大趋智能 TRENDIT	FILE NAME	**PCI Security Policy for T3**		
	FILE NO.			
PCI Approval	VERSION	V1.01	CLASS	PUBLIC

PCI Security Policy for T3

FILE NAME	**PCI Security Policy for T3**		
CLASS	PUBLIC	FILE NO.	

No	VER	DATE	REVISION	AUTHOR	AUDITOR
1	V1.00	2021-6-20	Original Version	HJW	SXL
2	V1.01	2021-8-25	Adjust format	HJW	SXL

CONTENTS

1 Introduction 4

2 Scope 4

3 Acronyms 4

4 Reference 4

5 Security Policy 5

5.1 Product Overview 5

5.2 Product Identification 6

5.3 User Guidance 6

5.4 Hardware Security 9

5.5 Software Security 10

5.6 System Administration 11

5.7 Key Management 11

5.8 Open Protocol 12

5.9 Account Data Proctection 13

5.10 Communication methods and protocols 13

5.11 Default Values 13

5.12 Roles and Services 13

1 Introduction

This document describes the basic security policy for TRENDIT T3 PED POS device. It is used to guide product users and developers utilizing the security features more properly. The device is compliant to PCI PTS POI V6.0.

2 Scope

This documentation is applicable for TRENDIT T3 POS terminal.

3 Acronyms

Abbr.	Description
TDES	Triple Data Encryption Standard
SHA	Secure Hash Algorithm
RSA	Rivest Shamir Adelman Algorithm
DUKPT	Derived Unique Key Per Transaction
PIN	Personal Identification Number
PED	PIN Entry Device
SRED	Secure Read Exchange Data
OP	Open Protocol
AES	Advanced Encryption Standard
ECC	Elliptic Curve Cryptography

4 Reference

[1] X9 TR-31 2018, Interoperable Secure Key Exchange Key Block Specification for Symmetric Algorithms

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

[3] ANSI X9.24 Par2: 2016, Retail Financial Services Symmetric Key Management Part 2: Using Asymmetric Techniques for the Distribution of Symmetric Keys

[4] ISO 9564-2, Banking — Personal Identification Number (PIN) management and security Part 2: Approved algorithms for PIN encipher

[5] PCI PTS POI Modular Derived Test Requirements Version 6.0 – June 2020

[6] TRENDIT POS Terminal Logical Security Specification for T3 v1.01.docx

[7] Software Development Control Program.docx

[8] Firmware Development Coding Rules Specification.docx

[9] TRENDIT POS Terminal Operation Manual for T3.docx

[10] POS Terminal Open Protocol Security Description.docx

[11] TRENDIT POS Terminal API Specification.docx

[12] TRENDIT POS Terminal Signature Specification.docx

5 Security Policy

5.1 Product Overview

The device is approved as a handheld PED (PIN Entry Device) under version 6.0 of the PCI PTS POI security standard, and designed to be used in an attended environment.

Use of the device in an unapproved method will violate the PCI PTS POI approval of the device.

TRENDIT POS T3 is a Stand-alone POS terminal for financial transactions which supports the following functions:

- Physical keypad
- Touch Panel (for signature only)
- Display
- Magnetic Stripe Reader (MSR)
- ICCR
- Speaker
- SIM Slot
- SAM Slot
- Printer
- Bar-code scanner
- Type-C USB Port
- Cellular
- Wi-Fi
- CTLS

And this device supports the following protocols:

- TLS, IP, TCP, UDP, ICMP, ARP, DHCP, PPP

The appearance of this device is shown as below:

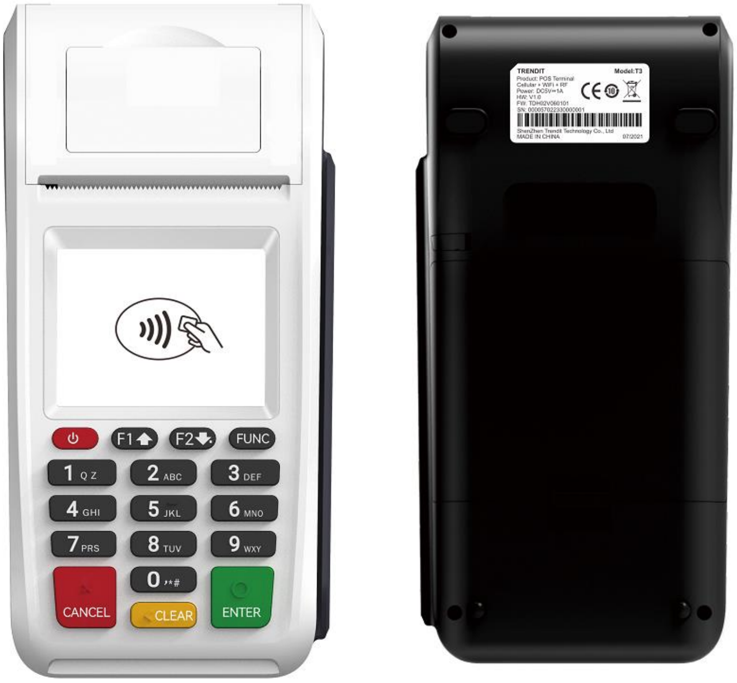
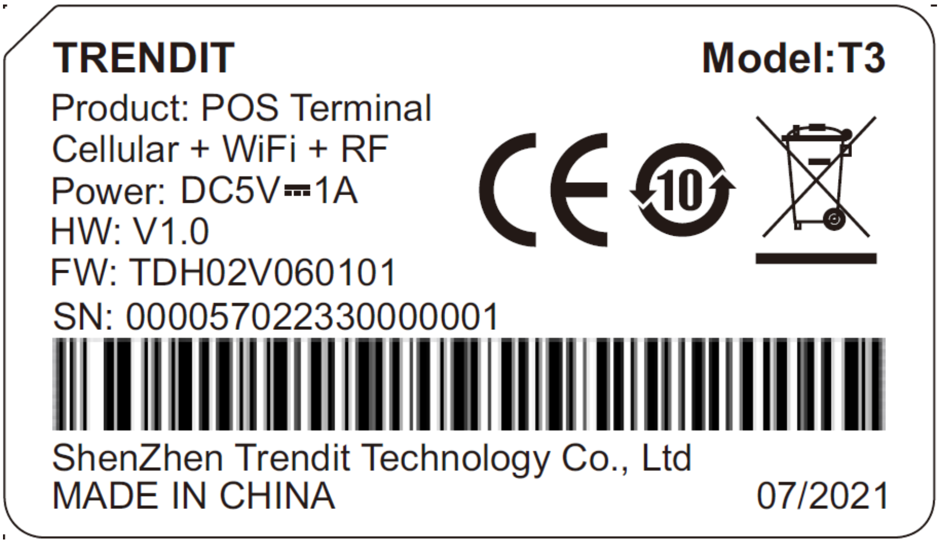


Figure 5-1 device appearance

5.2 Product Identification

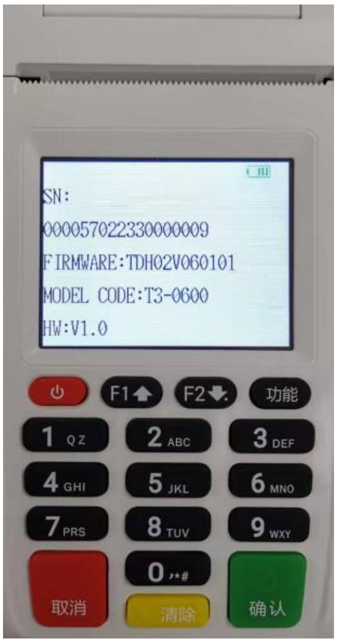
The product name and hardware version are printed on a label on the device. The HW version can be identified from this label. Please see below picture.



TRENDIT
Model:T3
Product: POS Terminal
Cellular + WiFi + RF
Power: DC5V⎓1A
HW: V1.0
FW: TDH02V060101
SN: 000057022330000001
ShenZhen Trendit Technology Co., Ltd
MADE IN CHINA
07/2021

Figure 5-2 Device Product Identification

The firmware version can be retrieved by using the software menu. User can press the buttons “Power + Function” to enter the manage menu, then select the “5.Version” and find the FW version as shown in “FIRMWARE” item of the following picture.



```
SN:
000057022330000009
FIRMWARE:TDH02V060101
MODEL CODE:T3-0600
HW:V1.0
```

Figure 5-3 Device FW Version

5.3 User Guidance

This chapter is aimed to introduce how to use this device securely.

5.3.1 User Guide

The user should check if all items are intact when he receives the device at the first time. The items along with the device include a T3 device, a battery, a power supply, and a copy of user guide specification. Before using this device, user needs to check if it is genuine and ready for use. If anything is lacking or damaged, user should contact with the vendor for inspection, refunded or exchange

5.3.2 Secure Usage Environment

This device is designed to be used in an attended environment.

Also, the device can only be used normally under a specific environmental condition. When the device detects an abnormal conditions existed, a tamper event will happen and all the sensitive data will be cleared.

5.3.3 PIN Entry Guide

Please note, if the device T3 is used in an unapproved method this will violate the PCI PTS approval of the device. As the T3 is a handheld PED without a privacy shield, so 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 the below picture:

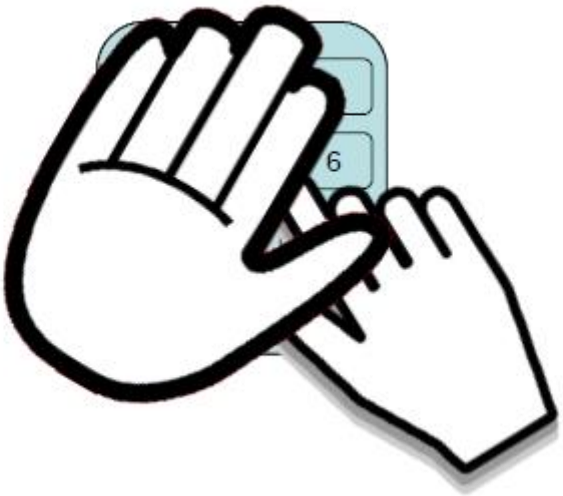


Figure 5-4 Safe PIN Input

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.

Note: Use the POI via an unapproved method will invalidate any PCI PTS approval of this POI.

5.3.4 Device Periodically Checking

The merchant or acquirer must visually inspect the terminal when received via shipping. The merchant or acquirer also must inspect the terminal daily to ensure that:

- The terminal is not destroyed.
- There is no malicious bug inserted in the terminal.
- No suspicious wires are connected to any ports of the terminal. No overlay is on the keypad of the device.
- HW and FW versions on terminal label or screen are consistent with the approved ones.
- No visible open case evidence via inspecting the device shell or the labels in screw holes.
- Installation and maintenance operations are performed by a trust person.
- No suspicious thing appearing in ICC and MSR reader, as shown in the below pictures:

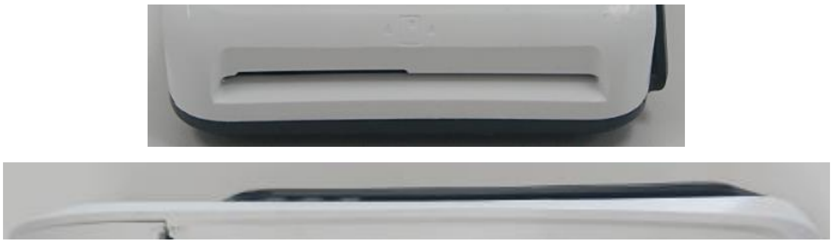


Figure 5-5 ICCR and MSR Slots

5.3.5 Secure Use ICC

To make sure IC card is being used securely, the merchant will be informed to check the following cases:

- Check whether a suspicious wire is around IC card opening. If yes, please stop using the device and inform the vendor for security inspection.
- Check whether IC card can be inserted smoothly. If no, please stop using and inform the vendor for security inspection.
- Check whether the shell of IC card reader interface is intact. If any damage evidence is found, please stop using and inform the vendor for security inspection.

5.3.6 Secure Use MSR

To make sure MSR being used securely, the merchant will be informed to note the following cases:

- Check whether a suspicious wire is around MSR guide. If yes, please stop using and inform the vendor for security inspection.
- Check whether swiping card is smooth. If no, please stop using and inform the vendor for security inspection.
- Check if there is any addition beside the MSR from the hollow guide. If yes, please stop using and inform the vendor for security inspection.
- Check if MSR guide is destroyed. If yes, please stop using and inform the vendor for security inspection.

5.3.7 Secure Use SRED

- This terminal support SRED function and a key of appropriate length is used mandatorily. Double-length TDES keys are not permitted for use in SRED in Master/Session.
- Account data and related key buffer must be cleared immediately after use or when the transaction exits. The device does not support pass-through of clear-text account data.
- The device does not allow the disablement (turning off) of SRED functionality.

5.3.8 Dealing with Fault

The merchant or acquirer should always check the status of the device being used. The devices which is locked or displays abnormal information must not be used for PIN transaction any more. When a tamper event occurs, the device must be inspected by the vendor. Users are advised to contact vendor for further and detail security inspection.

5.3.9 Procedures for Decommissioning Device

Devices should be gathered in a secure manner once they are decommissioned permanently. And all sensitive information must be erased mandatorily. This can be done by tampering the device by open the case to delete all sensitive information actively. Then these devices are mandatorily transported back to vendor factory for destruction and recycling.

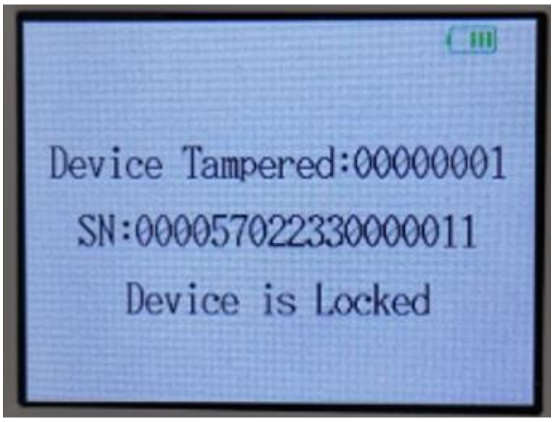
If a temporary removal is required, it is unnecessary to change the status of the device because all sensitive information is still under the protection of physical and logical security mechanism.

5.4 Hardware Security

The device has tamper mechanisms to protect the terminal from being attacked.

5.4.1 Tamper Response Event

When a tamper is detected, the device appears as follow:



Device Tampered:00000001

SN:00005702233000011

Device is Locked

Figure 5-6 Device Tamper Display

A merchant or acquirer can easily determine if a tamper event happened in the terminal. A warning message will be displayed on the screen and the terminal is locked when tampered. No other signal is used to prompt tamper. Then all the sensitive data are erased. Any happened tamper event will make the device go out of normal service. The device has 2 separate modes as below:

- Activated mode: the device is fully operational.
- Freezing Mode: the device is tampered and can’t be operated. It needs reactivation after maintenance and security checks.

The device should be mandatorily send back to the vendor for security checking and repairing when it is tampered.

5.4.2 Environmental Conditions

The environmental conditions to operate the device are specified in the device’s specifications.

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 range does not compromised the security.)

- Power
  Input power: DC 5.0V
- Operation Condition
  Temperature: 0 Celsius to 50 Celsius
  Relative Humidity: 5% to 95%
- Tamper Trigger Condition(out-of-range)
  Security Sensor Temperature: -40℃ to 105℃
  Backup Battery Voltage: 2.1V to 4.2V

When the terminal exceeds the above tamper trigger range, the device will be tampered.

5.5 Software Security

5.5.1 Software Development Guide

The developer must accept training course before development activity starting and must follow the coding rules during the whole development stage. Reference [7] and [8] document can provide more details.

The application development interface document please refer to document [11].

The device can communicate through Wi-Fi and Cellular interfaces. As public domain is not secure, user is recommended to refer to the OP document that guides how to communicate with public domain securely. For the guidance document for OP, please reference to document [10].

For getting SRED data such as PAN data of MSR, IC Card and CTLS. Please refer to SRED document that guides how to use API. The guidance document for SRED is referred to as document [11].

The terminal supports firmware updates. New firmware needs to be signed, and updates will be rejected when signature verification fails. The guidance document for the firmware please refer to document [12].

5.5.2 Firmware and Software Update

The terminal support local upgrade, the terminal only accepts firmware and applications that have legitimate and correct signatures.

The application and firmware loading process does not need protection by any special way. The device will reject to load and save any unauthenticated application and firmware.

5.5.3 Firmware and Software Authentication

This device implements asymmetric cryptographic algorithm for firmware authentication. RSA algorithm with 2048bits key is used for signature verification and SHA256 algorithm is used to calculate the digest of firmware.

The firmware is signed by RSA-2048 bits private key which is only controlled by TRENDIT. And signature is verified by the corresponding public key. The terminal will check the integrity and validation of firmware and application during every start-up. If the check fails, the terminal will stop working.

All the certificates related with application and firmware will also be verified. These certificates are based on couples of RSA keys.

5.5.4 Key Checking

All key stored in the terminal will be checked during every start-up and before each use. If the check fails, the keys will be erased.

5.5.5 Self-Test

Self-test is automatically executed upon start-up and every reboot. This checking is also performed periodically (once 23 hours) during the period of normal use. This test is not initiated by an operator.

The self-test will reinitialize the memory, verify the integrity and legitimacy of firmware and application, detect if the terminal is tampered and verify whether all keys are valid.

5.5.6 Signature Mechanism

TRENDIT use a client signature tool based on a signature server system to sign firmware and application files. The signature server system implements a serial of important functions such as access control, permission management, file signature, log management and etc.

A pair of signature operators will be granted permission to login this system and do signature operation. Only when both of them are identified by the system (through successful entry of respective passwords) during a window time, they can use the signature function to sign firmware or application.

During the whole signature process, private key always remains in the hardware encryption machine and can never be exported. Only signed file will be exported to outside. RSA-2048 and SHA-256 algorithms are used in the signing/authentication processes. Certainly, any operation trace will be recorded by this system to make it more secure.

5.6 System Administration

5.6.1 Configuration Settings

The device is functional when it is received by the merchant or acquirer. No security sensitive configuration settings are necessary to be tuned by the end user to meet security requirement.

5.7 Key Management

5.7.1 Key Management Techniques

The T3 terminal implements two different types of key management techniques:

- **Master Key/Session Key:** a method using a hierarchy of keys. The session keys are unique per terminal.
- **DUKPT:** a key management technique based on a unique key for each transaction

Note: Use of the POI with different key-management systems will invalidate any PCI approval of this POI.

5.7.2 Cryptographic Algorithms

The T3 POS terminal can support the following secure algorithm:

Algorithm	Size (Bits)
SHA-256	-
Triple DES	128/192
RSA	2048
AES	128/192/256
ECC	P-256/P-384/P-521

5.7.3 Key Management

RSA certificates are used in this device. The key sizes are 2048 bits.

Key Name	Purpose/Usage	Size (Bits)	Storage
TRENDIT ROOT PK	Used to authenticate TRENDIT PK	2048	Hardcoded in UBOOT
TRENDIT PK	Used to authenticate Firmware	2048	Verify by TRENDIT ROOT PK
ACQUIRER ROOT PK	Used to authenticate ACQUIRER PK	2048	Hardcoded in AP MANAGE APP
ACQUIRER PK	Used to authenticate user application	2048	Verify by ACQUIRER ROOT PK

The transaction related keys are classified as following description. The algorithm used by following keys is TDES and AES. These transaction keys are controlled and generated by acquirer. The key loading must be under dual control. And all key loaded into the device can’t be obtained from external by any way. These keys can only be used for their intended purpose via the interface or commands provided by the device.

Key Name	Purpose/Usage	Algorithm	Key Size (bits)	Storage
TMK	Master Key of MK/SK. Decryption of session keys (PINK/MACK/TDK).	TDES	128/192	SP Flash
PINK	Online PIN Encryption.	TDES	128/192	SP Flash
MACK	MAC Encryption.	TDES	128/192	SP Flash
TDK	Account Data Encryption.	TDES	192	SP Flash
AESTMK	Master Key of MK/SK. Decryption of AESPINK.	AES	128/192/256	SP Flash
AESPINK	Online PIN Encryption	AES	128/192/256	SP Flash
TDES_IPEK	Used to derive TDES Future Keys	TDES	128	SP Flash
TDES Future Keys	Derivation of PIN encryption keys, MAC keys and Data key for each transaction	TDES	128	SP Flash
AES_IPEK	Used to derive AES Future Keys	AES	128/192/256	SP Flash
AES Future Keys	Derivation of PIN encryption keys for each transaction	AES	128/192/256	SP Flash

5.7.4 Key Injection Method

All initial keys of the terminal support local key injection.
For local key injection, keys are injected to the device using an authentic Key Loading Device, provided by TRENDIT, in a secure environment.

5.7.5 Key Replacement Policy

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 a tamer event has happened, the device must be returned to TRENDIT for security inspection and use the Key Loading Device to inject keys again.

5.7.6 Key Removal

There are two ways to remove the keys installed. One is passively erasure by firmware or hardware, like when a tamper event happened. The other is actively cleared by security manager via dedicate tool, in case of repair or decommissioning.

5.8 Open Protocol

The following describes the communication methods and protocols available in the device.

	Interface	Protocols
Communication	Cellular	TLS, IP, TCP, ICMP, UDP, PPP, DHCP
	Wi-Fi	TLS, IP, TCP, ICMP, UDP, ARP, DHCP

Data transferred between terminal device and server is encrypted with security protocols TLS v1.2. Application developers can achieve by calling library. The device does not support SSL.
The device supports Cellular and Wi-Fi communication methods. The device supports Wi-Fi with WPA/WPA2 encryption options. WEP and no encryption options are not allowed by the device. Reference [10] document can provide more details.

5.9 Account Data Protection

The device owns a complete set of security mechanisms to protect the security of account data, support account data encryption and prevent the exhaustive search of account data.
The device does not allow output the plaintext account data, it only support truncated mode and encryption mode.
The application could not directly output the PAN in plaintext, it requires to output the PAN in truncated or cipher text mode.

5.10 Communication methods and protocols

The device supports USB, Cellular and Wi-Fi communication. The device supports the following protocols: TLS, IP, TCP, ICMP, UDP, ARP, DHCP, PPP.
The Type-C USB port using USB 2.0 specification, and only support the slave mode. The device Type-C USB interface can be used for local firmware upgrade, de-tamper function, and follow the standard USB serial protocol.
Use of any method not listed in the policy invalidates the device approval.

5.11 Default Values

There is no security related default value that is necessary to be changed before operating the device.
The device does not need any change of certificate.

5.12 Roles and Services

The customers of TRENDIT are acquirer or Value Added Resellers (VAR). TRENDIT as a vendor sells devices and provides support for technical issues as well as maintenance to acquirer. The acquirer sells the devices to end users and provides services to their end users. TRENDIT, acquirer and end users play different roles in operating the device.
Below table shows different roles and operations.

Entity	Role	Responsibilities
VAR/Acquirer /Merchant	administrator	1.Organize the third party to develop application program; 2.Download customer public key and application
End User	operator	Perform transaction
Vendor(TRENDIT)	maintainer	1.Sign customer public key 2.Repair device and unlock the device if tampered