D220 Security Policy

PAX Computer Technology (Shenzhen) Co.,Ltd.

Contents

Glossary of terms and abbreviations

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

[PWP] PAX White Paper
[PTOG] PAX TermAssist Operating Guide
[PAPG] Prolin 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

[PTOG], [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 use the device 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 a handheld terminal for financial transactions in an attended environment. It provides touchscreen, IC card reader (ICCR), security magnetic reader (MSR), color display, contactless reader and USB, Cellular, WiFi and Bluetooth optional communications.

1.1 Application Platform

1.1.1 Appearance

The front view of the device is shown as figure 1 below. The hardware version is printed on a label at the back of the device (See below figure 2). The labels at the back of the device shall not be taken off, altered or covered.

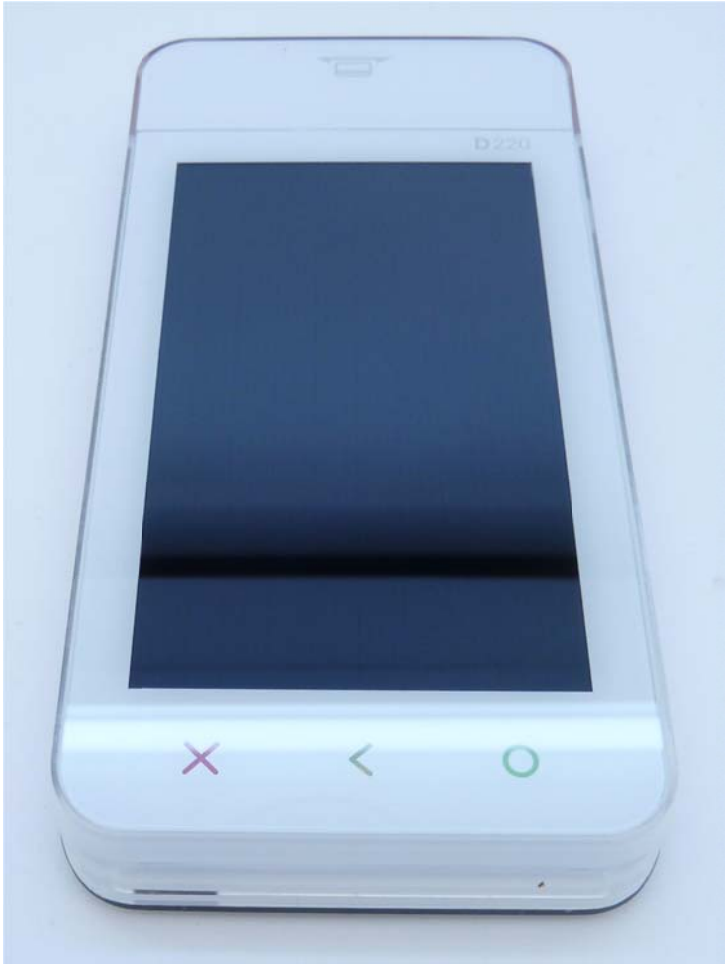

Figure 1 The front view of device

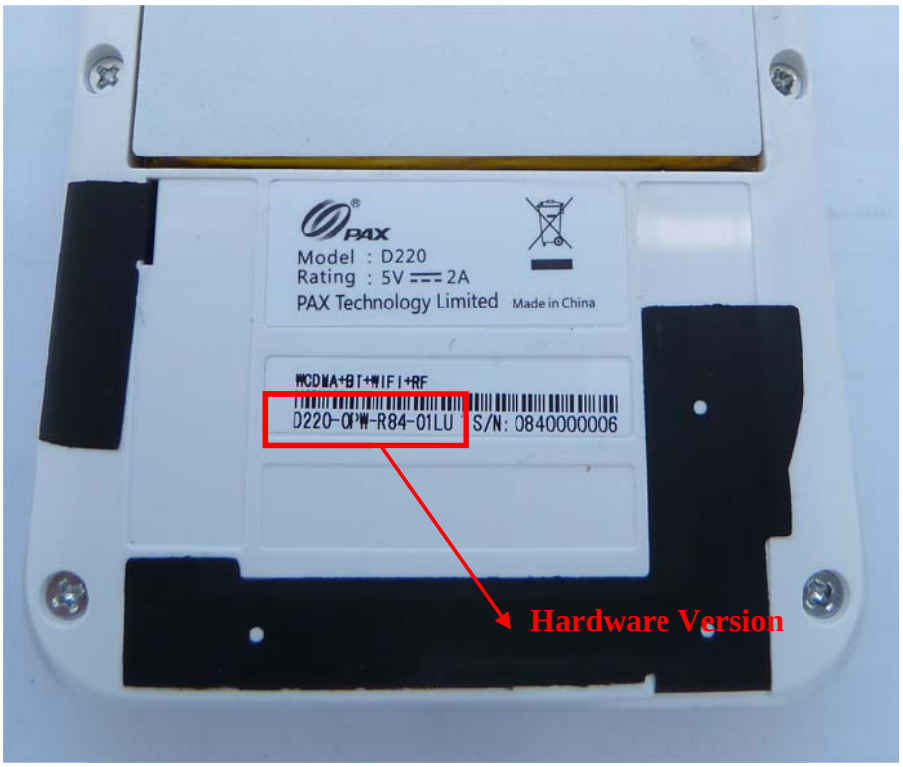

Figure 2 The back view of device

1.1.2 Hardware and Software Version

Hardware Version: D220-xxx-xx4-0xxx

The “x” is non-security related variables.

Software Version:

The software version can be retrieved as below operations.

1. Power on the device.
2. After the automatic self-test, press “CLEAR” button and the screen will show Menu information.
3. Select “Terminal Info”, enter the page-down button if the screen shows a QR code, and then the version information displays on the screen, including:
   - Serial number (same as the label at the backside of device)
   - Firmware version (shown as “Boot” and “Security 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 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.
- 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.

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 in order to meet security requirements.

2.5 Default value update

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 Hardware Security

3.1 Tamper Response

In the tamper event, the device will display 'PED TAMPERED!' message and enter the locked state. There will be no further secure function can be performed on the device.

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 Conditions

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

- Working Environment:

Temperature: -10℃~50℃ (14℉~122℉)

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

- Storage Environment:

Temperature: -20℃~70℃ (-4℉~158℉)

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

- Power supply: DC 5V/2A

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 PIN Entering Security

The device is designed to be used on hand. It is required to enter password as following ways:

- Make sure the cardholder keeps at a certain 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.

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

The software of device consists of Boot, OS and payment application.

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

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

OS is verified by Boot before loaded and executed. If the verification fails, OS can't be loaded to device and executed.

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

Payment application is verified by OS before loaded and executed. If the verification fails, application can't be loaded to device and executed.

The signature verification uses 2048 bits RSA and SHA-256 algorithm.

4.3 Software and Configuration Parameters Update

The terminal supports local update of software and configuration parameters.

Any security related 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 [PTOG] PAX TermAssist 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 <Prolin 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.

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 in these 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 and verifies the application periodically.

The following algorithms are used in the device:

- RSA (Signature verification, Account data encryption, 2048bits)
- Triple DES(Key, PIN and PAN encryption, 112 bits and 168 bits)
- SHA-256 (Signature digest)

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

Table 1RSA public key

Key name	Usage	Algorithm	Size(bits)	Storage
User public key	Public key for application authentication	RSA	2048	Flash with its signature
Manufacture firmware public key	Public key for firmware authentication	RSA	2048	Secure Unit
Manufacture key public key	Public key for user public key authentication	RSA	2048	Hardcoded in OS
Trans-Armor public	Account data encryption	RSA	2048	DDR

key				

Table 2Symmetric Key

Key name	Usage	Algorithm	Size(bits)	Storage
Key encryption key	Key encryption	TDES	192	Secure Unit
Terminal loading key	Key for loading other triple des key	TDES	128/192	Cipher-text in flash
PIN key	PIN encryption	TDES	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	DDR

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 application, a user public key has to be loaded into terminal using PAX loading tool. Other public keys are hardcoded in firmware.

Before key loading of Master/Session key, fixed key or DUKPT initial key, an initial terminal loading key must be loaded into the terminal.

The loading of terminal loading key must be performed in a secure environment strictly protected under the dual control and split knowledge techniques. And specific tools shall be used for key loading.

All Master/Session master keys, fixed keys and DUKPT keys are 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.

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:

Table 3Different 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

7 Communication

The terminal supports WIFI, Cellular and Bluetooth4.0 communication for transactions.

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.

D220 Security Policy

PAX Technology Limited
www.pax.com.hk

Hong Kong
Room 2416, 24/F, Sun Hung Kai Centre, 30 Harbour Road,
Warchai, Hong Kong
Tel: +852-25888800
Fax: +852-28023300

Shenzhen
4/F, No.3 Building, Software Park, Second Central Science-Tech Road,
High-Tech Industrial Park, Shenzhen, Guangdong 518057, P.R. China
Tel: +86-755-86169830
Fax: +86-755-86169834