures and indicates their applicability to each phase of the device life cycle.

Table 2 — Audit and Control Principles

	PROCEDURE	Mfg	Post Mfg	Pre Use	Use	Post Use
1	One person or group of people responsible for the device.	M	M	M	M	M
2	Careful screening of or control over personnel with access to a device used in a controlled environment	M	M	M	M	M/R
3	Careful screening of or control over personnel with access to a device used in a minimally controlled environment	M	M	R	NA	M/R
4	Control over the manufacturing process to ensure that the device includes (only) legitimate physical and functional characteristics	M	NA	NA	NA	NA
5	Control mechanisms or sealing of the device in counterfeit resistant, tamper evident packaging to prevent undetected access to the device	NA	M	R	NA	R
6	Preparation and use of Audit Check Lists	M	M	M	M	M
7	Verification that audit check lists are filled out accurately, on a timely basis, and by qualified personnel	R	R	R	R	R
8	Key management procedures implemented as specified in the appropriate International Standard	NA	M	M	M	M
9	Accurate tracking of each device, by means of computerized or manually written records	M	M	M	M	M
10	Documented procedures to prevent the theft of, or unauthorized access to, a device that requires compromise prevention when in operational use	NA	NA	M	M	M
11	Control of the distribution of device documentation	R	R	R	R	R
12	Periodic electronic interrogation of an operational device to cryptographically confirm that it is still in its operational location	NA	NA	NA	R	NA
13	Documented reporting procedures to cause timely detection of a device that has been removed without authorization from storage or from its operational location, or that has disappeared while in transit	R	M	M	M	M
14	Documented procedures to prevent the subsequent operational use of keys resident in a missing or permanently out of service device, e.g. keys under central control	NA	NA	M	M	M
15	Key erasure if a device is removed from its operational location for repair and key compromise during repair cannot be prevented nor detected	NA	NA	NA	NA	M
16	Key erasure if a device is permanently removed from service and contains keys that have been used to encipher still-secret data, (i.e. the device required compromise prevention).	NA	NA	NA	NA	M
17	Key erasure if a device is permanently removed from service and contains keys that are not invalidated at all facilities that were capable of cryptographic communication with the device.	NA	NA	NA	NA	M
18	For a device requiring compromise prevention in operational use, controls to prevent compromise of the device after removal from service unless its keys have been erased	NA	NA	NA	NA	M
19	Control over the maintenance process is required in order that device confidentiality is maintained	NA	NA	NA	NA	M/R
20	Control over the repair process, or inspection/testing subsequent to repair, to ensure that the device has not been subject to unauthorized modification	M	NA	NA	NA	M

M Mandatory
NA Not Applicable
R Recommended
M/R Mandatory when compromise prevention is required, otherwise recommended

7 Evaluation method selection

In order to ascertain whether a secure cryptographic device complies with this part of ISO 13491, three alternative evaluation methodologies are defined. The first is an informal method based upon audit checklists defined in another part of this International Standard. The second and third are evaluation methods based upon an independent evaluation undertaken by a third party, which will under some circumstances use the audit check lists as a base for the Formal Claims used during the assessment.

7.1 Evaluation Methods

A risk assessment **shall** be undertaken as an aid in choosing which methodology is appropriate (ref 7.2). The result of a risk assessment is a risk estimate which may determine the evaluation method to be used. If the risk is low, an informal methodology using audit checklists may be sufficient to ensure compliance. However, if the risk is high, then the time, cost and assurance of a formal or semi-formal evaluation are justified.

The comparison of estimated risk, cost, time, national constraints and international acceptance is found in Table 3.

Therefore there are three methodologies for verifying compliance with the specified requirements. These are:

- An informal evaluation undertaken by an independent auditor using the audit check lists to be found in another part of ISO 13491.
- A semi-formal evaluation undertaken by an evaluation agency.
- A formal evaluation conducted by an Accredited Evaluation Authority.

Where devices offer multi-functionality, it will be necessary to combine several checklists into the assessment process, e.g. a device could offer both PIN Entry and Digital Signatures, in which case both check lists would be used during the evaluation. In selecting the appropriate model (informal, semi-formal or formal) various factors need to be considered. Table 3 compares these considerations with the three models presented in this part of ISO 13491. It is the combination of these parameters that determines the appropriate methodology. For example, if the estimated risk is low, the cost and time factors are a constraint and an audit would provide an acceptable level of assurance, the informal methodology may be acceptable. On the other hand, if a higher level of assurance is needed for International acceptance and cost and time factors are not a constraint, the high risk environment may require a more formal methodology.

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 the international organization.

Table 3 — Risk Factors vs Evaluation Methods

	Informal	Semi-Formal	Formal
Estimated risk	Low	Medium/High	High
Cost	Low	Medium	High
Time factor	Short	Medium	Long
Assurance	Audit report	Evaluation report	Certificate
National constraints	Possible constraints and limitations are country dependent		
International acceptance	Dependent upon the rules of the international organization		

NOTE The level of assurance is directly related to the level of experience, competence and equipment involved in the evaluation process.

7.1.1 Informal Method

Figure 1 shows the informal method where a manufacturer or sponsor submits a device to an auditor for evaluation against the appropriate checklist(s). The results are forwarded to the audit review body which produces an audit report.

7.1.2 Semi-formal Method

Figure 1 shows the semi-formal method where a manufacturer or sponsor submits a device to an evaluation agency for testing against the appropriate checklist(s). The evaluation agency may also use its experience, knowledge and special equipment to perform additional tests.

The results are forwarded to the evaluation review body which produces an evaluation report.

NOTE The evaluation review body may also receive independent results from an auditor, as depicted by the dotted line.

7.1.3 Formal Method

The third method shown in Figure 1 is the formal evaluation process.

The manufacturer or sponsor submits a device to an accredited evaluation authority for testing against the formal claims where the appropriate checklist(s) were used as input. The results are submitted to an accreditation authority which issues an evaluation certificate.

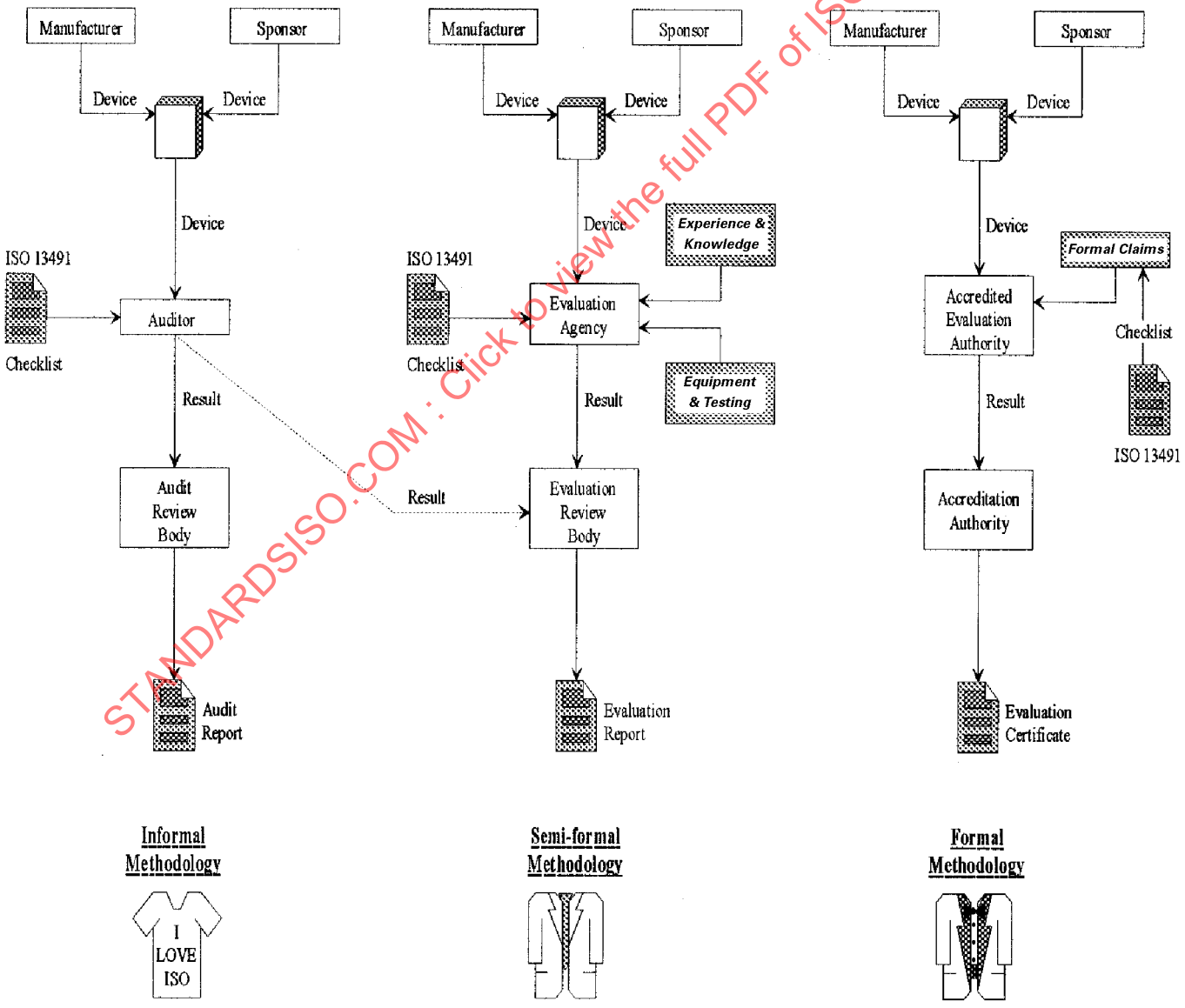

Figure 1 — Evaluation Methods

7.2 Risk Assessment

Since absolute security is not practically achievable, the assessment process considers the possible attack scenarios, the device protections available and the intended operational environments throughout the device life cycle. Other factors, including business requirements, technical requirements and the total system security are also incorporated into the assessment process.

Risk assessment is not solely based on, but always includes, value judgements. Risk assessment is an iterative process considering the following:

- The threats imposed by the attacks,
- The damages or loss from successful attacks,
- The probability of occurrence of these possible attacks.

Given all types of attacks, the risk is a function of the probability and losses associated with each attack. It is a policy and business decision whether the risk of a particular attack can be accepted or protective actions have to be taken. The complexity of an attack depends on tools, equipment, skills and resources (time and materials) required.

Various methods can be used to perform a risk assessment, but this topic is outside the scope of this part of ISO 13491.

7.3 Informal Evaluation Method

At the request of a sponsor an informal evaluation may be undertaken by an independent auditor. For this purpose the auditor **shall** complete the appropriate audit check list(s) for the device being evaluated. Upon completion of the evaluation, the results will be submitted to the Audit Review Body which will review the results and accept, reject or ask for clarification of those results. Upon completion of the review, the audit report is submitted to the sponsor.

Before commencement of any evaluation, there must be a common understanding between all parties to the audit on what is regarded as “feasible“ and “unfeasible“ for the environment and device in question.

This part of ISO 13491 describes the mandatory actions of the participating parties.

7.3.1 Manufacturer / Sponsor

The manufacturer can be the sponsor, or the sponsor can be an independent body, in either case the sponsor **shall** assume the following role and responsibilities :

- initiate the process,
- completion of risk assessment, (Note that other factors should be incorporated such as time, cost, etc.)
- choose the appropriate check list(s),
- submit the “deliverables“ to the evaluation process,
- receive the audit report.

7.3.2 Auditor

The auditor **shall** be independent of the sponsor, either from an external organization or, if internal to the sponsor organization, outside the sponsors influence.

The auditor **shall** assume the following role and responsibilities :

- answer the questions in the appropriate check list as True(T), False(F), or Not Applicable (N/A),
- if the answer is False or Not Applicable, the explanation **shall** be produced,
- submit results to the audit review body.

7.3.3 Audit Review Body

The audit review body can be either the sponsor itself or an independent body. In either case the audit review body **shall** assume the following role and responsibilities:

- receive the submitted results from the auditor
- if the answer is False or Not Applicable, determine whether the explanation is justified
- return the explanation to the auditor for further clarification, if necessary
- determine the security level of the intended environment
- determine whether the security level of the cryptographic device meets or exceeds the minimally acceptable security requirements appropriate for its operational environment