



D180 Security Policy

V2.04

PAX Computer Technology (Shenzhen) Co.,Ltd.

Copyright © 2000-2019 PAX Computer Technology (Shenzhen) Co., Ltd.

The information contained in this document is subject to change without notice. Although PAX Computer Technology (Shenzhen) Co., Ltd. has attempted to ensure the accuracy of the contents of this document, this document may include errors or omissions. The examples and sample programs are for illustration only and may not be suited for your purpose. You should verify the applicability of any example or sample program before placing the software into productive use.

Revision History

Date	Version	Note	Author
2019.03.26	V1.00	Initial version for D180.	WuXS, Liuzy
2019.06.03	V2.00	Modified	WuXS, Liuzy
2019.06.13	V2.01	Update the question for D180	WuXS, Liuzy
2019.06.14	V2.02	Update the detail for D180 description	WuXS, Liuzy
2019.06.17	V2.03	Update 1.1 2.3 3.3 4.4 the detail description	Liuzy
2019.07.01	V2.04	Update References	Liuzy

Contents

- Glossary of Terms and Abbreviations..... 1
- References 1
- Purpose 1
- 1 General Description..... 2
 - 1.1 Appearance 2
 - 1.2 Hardware and Firmware Version..... 3
- 2 Guidance..... 4
 - 2.1 Delivery Inspection..... 4
 - 2.2 Periodic Inspection and Maintenance 4
 - 2.3 Decommissioning/ Removal from Service 5
 - 2.4 Configuration Settings 5
 - 2.5 Default value update 5
- 3 Hardware Security..... 6
 - 3.1 Tamper Response..... 6
 - 3.2 Environmental Protection 6
 - 3.3 Privacy Shield 7
- 4 Software Security 8
 - 4.1 Self-test 8
 - 4.2 Software Signing/Authentication..... 8
 - 4.3 Software and Configuration Parameters Update 8
 - 4.4 Software Development Guidance 9
- 5 Key Management 10
 - 5.1 Key Management Methodologies 10
 - 5.2 Key Table and Usage..... 10
 - 5.3 Key Replacement..... 11
 - 5.4 Key Loading 11
- 6 Roles and Services 12
- 7 Communication 12

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

[PPOG] PAX PCLoader Operating Guide

[PAPG] PAX API Programming Guide

[SADG]Secure Application Development Guide.pdf

[ANSI-X9.24] ANSI-X9.24 Part 1-Symmetric Keys Management-2009

NOTE



[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 use PAX 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. Use of the device in an unapproved method will violate the PCI PTS 5.1 approval of the device.

It provides physical keypad, IC card reader (ICCR), security magnetic reader (MSR), display, contactless reader and USB, Bluetooth communications.

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 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 and side view of device



Figure 2 The back view of device

1.2 Hardware and Firmware Version


Hardware Version: D180-xxx-Rx5-0xxx (CTLS); D180-xxx-0x5-0xxx (Non CTLS)

The “x” are not security related variables.

Firmware Version: 5.00.00

The firmware version can be retrieved as below operations.



1. Press “power” button  to power on the device and at the first time the screen lights please press “Menu” button continuously until a “Beep” tone gives out.
2. After the automatic self-test, the screen will show Menu information.
3. Select “2-Show Version”, 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 shown on 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 exist.
- 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. If just temporary removal, it's not need to remove the keys.

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 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 only display 'PED TAMPERED!' message without any other tamper warning. There will be no further secure function can be performed on the device.



Figure 3 Tampered State of 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 Protection

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

- Working Environment:

Temperature: 0°C~50°C (32°F~122°F)

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

- Storage Environment:

Temperature: -20°C~70°C (-4°F~158°F)

R.H.: 0%~95% (Non-condensing)

- Power supply: DC 5V/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 it does not contain a privacy shield. It is compliant to the character of handheld device as required by Appendix A.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 at 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.
- 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 be used. 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.

The signature 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 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 PCLoader 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 < BT FAQs and User Guidance.pdf > [ISUG] when developing BT enabled applications.

For the SRED module, account data can be encrypted by TDES (128 bits for DUKPT, 192 bits for MK/SK and 192 bits for Fixed Key) encryption. 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 does not 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 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 application and verifies application periodically.

The following algorithms are used in the device:

- RSA (Signature verification 2048 bits)
- Triple DES(Key, PIN and PAN encryption 112 bits and 168 bits)
- SHA-256 (Signature digest)
- AES (Key Storage 192 bits, PIN and Account data encryption 128 bits)

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

5.2 Key Table and Usage

Key name	Usage	Algorithm	Size(bits)	Storage
User public key	Public key for application authentication	RSA	2048	External 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 firmware

Table 1 RSA public key

Key name	Usage	Algorithm	Size(bits)	Storage
Key encryption key	Key encryption	AES	192	Secure Unit
Terminal loading key	Key for loading other keys	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	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 key	Account Data encryption	TDES	128(DUKPT) 192(MK/SK) 192(Fixed)	Cipher-text in flash

Table 2 Triple DES 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 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 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.

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 USB communication.

The terminal supports Bluetooth v4.2 BLE mode for Bluetooth security communication. And BLE can use LE Security Mode 1 Level 4 only.