Desk/3500
PCI HSM Security Policy

Status	Release
Document date:	13 December 2023
Classification:	Public
Reference:	ICO-OPE-05399-EN
Version:	09

Version history

Version no.	Version date	Most important edit(s)
1	2018/12/27	Document creation
2	2019/01/21	Document update
3	2019/04/02	Document update
4	2019/07/08	Document update
5	2019/11/15	Document update
6	2020/06/08	Document update
7	2020/11/20	Document update
8	2022/08/22	Document update
9	2023/12/11	Document update

Table of contents

References

Latest version of documents is applicable.

[1] ANSI X9.24-1:2017, Retail Financial Services Symmetric Key Management Part 1: Using Symmetric Techniques

[2] ANSI X9.24-2:2021, Retail Financial Services Symmetric Key Management Part 2: Using Asymmetric Techniques for the Distribution of Symmetric Keys

[3] ANSI X9.24-3:2017 Retail Financial Services Symmetric Key Management - Part 3: Derived Unique Key Per Transaction

[4] X9 TR-31 2018, Interoperable Secure Key Exchange Key Block Specification for Symmetric Algorithms

[5] ANSI X9.143:2022, Retail Financial Services – Interoperable Secure Key Block Specification

[6] ISO 9564-1:2017, Financial services — Personal Identification Number (PIN) management and security — Part 1: Basic principles and requirements for PINs in card-based systems

[7] Recommendation for Key Derivation Using Pseudorandom Functions - NIST Special Publication 800-108:Rev.1

[8] ISO13491-1:2016 Banking – Secure Cryptographic Devices: Concepts, requirements and evaluation methods

[9] ISO13491-2:2023 Banking – Secure Cryptographic Devices: Security compliance checklists for devices used in financial transactions

[10] Derived Test Requirements for FIPS PUB 140-2

[11] Ingenico Desk/3500 User Guide

Notes

[11] is delivered to the end user.

Terminology and Abbreviations

Acronyms	Definition
ANS	American National Standards
ANSI	American National Standards Institute
DHCP	Domain Host Configuration Protocol
DNS	Domain Name System
DUKPT	Derived Unique Key per Transaction
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
FTP	File Transfer Protocol
HMAC	Hash-based Message Authentication Code
HTTP	Hyper-Text Transfer Protocol
ICC	Integrated Circuit Card
IK	Initialisation Key / Initial Key
IP	Internet Protocol
IPEK	Initial PIN Encryption Key
MAC	Message Authentication Code
PCI	Payment Card Industry
PIN	Personal Identification Number

Acronyms	Definition
POP3	Post Office Protocol
PPP	Point-to-Point Protocol
RSA	Rivest Shamir Adelman Algorithm
SFTP	SSH File Transfer Protocol
SHA	Secure Hash Algorithm
SMTP	Simple Mail Transfer Protocol
SNTP	Simple Network Time Protocol
SSL	Secure Sockets Layer
TCP	Transmission Configuration Protocol
TDES	Triple Data Encryption Standard
TLS	Transport Layer Security
TR31	Key Block Format (ANSI)
UDP	User Data Protocol
USB	Universal Serial Bus
Wi-Fi	Wireless Fidelity
WS/WSS	WebSocket Protocol
X9	Accredited Standards Committee X9 (ANS / ANSI)

1 Introduction

This document addresses the proper use of the Key Loading Device in a secure manner including information about key-management responsibilities, administrative responsibilities, device functionality, identification and environmental requirements.

The use of the device in an unapproved method, contrary to what is described in the security policy, will violate the PCI HSM approval of the device.

2 General Description

2.1 Product Name and Appearance

The product name is visible on the front and on the label of the device as shown in section 2.3.1.

The product name shall not be modified by the merchant, nor covered by any sticker or other attachment.

Figure 1 – Desk/3500

2.2 Product type

The Desk/3500 is a PCI HSM KLD device, designed to provide HSM capabilities.

It provides a portfolio of connectivity: USB host/device, Modem, Ethernet and RS232.

2.3 Identification

2.3.1 Product hardware version

The product hardware version is detailed on the rating plate (sticker) located on the back of the device.

The rating plate shall not be removed, covered, or otherwise altered in any way.

The hardware version number (HVN) is the concatenation of the article number and hardware revision.

The approved hardware version can be found on the PCI website.

Figure 2 – Desk/3500 hardware identification

Hardware Version Number and Positions							
	D	E	S	3	5	B	B
	D	E	S	3	5	A	B
Position	1	2	3	4	5	6	7
1-5	**Product identifier** Fixed value						
6-7	**Hardware security identifier** • AB: No contactless • BB: Contactless						

2.3.2 Product software versions

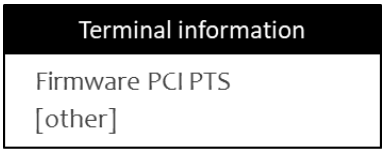
2.3.2.1 Product software versions display

The full list of approved firmware versions is available on the PCI PTS website.

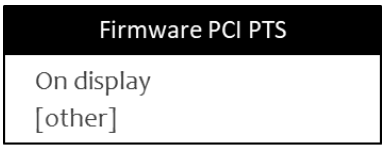
The software versions can be retrieved using the software menu.

To get this information on the device, select the following menu:

- "**Control Panel**", then "**Terminal information**",
- Select **Firmware PCI PTS** from the following configuration menu:



- Select **On display** from the following configuration menu:



The following item is displayed:

- M1 is the reference of the firmware (“Core Firmware”, “Security Services”)

2.3.2.2 Product software versions

Firmware versions												
	8	2	0	5	6	3	v	0	1	.	x	x
	8	2	0	5	6	3	v	0	2	.	x	x
	8	2	0	5	6	3	v	0	3	.	x	x
	8	2	0	3	8	0	v	0	1	.	x	x
	8	2	0	3	8	0	v	0	2	.	x	x
	8	2	0	3	8	0	v	0	3	.	x	x
	8	2	0	3	8	0	v	0	4	.	x	x
	8	2	0	3	8	0	v	0	5	.	x	x
	8	2	0	3	8	0	v	0	6	.	x	x
	8	2	0	3	8	0	v	0	7	.	x	x
	8	2	0	3	8	0	v	0	8	.	x	x
	8	2	0	3	8	0	v	0	9	.	x	x
Position	1	2	3	4	5	6	7	8	9	10	11	12

1-6	**Software identifier** Numerical value in range 820000 - 820999 • 820563 for Core Firmware • 820380 for Security Services
7	Fixed value ‘v’ (which stands for version)
8-9	**Software security version identifier** Numerical value in range 00 – 99
10	Fixed value ‘.’ as separator
11-12	**Non-security related change** Numerical value in range 00 – 99 Examples: System UI changes, functional bug fixes, driver updates, etc.

3 Installation and User Guidance

3.1 Initial Inspection

The user makes sure that they obtain the device from Ingenico or Ingenico approved resellers.

Upon receipt of the terminal:

- The user must carefully inspect the shipping carton and its content for shipping damage.
- The user must visually inspect the terminal for sign of tampering, as it is described in the User Guide [11].
- It is strongly advised that these checks are also performed on a regular basis after receipt and installation.
- The user must check the firmware version. (See section 2.3.2)
- The user must check the hardware version number. (See section 2.3.1)

For example, the user should inspect the terminal to ensure that:

- There is no evidence of unusual wires that have been connected to any ports of the terminal, or associated equipment, the chip card reader, or any other part of the terminal.
- There is no shim device in the slot of the ICC acceptor.
- The keypad is firmly in place.
- No warning flashing message is displayed.
- The terminal serial number (on the rear side label) corresponds to the inventory.

Such checks would provide warning of any unauthorized modifications to or substitution of the terminal, or suspicious behaviour of individuals that have access to the terminal.

3.2 Installation

A User Guide [11] including the following information is provided with the device:

- Equipment check list:
  - Device
  - Cable and connectors
  - Documents
- Power and cable connections information
- The main characteristics of the device (i.e., temperature, humidity, voltage)
- Safety recommendations
- Security recommendations
- Troubleshooting if the device does not work

3.3 Environmental Conditions

The environmental conditions to operate the device are specified in the User Guide [11].

The security of the device is not compromised by altering the environmental conditions (e.g., subjecting the device to temperature or operating voltages outside the stated operating ranges does not alter the security).

At extreme environmental conditions a tamper event will occur:

- Temperatures above +125 ºC or below -40 ºC
- Core voltage above 1,98V or below 1,62V
- Battery voltage above 2,15V or below 1,89V

The device is restricted to deployment in environments that comply with the security compliance checklist defined in [9].

3.4 Communication and Security Protocols

The following protocols and services are available on the device: TLS/SSL, IP, DNS, SMTP, POP3, DHCP, HTTP, HTTPS, SNTP, SOCKS, FTP, SFTP, WS/WSS, TCP/UDP, PPP.

4 Operation and Maintenance

4.1 Periodic Inspection

Information about periodic inspection is specified in the User Guide [11].

The user should daily check that the keypad is firmly in place. Such checks would provide warning of any unauthorized modification to the terminal, or suspicious behaviour of the terminal.

In the tampered state, the device displays a warning flashing message and further use of the device is not possible. If such a message is observed, the user must contact the device helpdesk immediately, remove it from service and keep it available for potential forensics investigation.

The user should also check that the installation/maintenance operations are performed by a trusted person and log the maintenance operations, including name of the operator.

4.2 Self-tests

Self-tests are performed upon start-up/reset and periodically (i.e., at least once a day during the normal use of the device). Self-tests are also performed conditionally. These tests are not initiated by an operator.

All these self-tests follow the requirements described in [10].

4.3 Roles and Responsibilities

4.3.1 Roles, Required Authentication and Associated Services

The types of roles and the associated authentication required are given in the table below.

Role	Authentication	Services description
Administrator	Password	Performs user enrolment and environment setup
Supervisor	Password or Smartcard & PIN	Performs tool configuration, key management functions (e.g. input of a key through components), logs loading operation, and sensitive services such as key import/export and key injection process
Operator	Password or Smartcard & PIN	Performs Key Injection process and logs loading operation.

All sensitive commands within the Desk/3500 require dual control authentication before they can be executed.

4.3.2 Strengths of Authentication Mechanisms using smartcards

The authentication mechanism is based on two distinct smartcards with their associated PIN codes. The probability that for multiple attempts within a one-minute period a random attempt will succeed is equal to 1/1016. Moreover, after three failed attempts, the smartcard remains blocked.

4.3.3 Strengths of Authentication Mechanisms using passwords

The authentication mechanism is based on two distinct users with their associated passwords. The probability that for multiple attempts within a one-minute period a random attempt will succeed is equal to 1/295. Moreover, after five failed attempts, the user account remains blocked.

4.4 System Administration

4.4.1 Configuration Settings

The device is functional when received by the user. No security sensitive configuration settings are necessary to be tuned by the user to meet security requirements.

4.4.2 Default Value Update

In smartcard mode, the device is functional when received by the user and there is no security sensitive default value (e.g. admin password) that needs to be changed before operating the device.

In password mode, at device initialization, the device comes with pre-expired administrator random password for any account creation which must be changed before operating the device.

4.5 Tamper Response

The device contains tamper mechanisms that will trigger when a physical penetration attempt of the device is detected. A user can easily detect a tampered terminal:

- The numerical keyboard is locked,
- A flashing warning message is displayed.

Any physical penetration will result in a “tamper event”. This event causes the activation of tamper mechanisms that make the device out of service.

There are two separate modes in which the device can be:

- Activated mode: the device is fully operational.
- Non-activated mode: the device is tampered, not operating and needs reactivation after maintenance and security checks.

Information about the tamper events is also described in the User Guide [11].

If the device is in tampered state, the merchant or acquirer should contact the device helpdesk immediately, remove it from service and keep it available for potential forensics investigation.

4.6 Patching and Updating

Firmware, application updates, patches and configuration parameters can be loaded in the device. They are cryptographically authenticated by the device. If the authenticity is not confirmed, the update or patch is rejected.

For the secure operation of the device, it is recommended to update the software with the latest distributed version.

Both local and remote updates are supported.

The remote update can be initiated either by the user or automatically by the embedded application.

For instructions on how to perform these updates, please contact your local helpdesk for applicable procedures.

4.7 Decommissioning

Sensitive data must be erased before refurbishing the device or removing it permanently from service.

The device shall go to tampered status, a state in which sensitive data are erased.

For example, disassembly of the device will lead to a tampered status.

4.8 Log Maintenance

Log size supported by the device is finite. Once log file has reached its limit, the device cannot perform any Key Injection until logs have been uploaded. Operators or Supervisors should ensure that log records are exported on a regular basis under the discretion of the end user as described in the User Guide [11].

5 Security

5.1 Signing

Application code is authenticated before being allowed to run. The certificate and signature of the application code is verified.

In case of incorrect signature or certificate, software is rejected. No action is expected from the end user.

The certificate and signature are based on couples of ECDSA keys. The authenticity is guaranteed by a certificate emitted by Ingenico.

5.2 Cryptographic Algorithms

Cryptographic algorithms implemented within the device are:

- DES[1]
- TDES (112 and 168 bits), ECB and CBC mode
- AES (128, 192, 256 bits), ECB and CBC mode
- RSA (2048, 4096 bits)
- ECDSA (256, 384, 521 bits)
- SHA 256, SHA-384, SHA-512
- ECDH (521 bits)
- MDC-2

5.3 Key Table

Key Name	Purpose / Usage	Algorithm	Size (Bits)	Storage
K_ROOT_CA	CA public keys for certificate verification	ECDSA	521	Secure unit
K_Sub_CA1	CA public keys for certificate verification	ECDSA	521	Secure unit
K_EE1_x[2]	CA public keys for certificate verification	ECDSA	521	Secure unit
ECC Key Pair	ECC Key pair for ECDSA signature	ECDSA	256	Secure unit
ECC Key Pair	ECC Key pair generation and export	ECC	256	Secure unit

Figure 3: ECC Keys and certificate

[1] For non-PCI payment brand relevant transactions

[2] x is a numerical variable

Key Name	Purpose / Usage	Algorithm	Size (Bits)	Storage
RSA Signature Key Pair	RSA key pair for TR34 Key exchange signature and the Log signature	RSA	2048	Secure unit
RSA Encryption Key Pair	RSA key pair for TR34 Key exchange encryption	RSA	2048	Secure unit
RSA RootCA	CA public keys for certificate verification	RSA	2048	Secure unit
RSA SubCA	CA public keys for certificate verification	RSA	2048	Secure unit
Card Authentication RSA Public Key	RSA public key for smartcard content authentication	RSA	2048	Secure unit

Figure 4: RSA Keys and certificate

Key Name	Size (Bits)	Algorithm	Purpose / Usage	Storage
K_TR31	112/168	TDES	Calculation of key encryption and MAC keys (according to ANSI31)	Secure unit
Key Encryption Key	112/168	TDES	Key encryption	Secure unit
Data Encryption Key	112/168	TDES	Data encryption, MAC calculation / verification	Secure unit
PIN Key	112/168	TDES	PIN encryption	Secure unit
DUKPT BDK	112	TDES	DUKPT Base Derivation Key	Secure unit

Figure 5: TDES Keys

Key Name	Size (Bits)	Algorithm	Purpose / Usage	Storage
K_TR31	128/192/256	AES	Calculation of key encryption and MAC keys (according to ANSI31)	Secure unit
Key Encryption Key	128/192/256	AES	Key encryption	Secure unit
Data Key	128/192/256	AES	Data encryption, MAC calculation / verification	Secure unit
PIN Key	128/192/256	AES	PIN encryption	Secure unit
DUKPT BDK	128/192/256	AES	DUKPT Base Derivation Key	Secure unit
MBK	256	AES	Master Backup key for confidentiality and integrity of Key Database backup	Secure unit
MBK_KBPK	256	AES	Used to cipher the LMK for Key Database backup	Secure unit

MBK_DATA	256	AES	Used to cipher the LMS for Key Database backup	Secure unit
MBK_CMAC	256	AES	Used to ensure the integrity of encrypted data of Key Database backup	Secure unit

Figure 6: AES Keys

Key Name	Size (Bits)	Algorithm	Purpose / Usage	Storage
HMAC Key	128	HMAC-SHA256	Calculation of MAC keys	Secure unit
HMAC Key	224	HMAC-SHA384	Calculation of MAC keys	Secure unit
HMAC Key	256	HMAC-SHA512	Calculation of MAC keys	Secure unit

Figure 7: HMAC Keys

5.4 Key Management

The device implements different types of key management techniques:

- Fixed Key: a key management technique based on a unique key for each terminal as specified in [1].
- Master Key/Session Key: a method using a hierarchy of keys. The session keys are unique per transaction as specified in [2].
- DUKPT: a key management technique based on a unique key for each transaction as specified in [3].

The device also provides the ability to:

- Derive Key per terminal
- Import/export encrypted key by a KBPK in a TR-31 or X9.143 format as specified in [4] and [5]
- Import/export keys through cryptograms
- Import/export key by components

The use of the device with different key-management systems will invalidate any PCI approval of this device.

5.5 Key Replacement

Any key should be replaced with a new key whenever the compromise of the original key is known or suspected, and whenever the time deemed feasible to determine the key by exhaustive attack elapses.

5.6 Key Archival

Secure key archival storage remains under the sole authority of their custodians, in accordance with the documentation provided with the device.