BS ISO 13491-1:2016

BSI Standards Publication

Financial services — Secure cryptographic devices (retail)

Part 1: Concepts, requirements and evaluation methods

bsi.

...making excellence a habit.™

National foreword

This British Standard is the UK implementation of ISO 13491-1:2016. It supersedes BS ISO 13491-1:2007 which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee IST/12, Financial services.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

ISBN 978 0 580 79378 3

ICS 35.240.40

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 March 2016.

Amendments issued since publication

Date	Text affected

BS ISO 13491-1:2016

INTERNATIONAL STANDARD

ISO 13491-1

Third edition
2016-03-15

Financial services — Secure cryptographic devices (retail) —

Part 1: Concepts, requirements and evaluation methods

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

Partie 1: Concepts, exigences et méthodes d'évaluation

Reference number
ISO 13491-1:2016(E)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

Page

Foreword

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

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is ISO/TC 68, *Financial services*, Subcommittee SC 2, *Security*.

This third edition cancels and replaces the second edition (ISO 13491-1:2007), which has been technically revised.

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

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

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

Introduction

ISO 13491 describes both the physical and logical characteristics and the management of the secure cryptographic devices (SCDs) used to protect messages, cryptographic keys, and other sensitive information used in a retail financial services environment.

This part of ISO 13491 contains the security requirements for SCDs. ISO 13491-2 is a tool for measuring compliance against these requirements. It provides a checklist of

— characteristics that a device has to possess,

— how devices have to be managed, and

— characteristics of the operational environments.

The security of retail electronic payment systems is largely dependent upon the security of these cryptographic devices. This security is based upon the premise that computer files can be accessed and manipulated, communications lines can be "tapped", and authorized data or control inputs into system equipment can be replaced with unauthorized inputs. When personal identification numbers (PINs), message authentication codes (MACs), cryptographic keys, and other sensitive data are processed, there is a risk of tampering or other compromise to disclose or modify such data. The risk of financial loss is reduced through the appropriate use of cryptographic devices that have proper characteristics and are properly managed.

Appropriate device characteristics are necessary to ensure that the device has the proper operational capabilities and provides adequate protection for the data it contains. Appropriate device management is necessary to ensure that the device is legitimate, that it has not been modified in an unauthorized manner (e.g. by "bugging"), and that any sensitive data placed within the device (e.g. cryptographic keys) has not been subject to disclosure or change.

Absolute security is not achievable in practical terms. Cryptographic security depends upon each life cycle phase of the SCD and the complementary combination of appropriate management procedures and secure cryptographic characteristics. These management procedures implement preventive measures to reduce the opportunity for a breach of SCD security. This aims for a high probability of detection of any unauthorized access to sensitive or confidential data should device characteristics fail to prevent or detect the security compromise.

INTERNATIONAL STANDARD ISO 13491-1:2016(E)

Financial services — Secure cryptographic devices (retail) —

Part 1: Concepts, requirements and evaluation methods

1 Scope

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

This part of ISO 13491 has two primary purposes:

— to state the security characteristics concerning both the operational characteristics of SCDs and the management of such devices throughout all stages of their life cycle;

— to provide guidance for methodologies to verify compliance with those requirements. This information is contained in Annex A.

ISO 13491-2 specifies checklists to be used to evaluate secure cryptographic devices (SCDs) incorporating cryptographic processes as specified in ISO 9564-1, ISO 9564-2, ISO 16609, ISO 11568-1, ISO 11568-2, ISO 11568-3, ISO 11568-4, ISO 11568-5, and ISO 11568-6 in the financial services environment.

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

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

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

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

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

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

ISO 11568-4, *Banking — Key management (retail) — Part 4: Asymmetric cryptosystems — Key management and life cycle*

3 Terms and definitions

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3.26
operational environment
environment in which the *SCD* (3.28) is operated, i.e. the system of which it is part, the location where it is placed, the persons operating and using it, and the entities communicating with it

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

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

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

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

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

3.32
sensitive state
device condition that provides access to the secure operator interface, such that it can only be entered when the device is under *dual control* (3.16)

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

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

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

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

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

4 Abbreviated terms

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

5 Secure cryptographic device concepts

5.1 General

Cryptography is used in retail financial services to help ensure the following objectives:

a) the integrity and authenticity of sensitive data, e.g. by MAC-ing transaction details;

b) the confidentiality of secret information, e.g. by encrypting customer PINs;

c) the confidentiality, integrity, and authenticity of cryptographic keys;

d) the security of other sensitive operations, e.g. PIN verification.

To ensure that the above objectives are met, the following threats to the security of the cryptographic processing shall be countered:

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

— unauthorized use or modification of cryptographic services.

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

Since absolute security is not achievable in practical terms, it is not realistic to describe an SCD as being "tamper proof" or "physically secure". With enough cost, effort, and skill, virtually any security scheme can be defeated. Furthermore, as technology continues to evolve, new techniques may be developed to attack a security scheme that was previously believed to be immune to feasible attack. Therefore, it is more realistic to categorize an SCD as possessing a degree of tamper protection where an acceptable degree is one that is deemed adequate to deter any attack envisaged as feasible during the operational life of the device taking into account the equipment, skills, and other costs to the adversary in mounting a successful attack and the financial benefits that the adversary could realize from such an attack.

Security of retail payment systems includes the physical and logical aspects of device security, the security of the operational environment, and management of the device. These factors establish jointly the security of the devices and the applications in which they are used. The security needs are derived from an assessment of the risks arising from the intended applications.

The required security characteristics will depend on the intended application and operational environment and on the attack types that need to be considered. A risk assessment should be made as an aid to selecting the most appropriate method of evaluating the security of the device. The results are then assessed in order to accept the devices for a certain application and environment. Evaluation methods are given in Annex A.

5.2 Attack scenarios

5.2.1 General

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

— penetration;

— monitoring;

— manipulation;

— modification;

— substitution.

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

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

5.2.2 Penetration

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

5.2.3 Monitoring

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

5.2.4 Manipulation

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

5.2.5 Modification

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

5.2.6 Substitution

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

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

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

5.3 Defence measures

5.3.1 General

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

— device characteristics;

— device management;

— environment.

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

5.3.2 Device characteristics

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

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

— tamper evidence characteristics;

— tamper resistance characteristics;

— tamper response characteristics.

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

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

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

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

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

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

— key management methods,

— security practices, and

— operational procedures.

The 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 General

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.

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 ensured that the device's internal operation has not been modified, (e.g. the insertion within the device of an active or passive "tapping" mechanism).

6.2 Physical security requirements for SCDs

6.2.1 General

— An SCD shall be so designed that any failure of a part in the device, or use of a part outside the device specification, does not result in the disclosure or undetected modification of sensitive data.

— An SCD shall be so designed and constructed such that without physical penetration of the device, any unauthorized access to, or modification of, sensitive data (including device software) that are input, stored, or processed in it is impractical.

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.

— An SCD shall be so designed and constructed such that regular maintenance does not require access to internal areas that could compromise security.

— An SCD shall be so designed and constructed such that repair, if it requires access to internal areas that could compromise security, shall cause immediate erasure of all cryptographic keys and other sensitive data.

— An SCD, including its data entry functions, shall be so designed, constructed, and/or deployed such that secret and sensitive data are shielded from monitoring by any practical attack.

— Each tamper protection mechanism shall be protected against modification or circumvention.

NOTE This may be accomplished through the use of additional tamper protection mechanisms, i.e. a layered defence.

6.3 Tamper evident requirements

6.3.1 General

Tamper evidence provides an indication that an attack has been attempted. If a device claims to rely on tamper evident characteristics to defend against substitution, penetration, or modification attacks, the manner in which the device defends against the attacks shall be as described in 6.3.1.1 to 6.3.1.3.

6.3.1.1 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.

6.3.1.2 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.

6.3.1.3 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.

6.3.1.4 Monitoring

— The device should be designed and constructed in such a way that any unauthorized additions to the exterior of the device, intended to monitor it for secret or sensitive information, shall have a high probability of being visually detected before such monitoring can occur.

6.4 Tamper resistant requirements

6.4.1 General

Tamper resistance provides passive physical protection against attacks. 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 6.4.1.1 to 6.4.1.3 and optionally, 6.4.1.4.

6.4.1.1 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 impracticable in its intended environment.

6.4.1.2 Modification

— An SCD shall be protected against successful modification by being tamper resistant to such a degree that its passive resistance is sufficient to make modification of an SCD (e.g. the implantation of a bug within the SCD) in its intended environment impracticable without rendering the SCD inoperable.

— The unauthorized modification of any key or other sensitive data stored within the SCD shall cause damage such that the SCD is rendered inoperable.

6.4.1.3 Monitoring

— The SCD shall not reveal secret or sensitive information (e.g. PINs or cryptographic keys) except

  a) when enciphered with the appropriate legitimate key, or

  b) in an authorized manner (e.g. PIN mailers).

— The SCD shall protect against electromagnetic emissions such that no sensitive information could feasibly be disclosed by monitoring the device.

— The SCD shall not display the digits of entered PINs in clear text.

— Where parts of the device cannot be appropriately protected from monitoring, these parts of the device shall not display, store, transmit, or process secret or sensitive information.

6.4.1.4 Substitution/removal

— In order to protect against substitution/removal, the device should be secured in such a manner that it is not practical to remove the device from its intended place of operation.

6.5 Tamper responsive requirements

6.5.1 General

Tamper responsiveness provides active protection against attacks.

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

Where an SCD employs a tamper response characteristic to defend against penetration or modification attacks, the manner in which the device defends against the attacks shall be as described in 6.5.1.1 and 6.5.1.2.

6.5.1.1 Penetration

Where an SCD employs tamper response characteristics, it 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.

6.5.1.2 Modification

Where an SCD employs tamper response characteristics, it 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.

6.6 Logical security requirements for SCDs

6.6.1 Dual control

Where a requirement for dual 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 control.

6.6.2 Unique key per device

Except in support of load balancing and disaster recovery processes, to limit the impact of a private key compromise, the private key of an SCD shall be unique, except by chance, to that device.

Except in support of load balancing and disaster recovery processes (e.g. HSMs and KLDs) 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 (e.g. HSM to PED or HSM to HSM).

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

6.6.3 Assurance of genuine device

The provision of a genuine, uncompromised device shall be ensured by the device management. 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.

6.6.4 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. Legitimate functions shall not be capable of disclosing sensitive information, except as explicitly allowed by the security scheme used. Therefore, protection against exhaustive searches is needed. When the environment does not provide this protection, it shall be provided by the device characteristics.

The following are examples of how this can be achieved:

— internal monitoring of statistics against predefined threshold parameters which then triggers an appropriate response, e.g. so that only some given percentage of failed PIN verifications are permitted amongst all PIN verifications in a given time;

— imposing between function calls, a minimum time interval that could protect against an exhaustive search.

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 successful discovery of sensitive information unless provided by the environment;

— measures that ensure the device only performs its designed functions (e.g. performing input validation to prevent buffer overflow attacks).

6.6.5 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 the key management schemes that comply with the principles outlined in ISO 11568-1.

6.6.6 Sensitive device states

If an SCD can be put into a sensitive state, then such a transition shall require dual control via a secure operator interface.

If passwords or other plaintext data are used to control transition to a sensitive state, then the input of such passwords shall be protected from monitoring.

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.

Activation of a tamper response mechanism shall not put the SCD into a sensitive state.

6.6.7 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.

6.6.8 SCD software authentication

The SCD shall ensure that only approved and authenticated software can be loaded and installed in the SCD. An example of an acceptable method is cryptographic verification of the software. Any keys used for this purpose shall be securely managed according to ISO 11568.

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 and its environment 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.

Throughout the life cycle of the device, key management shall comply with the principles of ISO 11568-1.

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.

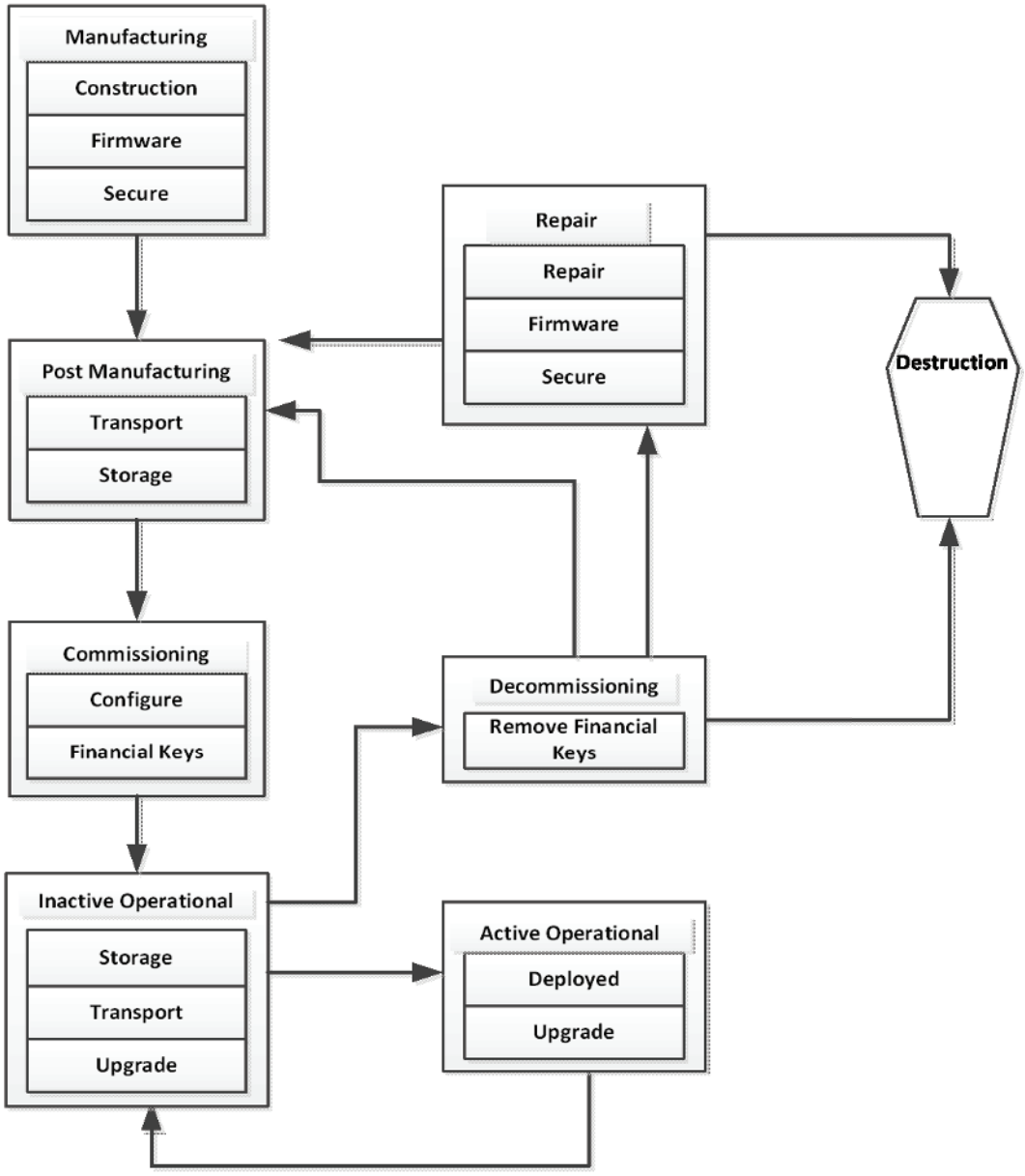

Figure 1 — Device life-cycle state diagram

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 phase:** The design, construction, and testing of a device so that the device incorporates the intended administrative functionality and physical security characteristics. The device will leave this stage with firmware, and where applicable, the manufacturer's embedded keys (known as the manufacturer's keys). These may be the PKI keys (known as the SCD's PKI keys) necessary for remote symmetric key distribution performed using asymmetric techniques. The device tamper responsive mechanisms shall be active in order to protect these keys.

— **Post manufacturing phase:** Phase consisting of the transport and storage of the device prior to initial financial key loading;

— **Commissioning phase (initial financial key loading phase):** Phase consisting of loading or self-generation of the initial financial keys (and payment application for PEDs). The device leaves this phase ready for operational use.

— **Inactive operational phase**: Phase in which the device contains financial keys, but is not in operational use. Devices in this phase will be stored and transported to the site of operational use. They include devices stored as spares or held as seasonal inventory.

— **Active operational phase:** A device can be regarded as being in a state of active operational use when it has been installed for its intended purpose at its intended location.

— **Decommissioning phase:** Phase in which the SCD is removed from operational service permanently, or for repair, and the financial keys are removed.

NOTE 1 It is permissible to leave the manufacturer's keys and the SCD's PKI keys intact.

NOTE 2 For PEDs, it is permissible to utilize an authorized agent to remove the keys.

— **Repair phase:** Phase where a decommissioned device is returned to the manufacturer or an authorized facility for repair and testing so that once again, the device incorporates the intended administrative functionality and physical security characteristics. The device will leave this stage with firmware and the manufacturer's embedded keys and may also receive or generate the SCD's PKI keys if remote symmetric key distribution is performed using asymmetric techniques.

— **Destruction phase:** Phase in which the device is destroyed or otherwise, rendered permanently inoperable.

7.3 Life cycle protection requirements

7.3.1 General

This subclause describes the protection requirements during each life cycle phase. The methods that shall be used to protect the device during its life cycle phases are described in 7.4. Both detection and prevention of device compromise shall be required throughout the life cycle of all devices.

NOTE As all SCDs are required to be tamper responsive once this protection is active, it is considered that prevention of device compromise is in place.

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.

7.3.2 Manufacturing phase

During the manufacturing phase, security relies on the manufacturer's procedures and environment. The security of the device shall not depend only upon the secrecy of the design details. However, such

secrecy contributes to the security of the device and therefore, the manufacturer's procedures shall be designed to prevent the disclosure of detailed design documentation.

As part of the manufacturing process, a series of cryptographic keys may be installed or generated. Prior to the loading or generation of the first cryptographic keys of the device, protection is provided by the characteristics of the device itself through the physical difficulty of opening the device or of obtaining a counterfeit version to substitute for the device.

The first cryptographic keys may include, but are not limited to, firmware protection keys and public/private key pairs used to protect initial financial key distribution such as the terminal master key for ATMs or the initial key for a POS PED. Subsequent to the loading of these keys, the device transitions to the inactive operational phase and the tamper responsive mechanisms of the device provide protection for the keys.

The manufactured device provides protection through the device characteristics, i.e. tamper evidence, resistance, and responsiveness. Thus, if the device is compromised, the keys loaded during manufacturing shall be erased, rendering the device inoperable, i.e. incapable of having the initial financial key loaded.

Some SCDs (e.g. HSMs) may be manufactured such that there are no cryptographic keys within the device. Until an initial key has been loaded or generated, it is necessary to detect, but not to prevent a compromise. 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 the device.

7.3.3 Post-manufacturing phase

Prior to initial financial key loading, the SCD shall be protected against modification. Such protection shall be a combination of the characteristics of the device (i.e. tamper evidence, resistance, and responsiveness) and device management procedures. If the device has any manufacturer keys loaded, compromise shall be both prevented and detected.

During the post-manufacturing phase, security relies on the device characteristics as described in 7.3.2 and the procedures surrounding the storage and transport of the device prior to the initialization of the device with financial keys. The entity responsible for the devices in the post manufacturing phase is the current owner which may still be the manufacturer, but could be the acquirer or even the merchant.

7.3.4 Commissioning (initial financial key loading) phase

During the commissioning phase, the device contains at least one initial financial key. Detection of device compromise is required.

During initial financial key loading, security relies on the loading organization's procedures. At the start of this process, the device shall be confirmed as legitimate and untampered. In order to detect substitution, the SCD shall be queried and the response verified against the device's serial number received via an out of band method (e.g. from the manufacturer, through e-mail).

7.3.5 Inactive operational phase

The protections are provided by the characteristics of the device, i.e. tamper evidence, resistance, and responsiveness, and device management procedures including the storage and transport of the device prior to the active deployment of the device. The entity responsible for the devices in this phase is the current owner which may be the acquirer or even the merchant.

During the inactive operational phase, the device contains at least one financial key. The device shall be managed in such a way as to detect compromise and protect against misuse

Upgrades to an SCD performed during this phase that could impact its security functionality shall be cryptographically verified or performed under dual control.

7.3.6 Active operational phase (use)

Detection of device compromise is required during this phase.

Device management shall prevent or detect the unauthorized functional alteration of the device, e.g. the unauthorized modification of the device's firmware and software.

Where a download feature is available, a specific technique for authentication of the software and/or data (payment related, e.g. BIN Tables) shall be included. Any firmware download shall be classified as an upgrade. Such a technique shall ensure that only items intended for download and which have been authenticated and are not out of sequence can be loaded and installed in the device

Upgrades to an SCD performed during this phase that could impact its security functionality shall be cryptographically verified or performed under dual control.

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.

7.3.7 Decommissioning (post-use) phase

Devices are decommissioned with the following intent to either

— transfer ownership of the device to another organization,

— repair the device, or

— destroy the device.

During the decommissioning phase, any financial keys stored in the SCD shall be erased.

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 post manufacturing phase of the life cycle.

If a device is to be destroyed, all the device's keys shall be erased or destroyed prior to the physical destruction of the device such that there is no possibility of the keys or other sensitive data being compromised.

7.3.8 Repair phase

Device management is required during this phase.

During repair, security relies on the repairer's procedures. Both prevention and detection of device compromise is required.

At the start of the repair process, the device shall be inspected for modification or substitution.

Upon receipt of the SCDs, the repair facility shall check the SCD and, if present, erase all keys. If it is not possible to confirm that all keys have been erased, those parts of the device in which keys or other sensitive data may remain shall be physically destroyed.

If any parts of the device are salvaged for spare parts, all such parts shall be accounted for and all other parts shall be destroyed.

As part of the repair process, a series of new cryptographic keys may be installed. These keys may include, but are not limited to the manufacturer's keys or the SCDs PKI keys.

The repaired device provides protection through the device characteristics, i.e. tamper evidence, resistance, and responsiveness. Thus, if the device is compromised, the keys loaded during repair shall be erased rendering the device inoperable.

A repaired device shall be loaded with new keys only when it can be ensured 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.

7.3.9 Destruction phase

Device management is required during this phase.

Each device shall be individually accounted for by serial number in the destruction process.

No physical component of the device shall remain physically intact rendering resale through retail commercial channels infeasible. This is to ensure that the device will not, accidentally or deliberately, be reloaded with keys and restored to service or used as a counterfeit substitute.

No keys or sensitive information should have remained in the device prior to entering the destruction phase. All financial keys should have been erased during the decommissioning phase.

7.4 Life cycle protection methods

7.4.1 Manufacturing

During the design and construction 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 and failing prevention detected. Methods shall exist that have a high probability of preventing and failing preventing detecting the replacement of the device with a substitute.

7.4.2 Post manufacturing phase

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.

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 the following:

— 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 Commissioning (initial financial key loading) phase

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 one or more of the following:

— testing and/or inspection of the device;

— auditing and control of the device 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.

NOTE ISO 11568 requires that initial plaintext key loading takes place in a secure facility under dual control and split knowledge referring to ISO 13491-2:2005, Annex H.

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

7.4.4 Inactive Operational Phase

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

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

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

If a device moves from the inactive operational phase to the decommissioned phase, all financial keys shall be erased.

7.4.5 Active operational (use) phase

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 repair phase of the device life cycle. Keys shall be erased from the malfunctioning device and 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.

7.4.6 Decommissioning phase

When a device enters the decommissioning phase, all financial keys shall be erased.

If a device enters the decommissioning phase for repair, all keys shall be erased.

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 financial keys are erased or destroyed. At this point, the device can be transferred to another organization to enter the post manufacturing phase of the life cycle.

If the device is to be neither transferred to another owner nor repaired, 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.

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

7.4.7 Repair

Special care shall be taken to ensure that repair processes do not result in unauthorized physical or functional modifications to the device

New keys shall be loaded into the device only when it can be ensured 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 referring to ISO 13491-2:2005, Annex H.

7.4.8 Destruction

Auditing and controls shall be implemented to detect and prevent any theft of devices or parts of devices so that they cannot be, accidentally or deliberately, reloaded with keys and restored to service or used as a counterfeit substitute.

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, records showing chain of custody 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 written confirmation that transfer of custody 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	Manufacture	Post manufacture	Commission	Inactive operational	Active operational	Decommissioning	Repair	Destruction
1	One or more parties responsible for the device	M	M	M	M	M	M	M	M
2	Careful screening of, and control over, personnel with access to a device designed for use in a controlled environment	M	M	M	M	M	M	M	M
3	Careful screening of, and control over, personnel with access to a device designed for use in a minimally controlled environment (see ISO 13491-2:2005, Annex H)	M	M	M	NA	NA	R	M	M
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	NA	M	M
5	Control mechanisms or sealing of the device in counterfeit resistant, tamper evident packaging to prevent undetected access to the device	M	M	R	NA	NA	R	M	R
6	Preparation and use of audit checklists	M	M	M	M	M	M	M	M
7	Verification that audit checklists are filled out accurately, on a timely basis, and by qualified personnel	M	M	M	M	M	M	M	M
8	Key management procedures implemented as specified in the appropriate International Standard	M	M	M	M	M	M	M	NA
9	Accurate tracking of each device	M	M	M	M	M	M	M	M
10	Documented procedures to prevent the theft of, or unauthorized access to, a device when in operational use	NA	NA	M	M	M	M	NA	NA
11	Control of the distribution of device specification documentation	R	R	R	R	R	R	R	R
12	Periodic electronic interrogation of a device to confirm cryptographically that it is still operational	NA	NA	NA	NA	R	NA	NA	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	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	M	M	M	M	M	M	M	NA

M mandatory

R recommended

NA not applicable

Table 1 *(continued)*

	Procedure	Manufacture	Post manufacture	Commission	Inactive operational	Active operational	Decommissioning	Repair	Destruction
15	Key erasure if a device is permanently removed from service	NA	NA	NA	NA	NA	M	M	NA
16	Control over the maintenance process in order that the confidentiality of the device design characteristics is maintained	R	R	R	R	R	R	R	R
17	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	NA	M	M	NA

M mandatory
R recommended
NA not applicable

Annex A
(informative)

Evaluation methods

A.1 General

The methodologies in this part of ISO 13491 should be used for the evaluation of devices when claiming compliance to ISO 13491.

A.1.1 Choice of evaluation method

In order to ascertain whether a secure cryptographic device complies with this part of ISO 13491, four 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 semi-formal evaluation with approval undertaken by an accredited evaluation agency;

d) a formal evaluation conducted by an accredited evaluation agency.

A risk assessment should be undertaken as an aid in choosing which methodology is appropriate (see A.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, approved semi-formal, or semi-formal evaluation may be justified. The comparison of estimated risk, cost and time is found in Table A.1. 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 A.1 — Risk factors versus evaluation methods

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

A.1.2 Informal method

In the informal method (see Figure A.1), a sponsor, who may be the manufacturer, 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.

A.1.3 Semi-formal method

In the semi-formal method (see Figure A.1), a sponsor, who may be the manufacturer, 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 A.1.

A.1.4 Semi-formal method with approval

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

The agency produces a report which is forwarded to the evaluation review body which notifies the approval authority of the result of the review.

Where the review result is positive, the approval authority produces an approval letter.

NOTE The evaluation review body may also receive independent results from an auditor as depicted by the dotted line in Figure A.1.

A.1.5 Formal method

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

The sponsor, who may be the manufacturer, submits a device to an accredited evaluation agency 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, which provides a model and ISO/IEC 19790, which provides security requirements for examples of formal evaluation methodologies).

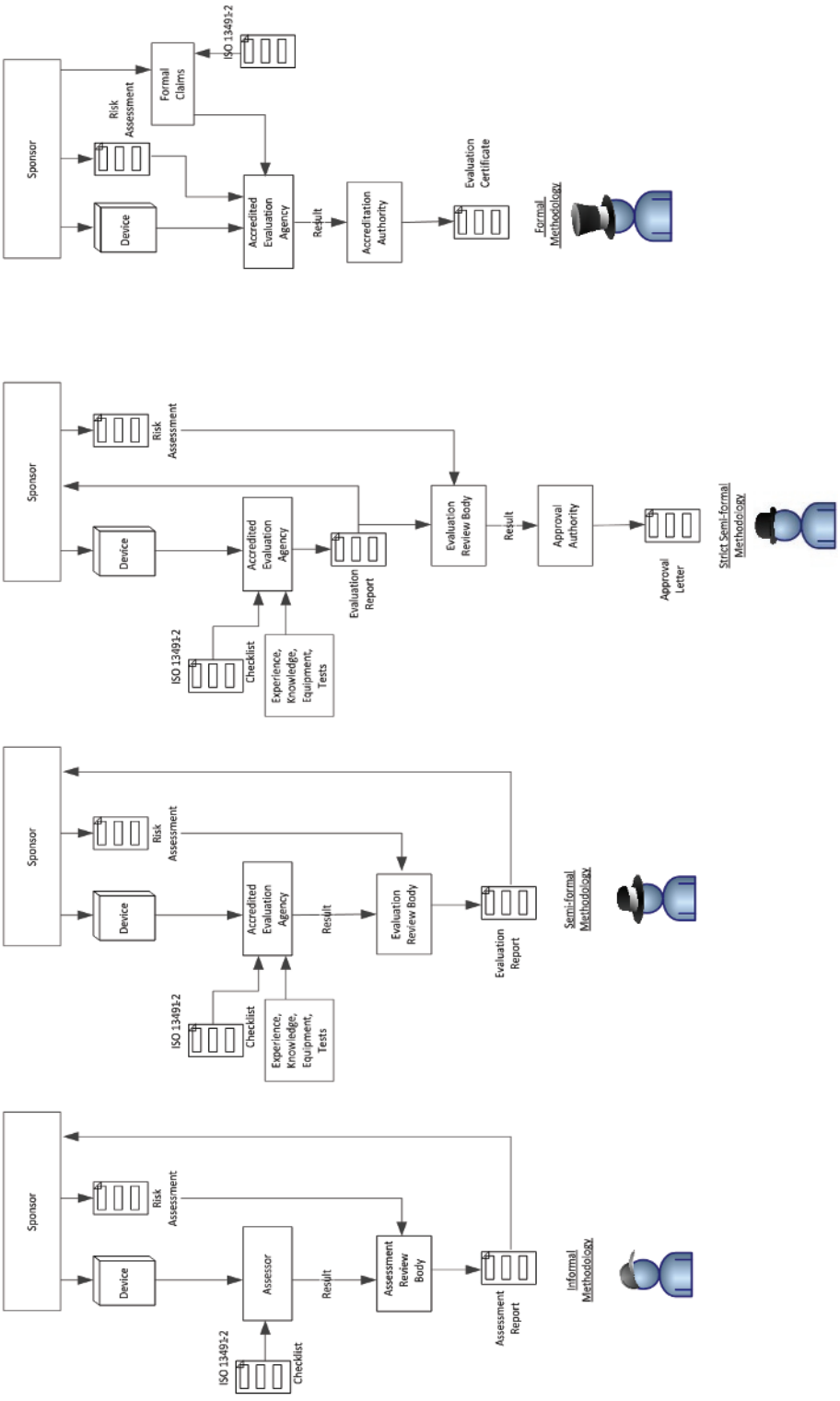

Figure A.1 — Evaluation methods

NOTE For all terms, reference the definitions in Clause 3.

A.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.

A.3 Informal evaluation method

A.3.1 General

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

Before commencement of any evaluation, there should 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.

A.3.2 Sponsor

The manufacturer may be the sponsor or the sponsor can be an independent body. In both cases, the sponsor should 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.

A.3.3 Assessor

The assessor should be independent of the sponsor.

The assessor should 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.

A.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 should 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.

A.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 should 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,

— 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.

A.3.6 Assessment results

The assessment results should 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.).

A.3.7 Assessment report

The assessment report should 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.

A.4 Semi-formal evaluation method

A.4.1 General

An evaluation undertaken by an evaluation agency will, in many ways, be the same as that undertaken by an accredited evaluation agency. 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 should use the assessment checklists found in ISO 13491-2 as a base upon which the device is evaluated.

Two methods of working are recommended as described below.

— The evaluation review body and/or sponsor produce(s) a set of requirements upon which the SCD is 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 is 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 actions of the participating parties.

A.4.2 Sponsor

The role and responsibilities of the sponsor are the same as those described in A.3.2.

A.4.3 Evaluation agency

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

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

— use its experience and knowledge to help to determine tests;

— use its specialized equipment to perform those tests;

— submit results to the evaluation review body via the sponsor;

— document the success or failure of all tests.

The evaluation agency should complete the evaluation checklists as described in A.3.5.

A.4.4 Evaluation review body

The evaluation review body can be the sponsor itself, or the evaluation review body can be independent. In both cases, the evaluation review body assumes the following role and responsibilities:

— receive the submitted results from the evaluation agency;

— if a test results in failure, determine whether the test case is relevant;

— return the results to the evaluation agency for further clarification or testing, if necessary;

— determine the security level of the intended environment;

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

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

The original risk assessment should be considered as part of the input for the evaluation review. In cases where the informal and semi-formal methods are employed in parallel, the evaluation review body would receive the results from both evaluations.

A.4.5 Evaluation results

The evaluation agency results should include the following:

— the list of pertinent documentation used for the evaluation;

— a completed list of all successful or failed tests;

— the name of the sponsor;

— the name of the evaluation agency;

— the date of the evaluation;

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

Additionally, the evaluation agency may provide the following:

— a detailed explanation of all tests;

— a detailed explanation of the failed tests.

A.4.6 Evaluation report

The evaluation report should include the following:

— part of the information received in the evaluation results (some of the information may be confidential);

— the list of pertinent documentation used for the review;

— the justification or rejection of all failed tests from the evaluation results;

— the name of the evaluation review body;

— the date of the review;

— a final recommendation of the acceptance or rejection of the device 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.

A.5 Semi-formal with approval evaluation method

A.5.1 General

Where the sponsor has a need for conformance, e.g. to a network or payment system which requires certification of the results, the SCD evaluation will be undertaken by an accredited evaluation authority and should be evaluated using the evaluation checklists from which a set of claims may be produced.

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 accredited evaluation agencies to conform to a common set of input requirements, the accredited evaluation agency should use the assessment checklists found in ISO 13491-2 as a base upon which the device is to be evaluated. Individual networks or payment system interfaces may have requirements additional to those presented in the checklist.

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

A.5.2 Sponsor

The role and responsibilities of the sponsor are the same as those described in A.3.2.

A.5.3 Accredited evaluation agency

The accredited evaluation agency should be independent of and external to the manufacturer and the sponsor and the accreditation authority and the approval authority and should assume the following role and responsibilities:

— use the appropriate evaluation check-lists to help to determine tests;

— use its experience and knowledge to help to determine tests;

— use its specialized equipment to perform those tests;

— submit results to the evaluation review body via the sponsor;

— document the success or failure of all tests.

The evaluation agency should complete the evaluation checklists as described in A.3.5.

A.5.4 Evaluation review body

The evaluation review body should be independent of the sponsor, although it need not be independent of the accreditation authority. In either case, the evaluation review body should assume the following role and responsibilities:

— receive the submitted results from the accredited evaluation agency;

— if a test results in failure, determine whether the test case is relevant;

— return the results to the accredited evaluation agency for further clarification or testing, if necessary;

— determine the security level of the intended environment;

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

— produce the evaluation report and submit it to the accreditation authority.

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

A.5.5 Evaluation results

The evaluation results should include the following:

— the list of pertinent documentation used for the evaluation;

— a completed list of all successful or failed tests;

— the name of the sponsor;

— the name of the evaluation agency;

— the date of the evaluation;

— identification of the device (e.g. manufacturers name, model number, etc.).

Additionally, the accredited evaluation agency may provide the following:

— a detailed explanation of all tests;

— a detailed explanation of the failed tests.

A.5.6 Evaluation report

The evaluation report should include the following:

— part of the information received in the evaluation results (some of the information may be confidential);

— the list of pertinent documentation used for the review;

— the justification or rejection of all failed tests from the evaluation results;

— the name of the evaluation review body;

— the date of the review;

— a final recommendation of the acceptance or rejection of the device 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.

A.5.7 Approval authority

The approval authority should be independent of the manufacturer, the sponsor, and the accredited evaluation agency, although it need not be independent of the evaluation review body. In either case, the approval authority should assume the following role and responsibilities:

— receive the submitted evaluation report from the evaluation review body;

— if the report results in failure, inform the sponsor of the failure and the reasons for that failure;

— if the report results in success, inform the sponsor of the successful certification;

— publish;

— identification of the device (e.g. manufacturers name, model number, etc.);

— the date of certification;

— the period of certification.

A.5.8 Accreditation authority

The accreditation authority should be independent of all other entities in the process, except it need not be independent of the approval authority. The accreditation authority should assume the following role and responsibilities:

— review evidence that the abilities and resources of the evaluation agency conform to the standards required by the approval authority;

— provide the evaluation agency with accreditation.

A.6 Formal evaluation method

Any formal method is beyond the scope of this part of ISO 13491 (for an example of a formal methodology, see ISO/IEC 15408). However, the checklists contained in ISO 13491-2 may be included as an input in the formulation of the formal claims.

Specific industry sectors may produce combined evaluation review bodies and accreditation authorities. These processes could be based on a network or payment system producing their own evaluation criteria. The techniques specified in this part of ISO 13491 are intended to be used in both environments.

Bibliography

[1] ISO 9564-1, *Financial services — Personal Identification Number (PIN) management and security — Part 1: Basic principles and requirements for PINs in card-based systems*

[2] ISO 9564-2, *Financial services — Personal Identification Number (PIN) management and security — Part 2: Approved algorithms for PIN encipherment*

[3] ISO 13491-2:2005, *Financial Services — Secure cryptographic devices (retail) — Part 2: Security compliance checklists for devices used in financial transactions*

[4] ISO 16609, *Financial services — Requirements for message authentication using symmetric techniques*

[5] ISO/IEC 15408 (all parts), *Information technology — Security techniques — Evaluation criteria for IT security*

[6] ISO/IEC 17025, *General requirements for the competence of testing and calibration laboratories*

[7] ISO/IEC 19790, *Information technology — Security techniques — Security requirements for cryptographic modules*

ICS 35.240.40
Price based on 33 pages

This page deliberately left blank

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email bsmusales@bsigroup.com.

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Copyright

Useful Contacts:

Customer Services
Tel: +44 845 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 845 086 9001
Email: subscriptions@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

bsi.