

# Lane/3000 and Desk/1500 PCI PTS Security Policy

**ICO-OPE-04818-EN-V16**

[www.ingenico.com](http://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

<b>1_ Document Information</b>	<b>4</b>
1_1 Evolution follow-up	4
1_2 Acronyms	4
1_3 References	5
<b>2_ Introduction</b>	<b>5</b>
<b>3_ General Description</b>	<b>6</b>
3_1 Product Overview	6
3_1_1 Product type	6
3_1_2 Product functionalities	6
3_2 Product Identification	8
3_2_1 Product name	8
3_2_2 Product hardware version	8
3_2_3 Product software versions	9
<b>4_ Guidance</b>	<b>10</b>
4_1 Initial Security Inspection	10
4_2 Installation Guide	10
4_3 PIN Confidentiality	10
4_4 Periodic Inspection and Maintenance	11
4_5 Product Service Removal	11
<b>5_ Product Hardware Security</b>	<b>12</b>
5_1 Tamper Response Event	12
5_2 Environment Conditions and Environmental Failure Protection	12
<b>6_ Product Software Security</b>	<b>13</b>
6_1 Software Development Guidance	13
6_2 Account data protection	13
6_3 Firmware, Software and Configuration Parameters Update	13
6_4 Software Authentication	13

**6\_5 Self-Tests..... 14**

**7\_ System Administration ..... 14**

**7\_1 Configuration Settings..... 14**

**7\_2 Default Value Update ..... 14**

**8\_ Key Management ..... 14**

**8\_1 Key Management Techniques ..... 14**

**8\_2 Cryptographic Algorithms..... 14**

**8\_3 Key Table..... 16**

**8\_4 Key Replacement..... 18**

**8\_5 Key Loading Policy ..... 18**

**9\_ Roles and Services ..... 19**

# 1\_Document Information

## 1\_1 Evolution follow-up

Revision	Type of modification	Date
1	Document creation	2017/10/23
2	Document update	2018/02/01
3	Document update	2018/04/13
4	Document update	2018/06/01
5	Document update	2018/07/03
6	Document update	2018/07/24
7	Document update	2018/11/15
8	Document update	2019/02/07
9	Document update	2019/06/07
10	Document update	2019/08/01
11	Document update	2020/02/28
12	Document update	2020/04/20
13	Document update	2020/05/06
14	Document update	2020/06/22
15	Fix date in revision	2021/11/04
16	Document update	2022/01/25

## 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 Adleman 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 2010, 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 Lane/3000 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 approval of the device.

## 3\_General Description

### 3\_1 Product Overview

#### 3\_1\_1 Product type

The Lane/3000 PED is a Point of Sale (POS) payment handheld device, to process credit and PIN-based debit card transactions in an attended environment or in a semi-attended environment.

A semi-attended environment is one where a transaction is completed under all of the following conditions:

- Card or Proximity Payment Device is present;
- Cardholder is present;
- Cardholder completes the Transaction and, if required, an individual representing the Merchant or Acquirer assists the Cardholder to complete the Transaction.

The Desk/1500 version is a dedicated PIN pad, it can be desk-mounted according to the installation guide.

#### 3\_1\_2 Product functionalities

The Lane/3000 and Desk/1500 PED are equipped to handle all form of payment including:

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

It provides USB host/device, RS232, Ethernet, Wi-Fi, Bluetooth and Bluetooth Low Energy<sup>1</sup>.



Figure 1 – Lane/3000



Figure 2 – Lane/3000 (PIN Shield version)

<sup>1</sup> The use of BLE Beacon interface shall respect guidance document [9]



Figure 3 – Desk/1500



Figure 4 – Desk/1500 (PIN Shield version)



Figure 5 – Lane/3000 equipped with removable camera module



Figure 6 – Lane/3000 “non modular”

Notes:

- The device has options for Touch Screen and Dual Head
- The Desk/1500 has the same hardware configurations.
- The removable camera module is available for all the Lane/3000 devices, except on “non modular” versions.

## 3\_2 Product Identification

### 3\_2\_1 Product name

The product name is visible on the front of the device (see Figure 1 to Figure 8).  
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 – Lane/3000 or Desk/1500 product hardware identification**

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

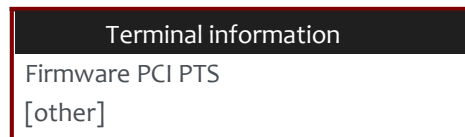


### 3\_2\_3 Product software versions

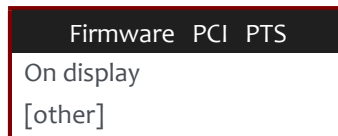
The software versions can be retrieved using the software menu.

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

- “**Control Panel**”, then “**Software management**” and “**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.

For the Desk/1500 device the information is retrievable from the Host Device.

## 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.

## 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<sup>3</sup>, 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.

### 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.

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.

---

<sup>3</sup> SSL is only allowed for non-web services. If web services are used, only TLS is allowed for web interfaces.

## 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_x4	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
DUKPT2009 – Data Key	Data encryption	TDES	112	Secure unit	Derived originally from IPEK	42

<sup>4</sup> 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 – 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
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

Key Name	Purpose / Usage	Algorithm	Size (Bits)	Storage	Form factor loaded to device In	Number of available Key Slots
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
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.