PAX A77

Security Policy

[V1.20]

PAX Computer Technology（Shenzhen）Co.,Ltd.

Contents

1 Purpose

This document is intended to provide guidance for users on how to use the device in a secure manner, including information on key-management responsibilities, administrative responsibilities, device functionality, identification and environmental requirements.

Any deviation from the approved use of the device will invalidate the PCI PTS POI v6.0 approval.

2 General Description

2.1 Product Model Name and Appearance

Figure 1 below shows the appearance of the PAX A77.

The product model name is visible both on the front of the device and on the label on the backside of the device. The product name shall not be covered by a sticker or modified in any way.

Figure 1 PAX A77 Appearance

Figure 2 PAX A77 Label

2.2 Product Type

The device is approved as a handheld PED product under PCI PTS POI v6.0 requirement, and designed to process online and offline financial transactions in an attended environment.

It provides display, touch screen (for PIN Entry), contact IC card reader (ICCR), contactless IC card reader, magnetic stripe reader (MSR), camera, barcode scanner, SAM card slot, SD card, cellular (SIM, eSIM), speaker, microphone, buzzer, LAN, Wi-Fi, Bluetooth® wireless technology, BLE Beacons, GPS, USB communications, headphone and power interface.

Use of any method not listed in the policy will invalidate the PCI PTS POI approval of the device.

2.3 Product Identification

2.3.1 Hardware Version

Hardware Version:

A77-xxx-0x6-0xxx (NON-CTLS)

A77-xxx-Rx6-0xxx (CTLS)

A77-xxx-0x6-1xxx (NON-CTLS)

A77-xxx-Rx6-1xxx (CTLS)

A77-1xx-0x6-2xxx (NON-CTLS)

A77-1xx-Rx6-2xxx (CTLS)

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 3). The label shall not be taken off, altered or covered in any way.

Figure 3 Hardware Identification

2.3.2 Software Version

Firmware Version:

26.00.xxxx

26.01.xxxx

26.02.xxxx

The right four “x” represents non-security related changes, such as system UI changed, functional bug fixed, drivers updated, etc.

The version information can be retrieved as below operations.

1. Power on the device.
2. After the system initializing and automatic self-test, the main system menu appears.
3. Swipe up from the bottom of the menu, then find and click "Settings" icon to enter the setting menu.
4. Find and click “About device” menu, then select and enter “SECURITY VERSION” menu. The security version information about the device will appear as follows, including:

- Firmware Version(shown as “Security Ver.”, “Firmware #”)
- Hardware Version (same as the label at the backside of device).

Figure 4 Firmware Version Example

Serial Number:

1. Return to “About device” menu.
2. Find and enter “Device Info” menu, the serial number (shown as ‘Serial number’ and same as the label at the backside of device) is displayed.

3 Installation and User Guidance

3.1 Initial Inspection

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

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

Please refer to [3] 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 attended environment.

The terminal should be kept away from the direct sunlight, high temperature, humidity or dusty places.

The wireless terminal should be kept away from the complex environment of electromagnetic radiation.

The terminal should be checked according to section 3.5 when installing.

3.3 Environmental Conditions

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

- Working Environment:

Temperature: 0℃~+50℃ (32℉~122℉)

R.H.: 5%~96% (Non-condensing)

- Storage Environment:

Temperature: -20℃~70℃ (-4℉~158℉)

R.H.: 5%~96% (Non-condensing)

- Power supply: DC 5.0V / 2.0A
- Environmental protection features:

Temperature sensor: -40±10℃~105±15℃ (-40±18℉~221±27℉)

Voltage sensor: 2.1±0.1V~4.2±0.1V

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

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

Check the device at least once a day, the actual frequency can be adjusted according to the specific situation. Users should check the following items:

- Missing or damaged screws
- Incorrect or redundant keyboard overlays.
- Holes that should not exist in the housing of the device.
- External wires around the device.
- Missing or unmatched manufacturer barcode label.
- Any suspicious objects in or around the IC card slot, refer to the below picture for normal state.

- Any suspicious objects in and around the MSR slot, refer to the below picture for normal state.

- Tamper message on the device display, refer to “Tamper Prompt” in section 4.1.

If any anomalies are found indicating the device may have been opened or tampered, stop using the device immediately and contact the supplier to explain any concern.

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 (for example, maintenance personnel unbind the server, etc.), 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.

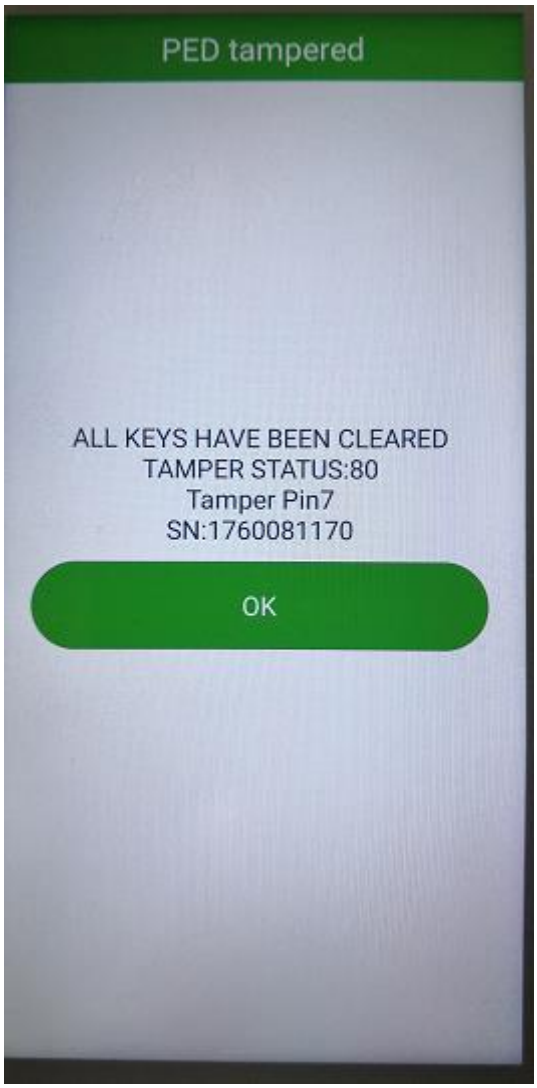

Figure 5 Tamper Prompt

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

The device is designed to be used as a handheld device; therefore, the device does not contain a privacy shield. The device is compliant with the character of a handheld device as required by Appendix A.2 of the DTRs.

It is recommended to enter the PIN in the following ways:

- Make sure the cardholder holds the device on hand during PIN entry.
- Make sure the cardholder keeps a distance from others at the check stand.
- Make sure no video camera is aimed towards the keypad.
- Remind the cardholder to examine if anyone can see the keypad before PIN entry.

5 Software Security

5.1 Self-test

The device employs the start-up self-test and periodic self-test to confirm the legality of the firmware and software, as well as to reinitialize the memory. The self-test includes:

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

If any of the above checks fail, the device will be disabled in a secure manner. In this case, please contact the supplier's service center.

The device provides two periodic restart schemes: 24-hour restart scheme and scheduled restart scheme.

5.1.1 24-hour Restart Scheme

The device performs self-test every time it is turned on. If the device has been running for 24 hours since being turned on, the device will restart, unless there is a delay due to business reasons. The default maximum delay for the device does not exceed 48 hours.

5.1.2 Scheduled Restart Scheme

The device also provides a scheduled restart scheme as an option for users.

The user can schedule a fixed time for the restart, in which case the device will restart at the scheduled time every day, unless there is a delay due to business reasons. The default maximum delay for the device does not exceed 48 hours.

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 RSA 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 SHA-256 in combination with RSA 2048 bits for authentication and signature verification.

Application is verified by the firmware before it is loaded and executed. If the verification fails, application cannot 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 a 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 functions.

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/AES/RSA encryption. The device supports account data protection by using format-preserving encryption (FPE) with AES FF1 mode.

The firmware of the device does not support whitelisting 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 DES (128 bits/192 bits)
- AES (128 bits/192 bits/256 bits)
- RSA (2048 bits)
- SHA-256
- ECC (In support with NIST P-256 and P521)

6.2 Key Management

The device supports the following key management methods:

- Master/Session Key

  This method uses a hierarchy of Terminal Loading Key, Master Key and Session Key. The highest level of Terminal Loading Key is distributed through the key loading device. The Master Key is distributed under the protection of Terminal Loading Key. The Session Key is distributed under the protection of Master Key. These keys can be replaced by the same methods whenever compromise is known or suspected.

- DUKPT

  This method uses a unique key for each transaction, and prevents the disclosure of any past keys used by the transaction-originating device.

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

Table 2 Supported Key Management

Purpose	Supported Key Management
Key Management – PIN encryption	TDES - MK/SK
	TDES - DUKPT
	AES - MK/SK
	AES - DUKPT

Key Management – Account Data Encryption	TDES - MK/SK
	TDES - DUKPT
	AES - MK/SK
	AES - DUKPT
	Format-Preserving Encryption
	RSA

6.3 Key Table

Table 3 RSA public key

Key name	Size (bits)	Algorithm	Usage
User public key (PAX_US_PUK/C_US_PUK)	2048	RSA	Public key for application authentication
Trans-Armor public key	2048	RSA	Account data encryption
CA_ROOT	2048	RSA	Root certificate of CA.
CA_PUK	2048	RSA	Used for verification of the device, LKI or RKI certificates.
DA_PVK / DA_PUK	2048	RSA	Used for authentication of the device by RKI server.
DE_PVK / DE_PUK	2048	RSA	Used to protect sensitive information during remote key injection.
RKIAK_PUK	2048	RSA	Used for authentication between RKI server and the device during remote key injection procedure.

Table 4 Symmetric Key

Key name	Size(bytes)	Algorithm	Purpose/Usage
Master Key (TMK)	16/24 (TDES) 16/24/32 (AES)	TDES/AES	To load encrypted session keys and encrypted DUKPT Initial keys.
DUKPT Initial Key (TIK)	16 (TDES) 16/24/32 (AES)	TDES/AES	DUKPT Initial Key
PIN Key (TPK)	16/24 (TDES MK/SK) 16 (TDES DUKPT)	TDES/AES	PIN encryption for PINBLOCK format 0,1,3 under TDES algorithm;

	16/24/32 (AES MK/SK) 16/24/32 (AES DUKPT)		PIN encryption for PINBLOCK format 4 under AES algorithm.
MAC Key (TAK)	16/24 (TDES MK/SK) 16 (TDES DUKPT) 16/24/32 (AES MK/SK) 16/24/32 (AES DUKPT)	TDES/AES	MAC Calculation
Account Data Encryption Key (TCHDK)	24 (TDES MK/SK) 16 (TDES DUKPT) 16/24/32 (AES MK/SK) 16/24/32 (AES DUKPT)	TDES/AES	Account Data Encryption
Data Key (TDK)	16/24 (TDES MK/SK) 16 (TDES DUKPT) 16/24/32 (AES MK/SK) 16/24/32 (AES DUKPT)	TDES/AES	Arbitrary Data Encryption
FPE key	16	AES	Account Data Encryption under Voltage FPE scheme

6.4 Key Loading

The terminal does not support manual cryptographic key entry.

The terminal supports local initial plaintext key injection by using a key loader tool under dual control and split knowledge in a secure environment.

The terminal supports local ciphertext key injection by using a key loader tool or application.

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 device supports the communications methods and protocols listed below. Use of any method not listed here invalidates the PCI PTS POI approval of the device.

7.1 Communication Interfaces

The following communication interfaces are available in the device:

- Cellular (2G/3G/4G, PPP, TCP/IP, UDP, ICMP and TLSv1.2/TLSv1.3)
- Wi-Fi (802.11 b/g/n, ARP, DHCP, TCP/IP, UDP, ICMP and TLSv1.2/TLSv1.3)
- Bluetooth v5.0 BR/EDR, BLE
- USB and USB-to-serial

7.2 Communication Protocols and Services

The following protocols and services are supported for TCP/IP communications by the device:

- IP (IPv4, IPv6)
- ICMP, TCP, UDP
- PPP, ARP
- TLS (TLSv1.2 and TLSv1.3)

For more details, please refer to [4].

7.3 Bluetooth Security Guidance

The terminal supports Bluetooth secure communications:

- BTv5.0 for BR/EDR in Security Mode 4 Level 4;
- BTv5.0 for BLE in Security Mode 1 Level 4;
- Just works cannot be used at any time

In addition, where the device communicates with Bluetooth BR/EDR 2.1 through 4.0 peripheral devices, it falls back to Security Mode 4 Level 3.

Appendix

Acronyms

Abbreviation	Description
PIN	Personal Identification Number
RSA	Rivest Shamir Adelman Algorithm
SHA	Secure Hash Algorithm
TDES	Triple Data Encryption Standard

AES	Advanced Encryption Standard
DUKPT	Derived Unique Key per Transaction

References

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