# Advanced Mobile Payment Inc.

# AMP 3000

***PCI PTS POI Security Policy***

***2019-07-19***

***V 1.0.2***

# Revision History

| Date | Revision Level | Description | Modified by |
|---|---|---|---|
| *2019-03-18* | *1.0.0* | *Original Version* | *Zoe Lin* |
| *2019-03-18* | *1.0.1* | *Update the Label* | *Kevin Chu* |
| *2019-07-19* | *1.0.2* | *Update Firmware version* | *Kevin Chu* |

# Contents

# Purpose

AMP 3000 is assessed for PTS POI v5.1. This document is to describe a security policy which addresses the proper use of AMP 3000 in a secure fashion, including information on key-management, roles and responsibilities, device functionality, identification and environmental requirements.

Any deviation from the approved use of AMP 3000 will invalidate the PCI PTS POI approval.

# General Description

## Product Name and Appearance

The device name: AMP 3000


**Figure 1: AMP 3000 appearance**

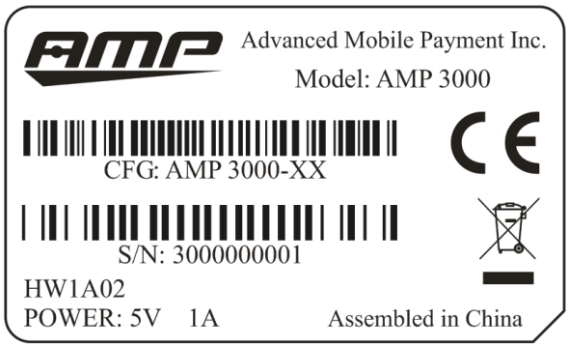



**Figure 2: Label**

The appearance of AMP 3000 is the same as Figure 1, and the label is on the back of

device.

# Product Type

AMP 3000 is a traditional mobile POS product; this device provides physical keypad, Contactless card reader, IC Card Reader (ICCR), Security Magnetic Reader (MSR), LCD. It is designed for attended device, a portable and handheld use, so that the device can be shielded by the body when in work. The power system is based on a DC 5V power supply or battery and the communications to the external world are based on WIFI, or GPRS wireless connection.

AMP 3000 is a single device, uses keyboard for PIN entry.

# Identification

## Hardware version

The hardware version is printed on the label which is on the back of device, as Figure 2. It is to be notice that the label should not be torn off or covered.

## Firmware version

The firmware version can be view as following:

1. Power up AMP 3000 and go to home screen. Press MENU button to enter System Manager.
2. Select the "**About**"-> "**About Versions**" item.
3. Please check the Security Firmware version, as Figure 3.

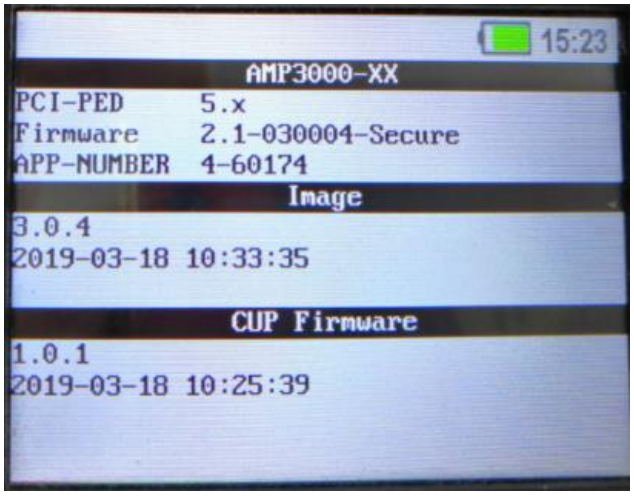



**Figure 3: Firmware version**

# Installation and User Guidance

## Initial Inspection

Before installation, Please look out the tampered information on LCD display to check if the device is tampered. If the device is tampered, please contact the authorized service or AMP (support@amobilepayment.com). Check if the appearance of AMP 3000 is altered, when some trace is found in the device, please reject it.

When the end-user or acquirer receives the AMP 3000, they must inspect and authenticate it. For example, the merchant or acquirer should inspect the terminal to ensure that:

1. Check if the origin that providing the AMP 3000 device is authorized, if not authorized, please reject.
2. Check if the device's name, firmware, hardware and application version are meet the approved identification number of PCI PTS POI in the website (www.pcisecuritystandards.org).
3. Check if the appearance of AMP 3000 is altered, if some trace are found, please reject the device.
4. Check if there is something overlay on the keyboard in order to prevent overlay attack.
5. Check if the ICC card slot has wire out or something that suspicious. If so, reject the device.
6. Check if the Magcard reader slot has other reader or some bug. If found, reject the device.

## Installation

User should refer user manual before installation this device.

The device consists of following items:

- 1 Device
- User manual

All software is installed before delivering to end user, then user can use PIN entry normally.

## Environmental Conditions

1. Temperature & Humidity Environments

   Operation Temperature & Humidity: 0℃ ~ 50℃ /10% ~ 90% (non-condense)

   Storage Temperature & Humidity: -20℃ ~ 60℃/ 5% ~ 95% (non-condense)

   If environment status is over that range, the terminal is not always working.

2. Power Environments

   The power supply specification:

   Input: 5.0V/1.0A DC

Terminal should stay away from all sources of heat, to prevent vibration, dust, moisture and electromagnetic radiation (such as a computer screen, motor, security facilities etc.).

## Communications and Security Protocols

The communication interfaces and protocols used by the device are showed in Table 1. For more details please refer to document [9].

| Interface | Protocols |
|---|---|
| Wireless Modem(GPRS) | PPP, ARP, TCP, IP, UDP, DHCP, DNS, TLS1.2 |
| Wi-Fi | ARP, TCP, IP, UDP, DHCP, DNS, TLS1.2 |
| Micro USB | The micro USB port is a OTG, using USB 2.0 specification, and only support the host mode. The device supports U-disk and USB to serial RS232 adapters. |

**Table 1** Communication and protocols

## Configuration Settings

The AMP 3000's firmware does not need any configuration setting.

# Operation and Maintenance

## Periodic Inspection

For the security using of AMP 3000, after a period using time, the device must be

inspected, only passed, the device can be used.

1. Please look out the tampered information on LCD display to check if the device is tampered. If tampered, please contact the authorized service or AMP.
2. Check if the appearance of AMP 3000 is altered. If can find some trace, please reject the device.
3. Check if there is something overlay on the keyboard in order to prevent overlay attack.
4. Check if the magnetic reader slot has other reader or some bug. If found, reject the device.

### ICC shim checking guide

For the security using of AMP 3000, every day before using the device, Operator must inspect the ICC slot.

1. Inspect the ICC slot to make sure that no any abnormal objects inside the slot or at the opening.
2. Insert an IC card; check if the card is inserted smoothly, without any obstacles.

## Self-Test

AMP 3000 using self-tests to check firmware authenticity in its processor. The self-test is performed:

1. Every time the unit is powered up.
2. At least once every 23 hours.

AMP 3000 performs a self-test, which includes firmware, application, stored keys, authenticity and any other sensitive properties tests to check whether the device is in a compromised state. If the result is failed, the device displays the lock icon and more tamper information on LCD and its functionality failed in a secure manner. When the device goes to the “Compromised” mode, all the stored keys are removed as well. The merchant must return the device to AMP for the repair. Self-tests are not initiated by an operator.

## Roles and Responsibilities

The customers of the AMP are acquirers. AMP sells devices to acquirer and provide

maintain and technique support. Acquirer sells devices to the end-users and service to the end-users. AMP, acquirer and end-users play different roles in operating device as shown in table below:

| | role | operation |
|---|---|---|
| acquirers | Administrator | 1. Organize the third party to developed application.<br>2. Download application and inject customer public key<br>3. Access to devices sensitive services |
| End-users | operator | Perform transaction |
| AMP | maintainer | 1. Sign customers public key<br>2. Repair devices and unlock the devices if tampered |

**Table1: Different roles and operations**

# Passwords and Certificates

When manufacturing in factory, the device of AMP 3000 is set to default password. The first time to entry sensitive function, the default password needs to be changed. So for security, when shipping the device to customer, the administrator must re-set a valid password to replace the default password.

The new passwords cannot be changed the same to the old passwords.

The AMP 3000 does not need any change of certificate.

# Tamper Response

## Tamper Trigger Events

- Front case removal
- Back case removal
- Physical penetration on all the sides of the device
- Temperature is >80˚C or < -25˚C.
- BBL voltage is >3.67V or <2.4V.
- Stored sensitive data authentication failed during the Self-test

## Tamper Response

Remove the stored key file.

Make the device unavailable and display the attack source information on the screen. When the device is tampered, some tampered information from LCD display as Figure 4, please stop using the device and contact authorized service or AMP to maintain it.

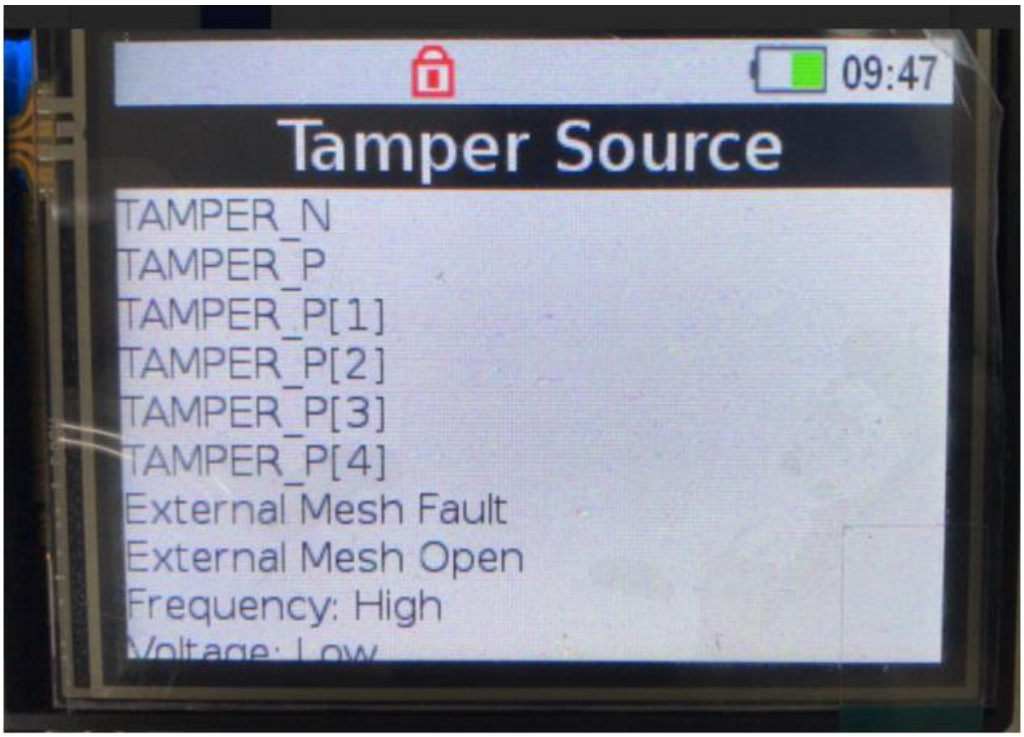
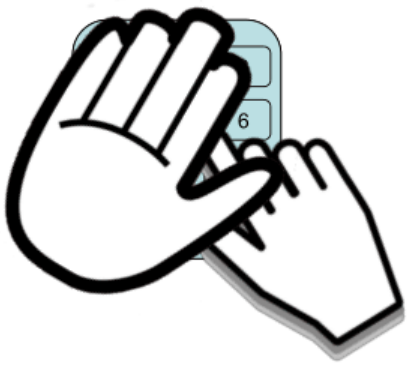



**Figure 4: Tamper status**

## Privace Shield

The POI is a hand-held device, it will not provide a physical Privacy Shield additional, but it is required to provide cardholders with the necessary privacy during PIN entry. The device will prompt for some messages to remind the cardholder to block the view of the keyboard with the body or free hands. For example:



# Patching and Updating

AMP 3000 supports two ways to update the system:

1) OTA upgrade
2) USB upgrade


**Figure 5: Update options**

## OTA upgrade

Steps:

1. Make sure the device have good Internet environment.
2. Press **MENU** button, and selecting "**System setup**"->"**Firmware Upgrade->OTA Upgrade**", start updating.
3. After the completion of download, system will reboot, and uboot will complete the upgrade work.

Customers can download the latest firmware by OTA. The OTA service will detect remote server if there is a new firmware version under the good network condition. If

there is a new version, the system will pop up a system update notification to prompt the user. Additionally, the device uses TLSv1.2 protocol to transmit data when it updates firmware or application. During the TLS handshake process, POS terminal will authenticate the server firstly as the POS terminal owns server's certificate. After the authentication is approved, a secure channel will be established to ensure the security of the data in the downloading process. When the download is complete, the integrity of the download firmware will be checked by SHA256.

After firmware is downloaded, old firmware in the terminal will immediately verify whether the signature is legal. Any non-signed firmware will be considered as unauthorized, and cannot be updated. Terminal type information is already contained in firmware, and firmware will also choose whether it could work in existing terminal. If terminal type is not compatible, firmware will not be updated. When firmware update is completed, restart device again, and new firmware version will be shown.

### USB upgrade

Steps:

1. Copy update firmware “AMP 3000.img” to the root directory of a USB disk;
2. Insert the USB disk to the AMP 3000 terminal;
3. Press Menu button and the select “**System setup**”->”**Firmware Upgrade**” -> “**USB Upgrade**”, start updating.
4. After the completion of the copy, the user need to reboot the device to complete the upgrade work.

## Decommissioning

### Permanent removal

When the device is no longer used, it can be decommissioned and removed from service. And then must remove all the key material that used to decrypt any sensitive data.

### Temporary removal

If just temporary removal, it’s not need to remove the keys.

### Decommissioning

To decommissioning device, merchants should return the device to acquirer or vendor; they will reset all the payment keys by using key loader. Disassemble device will make device to tamper status, which will also erase all payment keys and decommission device.

# Security

## Software Development Guidance

When developing applications, the developer must respect the guidance including APIs and environment described in the document [12]. The document [8] and document [9] are for SRED and SSL application guidance.

### SRED applications development

1. Account data read from IC, magnetic stripe card must be encrypted at once.
2. The plain-text account data cannot output of the device.
3. After transaction or time out or other abort, the plain-text account data must be deleted immediately.

### SSL applications development

For SSL application development please refer document [9] and the compliance with PCI PTS, the following points need to take attention.

1. The client must authenticate the CA certificate and client certificate.
2. The cipher suite of the server which terminal connects should be as secure as TLS_RSA_WITH_AES_128_CBC_SHA or more secure.
3. The server which terminal connects should be configured to require Client Authenticate.
4. Use TLS v1.2 or higher.
5. Application developer must use SHA-256 on top of the security protocol when it is being used for security functionality.

Application developer can get the security guidance from AMP website.

## SSL

The OpenSSL is customized by AMP and all weak cipher suite are removed from device, AMP 3000 only supports the cipher suites as PCI PTS required.

| |
|---|
| TLS_RSA_WITH_AES_128_CBC_SHA |
| TLS_RSA_WITH_AES_128_GCM_SHA256 |
| TLS_RSA_WITH_AES_256_CBC_SHA |
| TLS_RSA_WITH_AES_256_GCM_SHA384 |
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA |
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 |
| TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 |
| TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA |
| TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 |
| TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 |
| TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 |
| TLS_RSA_WITH_AES_128_CBC_SHA256 |
| TLS_RSA_WITH_AES_256_CBC_SHA256 |

**Table 2 SSL/TLS supported cipher suite**

## Signing

AMP supports turnkey system, and uses RSA2048-SHA256 for application authentication.

Application can be updated and downloaded into the device in a cryptographically authenticated way. The software is digitally signed with an IC card and a PC tool which provide by vendor. The third-part developer can apply to vendor for signature IC card and PC tool.

After get the signature IC card, by using PC tool, third-part developers can generate their RSA private keys. Then export public keys and send to vendor for sign the public key, after vendor sign them, developers can import signed public key into signature IC card, finally developers can use this signature IC card to sign their applications, for more detail, please refer document[10]and document[11].

When download application, the device will authenticate the signature of application, only authenticate successfully the application can be installed.

## Account Data Protection

For AMP 3000, the account data is protected by TDK in Table 2, the algorithm is

TDES, and the key length is limited to 192 bits. The device does not support the pass-through of clear-text account data using techniques white listing. The devices not allow the disablement of SRED functionality.

## Algorithms Supported

AMP 3000 supports the following cryptographic algorithms:

- TDES(128bits and 192bits)
- AES(128bits, 192bits, 256bits)
- SHA-256(digest signature, 256 bits)
- RSA-2048(signature verification, mutual authentication,2048 bits)

Device supports TR-31 for symmetric key management.

## Key Management

AMP 3000 supports the following key systems:

- Fixed key
- Master Key/Session key
- DUKPT

Master Key/Session key, the Session Keys are encrypted/decrypted by Master Keys.

DUKPT, the technique is based on a unique key per transaction.

AMP 3000 supports the following symmetric key types:

- TMK: Terminal master key. It’s generated by the acquirer and used to decrypt the MAC key, the PIN key.
- TPK: Terminal PIN encryption key. It’s generated by the acquirer and used to generate the PIN BLOCK.
- TAK: Terminal MAC encryption TDES key. It’s generated by the acquirer and used to calculate the MAC value.
- TDK: Terminal Account data encryption TDES key, it is generated by the acquirer and used to encrypt account data (SRED).

Key management for PIN protection and SRED protection is different.

Key management for PIN protection:

- Fixed Key(TDES and AES)
- Master Key/ Session Key (TDES and AES)
- DUKPT(TDES)

Key management for SRED protection:

- Fixed Key(TDES, only 192bits)
- Master Key/ Session Key (TDES, only 192bits)

| **Key Name** | **Purpose** | **Algorithm** | **Size** |
|---|---|---|---|
| TMK | Decryption of session keys (TPK, TAK, TDK) | TDES | 128/192 bits |
| | | AES | 128/192/256bits |
| TPK | Online PIN encryption key | TDES | 128/192 bits |
| | | AES | 128/192/256bits |
| TAK | Message authentication | TDES | 128/192 bits |
| TDK | Encrypt account data. | TDES | 192 bits |
| Fixed TAK | Message authentication | TDES | 128/192 bits |
| Fixed TPK | Online PIN encryption key | TDES | 128/192 bits |
| | | AES | 128/192/256bits |
| Fixed TDK | Encrypt account data. | TDES | 192 bits |
| DUKPT Key | Online PIN encryption key and Message authentication | TDES | 128 bits |

**Table2: Key table**

Using of the device with different key-management systems will invalidate any PCI PTS POI approval.

# Key Loading

When the product are manufactured, The initial keys including TMK, Fixed key and initial DUKPT are injected into AMP 3000 through security device under dual control

in security environment.

Remote key distribution applies to session key(TPK, TAK, TDK key) loading, encrypted by their respective TMK

The key loading method for application is referenced in ANSI X9 TR-31-2010.

## Key Replacements

Keys should be removed from the device 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. Keys can be removed by the sensitive service of MENU -> “System setup” -> “Key Injection” ->“CLEAR KEY” in AMP 3000’s menu. After key removal, the device should return to Key Injection facility for the secure key loading. The key must be review for every 2 years to see whether the key should be replaced with the new key to avoid exhaustive attack.

# Acronyms

| | |
|---|---|
| AES | Advanced Encryption Standard |
| CA | Certification Authority |
| DES | Data Encryption Standard |
| DUKPT | Derived Unique Key Per Transaction |
| IC | Integrated Circuit |
| ICCR | IC Card Reader |
| LCD | Liquid Crystal Display |
| MAC | Message Authentication Codes |
| MSR | Magnetic Security Reader |
| OTA | Over-the-Air Technology |
| PAN | Primary Account Number |
| PCI | Payment Card Industry |
| PIN | Personal Identification Number |
| POI | Point of Interaction |
| PTS | PIN Transaction Security |
| RSA | Rivest-Shamir-Adleman Algorithm |
| SRED | Secure Reading and Exchange of Data |
| SSL | Secure Sockets Layer |
| TAK | Terminal MAC encryption Key |
| TDEA | Triple Data Encryption Algorithm |
| TDES | Triple Data Encryption Standard |
| TDK | Terminal account Data encryption Key |
| TLS | Transport Layer Security |

| | |
|---|---|
| TMK | Terminal Master Key |
| TPK | Terminal PIN encryption Key |
| USB | Universal Serial Bus |
| WiFi | Wireless Fidelity |
| | |

# References


[1] PCI PTS POI Modular Derived Test Requirements Version 5.1 - March 2018

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

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

[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 management and security Part 2: Approved algorithms for PIN encipherment

[6] NIST Special Publication 800-90A Revision 1.pdf

[7] AMP 3000 Product Manual.pdf

[8] Software Security Guidance.doc

[9] Protocol Stack Security Guidance.doc

[10]Signature Card Request Guide.doc

[11] Application Signature Tool Guide.doc

[12]AMP XXXX EFT-POS APPLICATION DEVELOPMENT MANUAL.doc