D210 Security Policy

V 1.0.4

PAX Computer Technology（Shenzhen）Co.,Ltd.

Revision History

Date	Version	Note	Author
2 August 2019	V1.0.0	Initial version	Toris Tang, WT Xu
14 Oct 2019	V1.0.1	Version update	Toris Tang, WT Xu
16 Oct 2019	V1.0.2	Add a picture	Toris Tang, WT Xu
5 Nov 2019	V1.0.3	Update the description	Toris Tang, WT Xu
6 Nov 2019	V1.0.4	Add a tampered picture	Toris Tang, WT Xu

Contents

Glossary of terms and abbreviations

PIN Personal Identification Number

TDES Triple Data Encryption Standard

AES Advanced Encryption Standard

DUKPT Derived Unique Key per Transaction

References

[PWP] PAX White Paper
[PPOG] PAX PC Loader Operating Guide
[PAPG] PAX API Programming Guide
[SADG]Secure Application Development Guide.pdf
[ISUG] IP Stack User Guidance
[ANSI-X9.24] ANSI-X9.24 Part 1-Symmetric Keys Management-2009

[PPOG], [PAPG], [SADG] and [ISUG] are provided to the user in the product packaging.

Purpose

This document is to provide a security policy which addresses basic information for users to usePAX device D210 in a secure manner, including information on key-management responsibilities, administrative responsibilities, device functionality, identification and environmental requirements.
Any unapproved use of the device may result in an incompliant with PCI PTS POI security requirement.

1 General Description

The device is approved as handheld PED product under PCI PTS 5.1 requirement, and the D210 is a handheld terminal for financial transactions in an attended environment. It provides physical keypad, IC card reader (ICCR), security magnetic reader (MSR), color display, printer, touch screen, contactless reader and USB, RS232, WIFI, Bluetooth, Cellular, Ethernet and Modem optional communications.

1.1 Application Platform

1.1.1 Appearance

The model name is visible on the front of the device (See below figure 1). The product name shall not be covered by a sticker or modified by merchant. The hardware version isprinted on a label at the back of the device (See below figure 2, figure 3 and figure 4). The labels at the back of the device shall not be taken off, altered or covered.

Figure 1 The front view of device

Figure 2 The back view of device

Figure 3 The back view of device

Figure 4 The back view of device

1.1.2 Hardware and Software Version

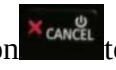
Hardware Version: D210-xxx-ax5-0xxx(a="3" support contactless reader, a="0" no support contactless reader); D210-xxx-ax5-1xxx (a="3" support contactless reader, a="0" no support contactless reader).

The “x”are not security related variables.

Software Version: 5.00.xx

The right two “x” are non-security related variables.

The software version can be retrieved asbelow operations.

1. Press “power/cancel” button 

to power on the device and at the first time the screen lightsplease press “Menu” button  continuously until a “Beep” voice gives out.
2. After the automatic self-test, the screen will show Menu information.
3. Select “4- Version Info”, the version information displays on the screen, including:

- Serial number (same as the label at the backside of device)
- Hardware version (same as the label at the backside of device)
- Firmware version

2 Guidance

2.1 Delivery Inspection

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

- Only obtain devices from PAX.
- 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 shownon the printed box and master carton.
  - Check the contents in each printed box are the same as 'Contents Checklist' which puts along with the 'Installation Manual'.
  - Package style: one machine into a printed box, then boxes into a master carton.
- Please refer to PAX white paper [PWP] for more detail information. If additional technical information needed, please contact our local support team.

2.2 Periodic Inspection and Maintenance

Detailed periodic inspection is specified in PAX white paper [PWP]. It is required the user checks daily as below.

- Damaged seal label. The label is broken and left words “VOID” on the device
- Missing or damaged screws.
- Incorrect or redundant keyboard overlays.
- Holes in the device housing that should not existent.
- External wires exist around the device.
- Missing or unmatched manufacturer barcode label.
- Any suspicious objects internal and around IC card slot.
- Any suspicious objects internal and around MSR slot.

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.

2.3 Decommissioning/ Removal from Service

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 tampered, such as disassemble the device.

2.4 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.

2.5 Default value update

The device does not include any default passwords.

The device does not include any certificate for testing purpose after manufacture.

3 Hardware Security

3.1 Tamper Response

In the tamper event, the device will display 'POS TAMPERED!' message and enter the locked state. 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.

3.2 Environmental Protection

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

- Working Environment:

Temperature: 0℃~50℃(32℉~122℉)

R.H.: 10%~93% (Non-condensing)

- Storage Environment:

Temperature: -20℃~70℃(-4℉~158℉)

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

- Power supply: DC 9V/1A

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).

3.3 Privacy Shield

The device is designed to be used on hand therefore the D210 do not contain a privacy shield. D210is compliant to the character of handheld device as required by Appendix A.1.1.

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 has a certain way to 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.

4 Software Security

4.1 Self-test

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

The self-test includes:

- Check firmware integrity and authenticity
- Check user public key and application integrity and authenticity
- Check installed keys' integrity

If any of the above check fails, the device will be disabled automatically and can't beused. In this case please contact the supplier center.

4.2 Software Signing/Authentication

Boot, Firmware, user public key and application must be signed before released.

Boot is verified by CPU ROM boot before downloaded and executed. If the verification fails, Boot can't be downloaded to device and executed.

Firmware is verified by Boot before downloaded and executed. If the verification fails, firmware can't be downloaded to device and executed.

User public key is verified by firmware before downloaded. If the verification fails, User public key can't be downloaded to device.

Application is verified by firmware before downloaded and executed. If the verification fails, application can't be downloaded to device and executed.

4.3 Software and Configuration Parameters Update

The terminal supports local update of software and configuration parameters.

Any updates loaded into PAX terminals must be signed. The terminal only run cryptographically authenticated software. If the authentication fails, the terminal will refuse to load and run the software.

Please refer to [PPOG] PAX PC Loader Operating Guide for detail information about local software and configuration parameters update operation.

4.4 Software Development Guidance

PAX provides software programming guide to developers to develop applications compliant with PCI security requirement. Please refer to <PAX API Programming Guide.pdf> [PAPG]and<Secure Application Development Guide.pdf> [SADG] when developing SRED applications and <IP Stack User Guidance.pdf> [ISUG] when developing IP enabled applications.

For the SRED module, account data can be encrypted by three methods: TDES encryption, Voltage FPE encryption and Trans-Armor public encryption. The algorithms of the three methods are respectively TDES (128/192 bits), AES (128 bits) . The firmware of device doesn’t support white listing for the pass-through of clear-text account data; also it always provides SRED functionality and doesn’t support the disablement (turning off) of SRED functionality. For more details please refer to <Secure Application Development Guide.pdf>.

5 Key Management

5.1 Key Management Methodologies

Symmetric and asymmetric keys are used by the terminal. Symmetric keys are used for online PIN encryption. Asymmetric keys are used for offline PIN encryption, firmware authentication and application authentication.

For symmetric keys,three types of key management techniques are supported, including Master/Session key, fixed key and DUKPT. All keys inthese three key management techniques are stored in cipher-text under the protection of key encryption key. The key encryption key is stored in CPU battery backed-up area.

For asymmetric keys, a public key from application is used to encrypt the offline PIN.

A manufacture public key hardcoded in firmware is used to authenticate firmware when performing self-testing.

A user public key stored in external flash with its signature is used to authenticate application when firmware loads application and verifies application periodically.

The following algorithms are used in the device:

- Triple DES(Key, PIN and PAN encryption 112 bits and 168 bits)
- AES (Key Storage, PIN and Account data encryption, 128 bits and 192 bits)

Use of the POI with unapproved key management systems may result inan incompliant with PCI PTS POI security requirement.

5.2 Key Table and Usage

Key name	Usage	Algorithm	Size(bytes)	Storage
Key encryption key	Key encryption	AES	192	Secure Unit
Terminal loading key	Key for loading other triple des key	TDES	128/192	Cipher-text in flash
PIN key	PIN encryption for PINBLOCK format 0, 1, 3	TDES	128/192	Cipher-text in flash
AES PIN key	PIN encryption for PINBLOCK format 4	AES	128/192	Cipher-text in flash
Mac key	Mac encryption	TDES	128/192	Cipher-text in flash
Data key	Data encryption	TDES	128/192	Cipher-text in flash
Account data encryption key(TDES)	Account data encryption	TDES	128/192	Cipher-text in flash
FPE key	Account data encryption	AES	128	Cipher-text in flash

Table 2Symmetric Key

5.3 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. The key technology must be review for every 2 years to see whether the key should be replaced with the new key to avoid exhaustive attack. If the terminal is compromised, all keys will be erased, please send the terminal to authorized center for technique analysis and re-loading new key.

5.4 Key Loading

Before loading a payment application, a user public key has to be loaded into terminal using PAX loading tool.

Before using RKI functionality to load session keys, certificate of RKI server certificate and device certificates has to be loaded into terminal within a secure environment.

For device certificate loading, a secure application is loaded into device to implement the key loading protocol in secure environment. After finishing key loading, the application is removed. The key loading operation in secure environment is under dual control.

Other public keys are hardcoded in firmware.

The device supports both local key loading and remote key injection functions for users.

As for local key loading, an initial terminal loading key must be loaded into the terminal before loading of Master/Session keys, fixed keys or DUKPT initial keys. The loading of terminal loading key and AES PIN key must be performed in a secure environment by two custodians. The two custodians have to enter two dual control passwords through key loader device and then have access to key injection sensitive service to enter two key components of the terminal loading key.

All Master/Session master keys, fixed keys and DUKPT keys could be loaded in cipher-text under the protection of this terminal loading key. For the session keys of Master/Session key system, they can be loaded in cipher-text under the protection of Master key of Master/Session key system.

As for remote key injection, the terminal loading key, all MK/SK master keys, fixed keys and DUKPT keys could be loaded remotely through the RKI server located in a secure room.

6 Roles and Services

The customers of PAX are acquirer or Value Added Resellers (VAR). We also refer to VAR as acquirer directly. PAX sells devices to VAR and provide technique and maintenance supports to VAR. VAR sells the devices to end users and provides services to their end user. PAX，VAR and end users play different roles in operating the device. Below table shows different roles and operations:

	Role	**Operation**
VAR	administrator	1. Organize the third party to develop application program; 2. Download application and customer public key 3. Access to device sensitive service
End user	operator	Perform transaction
PAX	maintainer	1. Sign customer public key 2. Repair device and unlock the device if tampered

Table 3 Different roles and operations

7 Communication

The terminal supports Cellular, WIFI, Bluetooth, Ethernet and Modem optional communication for transactions.

The terminal supports Bluetooth v4.0for Bluetooth security communication.

The terminal supports USB/UART 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.