PAX IM10

Security Policy

[V1.03]

PAX Computer Technology（Shenzhen）Co.,Ltd.

Contents

1 Purpose

This document is to provide a security policy which addresses basic information for users to use the device in a secure manner, including information on key-management responsibilities, administrative responsibilities, device functionality, identification and environmental requirements.

The use of any method not listed in this security policy will invalidate the PCI PTS POI approval of the device.

2 General Description

The device is approved as SCR product under PCI PTS 5.1 requirement, and designed to process financial transactions in an unattended environment.

The use of the device in an unapproved method will violate the PCI PTS approval of the device.

2.1 Product Name and Appearance

Figure 1 shows the appearance of PAX IM10.

The product name is visible on the label at the back side. The product name shall not be covered by a sticker or modified by merchant.

Figure 1PAX IM10

2.2 Product Type

The device is a SCR terminal designed to process online transactions in an unattended environment.

It provides color display, camera, WIFI, Bluetooth, LAN, USB, RS232 and other interface.

2.3 Product Identification

2.3.1 Hardware Version

Hardware Version:

IM10-xxx-Rx5-0xxx

The “x” is non-security related variables.

The product hardware version is visible on the label at the back side of the device (See figure 2). The label shall not be taken off, altered or covered in any way.

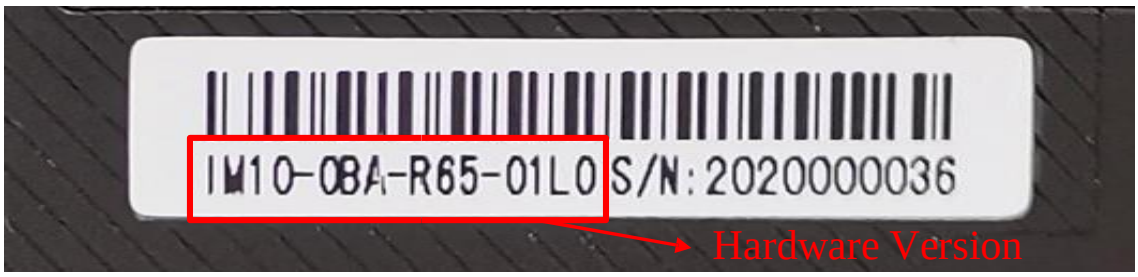

Figure 2 Hardware Identification

2.3.2 Software Version

Software Version:15.00.xx xxxx.

The “x” is non-security related variables.

The version information can be retrieved as below operations.

1. Power on the device.
2. After the application is running, press the red ‘CANCEL’ button to quit application. Then the screen will show system menu information.
3.

1) Select “Terminal Info”, enter the ‘Enter’ button if the screen shows a QR code, and then the version information displays on the screen, including: Serial number (same as the label at the backside of device).
2) Select “Security Info”, and then the version information displays on the screen, including: Firmware version (shown as “SecurityVer” and “Firmware #”).

3 Installation and User Guidance

3.1 Initial Inspection

In order to make sure the product received is exactly the same as what is specified, the acquirer or merchant must check the product according to below tips.

- Only obtain devices from PAX or PAX approved resellers.
- Check the integrity and correctness of devices.
  - Check the label of PAX logo outside the master carton is complete and non-defective.
  - Check the labels of serial number listed on the master carton are non-defective.
  - Check the serial number on each device the same as the one shown on the packing box and master carton.
  - Check the contents in each packing box are the same as the packing list.
  - Package style: one machine into a printed box, then boxes into a master carton.
  - Check whether there is tampered message on the display after power up.

Please refer to [3]PAX White Paper for more details. If additional technical information is needed, please contact our local support team.

3.2 Installation

The terminal must be used in an unattended environment.

3.3 Environmental Conditions

The environmental conditions to operate the device are specified in the below condition.

- Working Environment:

Temperature: -20℃~+70℃(-4℉~158℉)

R.H.: 5%~95% (Non-condensing)

- Storage Environment:

Temperature: -30℃~70℃(-22℉~158℉)

R.H.: 5%~95% (Non-condensing)

- Power supply: DC 5V/12-48V

The security of the device is not compromised by altering the environmental conditions (e.g. place the device outside the stated operating range temperature or operating voltages).

3.4 Configuration Settings

The security functions are an inherent part of firmware functions. No security sensitive configuration settings are necessary to be tuned by the end user in order to meet security requirements.

3.5 Periodic Inspection and Maintenance

Periodic inspection is required every day. Users should check the following items.

- Damaged seal label. The label is damaged and leaves words "VOID" on the device.
- Missing or damaged screws.
- Holes in the device housing that should not existed.
- External wires around the device.
- Missing or unmatched manufacturer barcode label.
- Tamper message on the device display.

If you find any anomalies, which indicate the device may have been opened even tampered, stop using the device immediately and contact your supplier to explain your doubt.

3.6 Roles and Responsibilities

The customers of PAX are acquirer or Value Added Resellers (VAR). We also refer to VAR as acquirer directly. PAX sells devices and provides support for technical issues as well as maintenance to acquirer. The acquirer sells the devices to end users and provides services to their end users. PAX, acquirer and end users play different roles in operating the device. Below table shows different roles and operations:

Table 1 Different roles and responsibilities

	Role	**Responsibilities**
VAR/Acquirer/Merchant	administrator	1.Organize the third party to develop application program;

		2.Download customer public key and application.
End user	operator	Perform transaction
PAX	maintainer	1. Sign customer public key 2. Repair device and unlock the device if tampered

3.7 Passwords and Certificates

There is no security related default value that is necessary to be changed before operating the device.

The device does not include any certificate for testing purpose after being manufactured.

3.8 Decommissioning

Sensitive data and keys must be erased before decommissioning the device and removing it from service permanently. This can be done by rendering the device into tampered status, such as disassemble the device. If just temporary removal, it's not necessary to remove the keys.

4 Hardware Security

4.1 Tamper Response

In the tamper event, the device will turn into the locked status and only tamper message will be displayed on the screen without any other tamper warning. No further secure function can be performed on the device.

Figure 3 Tamper Prompt

If the device is in tampered state, the user must contact the device maintenance or authorized center immediately, remove it from service and keep it away from potential illegal investigation.

4.2 Privacy Shield

Not applicable.

4.3 Removal Detection

The device doesn't equip removal protection, as it provides a complete tamper envelop around all sensitive parts.

5 Software Security

5.1 Self-test

The device employs a self-test to confirm the legality of firmware and software, as well as reinitialize memory.

The device performs self-test during initial start-up and the periodical self-test every 24 hours at least automatically.

The self-test includes:

- Check integrity and authenticity of firmware
- Check integrity and authenticity of application
- Check integrity of keys

If any of the above check fails, the device will be disabled in a secure manner. In this case, please contact the supplier center.

5.2 Patching and Updating

Update and/or patch to the firmware, software and configuration parameters can be installed into the device. And both local and remote update and/or patch downloading are supported.

Any security related update and/or patch loaded into PAX terminals must be signed using certificate. If the signature of the update and/or patch cannot be authenticated, the update and/or patch will be rejected and not be installed.

For the secure operation of the device, it is recommended to use the latest versions of the released firmware and software.

5.3 Software Signing/Authentication

The User Key Management Machine (uKMM) provided by PAX is used to sign User Application. The uKMM administrators perform user private key loading operation and signing process under dual control and split knowledge.

Only the application codes that have been authorized for release should be signed.

Application update uses in combination with bits for authentication and signature verification.

Application is verified by the firmware before it is loaded and executed. If the verification fails, application can't be loaded into device and executed. The signature and verification mechanism ensures the authenticity and integrity of the application that is loaded into device.

5.4 Software Development Guidance

PAX provides software programming guide to developers to develop applications compliant with PCI security requirement. Please refer to [5] Secure Application Development Guide when developing SRED applications and IP enabled applications. The device does not allow unauthorized or unnecessary function.

5.5 Account Data Protection

The device always provides SRED functionality and doesn't support the disablement (turning off) of SRED functionality.

For the SRED module, account data can be encrypted by TDES/ encryption. The device supports account data protection by using format-preserving encryption (FPE) with FF1 mode.

The firmware of device doesn't support white listing for the pass-through of clear-text account data. For more details, please refer to [5] Secure Application Development Guide.

6 Key Management

6.1 Algorithms Supported

The device supports the following algorithms:

- Triple DEA(128 bits and 192 bits)

6.2 Key Management

The device supports the following key management schemes:

- Master/Session key(TDEA)
- Fixed key(TDEA)
- DUKPT(TDEA)

The use of the POI with unapproved key management systems may result in incompliance with PCI PTS POI security requirement.

6.3 Key Table

Table 3 Symmetric Key

Key name	Size(bytes)	Algorithm	Usage
Terminal Loading Key	16/24	TDEA	To load encrypted master keys and session keys
Master Key	16/24	TDEA	To load encrypted session keys
MACKey	16/24	TDEA	MACCalculation
Data Key	16/24	TDEA	Data encryption
Account Data Encryption Key	16(DUKPT) 24(MK/SK)	TDEA	Account data encryption
FPE key	16	AES	Account data encryption

6.4 Key Loading

The terminal does not support manual cryptographic key entry.

The terminal supports local key injection by using a key loader tool under dual control and split knowledge in a secure environment. A secure application is loaded into device to

implement the key loading protocol in the secure environment. After finishing key loading, the application is removed.

The terminal also supports remote key injection after mutual authentication.

6.5 Key Replacement

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

7 Communication

The terminal supports Ethernet, WIFI and Bluetooth communication for transactions.

The terminal supports Bluetooth v5.0 for Bluetooth security communication.

The terminal supports USB communication.

The terminal supports TLS v1.2 security protocol for TCP/IP security communication, including WIFI and Ethernet. Mutual authentication is provided by TLS v1.2.

Appendix

Acronyms

Abbreviation	Description
PIN	Personal Identification Number
TDES	Triple Data Encryption Standard
DUKPT	Derived Unique Key per Transaction

References

[1] ANS X9.24 – 1:2009, Retail Financial Services Symmetric Key Management Part 1: Using Symmetric Techniques
[2] ANS X9.24 Part 2: 2006, Retail Financial Services Symmetric Key Management Part 2: Using Asymmetric Techniques for the Distribution of Symmetric Keys
[3] PAX White Paper.pdf
[4] PAX TermAssist Operating Guide.pdf
[5] Secure Application Development Guide.pdf