Move/2500
PCI PTS Security Policy

Status	Release
Document date:	2 November 2023
Classification:	Public
Reference:	ICO-OPE-04711-EN
Version:	11

Version history

Version no.	Version date	Most important edit(s)
1	10/01/2018	Document creation
2	05/04/2018	Document update
3	23/03/2020	Document update
4	21/04/2020	Document update
5	03/06/2020	Document update
6	22/06/2020	Document update
7	14/09/2020	Document update
8	24/01/2022	Document update
9	10/02/2022	Document update
10	14/03/2022	Document update
11	02/11/2023	Document update / New template

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 X9.143:2021, Retail Financial Services – Interoperable Secure Key Block Specification

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

[7] ISO 9564-2, Banking — Personal Identification Number management and security Part 2: Approved algorithms for PIN encipherment

[8] PCI PTS POI Derived Test Requirements V5.1, March 2018

[9] Ingenico Move/2500 Installation Guide

[10] Ingenico ICO-OPE-01390, Package IP: Security guidance user's guide

[11] Ingenico ICO-OPE-01391, Package SSL: Security guidance user's guide

[12] Ingenico ICO-OPE-01935, Secure Reading and Exchange of Data security guidance

Terminology and Abbreviations

Acronyms	Definition
ANS	American National Standards
ANSI	American National Standards Institute
CDA	Combined Dynamic Data Authentication
DDA	Dynamic Data Authentication
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
EMV	Europay Mastercard Visa
FPE	Format Preserving Encryption
FTP	File Transfer Protocol
HMAC	Hash-based Message Authentication Code
HTTP	Hyper-Text Transfer Protocol
IC	Integrated Circuit
ICC	Integrated Circuit Card
IK	Initialisation Key / Initial Key
IP	Internet Protocol
IPEK	Initial PIN Encryption Key
ISO	International Standards Organisation
MAC	Message Authentication Code
MC	MasterCard

Acronyms	Definition
N/A	Not Applicable
PCI	Payment Card Industry
PED	PIN Entry Device
PIN	Personal Identification Number
PK	Platform Key
POI	Point of Interaction
POP3	Post Office Protocol
POS	Point of Sale
PPP	Point-to-Point Protocol
PSTN	Public Switch Telephony Network Protocol
RAM	Random Access Memory
RSA	Rivest Shamir Adelman Algorithm
SDA	Static Data Authentication
SFTP	SSH File Transfer Protocol
SHA	Secure Hash Algorithm
SMTP	Simple Mail Transfer Protocol
SNTP	Simple Network Time Protocol
SRED	Secure Reading and Exchange of Data
SSH	Secure Shell 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
UI	User Interface
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 Point of Interaction (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.

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 – Move/2500

Figure 2 – Move/2500 with privacy shield

2.2 Product type

The Move/2500 PED is a Point of Sale (POS) payment handheld device, designed 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.

It is equipped to handle all forms of electronic payment including:

- EMV chip & PIN,
- Chip & sign,
- Magstripe including JIS I/II Tracks,
- Contactless.

It provides a portfolio of connectivity: USB, RS232, Ethernet, Modem, Wi-Fi[1], Network cellular connectivity, Bluetooth including Low Energy (BLE)[2].

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.

[1] The version with biometric sensor is not equipped with Wi-Fi.

[2] The use of BLE Beacon interface shall respect guidance document [10]. The BLE version used is 4.2 and only connections using Security Mode 1 Level 4 are supported.

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 3 – Move/2500 hardware identification

Hardware Version Number and Positions							
	M	O	V	2	5	A	C
	M	O	V	2	5	B	C
	M	O	V	2	5	B	D
	M	O	V	2	5	B	G
	M	O	V	2	5	C	C
	M	O	V	2	5	D	C
	M	O	V	2	5	D	D
	M	O	V	2	5	D	G
	M	O	V	2	5	E	C
	M	O	V	2	5	F	C
	M	O	V	2	5	F	D
	M	O	V	2	5	F	G
	M	O	V	2	5	G	C
	M	O	V	2	5	H	C
	M	O	V	2	5	H	D
	M	O	V	2	5	H	G
Position	1	2	3	4	5	6	7
1-5	**Product identifier** Fixed value • MOV25 for Move/2500						
6-7	**Hardware security identifier** • AC, EC: No contactless • BC, BD, BG, FC, FD, FG: Contactless • CC, GC: No Contactless + Privacy shield • DC, DD, DG, HC, HD, HG : Contactless + Privacy shield						

2.3.2 Product software versions

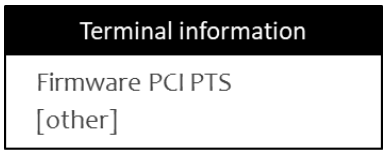
2.3.2.1 Product software versions display

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

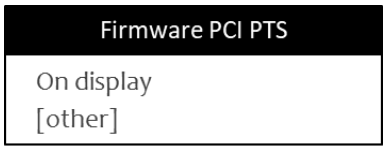
The software versions can be retrieved using the software menu:

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 items are displayed:

- M1 is the reference of the firmware ("Core Firmware", "Security Services"),
- M3 is the reference of the "Open Protocols" module,
- M4 is the reference of the "SRED" module.

2.3.2.2 Product software versions

Firmware versions												
	8	2	0	5	4	7	v	0	1	.	x	x
	8	2	0	3	7	6	v	0	1	.	x	x
	8	2	0	3	7	6	v	0	2	.	x	x
	8	2	0	3	7	6	v	0	4	.	x	x
	8	2	0	5	4	9	v	0	1	.	x	x
	8	2	0	5	5	6	v	0	1	.	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 • 820547 for Core Firmware • 820376 for Security Services • 820549 for SRED On-Guard FPE • 820556 for SRED On Guard SDE
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.

Application versions												
	8	2	0	5	4	8	v	0	2	.	x	x
	8	2	0	5	4	8	v	0	3	.	x	x
	8	2	0	5	4	8	v	0	6	.	x	x
	8	2	0	5	4	8	v	0	7	.	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 • 820548 for Open Protocols
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 merchant or acquirer make sure that they obtain the device from Ingenico or Ingenico approved resellers.

Upon receipt of the terminal:

- The merchant or acquirer must carefully inspect the shipping carton and its content for shipping damage.
- The merchant or acquirer must visually inspect the terminal for sign of tampering, as it is described in the Installation guide [9].
- It is strongly advised that these checks are also performed on a regular basis after receipt and installation. (See section 4.1)
- The merchant or acquirer must check the firmware version. (See section 2.3.2)
- The merchant or acquirer must check the hardware version number. (See section 2.3.1)

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 behaviour of individuals that have access to the terminal.

3.2 Installation

An Installation guide [9] 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.

The allowed installation height must ensure a sufficient view on the ICC card slot entry area (see Figure 4).

3.3 Environmental Conditions

The environmental conditions to operate the device are specified in the Installation guide [9].

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

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.

The security guidance [10] and [11] describe how protocols and services must be used/configured for each interface that is available on the platform.

3.5 Configuration Settings

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

4 Operation and Maintenance

4.1 Periodic Inspection

Information about periodic inspection is specified in the Installation guide [9].

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 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 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.

Especially check if the ICC reader slot is damaged, such as abrasion, painting and other machining marks, and if there is any suspicious object like lead wire over ICC reader slot, or any unknown object inside IC card. If you find these suspicious circumstances, please stop using the device immediately and contact the customer service to confirm if the device has been tampered.

Figure 4 - Card slot

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). These tests are not initiated by an operator. They include:

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

4.3 Roles and Responsibilities

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

4.4 Password and Certificates

The device is functional when received by the merchant or acquirer and there are no security sensitive default values (e.g., admin password) that require configuration 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 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 is also described in the Installation guide [9].

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 Privacy Shield

The device is designed to be used in an attended environment and can be equipped with a privacy shield.

It’s recommended that the position of the terminal must be in such a way to make cardholder PIN spying infeasible.

The Installation guide [9] provide 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 this guide.

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

4.7 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 version of distributed.

Both local and remote updates are supported.

Depending on the local acquirer’s policy, the update operations can be local, or remote.

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

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

4.8 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.

5 Security

5.1 Software Development Guidance

When developing IP enabled applications, the developer must abide by the coding rules and best practices described in the documents [10] and [11].

When developing SRED applications, the developer must follow the guidance described in the document [12].

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

5.2 Secure Sockets Layer protocol

The security guidance [11] describes how the SSL must be used/configured.

SSL protocol is inherently weak and should be removed unless required on an interim basis to facilitate interoperability as part of a migration plan.

5.3 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.

5.4 Account Data protection

The device supports account data protection using format-preserving encryption (FPE). The FPE method used are FF3.1.

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.

5.5 Algorithms supported

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

5.6 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	Boot RAM	1
K_Sub_CA1	CA public keys for certificate verification	ECDSA	521	Secure unit	Boot RAM	1
K_EE1_x[3]	CA public keys for certificate verification	ECDSA	521	Secure unit	Boot RAM	1
K_KBPK	Calculation of key encryption and MAC keys (according to ANSI TR-31 and X9.143)	TDES AES	112 168 128 192 256	Secure unit	Enciphered under K_KEK or K_KBPK	31 25 31 25 21
K_KEK	Key encryption key	TDES AES	112 168 128 192 256	Secure unit	Enciphered under K_KEK or K_KBPK	31 25 31 25 21
TDES Data encryption Key	Data encryption, MAC calculation / verification	DES[4] TDES	64 112 168	Secure unit	Enciphered under K_KEK or K_KBPK	42 31 25
AES Data encryption Key	Data encryption	AES	128 192 256	Secure unit	Enciphered under K_KEK or K_KBPK	31 25 21
PIN Encryption Key	PIN encryption	TDES AES	112 168 128 192 256	Secure unit	Enciphered under K_KEK or K_KBPK	31 25 31 25 21
Key Derivation Key	Key derivation	TDES AES	112 168 128 192 256	Secure unit	Enciphered under K_KEK or K_KBPK	31 25 31 25 21
HMAC Key	HMAC calculation / verification	HMAC-SHA256	128	Secure unit	Enciphered under K_KEK or K_KBPK	31
DUKPT2009 - IK	Initial DUKPT Keys	TDES	112	Secure unit	Enciphered under K_KEK or K_KBPK	2
DUKPT2009 - PIN Key	PIN encryption	TDES	112	Secure unit	Derived originally from IK	21
DUKPT2009 – Data Key	Data encryption	TDES	112	Secure unit	Derived originally from IK	21
DUKPT2009 – MAC Key	MAC Calculation / verification	TDES	112	Secure unit	Derived originally from IK	21
DUKPT2017 – IK	Initial DUKPT Keys	AES	128 192 256	Secure unit	Enciphered under K_KEK or K_KBPK	1

[3] X is a numerical variable

[4] Only used for non-PCI application data

Key Name	Purpose / Usage	Algorithm	Size (Bits)	Storage	Form factor loaded to device In	Number of available Key Slots
DUKPT2017 – PIN Key	PIN encryption	TDES AES	112 168 128 192 256	Secure unit	Derived originally from IK	32
DUKPT2017 – Data Key	Data encryption	TDES AES	112 168 128 192 256	Secure unit	Derived originally from IK	32
DUKPT2017 – MAC Key	MAC calculation / verification	TDES AES	112 168 128 192 256	Secure unit	Derived originally from IK	32
DUKPT2017 – HMAC Key	HMAC calculation / verification	HMAC	128 192 256	Secure unit	Derived originally from IK	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	Randomly generated	31
MC_MAC Key	MAC Generation and verification of MC_ECC_Payment_System PK	TDES	128	Secure unit	Derived from MC_Kernel_ECC private Key	1
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 factory	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
Vendor RSA Signature Key Pair	Signature usage RSA key pair	RSA	2048	Secure unit	Loaded ciphered into Manufacturer Facilities	1
Vendor RSA Encryption Key Pair	Encryption usage RSA key pair	RSA	2048	Secure unit	Loaded ciphered into Manufacturer Facilities	1
RSA Terminal RootCA	Terminal CA public keys for certificate verification	RSA	2048	Secure unit	Loaded into Manufacturer Facilities	1
RSA Terminal SubCA	Terminal SubCA public keys for certificate verification	RSA	2048	Secure unit	Loaded into Manufacturer Facilities	1
RSA Server RootCA	Server CA public keys for certificate verification	RSA	2048	Secure unit	Loaded into Manufacturer Facilities	1
TR34 Session Key	Session key used for TR34 Communication	TDES AES	128 128	Secure unit	Randomly generated	1
TR34 Ephemeral Key	Ephemeral key used for TR34 Communication	TDES AES	112 128	Secure unit	Randomly generated	1
ECDH Key Pair	ECDH Establishment for key Agreement	ECC	256	Secure unit	Randomly generated	1
Application RSA Signature Key Pair	Signature usage RSA key pair	RSA	2048	Secure unit	Randomly generated	1
Application RSA Encryption Key Pair	Encryption usage RSA key pair	RSA	2048	Secure unit	Randomly generated	1

5.7 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 [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].

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

5.8 Key Loading Policy

- The device does not support manual clear key or component entry. Role based security ensures that no security sensitive service functionality is available to the end-user.
- The device supports remote symmetric encrypted key loading. Prior to this, the loading of the Key-Encipherment Key is strictly protected under dual control and split knowledge techniques in a secure room. Such services are managed through dedicated tools, using cryptographic authentication.
- The device supports remote asymmetric key loading.

5.9 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.