INTERNATIONAL STANDARD

ISO 13491-2

Fourth edition
2017-03

Financial services — Secure cryptographic devices (retail) —

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

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

Partie 2: Listes de contrôle de conformité de sécurité pour les dispositifs utilisés dans les transactions financières

Reference number
ISO 13491-2:2017(E)

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 voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

This document was prepared by ISO/TC 68, *Financial services*, Subcommittee SC 2, *Security*.

This fourth edition cancels and replaces the third edition (ISO 13491-2:2016), of which it constitutes a minor revision with the following changes:

— references made to H.5 have been replaced with ISO 9564-1;

— editorially revised.

A list of all the parts in the ISO 13491 series can be found on the ISO website.

Introduction

This document 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 financial services environment.

The security of retail financial services 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, communication lines can be "tapped", and authorized data or control inputs in a 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 financial services (e.g. PIN entry devices, 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 can be tampered with, or otherwise, compromised to disclose or modify such data.

It is to 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 document provides the security compliance checklists for evaluating SCDs used in financial services systems in accordance with ISO 13491-1. Other evaluation frameworks exist and may be appropriate for formal security evaluations (e.g. ISO/IEC 15408-1, ISO/IEC 15408-2, ISO/IEC 15408-3, and ISO/IEC 19790) and are outside the scope of this document.

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) have 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.

Financial services — Secure cryptographic devices (retail) —

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

1 Scope

This document 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, and ISO 11568-4 in the financial services environment. Integrated circuit (IC) payment cards are subject to the requirements identified in this document up until the time of issue after which they are to be regarded as a "personal" device and outside of the scope of this document.

This document does not address issues arising from the denial of service of an SCD.

In the checklists given in Annex A to Annex 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 viable 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 documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

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

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*

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

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

ISO/IEC 18031, *Information technology — Security techniques — Random bit generation*

3 Terms and definitions

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

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— IEC Electropedia: available at http://www.electropedia.org/

— ISO Online browsing platform: available at http://www.iso.org/obp

3.1
auditor
person 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

3.2
data integrity
property that data has not been altered or destroyed in an unauthorized manner

3.3
dual control
process of utilizing two or more entities (usually persons) operating in concert to protect sensitive functions or information whereby no single entity is able to access or use the materials

Note 1 to entry: A cryptographic key is an example of the type of material to be accessed or utilized.

3.4
evaluation agency
organization trusted by the design, manufacturing, and sponsoring entities which evaluates the SCD (using specialist skills and tools)

Note 1 to entry: Evaluation is in accordance with ISO 13491-1.

3.5
exclusive or
bit-by-bit modulo two addition of binary vectors of equal length

3.6
security compliance checklist
list of auditable claims, organized by device type

Note 1 to entry: Checklist is as specified in this document.

3.7
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

4 Use of security compliance checklists

4.1 General

These checklists shall be used to assess the acceptability of cryptographic equipment upon which the security of the system depends. It is the responsibility of any sponsor, approval authority, or accreditation authority, depending on the evaluation method chosen, that adopts some or all of these checklists to

— approve evaluating agencies for use by suppliers to or participants in the system, and

— set up an audit review body to review the completed audit checklists.

Annex A to Annex H, which provide checklists defining the minimum evaluation to be performed to assess the acceptability of cryptographic equipment, shall be applied. Additional tests may be performed to reflect the state-of-the-art at the time of the evaluation.

The evaluation may be either “informal”, “semi-formal”, or “strict semi-formal” as specified in ISO 13491-1. Should a “formal” evaluation be chosen, 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, as they inherently include other criteria, are themselves outside of the scope of this document.

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 checklists, the environment in which the device is located shall be considered, e.g. a device intended for use in a public location might 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 document 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. Such a device can be deployed in a given facility, only if this facility itself has been audited to ensure that it provides the ensured environment. However, these audit checklists may be used with categorizations of the environment other than those suggested in Annex H.

The four evaluation methods specified in ISO 13491-1 are described in 4.2, 4.3, 4.4, and 4.5.

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 sponsor, who may be the manufacturer, shall submit a device to an evaluation agency for testing against the appropriate checklist(s).

4.4 Strict semi-formal evaluation

In the strict semi-formal method, the sponsor, who may be the manufacturer, shall submit a device to an evaluation agency for testing against the appropriate checklist(s) determined by an approval authority.

4.5 Formal evaluation

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

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 that 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 the criteria given in A.2.1.5 for tamper responsive characteristics and in A.2.1.3 for tamper-evident characteristics. Other devices shall additionally meet the criteria given in A.2.1.4 for tamper-resistant characteristics.

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 (side) channels (power supply, timing, etc.);

— failure attacks;

and has concluded the following as in Table A.1.

Table A.1 — General security characteristics

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).			
A2	Any ventilation and other openings in 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 point into 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 or similar security mechanisms.			
A6	The design of the device is such that a duplicate device cannot be constructed from components which are available through retail commercial channels.			
A7	If the device generates random numbers or pseudo random numbers, then the generation of those numbers conforms to ISO/IEC 18031.			
A8	If the device generates random numbers or pseudo random numbers, it is not feasible to influence the output of those numbers, e.g. by varying environmental conditions of the device such as resetting or reinitializing the device, or manipulating the power supply/electro-magnetic injection.			

A.2.1.3 Tamper-evident characteristics

The evaluating agency has concluded the following as in Table A.2.

Table A.2 — Tamper-evident characteristics

No.	Security compliance statement	True	False	N/A
A9	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, return the device without requiring specialized skills and equipment not generally available and: a) without damaging the device so severely that the damage would have a high probability of detection; or b) requiring that 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 the following as in Table A.3.

Table A.3 — Tamper-resistant characteristics

No.	Security compliance statement	True	False	N/A
A10	The device is protected against penetration by employing physical protection to such a degree that penetration is not feasible.			
A11	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 the following as in Table A.4.

Table A.4 — Tamper-responsive characteristics

No.	Security compliance statement	True	False	N/A
A12	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.			
A13	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.			
A14	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 service (decommissioning). There is also a defined method for ensuring, when permanently decommissioned, 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.			

Table A.4 *(continued)*

No.	Security compliance statement	True	False	N/A
A15	Any tamper detection/key erasure mechanisms function even in the absence of applied power.			
A16	If the device has no mechanism for detection of removal from its operational environment, then defeating the tamper detection mechanisms or discovery of secret information in the target device is not feasible, even when removed from its operational environment. Compromise of the device requires equipment and skill sets that are not readily available. As a possible example, discovery of such information requires a significant time, such as one month of preparation, 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.			
A17	If the device has a mechanism for detection of removal from its operational environment, 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. As a possible example, discovery of such information requires a significant time, such as one month of preparation, including analysis of other devices and at least 12 h of unlimited, undisturbed access to the target device.			

A.2.2 Logical security characteristics

The evaluating agency has concluded the following as in Table A.5.

Table A.5 — Logical security characteristics

No.	Security compliance statement	True	False	N/A
A18	The device includes self-test capabilities capable of manual or automatic initiation to ensure that its basic functions are operating properly.			
A19	The device only performs its designed functions.			
A20	It is not feasible to determine a key or other secret information by the use of diagnostic or special test modes.			
A21	The cryptographic algorithms, modes of operation, and lengths of cryptographic keys used by the device conform to ISO 11568-1, ISO 11568-2, and ISO 11568-4.			
A22	The device key management conforms to ISO 11568-1, ISO 11568-2, and ISO 11568-4 using each key for only one cryptographic purpose (although a variant of a key may be used for a different purpose).			
A23	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 (e.g. PIN mailers).			
A24	If the device is composed of several components, it is not possible to move a secret cryptographic key within the device from a component of higher security to a component providing lower security.			

Table A.5 *(continued)*

No.	Security compliance statement	True	False	N/A
A25	The loading of keys is performed when: — the device is in a sensitive state; or — the action of loading a key puts the device into a mode that activates all the tamper protection mechanisms within the device.			
A26	The following operator functions that may influence the security of a device are only permitted when the device is in a sensitive state, i.e. under dual or multiple control: — disabling or enabling of device functions; or — change of passwords or data that enable the device to enter the sensitive state.			
A27	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.			
A28	The secure operator interface is so designed that it is highly unlikely that the device can inadvertently be left in the sensitive state.			
A29	If sensitive state is established with multiple limits (e.g. on the number of function calls and a time limit), the device returns to normal state when the first of these limits is reached.			
A30	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.			
A31	If cryptographic keys are lost for any reason (e.g. long-term absence of applied power), the device will enter a non-operational state.			
A32	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.			
A33	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 for the following as in Table A.6.

Table A.6 — General consideration

No.	Security compliance statement	True	False	N/A
A34	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.			
A35	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].			
A36	Any physical keys used to unlock or operate the device are carefully controlled and available only to authorized persons.			
A37	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.			
A38	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.			
A39	If no sensitive state exists in the device, the loading of plaintext keys is 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, for the following as in Table A.7

Table A.7 — Device protection by manufacturer

No.	Security compliance statement	True	False	N/A
A40	The hardware and software design of the device has been 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.			
A41	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 post-manufacturing phases

The device manufacturer and those responsible for the transport and storage of the device prior to initial financial key loading, or else an independent auditor, have provided assurance for the following as in Table A.8.

Table A.8 — Device protection between manufacturer and post-manufacturing phases

No.	Security compliance statement	True	False	N/A
A42	Subsequent to manufacturing and prior to shipment, the device is stored in a protected area or sealed within tamper-evident packaging to detect unauthorized access to it.			
A43	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 is 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 manufacturer.			

A.3.4 Device protection during initial financial key loading and prior to pre use

Those responsible for device storage and transport during initial key loading, or else an independent auditor, have provided assurance, acceptable to the audit review body, for the following as in Table A.9.

Table A.9 — Device protection during initial financial key loading and prior to pre use

No.	Security compliance statement	True	False	N/A
A44	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 key, component, or password.			
A45	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.3.5 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, for the following as in Table A.10.

Table A.10 — Device protection during pre-use and prior to installation

No.	Security compliance statement	True	False	N/A
A46	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 theft or loss.			

A.3.6 Device protection subsequent to installation

The acquirer or an independent auditor has provided assurance, acceptable to the audit review body, which controls and procedures are in place to ensure the following as in Table A.11.

Table A.11 — Device protection subsequent to installation

No.	Security compliance statement	True	False	N/A
A47	If, for any reason, a device ceases to hold valid keys, — the device is removed from service as soon as possible, — transactions from the device are rejected, and — the device is not loaded with new keys 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.			
A48	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 until the unit has been inspected and tested as indicated in A.3.3.			
A49	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 a) the removal of a device from service, and b) the subsequent installation of a device containing the key(s) of a device previously removed from service.			
A50	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.			
A51	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.			
A52	If the device relies on tamper evidence, procedures are in place to ensure regular inspection for such evidence.			

A.3.7 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, for the following as in Table A.12.

Table A.12 — Device protection after removal from service

No.	Security compliance statement	True	False	N/A
A53	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.			
A54	If the device is being permanently removed from service, then any key contained within the device which has been used for any cryptographic purpose is erased from the device.			
A55	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; and

— 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 that are indicated as “N/A” shall also be explained in writing.

B.2 Device characteristics

B.2.1 Physical security characteristics

B.2.1.1 General physical security characteristics

The evaluating agency has concluded the following as in Table B.1.

Table B.1 — General physical security characteristics

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 (reference A.2.1.5); or — causing sufficient damage to preclude its continued use (reference A.2.1.3); or meeting the requirements of B27.			
B2	If the PIN entry device can be used to enter data that will not be enciphered, then the path to the display is physically protected or the requirements of B22 are met.			
B3	The path from the magnetic stripe card reader to the cryptographic processing unit is physically protected such that there is no feasible method of accessing and/or altering the data passed between the two without triggering the erasure of the secret or private cryptographic keys or the requirements of B28 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.			

Table B.1 *(continued)*

No.	Security compliance statement	True	False	N/A
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.			
B8	The slot of the IC reader into which the IC card is inserted does not have sufficient space to hold a PIN-disclosing "bug" when a card is inserted, nor can it feasibly be enlarged to provide space for a PIN-disclosing "bug". It is not possible for both an IC card and any other foreign object to reside within the card insertion slot. The opening for the insertion of the IC card is in full view of the cardholder so that any untoward obstructions or suspicious objects at the opening are detectable. NOTE A PIN entry device need not comply with this requirement if the PINs are only transferred to the IC card with logical (cryptographic) protection.			
B9	The IC reader is constructed so that wires running out of the slot of the IC reader to a recorder or a transmitter (an external bug) can be observed by the cardholder. NOTE A PIN entry device need not comply with this requirement if the PINs are only transferred to the IC card with logical (cryptographic) protection.			
B10	The PIN pad and the IC reader are either integrated in a single tamper-evident (as defined in ISO 13491-1) device or exist as two separate tamper-evident devices. NOTE A non-integrated IC reader need not comply with this requirement if the PINs are only transferred to the IC card with logical (cryptographic) protection.			

B.2.1.2 Tamper-responsive characteristics

The evaluating agency has concluded the following as in Table B.2.

Table B.2 — Tamper-responsive characteristics

No.	Security compliance statement	True	False	N/A
B11	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.			
B12	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.			
B13	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 service (decommissioning). There is also a defined method for ensuring, when permanently decommissioned, 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.			
B14	Any tamper detection/key erasure mechanisms function even in the absence of applied power.			
B15	If the device has no mechanism for detection of removal from its operational environment, then defeating the tamper detection mechanisms or discovery of secret information in the target device is not feasible even when removed from its operational environment. Compromise of the device requires 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, 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.			
B16	If the device has a mechanism for detection of removal from its operational environment, 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, including analysis of other devices and at least 12 h of unlimited, undisturbed access to the target device.			
B16A	If the device has a mechanism for detection of removal from its operational environment, then defeating the detection of removal mechanisms 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.			

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, for the following as in Table B.3.

Table B.3 — Logical security characteristics

No.	Security compliance statement	True	False	N/A
B17	PIN protection during transmission within the terminal (at least one should apply). — If the PED and the IC reader are not integrated and the cardholder verification method required by the IC card is an enciphered PIN, then the PIN block is enciphered between the PED and the IC reader using either an authenticated encipherment key of the IC card, or in accordance with ISO 9564-1, the PIN block is submitted to the IC card enciphered using an authenticated encipherment key of the IC card. — If the PED and the IC reader are not integrated and the cardholder verification method is determined to be a plaintext PIN, then the PIN block is enciphered from the PED to the IC reader (the IC reader will then decipher the PIN for transmission in plaintext to the IC card) in accordance with ISO 9564-1. — If the PED and the IC reader are integrated and the cardholder verification method is determined to be an enciphered PIN, then the PIN block is enciphered using an authenticated encipherment key of the IC card. — If the PED and the IC reader are integrated and the cardholder verification method is determined to be a plaintext PIN, then encipherment is not required if the PIN block is transmitted wholly through within a secure cryptographic device meeting the requirements of ISO 13491-1. If the plain text PIN is transmitted to the IC reader through an unprotected environment, then the PIN block is enciphered in accordance with ISO 9564-1.			
B18	PIN encipherment only occurs using a PIN block format and an encipherment algorithm specified in ISO 9564-1.			
B19	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 cryptographically authenticated the downloaded code.			
B20	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 cryptographically authenticated the downloaded data.			
B21	The PED 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 or by use of a PIN block format containing random data).			
B22	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" or an equivalent message cannot be displayed when data will be output in the clear or the requirements of B2 are met.			
B23	The PIN entry device only accepts PINs that are between four and 12 digits in length.			
B24	The mapping of numeric values of the entered PIN to the internal coding is in accordance with ISO 9564-1.			

Table B.3 *(continued)*

No.	Security compliance statement	True	False	N/A
B25	The PIN entry device uses different key slots for different acquirers and there is no feasible way in which any acquirer's personnel can ascertain or modify another acquirer's key.			
B26	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.			
B27	The path from the keypad to the cryptographic processing unit is logically protected (e.g. enciphered) or the requirements of B1 are met.			
B28	The path from the magnetic stripe 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, for the following as in Table B.4.

Table B.4 — PIN entry device protection during initial key loading

No.	Security compliance statement	True	False	N/A
B29	A repaired PIN entry device is not reloaded with the original key (except by chance).			
B30	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 the following as in Table B.5.

Table B.5 — PIN entry device protection after installation

No.	Security compliance statement	True	False	N/A
B31	The PIN entry device is placed where PIN entry cannot be viewed by surveillance cameras nor readily observed by bystanders.			
B32	Location and/or the device management practices of the PIN entry device are such that its absence or an 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; and

— PIN translation.

NOTE 1 PIN entry is addressed in Annex B.

NOTE 2 The requirements of this annex do not apply to POS and ATM devices that perform PIN translation for transmission of PINs to an IC card.

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; and

— 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 that 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, for the following as in Table C.1.

Table C.1 — Physical security characteristics

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 using a pick-resistant lock or similar measure such that the device cannot feasibly be removed from this surface without unlocking the lock; — 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; and — 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 are 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, for the following as in Table C.2.

Table C.2 — Logical security characteristics

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 complies with ISO 9654-1. The process of PIN translation protects 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 chosen plaintext quantity and all keys under which PIN blocks are deciphered cannot be used for any other purpose. In particular, there is no way of using this key to decipher a chosen quantity.			

Table C.2 *(continued)*

No.	Security compliance statement	True	False	N/A
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	The PIN generation device can only be enabled for the purpose of plaintext PIN issuance under dual control.			

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.

The following are the 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 procedure for evaluating message authentication devices is as follows:

— complete the checklists given in Annex A;

— complete the checklist given in this annex; and

— 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 that 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, for the following as in Table D.1.

Table D.1 — Logical security device characteristics

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 16609.			
D3	The MAC is generated using an approved algorithm in accordance with ISO 16609 as agreed to by the sender and receiver.			

Table D.1 *(continued)*

No.	Security compliance statement	True	False	N/A
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 16609.			
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 the following:

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

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

— 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; and

— 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 that 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, for the following as in Table E.1.

Table E.1 — Physical security characteristics

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 using a pick-resistant lock or similar measure, such that the device cannot feasibly be removed from this surface without unlocking the lock; — 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; and — 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 are 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, for the following as in Table E.2.

Table E.2 — Logical security characteristics

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, and/or — 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 required components (e.g. the components are exclusive-or'ed together to form the key, or a secret sharing technique is used).			
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 that are not used by the device, then the key pair and all related secret seed elements are deleted immediately after the transfer process.			

Table E.2 *(continued)*

No.	Security compliance statement	True	False	N/A
E8	The device will not output any plaintext key except under dual control. Such dual control is enforced by means such as the following: — the device requires that at least two passwords be correctly entered within a period of no more than five minutes before the device will output a key; and — the device requires that at least two different, physical keys (marked "not to be commercially reproduced") 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; and — permitting movement of the device without activating a key erasure mechanism.			
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.			
E11	Random numbers and pseudo random numbers conform to ISO/IEC 18031.			

E.3 Device management

The key generation device manufacturer or the organization in which the device is to be used or an independent evaluating agency has provided assurance, acceptable to the audit review body, for the following as in Table E.3.

Table E.3 — Device management

No.	Security compliance statement	True	False	N/A
E12	Unauthorized use of the device is prevented or detected by means such as the following: — the device has functional or physical characteristics (e.g. passwords or physical high-security keys) that prevent use of the device except under dual control 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; and — 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.			
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; and — 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 which 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; and — the device is stored, under dual control, in a safe that cannot feasibly be penetrated, and each incident of opening or closing the safe is recorded under dual control.			

Table E.3 *(continued)*

No.	Security compliance statement	True	False	N/A
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; and — the device is stored under dual control in a tamper-evident cabinet for which each incident of opening and closing is recorded under dual control.			
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; and — 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 the following:

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

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

— import of key components into an SCD from a tamper-evident package; and

— temporary storage of the key in plaintext, component, or enciphered form within an SCD 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 are as follows:

— complete the checklists given in Annex A;

— complete the checklists given in this annex; and

— 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 that 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, for the following as in Table F.1.

Table F.1 — Physical security characteristics

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 tamper-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; and — the device's tamper-resistance or tamper-responsive characteristics ensure that the extraction of cryptographic keys or other secret data are not feasible.			

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, for the following as in Table F.2.

Table F.2 — Logical security characteristics

No.	Security compliance statement	True	False	N/A
F2	Keys are protected against 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, if symmetric, are manually loaded as at least two components; and — any function used to input or output key components does not operate until authorized under dual control.			
F4	The device will not output any key except when under dual control. Such dual control is enforced by means such as the following: — the device requires that at least two passwords be correctly entered within a period of no more than five minutes, before the device will output a key; and — the device requires that at least two different, non-reproducible physical keys be concurrently inserted into the unit before it will output a key.			
F5	The following operator functions require use of the sensitive 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; and — change of passwords or data that enable the device to enter the sensitive state.			

Table F.2 *(continued)*

No.	Security compliance statement	True	False	N/A
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 additional (proprietary) functions are either: — totally equivalent to the series of standard and approved functions; or — limited to use-only keys that, by virtue of key separation, cannot be used with keys, modified keys, or sensitive data 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. NOTE This is not intended to preclude the following uses: — the use of the KLD for loading multiple HSMs with the same master file key (e.g. when the HSMs are used for load sharing with a single key database); and — the use of the KLD to generate unique keys per device, load them into a PED and later transfer the file of keys to an HSM.			

F.3 Device management

The key transfer and loading device manufacturer or the organization in which the device is to be used or an independent evaluating agency has provided assurance, acceptable to the audit review body, for the following as in Table F.3.

Table F.3 — Device management

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; and — the device is stored, under dual control, in a safe that cannot feasibly be penetrated, and each incident of opening or closing the safe is recorded under dual control.			
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; and — 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 under dual control, in a tamper-evident cabinet for which each incident of opening and closing is controlled and recorded under dual control; and — the tamper-evident cabinet, if used, is regularly monitored by at least two trusted people who are qualified to detect and able to observe any unauthorized access.			
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; and — 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.			

Table F.3 *(continued)*

No.	Security compliance statement	True	False	N/A
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.			
F18	The transfer of a key to another secure cryptographic device: — uses a secure communications path; — uses a key transfer device; — uses a secure cryptographic path; or — is carried out in a secure environment.			
F19	No person with knowledge of or access to one of the passwords or physical keys required to output a key from the device has knowledge of or access to any other such password or physical key of this device.			

Table F.3 *(continued)*

No.	Security compliance statement	True	False	N/A
F20	The device is loaded with a plaintext key only under the direct supervision of at least two authorized people, both of whom ensure that there is no "bug" or other disclosing mechanism on the path that the key traverses from the key generation device to the key transport device itself.			
F21	The device is used to inject a plaintext key into a cryptographic device only under the direct supervision of at least two authorized people, both of whom ensure that there is no "bug" or other disclosing mechanism on the path that the key traverses from the key transport device to the cryptographic device.			
F22	Functionality needed to import, export, or transfer cryptographic keys from external sources ensures that the keys are in one or more of the following forms: — enciphered under the proper variant of a symmetric key encipherment key; — enciphered under the asymmetric public key of the recipient; — enciphered with an import key being specifically enabled for a limited time and limited number of function calls; — input under dual or multiple control through the secure operator interface, in components such that full knowledge of all, but one component gives no usable information on any bit of the cryptographic key; and — public keys are entered under dual control or enciphered under the appropriate key or signed as required to ensure authenticity.			

Annex G
(normative)

Devices with digital signature functionality

G.1 General

Digital signature devices generate or verify a digital signature for the purpose of providing data integrity and authenticity. In some cases, under strict control, the digital signature may also provide non-repudiation. For generation, inputs consist of the message and the private cryptographic key. For verification, inputs consist of the message and the public cryptographic key. For either function, the calculation is performed within the confines of a secure cryptographic device (SCD).

The public key used to verify the digital signature is not considered to be secret data, nor are the data being protected by the digital signature. However, the integrity of the public key shall be ensured.

The procedure for evaluating digital signature devices is as follows:

— complete the checklists given in Annex A;

— complete the checklists given in Annex E if the device has key generation functionality;

— complete the checklists given in this annex; and

— submit all 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 that are indicated as “N/A” shall also be explained in writing.

G.2 Device management

G.2.1 General considerations

The security device manufacturer and user, or one or more individuals or organizations in which the device is to be used, have provided assurance, acceptable to the audit review body, that the following requirements are fulfilled as in Table G.1.

Table G.1 — General considerations

No.	Security compliance statement	True	False	N/A
G1	If non-repudiation is claimed then: — the asymmetric private and public key pair is generated within the digital signature device; — the asymmetric private key is not exported outside the original digital signature device for any reason, including backup and archival purposes; and — mechanisms for the control of the use of the private key are provided.			

G.2.2 Device management for digital signature verification

An independent agency, internal or external, has evaluated management of the digital signature device, and has concluded the following as in Table G.2.

Table G.2 — Device management for digital signature verification

No.	Security compliance statement	True	False	N/A
G2	For audit and control purposes, the binding between the public key and the identity of the owner of the private key is readily determined by: — use of public key certificates where the public key certificate was obtained from an authorized certificate authority; — use of public key certificates and appropriate certificate management procedures; or — other equivalent mechanisms to irrefutably determine the identity of the owner of the corresponding private key.			
G3	The device key management functions conform to ISO 11568, specifically preventing the use of the signing key for any other purpose.			

Annex H
(normative)

Categorization of environments

H.1 General

The environments are determined by a risk assessment undertaken by the sponsor in accordance with ISO 13491-1.

H.2 Uncontrolled environments

There are no security requirements for uncontrolled environments.

H.3 Controlled environments

A controlled environment is similar to normal computer rooms where there are access controls, allowing access only to authorized personnel. A controlled environment, however, has more stringent access controls and both its interior and the entrances are under surveillance.

The objective of a controlled environment is to limit the types of attack that can be made on a device (e.g. by making it impossible to use certain kinds of equipment) and the time available for (some kinds of) attack (see Table H.1).

All organizational security procedures are well documented and installed. Periodic reviews of those procedures are performed by an auditor and the audit results submitted to the audit review body.

Table H.1 — Controlled environments

No.	Security compliance statement	True	False	N/A
H4	Access is restricted by physical locks and continually supervised access points to authorized and trusted staff and persons accompanied by authorized and trusted staff.			
H5	Any access by other than authorized and trusted staff is logged, and the log securely kept and periodically audited.			
H6	The devices are either: — at all times in full view of at least two staff members who have been instructed to check the devices for signs of attack or presence of any other persons at the devices; or — in view of a video camera (through a secure video system) being monitored at least once every X/2 min or whenever movement close to the devices is automatically detected by persons who have been specifically tasked with checking the devices for signs of attacks. NOTE The time "X/2 min" is half the time "X min" which is the time estimated to successfully 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 reinstall the device without requiring specialized skills and equipment not generally available and without damaging the device so severely that the damage would have a high probability of detection. Care shall be taken with the installation of the video system to ensure that opportunities for shoulder surfing are not created.			
H7	There are no entry or exit points for people or equipment except for continually supervised access points, e.g. watched by guards who have been instructed not to permit any import or export of equipment without written authorization identifying the equipment signed by an authorized person other than the person moving the equipment.			
H8	It is not feasible to gain unauthorized access to the controlled environment or import or export equipment from under the floor or from above the ceiling.			

H.4 Minimally controlled environments

The requirements given in Table H.2 aim to detect an attack or theft, within a given maximum period of time.

Table H.2 — Minimally controlled environments

No.	Security compliance statement	True	False	N/A
H1	Authorized access is restricted by physical locks or supervised access points to authorized staff and persons accompanied by authorized staff.			
H2	The environment provides facilities for secure fastening of devices with lockable fastening mechanisms if such devices are to be installed.			
H3	The minimally controlled environment remains intact until all keys and other secret data stored in devices within the environment are destroyed or until all such devices are removed from the environment.			

H.5 Secure environments

A secure environment provides an outer shell of protection around an insecure device and should be significantly more secure than a controlled environment. It can be a room designed and built for this specific purpose or it could be a safe or a secure cabinet. Whatever form the secure environment takes, only persons with authorized access to the device shall have access to the secure environment. A secure environment is often located within a controlled environment (see Table H.3).

All organizational security procedures are well documented and installed. Periodic reviews of those procedures are performed by an auditor and the audit results submitted to the audit review body.

Table H.3 — Secure environments

No.	Security compliance statement	True	False	N/A
H9	Access is restricted: — by physical locks and continually supervised access points; — to pairs of authorized and trusted staff; and — to persons accompanied by pairs of authorized and trusted staff. Access points that are not supervised are locked and alarmed, so that any entry or exit causes intervention by guards.			
H10	Any non-authorized person(s) requiring access to the secure environment will be supervised at all times by at least two authorized and trusted staff while in the secure environment.			
H11	All accesses to the secure environment are logged and the log securely kept and periodically audited.			
H12	All possible access points to the secure environment are either: — at all times in full view of at least two authorized and trusted staff members who have been instructed to check the devices for signs of attack; or — in view of a video camera (through a secure video system) coupled with circuitry that automatically raises an alarm whenever movement close to the devices is detected or tamper detection circuitry is activated. Even when no alarm is raised, the camera is monitored at least once every 10 min. The images are watched by persons who have been specifically tasked with checking the secure environment for signs of attack.			

Table H.3 *(continued)*

No.	Security compliance statement	True	False	N/A
H13	There are no entry or exit points for people or equipment except for continually supervised access points watched by guards who have been instructed not to permit any import or export of equipment without written authorization identifying the equipment signed by an authorized person other than the person moving the equipment.			
H14	If the secure environment is implemented as a secured room, then the device(s) in the secure environment are in view of a video camera (through a secure video system) coupled with circuitry that automatically raises an alarm whenever movement close to the devices is detected or tamper detection circuitry is activated. Even when no alarm is raised, the camera is monitored at least once every 10 min. The images are watched by persons who have been specifically tasked with checking the secure environment for signs of attack.			
H15	The secure environment provides, at most, limited opportunity for concealment of activity and for the storage of tools and other equipment.			
H16	A secure environment remains such until all keys and other secret data stored in devices within the environment are destroyed or until all such devices are removed from the environment.			
H17	The secure environment contains either: — both the device and its host and there are controls on the environment which prevent the device from being connected to any unauthorized device and on the host to ensure that exhaustive attacks (on PINs), using legitimate function calls, are not feasible; or — the device alone which contains security mechanisms that protect against exhaustive attacks.			

Bibliography

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

[2] ISO/IEC 15408-1, *Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model*

[3] ISO/IEC 15408-2, *Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional components*

[4] ISO/IEC 15408-3, *Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance components*

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

ICS 35.240.40

Price based on 39 pages