Desk/3200 and Desk/3500
PCI PTS Security Policy

ICO-OPE-04972-EN-V12

www.ingenico.com

28/32, boulevard de Grenelle, 75015 Paris - France / (T) +33 (0)1 58 01 80 00 / (F) +33 (0)1 58 01 91 35

Ingenico – S.A. au capital de 53 086 309 € / 317 218 758 RCS PARIS

Contents

1_Document Information

1_1 Evolution follow-up

Revision	Type of modification	Date
1	Document Creation	2018/01/15
2	Document Update	2018/03/08
3	Document Update	2018/11/12
4	Document Update	2020/05/05
5	Document Update	2020/06/03
6	Document Update	2020/06/09
7	Document Update	2020/06/12
8	Document Update	2020/06/29
9	Document update	2022/02/04
10	Document update	2022/02/05
11	Document update	2022/02/10

1_2 Acronyms

AES	Advanced Encryption Standard
DUKPT	Derived Unique Key per Transaction
N/A	Not Applicable
PED	PIN Entry Device
PIN	Personal Identification Number
RSA	Rivest Shamir Adelman Algorithm
SHA	Secure Hash Algorithm
TDES	Triple Data Encryption Standard
ECDSA	Elliptic curve digital signature algorithm

1_3 References

[1] ANS X9.24 Part 2: 2016, Retail Financial Services Symmetric Key Management Part 2: Using Asymmetric Techniques for the Distribution of Symmetric Keys
[2] ANS X9.24 - 1: 2017, Retail Financial Services Symmetric Key Management Part 1: Using Symmetric Techniques
[3] ANS X9.24 - 3: 2017, Retail Financial Services Symmetric Key Management Part 1: Unique Key Per Transaction
[4] X9 TR-31 2018, Interoperable Secure Key Exchange Key Block Specification for Symmetric Algorithms
[5] ISO 9564-1, Financial services — Personal Identification Number (PIN) management and security — Part 1: Basic principles and requirements for PINs in card-based systems
[6] ISO 9564-2, Banking — Personal Identification Number management and security Part 2: Approved algorithms for PIN encipherment
[7] PCI PTS POI Derived Test Requirements V5.1 – March 2018
[8] Ingenico Desk/3500 and Desk/3200 Installation guide
[9] Ingenico ICO-OPE-01390, Package IP: Security guidance user's guide
[10] Ingenico ICO-OPE-01391, Package SSL: Security guidance user's guide
[11] Ingenico ICO-OPE-01935, Secure Reading and Exchange of Data security guidance

Notes:
[8] is delivered to the end user.
[9], [10], [11] are delivered to authorized software developers:

2_Introduction

This document addresses the proper use of the POI 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, as described in the security policy, will violate the PCI PTS v5.1 approval of the device.

3_General Description

3_1 Product Overview

3_1_1 Product type

The Desk/3200 and Desk/3500 PED is a Point of Sale (POS) payment desktop device, to process credit and PIN-based debit card transactions in an attended environment. The device can also be used as a desk mounted device, when following the guidance as stated in the installation guide.

3_1_2 Product functionalities

The Desk/3200 and Desk/3500 PED is equipped to handle all form of payment including:

- EMV chip & PIN
- Chip & Sign
- Magstripe including JISII Tracks
- Contactless

It provides a portfolio of connectivity: USB host/device, Modem, Ethernet, Network cellular, Wi-Fi and RS232.

3_1_3 Version without privacy shield

Figure 1: Desk/3200

Figure 2: Desk/3500

3_1_4 Version with privacy shield

Figure 3: Desk/3200

Figure 4: Desk/3500

3_2 Product Identification

3_2_1 Product name

The product name is visible on the front of the device (see Figure 1 and Figure 2).
The product name shall not be modified by the merchant or covered by a sticker.

3_2_2 Product hardware version

The product hardware version is printed on a label at the back of the device.
The label at the back of the device shall not be teared off, covered or altered.

Figure 5 - Desk/3200 product hardware identification

Figure 6 - Desk/3500 product hardware identification

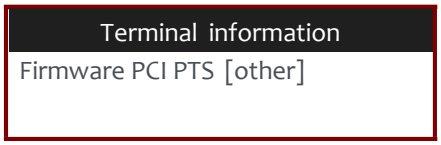
The full list of approved Hardware Version Number is available on the PCI PTS website.

3_2_3 Product software versions

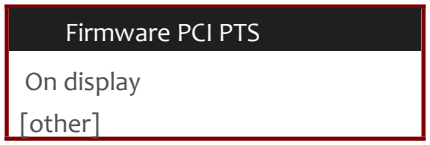
The software versions can be retrieved using the software menu.

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 items are displayed:

- "M1" is the reference of the firmware.
- "M3" is the reference of the "Open Protocols" module.
- "M4" is the reference of the "SRED" module.

4_Guidance

4_1 Initial Security Inspection

The merchant or acquirer must visually inspect the terminal for sign of tampering when received via shipping, as it is described in the Installation Guide [8].
It is strongly advised that these checks are also performed on a regular basis after receipt and installation.

For example, the merchant or acquirer 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 behavior of individuals that have access to the terminal.

4_2 Installation Guide

An installation guide [8] 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.

4_3 PIN Confidentiality

The device is designed to be used in attended environment.
It's recommended that the position of the terminal must be in such a way to make cardholder PIN spying infeasible.

The installation guide [8] provides instructions for the installation and use of the terminal in a secure manner depending on the device environment.
Further recommendations about the installation of the terminal variants without privacy shield are specified in the installation guide [8].

NEVER ask the customer to divulge their PIN Code.
With guidance message or logos, indicate to the cardholder to use his hands and/or his body to cover up the keypad.
The cardholder shall be advised to ensure that he is not being overlooked when entering his PIN code.

4_4 Periodic Inspection and Maintenance

Information about periodic inspection is specified in the installation guide [8].
The merchant or acquirer should daily check that the keypad is firmly in place. Such checks would provide warning of any unauthorized modification to the terminal, or suspicious behavior 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 merchant or acquirer must contact the device helpdesk immediately, remove it from service and keep it available for potential forensics investigation.

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

The merchant or acquirer should check if the ICC reader slot is damaged, such as abrasion, painting and other machining marks or if there is any suspicious object like lead wire or any unknown object inside ICC reader.
If such suspicious circumstances are observed, the merchant or acquirer shall stop using the device immediately and contact the customer service to confirm the device has been tampered.

Figure 7 : ICC reader slot

4_5 Product Service Removal

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.

5_Product Hardware Security

5_1 Tamper Response Event

The device contains tamper mechanisms that will trigger when a physical penetration attempt of the device is detected. A merchant or acquirer 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 are also described in the installation guide [8].

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.

5_2 Environment Conditions and Environmental Failure Protection

The environmental conditions to operate the device are specified in the installation guide [8].
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).

6_Product Software Security

6_1 Software Development Guidance

When developing IP enabled applications, the developer must abide by the coding rules and best practices described in the document [9], [10].

The following protocols and services are available on the device: TLS/SSL[1], IP, DNS, SMTP, POP3, DHCP, HTTP, HTTPS, SNTP, SOCKS, FTP, SFTP, WS/WSS, TCP/UDP, PPP.

This security guidance describes how protocols and services must be used/configured for each interface that is available on the platform.
Note that SSL protocol is inherently weak and should be removed unless required on an interim basis to facilitate interoperability as part of a migration plan.

When developing SRED applications, the developer must follow the guidance described in the document [11].

The document provides security guidance for account data management and remote connection authentication using cryptographic mechanisms.

When developing applications, the developer must follow the guidance described in the document [11].

6_2 Account data protection

The device supports account data protection using format-preserving encryption (FPE). The FPE methods used are BPS and FF1.
The device also supports account data protection using standard TDES and standard AES.

The pass-through of clear-text account data is supported using whitelisting technique.

6_3 Firmware, Software and Configuration Parameters Update

Updates and patches 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 use the latest version of software distributed

6_4 Software Authentication

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

[1] SSL is only allowed for non-web services. If web services are used, only TLS is allowed for web interfaces.

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.

6_5 Self-Tests

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

Self-tests include:

- Check of integrity and authenticity of the software
- Check of the security mechanisms for sign of tampering

7_System Administration

7_1 Configuration Settings

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

7_2 Default Value Update

The device is functional when received by the merchant or acquirer and there is no security sensitive default value (e.g. admin password) that needs to be changed before operating the device.

8_Key Management

8_1 Key Management Techniques

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 [2].
- 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].

8_2 Cryptographic Algorithms

The device includes the following algorithms:

- Triple DES (112 bits, 168 bits)
- AES (128, 192 and 256 bits)
- RSA (2048 bits)
- ECDSA (256, 384, 521 bits)
- SHA-256, SHA-384, SHA-512

8_3 Key Table

Key Name	Purpose / Usage	Algorithm	Size (Bits)	Storage	Form factor loaded to device In	Number of available Key Slots
K_Root_CA	CA public keys for certificate verification	ECDSA	521	Secure unit	ROM	1
K_Sub_CA1	CA public keys for certificate verification	ECDSA	521	Secure unit	ROM	1
K_EE1_x2	CA public keys for certificate verification	ECDSA	521	Secure unit	ROM	1
K_TR31	Calculation of key encryption and MAC keys (according to ANSI31)	TDES TDES AES AES AES	112 168 128 192 256	Secure unit	Enciphered under K_Key or K_TR31	31 25 31 25 21
Key Encryption Key	Key encryption	TDES TDES AES AES AES	112 168 128 192 256	Secure unit	Enciphered under K_Key or K_TR31	31 25 31 25 21
Data encryption Key	Data encryption, MAC calculation / verification	DES TDES TDES AES AES AES	64 112 168 128 192 256	Secure unit	Enciphered under K_Key or K_TR31	42 31 25 31 25 21
PIN Encryption Key	PIN encryption	TDES TDES AES AES AES	112 168 128 192 256	Secure unit	Enciphered under K_Key or K_TR31	31 25 31 25 21
DUKPT2009 – IPEK	Initial DUKPT Keys	TDES	112	Secure unit	Enciphered under K_Key	2
DUKPT2009 – Pin Key	Pin encryption	TDES	112	Secure unit	Derived originally from IPEK	42

[2] X is a numerical variable

Key Name	Purpose / Usage	Algorithm	Size (Bits)	Storage	Form factor loaded to device In	Number of available Key Slots
DUKPT2009 – Data Key	Data encryption	TDES	112	Secure unit	Derived originally from IPEK	42
DUKPT2009 – MAC Key	MAC calculation / verification	TDES	112	Secure unit	Derived originally from IPEK	42
DUKPT2017 – IPEK	Initial DUKPT Keys	AES AES AES	128 192 256	Secure unit	Enciphered under K_Key	1
DUKPT2017 – Pin Key	Pin encryption	TDES TDES AES AES AES	112 168 128 192 256	Secure unit	Derived originally from IPEK	32
DUKPT2017 – Data Key	Data encryption	TDES TDES AES AES AES	112 168 128 192 256	Secure unit	Derived originally from IPEK	32
DUKPT2017 – MAC Key	MAC calculation / verification	TDES TDES AES AES AES	112 168 128 192 256	Secure unit	Derived originally from IPEK	32
DUKPT2017 – HMAC Key	HMAC calculation / verification	HMAC HMAC HMAC	128 192 256	Secure unit	Derived originally from IPEK	32
EMV_PK_MAC Key	MAC Generation and verification of EMV PK	TDES	128	Secure unit	Randomly generated	31
EMV_PK_CA Key	CA public keys for certificate verification (EMV_Issuer_PK)	RSA	2048	Secure unit	Received from bank host	1

Key Name	Purpose / Usage	Algorithm	Size (Bits)	Storage	Form factor loaded to device In	Number of available Key Slots
EMV_Issuer_PK Key	Issuer public key for certificate verification (EMV_ICC_PK and PIN_Cipher_PK) and EMV Data authentication (SDA case)	RSA	2048	Secure unit	Received from CARD	1
EMV_ICC_PK Key	EMV Data authentication (DDA and CDA cases) and PIN Encryption	RSA	2048	Secure unit	Received from CARD	1
PIN_Cipher_PK Key	Offline PIN Encryption	RSA	2048	Secure unit	Received from CARD	1
MC_MAC Key	MAC Generation and verification of MC_ECC_Payment_System PK	TDES	128	Secure unit	Randomly generated	31
MC_Session_Cipher Key	Encryption and Decryption of Data	AES	128	Secure unit	Derived from MC_Kernel_ECC private Key	1
MC_Session_Authent Key	Authentication of Data	AES	128	Secure unit	Derived from MC_Kernel_ECC private Key	1
MC_ECC_Payment_System_PK Key	Verification of MC_Issuer_ECC_PK Key	ECC	256	Secure unit	Received from bank host	5
MC_Kernel_ECC Private Key	ECDH Establishment and Generation of MC_Session Keys	ECC	256	Secure unit	Randomly generated	5
MC_Kernel_ECC Public Key	ECDH Establishment	ECC	256	Secure unit	Randomly generated	5
MC_Issuer_ECC_PK Key	Verification of MC_ICC_ECC_PK Key	ECC	256	Secure unit	Received from CARD	5

Key Name	Purpose / Usage	Algorithm	Size (Bits)	Storage	Form factor loaded to device In	Number of available Key Slots
MC_ICC_ECC_PK Key	Validation of blinding factor	ECC	256	Secure unit	Received from CARD	5

8_4 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.

8_5 Key Loading Policy

The device has no functionality that gives access to security sensitive services, based on roles. Such services are managed through dedicated tools, using cryptographic authentication.

9_Roles and Services

The device has no functionality that gives access to security sensitive services, based on roles. Such services are managed through dedicated tools, using cryptographic authentication.