Baibu Technology i80

PCI PTS POI Security Policy

Version: 1.2

Content

0. Document change

Version	Author	Date	Description
V1.0	Tangdy	2023-04-22	Initial version
V1.1	Tangdy	2023-05-18	Add description of APP_AUK
V1.2	Tangdy	2023-07-04	Remove the description of SCTP in chapter 3.4

1. Purpose

This document is to provide a security policy which addresses basic information for users (merchants, acquirers) to use the device in a secure manner, including information on secure feature implementation, key-management details, administrative responsibilities, device functionality, product identification and user guidance. The use of any method not listed in this security policy will invalidate the PCI PTS POI V6.2 approval of the device.

2. General description

2.1 Product name and appearance

Figure 1 shows the appearance of the i80.
The product name is visible on the label at the back side. The product name shall not be covered by a sticker or modified by the merchant.

Figure 1 i80 appearance

2.2 Product type

The device is a handheld terminal designed to process online and offline transactions in an attended environment.
It provides display, PIN entry, IC card reader (ICCR), MSR, CTLS, cellular, WIFI and USB interfaces.

The approval class of i80 is stand-alone POS terminal under PCI PTS v6.2 requirements, and it is 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.

2.3 Identification

Hardware Version: V2.0.x

- x: different colors of product. “0” means black.

The product hardware version is visible on the label at the back side of the device (See Figure).
The label shall not be taken off, altered or covered in any way.

Figure 2 label of i80

Firmware Version:

V1.0.x

Figure 3 Firmware version methodology

- First x**:** Possible changes not related to security of SP firmware, such as device driver modification and so on. For example, 0-First version submitted to PCI for certification.

When the software of the project is modified and the change is irrelevant to security, only the “x” will be incremented by 1, the major and minor version is kept unchanged.

The version information can be retrieved with the operations below.

1. Power on the device.
2. After system initializing and automatic self-test, run in the normal status.
3. Press the “MENU” button to enter menu list.
4. Then press the ‘“6.Terminal info” button to enter terminal information shown.

The version numbers will be shown on the screen:

Hardware Version (shown as “HW version:V2.0.0” in Figure , and the same as the label at the backside of the device)
Firmware Version (shown as “V1.0.0” in Figure)

Serial Number:

The SN will be shown on the screen (shown as ‘SN:’ and the same as the label at the backside of the device).

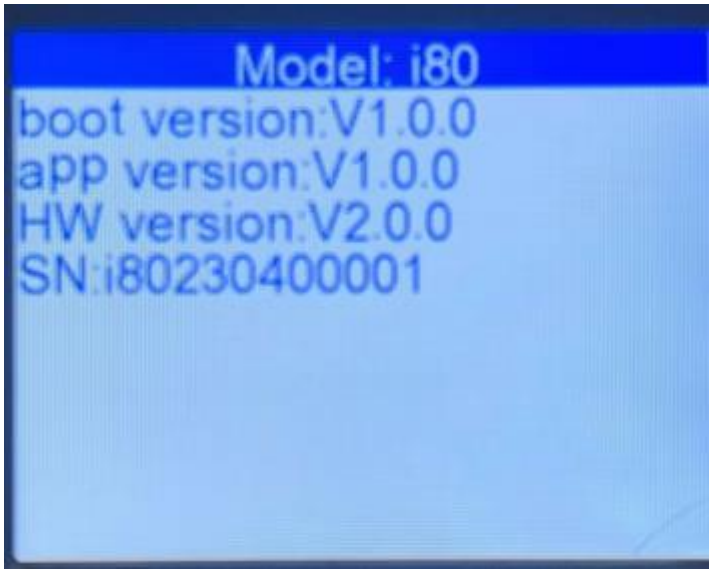

Figure 4 Version and SN Info

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 the below tips.

1. Check if the sender that is providing the i80 device is authorized, if not authorized, please reject the product and send back to the provider.
2. Check if the device's name, firmware version, hardware version meet the approved identification number of PCI PTS POI in the website (www.pcisecuritystandards.org).
3. Check if the appearance of i80 is altered, if the device is different from the picture in this document, please reject the device.
4. Check if something overlay on the keypad area in order to prevent overlay attack.
5. Check if the ICC card slot has wire coming out or something that is suspicious (refer to Figure), if so, reject the device.
6. Check if the magnetic strip card reader slot has other reader or some bug (refer to Figure), if found, reject the device.

To further inspect and use the received device, please check carefully the following aspects described in the rest of this section.

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.

Working Environment:

Temperature: 0℃～50℃ (32℉～122℉)
R.H.: 10%～90% (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:

- Low temperature：-45～-30℃ (-49～-22℉)
- High temperature: 105±10℃ (221±50℉)

Voltage sensor:

- Main voltage sensor: 2.8±0.1V～4.0±0.2V
- VBAT：1.9±0.1V～4.0±0.1V

Failure to comply with the conditions above will trigger the device's environmental protection mechanisms.
The security of the device is not compromised by altering the environmental conditions (e.g., placing the device outside the stated operating range temperature or operating voltages).

3.4 Communications and security protocols

Communication interface	Protocol
USB	Serial
WIFI	ARP,TCP,IP, DHCP,UDP,ICMP,DNS,TLS
Cellular	TCP,IP,UDP,PPP,DHCP, ICMP,DNS,TLS

Table 1 Communication interfaces and protocols

The device supports Cellular, WIFI communication for transaction purpose.
The device supports USB communication as virtual serial port; one Type C USB Port is provided.

The device supports TLS v1.2 security protocol for TCP/IP security communication, including WIFI (ARP), Cellular (PPP), IP, DHCP client. Mutual authentication is provided by TLS v1.2.

3.5 Configuration settings

The device is configured and set by the administrator before being deployed in the field, including the sensitive configuration settings.

No security sensitive configuration settings are necessary to be tuned by the end user to meet security requirements. Also, there is no security default value that needs to be updated by the end user.

3.6 Handheld devices

The device is a handheld device that support SRED encryption.

4. Operation and Maintenance

4.1 Periodic Inspection and maintenance

The user should conduct the following daily inspection:

1. Inspect the appearance of the device to make sure it is the right product.
2. Inspect whether the IC card reader slot has wire coming out, untoward obstructions or suspicious objects at the opening.

Figure 5 View of the ICC slot

3. Inspect whether the MSR card slot has an additional card reader and other inserted bugs.

Figure 6 View of the MSR slot

4. Inspect whether the product appearance has been changed, such as the display, keypad area and so on.
5. Check if the firmware version is correct.

6. Observe whether there are any visual observation corridors, and deter them by body or other shields.
7. Power on the device and check if the firmware runs well. The start-up will inspect the hardware security, authenticity and integrity of firmware.

Such checks would provide warning of any unauthorized modifications to or substitution of the terminal.

Devices, which are detected as disabled through the system must not be used without further investigation of the causes of the tamper. Users are advised to seek technical support from their terminal service partners or directly from vendor.

4.2 Self-Test

The device will perform self-test upon start-up and every 24 hours. Periodic self-test is triggered by automatic reboot every 24 hours. This reboot period starts counting once the device is powered on.

The self-test includes:

- Firmware and application integrity and authenticity check
- Keys correctness check
- Hardware security status check

If any of the above checks fail, the device will be disabled in a secure manner. In this case, please contact the supplier center.

4.3 Roles and responsibilities

Roles	**Responsibilities**
Vendor	1. Sign customer public key 2.Repair device and unlock the device if tampered
Acquirer	1. Organize the third party to develop application program 2.Generate customer public key and download master keys, DUKPT initial key and application
End user	Perform transaction

Table 2 Roles and responsibilities

4.4 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 passwords or certificates for testing purpose after being manufactured.

4.5 Tamper response

In the event of tamper detection, the device will turn into the DISABLED state. The device will be locked and no further secure function can be performed on it.

Figure 7 Tamper Prompt

If the device is in tampered state, the user must contact the vendor for device maintenance immediately, remove it from service and keep it away from potential illegal investigation.

4.6 Privacy shield

The device is designed to be used on hand; therefore, the device does not contain a privacy shield.

The customer should care to cover the keypad area with his (or her) hands and body during PIN entry. In this way, the keypad area will not be seen except by the user and the PIN is protected from being revealed, as shown in Figure .

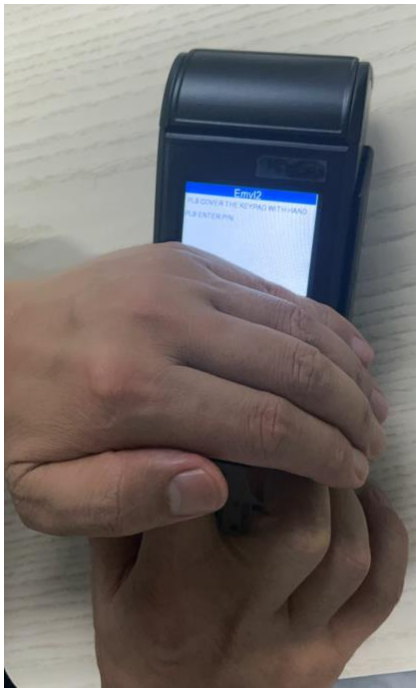

Figure 8 PIN Entry

It is recommended to enter the PIN in the following ways:

1. Make sure the cardholder holds the device on hand during PIN entry.
2. Make sure the cardholder keeps a distance from others at the check stand.
3. Indicate user to use his (or her) body or free hand to block the view of soft random keypad through guidance message or logo.
4. Make sure no video camera is turned towards the soft random keypad.
5. Remind the cardholder to examine if anyone is looking at the soft random keypad before PIN entry.

4.7 Patching and updating

Software can be installed into the device. Local update is supported for software update and patching.

Any security related update and/or patch loaded into terminals must be signed using vendor's firmware sign key. 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.

4.8 Decommissioning/Removal

Devices destined for permanent decommissioning must undergo a secure decommissioning process before they are finally disposed of, making sure that no sensitive information remains in them. Device decommissioning does not require any sensitive tool or service. Terminal administrators shall force a hardware tamper condition by opening the casing of the device to ensure no sensitive information is recoverable from the device.

For temporary removal, there is no need to change the state of the device, as all the keys are still protected safely with the main board battery power supply.

5. Security

5.1 Software Development Guidance

The terminal implements the necessary security measures and functions to provide compliance with the PCI security requirements for authenticated applications.

To develop an application base on the device while ensuring compliance, please follow the [2] Application development guide and [3] Application programming guide, the [4] Secure software development guide and the [5] OP secure software development guide that Baibu provides, prepare the development environment, install the compiler, refer to the demo and study how to use all the API provided to operate corresponding function module.

The device does not allow unauthorized or unnecessary functions.

5.2 SSL

The device does not support SSL, only TLSv1.2 is implemented.

5.3 Signing

A sign tool is used to sign user application and vendor firmware. The signing tool administrators perform the signing process under dual control.

Application and firmware 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, the application cannot be loaded into device or executed. The signature and verification mechanism ensures the authenticity and integrity of the application that is loaded into device.

5.4 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 (192 bits)/AES (128/192/256 bits) under MK/SK and encrypted by TDES (128 bits) under DUKPT.

The firmware of device does not support white listing for the pass-through of clear-text account data. For more details, please refer to [3] Secure software development guide.

5.5 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
- ECC (in support with NIST P-256 and P-521)

5.6 Key Management

Master/Session key (TDEA/AES)

This method uses a hierarchy of Master keys and Session Keys.
The Master keys are injected into the device through key components entry. 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)

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 may result in incompliance with PCI PTS POI security requirements.

5.7 Key Table

RSA public keys

Key name	Size(bits)	Algorithm	Usage
FRW_AUK	2048	RSA	Public key for SP firmware authentication
APP_AUK	2048	RSA	Public key for SP application authentication
Server_AUK	2048	RSA	Public key for server authentication during tamper recovery

Table 3 Key table – RSA public keys

Symmetric keys

Key name	Size(bits)	Algorithm	Usage
AES_MMK	256	AES	Used to encrypt/decrypt all other keys stored inside the device's internal flash
Master Keys (TMK/AES_TMK)	192 256	TDEA AES	To load encrypted session keys
PIN Keys (TPK/AES_TPK)	128/192 128/192/256	TDEA AES	PIN encryption for PINBLOCK format 0,3,4
MAC Keys (TAK/AES_TAK)	128/192 128/192/256	TDEA AES	MAC Calculation
Data Keys (TDK/AES_TDK)	128/192 128/192/256	TDEA AES	Transaction Data encryption/decryption
Cardholder Data Keys (TCHDK/AES_TCHDK)	192 128/192/256	TDEA AES	Exclusively used for Account data (PAN) encryption / decryption
DUKPT Initial Keys	128	TDEA	Derive all DUKPT future keys for PIN encryption, MAC calculation and data encryption.

Table 4 Key table – symmetric keys

5.8 Key Loading

The terminal supports entry of clear-text key components through the physical keypad.

Two components of TMK/AES_TMK/DUKPT initial key are entered through device's physical keypad in a secure room, and the entry of key components results in the zeroization of pre-existing secret keys in the device.

The terminal also supports local cipher text key injection using a key loader.

5.9 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.

6. Acronyms

Abbreviation	Description
Baibu	Short for vendor Baibu Technology Co., Ltd.
AES	Advanced Encryption Standard
ECC	Elliptical Curve Cryptography
TDEA	Triple Data Encryption Algorithm
SHA	Secure Hash Algorithm
RSA	Rivest-Shamir-Adelman Algorithm
CTLS	Contactless Module
ICC	Integrated Circuit Card
MSR	Magnetic-Stripe Reader
DUKPT	Derived Unique Key Per Transaction
PIN	Personal Identification Number
TLS	Transport Layer Security

7. References

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

[2] Application development guide

[3] Application programming guide
[4] Secure software development guide
[5] OP secure software development guide