PAX A6630

Security Policy

[V1.10]

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 v6.2 approval.

2 General Description

2.1 Product Name and Appearance

Figure 1 shows the appearance of PAX A6630.

The product name is visible both on the front view of the device and on the label at the back side. The product name shall not be covered by a sticker or modified by merchant.

Figure 1 PAX A6630 Appearance

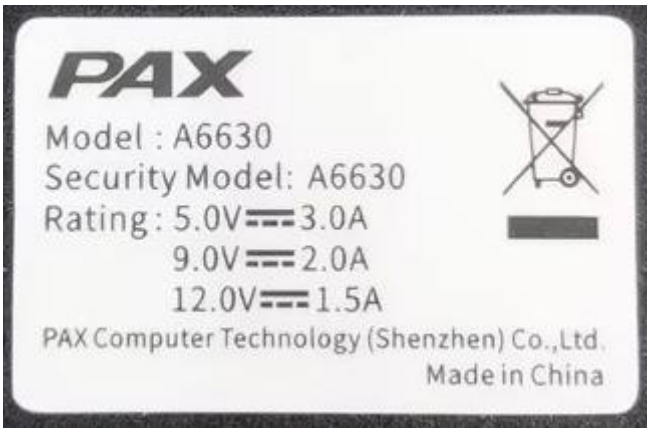

Figure 2 PAX A6630 Model Name

2.2 Product Type

The device is approved as a handheld PED product under PCI PTS POI v6.2 requirements, and designed to process online and offline financial transactions in an attended environment.

It provides LCD display, touch screen (for PIN entry), IC card reader (ICCR), MSR, Contactless card reader, cameras, Barcode scanner, SIM card slot, eSIM module, Speaker, GPS, Cellular, Wi-Fi, Bluetooth® wireless technology, SD/SAM card reader, USB communications, 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:

A6630-0xx-Rx6-0xxx

A6630-0xx-Rx6-1xxx

A6630-0xx-Rx6-2xxx

The first five positions represent the model name.

The “x” is non-security related variables.

Position "8","9" indicate the communication method supported by the device.

Position "12" represents memory capacity.

Position "16" represents the different custom code.

Position "17" represents the different packaging materials.

Position "18" represents the different power cable.

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.xx xxxxx

26.01.xx xxxxx

The right seven “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. 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 “Firmware #”)
- Hardware Version (same as the label at the backside of device).

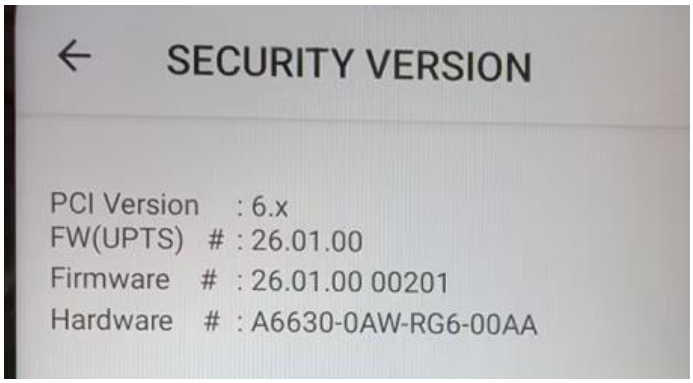

Figure 4 Device Version Information Example

Serial Number:

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

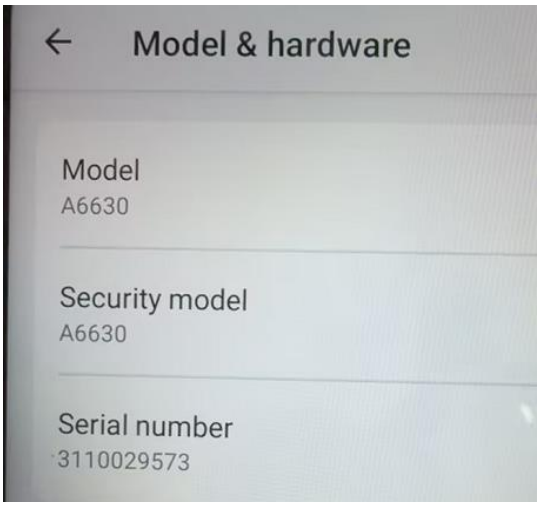

Figure 5 Serial Number Example

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] 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 for installation.

3.3 Environmental Conditions

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

- Working Environment:

Temperature: -10℃~+50℃ (14℉~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 / 3.0A
  DC 9.0V / 2.0A
  DC 12.0V/1.5A

- Environmental protection features:

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

Temperature sensor: -40℃±5℃~105±10℃ (-40±9℉~221±18℉)

Voltage sensor: 2.1±0.1V~4.2±0.1V

If the device is placed in an environment of which condition listed above is not satisfied, the device is tampered, and all sensitive information is erased.

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.

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

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

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

If any anomalies are found, 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 application and request certificate from vendor.
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

No security related default value exists.

The device does not come with any certificates for testing purposes after being manufactured.

3.8 Decommissioning

Sensitive data and keys must be erased before the device is decommissioned and removed from service permanently. This can be done by rendering the device into tampered status, such as by disassembling the device. In the case of temporary removal (e.g., maintenance personnel unbind the server, etc.), it is 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 the tamper message will be displayed on the screen without any other tamper warning, as shown in the figure below. No further secure functions can be performed on the device.

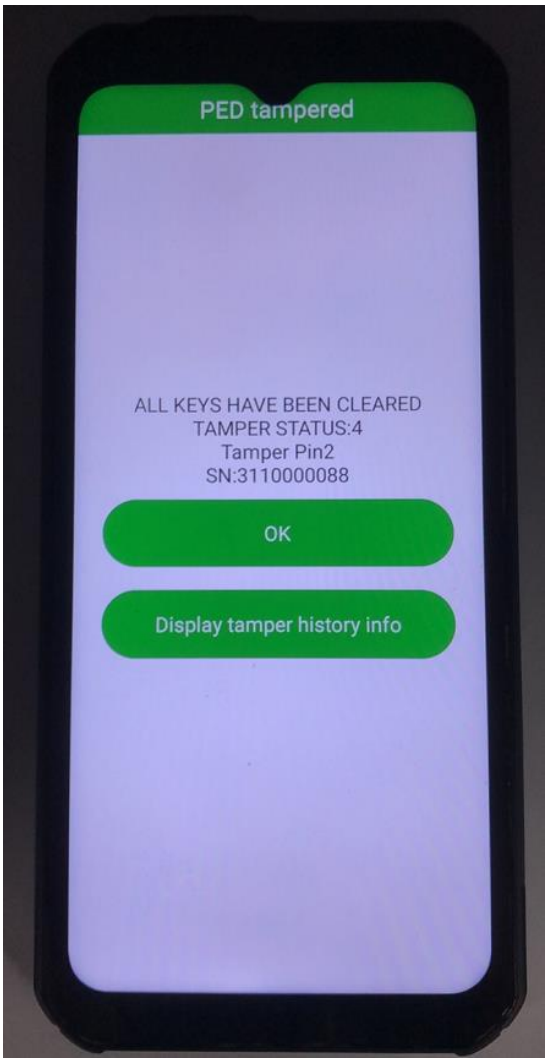

Figure 6 Tamper Prompt

If the device is in tampered status, the user must immediately contact the device maintenance or authorized service center and remove the device from service.

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 characteristics of a handheld device as required by Appendix A.2 of the DTR.

It is recommended to enter password as following ways:

- Make sure the cardholder holds the device on hand during PIN entry.
- Make sure the cardholder keeps a distance from others on check stand.
- Through guidance message or logos to indicate user to use his body or free hand to block the view of keypad.
- Make sure no video camera towards the keypad.
- Remind the cardholder to examine if anyone spies the keypad before PIN entry.

The following table shows the combination of methods that could be used when installing the terminal to protect the cardholder's PIN during PIN entry.

Table 2 combination of methods to protect PIN entry

Methods	Observation Corridors				
	Cashier	Customers in Queue	Customers Elsewhere	On-Site Cameras	Remote Cameras
With stand	No action needed	Customer positions terminal	No action needed.	Out of sight of the camera	Out of sight of the camera
Without stand	Block the view of cashier by body	Block the view of other customers by body	Block the view of other customers by body	Out of sight of the camera	Out of sight of the camera
Customer Instruction	Remind the customer to shield PIN	Keep a distance	Keep a distance	Out of sight of the camera	Out of sight of the camera

5 Software Security

Software security includes self-test, patching/updating and software signing. The device does not allow unauthorized or unnecessary functions.

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

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

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

5.1.1 24-hour Restart Scheme

The device performs a 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. The device supports local update through USB. The device supports remote update through Wi-Fi or Cellular.

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 Singing/Authentications

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 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 function compliant with PCI security requirement. Please refer to [4] when developing SRED function and OP function.

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 device doesn't support the pass-through of clear-text account data using techniques such as whitelisting. For more details, please refer to [4].

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 (256/512 bits)
- ECC (In support with NIST P-256, P-384 and P-521)

6.2 Key Management

The device supports the following key management methods:

- Master/Session Key

  This method uses a hierarchy of Master Key and Session Key.

- DUKPT

  This method uses a unique key for each transaction.

Use of the device with different key-management systems will invalidate the PCI PTS POI approval of the device.

Table 3 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

Purpose	Supported Key Management
	AES - DUKPT
	Format-Preserving Encryption
	RSA

6.3 Key Table

Table 4 RSA Public Key

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

Table 5 Symmetric Key

Key name	Purpose/Usage	Algorithm	Size(bytes)
Master Key (TMK)	To load encrypted session keys	TDES	16/24
		AES	16/24/32
DUKPT Initial Key (TIK)	DUKPT Initial Key, used to generate DUKPT future keys	TDES	16
		AES	16/24/32
DUKPT Future Key	DUKPT Encryption Keys, used for PIN encryption, Account data encryption and MAC calculation	TDES	16
		AES	16/24/32

Key name	Purpose/Usage	Algorithm	Size(bytes)
PIN Key (TPK)	PIN encryption for PINBLOCK format 0,1,3 under TDES algorithm; PIN encryption for PINBLOCK format 4 under AES algorithm.	TDES	16/24
		AES	16/24/32
MAC Key (TAK)	MAC Calculation	TDES	16/24
		AES	16/24/32
Account Data Encryption Key (TCHDK)	Account Data Encryption	TDES	24
		AES	16/24/32
Data Key (TDK)	Arbitrary Data Encryption	TDES	16/24
		AES	16/24/32
FPE Key	Account Data Encryption under Voltage FPE scheme	AES	16

6.4 Key Loading

The terminal supports the following key loading methods:

- Clear-text key injection;
- Symmetric encrypted keys;
- Remote key loading using asymmetric technique;
- Local key loading using asymmetric technique.

The terminal supports clear-text key injection by using a key loader tool under dual control and split knowledge in a secure environment.

6.5 Key Replacement

Whenever it is known or suspected that a key has been compromised, and whenever it is considered feasible to determine the timing of the key using the exhaustive method, the key must be deleted or replaced with a new one.

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 (TLSv1.2/TLSv1.3, SCTP, TCP, UDP, DHCP, ICMP, IP and PPP)
- Wi-Fi (TLSv1.2/TLSv1.3, SCTP, TCP, UDP, DHCP, ICMP, IP and ARP)
- Bluetooth v5.2 BR/EDR, BLE
- USB

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:

- BTv5.2 for BR/EDR in Security Mode 4 Level 4;
- BTv5.2 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] Secure Application Development Guide.pdf