PAX A50

Security Policy

[V1.05]

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

2.1 Product Name and Appearance

Figure 1 shows the appearance of PAX A50.

The product name is visible both on the front view of the device and on the label at the back side (See Figure 1 and Figure 2). The product name shall not be covered by a sticker or modified by merchant.

Figure 1 PAX A50

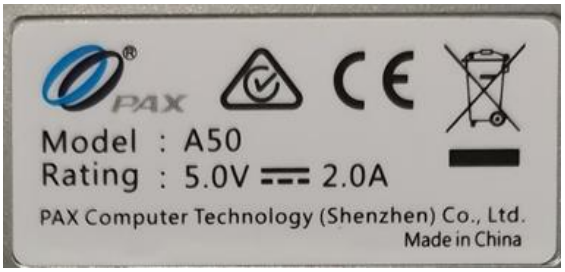

Figure 2 The label of PAX A50

2.2 Product Type

The device is approved as a handheld PED product under PCI PTS 5.1 requirement, and designed to process online and offline financial transactions in an attended environment.

It provides color display, touch screen, PIN entry, IC card reader (ICCR), Contactless reader, camera, cellular, WIFI, Bluetooth, USB communications, headphone and power interface.

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

2.3 Product Identification

2.3.1 Hardware Version

Hardware Version:

A50-xxx-Rx5-0xxx (with CTLS)

A50-xxx-0x5-0xxx (without CTLS)

A50-xxx-Rx5-1xxx (with CTLS)

A50-xxx-0x5-1xxx (without CTLS)

A50-xxx-Rx5-2xxx (with CTLS)

A50-xxx-0x5-2xxx (without CTLS)

The “x” is non-security related variables. Position "5","6","7" indicate the communication method supported by the device. Position "10" is used for product functions. "14","15","16" represents packaging option, customer logo, etc (non security related).

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

Software Version: 25.00.xxxx, 25.01.xxxx.

The right four “x” are non-security related variables, for errors rectification and non-security related function updates.

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 screen appears.
3. Find and click the "Settings" icon to enter the setting menu.
4. Find and click the "System" to enter the system menu.
5. Find and click “About device” menu, then select and enter the “SECURITY VERSION” menu. The security version information about the device is following, including:

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

Serial Number:

1. Return to the “About device” menu.
2. Find and enter the “Status” menu, the serial number (shown as ‘SN’ 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 what 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 list 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 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 detail information. If additional technical information 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 electromagnetic radiation complex environment.

3.3 Environmental Conditions

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

- 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---2A
- 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. setting 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

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

- Damaged seal label.
- Missing or damaged screws.
- Incorrect or redundant touchscreen overlays.
- Holes in the device housing that should not existed.
- External wires around the device.
- Missing or unmatched manufacturer barcode label.
- Any suspicious objects inside or around IC card slot, refer to section 2.1.
- Tamper message on the device display, refer to section 4.1.

If any anomalies you find, 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 to acquirer and provide technique and maintenance supports 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 manufacture.

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. There will be no further secure function can be performed on the device.

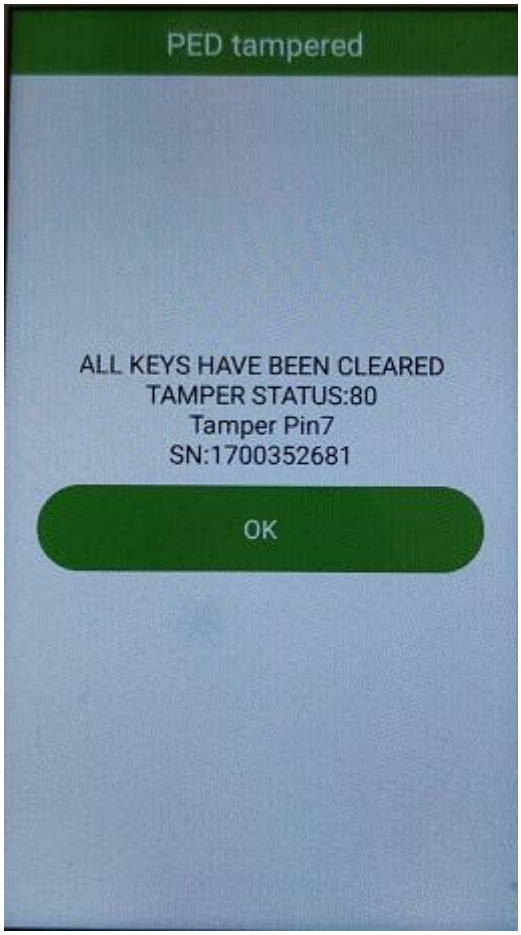

Figure 5 Tamper Prompt

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 on hand therefore the device do not contain a privacy shield. The device is compliant to the character of handheld device as required by Appendix A.2.

It is recommended to enter password as following ways:

- Make sure the cardholder hold the device on hand during PIN entry.
- Make sure the cardholder keeps at 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.
- Warning the cardholder should examine if anyone spies 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

5.1 Self-test

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

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

The self-test includes:

- Check firmware integrity and authenticity
- Check application integrity and authenticity
- Check installed keys' integrity

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, application 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 installed.

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

5.3 Software Signing/Authentication

The User Key Management Machine (uKMM) provided by PAX is used by acquirer 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 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 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.

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 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 and 192 bits)
- AES (128 bits, 192 bits and 256 bits)
- RSA (2048 bits)
- SHA-256
- ECC (NIST P-256 and P-521)

6.2 Key Management

The device supports the following key management schemes:

- Master/Session key (TDES)

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

- DUKPT (TDES, AES)

  This method uses a unique key for each transaction.

Use of the POI with unapproved key management systems will result in an incompliant with PCI PTS POI security requirement.

6.3 Key Table

Table 3 Asymmetric 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
IBE public key in Voltage encryption mechanism	3072	IBE	Used to wrap the FPE base key to create a Key Transfer Block.
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
Terminal Loading Key (TLK)	16/24 (TDES) 16/24/32 (AES)	TDES/AES	To load encrypted master keys
DUKPT Initial Key (TIK)	16 (TDES) 16/24/32 (AES)	TDES/AES	DUKPT Initial Key
Master Key (TMK)	16/24 (TDES) 16/24/32 (AES)	TDES/AES	To load encrypted session keys
PIN Key (TPK)	16/24 (TDES MK/SK) 16 (TDES DUKPT) 16/24/32 (AES MK/SK) 16/24/32 (AES DUKPT)	TDES/AES	PIN encryption for PINBLOCK format 0,1,3 under TDES algorithm; 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 key injection using a key loader tool under dual control and split knowledge in a secure environment.

The terminal also supports remote key injection after mutual authentication.

6.5 Key Replacement

Whenever compromise of the key is suspected or known 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 Cellular, WIFI and Bluetooth communications for transactions.

The terminal supports USB communication.

The terminal supports Bluetooth v4.0 and Bluetooth secure connection (Bluetooth BR/EDR in mode 4 level 3).

The terminal supports TLS v1.2 and TLSv1.3 security protocol for TCP/IP security communication, including WIFI and cellular. Mutual authentication is provided by TLS v1.2 and TLS v1.3.

Use of any method not listed in the policy invalidates the device approval.

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 - 1:2009, 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] PayDroid Tool Operating Guide.pdf
[5] Secure Application Development Guide.pdf