International Standard

ISO 13491-1

Fourth edition
2024-07

Financial services — Secure cryptographic devices (retail) —

Part 1: Concepts and requirements

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

Partie 1: Concepts et exigences

Reference number
ISO 13491-1:2024(en)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

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

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 document 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).

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents. ISO shall not be held responsible for identifying any or all such patent rights.

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

For an explanation of 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 www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 268, *Financial services*, Subcommittee SC 2, *Financial Services, security*.

This fourth edition cancels and replaces the third edition (ISO 13491-1:2016), which has been technically revised.

The main changes are as follows:

— revision for classes of secure cryptographic devices (SCDs);

— updated life cycle guidance.

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

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

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

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

— characteristics that a device has to possess;

— how devices have to be managed;

— characteristics of the operational environments.

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

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

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

Financial services — Secure cryptographic devices (retail) —

Part 1:
Concepts and requirements

1 Scope

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

This document states the security characteristics concerning both the operational characteristics of SCDs and the management of such devices throughout all stages of their life cycle.

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

This document does not address software services that use multi-party computation (MPC) to achieve some security objectives and, relying on these, offer cryptographic services.

NOTE These are sometimes called "soft" or software hardware security modules (HSMs) in common language, which is misleading and does not correspond to the definition of HSM in this document.

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 11568, *Financial services — Key management (retail)*

ISO 13491-2:2023, *Financial services — Secure cryptographic devices (retail) — Part 2: Security compliance checklists for devices used in financial transactions*

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

NIST SP 800-90A, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*

NIST SP 800-90B, *Recommendation for the Entropy Sources Used for Random Bit Generation*

3 Terms and definitions

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

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

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

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

3.1
audit
evaluates compliance with an evaluation on behalf of an evaluation agency

3.2
auditor
person who conducts an *audit* (3.1)

3.3
attack
attempt by an adversary on the device to obtain or modify *sensitive data* (3.20) or a service they are not authorized to obtain or modify

3.4
controller
entity responsible for the secure management of a *secure cryptographic device (SCD)* (3.18)

3.5
derived unique key per transaction
DUKPT
key management method that uses a unique key for each transaction and prevents the disclosure of any past key used by the transaction originating *secure cryptographic device (SCD)* (3.18)

[SOURCE: ISO 11568:2023, 3.35]

3.6
device compromise
successful defeat of the physical or logical protections provided by the *secure cryptographic device (SCD)* (3.18), resulting in the potential disclosure of *sensitive data* (3.20) or unauthorized use of the SCD

3.7
device security
security of the *secure cryptographic device (SCD)* (3.18) related to its characteristics only, without reference to a specific *operational environment* (3.15)

3.8
device management
processes, including procedures, controlling the access to and use of the device

Note 1 to entry: These processes can vary depending on the deployed environment.

3.9
dual control
process of utilizing two or more separate individuals operating in concert to protect *sensitive functions* (3.21) or *sensitive information* (3.20) whereby no single individual is able to use the function or access all the information alone

Note 1 to entry: A cryptographic key is an example of the type of material protected by dual control.

[SOURCE: ISO 11568:2023, 3.39, modified — Note 2 to entry deleted.]

3.10
financial key
cryptographic key used to protect financial transaction data

EXAMPLE Entity's public key used for mutual authentication with the payment terminal, initial derived unique key per transaction (DUKPT) key, terminal master key, personal identification number (PIN) encryption key.

3.11
hardware management device
HMD
non-*secure cryptographic device (SCD)* (3.18), typically a dedicated integrated circuit card (ICC), with security features similar to an SCD but lacking *tamper-response characteristics* (3.25), which provides a set of cryptographic services in support of the management of SCDs

Note 1 to entry: HMDs are subject to additional environment controls (see 5.2) due to their limited security features.

Note 2 to entry: Cryptographic services can include key generation, secure storage of key shares and key components, cryptogram creation and signature generation.

3.12
hardware security module
HSM
secure cryptographic device (SCD) (3.18) that provides a set of secure cryptographic services

Note 1 to entry: Secure cryptographic services can include key generation, cryptogram creation, personal identification number (PIN) translation and certificate signing.

3.13
key loading device
KLD
secure cryptographic device (SCD) (3.18) that loads keys into other SCDs

3.14
logical security
ability of a device to withstand *attacks* (3.3) through its functional interface

3.15
operational environment
environment in which the *secure cryptographic device (SCD)* (3.18) is operated, i.e. the system of which it is part, the location where it is placed, the persons operating and using it and the entities communicating with it

3.16
physical security
ability of a device to withstand *attacks* (3.3) against its physical construction, including exploitation of physical characteristics such as electromagnetic emissions and power fluctuations, the analysis of which can lead to side-channel attacks

3.17
public key infrastructure
PKI
structure of hardware, software, people, processes and policies that employs digital signature technology to facilitate a verifiable association between the public component of an asymmetric public key pair with a specific subscriber that possesses the corresponding private key

Note 1 to entry: The public key may be provided for digital signature verification, authentication of the subject in communication dialogues, and/or for message encryption key exchange or negotiation

[SOURCE: ISO 21188:2018, 3.48]

3.18
secure cryptographic device
SCD
device that provides physically and logically protected cryptographic services and storage, and which can be integrated into a larger system, such as an automated teller machine (ATM) or point-of-sale terminal

EXAMPLE Personal identification number (PIN) entry device (PED), *hardware security module (HSM)* (3.12).

3.19
security scheme
configuration that supports the secure status of the device

3.20
sensitive data
sensitive information
data which need to be protected against unauthorized disclosure, alteration or destruction

EXAMPLE Status information, cryptographic key, personal identification number (PIN).

3.21
sensitive function
function which is accessible when the device is in a *sensitive state* (3.22)

3.22
sensitive state
device condition that provides access to the secure operator interface, such that it can only be entered when the device is under *dual control* (3.9)

3.23
tamper-evident characteristic
characteristic that provides evidence that an *attack* (3.3) has been attempted

3.24
tamper-resistant characteristic
characteristic that provides passive physical protection against an *attack* (3.3)

3.25
tamper-response characteristic
characteristic that provides an active response to the detection of an *attack* (3.3)

4 Abbreviated terms

API	application programming interface
ATM	automated teller machine
DUKPT	derived unique key per transaction
EPP	encrypting PIN pad
HMD	hardware management device
HSM	hardware security module
KLD	key loading device
MAC	message authentication code
MPC	multi-party computation
PED	PIN entry device
PIN	personal identification number
PKI	public key infrastructure
POS	point of sale
SCD	secure cryptographic device
SCR	secure card reader
SCRP	SCR with PIN function

5 Secure cryptographic device concepts

5.1 General

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

a) the integrity and authenticity of sensitive data (e.g. by using a MAC over transaction details);

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

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

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

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

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

— unauthorized use or modification of cryptographic services.

A secure cryptographic device provides a defined set of cryptographic functions, access controls and secure key storage. SCDs are employed to protect against these threats. The requirements of this document pertain to the SCD and not the system in which the SCD might be integrated. However, it is important to analyse the interfaces between the SCD and the remainder of the system to ensure that the SCD will not be compromised.

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

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

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

5.2 Hardware management devices

Some key management activities necessitate the use of non-SCD devices where their form factors have inherent limitations preventing them from meeting some SCD security requirements, especially tamper-responsiveness. These limitations have associated security risks which shall be addressed by restricted usage and additional controls. These devices are hardware management devices (HMDs).

Examples of HMDs include, but are not limited to:

a) smart cards used for component or share transport or storage;

b) smart cards containing public or private key pair(s) used to facilitate management of HSMs;

c) devices used to authorize or enable key management functions.

HMDs shall only be used in cases where the compromise of a single HMD would not compromise keys or secrets not held within that HMD.

An HMD shall be stored in an environment that meets at least the criteria of a minimally controlled environment as identified in ISO 13491-2, with additional controls providing reasonable assurance that any unauthorized access to the device can be detected. Because the device cannot respond to an attack, the additional controls minimize the probability of unauthorized modifications.

NOTE 1 An SCD can be used for the same purposes as an HMD (e.g. key loading to another SCD).

NOTE 2 General-purpose smart cards are usually certified in accordance with the common criteria methodology (see the ISO/IEC 15408 series), which specifies different levels of evaluation assurance level (typically EAL 4+).

5.3 Secure cryptographic device types

5.3.1 General types

SCD types are broadly considered in this document to aid description of the different security considerations for each class of SCD. The types of SCDs considered in the following subclauses are:

a) SCD components (PED, EPP, SCR, SCRP);

b) HSM (single-tenant, multi-tenant, hosted or cloud);

c) KLD;

d) smart cards.

Financial terminals, appliances that include one or more SCD components, are commonly called by the following names, some of which are also known as “payment terminals”:

— ATM;

— point of interaction (POI);

— unattended payment terminal (UPT).

A financial terminal consists of a number of components, which can include PED, printer, communications devices, customer–merchant interface, acquirer application, integrated circuit (IC) card reader and magnetic stripe reader. These components may be configured in various fashions, dependent upon requirements.

Those components of a financial terminal that provide cryptographic services and/or any services involved in requesting, reception and/or processing of the cardholder PIN shall collectively meet the requirements of an SCD. The components which process other data (e.g. the customer primary account number (PAN)) received from the payment instrument should be SCDs.

NOTE They can also be required by local regulations to be SCDs.

While financial terminals commonly include one or more SCD components which are considered in this document, financial terminals are not SCDs under the definition used in this document.

5.3.2 Secure cryptographic device components

The following SCD components, which are commonly used in financial terminals, are considered:

a) PED: A device providing for the secure entry of PINs.

b) EPP: An approved device which is a component of a terminal that provides secure PIN entry and cryptographic services to that terminal.

c) SCR: A device with the primary function of reading cards and the added feature of supporting cryptographic function.

d) SCRP: Both SCR and SCRP are secure card readers which evaluate as SCDs (the “P” indicates that the device can perform PIN management functions such as PIN block formation but neither device has PIN entry capability, nor can they perform as financial terminals).

5.3.3 Hardware security module

5.3.3.1 Overview

An HSM as used in financial systems and as illustrated in its ecosystem context in Figure 1 is a type of SCD that typically:

— safeguards keys and functions using those keys in high-performance backend transaction processing environments;

— provides a set of approved core cryptographic algorithms and key lengths;

— provides a set of cryptographic mechanisms built around those algorithms;

— provides secure random number generation using an approved methodology;

— exposes its security services to administrators and user clients via one or more structured APIs;

— interconnects with clients via an approved secure transport layer discipline for communication over open networks.

An HSM may provide configuration and administration options, such as the following:

— Key and access control hierarchy: A layered, partitioned, cryptographic key and access control hierarchy separating:

  — manufacturer low-level firmware management functions;

  — HSM owner (host) on-site HSM initialization;

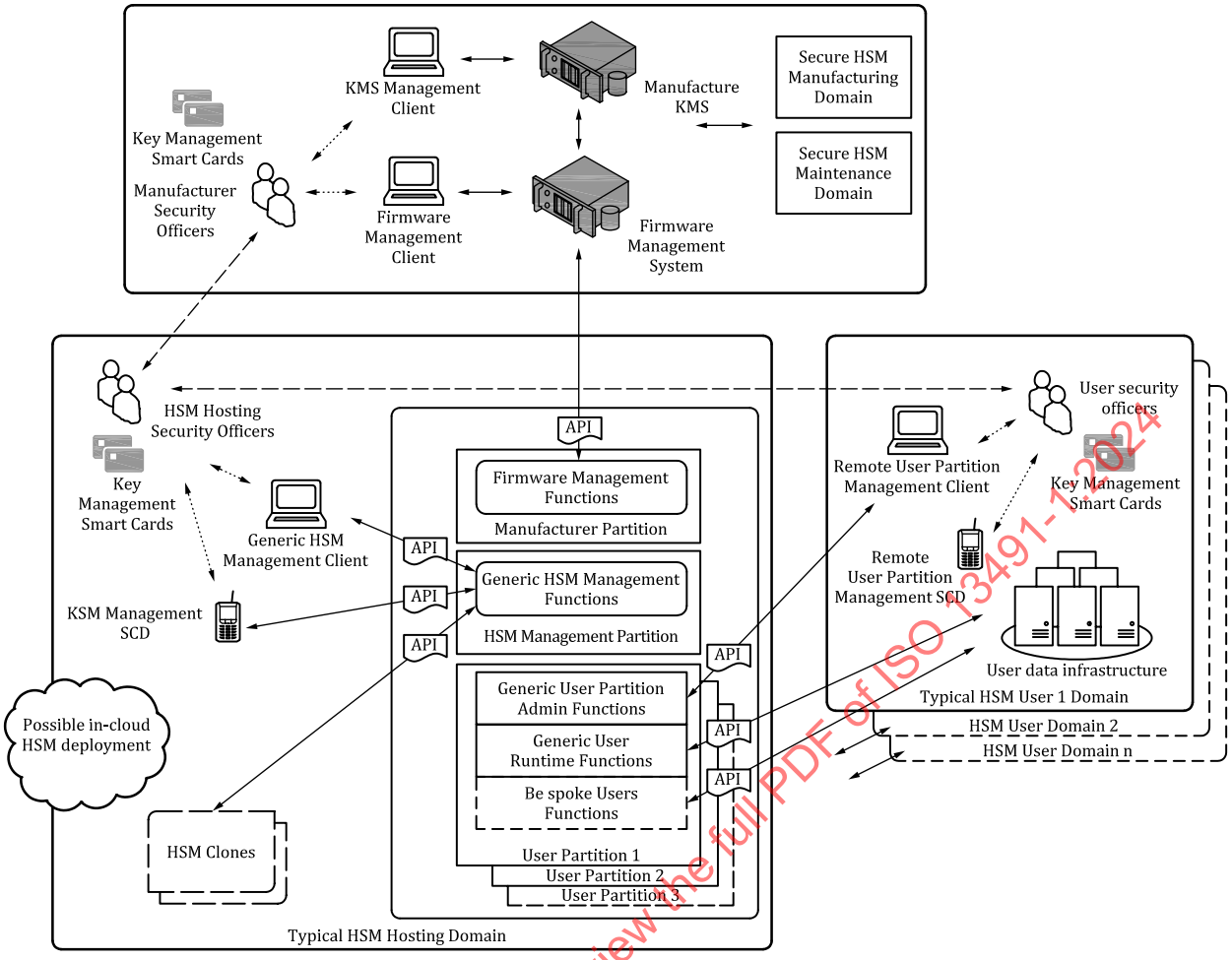
  — user partition management functions and end-user functions.

— Partitioning: Supporting at least one and potentially multiple isolated end-user partitions, such partitions often also providing cryptographically segregated configuration and final end-use functionality to the end-user domain.

— Cloning or backup: Secure cloning capabilities for load sharing or backup purposes via a secure channel established between HSMs that have an authenticated cryptographic relationship, having been preconfigured by the HSM owner with purpose-specific shared keying material.

— SCD or HMD secured administration: This may support or enhance the security of HSM administration through the use of additional locally or remotely secure-channel attached SCD types or through the use of smart cards (HMDs) for log-on authentication, storage or transfer of key parts.

— Secure user function definition: Beyond its generic capabilities, the HSM may incorporate within its tamper-protection boundary supplementary user-partition-specific functionality, developed using a secure programming discipline and inducted into the relevant partition via a higher-layer cryptographic authentication process.



Key

in-band secure channel

out-of-band secure channel

authenticated human interfaces

Figure 1 — HSM ecosystem

5.3.3.2 Security requirements

The following security requirements for HSMs assume and supplement the security requirements for SCDs elsewhere in this document:

— Owner and manufacturer administrative functions shall allow for dual control.

— User administrative functions should provide for dual control.

— Handover from manufacturer to the HSM owner (hosting entity) shall be via functionality which provides for and entails cryptographic decoupling of HSM administration from the manufacturer for cases where the manufacturer has default administrative keys that ship with the device. The manufacturer will then not be able to access or control the keys of the owner of the HSM after the owner's keys have been entered or generated.

— Handover of an end-user partition from the HSM owner (hosting entity) to the end-user shall be via functionality which provides for and entails cryptographic decoupling of HSM partition administration from the HSM owner.

— A partition when assigned shall have no keys from or traces of the previous end-user or HSM owner other than default administrative keys that allow for end-user initialization and shall be replaced during initialization.

— The only owner operations on an end-user partition permitted by the HSM firmware shall be to suspend or terminate the end-user partition.

— When an end-user partition is terminated it shall be with complete erasure of key material, administrative access and configuration settings. If the end-user relationship with the HSM owner continues after the termination (e.g. for cloud-based provisioning or reprovisioning events), the partition's secure log file shall be retained by the partition end-user or potentially under secure log delegation from the end-user to the HSM owner.

— Secure cloning refers to replication of the keys and configuration of a partition or HSM to a receiving partition or HSM. The following applies:

  — Secure cloning shall only be feasible using a clearly defined secure-channel API and transfer process under control of the HSM owner which protects confidentiality and integrity of keys and other secret cryptographic material. The keys used for the security of the secure channel shall be at least as strong as the strongest key material being cloned.

  — Secure cloning shall protect integrity of the configuration of the end-user and should provide confidentiality.

  — Secure cloning shall not include log files; secure cloning shall be logged as a sensitive operation.

  — The end-user of a partition being cloned shall control the cloning, even when the end-user of the partition is not the HSM owner.

— Where a secure firmware update path is provided between manufacturer and HSM, such updates shall only be feasible via a dedicated, segregated and authenticated channel, which should entail owner pre-authorization using a secure owner-operated mechanism such as cryptographic countersigning. The manufacturer should be unable to affect a firmware update without owner participation. Firmware updates should be encrypted.

— To protect against protocol attacks, APIs used for financial application end use should be such that multi-step cryptographic mechanisms or other sensitive operations do not necessitate orchestration by the controlling client. These should progress atomically within the HSM from initiation to conclusion in a single API call. In the absence of atomic API calls, the administrator of the HSM shall ensure that the risk of exploitation is mitigated. Examples include PIN verification or PIN block translation, especially when using EMV or DUKPT derived operational keys.

5.3.3.3 Hardware security module usage

Typical financial industry deployments of HSMs exhibiting these architectural characteristics and adhering to these security requirements include:

— single or multi-partition HSMs, used within the one organization for its end-use applications;

— dedicated single or multi-partition HSMs hosted by one, possibly cloud-based, organization on behalf of a single remote end-user;

— shared-use multi-partition HSMs hosted by one, possibly cloud-based, organization on behalf of multiple end-users.

Typical financial end uses for HSMs include:

— certificate authority operations;

— payment terminal key management;

— payment transaction acquiring, including PIN and PAN processing protection;

— biometric authentication processing;

— payment card issuance;

— mobile financial application key management, provisioning and attestation operations;

— internet banking transport layer and application layer security operations;

— key management of secure cryptographic tokens;

— HSM or payment terminal firmware update signing.

5.3.4 Key loading devices

KLDs are SCDs that support functionality limited to entry, recombination and transfer of financial keys.

KLDs usually have a portable form-factor.

The key loading methods of an SCD shall conform to ISO 11568.

5.4 Attack scenarios

5.4.1 General

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

— penetration;

— monitoring;

— manipulation;

— modification;

— substitution.

These attack scenarios do not form an exhaustive list but are an indication of the main areas of concern and are described in 5.4.2 to 5.4.6.

NOTE The internet enables classes of attackers who share information for the dissemination of exploits to be both wide reaching and rapid, and to market attacks developed against particular SCDs (particularly payment terminals). These attackers expend considerable time, effort and expertise to develop an attack which is packaged and then sold to other attackers.

5.4.2 Penetration

Penetration is an attack which involves the physical perforation and unauthorized opening of the device to ascertain sensitive data contained within the device, such as cryptographic keys.

5.4.3 Monitoring

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

5.4.4 Manipulation

5.4.4.1 Physical manipulation

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

Smart cards and other HMDs are also subject to physical manipulation attacks.

5.4.4.2 Logical (API) manipulation

SCDs and HSMs in particular implement APIs with many services and parameters. Manipulation of the logical interface might involve sending to the device API a sequence of inputs designed to exploit programming flaws, so as to cause the disclosure of sensitive data or to obtain a service in an unauthorized manner, exploiting poorly designed or legacy mechanisms to change types of keys or derive the same key with multiple uses or manipulating the device API to cause execution of arbitrary code.

Smart cards and other HMDs are also subject to logical manipulation attacks.

5.4.5 Modification

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

5.4.6 Substitution

Substitution is the unauthorized replacement of one device with another. The replacement device could be a lookalike "counterfeit" or emulating device having all or some of the correct logical characteristics plus some unauthorized functions, such as a PIN-disclosing bug.

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

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

Substitution can also involve duplication of a cloud-based HSM or HSM partition allowing an attacker access to an instance which is not subject to the user's controls, or manipulation of the instance mapping to allow use by an unauthorized party.

5.5 Defence measures

5.5.1 General

To defend against the attack scenarios discussed in 5.4, the following three factors work together to provide the security required:

— device characteristics;

— device management;

— environment.

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

5.5.2 Device characteristics

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

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

— tamper-evident characteristics;

— tamper-resistant characteristics;

— tamper-response characteristics.

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

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

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

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

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

5.5.3 Device management

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

— key management methods;

— security practices;

— operational procedures.

The primary objective of device management is to ensure that device characteristics are not subject to unauthorized alteration during the life of the device.

5.5.4 Environment

The objective of environment security is to control access to the SCD and its services, thus preventing, or at least detecting, attacks on the SCD. Throughout its life cycle, an SCD will reside in a variety of environments (see Clause 7). These environments may be characterized as ranging from highly controlled to minimally controlled. A highly controlled environment is one that includes constant surveillance by trusted individuals, while a minimally controlled environment might not include any special environmental security supplements. If the security of an SCD is dependent on some function of a controlled environment, it shall be satisfactorily proven that the controlled environment actually provides this function.

6 Requirements for device security characteristics

6.1 General

Device characteristics of an SCD may be categorized as either physical or logical, as follows:

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

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

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

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

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

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

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

6.2 Physical security requirements for secure cryptographic devices

The following physical security requirements apply:

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

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

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

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

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

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

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

It is advisable that an SCD should be so designed and constructed that any additions of external devices which intercept or substitute data input to or output from the SCD for the purpose of masquerade have a high probability of being detected and/or recognized as not being part of a correct device.

6.3 Tamper-evident requirements

6.3.1 General

Tamper evidence provides an indication that an attack has been attempted. If a device claims to rely on tamper-evident characteristics to defend against substitution, penetration or modification attacks, the manner in which the device defends against the attacks shall be as described in 6.3.2 to 6.3.5.

6.3.2 Substitution

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

6.3.3 Penetration

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

6.3.4 Modification

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

6.3.5 Monitoring

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

6.4 Tamper-resistant requirements

6.4.1 General

Tamper resistance provides passive physical protection against attacks. If a device claims to rely on tamper-resistant characteristics to defend against penetration, modification, monitoring or substitution or removal attacks, the manner in which the device defends against the attacks shall be as described in 6.4.2 and 6.4.3 and, optionally, 6.4.4.

6.4.2 Penetration

An SCD shall be protected against successful penetration by being tamper-resistant to such a degree that its passive resistance is sufficient to make penetration impracticable in its intended environment.

6.4.3 Modification

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

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

6.4.4 Monitoring

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

a) when enciphered with the appropriate legitimate key; or

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

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

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

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

6.4.5 Substitution or removal

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

6.5 Tamper-responsive requirements

6.5.1 General

Tamper responsiveness provides active protection against attacks.

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

Where an SCD employs a tamper-response characteristic to defend against penetration or modification attacks, the manner in which the device defends against the attacks shall be as described in 6.5.2 and 6.5.3.

6.5.2 Penetration

Where an SCD employs tamper-response characteristics, it shall be designed and constructed to ensure that penetration of the device results in the immediate and automatic erasure of all keys and other sensitive data and all useful residues of sensitive data.

6.5.3 Modification

Where an SCD employs tamper-response characteristics, it shall be designed to detect any unauthorized modification and shall cause the immediate and automatic erasure of all keys and other sensitive data and all useful residues of such sensitive data.

6.6 Logical security requirements for SCDs and HMDs

6.6.1 General

The requirements in this subclause apply to SCDs. The requirements apply additionally to HMDs except where noted.

6.6.2 Dual control

Where a requirement for dual control is stated in the following subclauses, the requirement for logical security device characteristics is that the device shall provide facilities which support the secure implementation of dual control.

6.6.3 Unique key per device

Private keys or an asymmetric key pair shall be statistically unique to each SCD, except where an SCD is replicated for load sharing or disaster recovery purposes. Secret symmetric keys shall be statistically unique to each cryptographic relationship to which they are assigned.

Secret symmetric keys used to protect storage of domain secrets, i.e. where there is only one cryptographic end point, shall be statistically unique to each SCD, except where duplicate SCDs need to share secure databases or where SCD duplication is required for disaster recovery purposes. Statistical uniqueness shall be achieved either through the use of an approved random number generation process (generated at random using either a deterministic or non-deterministic process or function as specified in ISO/IEC 18031 and verified using NIST SP 800-90A and NIST SP 800-90B) or through the use of an approved key derivation function.

6.6.4 Assurance of genuine device

The provision of a genuine, uncompromised device shall be ensured by the device management. This can be accomplished by delivering the device with secret information installed (i.e. a random, device-specific key) which enables the recipient to ascertain that the device is genuine and not compromised.

6.6.5 Design of functions

The function set of an SCD shall be so designed that no single function, nor any combination of functions, can result in disclosure of sensitive data, except as explicitly allowed by the security scheme used. Legitimate functions shall not be capable of disclosing sensitive data, except as explicitly allowed by the security scheme used. Therefore, protection against exhaustive searches is needed for PINs. When the environment does not provide this protection, it shall be provided by the device characteristics.

The following are examples of how this can be achieved:

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

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

Logical design features shall include the following:

— measures to prevent the successful discovery of keying material through monitoring external connections to the device (e.g. protection against differential power analysis and timing attacks), including the implementations of cryptographic algorithms that are robust by design against side-channel attacks;

NOTE This can be achieved generally either through the use of a cryptographically strong mechanism such as HKDF from RFC 5869, for the key schedule of block ciphers, or the use of a stream cipher that itself relies on similar (i.e. cryptographic hash-based) mechanisms.

— measures to prevent the successful discovery of sensitive data, unless provided by the environment;

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

6.6.6 Use of cryptographic keys

An SCD shall enforce a key separation scheme such that no key can be used for any purpose other than its intended purpose (see ISO 11568).

The key generation methods of an SCD shall conform to ISO 11568.

An SCD shall implement only the key management schemes that conform to the principles outlined in ISO 11568.

6.6.7 Sensitive device states

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

If passwords or other plaintext data are used to control transition to a sensitive state, then the input of such passwords shall be protected from monitoring, and those passwords should follow best practices in terms of length and complexity (e.g. use of non-alphabetic characters).

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

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

6.6.8 Multiple cryptographic relationships

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

6.6.9 Secure device software authentication

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

7 Requirements for device management

7.1 General

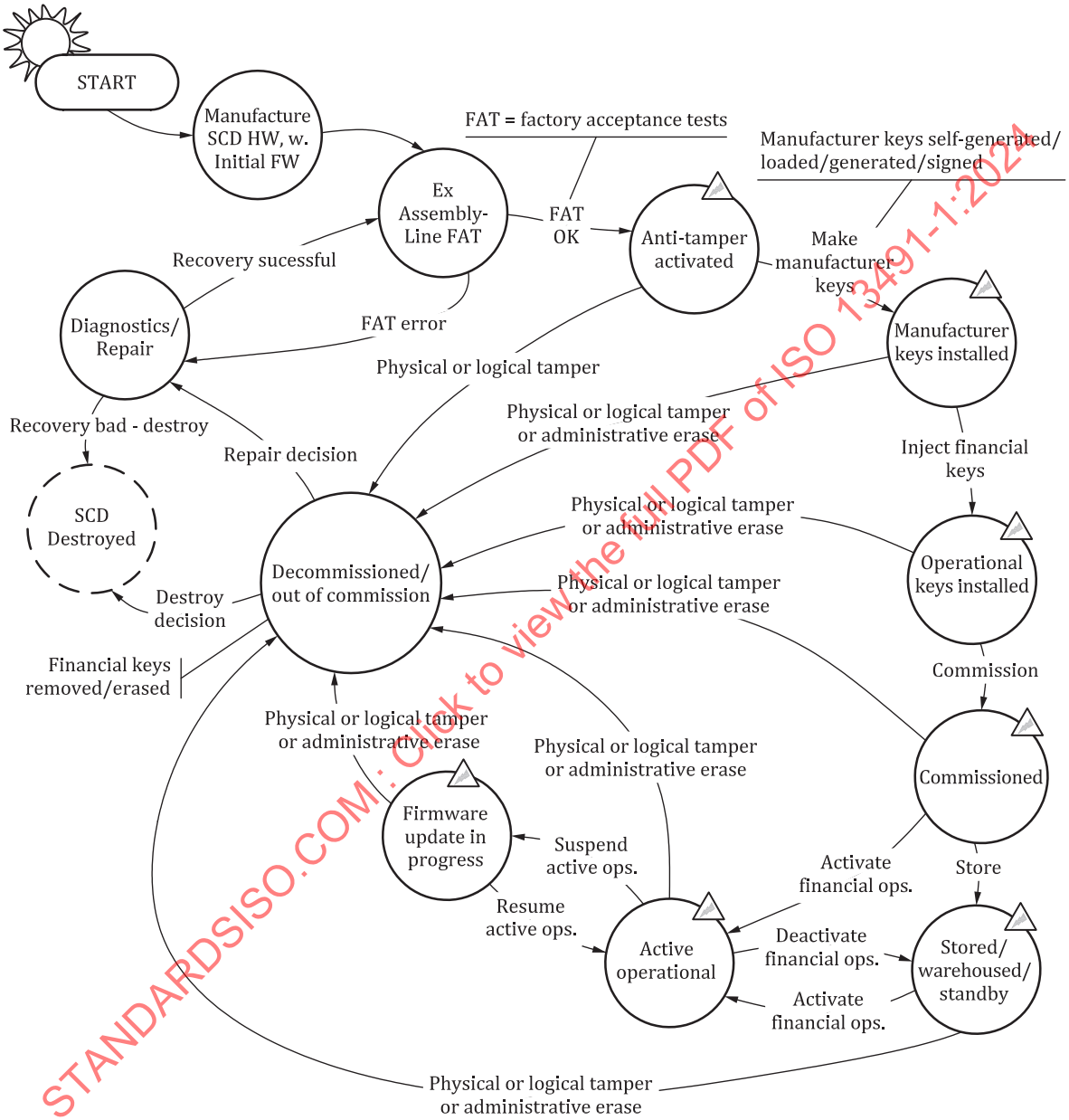
The device and its environment shall be subject to appropriate auditing and controls that are applied at each phase of the device's life cycle. If this is not done, the device could be subject, in one or more phases of its life cycle, to the attack scenarios identified earlier. Device management includes control elements which are preventive, detective, corrective and recovery in nature. An example of a control that is preventive and detective is comprehensive inventory control (including monitoring) to accurately track SCDs and HMDs, thereby creating a chain-of-custody audit trail throughout the life cycle of the devices. The security of an SCD depends upon the characteristics of the device but might also depend upon the characteristics of the environment in which the device is located.

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

Throughout the life cycle of the device, key management shall conform to the principles of ISO 11568.

7.2 Life cycle phases

A life cycle phase is a result of a change in either the environment and/or the state of the device. Different SCDs can have substantially different life cycles. Figure 2 presents a generalized device life cycle, indicating the possible phases in the life of an SCD and the events that cause a transition from one phase to the next. It is important to distinguish between these phases because the protection requirements for the device, as well as the means of providing protection, can change as the device moves from one life cycle phase to another.



Key

anti-tamper active

final state of SCD

Figure 2 — Device life-cycle state diagram

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

— Manufacturing phase: Phase including the design, construction, factory acceptance testing (FAT) and security evaluation of the device so that the device incorporates the intended administrative functionality and physical security characteristics. The device will leave this stage with firmware and, where applicable, the manufacturer's self-generated embedded keys (known as the manufacturer's keys). These can be the PKI keys (known as the SCD's PKI keys) necessary for remote symmetric key distribution performed using the asymmetric techniques given in ISO 11568. The device tamper responsive mechanisms ("anti-tamper" in Figure 2) shall be active in order to protect these keys. In any later stage, anti-tamper mechanisms ensure that any attempt to tamper physically and/or logically the SCD results in the transition of the internal device state to the decommissioned state as illustrated in Figure 2.

— Post-manufacturing phase: Phase consisting of the transport and storage of the device prior to initial financial key loading. The SCD is to be equipped with specific security controls to allow the SCD owner to verify that the device was not intercepted in transit or otherwise tampered with before its reception and subsequent commissioning.

— Commissioning phase (initial financial key loading phase): Phase consisting of loading or self-generation of the initial financial keys (and payment application for PEDs) that might replace the initial manufacture's keys. The commissioned device leaves this phase enabled for activation and operational use ("active operational" phase in Figure 2). Yet the SCD owner might decide to store the commissioned device for a later activation and operational use by putting the device in an intermediary "inactive operational stage" or "stored stage".

— Inactive operational phase ("stored" in Figure 2): Phase in which the device contains financial keys but is not in operational use. Devices in this phase will be stored and transported to the site of operational use. They include devices stored as spares or held as seasonal inventory.

— Active operational phase: A device can be regarded as being in a state of active operational use when it has been installed for its intended purpose at its intended location. Notice that during this phase, firmware might be subject to maintenance operations and the SCD be temporary suspended. Upon the validation of the maintenance operations, the SCD is to be resumed to its original active operational state.

— Decommissioning phase: Phase in which the SCD is removed from operational service permanently, or for repair, and the financial keys are removed. The decommissioning phase might leave the manufacturer's keys and the SCD's PKI keys intact. For PEDs, the decommissioning phase might utilize an authorized agent to remove the keys.

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

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

7.3 Life cycle protection requirements

7.3.1 General

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

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

The security of the device shall not depend only upon the secrecy of the design details. However, where such secrecy contributes to the security of the device, compromise prevention is required throughout all life

cycle phases. When secrecy of the design features is not required, the general requirements for each phase are described as given in 7.3.2 to 7.3.5.

7.3.2 Manufacturing phase

During the manufacturing phase, security relies on the manufacturer's procedures and environment. The security of the device shall not depend only upon the secrecy of the design details. However, such secrecy contributes to the security of the device and, therefore, the manufacturer's procedures shall be designed to prevent the disclosure of detailed design documentation.

As part of the manufacturing process, a series of cryptographic keys might be installed or generated. Prior to the loading or generation of the first cryptographic keys of the device:

— protection is provided by the characteristics of the device itself through the physical difficulty of opening the device or of obtaining a counterfeit version to substitute for the device;

— protection is provided by maintaining chain of custody through environmental controls and device management processes.

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

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

Some SCDs (e.g. HSMs) may be manufactured such that there are no cryptographic keys within the device. Until an initial key has been loaded or generated, it is necessary to detect a compromise. If a compromise is detected, it is only necessary to ensure that keys are not injected into the device, and it is not placed in service until all effects of the compromise have been eliminated from the device.

7.3.3 Post-manufacturing phase

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

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

7.3.4 Commissioning (initial financial key loading) phase

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

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

7.3.5 Inactive operational phase

The protections are provided by the characteristics of the device, i.e. tamper evidence, resistance and responsiveness, and device management procedures including the storage and transport of the device prior

to the active deployment of the device. The entity responsible for the devices in this phase is the current owner, which might be the acquirer or even the merchant.

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

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

7.3.6 Active operational phase (use)

Detection of device compromise is required during this phase.

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

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

Upgrades to an SCD performed during this phase that could impact its security functionality shall be cryptographically verified or performed under dual control. Upgrades to an SCD should be encrypted to protect from vulnerability analysis.

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

7.3.7 Decommissioning (post-use) phase

Devices are decommissioned with the intention to:

— transfer ownership of the device to another organization;

— repair the device; or

— destroy the device.

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

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

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

7.3.8 Repair phase

Device management is required during this phase.

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

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

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