MAXPAY INTERNATIONAL PAZARLAMA TRADE LLC.

TECHNO-P3

PCI PTS POI Security Policy

2022-04-11

V0.4

Revision History

Date	Revision Level	Description	Revisor
2021-8-1	V0.1	Create Document	Cedar
2021-9-26	V0.2	Update figures	Cedar
2021-12-17	V0.3	Fix misspellings. Update section 2.2, 2.3, 4.5, 4.6, 4.8, 5.3 and 5.8	Cedar
2022-04-11	V0.4	Update section 2.1	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 V5.1.

This product is for indoor usage, and 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, which is not 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 TECHNO-P3 , the appearance shown in Figure 2-1.

Figure 2-1 TECHNO-P3 Appearance

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

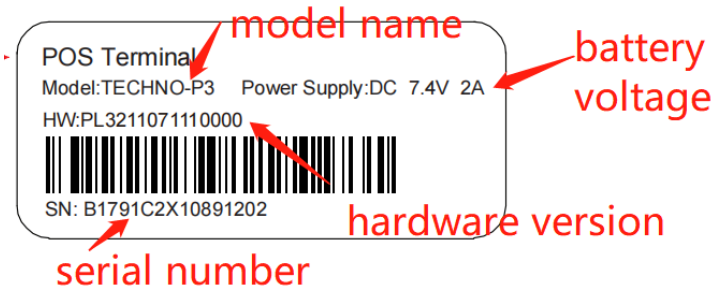

Figure 2-2 Device Label

TECHNO-P3 has several hardware configurations shown in the Table 2-1.

Table 2-1 Hardware Configurations

Configuration	Parameter and Capability
Front Camera	None
	0.3M Pixels
Cellular Network	2G + 3G + 4G
	2G + 3G

.

Micro SD Card	None
	1 Slot
Magnetic Cable	None
	Support

2.2. Product Type

Generally, TECHNO-P3 is a handheld PED device for financial transaction in attended environment. When fixed on desktop, TECHNO-P3 is used as a desktop PED device.
TECHNO-P3 provides integrated physical keypad for PIN Entry, color display, touch screen (not for PIN entry), magnetic-stripe reader (MSR), IC card reader (ICCR), contactless card reader (CTLS), thermal printer, camera(optional), cellular(2G/3G/4G), Wi-Fi, Bluetooth and USB communications.

2.3. Identification

Hardware Version Number Description:
PL31111x111xxxx (with MediaTek MT6739, with fiscal module)
PL32111x111xxxx (with MediaTek MT8765, with fiscal module)
PL32110x111xxxx (with MediaTek MT8765, without fiscal module)

The role of "x" is shown in the Table 2-2.
Table 2-2 Hardware Version Format

Variable “x” Position	Description of Variable “x” in the Selected Position
8	Used to Cellular RF technology support code configuration.
12	Device color style configuration.
13	Front camera configuration.
14	MicroSD slot configuration.
15	Magnetic cable configuration.

Firmware Version Number Description:

3901.25.xxxx.xxx.xxx

‘x’ indicates minor non-security related changes.

The role of "X" is shown in the Table 2-3.
Table 2-3 Firmware Version Format

Variable “x” Position	Description of Variable “x” in the Selected Position
9-12	Changes to rectify errors, faults and non-security function on application processor.
14-16	Changes to rectify errors, faults and non-security function on cellular module.
18-20	Changes to rectify errors, faults and non-security function on security processor.

.

The hardware version is located on device label as is shown in Figure 2-2.

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

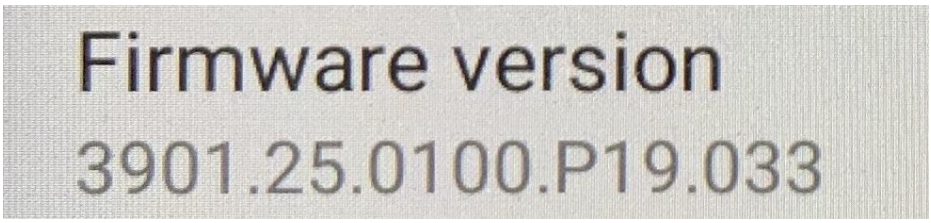

Figure 2-3 Firmware Version Example Screen Shot

.

3. Installation and User Guidance

3.1. Initial Inspection

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

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

TECHNO-P3 is an integrated payment terminal. Please ensure the terminal been installed in favor of merchants and cardholders, as close as possible to the power socket.
To prevent PIN leakage, the PIN entry device should avoid being monitored by security cameras.
Terminal should keep away from heating source, vibration, dust, moisture and electromagnetic radiation (such as computer screen, motor etc.).
Be sure this terminal is used only in attended way.
The power socket is USB cable and magnetic suction cable dock on left side of device.

Figure 3-1 Power Socket

.

3.3. Environmental Conditions

The environmental conditions to operate the device are specified in the user manual.
This device is a handheld or desktop 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.

Power Adaptor Specification:

Input: 100 to 240V AC, 50 Hz/60Hz
Output: 5V 2A

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)	TCP/IP, SSL/TLS, UDP, DHCP, ICMP and PPP
Wi-Fi	TCP/IP, SSL/TLS, UDP, DHCP, ICMP and ARP
Bluetooth	Bluetooth 4.2 BR/EDR/HS Security mode 4 Level 4

Merchant can use all these communication interface directly after installed 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

Daily check the terminal (including LCD, keypad, etc.) to ensure that it is free of rogue overlays.
The end users or acquirer should daily check that the 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 or acquirer should also daily check that the installation/maintenance operations are performed by a trusted person.
Especially daily 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.

Figure 4-1 ICCR/MSR slot

Daily check if terminal is triggered. Please refer to chapter 4.5 for trigger prompt.

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

Three roles involved in the device operating.

- The vendor sells devices to acquirers or re-sellers and provides technique and maintenance supports.
- Re-sellers sell the devices to end users and provide services to their end users.
- 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	Vendor	● Sign software and firmware ● Develop firmware ● Repair device and unlock device of tampered
Administrator	Re-Sellers/ Acquirers	Access device sensitive service
Operator	End Users	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 password, please refer to the *[6].*

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:

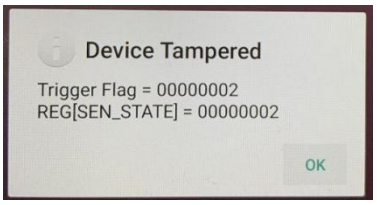

Figure 4-2 Device Blocked Prompt Demo

.

- Cannot enter normal application and cannot do any transaction.
- Beep alarm and blink on LED indicator.

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

TECHNO-P3 is used only in an attended environment. It is generally used as a handheld device, and also is used as desktop device when it is fixed on the desktop. It is required to provide cardholders with the necessary privacy during PIN entering when TECHNO-P3 is used as desktop device.

For example, the device will demonstrate a safe PIN-entry process how to entry PIN. This message reminds cardholder that he can use his own body or their free hand to block the view of keypad.

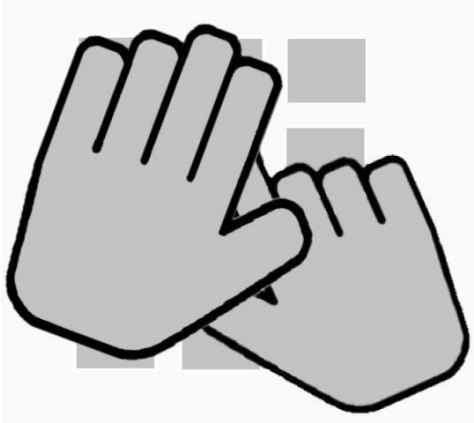

Figure 4-3 Safe PIN Entering Logo Example

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

Method	**Observation Corridors**				
	Cashier	Customer in Queen	Customer Elsewhere	On-Site Cameras	Remote Cameras
With Stand	No Action Needed.	Customer positions PED	No Action Needed.	Do not install within view of cameras.	Do not install within view of cameras.
Without stand	Position unit to face away from the cashier. Use signage to block cashiers view.	Position unit between customer and the next in cue.	Used the body to block the view of other customers and the device.	Do not install within view of cameras.	Do not install within view of cameras.
Customer Instruction	Used the body to block the view of the cashier and the device.	Used the body to block the view of other customers and the device.	Used the body to block the view of other customers and the device.	Do not operate within view of cameras.	Do not operate within view of cameras.

.

4.7. Patching and Updating

This terminal supports remote updating or patching the software.

- Power on device.
- Configure device to connect network via Wi-Fi or Cellular.
- Device will automatically connect to remote server to check update or patch.
- Device will download update or patch.
- Device will verify the update or patch.
- Device will apply the update or patch which has been verified.
- Device will reject and delete the incorrect update or patch.

After update, the device firmware version will be updated synchronously, and you can check the firmware version as is shown in Figure 2-3.

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. It can be done by directly disassembling the device to make it unavailable.

Because, disassembling the device will make it to tamper status and the device will erase all payment keys. Thus, the device is decommissioned securely.

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 and 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. SSL/TLS

The device does not support SSL. For SSL/TLS firmware development please refer *[7]* and the compliance with PCI PTS, the following points need to take attention.

- The client must authenticate the CA certificate and client 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. BLUETOOTH

Bluetooth interface is configured by the Operating System to enforce encryption and use secure pairing options only. The device uses Bluetooth 4.2 BR/EDR/HS Security mode 4 Level 4. No security sensitive configuration settings are necessary to be modified by the end user to meet the security requirements. Bluetooth Low Energy is not supported.

5.4. Signing

The digital signature algorithm is based on RSA-2048 bits and SHA-256.
TECHNO-P3 software is signed by vendor including boot stages code, firmware, updates and patches. The detailed signing flow please refer to *[8].*

5.5. Account Data Protection

TECHNO-P3 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.
TECHNO-P3 has printer function and support printing the payment list, to protect account data, the account data printed has to be masked to show the first six and the last four digits of PAN data. The clear text account data cannot output in printer or display screen in any situation.
TECHNO-P3 enables SRED function by default, and this function cannot be disabled.
The account data is protected by TTK which allows TDEA-192bits, AES-128bits and AES-192bits algorithm.

5.6. Algorithms Supported

All of algorithms TECHNO-P3 support is list 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 and DUKPT
AES (128/192bits)	Keys	MK/SK

All keys information TECHNO-P3 support is list 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 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.

5.8. 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 cipher text 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.

5.9. 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 inform and notify 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
TRSM	Tamper-Resistant Security Modules

.

7. References

[1]. ANS X9.24 Part 1:2009/2017, 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]. XC-PCI-L206_Device_Default_Settings_Overview_V1.2
[7]. Software_Development_Secure_Guidance_V1.0
[8]. XC-PCI-L205_Key_Management_P1_for_Firmware_Developer_V1.1

.