INTERNATIONAL STANDARD

ISO 13491-1

Second edition
2007-06-15

Banking — Secure cryptographic devices (retail) —

Part 1: Concepts, requirements and evaluation methods

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

Partie 1: Concepts, exigences et méthodes d'évaluation

Reference number
ISO 13491-1:2007(E)

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

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

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

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

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

ISO 13491-1 was prepared by Technical Committee ISO/TC 68, *Financial services*, Subcommittee SC 2, *Security management and general banking operations*.

This second edition cancels and replaces the first edition (ISO 13491-1:1998), which has been technically revised.

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

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

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

Introduction

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.

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.

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 (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 requirements concerning both the operational characteristics of SCDs and the management of such devices throughout all stages of their life cycle, and

— 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 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. These aim 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.

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 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 referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 11568-1, *Banking — Key management (retail) — Part 1: Principles*

ISO 11568-2:2005, *Banking — Key management (retail) — Part 2: Symmetric ciphers, their key management and life cycle*

ISO 11568-4, *Banking — Key management (retail) — Part 4: Key management techniques using public key cryptosystems*

ISO 13491-2, *Banking — Secure cryptographic devices (retail) — Part 2: Security compliance checklists for devices used in financial transactions*

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 authorities and supervision of their work in order to guarantee the reproducibility of the evaluation results

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

NOTE An example of a set of rules is ISO/IEC 17025.

3.3
assessment checklist
list of claims, organized by device type, and contained in ISO 13491-2

3.4
assessment report
output of the assessment review body, based on the results from an assessor

3.5
assessment review body
group with responsibility for reviewing and making judgements on the results from the assessor

3.6
assessor
person who checks, assesses, reviews and evaluates compliance with an informal evaluation on behalf of the sponsor or assessment review body

3.7
attack
attempt by an adversary on the device to obtain or modify sensitive information or a service he is not authorized to obtain or modify

3.8
certification report
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 SCD

3.11
device compromise
successful defeat of the physical or logical protections provided by the SCD, resulting in the potential disclosure of sensitive information or unauthorized use of the SCD

3.12
device security
security of the SCD related to its characteristics only, without reference to a specific operational environment

3.13
environment-dependent security
security of an SCD as part of an operational environment

3.14
evaluation agency
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

3.15
evaluation report
output of the evaluation review body, based on the results from an evaluation agency or auditor

3.16
evaluation review body
group with responsibility for reviewing, and making judgements on, the results of the evaluation agency

3.17
formal claim
statement about the characteristics and functions of an SCD

3.18
logical security
ability of a device to withstand attacks through its functional interface

3.19
operational environment
environment in which the SCD 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

3.20
physical security
ability of a device to withstand attacks against its physical construction, including physical characteristics such as electromagnetic emissions and power fluctuations, the analysis of which can lead to side channel attacks

3.21
secure cryptographic device
SCD
device that provides physically and logically protected cryptographic services and storage (e.g. PIN entry device or hardware security module), and which may be integrated into a larger system, such as an automated teller machine (ATM) or point of sale (POS) terminal

3.22
sensitive data
sensitive information
data, status information, cryptographic keys, etc., which need to be protected against unauthorized disclosure, alteration, or destruction

3.23
sensitive state
device condition that provides access to the secure operator interface, such that it can only be entered when the device is under dual or multiple control

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

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

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

3.27
tamper response characteristic
characteristic that provides an active response to the detection of an attack

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:

— disclosure or modification of cryptographic keys and other sensitive information;

— unauthorized use of cryptographic keys and 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 Clause 8.

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 attacks are described below.

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

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 radiation, power consumption differentials, timing differentials, etc. for the purposes of discovering sensitive information contained within the device. Alternatively, it may involve the visual, aural or electronic monitoring of secret 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, 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 three classes:

— tamper evidence characteristics;

— tamper resistance characteristics;

— tamper response characteristics.

Physical implementations are usually a combination of these three 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.

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.

The intent of tamper response is to employ active mechanisms against attacks. The active protection mechanisms are triggered when the device detects abnormal operating conditions and they are intended to alter protected information into an unusable form.

The implementation of the various protection characteristics is dependent on the designer's knowledge and experience of known attacks against the particular implementation. For that reason, attacks against tamper characteristics are usually directed to discovering which, if any, of the known threats the implementer failed to address. The attacker will also attempt to discover new attacks that are likely to be unknown to the implementer. Evaluation of the security of an SCD is difficult and not conclusive, in that the evaluation normally only proves that the design successfully blocks attacks known to the evaluator at the time of the evaluation, but does not, or cannot, evaluate resistance to unknown attacks.

5.3.3 Device management

Device management refers to the external controls placed on the device during its life cycle and by its environments (see Clause 7). 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.

5.3.4 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, an SCD will reside in a variety of environments (see Clause 7). 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 shall be satisfactorily proven that the controlled environment actually provides this function.

6 Requirements for device security characteristics

6.1 Introduction

Device characteristics of an SCD may be categorized as either physical or logical, as described below.

— Physical characteristics are the physical components that comprise the SCD and the way the device is constructed using those components.

— Logical characteristics are the way that inputs are processed to produce device outputs or to change logical state.

The SCD shall have characteristics that ensure the device or its interface does not compromise any sensitive data which is input to or output from the device, or stored or processed in the device.

Where the SCD is operated in a controlled environment, the requirements for device characteristics may rely on the protection provided by the controlled environment and the management of the device.

6.2 Physical security requirements for SCDs

6.2.1 General

An SCD shall be so designed that any failure of a component in the device, or use of that component outside the device specification, does not result in 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, necessitates physical penetration of the device.

NOTE 1 It is advisable that an SCD should be so designed and constructed that any additions of external devices which intercept or substitute data input to or output from the SCD for the purpose of masquerade 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, e.g. for maintenance, if such access could compromise security, 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.

NOTE 2 For the purposes of this part of ISO 13491, maintenance covers the following three states of the device:

— service: up-keep of the device to ensure its operational condition;

— inspection: physical inspection of the device and assessment of its actual condition;

— repair: reinstatement of the device to its operational condition.

The SCD and its data entry functions shall be, by design, construction and/or deployment, capable of being shielded from direct and indirect monitoring such that no feasible attack will result in compromise of any secret or sensitive data.

The integrity of each tamper protection mechanism shall be ensured. This may be accomplished through the use of additional tamper protection mechanisms, i.e. a layered defence.

6.2.2 Tamper evidence requirements

6.2.2.1 If a device claims to rely on tamper evidence characteristics to defend against substitution, penetration or modification attacks, the manner in which the device defends against the attacks shall be as described in 6.2.2.2 to 6.2.2.4 below.

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

6.2.2.3 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 when returned to operational use.

6.2.2.4 Modification To ensure that modification of an SCD is detected, the device shall be so designed and constructed that any successful modification 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 when returned to operational use.

6.2.3 Tamper resistance requirements

6.2.3.1 If a device claims to rely on tamper resistance characteristics to defend against penetration, modification, monitoring or substitution/removal attacks, the manner in which the device defends against the attacks shall be as described in 6.2.3.2 to 6.2.3.5 below.

6.2.3.2 Penetration An SCD shall be protected against successful 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.

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

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

— shielding against electromagnetic emissions, such that no sensitive information could feasibly be disclosed by monitoring the device;

— privacy shielding, such that during normal operation, sensitive information entered will not be easily observable to other persons (e.g. the device could be designed and installed so that the device can be 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.

6.2.3.5 Substitution/Removal If protection against substitution/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.

6.2.4 Tamper response requirements

6.2.4.1 Where an SCD employs a tamper response mechanism, the integrity of the mechanism shall be ensured by employing tamper response characteristics and/or tamper resistant characteristics.

If a device claims to rely on tamper response characteristics to defend against penetration, modification or substitution/removal attacks, the manner in which the device defends against the attacks shall be as described in 6.2.4.2 to 6.2.4.4 below.

6.2.4.2 Penetration A device that claims tamper response 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.

6.2.4.3 Modification A device that claims tamper response 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.

6.2.4.4 Substitution/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.

6.2.5 Physically secure devices

A physically secure device is a hardware device which cannot be feasibly penetrated or manipulated to disclose all or part of any cryptographic key, PIN or other secret value resident within the device.

Penetration of the device shall cause the automatic and immediate erasure of all PINs, cryptographic keys and other secret values and all useful residues of those contained within the device; i.e. the device has tamper response characteristics.

A device shall only be operated as a physically secure device when it can be assured that the device's internal operation has not been modified to allow penetration (e.g. the insertion within the device of an active or passive "tapping" mechanism).

6.2.6 Devices using exclusively unique key per transaction key management

Key management techniques exist where penetration of an SCD does 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 another SCD, e.g. a key loading device. Devices that exclusively use these key management techniques may have reduced tamper protection requirements, providing that the unauthorized determination of the secret data (e.g. PINs and keys) stored within the SCD, or the placing within the device of a "tap" to record secret data, shall require that the device be taken to a specialized facility and either:

— be unavailable for a sufficiently long time, such that there is a high probability that its absence from its operational location is detected, and/or

— be subjected to physical damage at this facility, such that the device cannot be placed back in service without a high probability of the tampering being detected: furthermore, the determination of secret data or the placing of a "tap" within the device shall require specialized equipment and skills, which are not generally available.

Devices that do not exclusively use these key management techniques shall be physically secure devices, as defined in 6.2.5.

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 irreversibly 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 SCDs.

6.3 Logical security requirements for SCDs

6.3.1 Dual control

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 which support the secure implementation of dual or multiple control.

6.3.2 Unique key per device

To limit the impact of a private key compromise, the private key of an SCD shall be unique to that device.

To limit the impact of a secret key compromise, the secret keys used by a pair of communicating SCDs shall be unique, except by chance, to that pair of SCDs.

As a consequence of the above requirements, each PIN entry device within a population of such devices shall have unique keys, except by chance.

NOTE In support of load balancing and disaster recovery processes, a collection of SCDs can employ a common key where all devices within that collection are used strictly for a single common purpose, e.g. host security modules and key loading devices.

6.3.3 Assurance of genuine device

The provision of a genuine, uncompromised device shall be assured by device management. Where a device possesses tamper response characteristics, this may be accomplished by delivering the device with secret information installed (e.g. a key or password) which enables the recipient to ascertain that the device is genuine and not compromised.

6.3.4 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. Care shall be taken to ensure that legitimate functions cannot be used to disclose sensitive information. Therefore, protection against exhaustive searches is needed. When the environment does not provide this protection, it shall be provided by device characteristics.

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 between function calls a minimum time interval that could facilitate an exhaustive search.

6.3.5 Use of cryptographic keys

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

The key generation methods of an SCD shall comply with ISO 11568-2 or ISO 11568-4.

An SCD shall implement only key management schemes that comply with the principles outlined in ISO 11568-1.

6.3.6 Sensitive device states

If an SCD can be put into a “sensitive state”, i.e. a state that allows functions which are normally not permitted (such as manual loading of plaintext cryptographic keys into a device that already has operational keys), then such a transition shall require dual control via a secure operator interface.

NOTE An SCD need not necessarily be put into a sensitive state in order to perform initial loading of plaintext cryptographic keys.

Activation of a tamper response 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.

To minimize the risks of unauthorized use of sensitive functions, the sensitive state shall be established with one or more limits on its use (e.g. the number of function calls and a time limit). After the first of these limits is reached, the device shall immediately and automatically return to its normal state.

6.3.7 Multiple cryptographic relationships

Where multiple cryptographic relationships are to be maintained in a device (e.g. a multi-acquirer PIN pad), the selection of cryptographic key sets for encipherment of sensitive data (e.g. PINs) shall be controlled so that there is no feasible way to select the incorrect key set deliberately or by accident. In this situation, the source and path of data used to select a cryptographic key set shall be physically or logically protected.

6.3.8 SCD software authentication

The SCD shall support a mechanism that ensures that only software approved by the controller can be loaded and installed in the SCD.

NOTE Examples of acceptable methods include generating a cryptographic check value for the software or enciphering the software. Any keys used for this operation need to be managed by the controller or their agent.

6.3.9 Logical design features

Logical design features shall include the following:

— measures to prevent the successful discovery of keying material through monitoring external connections to the device (e.g. protection against differential power analysis and timing attacks);

— measures to prevent the cost-effective discovery of sensitive information, such as PINs, through exhaustive search.

7 Requirements for device management

7.1 General

The security of an SCD 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 or more phases of its life cycle, to the attack scenarios identified earlier.

Depending on where the device is in its life cycle, it may be sufficient to rely on detection of compromise, or it may be necessary to prevent compromise. The method for compromise detection or prevention can also vary depending on the life cycle phase of the device.

7.2 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 SCDs can have substantially different life cycles. Figure 1 presents a generalized device life cycle, indicating the possible phases in the life of an SCD 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.

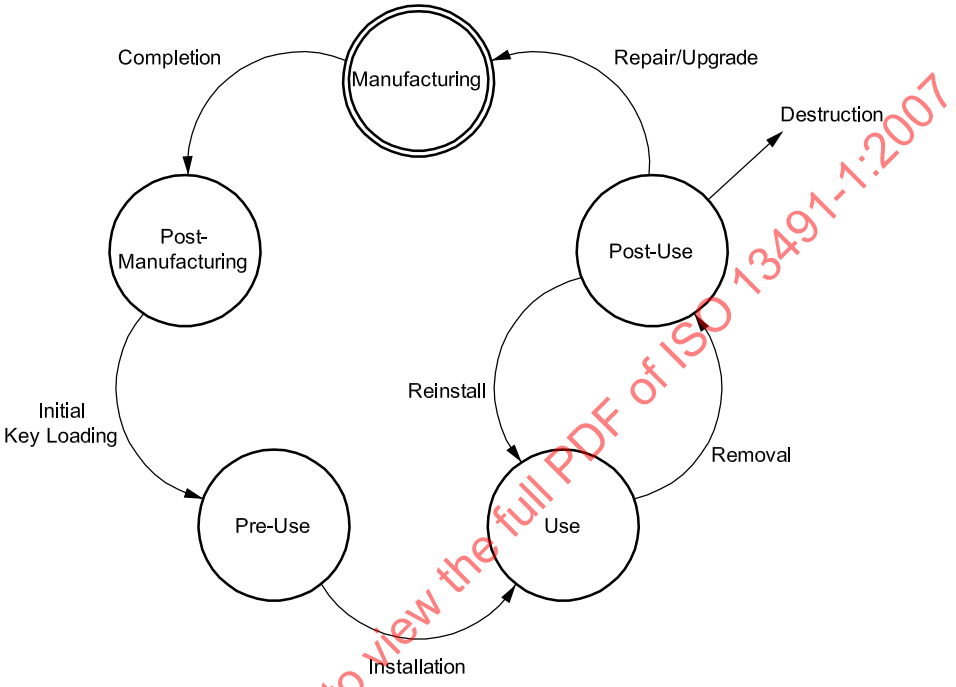

Figure 1 — Device life-cycle state diagram

For the purpose of this part of ISO 13491, the phases of the life cycle are defined for the security sensitive portions of the device as follows:

— manufacturing/repair: 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: phase consisting of the transport and storage of the device up to and including initial key loading;

— pre-use: phase 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 a state of operational use when it has been installed for its intended purpose at its intended location;

— post-use: phase in which the device is removed from service; the removal may be temporary (e.g. to transport the device to a repair centre, to move the device to another operational location or to store the device prior to reuse) or it may be permanent (if the device is removed from service without the intent to subsequently reuse it).

7.3 Life cycle protection requirements

7.3.1 General

This subclause describes the protection requirements during each life cycle phase. The methods that may be used to protect the device during its life cycle phases are described in 7.4.

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 are or have 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 described as given in 7.3.2 to 7.3.5 below.

7.3.2 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 keys are not injected into the device and it 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 device transitions to the pre-use state and the key-erasure mechanisms of the device can offer substantial additional protection, if provided.

7.3.3 Pre-use

During the pre-use phase, the device contains at least one initial key. Detection of device compromise is required.

Prevention of device compromise is required if

— the initial key is, or has been, in use in other devices (other than by chance) to encipher secret data;

NOTE 1 This applies in particular to host security modules and key loading devices as allowed for in ISO 11568-2:2005, 4.10, which requires that: “Any key shall exist in the 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 transaction originating 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.

NOTE 2 When an SCD requires only compromise detection prior to use, the presence of an initial key in the device can serve as an effective means of detection, providing that 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.

7.3.4 Use

Detection of device compromise is required during this phase.

When in operational use, an SCD requires compromise prevention if it contains any key that has been used by this or any other device, or if it contains information from which such a key could be obtained.

NOTE To minimize requirements for compromise prevention, it is advisable that a device 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, e.g. 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 which have been authenticated and/or enciphered by the controller or his agent can be loaded and installed in the device.

For some types of SCDs, 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.

7.3.5 Post-use

Detection of device compromise is required during this phase.

During the post-use phase, an SCD requires compromise prevention if the cryptographic keys or other sensitive data are still stored in an SCD which required compromise prevention in the use cycle.

7.4 Life cycle protection methods

7.4.1 Manufacturing

During the design, construction and repair processes, 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 to, or deletions from, 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, e.g. by dual control over the device. Special care shall be taken to ensure that repair processes do not result in unauthorized physical or functional modifications to the device.

7.4.2 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 private 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 or private key cannot be determined without collusion.

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;

— auditing and control of the device post-manufacture, or subsequent to the most recent testing and/or inspection of the device;

— confirmation of the existence within the device of secret data by the manufacturer for the sole purpose 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 plaintext key loading takes place in a secure facility under dual control and split knowledge.

7.4.3 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 would result in key erasure, which can 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 make unauthorized modifications to the device and then return the device into operational use.

If a particular SCD is potentially subject to fraud that might occur if the device is misappropriated and installed in an unauthorized location or by unauthorized personnel, or is left unguarded for long periods, then controls shall be applied to prevent the unauthorized installation and operation of the device. Such controls may include the entry of an "unlocking code" before it permits operational use.

Device management shall provide detection of unauthorized removal of the device.

7.4.4 Use

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

If an SCD is operated in a minimally controlled environment, the security of the device depends upon its characteristics. Additionally, management controls may be implemented, e.g. review of transaction logs to ensure the device is still in service.

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

— reporting procedures, such that users of the device report missing devices in a timely manner, as specified by the device controller or his agent;

— electronic interrogation procedures, whereby 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 malfunctioning 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 and functional characteristics of the device have not been altered. If an SCD outputs alarms that indicate a malfunction has occurred which might jeopardise the device’s security, then the keys shall be erased and the device shall be removed from service immediately.

7.4.5 Post-use

If a device enters the post-use phase and it is intended to reuse the device in the same organization, it may be stored until such reuse with the key still present, providing that it is given the same type of protection as that required by the device while in use.

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

If a device enters the post-use phase for repair, all keys shall be erased.

If the device's keys are erased before it is stored for repair and/or possible reuse, new keys shall 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 plaintext key replacement takes 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 phase of the life cycle.

Alternatively, the device shall 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.

7.5 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 can reside with different parties in different organizations.

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

Independent auditors may be either internal or external to the organization. Using the audit checklists, they shall periodically confirm that all device management requirements are being met by the organization in question and that the accountable parties 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 party shall be identified by these records. When devices are transferred to another organization, another party becomes accountable for the devices. Therefore, the records at both the originating and receiving organization shall 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 shall be

some means of confirming that accountability has been accepted by the receiving organization and the name of the party that is presently accountable for the transferred devices shall be included in the records of the transferring organization.

7.6 Device management principles of audit and control

Audit and control are essential parts of device management. Table 1 summarizes some general principles relating to audit and control procedures, and indicates their applicability to each phase of the device life cycle.

Table 1 — Audit and control principles

	Procedure	Manufact.	Post-manufact.	Pre-use	Use	Post-use
1	One or more parties responsible for the device.	M	M	M	M	M
2	Careful screening of, or control over, personnel with access to a device designed for use in a controlled environment	M	M	M	M	M/R
3	Careful screening of, or control over, personnel with access to a device designed for use in a minimally controlled environment	M	M	M	NA	M/R
4	Control over the manufacturing (design, construction, repair) 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 checklists	M	M	M	M	M
7	Verification that audit checklists 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 a device to confirm cryptographically that it is still operational	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	M	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 or detected	M	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 in order that the confidentiality of the device design characteristics is maintained	M/R	M/R	M/R	M/R	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

R Recommended

M/R Mandatory when compromise prevention is required, otherwise recommended

NA Not applicable

8 Evaluation methods

8.1 General

8.1.1 Choice of evaluation method

In order to ascertain whether a secure cryptographic device complies with this part of ISO 13491, three alternative evaluation methodologies for verifying compliance with the specified requirements are defined, as follows:

a) an informal evaluation undertaken by an independent assessor using the assessment checklists to be found in ISO 13491-2;

NOTE Where devices offer multi-functionality, it is 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 checklists would be used during the evaluation.

b) a semi-formal evaluation undertaken by an evaluation agency;

c) a formal evaluation conducted by an accredited evaluation authority.

A risk assessment shall be undertaken as an aid in choosing which methodology is appropriate (see 8.2). 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 may be justified. The comparison of estimated risk, cost and time is found in Table 2. There may additionally be constraints and requirements imposed by individual countries or by international organizations upon their members. 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 2 — Risk factors versus evaluation methods

Risk factor	Evaluation method		
	Informal	Semi-formal	Formal
Estimated risk	Low	Medium/High	High
Cost	Low	Medium	High
Time factor	Short	Medium	Long
Assurance	Assessment report	Evaluation report	Certificate
NOTE The level of assurance is directly related to the level of experience and competence and the equipment involved in the evaluation process.			

8.1.2 Informal method

In the informal method (see Figure 2), a manufacturer or sponsor submits a device to an assessor for evaluation against the appropriate checklist(s). The results are forwarded to the assessment review body, which produces an assessment report.

8.1.3 Semi-formal method

In the semi-formal method (see Figure 2), 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 can also receive independent results from an auditor/assessor, as depicted by the dotted line in Figure 2.

8.1.4 Formal method

The third method shown in Figure 2 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. (See ISO/IEC 15408 and ISO/IEC 19790 for examples of formal evaluation methodologies.)

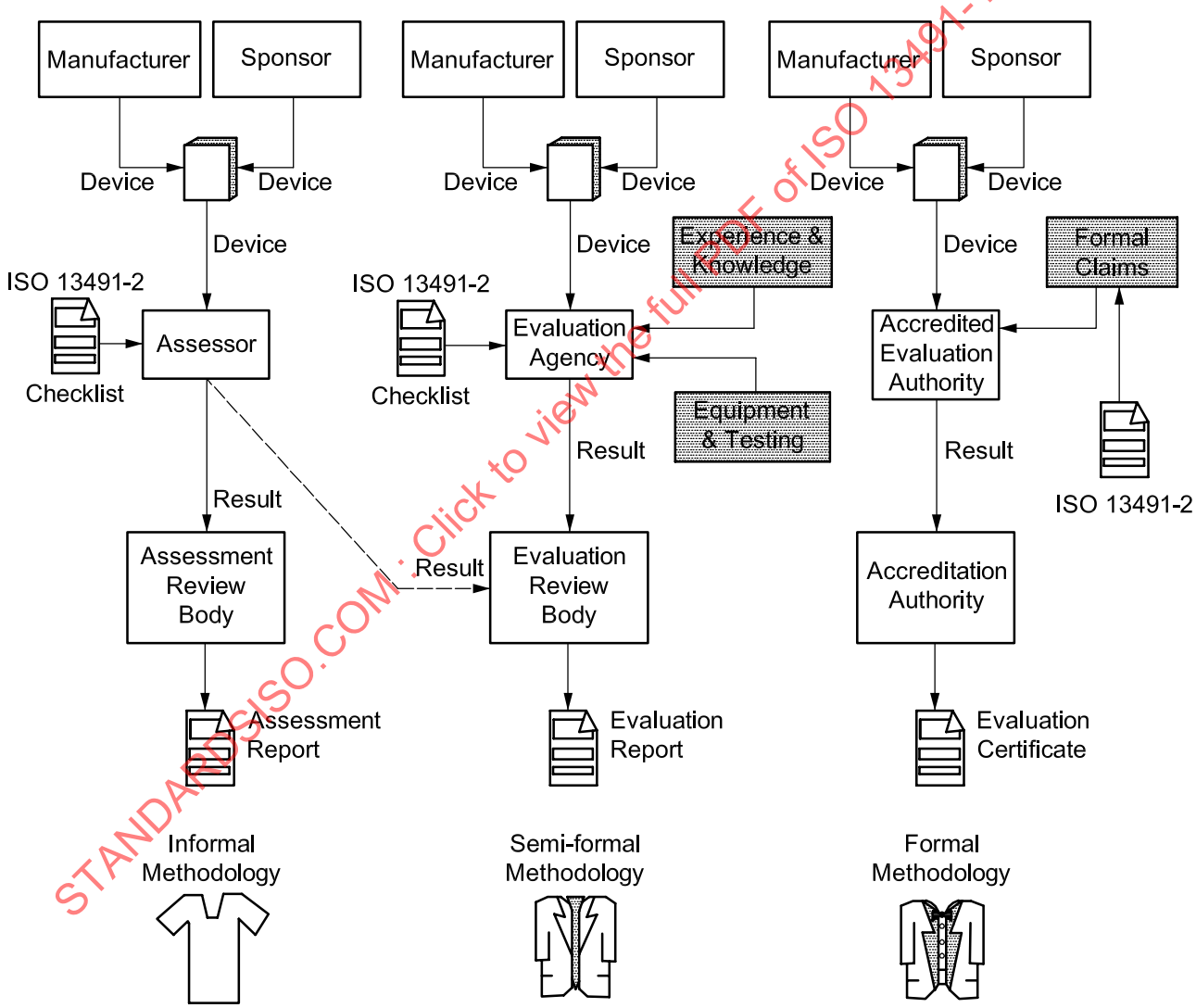

Figure 2 — Evaluation methods

8.2 Risk assessment

Since absolute security is not achievable in practical terms, 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 an iterative process considering the following:

— threats imposed by the attacks;

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

Risk assessment is not solely based on value judgements, but it always includes them. Various methods can be used to perform a risk assessment, but this topic is outside the scope of this part of ISO 13491.

8.3 Informal evaluation method

8.3.1 General

At the request of a sponsor, an informal evaluation may be undertaken by an independent assessor. For this purpose, the assessor shall complete the appropriate assessment checklist(s) for the device being evaluated. Upon completion of the evaluation, the results shall be submitted to the assessment review body, which shall review the results and accept, reject or ask for clarification of those results. Upon completion of the review, the audit report shall be submitted to the sponsor.

Before commencement of any evaluation, there shall 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.

8.3.2 Manufacturer/sponsor

The manufacturer can be the sponsor, or the sponsor can be an independent body. In both cases, the sponsor shall assume the following role and responsibilities:

— initiate the process;

— complete the risk assessment (incorporating other factors, such as time, cost, etc.);

— choose the appropriate checklist(s);

— submit the “deliverables” to the evaluation process;

— receive the assessment report.

8.3.3 Assessor

The assessor shall be independent of the sponsor, either from an external organization or, if internal to the sponsor organization, outside the sponsor’s influence.

The assessor shall assume the following role and responsibilities:

— answer the questions in the appropriate checklist as true (T), false (F), or not applicable (N/A);

— if the answer is false or not applicable, produce the explanation;

— submit results to the assessment review body.

8.3.4 Assessment review body

The assessment review body can be either the sponsor itself or an independent body. In both cases, the assessment review body shall assume the following role and responsibilities:

— receive the submitted results from the assessor;

— if the answer is false or not applicable, determine whether the explanation is justified;

— return the explanation to the assessor for further clarification, if necessary;

— determine the security level of the intended environment;

— determine whether the security level of the SCD meets or exceeds the minimally acceptable security requirements appropriate for its operational environment;

— produce the assessment report and submit it to the sponsor.

The original risk assessment should be considered as part of the input for the assessment review.

8.3.5 Assessment checklist

The assessment checklists found in ISO 13941-2 are a list of statements, where an assessor indicates, for each such statement, whether or not this statement applies for the equipment under assessment. These statements may be much more thorough than the requirements they represent and may present implications of the requirements or preferred implementations to meet the requirements. Thus a false or not applicable answer to a checklist statement does not necessarily mean non-compliance, it simply means that compliance might be questionable and needs to be considered.

Therefore, the assessor shall produce a result which contains the reason for the false or not applicable response and then either

— explain how the underlying security requirement is adequately fulfilled by other means, or

— indicate how and when the non-compliant situation will be corrected, or

— indicate why non-compliance is not applicable.

Additional checklists such as national and/or local standards, can be used by the assessor, and in order to complete the evaluation, several assessment functionality lists may be required.

8.3.6 Assessment results

The assessment results shall include the following:

— the list of pertinent documentation used for the evaluation;

— a completed assessment checklist with all statements completed as either true, false or not applicable;

— an explanation of all exceptions (i.e. false and not applicable);

— the name of the sponsor;

— the name of the assessor and the assessor's organization;

— the date of the assessment;

— identification of the device (e.g. manufacturer's name, model number, etc.).

8.3.7 Assessment Report

The assessment report shall include the following:

— all the information received in the assessment results;

— the list of pertinent documentation used for the review;

— the justification or rejection of all exceptions from the assessment results;

— the name of the assessment review body;

— the date of the review;

— a final recommendation of the device's acceptance or rejection for its intended environment.

If the device has been rejected, the report may additionally include recommendations for increasing the device's security and/or increasing environmental controls so that the device might obtain acceptance.

8.4 Semi-formal evaluation method

8.4.1 General

An evaluation undertaken by an evaluation agency will in many ways be the same as that undertaken by an accredited evaluation authority. Independence and the relevant skills needed to undertake the evaluation will be required, but will be free from the rigors imposed by the formal methods needed for certification. To enable an SCD evaluated by different evaluation agencies to conform to a common set of input requirements, the evaluation agency shall use the assessment checklists found in ISO 13491-2 as a base upon which the device shall be evaluated.

Two methods of working are recommended, as described below.

— The evaluation review body and/or sponsor produces a set of requirements upon which the SCD shall be evaluated. Where such an evaluation is undertaken, the results are made available only to the sponsor and/or review body as necessary.

— Where the sponsor and/or review body have/has a need for conformance, e.g. to a network or payment system interface, the SCD shall be evaluated using the evaluation checklists from which a set of claims are produced. These claims are used as part of the evaluation process.

Where the risk is seen as sufficient to need a third party evaluation, yet formal certification of the results is not required, evaluation by an evaluation agency is recommended.

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

8.4.2 Manufacturer/sponsor

The role and responsibilities of the manufacturer and the sponsor are the same as those described in 8.3.2.

8.4.3 Evaluation agency

The evaluation agency shall be independent of, and external to, the manufacturer and the sponsor and shall assume the following role and responsibilities:

— use the appropriate evaluation checklists to help to determine tests;