Shanghai NRT Technology Co.,Ltd.

P90

PCI PTS POI Security Policy

2023-11-09

V1.0

P90 PCI PTS POI Security Policy

Revision History

Date	Revision Level	Description	Reviser
2023-11-09	V1.0	Create document	Shao

Contents

1. Purpose

This document addresses the proper use of the POI in a secure manner including information about key-management responsibilities, administrative responsibilities, device functionality, identification and environmental requirements.

The PCI PTS POI version of device assessed is V5.1.

This product is mainly for indoor usage, its target merchant are the restaurants, entertainment, chain stores, supermarkets, E-commerce and so on.

The use of the device in any other than the approved method, as described on the security policy, will violate the PCI PTS approval of the device.

2. General Description

2.1. Product Name and Appearance

The product name is P90, the appearance shown in figure 2-1.

Figure 2-1 P90 Appearance

The device serial number is located on device label 1 on back of device, shown in figure 2-2.

Figure 2-2 Device Label 1

The product model name and hardware version are located on device label 2 on back of device, shown in figure 2-3.

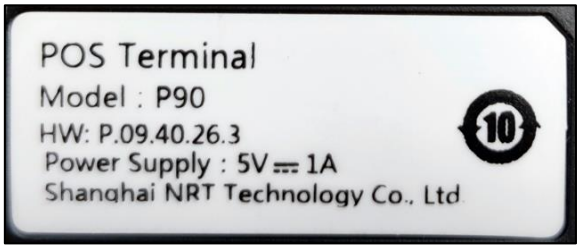

Figure 2-3 Device Label 2

2.2. Product Type

P90 is a handheld PED device for financial transaction in attended environment.

P90 provides integrated physical keypad for PIN Entry, color display, magnetic-stripe reader (MSR), IC card reader (ICCR), contactless card reader (CTLS), thermal printer, camera (optional), cellular (2G/3G), Wi-Fi (optional) and USB communications.

2.3. Identification

The hardware version is located on device label 2 as is shown in figure 2-3.
P90 has different hardware version with different configuration, all probable configurations and hardware version shown in the table 2-1.

Table 2-1 Hardware version & Configurations

Hardware Version	Configuration
P.09.40.x4.x	2G + 3G + Camera + Wi-Fi
P.09.40.x5.x	2G + 3G
P.09.40.x6.x	2G + Camera + Wi-Fi
P.09.40.x7.x	2G + Wi-Fi
P.09.40.x8.x	2G

Hardware	P	.	0	9	.	4	0	.	x	4\5\6\7\8	.	x
Number	1	2	3	4	5	6	7	8	9	10	11	12
9	SIM/SAM2 slot (on Cover board) configure: 0 – Slot used to SAM card; 1 – Slot used to SIM card; 2 – None.											
12	Device front color style code: 1 – Red; 2 – Blue; 3 – White; 4 – Black; 5 – Green; 6 – Gray; 7 – Orange; 8 – Yellow; 9 - Purple; A - Silvery.											

The device firmware version is 0F020403.00.xxxx.xxx.xxx.

Meanings of the number in version numbers：

Firmware	0	F	0	2	0	4	0	3	.	0	0	.	xxxx	.	xxx	.	xxx
Number	1	2	3	4	5	6	7	8	9	10	11	12	13-16	17	18-20	21	22-24

13-16	Non-security-related application module software version number. 4 characters, alphabet or numeric characters.
18-20	Non-security-related baseband/modem software revision number. 3 characters, alphabet or numeric characters.
22-24	Non-security-related security module software revision number. 3 characters, alphabet or numeric characters.

The firmware version can be viewed on device display screen via software menu. To examine the firmware version, after POS boot up, enter into menu "Setting" - "Firmware version":

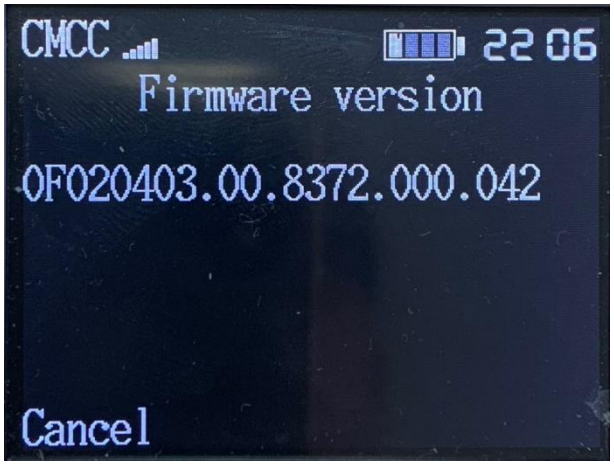

Figure 2-4 Firmware Version Example Screen Shot

3. Installation and User Guidance

3.1. Initial Inspection

After open the device package, the merchant have to check the device appearance and physical components to ensure device has not been tampered or modified in transit.

Merchant need to check the following items:

- Tamper proof seal is not broken.
- Device housing is integrated, no breakage.
- If the ICCR or MSR slot is damaged, such as abrasion, painting and other machining marks
- If there is any suspicious object like lead wire over ICCR or MSR slot.
- If there is any unknown object inside ICCR or MSR slot. The complete MSR and ICCR of the terminal are shown below.

Figure 3-1 ICCR of P90

Figure 3-2 MSR of P90

If you find these suspicious circumstances, please stop using the device immediately and contact the customer service to confirm if the device has been tampered.

3.2. Installation

P90 is an integrated payment terminal, not need connect cable to other device or component. Please ensure the terminal installation in favor of merchants and cardholders have very convenient level, as close as possible to the power socket.

Terminal PIN entry device should not in the face of security cameras to prevent PIN leakage. Terminal should stay away from all sources of heat, to prevent vibration, dust, moisture and

electromagnetic radiation (such as a computer screen, motor, security facilities etc.). Be sure this terminal is used in only attended way.

The power socket is USB cable on left side of device.

Figure 3-3 Power Socket

P90 has two screw holes at back of the device which is used to combine the camera mirror structure, figure 3-4 shows the picture of device which has installed camera mirror structure.

Figure 3-4 P90 with Camera Mirror Structure

3. 3. Environmental Conditions

The environmental conditions to operate the device are specified in the user manual. This device is a handheld device used in an attended environment, and the use of the device in an unapproved method will violate the PCI PTS approval of the device. The security of the device is not compromised by altering the environmental conditions (e.g. subjecting the device to temperature or operating voltages outside the stated operating ranges does not alter the security). It will cause the device get tampered when the environmental conditions are out of below ranges:

- The stated range of temperature is -40 °C to 110 °C.
- The stated range of back up battery voltage is 1.8V to 4.0V.

Temperature Environments:

Operation Temperature: -10°C～50°C;
Storage Temperature: -20°C～60°C;

Power Adaptor Specification:
Input：100 to 240V AC, 50Hz/60Hz
Output: 5V 1A

3.4. Communications and Security Protocols

The communication methods and protocols supported by this terminal shown in the table 3-1.
Table 3-1 Communication and Protocols

Communication Interface	Protocols
USB	Standard USB Interface
Cellular (2G/3G)	TLSv1.2, TCP, UDP, DHCP, DNS, PPP, IP.
Wi-Fi	TLSv1.2, TCP, UDP, DHCP, DNS, ARP, IP.

Merchant can use all these communication interface directly after installed without any configuration.

3.5. Configuration Settings

For merchant or acquirer, the device is functional when received by the merchant or acquirer. No security related configuration settings are necessary to be tuned by the end user to meet security requirements.

4. Operation and Maintenance

4.1. Periodic Inspection

The merchant or acquirer should daily check that the physical keypad is firmly in place. Such checks would provide warning of any unauthorized modification to the terminal, and other suspicious behavior of the terminal.

The merchant or acquirer should also check that the installation/maintenance operations are performed by a trusted person.

Especially check if the ICCR/MSR slot is damaged, such as abrasion, painting and other machining marks, additional labels, and if there is any suspicious object like lead wire over ICCR/MSR slot, or any unknown object inside ICCR/MSR slot. The legal ICCR and MSR please refer to Figure 4-1 and Figure 3-2.

If you find these suspicious circumstances, please stop using the device immediately and contact the customer service to confirm if the device has been tampered.

4.2. Self-Test

Self-tests are performed in startup and reset process to initialize memory and check firmware/software integrity and validity via digital signature verification. If self-tests failed, it will stop running.
In order to reinitialize memory, the device will reboot in 24 hours after it starts up.
Self-tests are not initiated by an operator.

4.3. Roles and Responsibilities

There are 3 type of roles in operating the device:

- NRT sells devices to acquirer or re-sellers and provide technique and maintenance supports.
- Re-sellers sells the devices to end users and provide services to their end user.
- End users use the device to perform transaction.

Each role has its own permission and responsibility shown in the table 4-1.

Table 4-1 Roles and Permission Definition

Role	Typical Entity	Permission & Service
Maintainer	NRT	1. Sign software and firmware 2. Develop firmware 3. Repair device and unlock device of tampered
Administrator	Re-Sellers	Access device sensitive service

Operator	End Users/ Acquirer/ Merchant	Perform transaction

4.4. Passwords and Certificates

For Key-Loading Facility, the device needs to configure after received by key-loading facility. About the configuration settings of admin and key-loading operator passwords, please refer to the [6].

For merchant or acquirer, the device is functional when received by the merchant or acquirer. No certificate needs to be configured in this device.

4.5. Tamper Response

The device contains tamper mechanisms that will trigger when a physical penetration attempt of the device is detected. A merchant or acquirer can easily detect a tampered terminal via:

- Warning message is displayed on LCD screen like message "Device is tampered". There is no any other response except the displayed message.

Figure 4-2 Tamper Prompt Demo

- Cannot enter normal application and cannot do any transaction.

Any physical penetration will result in a "tamper event". This event causes the activation of tamper mechanisms that make the device out of service.

If any device is found to be under the tampered condition, please deactivate it immediately, keep it properly for possible evidence collection and investigations, and notify the security personnel of vendor and service provider.

4.6. Privacy Shield

P90 is a handheld device, it is required to provide cardholders with the necessary privacy during PIN entry.

For example, the device will demonstrate a safe PIN-entry process how to entry PIN. This message

reminds cardholder that he or she can use his own body or their free hand to block the view of physical keypad.

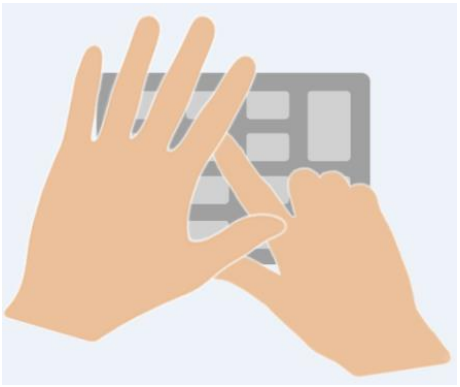

Figure 4-3 Safe PIN Entry Logo Example

The device has been PCI PTS approved as a hand-held device, and is not provided with a privacy shield. Use of the device for payments on a table, desk or in a dock will invalidate the PCI PTS approval.

The following table shows the combinations of methods that should be used when installing the device to protect the cardholder's PIN during PIN entry.

Method	**Observation Corridors**				
	Cashier	Customer in Queue	Customer Elsewhere	On-Site Cameras	Remote Cameras
With stand	No Action Needed.	No Action Needed.	No Action Needed.	Out of sight of the cameras.	Out of sight of the cameras.
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 cameras.	Out of sight of the cameras.
Customer Instruction	Remind the customer to shield PIN.	Keep a distance.	Keep a distance.	Out of sight of the cameras.	Out of sight of the cameras.

4.7. Patching and Updating

This terminal supports remote updating or patching the software.

- Power on the device.
- Configure device to connect network via Wi-Fi or Cellular.
- Device will automatic connect to remote server to check update or patch.
- Device will download update or patch if new version was found.
- Device will check the update or patch to make sure it is integrity.
- Device will apply the update or patch if it pass the signature verification.
- Device will not apply and delete the incorrect update or patch.

After update, the device firmware version will be updated synchronously, you can check the firmware version as is shown in figure 2-4.

4.8. Decommissioning

When the device is no longer used for permanent decommissioning reason, the administrator of the device needs to gather the device and then erase all the key materials on it. It can be done by directly disassemble the device to make it unavailable. After, disassembling device will make device to tamper status, which will erase all payment keys and decommission your device.

For the temporary removal, there is no need to change the state of the device, as all the keys are still protected safely by the hardware tamper protection mechanism.

5. Security

5.1. Software Development Guidance

During the software development, the following steps should be implemented：

1) Developer training.
2) Code Review.
3) Security review and audit.
4) Module test.
5) Source code management and version control.
6) Software test.
7) Signing

For SRED firmware, developer must respect the following rules:

- Account data read from IC, magnetic stripe card must be encrypted at once.
- No clear-text account data output.
- Firmware must be signed, and only legal signed firmware can be load into device.

There are two separate modes in which the device can be:

- Activated mode: the device is fully operational.
- Inactive mode: the device is tampered, not operating and needs to reactivation after maintenance and security checks by vendor.

The reactivation of tampered device can only be performed by vendor. For more information about software development guidance, please refer to the document [7].

5.2. TLS

For TLS firmware development please refer the [7] and the compliance with PCI PTS, the following points need to take attention.

- The client must authenticate server certificate.
- The cipher suite of the server which terminal connects should be as secure as TLS_RSA_WITH_AES_128_CBC_SHA or more secure.
- The server which terminal connects should be configured to require Client Authenticate.
- Use TLS v1.2 or higher.
- Firmware developer must use SHA-256 on top of the security
- Protocol when it is being used for security functionality.

5.3. Signing

The digital signature algorithm is based on RSA-2048 bits and SHA-256.

P90 software is signed by vendor including boot stages code, firmware, updates and patches.
The detailed signing flow please refer to the [9].

5.4. Account Data Protection

P90 uses the account data to perform payment transaction, the account data is encrypted by protection key to prevent clear-text account data transmit via open network.

P90 has printer function and supports printing of the payment list. To protect account data, the account data printed has to be masked to meet first six and last four digits of PAN data.

The clear-text account data cannot output in printer or display screen in any situation.

P90 enabled SRED function by default, and this function cannot be disabled. The account data is protected by TTK which allows TDEA-192bit, AES-128bits and AES-192bits algorithm.

5.5. Algorithms Supported

All of algorithms P90 support is list in table 5-2.

Table 5-1 Algorithms Supported

Algorithm	Usage	Key Management Method
RSA (2048bits)	Internal Signature verification.	N/A
SHA-2	Internal Signature verification.	N/A
TDES (128/192bits)	Keys	MK/SK and DUKPT
AES (128/192bits)	Keys	MK/SK

All keys information P90 support is list in table 5-3.

Table 5-2 Key Table

Key Name	Key Management Method	Purpose/Usage	Algorithm	Size(bits)	Storage
TLK	MK/SK	Terminal Loading Key.	TDES/AES	128/192	Internal Flash
TMK	MK/SK	Master Key.	TDES/AES	128/192	Internal Flash
TPK	MK/SK	PIN Encryption Key	TDES/AES	128/192	Internal Flash
TAK	MK/SK	MAC Key	TDES/AES	128/192	Internal Flash
TEK	MK/SK	Data Encryption Key	TDES/AES	128/192	Internal Flash
TDK	MK/SK	Data Decryption Key	TDES/AES	128/192	Internal FLASH
TTK	MK/SK	Account Data Encrypt	TDES	192	Internal FLASH

		Key	AES	128/192	
TIK	DUKPT	DUKPT Initial Key	TDES	128	Internal FLASH
Future Key	DUKPT	DUKPT Future Key	TDES	128	Internal FLASH

5.6. Key Management

This device implements different types of key management methods:

- Master Key/Session Key

  The method uses a hierarchy of Key Encrypting Keys and Transaction Keys. The highest level of Key Encrypting Key is known as a Master Key. Master Keys are distributed using some physical process, e.g. key loading device.

  Master Keys are replaced by the same methods whenever compromise is known or suspected. Transaction Keys are distributed, replaced and encrypted under a Key Encrypting Key.

- DUKPT

  With this method, each transaction-originating TRSM uses a unique key for each transaction, yet never contains any information which would allow the determination of any key previously used by this TRSM, nor of any key which has been or will be used by any other transaction-originating TRSM. The receiving TRSM must determine the current Transaction Key used by any transaction-originating TRSM from the non-secret information contained in the transaction's SMID and a Based Derivation Key.

  This Base Derivation Key

  - MUST reside in a TRSM which relies exclusively on physical barriers.
  - resides in one or more receiving (e.g., acquirer's) TRSMs.
  - does not reside in any originating (e.g., terminal's) TRSMs.
  - is used to generate the originating TRSM's unique Initial Key using the KEY NAME.
  - can be used to generate the unique Initial Keys for many originating TRSMs.
  - MUST be a double-length or triple-length key.

Use of the terminal with a key-management system other than these two mentioned above will invalidate any PCI approval of the terminal.

5.7. Key Loading

The TLK loading has been performed in key loading facility which provides secure room.
The TLK are loaded into device as two components. Each component of TLK is input by different person. Each person should only know their own component.
The Master Keys are loaded into device in ciphertext which is encrypted by TLK.
The Session Keys can be divided into five types: TPK (Pin Encryption Key), TAK (MAC Key) and TDK (Data Encryption Key), TEK (Data Decryption Key) and TTK (Track Encryption Key) which are loaded

into device in cipher text which is encrypted by Master key.
The DUKPT initial key is loaded into device in secure room, then it will generate 21 future keys under the ANSI X9.24 future key generate algorithm, and the initial key will be also replaced by new generated future key.

5.8. Key Replacement

Any key should be replaced with a new key whenever the compromise of the original key is known or suspected, and whenever the time deemed feasible to determine the key by exhaustive attack elapses.
If keys are stolen, please inform should inform the acquirer.

The key lifetime is controlled by Acquirer.
Suggestions from the manufacturer:

- The maximum lifetime of TLK is suggested to be 2 years.
- The maximum lifetime of TMK is suggested to be 2 years.
- The maximum lifetime of SK (TPK/TAK/TEK/TDK/TTK) is suggested to be 1 day.
- The maximum lifetime of DUKPT cannot exceed 1million transactions.

6. Acronyms

Abbreviation	Description
DUKPT	Derived Unique Key Per Transaction
N/A	Not Applicable
PED	PIN Entry Device
PIN	Personal Identification Number
RSA	Rivest Shamir Adelman Algorithm
SHA	Secure Hash Algorithm
TDES	Triple Data Encryption Standard
AES	Advanced Encryption Standard
IC Card	Integrate Circuit Card
RF Card	Radio Frequency Card
SK	Session Key/Transaction Key
ICCR	IC Card Reader
MSR	Magnetic Stripe Reader

7. References

[1]. ANS X9.24 Part 1:2009, Retail Financial Services Symmetric Key Management Part 1: Using Symmetric Techniques

[2]. X9 TR-31 2010, Interoperable Secure Key Exchange Key Block Specification for Symmetric Algorithms

[3]. ISO 9564-1, Financial services-Personal Identification Number (PIN) management and security - Part 1: Basic principles and requirements for PINs in card - based systems

[4]. ISO 9564-2, Banking-Personal Identification Number management and security Part 2: Approved algorithms for PIN encipherment

[5]. Payment Card Industry PTS POI Derived Test Requirements, v5.1

[6]. Device Default Settings Overview

[7]. Software_Development_Secure_Guidance

[8]. Firmware Update User Manual

[9]. Key Management for Firmware Developer