鼎智通讯
Topwise Communication co., LTD

# SECURITY POLICY FOR T1

鼎智通讯 TopWise Communication Co.,Ltd

# Security Policy for T1

# Contents

# Security Policy for T1

RECORD OF REVISIONS

| Revision | Type of modification | Author | Date |
|---|---|---|---|
| V1.0 | Document creation | Ouyangweiquan | 2017-09-27 |
| V1.1 | Update | Ouyangweiquan | 2017-11-13 |
| V1.2 | Update | Leila Zhang | 2017-12-04 |
| V1.3 | Update | Ouyangweiquan | 2018-01-17 |
| V1.4 | Update | Leila Zhang | 2018-02-05 |
| | | | |

# Security Policy for T1

## 1. Introduction

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 use of the device in an unapproved method, as describe on the security policy, will violate the PCI PTS approval of the device.

## 2. Acronyms

- TDES/3DES: Triple Data Encryption Standard.
- AES: Advanced 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.
- N/A: Not Applicable.
- IC Card: Integrate Circuit Card.
- RF Card: Radio Frequency Card.
- KCV: key check value.
- KMS: Key Management System

## 3. Scope

This documentation is applicable for Topwise intelligent POS terminal and will be only released for trusted developers, testers, internal users and end users.

This document describes the basic security policy for developers and users to ensure the proper use of FW security features in Topwise Devices and for compliance with current security standards.

This document must be read in conjunction with the related Reference Documentations. The document covers the following products: T1 (Handheld POS).

## 4. Reference

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

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

[3] ANSI X9.24 Par2: 2006, Retail Financial Services Symmetric Key Management Part 2: Using Asymmetric Techniques for the Distribution of Symmetric Keys

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

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

[6] PCI PTS POI Modular Derived Test Requirements V5.0 –September 2016

[7] T1 user manual

[8] open protocol guidance

[9] application development guide

# 5. General Description

The device is an integrated handheld Point of Sale (POS) terminal, to process PIN-based transactions in an attended environment. The device is PCI PTS Version 5. approved as PED device class.

## 5.1 Production Overview

T1 is the new generation of intelligent wireless POS with touch-screen and high-speed communications. This product is mainly for indoor usage and its target merchant are the restaurants, entertainment, chain stores, supermarkets, E-commerce and so on.

This device is a PIN entry device; it can be used as the standard POS to undertake financial transactions. Performing the PIN entry, MAC calculation, Data encryption/decryption and some other functionality provided.

This device provides touch screen keypad, contactless card reader, ICCR, MSR, LCD, SAM card reader and high performance thermal printer. It is designed for a portable and handheld use, so that the device can be shielded by the body when in work. The power system is based on battery and the communications to the external world are based on USB, Bluetooth, WIFI, 2G/3G/4G wireless connection.

Figure 1: T1 Appearance

## 5.2 Production Identification

Product Name: T1.

Hardware Version: V1.x.x. The “x” is non-security related.

The product name and hardware version are printed on a label on the device.


Figure 2: T1 Label

The merchant or acquirer must visually inspect the terminal when received via shipping, as it is described in the user manual.

For example, the merchant or acquirer should inspect the terminal to ensure that:

- There is no evidence of unusual wires that have been connected to any ports of the terminal
- There is no shim device in the of the ICC acceptor

To examine the version of firmware of the device, we can launch “Settings”, then “about pos”, the version info will be shown in the column “Firmware version”.

To examine the version of hardware of the device, we can launch “Settings”, then “about pos”, the version info will be shown in the column “Hardware version”.

## 5.3 Communication Methods and Protocols

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

| | Interface | Protocols |
|---|---|---|
| **Communication** | Wireless Modem (Support GSM, CDMA, TD-SCDMA, WCDMA, EVDO, TD-LTE, FDD-LTE) | SSL/TLS, TCP, UDP, DHCP, DNS, ICMP, HTTP, PPP, IP Stack |
| | Wi-Fi | SSL/TLS, TCP, UDP, DHCP, DNS, ICMP, HTTP, IP Stack |
| | Bluetooth | Classic Bluetooth |
| | USB | USB 2.0 |

Table 1. T1 Communication Methods and Protocols

# 6. Security Guidance

Before using the device, user need to check device firstly to see if it is genuine and ready for use.

Meanwhile user should also refer to the <T1 user manual> attached within the packing case.

To inspect the received device, please check carefully of the following aspect described in the rest of this section.

## 6.1 Installation Guide

A user manual including the following information is provided with the device.

Equipment check list:

- Device
- Cable and connectors
- T1 user manual

## 6.2 Installation and Environment

Please ensure the terminal installation in favor of merchants and cardholders have very convenient level, as close as possible to the power socket.
Terminal should stay away from all sources of heat, to prevent from vibration, dust, moisture and electromagnetic radiation (including computer screen, motor, security facilities etc.). Please be noted that the wireless terminal should also be away from complex condition like electromagnetic radiation when in use.
Be sure that terminal is used in an attended way.

## 6.3 Decommissioning/Removal

When the device is no longer used for permanent decommissioning reason, the administrator of the device needs to gather the device and disassemble the device to makes it unavailable. Even though someone reassembles the device, it still cannot work as its all keys have been erased automatically and it will warn exception because of the tamper triggered by disassembling.
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 main board hardware tamper mechanism.

## 6.4 PIN Confidentiality

T1 is a hand-held devices, 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 enter PIN. This message reminds cardholder that he can use his/her own body or his/her free hand to block the view of keypad.

Figure 3: Safe PIN Entry Logo Example

## 6.5 Periodic Inspection

The merchant 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 merchant or acquirer should also check that the installation/maintenance operations are performed by a trusted person, especially check if the ICC reader slot is damaged, such as abrasion, painting and other

machining marks, and if there is any suspicious object like lead wire over ICC reader slot, or any unknown object inside IC card. If these suspicious circumstances are found, please stop using the device immediately and contact the customer service to confirm if the device has been tampered.

# 7. Product Security

Users should refer to T1 user manual before installation. The following requirements and recommendations are applicable during the Installation Phase.

## 7.1 Tamper Response Event

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:

- Warning message is displayed on the screen, for instance, please refer the Figure4
- Can't enter normal application and can't do any transaction but online activation


Figure 4: Locked mode

The user needs to send the device to the manufacturer for safety inspection and repair.

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

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

- Activated mode: the device is fully operational
- Locked mode: the device is tampered, not operating and needs reactivation after maintenance and security checks
- From Locked mode switch to Activated mode, the device has to do online activation for authentication

In the Locked mode, we can click 7 times the screen continuously at the location of the prompt information. We can enter the online activation operation interface and complete the online activation according to the prompt. However, the online activation requires the authorization of the manufacturer, and the unauthorized operation is unsuccessful.

## 7.2 Environment Conditions and Environmental Failure Protection

The environmental conditions to operate the device are specified in the below condition.

- Working Environment:

Temperature: 0℃~50℃(32℉~122℉)

R.H.: 10%~93% (Non-condensing)

- Storage Environment:

Temperature: -20℃~70℃(-4℉~158℉)

R.H.: 5%~95% (Non-condensing)

- Power supply:

DC 5V/2A

The security of the device is not compromised by altering the environmental conditions (e.g. setting the device to outside the stated operating ranges' temperature or operating voltages does not alter the security).

## 7.3 Software Development Guidance

When developing applications, the developer must respect the security guidance described in the document.
During the software development, the following steps must be implemented：

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

For use of open protocol, the developer must respect the Open Protocol Security Guide. It is important to note that SSL3.0, TLS1.0, TLS1.1 are inherently weak and has been removed. We strongly recommend a server should disable SSL protocol, and select TLS 1.2 or higher instead. To make it more secure, mutual authentication is recommended. The device use Classic Bluetooth, Bluetooth Low Energy (BLE) not be used. The device not support or allow for the use of insecure communication options such as, but not limited to, security modes 1 &2 and the "Just Works" secure pairing option of security mode 4. Any insecure communication options are not allowed.
For SRED, the device doesn't support pass-through of clear-text account data. All applications running on device are considered to be in "Account Data Encrypting Mode".
For SRED, Applications MUST enforce to use triple length TDES keys of Master/Session or Fixed implementation for Account data encryption or MAC encryption. And it is recommended that the ECB mode of operation should not be used for Account Data protection.

## 7.4 Firmware, Software and Configuration Parameters Update

Updates and patches can be loaded in the device. They are cryptographically authenticated by the device. If the authenticity is not confirmed, the update or patch is rejected.
Prompts updates are security related and any security related firmware changes will cause firmware version

update.

## 7.5 Software Signing/Authentication

The software of device consists of SP Boot, SP Task, AP Boot, AP OS and application.
SP Task, AP OS and application must be signed before released.
SP Boot and AP Boot is downloaded into device in factory, and they can't be updated after leaving factory.
SP Task is verified by SP Boot before loaded and executed. If the verification fails, SP Task can't be loaded to device and executed.
AP OS is verified by AP Boot before loaded and executed. If the verification fails, AP OS can't be loaded to device and executed.
Application is verified by AP OS before loaded and executed. If the verification fails, application can't be loaded to device and executed.
The signature verification uses 2048 bits RSA and SHA-256 algorithm.

## 7.6 Update and Patch Management

The device supports both local and remote methods for updating or patching the software, the firmware, and the configuration parameters.

1) The patch must be Security reviewed and audited before releasing.
2) The patch must be tested before releasing.
3) The patch must be digital signed before releasing.
4) The downloaded patch is stored in the temporary directory of the device, then the device uses digital signature to authenticate the patch. If the patch is illegal, then the device will delete it.

## 7.7 Self-Tests

The device will perform self-test upon startup and also every 24 hours. Periodical self-test is done by automatically reboot. This reboot period is count up once the device is powered on.
Self-Test include:

- Firmware integrity and authenticity
- Hardware security status
- Check all keys KCV
- Authenticated application integrity and authenticity

And if there is any kind of failure detected by self-test mechanism, the firmware will display a prompt indicating tampering status. At this situation, the device will be disabled and cannot be used. It should be sent to an authorised service center for repair.

## 7.8 Maintenance

Devices, which are detected as LOCKED through the system of requirement, 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 Topwise.

# 8. Key Management

The device supports the following key management: FIXED, MK/SK, DUKPT. (Please refer to ANS X9.24 for more details of these techniques).

## 8.1 Key Management System

The device implements different types of key management techniques:

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

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

**NOTE**: For the account data protection, please note that it is forbidden to load same key to multiple devices. Each device must have unique key. And it is required that only triple-length TDES keys are permitted for use in SRED in Master/Session or FIXED key implementations.

## 8.2 Cryptographic Algorithms

The device includes the following algorithms:

1) RSA (Signature verification, 2048 bits).
2) SHA-256 (Signature digest).
3) Triple DES (112 bits and 168 bits).
4) AES (128 bits).

## 8.3 Key Types / Usages

| Key Name | Purpose/Usage | Algorithm | Size(bits) | Storage |
|---|---|---|---|---|
| Main Master Key (MMK) | Encrypt/decrypt Master keys, PIN keys, MAC keys，Fixed Key and DUKPT keys when storing them in Device | AES | 128 | BPK |
| KEK | Key Encryption Key of TR-31, it is used to encrypt the keys transported from KMS to Device. | AES for AES key<br>TDES for TDES key | 128 for AES key<br>168 for TDES key | SRAM |
| KMK | Verify MAC Key of TR-31, it is used to Verify MAC the keys transported from KMS to Device. | AES for AES key<br>TDES for TDES key | 128 for AES key<br>168 for TDES key | SRAM |
| Terminal Master Key (TMK) | Encryption of working keys (PEK, MAC) for down-line | TDES | 192 or 128 | Flash |

| | | | | |
|---|---|---|---|---|
| | transmission to the device | | | |
| PIN-encryption Key (PEK) | PIN encipherment for online PIN | TDES | 192 or 128 | Flash |
| MAC Key | Message authentication | TDES | 192 or 128 | Flash |
| TDKey | Data encryption | TDES | 192 | Flash |
| Fixed PIN Key | PIN encipherment for online | TDES | 192 or 128 | Flash |
| Fixed MAC Key | Message authentication | TDES | 192 or 128 | Flash |
| Fixed TDKey | Data encryption | TDES | 192 | Flash |
| Fixed PIN Key for AES | Encrypt PIN blocks | AES | 128 | Flash |
| IPEK | Initial DUKPT Key | TDES | 128 | Flash |
| DUKPT PEKs (Future Keys Register) | PIN encipherment for online PIN | TDES | 128 | Flash |

Table 2: Key Table

## 8.4 Key Injection

The device does not propose manual cryptographic key entry. Specific tools, compliant with key management requirements, shall be used for key loading.
The initial key includes:

- TMK of MK/SK system
- PEK/MAK/TDK of Fixed system
- DUKPT Initial key.

The plain-text key (including MK, Fixed Key and DUKPT Initial Key) loading process must be implemented in a secure room of acquirer and strictly protected under following dual control and split knowledge techniques. For the working keys of MK/SK system, they can be loaded in cipher text under protection of TMK. The encrypted key loading is controlled by the acquirer through remote network. For Fixed key method, no encrypted keys are used. And for DUKPT method, transaction keys are automatically generated, hence no encrypted keys are needed to be loaded.

## 8.5 Key Replacement

A key should be replaced whenever the compromise of that key is suspected, or when the time is deemed feasible for determining it by exhaustive attack. This replacement operation can be done same as key injection.

## 8.6 Key Removal

Once the keys are loaded into the device successfully. They will be available unless the administrator wants to erase all keys for some reason like decommissioning. Or when a tamper issue is detected so that all the keys will be erased by the firmware automatically.
**NOTE:** If one key has been COMPROMISED, this key and its distributed keys should not be used any more.

User can use another working keys that are still safe. But if the device is tampered, it's requested to send the device to an authorised service center for repair and re-download the new keys.

### 8.7 key Lifetime

The key lifetime is controlled by Acquirer.
Suggestions from the Manufacturer are:
The maximum lifetime of MK is suggested to be 2 years.
The maximum lifetime of SK is suggested to be 1 day.
The maximum lifetime of DUKPT cannot exceed 1million transactions.

### 8.8 Signature Mechanism

The signature system used by Topwise is a localized signature server deployed in the security room of the manufacturer. This signature system implements a serial of important functions such access control, permission management, file signature, log management and etc.
A pair of signature operators will be granted and permitted to login this system and do signature operation. Only both of them are identified by the system (through entry respective passwords successfully) 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 encryption machine and never be exported.
Only signed file will be output to outside. Certainly, any operation trace will be recorded by this system to make it more secure.

## 9. System Administration

The following requirements and recommendations are applicable during the System Administration:

### 9.1 Configuration Settings

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

### 9.2 Default Value Update

The device is distributed to acquirer with default passwords to access of key injection. The default passwords used for key loader are informed to acquirer by training. When the administrators logon and use the key injection function at the first time, they are required to modify the key injection access default passwords.
The device does not include any certificate for testing purpose after manufacture.

## 10. Roles and Services

The customers of maintainer are acquirer or administrator. We also refer to administrator as acquirer directly. Maintainer sells devices to administrator and provide technique and maintenance supports to administrator. Administrator sells the devices to end users and provides services to their end user. Maintainer，administrator

and operator play different roles in operating the device. Below table shows different roles and operations:

| Roles | Operations |
|---|---|
| administrator | 1. Organize the third party to develop application program;<br>2. Download application<br>3. Access to device sensitive service |
| operator | Perform transaction |
| maintainer | 1. Sign customer public key<br>2. Repair device and unlock the device if tampered.<br>3. Download customer public key |

Table 3: Different roles and operations