Shanghai Xiangcheng Communication Technology Co., Ltd

P10

PCI PTS POI Security Policy

2023-10-27

V1.3

Revision History

Date	Revision Level	Description	Revisor
2023-08-01	V1.0	Create Document	Cedar
2023-08-10	V1.1	Update the content	Cedar
2023-08-19	V1.2	Update the content	Cedar
2023-10-27	V1.3	Update the section 2	Cedar

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 PTS POI version of device assessed is V6.1.

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

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

The device does not support undefined and unauthorized instructions.

2. General Description

2.1. Product Name and Appearance

The product name is P10, the appearance is shown in figure 2-1.

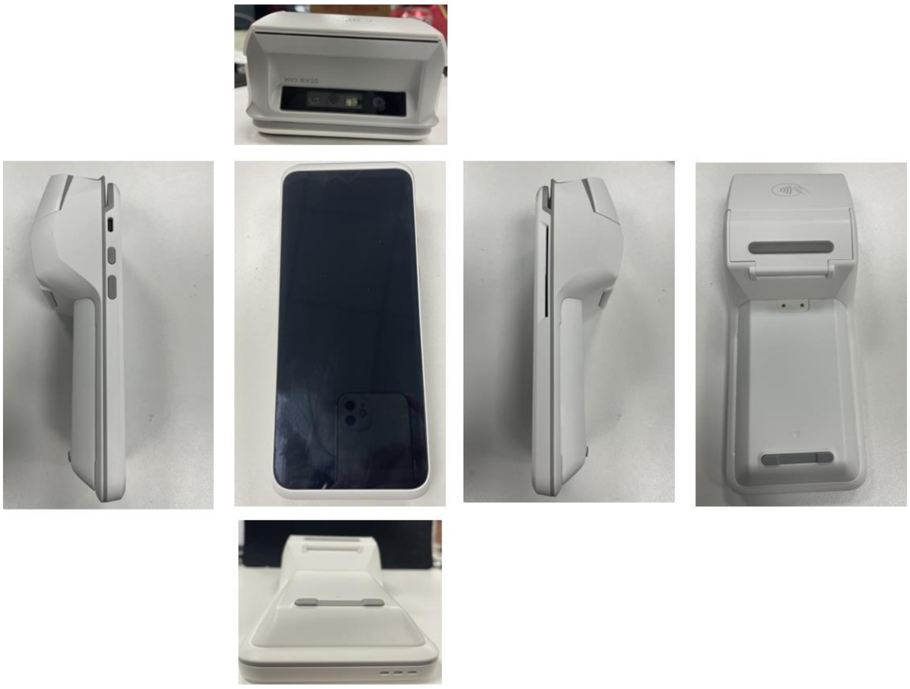
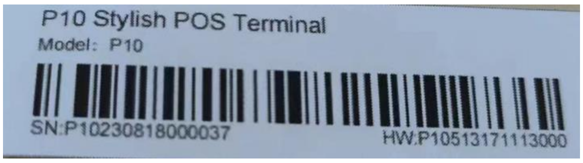


Figure 2-1 P10 Appearance

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



P10 Stylish POS Terminal
Model: P10
SN:P10230818000037
HW:P10513171113000

Figure 2-2 Device Label

2.2. Product Type

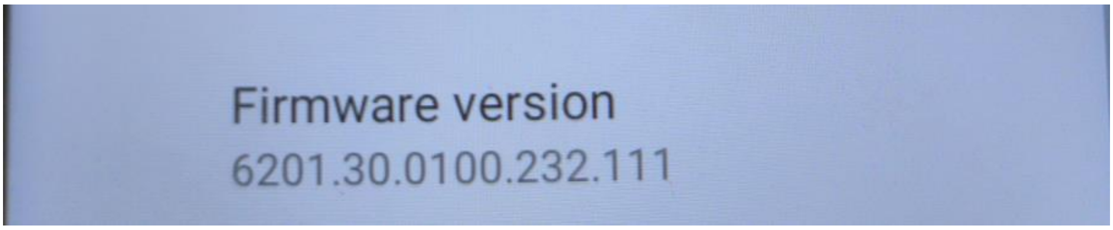
P10 is a handheld PED device for financial transactions in an attended environment.
P10 provides device physical keypad for PIN Entry, color display, magnetic stripe reader (MSR), IC card reader (ICCR), contactless card reader (CTLS), thermal printer, camera, Wi-Fi, cellular and USB communications.

2.3. Version Description

Hardware version:
P10513071110000
P10513071112000
P10513171113000
Firmware version:
6201.29.0100.193.xxx
6201.30.0100.193.xxx
6201.30.0100.232.xxx
The “x” represents non-security related SP version changes (such as refactoring features, function bug fixes, driver updates, etc), ranging from 000 to 999.

2.4. Identification

The hardware version is located on the device label as shown in figure 2-2.
The firmware version can be viewed on the display screen via software menu. To examine the firmware version, after POS boot up, enter menu Settings - About device - Firmware version.



Firmware version
6201.30.0100.232.111

Figure 2-3 Firmware Version Example Screen Shot

3. Installation and User Guidance

3.1. Initial Inspection

When receiving the device, the merchant needs to check the device appearance and physical components to ensure the device has not been tampered or modified in transit.

The merchant needs to check the following items:

- Tamper proof seal is not broken
- Device housing is integrated, no breakage
- If the ICCR slot is damaged, such as abrasion, painting and other machining marks
- If there is any suspicious object like lead wire over ICCR slot
- If there is any unknown object inside ICCR slot

If you find these suspicious circumstances, please stop using the device immediately and contact customer service for inspection.

3.2. Installation

P10 is a payment terminal with battery. Please ensure the terminal has been installed in favor of merchants and cardholders.

To prevent PIN leakage, the PIN entry device should avoid being monitored by security cameras.

Terminal should be kept away from heating sources, vibration, dust, moisture and electromagnetic radiation (such as computer screen, motor etc.).

Be sure this terminal is used only in an attended way.

Be sure the battery package has been installed in the battery compartment.

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).

When sensors detect an out-of-range situation, a tamper event is triggered and the secret information in the SP is erased.

Power

Non-replaceable battery, 3.85V / 1700mAh

Operating Temperature and Humidity

Temperature: 0 °C to +60 °C
Relative Humidity: 45% to 85% RH (non-condensing)

Storage Temperature and Humidity
Temperature: -20 °C to +45 °C
Relative Humidity: 45% to 95% RH (non-condensing)

Failure Protection
If the following conditions happen, it will trigger tamper events.

- Temperature below -35 °C or above +109 °C.
- Battery Backed Voltage below 1.91V or above 3.62V.

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 Type-C	USB
Cellular (2G/3G/4G)	TLS v1.2
Wi-Fi	TLS v1.2

Merchant can use all these communication interfaces directly after installation without any configuration.
Use of any method not listed in the policy invalidates the device approval.

3.5. Configuration Settings

For end users, the device is functional when received.
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

Check the terminal daily (including physical keypad) to ensure that it is free of rogue overlays.
The end users should check daily 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 end users should check daily that the installation/maintenance operations are performed by a trusted person.
Especially check daily if the ICCR 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 slot, or any unknown object inside ICCR slot.

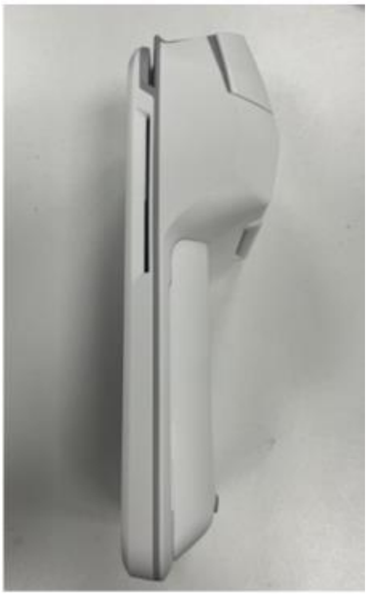


Figure 4-1 ICCR Slot Detailed

If you find these suspicious circumstances, please stop using the device immediately and contact customer service for inspection.
Please refer to Section *4.5 Tamper Response* to check whether the device is tampered or not while operating or maintaining this device.

4.2. Self-Test

Self-tests are performed when the device starts up and resets to initialize memory and check firmware/software integrity and validity via digital signature verification. Self-tests also check the tamper sensor state and integrity of keys. If self-tests fail, the device 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

Three roles are involved in the device operation, Maintainer, Administrator, and Operator.

- The vendor sells devices to acquirers or re-sellers and provides technical and maintenance support.
- Re-sellers sell devices to end users and provide services to their end users.
- End users use this device to perform transactions.

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

Table 4-1 Roles and Permission Definition

Role	Typical Entity	Permission & Service
Maintainer	Device Vendor	● Sign software and firmware ● Develop firmware ● Repair device and reactivate device if tampered
Administrator	Re-Sellers/ Acquirers	Access device sensitive services
Operator	End Users	Perform transactions

4.4. Passwords and Certificates

The default passwords must be changed at first use.

About the detailed configuration settings of admin and key-loading operator password, please refer to the *Device_Default_Settings_Overview*.

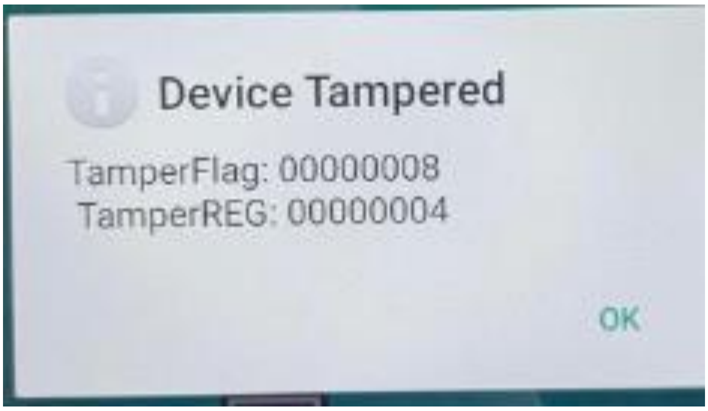
For end users, the device is functional when received.

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. End user can easily detect a tampered terminal via:

- Device blocked and warning message displayed on screen, for example:



Device Tampered

TamperFlag: 00000008
TamperREG: 00000004

Figure 4-2 Device Blocked Prompt Demo

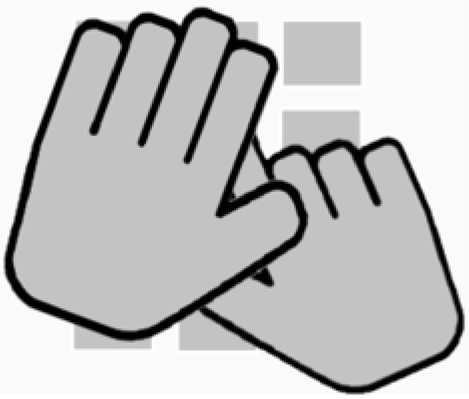
- Cannot enter normal application and cannot do any transactions.
- The device will pop up an alarm window and the buzzer alarm.

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 investigation, and return to the security personnel of vendor or service provider for examination.

4.6. Privacy Shield

P10 is used only in an attended environment. It is generally used as a handheld device. It is designed to be used by cashiers (It is recommended that cardholders use their body or hands to cover themselves).



Merchant should position all surveillance cameras (if any) so that PIN entry cannot be recorded, as a patron enters it, on all tables.

Merchant should train staff to monitor and prevent other patrons from trying to observe PIN entry.

For different roles, devices and positions, please refer to Table 4-2 for guidance on the security measures for PIN entering.

Table 4-2 PIN Entering Protection Guidance

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	Keep a distance.	Keep a distance.	Out of sight of the	Out of sight of the cameras.

	shield PIN.			cameras.	

4.7. Patching and Updating

The firmware is downloaded remotely through Wi-Fi or Cellular. The application is downloaded and installed through the USB interface.

4.7.1 Firmware

1. Vendor releases new versions of firmware and notifies users of updates or patches through system notifications.
2. The released firmware is signed by the vendor.
3. After the device verifies the firmware, correct firmware will be installed and successfully run, while incorrect ones will be rejected and removed.

After update, the device firmware version will be updated synchronously, the firmware version can be checked as shown in figure 2-3.

4.7.2 Application

1. The developers releases the new version of the Application. The system notifies end users (merchants) to update the application.
2. The released application is signed by the developers.
3. After the device verifies the application, correct application will be installed and successfully run, while incorrect ones will be rejected and removed.

4.8. Decommissioning

When the device is no longer used because of permanent decommissioning reason, the administrator of the device needs to gather the device and then erase all the key materials on it. This can be done by directly disassembling the device to make it unavailable.
Disassembling the device will cause it to tamper and the device will erase all payment keys. Thus, the device can be safely deactivated.
For 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 mechanisms.

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 more information about software development guidance, please refer to the document *Software_Development_Secure_Guidance*.

5.2. TLS

The device supports TLS. However, for TLS firmware development please refer *Software_Development_Secure_Guidance* and for compliance with PCI PTS v6.2, the following points need to take attention.

◆ The device verifies the certificate of the server.

◆ The cipher suite of the server to which the terminal connects should be as secure as TLS_RSA_WITH_AES_128_CBC_SHA or more secure.

◆ The server to which the terminal connects should be configured to require Client Authentication.

◆ TLS v1.2 or higher should be used.

◆ The firmware developer must use SHA-256 on top of the security protocol when it is being used for security functionality.

5.3. Wi-Fi

The Wi-Fi interface is configured by the operating system to enforce encryption, the WEP access point has been disabled. All shared and open networks have been disabled.

5.4. Signing

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

P10 software is signed by the vendor including boot stages code, firmware, updates and patches.

The signing tool is used to sign user applications and vendor firmware. The signing tool administrator performs the signing process under dual control.

The application is verified by the firmware before it is loaded and executed. If the verification fails, the application cannot be loaded into the device and executed. The signature and verification mechanism ensures the authenticity and integrity of the application that is loaded into device.

For the detailed signing flow, please refer to Key Management for Firmware Developer.

5.5. Account Data Protection

P10 uses the account data to perform payment transactions, the account data is encrypted by a protection key to prevent clear text account data from transmitting via an open network.

The clear text account data cannot be output on the device in any situation.

P10 enables SRED function by default, and this function cannot be disabled.

The account data is protected by encryption keys, which allows TDEA-192bits, AES-128bits and AES-192bits algorithms.

Manual PAN entry where no more than one clear-text PAN digit may be displayed at a time, and a PAN digit displayed during entry must be obfuscated prior to the display of the next digit.

P10 does not support whitelists.

5.6. Algorithms Supported

All of algorithms the P10 supports are listed in table 5-1.

Table 5-1 Algorithms Supported

Algorithm	Usage	Key Management Method
RSA (2048bits)	Internal Signature verification.	N/A
SHA256	Internal Signature verification.	N/A
TDES (128/192bits)	Keys	MK/SK
TDES (128bits)	Keys	DUKPT
AES (128/192bits)	Keys	MK/SK
ECC (P-224/P-256/P-384)	keys	N/A

All key information the P10 supports are listed in table 5-2.

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

5.7. 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 Base Derivation Key.
  This Base Derivation Key
  -MUST reside in a TRSM which relies exclusively on physical barriers.
  -reside 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.

5.8. Key Loading

The TLK loading has been performed in a key loading facility which provides a secure room.
Two operators need to enter their own password to start the key loading process to meet the dual control requirement.
The TLK is loaded into device as two components. Each component of TLK is input by a different person via the touch screen. Each person should only know their own component to meet the knowledge separating requirement.
The Master Keys are loaded into device in cipher text, which is encrypted by TLK.
The Session Keys can be divided into five usages: TPK (Terminal PIN Encryption Key), TAK (Terminal MAC Key), TDK (Terminal Data Decryption Key), TEK (Terminal Data Encryption Key) and TTK (Terminal Account data Encryption Key) which are loaded into device in cipher text, which is encrypted by Master key.
The initial key of DUKPT is loaded through API, 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 newly generated future key.

5.9. 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 notify the security personnel of vendor and service provider.
The key lifetime is controlled by the 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.

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
TRSM	Tamper-Resistant Security Modules

7. References

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

[2]. ANSI X9.143-2021 Retail Financial Services Interoperable Secure Key Exchange Key Block Specification

[3]. ISO 9564-1 2017, 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, v6.2

[6]. Device Default Settings Overview

[7]. Software_Development_Secure_Guidance

[8]. Firmware Update User Manual

[9]. Key Management for Firmware Developer