PAX D230

Security Policy

[V1.03]

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 product identification, secure feature implementation, key-management details, administrative responsibilities, device installation and user guidance.

The use of any method not listed in this security policy will invalidate the PCI PTS POI approval of the device.

2 General Description

The device is implemented as handheld PED product under PCI PTS v5.1 requirement, and designed to process financial transactions in an attended environment.

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

2.1 Product Name and Appearance

Figure 1 shows the appearance of PAX D230.

The product name is visible on the label at the back side. The product name will not be covered by a sticker or modified by merchant.

Figure 1 PAX D230

2.2 Product Type

The device is a handheld terminal designed to process online and offline transactions in an attended environment.

It provides color display, physical keypad for PIN entry, IC card reader (ICCR), MSR, Contactless reader, Camera, Cellular, WIFI, Bluetooth, printer, USB and Power Charger Interface.

2.3 Product Identification

2.3.1 Hardware Version

Hardware Version:

D230-xxx-Rx5-0xxx

D230-xxx-0x5-0xxx

D230-xxx-Rx5-1xxx

D230-xxx-0x5-1xxx

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 will not be taken off, altered or covered in any way.

Figure 2 Hardware Identification

2.3.2 Software Version

Firmware Version: 15.01.xx xxxx

The first two digits are fixed digits for device platform and PCI version.

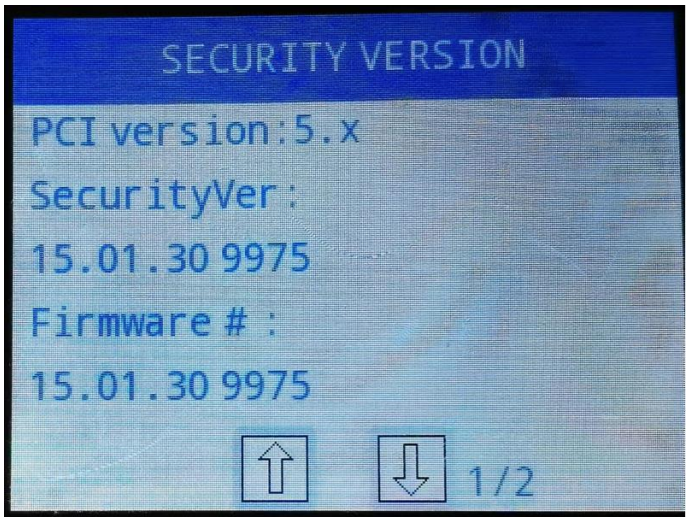
The middle two digits are for delta changes

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

The version information can be retrieved with operations below.

1. Power on the device.
2. After the system initializing and automatic self-test, the main system menu appears.
3. If any application is running, press the red ‘CANCEL’ button to quit application. Then the screen will show the default system menu.
4. Navigate to “Security Info” Tab and Press Enter, the version will be shown on screen:

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



Serial Number:

Select “Terminal Info”, enter the ‘Enter’ button if the screen shows a QR code, and then the version information displays on the screen, including the serial number (shown as ‘SN’ and same as the label at the backside of device) is displayed.

For more terminal information: Select “Terminal Info”, enter the ‘Enter’ button if the screen shows a QR code, and then the version information displays on the screen, including:

1) Serial number (same as the label at the backside of device).
2) Boot Version, Config Version, BoardID and PN number.
3) System Configuration, IMEI, MAC and US_PUK CRC (if applicable).

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 the device.

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 terminal should also be kept away from the complex environment of electromagnetic radiation to prevent interference or damage to the device.

3.3 Environmental Conditions

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

- Working Environment:

Temperature: 0℃~50℃(32℉~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

Failed to comply with the condition above will trigger the device's environmental protection mechanisms.

The security of the device is not compromised by altering the environmental conditions (e.g. place the device outside the stated operating range temperature or operating voltages).

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. The label is damaged and leaves words "VOID" on the device.
- Missing or damaged screws.
- Incorrect or redundant keyboard 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 figure 1.
- Tamper message on the device display, refer to figure 3.
- Any suspicious objects internal and around MSR slot.

If you find any anomalies, which indicate the device may have been opened even tampered, please 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, 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.

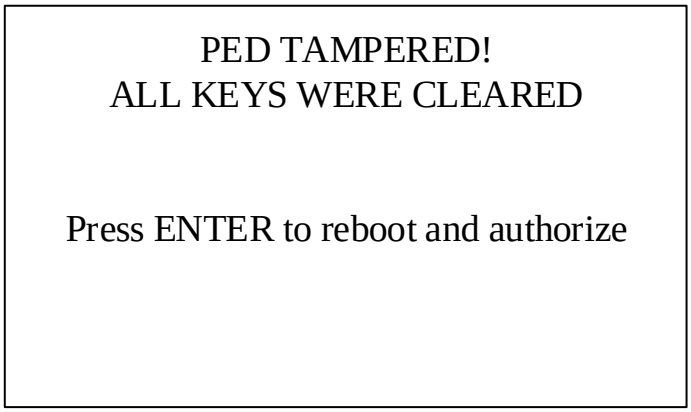


Figure 3 Tamper Prompt

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 does not contain a privacy shield. The device is compliant to the character of handheld device as required by PCI_PTS_POI_DTRs_v5.1 Appendix A 1.2.

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 a distance from others on the check stand.
- Indicate user to use his body or free hand to block the view of keypad through guidance message or logo.
- Make sure no video camera towards the keypad.
- Remind the cardholder to examine if anyone is looking at 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

4.3 Removal Detection

Not applicable.

5 Software Security

5.1 Self-test

The device employs a self-test to mechanism confirm the legality and authenticity of the firmware and software, as well as memory re-initialization for every 24 hours.

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

The self-test includes:

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

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

5.2 Patching and Updating

Update and/or patch to the firmware, application and configuration parameters 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 be 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 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 [4] 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 encryption.

The firmware of device doesn't support white listing for the pass-through of clear-text account data. For more details, please refer to [4] Secure Application Development Guide.

6 Key Management

6.1 Algorithms Supported

The device supports the following algorithms:

- TDEA (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 and P521)

6.2 Key Management

The device supports the following key management schemes:

- **Master/Session key (TDEA/AES)**

  This method uses a hierarchy of Terminal Loading Key, Master keys and Session Keys. The highest level of Terminal Loading Key is distributed through key loading device. The Master keys are distributed under the protection of Terminal Loading Key. The Session Keys are distributed under the protection of Master Keys. These keys can be replaced by the same methods whenever compromise is known or suspected.

- **DUKPT (TDEA/AES)**

  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.

6.3 Key Table

Table 3 RSA public key

Key name	Size (bits)	Algorithm	Usage
User public key (US_PUK)	2048	RSA	Public key for application authentication
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/AES_TLK)	16/24 (TDES) 16/24/32 (AES)	TDES/AES	To load encrypted master keys
DUKPT Initial Key (TIK/AES_TIK)	16 (TDES) 16/24/32 (AES)	TDES/AES	DUKPT Initial Key
Master Key (TMK/AES_TMK)	16/24 (TDES) 16/24/32 (AES)	TDES/AES	To load encrypted session keys
PIN Key (TPK/AES_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/AES_TAK)	16/24 (TDES MK/SK) 16 (TDES DUKPT) 16/24/32 (AES MK/SK) 16/24/32 (AES	TDES/AES	MAC Calculation

	DUKPT)		
Account Data Encryption Key (TCHDK/AES_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/AES_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

6.4 Key Loading

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

The terminal does not support manual cryptographic key entry.

Key loading can be performed by PAX or Acquirer under trusted secure environment.

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 and Bluetooth communication for transactions.

The terminal supports USB communication, USB Port and USB connector is provided.

The terminal supports 2G/3G/4G as cellular functions.

The terminal supports Bluetooth BR/EDR and BLE Secure Connection.

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.

SSL connection other than TLS v1.2 is inherently weak and should not be used unless user required on an interim basis to facilitate interoperability as part of a migration plan.

Appendix

Acronyms

Abbreviation	Description
AES	Advanced Encryption Standard
CTLS	Contactless Module
CRC	Cyclic Redundancy Check
DUKPT	Derived Unique Key Per Transaction
ECC	Elliptical Curve Cryptography
ICC	Integrated Circuit Card
KMM	Key Management Machine
MSR	Magnetic-Stripe Reader
PED	PIN Entry Device
PIN	Personal Identification Number
RSA	Rivest-Shamir-Adelman Algorithm
SHA	Secure Hash Algorithm
UART	Universal Asynchronous Receiver/Transmitter
TDES	Triple Data Encryption Algorithm
TLS	Transport Layer Security

References

[1] ANS X9.24-1-2017, Retail Financial Services Symmetric Key Management Part 1: Using Symmetric Techniques
[2] ANS X9.24 Part 2: 2016, 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