PAX A930

Security Policy

[V1.01]

PAX Computer Technology（Shenzhen）Co.,Ltd.

Contents

1 Purpose ... 1
2 General Description ... 2
2.1 Product Name and Appearance ... 2
2.2 Product Type ... 2
2.3 Product Identification ... 3
2.3.1 Hardware Version ... 3
2.3.2 Software Version ... 4
3 Installation and User Guidance ... 5
3.1 Initial Inspection ... 5
3.2 Installation ... 5
3.3 Environmental Conditions ... 5
3.4 Configuration Settings ... 6
3.5 Periodic Inspection and Maintenance ... 6
3.6 Roles and Responsibilities ... 7
3.7 Passwords and Certificates ... 7
3.8 Decommissioning ... 7
4 Hardware Security ... 8
4.1 Tamper Response ... 8
4.2 Privacy Shield ... 8
5 Software Security ... 10
5.1 Self-test ... 10
5.2 Patching and Updating ... 10
5.3 Software Signing/Authentication ... 11
5.4 Software Development Guidance ... 11
5.5 Account Data Protection ... 11
6 Key Management ... 12
6.1 Algorithms Supported ... 12
6.2 Key Management ... 12

6.3 Key Table 13

6.4 Key Loading 14

6.5 Key Replacement 15

7 Communication 16

Appendix 17

Acronyms 17

References 17

1 Purpose

This document is to provide guidance 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 v6.0 approval of the device.

2 General Description

2.1 Product Name and Appearance

Figure 1 shows the appearance of PAX A930.

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.

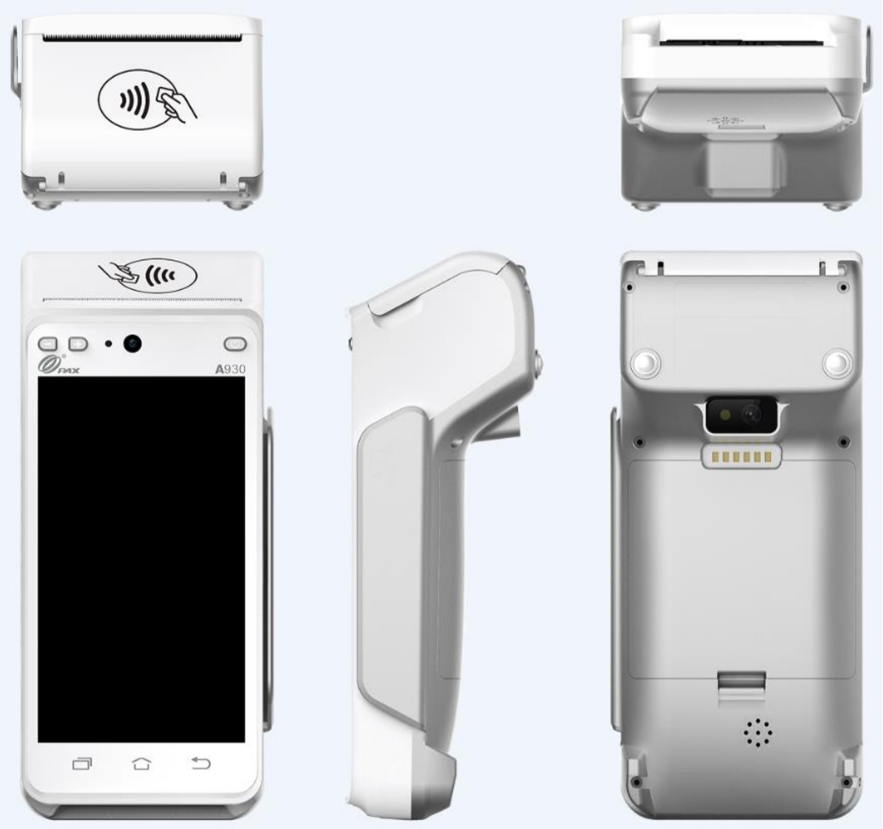


Figure 1 PAX A930 Appearance

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 color display, touch screen, PIN entry, IC card reader (ICCR), MSR, Contactless card reader, printer, camera, headphone, cellular, WIFI, Bluetooth® wireless technology and BLE, UART,USB communications and power interface.

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

The Bluetooth® word mark and logos are registered trademarks owned by Bluetooth SIG, Inc. and any use of such marks by PAX Technology Limited is under license. Other trademarks and trade names are those of their respective owners.

2.3 Product Identification

2.3.1 Hardware Version

Hardware Version:

A930-xxx-0x6-0xxx (without CTLS)

A930-xxx-Rx6-0xxx (with 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 2). The label shall not be taken off, altered or covered in any way.

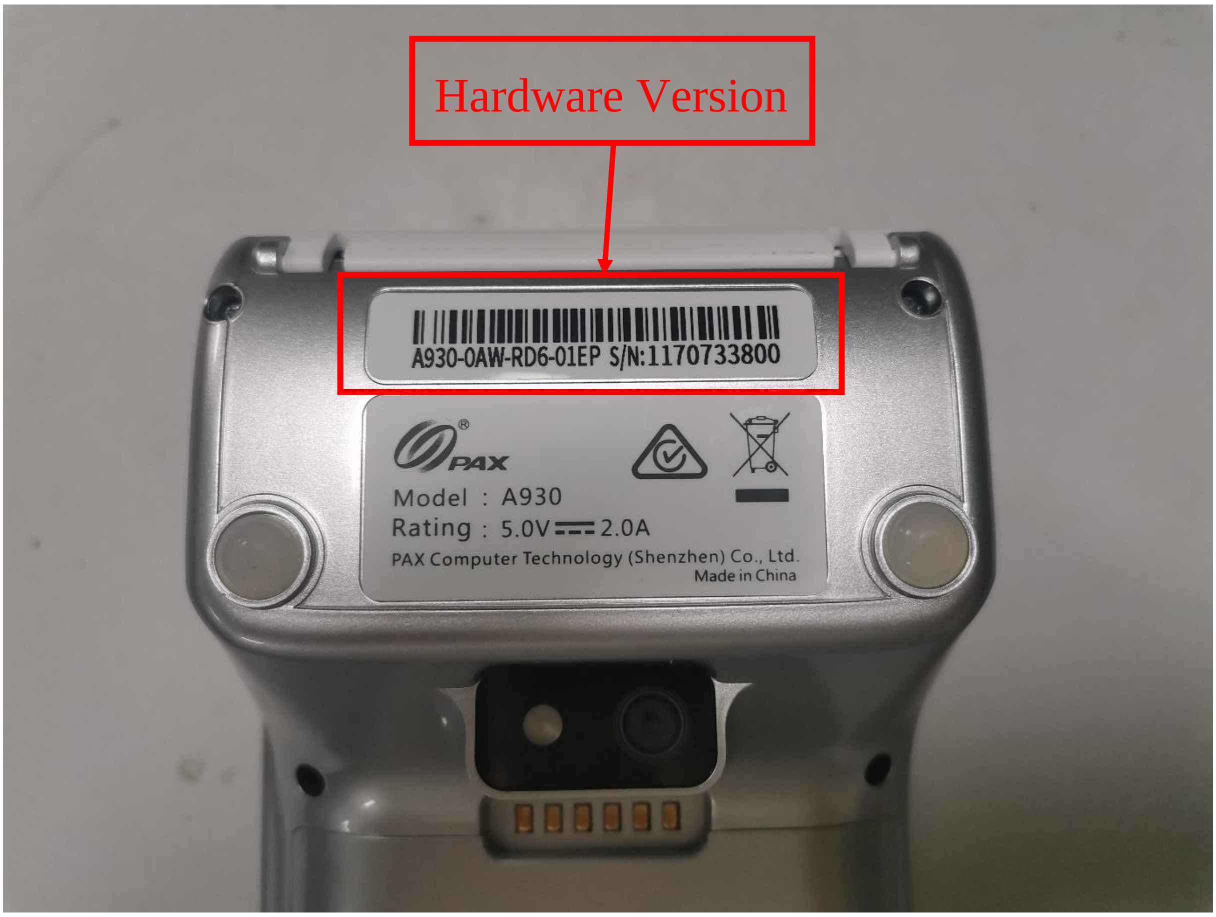

Hardware Version
A930-0AW-RD6-01EP S/N:1170733800
PAX
Model : A930
Rating : 5.0V 2.0A
PAX Computer Technology (Shenzhen) Co., Ltd.
Made in China

Figure 2 Hardware Identification

2.3.2 Software Version

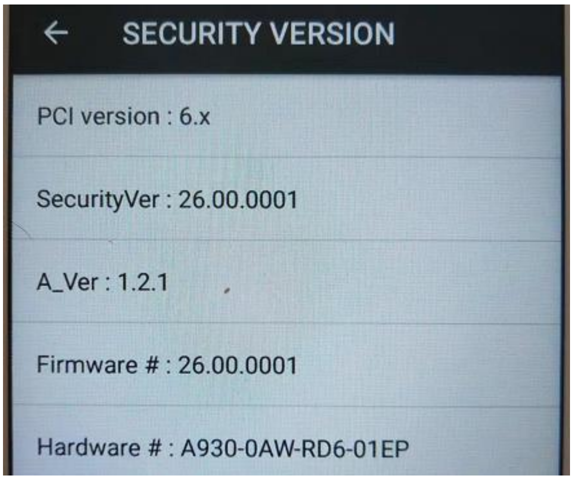
Firmware Version: 26.00.xxxx.

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



SECURITY VERSION

PCI version : 6.x

SecurityVer : 26.00.0001

A_Ver : 1.2.1

Firmware # : 26.00.0001

Hardware # : A930-0AW-RD6-01EP

Figure 3: Firmware Version Example

Serial Number:

1. Return to “About device” menu.
2. Find and enter “Status” 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 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 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 installation.

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 / 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 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.

- Missing or damaged screws.
- Incorrect or redundant 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 section 2.1.
- Any suspicious objects internal and around MSR slot, refer to section 2.1.
- Tamper message on the device display, refer to “Tamper Prompt” in section 4.1.

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.

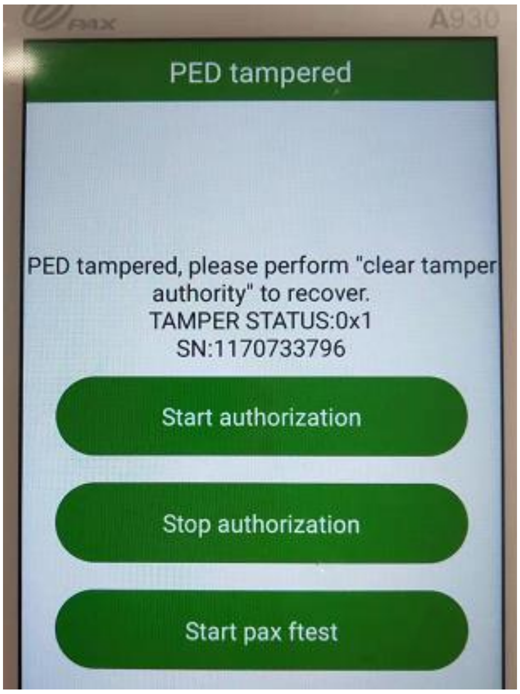
3.8 Decommissioning

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 (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.



PED tampered

PED tampered, please perform "clear tamper authority" to recover.
TAMPER STATUS:0x1
SN:1170733796

Figure 4 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 terminal and the device does not contain a privacy shield. The device is compliant to the character of handheld device as required by Appendix A.2.

The cardholder should guided during PIN entry in the following way:

- Make sure the cardholder hold 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.

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 at least every 24 hours automatically.

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.

5.2 Patching and Updating

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

Local firmware/patch update uses **PAX PayDroid Tool** to perform firmware upgrade on a local PC device, refer to [4] for more details.

Remote firmware/patch updates follow the instruction below:

a) Find and click "Settings" icon to enter the setting menu.
b) Please input the Password provided by PAX.
c) Navigate to “Software Update” menu, press to enter
d) Press “Check Update” to check for the latest firmware updates.

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 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 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 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, 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 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	**Usage**	**Algorithm**	**Size (bits)**
User public key (PAX_US_PUK/C_US_PUK)	Public key for application authentication	RSA	2048
Trans-Armor public key	Account data encryption	RSA	2048
CA_ROOT	Root certificate of CA.	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 4 Symmetric Key

Key name	Purpose/Usage	Algorithm	Size(bytes)
Terminal Loading Key (TLK)	To load encrypted master 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	TDES	16
		AES	16/24/32
Master Key (TMK)	To load encrypted session keys	TDES	16/24
		AES	16/24/32
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 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 terminal supports cellular, WIFI, Bluetooth and BLE secure communications for transactions, please refer to [5] Secure Application Development Guide for more information.

The terminal supports USB communication.

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

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