Self/4000
PCI PTS Security Policy

EDOCSECU-1489963037-17

Version V8

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 **4**
1_1 Evolution Follow-up 4
2_ Purpose **4**
3_ General Description **5**
3_1 Product Name and Appearance 5
3_2 Product Type 6
3_3 Identification 6
3_3_1 Product Hardware Version 6
3_3_2 Product Software Versions 7
4_ Installation and User Guidance **8**
4_1 Initial Inspection 8
4_2 Installation 8
4_3 Environment Conditions 8
4_4 Communication and Security Protocol 9
4_5 Configuration Settings 9
5_ Operation and Maintenance **9**
5_1 Periodic Inspection 9
5_2 Self-Tests 9
5_3 Roles and Responsibilities 10
5_4 Passwords and Certificates 10
5_5 Tamper Response 10
5_6 Privacy Shield 11
5_7 Patching and Updating 11
5_8 Decommissioning 11
6_ Security **12**

Please check document validity before using

6_1 Software Development Guidance 12
6_2 SSL 12
6_3 Signing 12
6_4 Account Data Protection 12
6_5 Supported Algorithms 12
6_6 Key Table 13
6_7 Key Management 16
6_8 Key Loading Policy 16
6_9 Key Replacement 16

7_ Acronyms 17

8_ References 17

Please check document validity before using

1_Document Information

1_1 Evolution Follow-up

Revision	Type of modification	Date
1	Document Creation	2019/11/28
2	Update	2019/12/26
3	Update	2020/01/20
4	Update	2020/06/22
5	Update	2020/10/21
6	Update	2020/11/12
7	Update	2021/11/15
8	Update	2022/01/25

2_Purpose

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 5.1 approval of the device.

Please check document validity before using

ingenico GROUP

3_General Description

3_1 Product Name and Appearance

The product name shall not be modified by the merchant or covered by a sticker.



Figure 1 - Self/4000

Please check document validity before using

3_2 Product Type

The Self/4000 is an OEM PED device designed to process based payment transaction in an unattended 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 Self/4000 is equipped to handle the following forms of payment:

- EMV chip & PIN,
- Magstripe
- Contactless

It provides a portfolio of connectivity: USB host/device, Ethernet, Network cellular connectivity (Optional), Serial link, Bluetooth (Optional), and Bluetooth Low Energy Beacon (Optional).[1]

3_3 Identification

3_3_1 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.

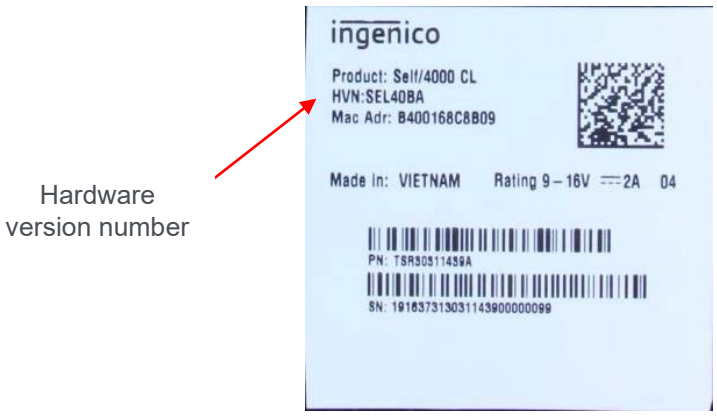


Figure 2 - Self/4000 product hardware identification

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

[1] The use of BLE Beacon interface shall respect guidance document [9]

Please check document validity before using

3_3_2 Product Software Versions

The software versions can be retrieved using the procedure [12].

The following items are displayed (as example):



Figure 1 : Firmware version example

Please check document validity before using

4_Installation and User Guidance

4_1 Initial 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 (see §5.1).

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.

4_2 Installation

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 Environment Conditions

The environmental conditions to operate the device are specified in the installation guide [8].
The minimum installation height for the device is 40cm.
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).

Please check document validity before using

4_4 Communication and Security Protocol

The following protocols and services are available on the device: TLS /SSL[2], IP, DNS, SMTP, POP3, DHCP, HTTP, HTTPS, SNTP, SOCKS, FTP, SFTP, WS/WSS, TCP/UDP, PPP.

The security guidance [9] and [10] describe how protocols and services must be used/configured for each interface that is available on the platform.

4_5 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.

5_Operation and Maintenance

5_1 Periodic Inspection

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 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.

5_2 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

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

Please check document validity before using

5_3 Roles and Responsibilities

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.

5_4 Passwords and Certificates

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.

5_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 (see figure 3).



Figure 2 : Example of tamper message

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.

Please check document validity before using

5_6 Privacy Shield

The device is designed to be used in unattended 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.
The device should be installed such that no cameras have view on the keypad.

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.

5_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 acquirer's application.
For instructions on how to perform these updates, please contact your local helpdesk for applicable procedures.

5_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.

Please check document validity before using

6_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].

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 SSL

The security guidance [10] 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.

6_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.

6_4 Account Data Protection

The device supports account data protection using format-preserving encryption (FPE). The FPE method used is FF3.1 and FF1.
The device supports also account data protection using standard TDES and standard AES.

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

6_5 Supported 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

6_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	ROM	1
K_Sub_CA1	CA public keys for certificate verification	ECDSA	521	Secure unit	ROM	1
K_EE1_x3	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

[3] X is a numerical variable

Please check document validity before using

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	Encipher ed 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	Randoml y generate d	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

Please check document validity before using

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

Figure 4 : Key Table

Please check document validity before using

6_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].

6_8 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.

6_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.

Please check document validity before using

7_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

8_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 Self/4000 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

[12] Self/4000 firmware and hardware recovery

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

Please check document validity before using