SECURITY POLICY FOR M3P

目录

1. INTRODUCTION 1

2. ACRONYMS 1

3. SCOPE 1

4. REFERENCE 1

5. GENERAL DESCRIPTION 2

5.1 PRODUCTION OVERVIEW 2
5.2 PRODUCTION IDENTIFICATION 3
5.3 HOW TO CHECK THE DEVICE 3
5.4 COMMUNICATION METHODS AND PROTOCOLS 3

6. SECURITY GUIDANCE 4

6.1 INSTALLATION GUIDE 4
6.2 INSTALLATION AND ENVIRONMENT 4
6.3 DECOMMISSIONING/REMOVAL 4
6.4 PIN CONFIDENTIALITY 4
6.5 PERIODIC INSPECTION 5

7. PRODUCT SECURITY 6

7.1 TAMPER RESPONSE EVENT 7
7.2 ENVIRONMENT CONDITIONS AND ENVIRONMENTAL FAILURE PROTECTION 7
7.3 SOFTWARE DEVELOPMENT GUIDANCE 8
7.4 FIRMWARE AND SOFTWARE UPDATE 8
7.5 SOFTWARE AUTHENTICATION 8
7.6 UPDATE AND PATCH MANAGEMENT 8
7.7 SELF-TESTS 9
7.8 MAINTENANCE 9

8. KEY MANAGEMENT 9

8.1 KEY MANAGEMENT SYSTEM 9
8.2 CRYPTOGRAPHIC ALGORITHMS 10
8.3 KEY TYPES / USAGES 10
8.4 KEY INJECTION 10
8.5 KEY REPLACEMENT 11
8.6 KEY REMOVAL 11
8.7 KEY LIFETIME 11
8.8 FIRMWARE SIGNING 11
8.9 ACCOUNT DATA PROTECTION 11

9. SYSTEM ADMINISTRATION 11

9.1 CONFIGURATION SETTINGS 12

9.2 DEFAULT VALUE UPDATE 12

10. ROLES AND SERVICES 12

RECORD OF REVISIONS

Revision	Type of modification	Author	Date
V1.0	Document creation	Weiquan Ouyang	2022-7-30
V1.1	Update section 10	Weiquan Ouyang	2022-10-17

Security Policy for M3P

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 v6.1 approval of the device.

2. Acronyms

- TDES/3DES: Triple Data Encryption Standard.
- AES: Advanced Encryption Standard.
- BPK: Backup Register.
- FW: Firmware.
- DUKPT: Derived Unique Key Per Transaction.
- FOTA: Firmware Over-The-Air.
- RSA: Rivest Shamir Adelman Algorithm.
- SHA: Secure Hash Algorithm.
- SP: Security Processor.
- SRAM: Static Random-Access Memory.
- SRED: Secure Reading and Exchange of Data.
- PIN: Personal Identification Number.
- PED: PIN Entry Device.
- IC Card: Integrate Circuit Card.
- RF Card: Radio Frequency Card.
- KCV: key check value.
- KMS: Key Management System
- KLD: Key Loading Device.

3. Scope

The documentation is applicable for Topwise intelligent POS terminal.

The 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.

The document must be read in conjunction with the related Reference Documentations.

The document covers the following products: M3P (Handheld POS).

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 X9.24-2: 2021, Retail Financial Services Symmetric Key Management Part 2: Using Symmetric Techniques.

[4] ANSI X9.24-3: 2017, Retail Financial Services Symmetric Key Management Part 3: Derived Unique Key Per Transaction.

[5] ISO 9564-1: Financial Services-Personal Identification Number (PIN) management and security Part 1:

Basic principles and requirements for PINs in card-based systems.

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

[7] PCI PTS POI Modular Derived Test Requirements Version 6.1-March 2022.

[8] M3P user manual.

[9] M3P Open protocol guidance.

[10] M3P Application development guide.

5. General description

The device is a handheld Point of Sale (POS) PED terminal, to process PIN-based transactions in attended environment. Use of the device in an unapproved method will violate the PCI PTS V6.1 approval of the device.

5.1 Production Overview

M3P are the new generation of intelligent wireless POS with touch-screen and high-speed communications. The product is mainly for indoor usage and its target merchant are the restaurants, entertainment, chain stores, supermarkets, E-commerce and so on.

The device is a PIN entry device; it can be used as the standard POS to undertake financial transactions. The device can perform the PIN entry, MAC calculation and Data encryption/decryption.

The device provides touch screen (not used for PIN input), physical keypad, contactless card reader, ICCR, MSR, PSAM, printer, camera, LCD and SIM card reader. It is designed for a portable and handheld use, and the device does not have a shielded, so it is needed to be shield by the body when entering the PIN in a transaction. The power system is based on battery and the communications to the external world are based on USB, WIFI, Cellular (2G/4G) connection.

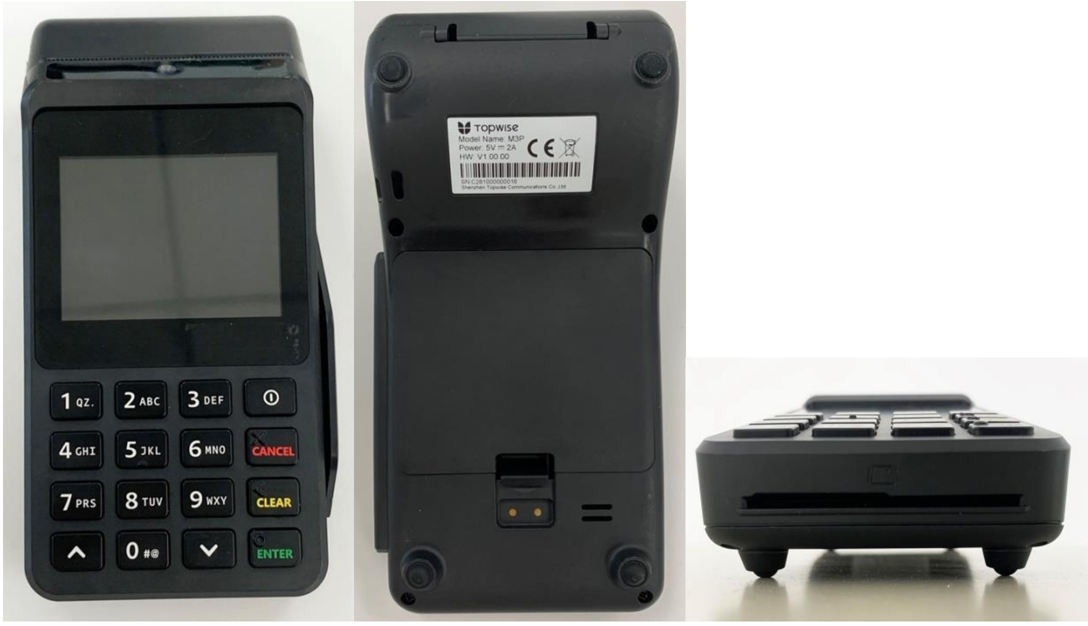
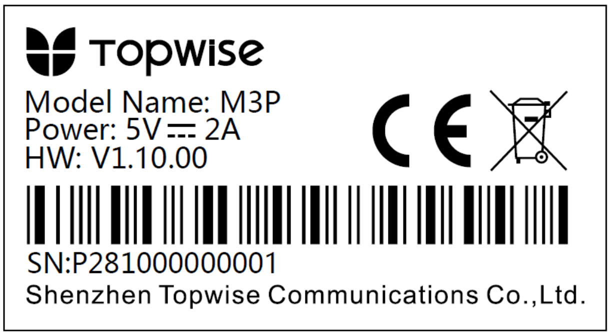


Figure 1: M3P Appearance

5.2 Production Identification

There is a product label with product name and hardware version printed on the device.
The hardware versions are V1.0x.xx (one-layer key mesh) and V1.1x.xx (two-layer key mesh). The first “x” represents the different communication configuration. The second “x” represents the Customer Number. The third “x” represents the device’s Color.
Firmware Version: V0004.



Topwise
Model Name: M3P
Power: 5V ⎓ 2A
HW: V1.10.00
SN:P281000000001
Shenzhen Topwise Communications Co.,Ltd.

Figure 2: M3P Label

5.3 How to check the device

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 “Terminal info”, and the firmware version info will be shown in the LCD.
To examine the version of hardware of the device, we can check the device label in the column “HW” which has been listed in chapter 5.2.

5.4 Communication methods and protocols

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

Communication	**Interface**	**Protocols**
	Cellular (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, ARP, IP Stack
	USB	USB 2.0

Table 1. M3P Communication Methods and Protocols

Use of any method not listed in the policy invalidates the device approval.

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 [8] 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
- M3P 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

M3P are a hand-held devices, it’s recommended that the merchants reminding cardholders to block the view of the keyboard with their hands or body when entering the PIN code to avoid being peeped by others.

Figure 3: Safe PIN Entry Logo Example

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

Method	Observation Corridors				
	Cashier	Customer in Queue	Customer Elsewhere	On-Site Cameras	Remote Cameras
Check stand	Customer positions PED.	Customer positions PED.	Customer positions PED.	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.

Table 2. M3P methods for protecting the cardholder's PIN during PIN entry.

6.5 Periodic Inspection

The merchant or acquirer should daily check that the keypad is firmly in place. The device should be daily checked to make sure that there are no incorrect or redundant keyboard overlays. 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.

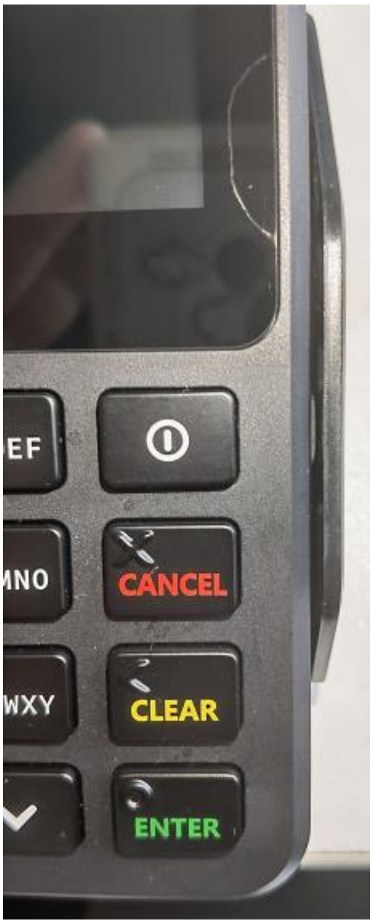


Figure 4: M3P MSR slot

The merchant or acquirer should also daily check whether the magnetic stripe card slot is damaged or not, such as abrasion, painting and other machining marks, and if there is any suspicious object like lead wire over the slot, or any unknown object inside the slot.

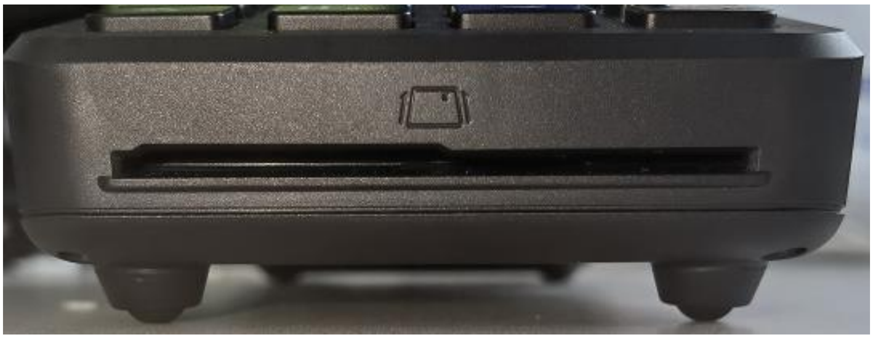


Figure 5:M3P ICCR slot

The merchant or acquirer should also daily check whether the tamper message on the device display. Please refer to “Tamper Response Event” in section 7.1.

When these suspicious circumstances are found, please stop using the device immediately and contact the customer service to confirm if the device has been tampered.

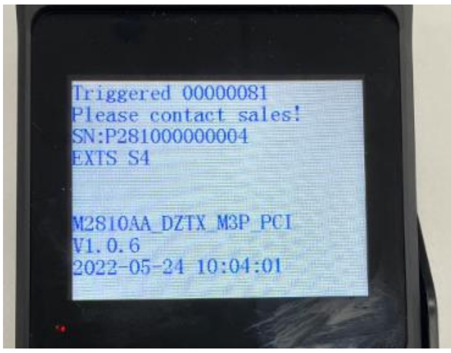
7. Product Security

Users should refer to M3P 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



```
Triggered 00000081
Please contact sales!
SN:P281000000004
EXTS S4

M2810AA_DZTX_M3P_PCI
V1.0.6
2022-05-24 10:04:01
```

- Can't enter normal application and can't do any transaction

If the device is in tampered state, it should immediately be removed from service and the user needs to send the device to the manufacturer for safety inspection and repair.

Any physical penetration or environmental conditions that exceed the trigger temperature and voltage range 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

Note: From Locked mode switch to Activated mode, the device has to do networking activation for authentication

7.2 Environment Conditions and Environmental Failure Protection

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

- Working Temperature: -10℃~55℃
- Storage Temperature: -20℃~70℃
- R.H.: 5%~95% (Non-condensing)
- Power supply: DC 5V

When the following conditions occur, the tamper detector will clear sensitive data information immediately:

- The battery voltage VBAT rises above 4.0V ±0.1V
- The battery voltage VBAT falls below 1.9V ±0.1V
- The on-chip temperature rises above approximately 100±10℃
- The on-chip temperature falls below approximately -30~-40℃

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).

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 should be removed, but considering these versions still exist in the world, in order to be compatible, we temporarily keep them for non-financial applications use. In addition, 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.

7.4 Firmware and Software 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 Authentication

Application code is authenticated before being allowed to run. The certificate and signature of the application code is verified.

The certificate and signature are based on couples of RSA keys. The authenticity is guaran-teed by a certificate issued by Topwise.

- SHA256 is used to compute the digest of software
- RSA 2048 bits key is used for signature verification

The application managers must implement a full source code review to make sure that the application does not have one of following behaviors:

- PIN entry prompt while the keypad digit is displayed in plain-text.
- Not using the correct security mechanism and APIs recommended in the user guidance for PIN entry.
- Storing or outputting any card holder’s account data without his/her authorization.

It is recommended that the application source code review and signing process is executed by at least two persons and that an audit log is recorded for future trace back.

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 authorized 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: 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.
- 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: Please note that it is forbidden to load same key to multiple devices. Each device must have unique key. And for the account data protection, it is required that only triple-length TDES keys are permitted for use in SRED in Master/Session 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 (128 bits and 192 bits).
4) AES (128 bits, 192 bits and 256 bits).
5) ECC (P-192, P-224, P-256, P-384, P-521).

8.3 Key Types / Usages

Key Name	Purpose/Usage	Algorithm	Size(bits)	Storage
MMK	Encrypt or decrypt other keys	AES	256	BPK
KBPK	Key Block Protection Key of TR-31, it is used to encrypt the keys transported from KLD to Device.	AES	256	SRAM temporarily
TMK (MK/SK)	Encrypt or decrypt SK (PEK, MAK)	TDES, AES	TDES: 128/192 AES: 128/192/256	Flash
PEK (MK/SK)	Encrypt PIN blocks	TDES, AES	TDES: 128/192 AES: 128/192/256	Flash
TDKey (MK/SK)	Encrypt account data	TDES, AES	TDES: 192 AES: 128/192/256	Flash
MAC Key (MK/SK)	Generate or verify MAC of data blocks	TDES, AES	TDES: 128/192 AES: 128/192/256	Flash
IPEK	Initial DUKPT Key	TDES, AES	128	SRAM temporarily
DUKPT PEK	Encrypt PIN blocks	TDES, AES	128	Flash

Table 3: Key Table

8.4 Key Injection

The device supports the following key-loading techniques:

- Clear-text key injection from KLD;
- Symmetric encrypted keys.

The initial key includes:

- TMK of MK/SK system
- DUKPT Initial key.

Initial keys should be loaded to the device by an authentic key management system in a secure environment.

For the working keys of MKSK system, they can be loaded in ciphertext under protection of TMK.

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 device successfully, they will be available unless the administrator wants to erase all keys for some reason like decommissioning. Or once a tamper issue is detected, then 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 key that are still safe. But if the device is tampered, it's requested to send the device to an authorized 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 Firmware Signing

Asymmetric cryptographic algorithm is used for the firmware authentication:

- SHA256 is used to compute the digest of firmware
- RSA 2048bits key is used for signature verification

The firmware is signed by RSA-2048bits private key. And this signer key is only controlled by Topwise. And the firmware authentication is done by signature verification using corresponding public key of Topwise.

8.9 Account Data Protection

The device always provides SRED functionality and doesn't support the disablement (turning off) of SRED functionality. For the SRED module, account data can be encrypted by TDES and AES encryption. The device does not support the pass-through of clear-text account data.

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 functional when received by the merchant or acquirer and there is no security sensitive default value (e.g. admin password) that needs to be changed before operating the device.
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 provides 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; 2. Download application
operator	Perform transaction
maintainer	1. Sign customer public key 2. Repair device and unlock the device if tampered. 3. Download customer public key