PAX A910S_A910S-X

Security Policy

[V1.51]

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 v6.1 approval.

2 General Description

2.1 Product Name and Appearance

Figure 1 show the appearance of PAX A910S and A910S-X.

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 A910S Appearance

Figure 2 A910S-X Appearance

Figure 3 PAX A910S Model Name

Figure 4 PAX A910S-X Model Name

2.2 Product Type

The device is approved as a handheld PED product under PCI PTS POI v6.1 requirements, and it is 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 card reader, magnetic stripe reader (MSR), camera, SAM card slot, SD card, printer, cellular (SIM, eSIM), speaker, buzzer, TF card slot, Microphone, fingerprint, tax module, Wi-Fi, Bluetooth® wireless technology, BLE, GPS and USB communication 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 Versions:

A910S-0xx-Rx6-0xxx (CTLS)	A910S-0xx-0x6-0xxx (NON-CTLS)
A910S-0xx-Rx6-1xxx (CTLS)	A910S-0xx-0x6-1xxx (NON-CTLS)
A910S-0xx-Rx6-2xxx (CTLS)	A910S-0xx-0x6-2xxx (NON-CTLS)
A910S-0xx-Rx6-3xxx (CTLS)	A910S-0xx-0x6-3xxx (NON-CTLS)
A910S-0xx-Rx6-4xxx (CTLS)	A910S-0xx-0x6-4xxx (NON-CTLS)
A910S-0xx-Rx6-5xxx (CTLS)	A910S-0xx-0x6-5xxx (NON-CTLS)
A910S-1xx-Rx6-6xxx (CTLS)	A910S-1xx-0x6-6xxx (NON-CTLS)
A910S-1xx-Rx6-7xxx (CTLS)	A910S-1xx-0x6-7xxx (NON-CTLS)
A910S-1xx-Rx6-8xxx (CTLS)	A910S-1xx-0x6-8xxx (NON-CTLS)
A910S-0xx-Rx6-9xxx (CTLS)	A910S-0xx-0x6-9xxx (NON-CTLS)

The “x” is non-security related variables.

- The 8th and 9th "x" indicate the communication method supported by the device.
- The 12th "x" represents memory capacity.
- The 16th "x" represents the different custom code.
- The 17th "x" represents the different packaging materials.
- The 18th "x" represents the different power cable.

The product hardware version is visible on the label on the backside of the device (see figure 3). The label shall not be removed, modified or covered in any way.

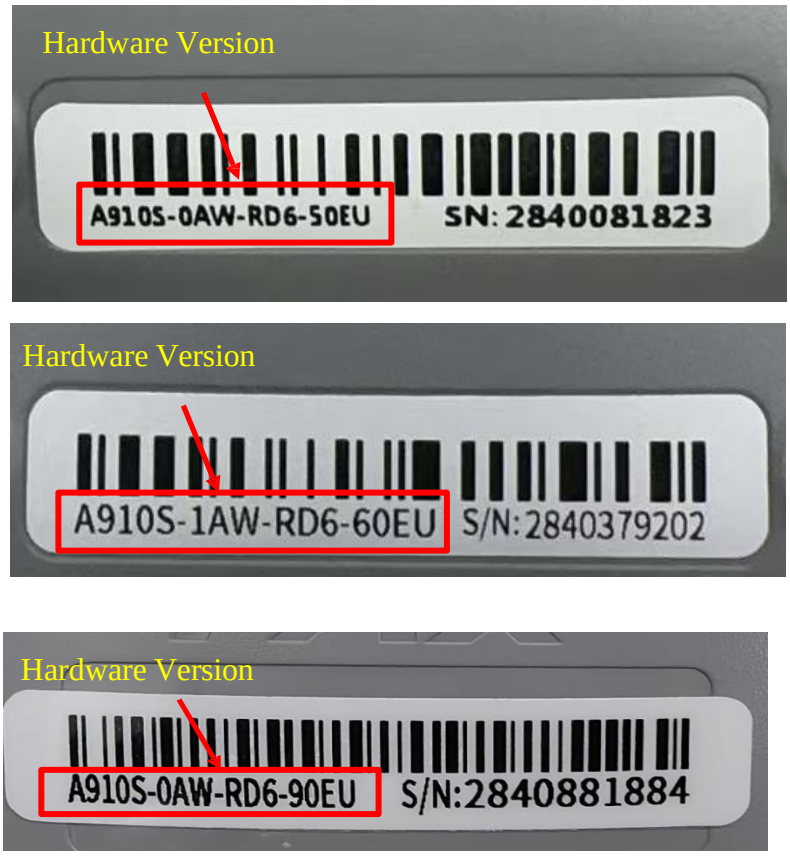

Figure 5 Hardware Identification

2.3.2 Software Version

Firmware Version:

26.00.xx xxxxx

26.01.xx xxxxx

26.02.xx xxxxx

26.03.xx xxxxx

26.04.xx xxxxx

26.05.xx xxxxx

26.06.xx xxxxx

26.07.xx xxxxx

The seven “x”s on the right side represent non-security related changes, such as system UI changes, functional bug fixes, driver updates, etc.

The version information can be retrieved by performing the operations below.

1. Power on the device.
2. After system initialization and automatic self-test, the main screen appears.
3. Find and click "Settings" icon to enter the setting menu.
4. Find and click the “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 on the backside of the device)

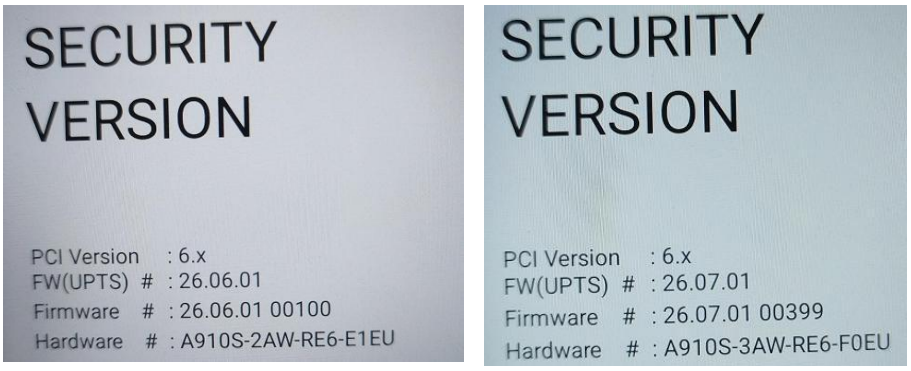

Figure 6: Version Information Example

Serial Number:

1. Return to the “About device” menu.

2. Find and enter “Model & hardware” 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 purchase devices from PAX or PAX authorized resellers.
- Check the integrity and correctness of the devices.
  - Check that the PAX logo labels on the outside of the master carton is 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 are 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, high 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 installed.

3.3 Environmental Conditions

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

- Working Environment:
  - Temperature: 0℃~45℃ (32℉~113℉)

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

- Storage Environment:
  - Temperature: -20℃~70℃ (-4℉~158℉)
  - R.H.: 5%~95% (Non-condensing)
- Power supply: DC 5.0V / 2A
- Environmental protection features:
  - Temperature sensor: -40±10℃~105±15℃ (-40±15℉~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. placing the device outside of the stated operating temperature ranges or the operating voltages do 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 adjusted by the end user in order to meet security requirements.

3.5 Periodic Inspection and Maintenance

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

- Missing or damaged screws
- Incorrect or redundant keypad 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 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 “4.1 Tamper Prompt”

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 referred to as the Acquirer or Value Added Resellers (VAR). PAX also refers to VAR directly as the Acquirer. PAX sells devices and provides technical support as well as maintenance to the Acquirer. The Acquirer sells the devices to the end users and provides services to their end users. PAX, the Acquirer and the End Users play different roles in the operation of the device. The table below 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 is existed.

The device does not come with any certificates for testing purpose 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 show in the figure below. No further secure functions can be performed on the device.

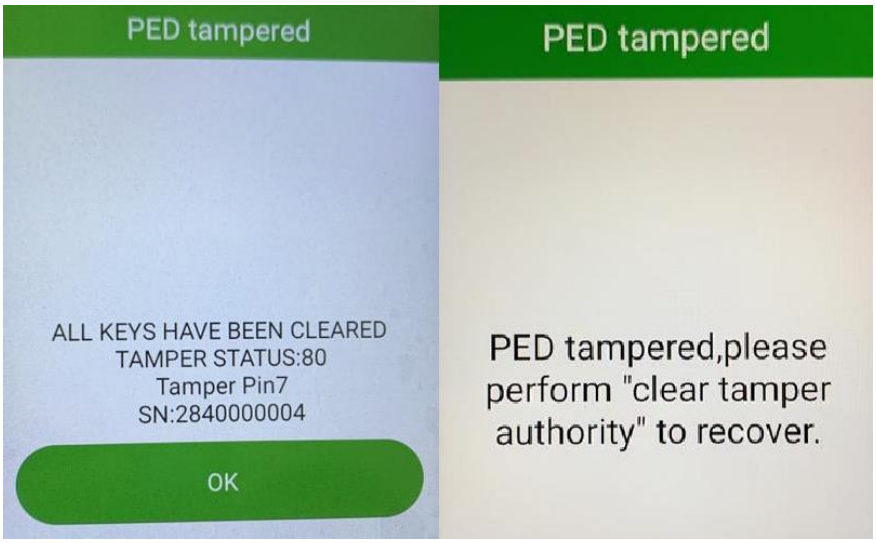

Figure 7 Tamper Prompt

If the device is in tampered state, 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 character of a handheld device as required by Appendix A.2 of the DTR.

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.
- 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 is aimed towards the device touch screen.
- Remind the cardholder to examine if anyone spies the device touch screen 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 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. 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. The signature will be verified by the firmware. 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 the user application. The uKMM administrators perform the 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.

The application update uses SHA-256 in combination with RSA 2048 bits for authentication and signature verification.

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

5.4 Software Development Guidance

PAX provides a software-programming guide for developers to develop applications 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 does not 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 the pass-through of clear-text account data by 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 (112 bits/168 bits)
- AES (128 bits/192 bits/256 bits)
- RSA (2048 bits/4096 bits)
- SHA-256
- IBE (3072 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
	AES – DUKPT
	Format-Preserving Encryption
	RSA

6.3 Key Table

Table 4 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_PUK	Used for verification of the device, LKI or RKI certificates.	RSA	2048
DA_PVK / DA_PUK	Used for device authentication 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)**
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

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 supports the following key loading methods:

- Clear-text key injection.
- Symmetric encrypted keys, remote asymmetric key loading.
- Local asymmetric key loading.

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 (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
- DHCP client, DNS client
- TLS (TLSv1.2 and TLSv1.3)
- VPN
- HTTP/HTTPS
- SOCKS
- NTP
- OCSP
- SSH, SFTP
- WS/WSS
- MQTT/MQTTS

About the details, please refer to [4] for more information.

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] Secure Application Development Guide.pdf