INTERNATIONAL STANDARD

ISO 13491-2

First edition
2000-11-01

Banking — Secure cryptographic devices (retail) —

Part 2: Security compliance checklists for devices used in magnetic stripe card systems

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

Partie 2: Listes de contrôle de conformité de sécurité pour les dispositifs utilisés dans les systèmes de cartes à bande magnétique

Reference number
ISO 13491-2:2000(E)

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

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.ch
Web www.iso.ch

Printed in Switzerland

Contents

Foreword

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

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 3.

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

Attention is drawn to the possibility that some of the elements of this part of ISO 13491 may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

International Standard ISO 13491-2 was prepared by Technical Committee ISO/TC 68, *Banking, securities and other financial services*, Subcommittee SC 6, *Retail financial services*.

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

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

— *Part 2: Security compliance checklists for devices used in magnetic stripe card systems*

Annexes A to G form a normative part of this part of ISO 13491. Annex H is for information only.

Introduction

This International Standard specifies 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 banking environment.

The security of retail electronic banking is largely dependent upon the security of these cryptographic devices. Security requirements are 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 device can be replaced with unauthorized inputs. While certain cryptographic devices (e.g. host security modules) reside in relatively high security processing centres, a large proportion of cryptographic devices used in retail banking (e.g. PIN pads, ATMs, etc.) now reside in non-secure environments. Therefore when PINs, MACs, cryptographic keys and other sensitive data are processed in these devices, there is a risk that the devices may be tampered with or otherwise compromised to disclose or modify such data.

It must be ensured that the risk of financial loss is reduced through the appropriate use of cryptographic devices that have proper physical and logical security characteristics and are properly managed. To ensure that SCDs have the proper physical and logical security, they require evaluation.

This part of ISO 13491 provides the security compliance checklists for evaluating SCDs used in magnetic stripe systems in accordance with ISO 13491-1.

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

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

Banking — Secure cryptographic devices (retail) —

Part 2:
Security compliance checklists for devices used in magnetic stripe card systems

1 Scope

This part of ISO 13491 specifies checklists to be used to evaluate secure cryptographic devices (SCDs) incorporating cryptographic processes, as specified in ISO 9564, ISO 9807 and ISO 11568, in a magnetic stripe card environment. It does not specify checklists for SCDs used in an integrated circuit card (ICC) environment.

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

In the checklists given in annexes A to H, the term “not feasible” is intended to convey the notion that although a particular attack might be technically possible it would not be economically prudent, since carrying out the attack would cost more than any benefits obtained from a successful attack. In addition to attacks for purely economic gain, malicious attacks directed toward loss of reputation need to be considered.

2 Normative references

The following normative documents contain provisions which, through reference in this text, constitute provisions of this part of ISO 13491. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. However, parties to agreements based on this part of ISO 13491 are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. For undated references, the latest edition of the normative document referred to applies. Members of ISO and IEC maintain registers of currently valid International Standards.

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

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

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

ISO 9564-2, *Banking — Personal Identification Number management and security — Part 2: Approved algorithm(s) for PIN encipherment*.

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

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

ISO 13491-1, *Banking — Secure cryptographic devices (retail) — Part 1: Concepts, requirements and evaluation methods.*

3 Terms and definitions

For the purposes of this part of ISO 13491, the terms and definitions given in ISO 13491-1 and ISO 8908 and the following apply.

3.1
accredited evaluation authority
body accredited in accordance with a set of rules (e.g. EN 45000 or ISO Guide 25) and accepted by the accreditation authority for the purpose of evaluation

3.2
attack
attempt by an adversary on the device to obtain or modify sensitive information or a service he/she is not authorized to obtain or modify

3.3
audit report
output of the audit review body based on the results from an auditor

3.4
audit review body
group with responsibility for reviewing and making judgements on the results from the auditor

3.5
auditor
one who has the appropriate skills to check, assess, review and evaluate compliance with an informal evaluation on behalf of the sponsor or audit review body

3.6
device security
security of the SCD related to its characteristics only, without reference to a specific operational environment

3.7
evaluation agency
organization trusted by the design, manufacturing and sponsoring authorities which evaluates the SCD (using specialist skills and tools) in accordance with ISO 13491-2

3.8
evaluation report
output of the evaluation review body based on the results from an evaluation agency or auditor

3.9
evaluation review body
group with responsibility for reviewing, and making judgements on, the results of the evaluation agency

3.10
formal claims
statements about the characteristics and functions of a secure cryptographic device

3.11
logical security
ability of a device to withstand attacks through its functional interface

3.12
operational environment
environment in which the SCD is operated, i.e. the application system of which it is part, the location where it is placed, the persons operating and using it, the entities communicating with it

3.13
physical security
ability of a device to withstand attacks against its physical construction

3.14
secure cryptographic device
SCD
physically and logically protected hardware device that provides a set of secure cryptographic services

3.15
secure operator interface
interface which allows the protective mechanisms of the device to be disabled by using a data entry mechanism and which can only be accessed when the device is in a sensitive state

3.16
security compliance checklist
list of auditable claims, organized by device type, as specified in ISO 13491-2

3.17
sensitive data
sensitive information
data which must be protected against unauthorized disclosure, alteration or destruction, especially plaintext PINs and cryptographic keys, and which includes design characteristics, status information, etc.

3.18
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

3.19
software
programs and/or data that will be used within the SCD or downloaded for use by the SCD

3.20
sponsor
sponsoring authority
individual, company or organization that requires the SCD to undergo evaluation

3.21
tamper-evident characteristic
characteristic that provides evidence that an attack has been attempted

3.22
tamper-resistant characteristic
characteristic that provides passive physical protection against an attack

3.23
tamper-responsive characteristic
characteristic that provides an active response to the detection of an attack preventing its success

4 Use of security compliance checklists

4.1 General

These checklists shall be used by the evaluation sponsor that wishes to assess the acceptability of cryptographic equipment upon which the security of the system depends. It is the responsibility of any sponsor that adopts some or all of these checklists to:

a) approve evaluating agencies for use by suppliers to or participants in the system; and

b) set up an audit review body to review the completed audit checklists.

Annexes A to H give checklists defining the minimum evaluation to be performed to assess the acceptability of cryptographic equipment. Additional tests may be performed to reflect the state-of-the-art at the time of the evaluation.

The evaluation may be either “informal” or “semi-formal”, as specified in ISO 13491-1, depending upon the nature of the evaluating agencies approved by the sponsor. Should the sponsor decide on a “formal” evaluation, these audit checklists shall not be used as presented here, but shall rather be used as input to assist in the preparation of the “formal claims” that such an evaluation requires.

NOTE These formal claims themselves are outside of the scope of this part of ISO 13491.

A cryptographic device achieves security both through its inherent characteristics and the characteristics of the environment in which the device is located. When completing these audit check lists, the environment in which the device is located must be considered. For example, a device intended for use in a public location could require greater inherent security than the equivalent device operating in a controlled environment. So that an evaluating agency need not investigate the specific environment where an evaluated device may reside, this International Standard provides a suggested categorization of environments in annex H. Thus an evaluating agency may be asked to evaluate a given device for operation in a specific environment. Then such a device can be deployed in a given facility only if this facility itself has been audited to ensure that it provides the assured environment. However these audit check lists may be used with categorizations of the environment other than those suggested in annex H.

The three evaluation methods specified in ISO 13491-1 are described in 4.2, 4.3 and 4.4.

4.2 Informal evaluation

As part of an informal evaluation, an independent auditor shall complete the appropriate checklist(s) for the device being evaluated.

4.3 Semi-formal evaluation

In the semi-formal method, the manufacturer or sponsor shall submit a device to an evaluation agency for testing against the appropriate checklist(s).

4.4 Formal evaluation

In the formal method, the manufacturer or sponsor shall submit a device to an accredited evaluation authority for testing against the formal claims where the appropriate checklist(s) were used as input

5 Summary

The security compliance checklist is used in the evaluation method to determine compliance with the requirements of standards listed in the references of this International Standard where the estimated risk is seen as low. It is recommended for use whenever the security compliance statements are facts that can be verified without the need for specialized knowledge or skills. In general, compliance with functional requirements can be performed by means of security compliance checklists.

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 an international organization.

Annex A
(normative)

Physical, logical and device management characteristics common to all secure cryptographic devices

A.1 General

This annex is intended for use with all evaluations and shall be completed prior to any device specific security compliance checklists.

The following statements in this security compliance checklist are required to be specified by the auditor as “true (T)”, “false (F)” or “not applicable (N/A)”. A “false” indication does not necessarily indicate unacceptable practice, but shall be explained in writing. Those statements which are indicated as “N/A” shall also be explained in writing.

A.2 Device characteristics

A.2.1 Physical security characteristics

A.2.1.1 General

All devices shall meet the criteria given in A.2.1.2 for general security characteristics and in A.2.1.3 for tamper-evident characteristics. Many devices shall additionally meet either the criteria given in A.2.1.4 for tamper-resistant characteristics or the criteria given in A.2.1.5 for tamper-responsive characteristics. However some devices need meet only the criteria for general security characteristics and tamper-evident characteristics. Such devices meet the following requirements:

a) the device retains no key that has ever been used to encipher any secret data, nor does it retain any information from which such a key could feasibly be determined, even with knowledge of any data that has ever been available in plaintext form;

b) the device is managed in such a way that there is a high probability of noting and reporting on a timely basis either the extended absence of the device from its authorized location, or any obvious damage to the device;

c) means exist at all facilities capable of direct cryptographic communication with the device to not process any enciphered data received from the device after it has been reported absent or damaged.

A.2.1.2 General security characteristics

An evaluation agency has evaluated the device bearing in mind susceptibility to physical and logical attack techniques known at the time of the evaluation, such as (but not limited to) the following:

— chemical attacks (solvents);

— scanning attacks (scanning electron microscope);

— mechanical attacks (drilling, cutting, probing, etc.);

— thermal attacks (high and low temperature extremes);

— radiation attacks (X-rays);

— information leakage through covert channels (power supply, timing, etc.);

— failure attacks;

and has concluded that:

No.	Security compliance statement	True	False	N/A
A1	It is not feasible to determine a PIN, a key, or other secret information by monitoring (e.g. the electro-magnetic emissions from the device, with or without the cooperation of the device operator), when the device is operating in its intended environment.			
A2	Any ventilation and other openings into the module are positioned and protected so that it is not feasible to use such an opening to probe any component of the module such that plaintext PINs, access codes, or cryptographic keys might be disclosed; or to disable any of the protection mechanisms of the device.			
A3	All sensitive data and cryptographic keys, including residues, are stored in the security module.			
A4	All transfer mechanisms within the device are implemented in such a way that it is not feasible to monitor the device to obtain unauthorized disclosure of any such information.			
A5	Any access entry to the device's internal circuitry is locked in the closed position when the device is operative, by means of one or more pick-resistant locks.			

A.2.1.3 Tamper-evident characteristics

The evaluating agency has concluded that:

No.	Security compliance statement	True	False	N/A
A6	The device is designed and constructed so that it is not feasible to penetrate the device in order to: — make any additions, substitutions, or modifications (e.g. the installation of a bug) to the hardware or software of the device; or — determine or modify any sensitive information (e.g. PINs, access codes, and cryptographic keys) and then subsequently re-install the device, without requiring specialized skills and equipment not generally available, and: 1) without damaging the device so severely that the damage would have a high probability of detection, or 2) requiring the device be absent from its intended location for a sufficiently long time that its absence, or reappearance, would have a high probability of being detected.			

A.2.1.4 Tamper-resistant characteristics

The evaluating agency has concluded that:

No.	Security compliance statement	True	False	N/A
A7	The device is protected against penetration by employing physical protection to such a degree that penetration is not feasible.			
A8	Even after having gained unlimited, undisturbed access to the device, discovery of secret information in the target device is not feasible.			

A.2.1.5 Tamper-responsive characteristics

The evaluating agency has concluded that:

No.	Security compliance statement	True	False	N/A
A9	The device is protected against penetration by including features that detect any feasible attempts to tamper with the device and cause immediate erasure of all cryptographic keys and sensitive data when such an attempt is detected.			
A10	Removal of the case or the opening, whether authorized or unauthorized, of any access entry to the device's internal components causes the automatic and immediate erasure of the cryptographic keys stored within the device.			
A11	There is a defined method for ensuring that secret data or any cryptographic key that has been used to encrypt secret data, is erased from the unit when permanently removing the unit from operation. There is also a defined method for ensuring, when permanently removing the unit from operation, that any cryptographic key contained in the unit that might be usable in the future is either erased from the unit or is invalidated at all facilities with which the unit is capable of performing cryptographically protected communications.			
A12	Any tamper detection/key erasure mechanism functions even in the absence of applied power.			
A13	If the device has no mechanism for secure detection of movement, then defeating the tamper detection mechanisms, or discovery of secret information in the target device is not feasible, even when removed from its operating environment. Compromise of the device shall require equipment and skill sets that are not readily available. NOTE As a possible example, discovery of such information requires a significant time, such as **one month** of preparation — perhaps including analysis of other devices — and at least **one week** of effort to compromise the device after having gained unlimited, undisturbed access to the target device.			
A14	If the device has a mechanism for secure detection of movement, then defeating the tamper-detection mechanisms, or discovery of secret information in the target device is not feasible. Compromise of the device shall require skill sets that are not readily available; and equipment that is not readily available at the device site nor can be feasibly transported to the device site. NOTE As a possible example, discovery of such information requires a significant time, such as **one month** of preparation — perhaps including analysis of other devices — and at least **twelve hours** of unlimited, undisturbed access to the target device.			

A.2.2 Logical security characteristics

The evaluating agency has concluded that:

No.	Security compliance statement	True	False	N/A
A15	The device includes self-test capabilities, capable of manual or automatic initiation, to ensure that its basic functions are operating properly.			
A16	The device only performs its designed functions.			
A17	The device is designed in such a way that it cannot be put into operational service until the device initialization process has been completed. This will include all necessary keys and other relevant material needed to be loaded into it.			
A18	It is not feasible to determine a key or other secret information by the use of diagnostic or special test modes.			
A19	The cryptographic algorithms, modes of operations, and lengths of cryptographic keys used by the device comply with ISO 11568.			
A20	The device key management complies with ISO 11568, using each key for only one cryptographic purpose (although a variant of a key may be used for a different purpose).			
A21	The functionality implemented within the device is such that there is no feasible way in which plaintext secret information, e.g. PINs or cryptographic keys, or secret information enciphered under other than the legitimate key, can be obtained from the device, except in an authorized manner.			
A22	If the device is composed of several components, it is not possible to move a cryptographic key within the device from a component of higher security to a component providing lower security.			
A23	The loading of keys shall be performed when: — the device is in a sensitive state; or — the action of loading a key puts the device into a state that activates all the tamper protection mechanisms within the device.			
A24	The following operator functions that may influence the security of a device are only permitted when the device is in a sensitive device state, i.e. under dual or multiple control: — disabling or enabling of device functions; — change of passwords or data that enable the device to enter the sensitive state.			
A25	The secure operator interface is so designed that entry of more than one password (or some equivalent mechanism for dual or multiple control) is required in order to enter this sensitive state.			
A26	The secure operator interface is so designed that it is highly unlikely that the device can inadvertently be left in the sensitive state.			
A27	If sensitive state is established with limits on the number of function calls (where appropriate), and a time limit after the first of these limits is reached, the device returns to normal state.			
A28	Where passwords or other plaintext data are used to control transition to a sensitive state, then these are protected in the same manner as other secret or sensitive information.			
A29	If cryptographic keys are lost for any reason, e.g. long-term absence of applied power, the device will revert to a logical state of not being initialized (and therefore not operational).			
A30	The only function calls and sensitive operator functions that exist in the device are functions approved by the sponsor, or the system in which the device is to operate.			
A31	Keys are never translated from encipherment under one variant to encipherment under another variant of the same key.			

A.3 Device management

A.3.1 General consideration

For each life cycle stage, the entity responsible for completing the audit checklist for that stage has provided assurance, acceptable to the audit review body, that:

No.	Security compliance statement	True	False	N/A
A32	For audit and control purposes, the identity of the device (e.g. its serial number) can be determined, either by external tamper-evident marking or labelling, or by a command that causes the device to return its identity via the interface or via the display.			
A33	When the device is in a life cycle stage such that it contains cryptographic keys, the identity of these keys can be easily determined from the identity of the device (so that the key(s) can be invalidated if the device is reported lost or stolen).			
A34	Any physical keys used to unlock or operate the device are carefully controlled, and available only to authorized persons.			
A35	If a device contains a secret cryptographic key and there is an attack on a device, or a device is stolen, then procedures are in place to notify the party responsible for the security of the device immediately after detection.			
A36	If a device does not yet contain a secret cryptographic key and there is an attack on a device, or a device is stolen, then procedures are in place to prevent the substitution of the attacked or stolen device for a legitimate device that does not yet contain a secret cryptographic key.			
A37	If no sensitive state exists in the device, the loading of plaintext keys shall be performed under dual control.			

A.3.2 Device protection by manufacturer

The device manufacturer or an independent auditor has provided assurance, acceptable to the audit review body, that:

No.	Security compliance statement	True	False	N/A
A38	The hardware and software design of the device has been carefully evaluated to ensure that the functional capabilities provided with the device are all legitimate, documented functions, and that no unauthorized function (e.g. a “Trojan Horse”) resides in the device software.			
A39	The device, including software, is produced and stored in a controlled environment under the control of qualified personnel to prevent unauthorized modifications to the physical or functional characteristics of the device.			

A.3.3 Device protection between manufacturer and pre-use

The device manufacturer and those responsible for the transport, repair, and storage of the device prior to initial key loading or to the repeat of initial key loading, or else an independent auditor, have provided assurance, acceptable to the audit review body, that:

No.	Security compliance statement	True	False	N/A
A40	The transfer mechanisms by which plaintext keys, key components or passwords are entered into the device are protected and/or inspected so as to prevent any type of monitoring that could result in the unauthorized disclosure of any component or password.			
A41	Subsequent to manufacturing and prior to shipment, the device is stored in a protected area or sealed within tamper-evident packaging to prevent undetected unauthorized access to it.			
A42	The device is shipped in tamper-evident packaging, and inspected to detect unauthorized access to it; or — before a device is loaded with cryptographic keys, it is closely inspected by qualified staff to ensure that it has not been subject to any physical or functional modification; or — the device shall be delivered with secret information that is erased if tampering is detected to enable the user to ascertain that the device is genuine and not compromised. NOTE One example of such information is the private key of an asymmetric key pair, with the public key of the device signed by a private key known only to the supplier.			
A43	The device is loaded with initial key(s) in a controlled manner only when there is reasonable assurance that the device has not been subject to unauthorized physical or functional modification.			

A.3.4 Device protection during pre-use and prior to installation

Those responsible for device storage and transport subsequent to initial key loading, or else an independent auditor, have provided assurance, acceptable to the audit-review body, that:

No.	Security compliance statement	True	False	N/A
A44	Any uninstalled device is controlled so as to prevent or detect unauthorized access to it, and records are kept and audited so as to detect and report thefts or losses.			

A.3.5 Device protection subsequent to installation

The acquirer or an independent auditor have provided assurance, acceptable to the audit review body, that controls and procedures are in place to ensure that:

No.	Security compliance statement	True	False	N/A
A45	If for any reason a device ceases to hold valid keys: — the device is removed from service as soon as possible, and — transactions from the device are rejected, and — the device is not loaded with new keys, by a repeat of the initial-key-loading process, until it has been carefully inspected and tested by at least two knowledgeable and qualified individuals who have determined that the device has not been subject to any physical or functional modification.			
A46	If a device is lost or stolen and then recovered, or if unauthorized modification of the device is suspected for any reason, all cryptographic keys contained in the unit are erased, and new keys are not loaded (by a repeat of the key-initialization process) until the unit has been inspected and tested as indicated in A.2.3 above.			
A47	Manual and/or automated auditing and control procedures have been implemented to detect the unauthorized reinstallation of a previously used device, or of a device containing the key(s) of a previously used device. Such instances are investigated, and if potentially fraudulent activity is suspected, the device is removed from service as soon as possible. When each transaction identifies the key(s) used in the transaction, host software can be used to automatically detect: 1) the removal of a device from service, and 2) the subsequent installation of a device containing the key(s) of a device previously removed from service.			
A48	When the device is being serviced or installed, procedures are in place to ensure that the device cannot be compromised by the staff performing these functions.			
A49	When the secure operator interface is to be used, the data entry device and cables connected to the device are carefully inspected to ensure that no unauthorized hardware has been inserted.			

A.3.6 Device protection after removal from service

Those responsible for device removal, or else an independent auditor, have provided assurance, acceptable to the audit review body, that:

No.	Security compliance statement	True	False	N/A
A50	If the device is to be reinstalled, then it is controlled so as to prevent unauthorized access to it, and is audited so as to detect and report its theft or loss.			
A51	If the device is being permanently removed from service, then any key contained within the device that has been used for any cryptographic purpose is erased from the device.			
A52	If the device case is intended to provide tamper-evident characteristics and the device is being permanently removed from service, then the case is destroyed. The storage of the case is controlled and audited until its destruction.			

Annex B
(normative)

Devices with PIN entry functionality

B.1 General

The procedure for evaluating PIN entry devices is as follows:

— complete the checklists given in annex A;

— complete the checklists given in this annex.

The following statements in this security compliance checklist are required to be specified by the auditor as “true (T)”, “false (F)” or “not applicable (N/A)”. A “false” indication does not necessarily indicate unacceptable practice, but shall be explained in writing. Those statements which are indicated as “N/A” shall also be explained in writing.

B.2 Device characteristics

B.2.1 Physical security characteristics

The evaluating agency has concluded that:

No.	Security compliance statement	True	False	N/A
B1	The path from the keypad to the cryptographic processing unit is physically protected, such that there is no feasible method of ascertaining the data passed between the two without triggering the erasure of the device’s cryptographic keys; or, the requirements of B17 are met.			
B2	If the PIN entry device can be used to enter data that will not be enciphered, then the path from the cryptographic processing unit to the display is physically protected; or, the requirements of B18 are met.			
B3	If the PIN entry device is to be used in a multi-acquirer environment, then the path from the card reader to the cryptographic processing unit is physically protected, such that there is no feasible method of altering the data passed between the two without triggering the erasure of the cryptographic keys; or, the requirements of B19 are met.			
B4	If PIN entry is accompanied by an audible tone, the tone for each entered PIN digit is indistinguishable from the tone for any other entered PIN digit.			
B5	If the PIN entry device has a display, this display does not disclose any entered PIN digit but may display a string of non-significant symbols, such as asterisks, to denote the number of PIN digits entered.			
B6	The PIN entry device is equipped with a privacy shield, or is designed so that the cardholder can shield it with his/her body to protect against observation of the PIN during PIN entry.			
B7	Any residues of PINs, or cryptographic keys used during a transaction are either stored in a tamper-resistant or tamper-responsive module, or are overwritten immediately after the completion of the transaction. NOTE Plaintext PINs are always overwritten immediately after being enciphered.			

B.2.2 Logical security characteristics

The PIN entry device manufacturer or an independent evaluating agency has provided assurance, acceptable to the audit review body, that:

No.	Security compliance statement	True	False	N/A
B8	The PIN is enciphered within the PIN entry device using a PIN block format and an encipherment algorithm specified in ISO 9564. NOTE A PIN verification device needs to comply with this requirement only where PINs are to be transferred from the device.			
B9	If the PIN entry device offers functionality for downloading of software, then any such software downloaded is rejected by the device (the device's cryptographic keys may also be automatically erased) unless the device has successfully authenticated the download.			
B10	If the PIN entry device is designed to cater for more than one acquirer, then any downloaded changes to the table controlling the choice of the acquirer key set are accepted by the device only if it has successfully authenticated the download.			
B11	The device has characteristics that prevent or significantly deter exhaustive PIN determination (e.g. use a unique-key-per-transaction technique to prevent the attack or limit the number of permitted PIN entries per minute to deter the attack).			
B12	Where the keypad is used for PIN entry as well as other data, the display is under the control of the device such that an "enter PIN" message cannot be displayed when data will be output in the clear.			
B13	The PIN entry device only accepts PINs that are between four and 12 digits in length.			
B14	The mapping of numeric values of the entered PIN to the internal coding is in accordance with ISO 9564-1.			
B15	The PIN entry device uses different keys for different acquirers, and there is no feasible way in which any acquirer's personnel can ascertain or modify another acquirer's key.			
B16	The PIN entry device uses different keys for different acquirers, and the means to select the key to be used for a given transaction are controlled (e.g. by an internal table look-up) so that there is no feasible way to deliberately or accidentally select the key of another acquirer.			
B17	The path from the keypad to the cryptographic processing unit is logically protected (e.g. enciphered and/or authenticated), or the requirements of B1 are met.			
B18	If the PIN entry device can be used to enter data that will not be enciphered, then the path from the cryptographic processing unit to the display is logically protected, or the requirements of B2 are met.			
B19	If the PIN entry device is to be used in a multi-acquirer environment, then the path from the card reader to the cryptographic processing unit is logically protected, or the requirements of B3 are met.			

B.3 Device management

B.3.1 PIN entry device protection during initial key loading

Those responsible for initial key loading, or an independent auditor, have provided assurance, acceptable to the sponsor, that:

No.	Security compliance statement	True	False	N/A
B20	A repaired PIN entry device is not reloaded with the original key (except by chance).			
B21	Automated techniques are used, or manual procedures are in place and are followed to ensure each PIN entry device is given at least one statistically unique key unknown to any person and never previously given (except by chance) to any other PIN entry device.			

B.3.2 PIN entry device protection after installation

The acquirer or an independent auditor has provided assurance, acceptable to the audit review body, that controls and procedures are in place to ensure that:

No.	Security compliance statement	True	False	N/A
B22	The PIN entry device is placed where PIN entry cannot be viewed by surveillance cameras nor readily observed by bystanders.			
B23	Location of the device is such that its absence or unauthorized access (attack) would be detected within 24 h.			

Annex C
(normative)

Devices with PIN management functionality

C.1 General

PIN management functions include:

— PIN issuance;

— PIN verification;

— PIN translation.

The procedure for evaluating devices containing PIN management functionality is as follows:

— complete the checklists given in annex A;

— complete the checklists given in this annex;

NOTE PIN entry is discussed in annex B.

— submit both sets of results to the audit review body.

The following statements in this security compliance checklist are required to be specified by the auditor as “true (T)”, “false (F)” or “not applicable (N/A)”. A “false” indication does not necessarily indicate unacceptable practice, but shall be explained in writing. Those statements which are indicated as “N/A” shall also be explained in writing.

C.2 Device characteristics

C.2.1 Physical security characteristics

The PIN management device manufacturer or an independent evaluating agency has provided assurance, acceptable to the audit review body, that:

No.	Security compliance statement	True	False	N/A
C1	Unauthorized removal of the device from its operational location is deterred by one or more of the following mechanisms: — the device weighs more than 40 kg or else locks into a structure weighing more than 40 kg; or — the device is locked to its mounting surface using a pick-resistant lock, such that the device cannot feasibly be removed from this surface without unlocking the lock; or — the device includes mechanisms such that the removal of the device from its operational location will cause the automatic erasure of the cryptographic keys contained within the device; or — removal of the device would be of no benefit because its tamper-resistance or tamper-responsive characteristics ensure that the extraction of cryptographic keys or other secret data is not feasible.			

C.2.2 Logical security characteristics

The PIN management device manufacturer or an independent evaluating agency has provided assurance, acceptable to the audit review body, that:

No.	Security compliance statement	True	False	N/A
C2	Any residues of PINs, or cryptographic keys used during a transaction are either stored in a tamper-resistant or tamper-responsive module, or are overwritten as soon as they are no longer needed. NOTE Plaintext PINs are always overwritten immediately after being enciphered.			
C3	When a PIN is derived from an account number or other data, the keys used in this process are not used for any other purpose.			
C4	When a PIN verification reference is calculated, the keys used in this process are not used for any other purpose.			
C5	Where the intended operating environment does not provide protection against exhaustive PIN searches, internal monitoring of statistics is made so that only some given proportion of incorrect PIN verifications are permitted. Multiple function calls containing the same correct PIN/PAN pair are not counted when computing the proportion of incorrect PIN verification calls.			
C6	It is not feasible to determine any PIN verification keys given knowledge of PIN reference values, the corresponding PINs, and other non-secret relevant data.			
C7	PIN translation functionality shall comply with ISO 9564-1. The purpose of PIN translation is to change the PIN block from encipherment under one key (most often the key used by the PIN entry device) to encipherment under a key used to send the PIN block through the network to the PIN issuer. PIN translation shall protect the PINs from disclosure.			
C8	All keys under which input PIN blocks are enciphered cannot be used for any other purpose, in particular there is no way of using this key to encipher a known plaintext quantity.			
C9	There is no translation of input PIN block formats to another PIN block format that is not described in ISO 9564-1.			
C10	To deter misuse of the PIN translation capability for exhaustive PIN determination, either: — the operational environment prevents this misuse, or — all PIN translations are between formats that encrypt the PIN as a function of a significant portion of the account number, and the PIN translation capability requires that the account number digits in the input PIN block match the corresponding account number digits in the output PIN block.			
C11	When a plaintext PIN is generated for the purpose of PIN issuance, the device can only be enabled for this function under dual control.			
C12	The functionality to output plaintext PINs for issuance requires supervision by at least two designated people. Once generated, the PIN shall only be visible to the PIN owner.			

C.3 Device management

The requirements for device management are the same as those presented in annex E.

Annex D
(normative)

Devices with message authentication functionality

D.1 General

Message authentication devices calculate a message authentication code (MAC) for the purpose of providing data integrity and verification of an alleged origin.

There are three types of input:

— cryptographic keys;

— messages to be authenticated (followed by a MAC for MAC verification devices), and

— operator input (e.g. choice of message authentication key).

For MAC generation devices, there are two types of output: key verification code of the cryptographic key that has been input or used and the computed message authentication code (MAC).

For MAC verification devices, there are two types of output: key verification code of the cryptographic key that has been input or used, and a yes/no response, indicating whether the MAC of the message, using the indicated key, was correct.

Some devices use different MAC keys for verification and generation, i.e. unidirectional keys.

The initialization vector (IV), if used, is not considered secret data, nor is the data protected by the MAC.

The procedure for evaluating message authentication devices is as follows:

— complete the checklists given in annex A;

— complete the checklist given in this annex;

— submit both sets of results to the audit review body.

The following statements in this security compliance checklist are required to be specified by the auditor as “true (T)”, “false (F)” or “not applicable (N/A)”. A “false” indication does not necessarily indicate unacceptable practice, but shall be explained in writing. Those statements which are indicated as “N/A” shall also be explained in writing.

D.2 Logical security device characteristics

The message authentication device manufacturer or an independent evaluating agency has provided assurance, acceptable to the audit review body, that:

No.	Security compliance statement	True	False	N/A
D1	If the message authentication device can be manually activated and can contain different MAC keys, then the identity of the key used is displayed by the device.			
D2	The length of the MAC being generated or verified is in accordance with ISO 9807.			
D3	The MAC is generated using an approved algorithm in accordance with ISO 9807, as agreed to by the sender and receiver.			
D4	The device only outputs a confirmation or denial of a MAC provided for verification, never the plaintext computed MAC.			
D5	If the device uses two keys for MAC generation or verification, the technique utilized is in accordance with ISO 9807.			
D6	If the message authentication device is designed to use unidirectional MAC keys, then a MAC key is only used for one type of MAC function, i.e. verify the MAC of received text or generate and output a MAC for a text being transmitted.			

Annex E
(normative)

Devices with key generation functionality

E.1 General

Key generation functions include:

— random or pseudo-random number generator for the purpose of generating a symmetric key or a symmetric key component;

— random or pseudo-random prime number generator for the purpose of generating the private key and public key of an asymmetric key pair;

— function(s) to calculate a secret value for public key distribution systems.

There are two types of device that can be used to generate and inject keys. One type of device requires "compromise prevention" because a compromise of the device could disclose keys previously generated or injected by the device prior to the compromise. The other type of device requires only "compromise detection" because the device retains no information that, if disclosed, could disclose any key that had been injected into a cryptographic device prior to the compromise.

The procedure for evaluating key generation devices is as follows:

— complete the checklists given in annex A;

— complete the checklists given in this annex;

— submit both sets of results to the audit review body.

The following statements in this security compliance checklist are required to be specified by the auditor as "true (T)", "false (F)" or "not applicable (N/A)". A "false" indication does not necessarily indicate unacceptable practice, but shall be explained in writing. Those statements which are indicated as "N/A" shall also be explained in writing.

E.2 Device characteristics

E.2.1 Physical security characteristics

The key generation device manufacturer or an independent evaluating agency has provided assurance, acceptable to the audit review body, that:

No.	Security compliance statement	True	False	N/A
E1	Unauthorized removal of the device from its operational location is deterred by one or more of the following mechanisms: — the device weighs more than 40 kg or else locks into a structure weighing more than 40 kg; or — the device is locked to its mounting surface using a pick-resistant lock, such that the device cannot feasibly be removed from this surface without unlocking the lock; or — the device includes mechanisms such that the removal of the device from its operational location will cause the automatic erasure of the cryptographic keys contained within the device; or — removal of the device would be of no benefit because its tamper-resistance or tamper-responsive characteristics ensure that the extraction of cryptographic keys or other secret data is not feasible.			

E.2.2 Logical security characteristics

The key generation device manufacturer or an independent evaluating agency has provided assurance, acceptable to the audit review body, that:

No.	Security compliance statement	True	False	N/A
E2	The device's key management functions are designed so that no disclosure of any key is possible without collusion between trusted individuals. Specifically: — the device's highest-level keys are manually loaded as at least two components under dual control; — any function used to input or output key components does not operate until at least two different passwords have been entered.			
E3	The device decomposes an actual key into key components in such a way that no "active" bit of the key could be determined without the knowledge of all components. (For example, the components are exclusive-or'ed together to form the key.)			
E4	Key generation methods comply with ISO 11568.			
E5	Each call to obtain a generated key yields a different, statistically-unique key (except by chance).			
E6	If the device is capable of generating asymmetric key pairs, then the private key will not be visible in comprehensible form at any time during the generation process.			
E7	If the device is capable of generating asymmetric key pairs which are not used by the device, then the key pair and all related secret seed elements are deleted immediately after the transfer process.			
E8	The device will not output any key except when at least two authorized people are present. Such dual control is enforced by means such as the following: — at least two passwords shall be correctly entered, within a period of no more than five minutes, before the device will output a key; — at least two different, physical keys (marked "not to be commercially reproduced") shall be concurrently inserted in the unit before it will output a key.			
E9	The following operator functions (if available) require the use of special "sensitive" states: — manual input of control data (e.g. key verification code) to enable export, import, or use of a key; — permitting movement of the device without activating a key erasure mechanism; — change of passwords or data that enable the device to enter the sensitive state.			
E10	Any proprietary functions are either: — totally equivalent to a series of standard and approved functions; or — limited to use only keys that, by virtue of key separation, cannot be used with keys, or modified keys, of non-proprietary functions.			

E.3 Device management

The key generation device manufacturer or the organisation in which the device is to be used or an independent evaluating agency has provided assurance, acceptable to the audit review body, that:

No.	Security compliance statement	True	False	N/A
E11	Unauthorized removal of the device from its operational location is deterred by one or more of the following mechanisms: — the device weighs more than 40 kg or else locks into a structure weighing more than 40 kg; or — the device is locked to its mounting surface using a pick-resistant lock, such that the device cannot feasibly be removed from this surface without unlocking the lock; or — the device includes mechanisms such that the removal of the device from its operational location will cause the automatic erasure of the cryptographic keys contained within the device; or — the device depends on the difficulty of extracting keys from its tamper-resistant or tamper-responsive module.			
E12	Unauthorized use of the device is prevented or detected by means such as the following: — the device is at all times either locked or sealed in a tamper-evident cabinet or else is under the continuous supervision of at least two authorized people who ensure that any unauthorized use of the device would be detected; — the device has functional or physical characteristics (e.g. passwords or physical high-security keys) that prevent use of the device except under the dual control of at least two authorized people, and when in a state in which it is useable, the device is under the continuous supervision of at least two such people who ensure that any unauthorized use of the device would be detected.			
E13	When the device is in or ready for active use, unauthorized access to its internal circuitry is prevented by means such as the following: — the facility where the device operates has sufficient supervision and controls to prevent any such unauthorized access to the device that could successfully disclose any cryptographic key or any other secret data; — the device is under the continuous supervision of at least two trusted people who are qualified to detect and able to observe any attempted unauthorized access, and able also to prevent such access before it is successful.			
E14	Controls are in place to prevent the removal of the security device from the facility where it has been in service without first ensuring that no information remains within the device that could disclose any cryptographic key that ever existed within the device.			
E15	When the device is not in active use, any unauthorized access to its internal circuitry is prevented by means such as the following: — the facility where the device operates has sufficient supervision and controls to prevent any unauthorized access to the device; — the device is stored in a safe that cannot feasibly be penetrated, and each incident of opening or closing the safe is controlled and recorded by at least two authorized people.			
E16	When the device is not in active use, undetected access to its internal circuitry is prevented by means such as the following: — the facility where the device operates has sufficient supervision and controls to detect any such unauthorized access to the device before the device is subsequently put into active use; — the device is stored in a tamper-evident cabinet for which each incident of opening and closing is controlled and recorded by at least two authorized people.			
E17	When the device is in or ready for active use, undetected access to its internal circuitry is prevented by means such as the following: — the facility where the device operates has sufficient supervision and controls to detect any such unauthorized access to the device before the device is subsequently used for any cryptographic function; — the device is under the continuous supervision of at least two trusted people who are qualified to detect and able to observe any such access.			
E18	Controls are in place to detect the unauthorized reinstallation of a device previously removed from a facility.			

Annex F
(normative)

Devices with key transfer and loading functionality

F.1 General

Key transfer and loading functions include:

— export of a key from one secure cryptographic device to another SCD in plaintext, component, or enciphered form;

— export of a key component from a secure cryptographic device into a tamper-evident package (e.g. blind mailer);

— import of key components into a secure cryptographic device from a tamper-evident package;

— temporary storage of the key in plaintext, component, or enciphered form within a secure cryptographic device during transfer.

There are two types of device that can be used to transport keys in this manner. One type transfers only a single component (from a set of at least two components) of the key. The other type transfers the entire key in plaintext form. This audit considers both types of device.

The procedures for evaluating key transfer and loading devices is as follows:

— complete the checklists given in annex A;

— complete the checklists given in this annex;

— submit both sets of results to the audit review body.

The following statements in this security compliance checklist are required to be specified by the auditor as “true (T)”, “false (F)” or “not applicable (N/A)”. A “false” indication does not necessarily indicate unacceptable practice, but shall be explained in writing. Those statements which are indicated as “N/A” shall also be explained in writing.

F.2 Device characteristics

F.2.1 Physical security characteristics

The key transfer and loading device manufacturer or an independent evaluating agency has provided assurance, acceptable to the audit review body, that:

No.	Security compliance statement	True	False	N/A
F1	Unauthorized removal of the device from its operational location will be deterred by one or more of the following mechanisms: — the device includes tampe-responsive mechanisms such that the removal of the device from its operational location will cause the automatic erasure of the cryptographic keys contained within the device; or — the device depends on the difficulty of extracting keys from its tamper-resistant module.			

F.2.2 Logical security characteristics

The key transfer and loading device manufacturer or an independent evaluating agency has provided assurance, acceptable to the audit review body, that:

No.	Security compliance statement	True	False	N/A
F2	Enciphered private keys are protected against key substitution and modification.			
F3	The device's key management functions are designed so that no disclosure of any key is possible without collusion between trusted individuals. Specifically: — the device's highest-level keys are manually loaded as at least two components; — any function used to input or output key components, except for components of the device's highest-level keys, does not operate until authorized under dual control.			
F4	The device will not output any key except when at least two authorized people are present. Such dual control is enforced by means such as the following: — at least two passwords shall be correctly entered, within a period of no more than five minutes, before the device will output a key; — at least two different, non-reproducible physical keys shall be concurrently inserted in the unit before it will output a key.			
F5	If the device has a sensitive state, then the following operator functions require use of this state: — production of control data (e.g. key verification code) to enable export, import, or use of a key; — permitting movement of the device without activating a key erasure mechanism; — change of passwords or data that enable the device to enter the sensitive state.			
F6	The only function calls and sensitive operator functions that exist in the device are functions approved by the sponsor, or the system in which the device is to operate. Any proprietary functions are either: — totally equivalent to a series of standard and approved functions, or — limited to use only keys that, by virtue of key separation, cannot be used with keys, or modified keys, of non-proprietary functions.			
F7	Once the device has been loaded with cryptographic keys, there is no feasible way in which the functional capabilities of the device can be modified without causing the automatic and immediate erasure of the cryptographic keys stored within the device, or causing the modification to be otherwise detected before the device is next used to load a key.			
F8	The device retains no information that could disclose any key that the device has already transferred into another cryptographic device.			

F.3 Device management

The key transfer and loading device manufacturer or the organisation in which the device is to be used or an independent evaluating agency has provided assurance, acceptable to the audit review body, that:

No.	Security compliance statement	True	False	N/A
F9	The transfer mechanisms by which keys, components or passwords are transferred into or out of the device are protected and/or inspected so as to prevent any type of monitoring that could result in the unauthorized disclosure of any keys, components or passwords.			
F10	If the device requires “compromise prevention” then, when the device is not in active use, any unauthorized access to its internal circuitry is prevented by means such as the following: — the facility where the device operates has sufficient supervision and controls to prevent any such unauthorized access to the device; — the device is stored in a safe that cannot feasibly be penetrated, and each incident of opening or closing the safe is controlled and recorded by at least two authorized people.			
F11	If the device requires “compromise prevention” then, when the device is in or ready for active use, unauthorized access to its internal circuitry is prevented by means such as the following: — the facility where the device operates has sufficient supervision and controls to prevent any such unauthorized access to the device; — the device is under the continuous supervision of at least two trusted people who are qualified to detect and able to observe any such attempted access, and able also to prevent such access before it is successful.			
F12	If the device only requires “compromise detection” then, when the device is not in active use, undetected access to its internal circuitry is prevented by means such as the following: — the facility where the device operates has sufficient supervision and controls to detect any such unauthorized access to the device before the device is subsequently put into active use; — the device is stored in a tamper-evident cabinet for which each incident of opening and closing is controlled and recorded by at least two authorized people.			
F13	If the device only requires “compromise detection” then, when the device is in or ready for active use, undetected access to its internal circuitry is prevented by means such as the following: — the facility where the device operates has sufficient supervision and controls to detect any such unauthorized access to the device before the device is subsequently used for any cryptographic function; — the device is under the continuous supervision of at least two trusted people who are qualified to detect and able to observe any such access.			
F14	Controls are in place to detect the unauthorized removal of the device from, and its unauthorized replacement back into, its authorized location.			
F15	The device is loaded with a key component under the direct supervision of a person who is allowed access to this component, and only when there is reasonable assurance that there is no “bug” or other disclosing mechanism on the path that the key component traverses from the key generation device to the transport device itself.			
F16	If the device contains a plaintext key component, the device is either under the continuous supervision of a person who is allowed access to this component (and who is aware of his/her responsibilities to ensure the secrecy of this component), or else is locked or sealed in a security container that cannot feasibly be opened without detection by anyone other than those who are allowed access to the component.			
F17	The device is used to inject a component into a cryptographic device only under the direct supervision of a person who is allowed access to this component, and only when there is reasonable assurance that there is no “bug” or other disclosing mechanism on the path that the key component traverses from the key transport device to the cryptographic device.			