

Advanced Mobile Payment Inc.

AMP 6500

PCI PTS POI Security Policy

2018-04-02

V 1.0.5

Revision History

Date	Revision Level	Description	Modified by
<i>2018-01-18</i>	<i>1.0.0</i>	<i>Original Version</i>	<i>Brian.Yang</i>
<i>2018-03-02</i>	<i>1.0.1</i>	<i>1. Add Key Management description. 2. Add privacy shield installation guidance.</i>	<i>Brian.Yang</i>
<i>2018-03-28</i>	<i>1.0.2</i>	<i>Update policy to meet PCI 5.1 standard</i>	<i>Brian.Yang</i>
<i>2018-03-29</i>	<i>1.0.3</i>	<i>Fix tiny error.</i>	<i>Brian.Yang</i>
<i>2018-03-30</i>	<i>1.0.4</i>	<i>Update figure3 firmware version</i>	<i>Brian.Yang</i>
<i>2018-04-02</i>	<i>1.0.5</i>	<i>1. Add tamper voltage range 2.Add modify default password requirement</i>	<i>Brian.Yang</i>

Contents

Purpose.....	4
General Description	5
Product Name and Appearance	5
Product Type	5
Identification	6
Installation and User Guidance	7
Initial Inspection	7
Installation.....	7
Environmental Conditions	8
Communications and Security Protocols	8
Configuration Settings	8
Unattended Installation	8
Operation and Maintenance	10
Periodic Inspection.....	10
Self-Test	10
Roles and Responsibilities	11
Passwords and Certificates.....	11
Tamper Response	12
Privacy Shield	13
Patching and Updating	13
Decommissioning.....	15
Removal Detection.....	16
Security	17
Software Development Guidance	17
SSL.....	17
Signing	18
Account Data Protection	18
Algorithms Supported	18
Key Management	19
Key Loading.....	20
Key Replacement	20
Acronyms.....	22
References.....	23

Purpose

AMP 6500 is assessed for PTS POI v5.1. This document is to describe a security policy which addresses the proper use of AMP 6500 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 6500 will invalidate the PCI PTS POI approval.

General Description

Product Name and Appearance

The device name: AMP 6500



Figure 1: AMP 6500 appearance

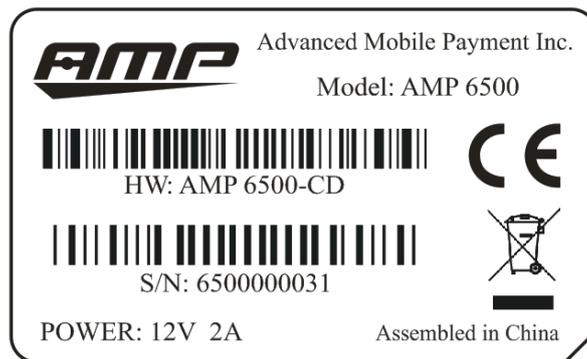


Figure 2: Label

The appearance of AMP 6500 is the same as Figure 1, and the label is on the back of device.

Product Type

AMP 6500 is a new generation of unattended POS products, and should be mounted into a greater housing providing a privacy screen.

AMP 6500 provides Touch keypad, Contactless card reader, IC Card Reader (ICCR), Magnetic Security Reader (MSR), LCD. The power system is based on a DC

12V 2A power supply and the communications to the external world are based on Ethernet, USB, WIFI, or LTE wireless connection.

AMP 6500 is a single device, uses Touch keypad for PIN entry. It does not have beacons.

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 6500 and go to home screen. Enter the Settings function of system.
2. Select the “About” item.
3. You can see the Android version, Kernel version and Security Firmware version, as Figure 3.

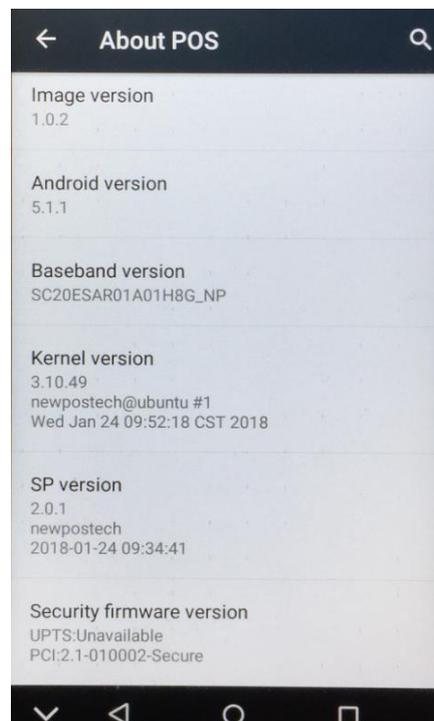


Figure 3: Firmware version

Installation and User Guidance

Initial Inspection

Before installation, you can look out the tampered information on LCD display to check if the device is tampered. If tampered, please contact the authorized service or AMP (support@amobilepayment.com). Check if the appearance of AMP 6500 is altered, if you can find some trace, please reject the device.

For security, when receive the device via shipping, it must be inspected and authenticated. If pass, you can use the device. Please inspect as following:

1. Check if the origin that providing the AMP 6500 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 6500 is altered, if some trace are found, please reject the device.
4. Check if something overlay on the LCD display 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 bugger. 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 deliver to end user. User can use PIN entry normally.

Environmental Conditions

1. Temperature & Humidity Environments

Operation Temperature & Humidity: -20°C ~ 60°C /0% ~ 90% (non-condense)

Storage Temperature & Humidity: -25°C ~ 75°C/ 0% ~ 95% (non-condense)

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

2. Power Environments

The power supply specification:

Input: 12V/2A 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

Please refer document [9] for proper use and configuration of all communication type and open protocol the device supported.

Configuration Settings

The AMP 6500's firmware does not need any configuration setting.

Unattended Installation

AMP 6500 is designed to be used in an unattended environment, should be mounted into a greater housing providing a privacy screen.

The ICCR slot is designed not positioned straight (horizontal) to the cardholder, please install at a proper height ensuring a sufficient view on the card-slot entry area.

Installation instructions recommend positioning the terminal in a location where spying on the cardholder PIN is difficult or impossible.

Cardholders should be advised to take care no-one can see/deduce the PIN they enter.

Before using, please check if the origin that providing the AMP 6500 device is

authorized, check if the appearance of AMP 6500 is altered, check if the ICC card slot has wire out or something that suspicious, check if the magnetic card reader slot has other reader or some bugger, if you find the above problems, please refuse to use.

Operation and Maintenance

Periodic Inspection

For the security using of AMP 6500, after a period using time, the device must be inspected, only passed, the device can be used continue.

1. You can 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 6500 is altered. If can find some trace, please reject the device.
3. Check if something overlay on the LCD display in order to prevent overlay attack.
4. Check if the magnetic reader slot has other reader or some bugger. If found, reject the device.

ICC shim checking guide

For the security using of AMP 6500, 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.

The device picture and screen shots of version information please refer Figure 1 and Figure 3.

Self-Test

AMP 6500 using self-tests to check firmware authenticity in both its processors. The self-test is performed:

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

AMP 6500 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 fail 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.

Adjustment process does not influence the periodic of self-test, because the self-test periodic will changed depends on the adjustment.

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	<ol style="list-style-type: none"> 1. Organize the third party to developed application. 2. Download application and inject customer public key 3. Access to devices sensitive services
End-users	operator	Perform transaction
AMP	maintainer	<ol style="list-style-type: none"> 1. Sign customers public key 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 6500 is set to default password. The first time to entry sensitive function, need to change the default password. So for security, when shipping the device to customer, the administrator must re-set a valid password to replace the default password.

When changing, the new passwords cannot be the same to the old passwords.

The AMP 6500 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
- MSR head cover removal
- MSR connector removal
- Temperature is $>95^{\circ}\text{C}$ or $<-35^{\circ}\text{C}$.
- BBL voltage is $>3.65\text{V}$ or $<2.0\text{V}$.
- 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 you can see from LCD display as Figure 4, you must stop using the device and contact your authorized service or AMP to maintain it.

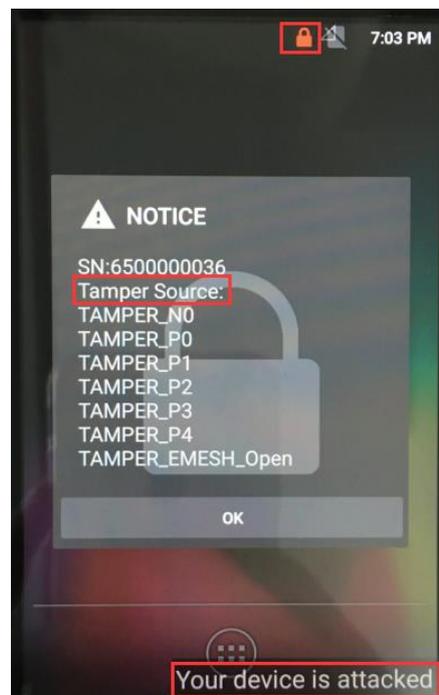


Figure 4: Tamper status

Privacy Shield

A privacy shield, meeting PCI requirements and any additional local regulations, must be fitted before the terminal is used, as Figure 5.



Figure 5: Privacy shield installation

Patching and Updating

AMP 6500 supports two ways to update the system:

- 1) OTA upgrade
- 2) USB disk upgrade

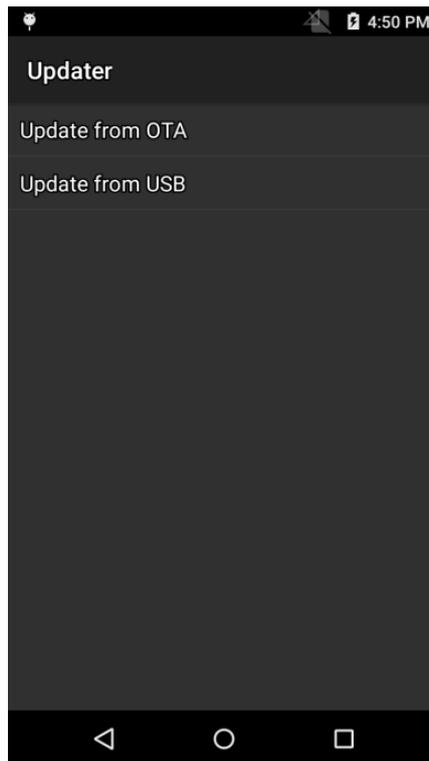


Figure 6: Update options

OTA upgrade

Steps:

1. Make sure the device have good Internet environment.
2. Click the system application, “Settings” -> “Updater” -> “Update from OTA”, start updating.
3. After the completion of download, system will reboot to recovery mode to recovery mode to complete the upgrade work.

Customers can download the latest firmware by OTA. The system will start background service 5 minutes later after it boots. Then, the 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, we use TLSv1.2 protocol to transmit data when it updates. 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 disk upgrade

Steps:

1. Copy update firmware “amp 6500.img” to the root directory of a USB disk;
2. Insert the USB disk to the AMP 6500 terminal;
3. Click the system application, “Settings” -> “Updater” -> “Update from USB”, start updating.
4. After the completion of the copy, system will reboot to recovery mode 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 your 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 your device.

Removal Detection

AMP 6500 is designed as an unattended device. It should be installed to comply with PCI PTS. The anti-removal switch is protected by dual control. The anti-removal must be turn on after installed. Otherwise, it cannot perform transaction at all.

Once AMP 6500 removed without permission, an attack will rise, and the key encryption key will be erased immediately.

Security

Software Development Guidance

When developing applications, the developer must respect the guidance including APIs and environment described in the document [6] and 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

All weak cipher suite are removed from device, AMP 6500 only supports the cipher suites as PCI PTS required.

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

AMP 6500 supports SRED functionality, and cannot turn off it. For AMP 6500, 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.

Algorithms Supported

AMP 6500 supports the following cryptographic algorithms:

- TDES(112 bits and 168 bits)
- 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 6500 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 6500 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 168 bits)
- Master Key/ Session Key (TDES, only 168 bits)

Key Name	Purpose	Algorit hm	Size
TMK	Decryption of session keys (TPK, TAK, TDK)	TDES	128/192 bits
		AES	128/192/25 6bits

TPK	Online PIN encryption key	TDES	128/192 bits
		AES	128/192/256 bits
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	128/192/256 bits
Fixed TDK	Encrypt account data.	TDES	192 bits
DUKPT Key	Online PIN encryption key and Message authentication	TDES	128/192 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 6500 under dual control and split knowledge 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 Replacement

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 “Clear Key” in AMP 6500’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
LTE	Long Term Evolution
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] AMP 6500 Software Development Kit
- [7] AMP 6500 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 6500-API-DOC