AMP 1200 Security Policy

V 1.0.2

Advanced Mobile Payment Inc

www.amobilepayment.com

Revision History

Date	**Revision Level**	**Description**	**Modified by**
2017-11-08	*1.0.0*	*Original Version*	*Brian*
2018-01-15	*1.0.1*	*Update temperature details*	*Stephen*
2018-01-16	*1.0.2*	*Update temperature details*	*Xilink*

Table of content

1 Purpose

This document is to describe a security policy which addresses the proper use of AMP 1200 in a secure fashion, including information on key-management responsibilities, administrative responsibilities, device functionality, identification and environmental requirements.

Any unapproved using of AMP 1200 will violate the PCI PTS approval of the device.

2 References

[1] PCI PTS POI Modular Derived Test Requirements Version 5.0 - Sept 2016

[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 1200 application development manual.doc

[7] AMP 1200 PRODUCT MANUAL.pdf

[8] Software Security Guidance.doc

[9]Signature Card Request Guide.doc

[10] Application Signature Tool Guide.doc

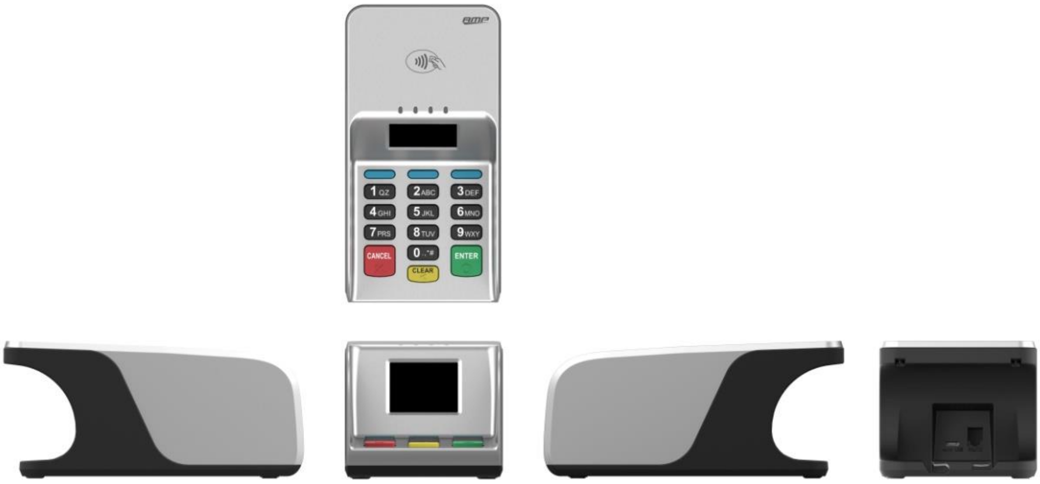
3 Device Identification And Inspection

3.1 Device Functions

AMP 1200 is an attended PIN PAD products; this device provides physical keypad, contactless card reader, LCD display. AMP 1200 is a desk-mounted PIN PAD and there is a privacy shield covering the keypad area which can prevent the peep. The power system is based on DC 5V power supply and the communications to the external are based on USB, UART connection.

3.2 Appearance

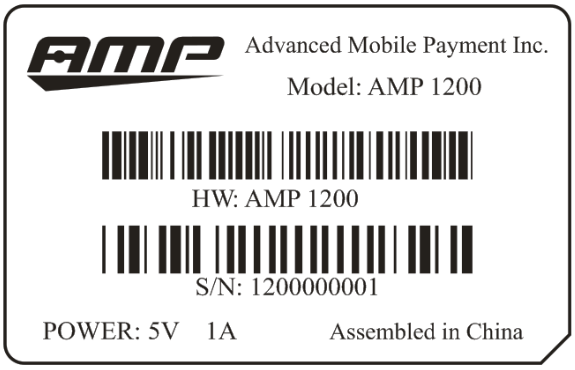
Please check whether the appearance of AMP 1200 is the same as follow:



3.3 Version Information

Hardware version

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



Advanced Mobile Payment Inc.
Model: AMP 1200

HW: AMP 1200

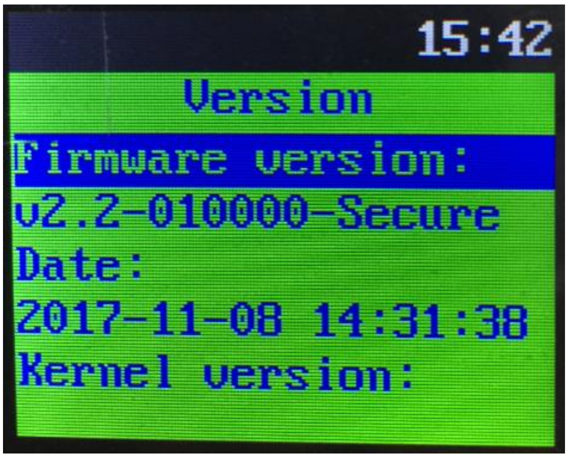
S/N: 1200000001

POWER: 5V 1A Assembled in China

Firmware version

The Firmware version can be view as following:

1. Power up AMP 1200 and go to home screen. Enter the Settings function of system.
2. Select the “About version” item.
3. You can see the Firmware version, Kernel version and Boot version.



15:42
Version
Firmware version:
v2.2-010000-Secure
Date:
2017-11-08 14:31:38
Kernel version:

3.4 Identification

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 1200 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 1200 is altered, if found some

trace, please reject the device.

4. Check if something overlay on the physical keypad in order to prevent overlay attack.

3.5 H/W specification

Display	1.77 inch,128*160 LCD
Contactless Card Reader (Optional)	Supports Mifare classic, Mifare Ultralight, Mifare DESFire, ISO 14443 A & B
Internal PIN Pad	Supports MK/SK, Fixed, DUKPT;
Peripheral Port	1 micro USB device (communication +5VDC power) 1 4P4C RS232 serial ports (communication +5VDC power)
Working Environment	Temperature: 0℃ ~ 50℃(32℉ ~ 122℉); Humidity: 10% ~ 90% (non-condense)
Storage Environment	Temperature: -20℃ ~ 60℃(-4℉ ~ 140℉); Humidity: 5% ~ 95% (non-condense)
Size	157.5*82.5*71mm
Weight	230g

4 Security Guidance

This section is mainly describe the security about how to use the device and how to development process. Before using the device, you should inspect the device carefully as following.

4.1 Environmental Requirements

AMP 1200 provides a privacy shield, when using, please cover by your body to take care it is not overlooked behind your back when entering PIN code.

1. Temperature & Humidity Environments
   Operation Temperature & Humidity : 0 ℃ ~ 50℃ /10% ~ 90%

(non-condense)

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

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

2. Tamper Conditions

   Tamper temperature: when CPU temperature lower than -35℃ or higher than 95℃, tamper will occur.

   Tamper voltage: when BBL (Battery Backed Logic) voltage lower than 2.0V or higher than 3.6V, tamper will occur.

   Tamper frequency: when BBL (Battery Backed Logic) frequency out of range 32.768KHz ± 10%, tamper will occur.

   When tamper occurred, the keys used for transaction will lost, you have to send device to vendor for repair.

3. Power Environments

   The power supply is used for working by connect USB or RS232 cable.

   The power supply specification:

   Input: +5VDC

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.).

4.2 Self-Test

AMP 1200 using self-tests to check firmware authenticity in both its processors. The self-test is performed:

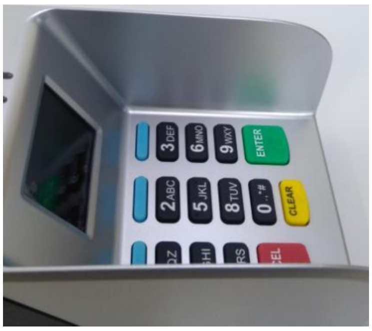
1. Every time the unit is powered up.
2. At least once every 24hours.

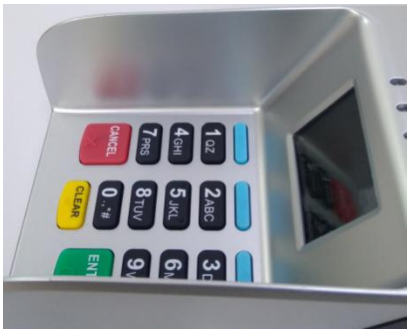
AMP 1200 performs a self-test, which includes firmware, application, stored keys, authenticity and any other sensitive properties tests to check whether the device is in a compromised state. If the result is failed, the device displays the lock icon and more tamper information on LCD and its functionality 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.

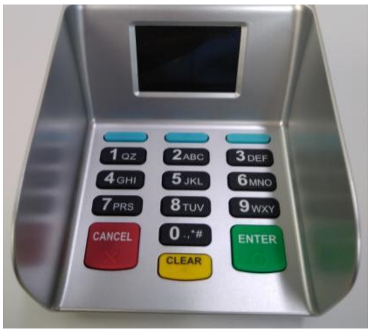
4.3 Pin Shield checking guide

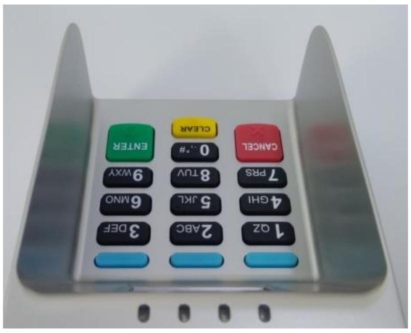
For the security using of AMP 1200, every day before using the device, operator must inspect the pin shield as follow:

1. Tilt the device to the angle as the following pictures, to view the area between keypad and Pin Shield area. If there are some barriers in, the device cannot be used.

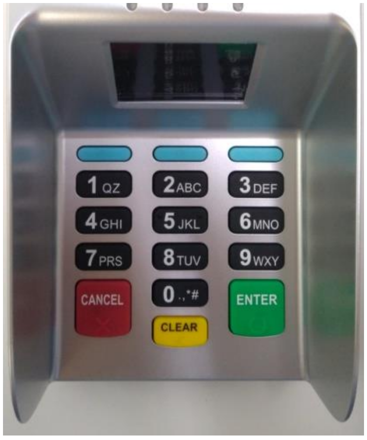


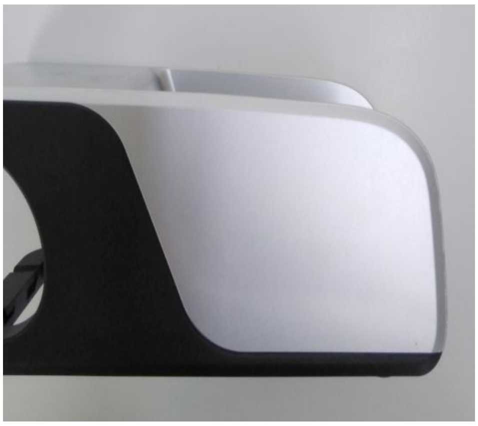






2. Check if the Pin Shield is the same as follow pictures or not. If not, the device cannot be used.





3. Check the area around the Pin Shield; if there is some obstacle or the Pin Shield seems being changed, the device cannot be used.

4.4 Periodic Security Inspection

For the security using of AMP 1200, 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 1200 is altered, if can find some trace, please reject the device.
3. Check if something overlay on the physical keypad in order to prevent overlay attack.

4.5 Change Default Values

When manufacturing in factory, the device of AMP 1200 is set to 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.

4.6 Installation Guidance

User should refer user manual before installation this device.

The device consists of following items:

- 1 Device
- 1 USB cable
- 1 RS232 cable
- User manual

All software is installed before deliver to end user. User can use PIN entry normally.

This device is an attended desk-mounted PIN PAD and it provided a privacy shield. The customer should be advised to cover by his body to take care it is not overlooked behind his back when entering PIN code.

The AMP 1200 is designed to be an attended desk-mounted PIN PAD. Before using, please check if the origin that providing the AMP 1200 device is authorized, check if the appearance of AMP 1200 is altered, check if there something or bugger around the Pin shield area, if found, reject the device. If you find the above problems, please refuse to use.

4.7 Configuration Setting

The AMP 1200's firmware does not need any configuration setting.

4.8 Sensitive Roles

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. 2. Download application 3. Access to devices sensitive services
End-users	operate	Perform transaction
AMP	maintainer	1. Sign customers public key 2. Repair devices and unlock the devices if tampered

Table Different roles and operations

4.9 Update/Download

Since the device only has USB and UART interfaces, does not have remote communication ability, so can’t support OTA, it can only update by USB cable. Firmware update under dual control in security environment.

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 device. If device type is not compatible, firmware will not be updated. When firmware update is completed, restart device again, and new firmware version will be shown.

4.10 Software develop Guidance

When developing applications, the developer must respect the guidance described in the document [6]; document[6] including document[8] for SRED application guidance.

4.10.2 SRED applications development

1. Account data read from contactless card reader, 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.

4.11 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 [9] and document [10].

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

5 Key Management

5.1 Key Management systems

1. AMP 1200 supports the following key systems:
   - Fixed key
   - MK/SK key
   - DUKPT

   MK/SK key, a master key and session key hierarchy. The Session Keys are encrypted/decrypted by Master Keys.

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

2. AMP 1200 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)

3. AMP 1200 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)

5.2 Key Loading

When the product are manufactured, The initial keys including TMK, Fixed key and initial DUKPT are injected into AMP 1200 under dual control and split knowledge in security environment.

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

5.3 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 1200’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.

5.4 Key Table

Key Name	**Purpose**	**Algorithm**	**Size**
Master Key	Decryption of session keys (PIN Key, EAK, MAC Key)	TDES	128/192 bits
		AES	128/192/256bits
PIN Key	Online PIN encryption key	TDES	128/192 bits
		AES	128/192/256bits
MAC Key	Message authentication	TDES	128/192 bits
EAK	Encrypt account data.	TDES	192 bits
Fixed MAC key	Message authentication	TDES	128/192 bits
Fixed PIN key	Online PIN encryption key	TDES	128/192 bits
		AES	128/192/256bits
Fixed EAK	Encrypt account data.	TDES	192 bits
DUKPT Key	Online PIN encryption key and Message authentication	TDES	128/192 bits

5.6 Key removal

If tamper event is detected, all the keys in the device will be erased automatically.

After the keys are loaded to device, they will be available until administrator wants to erase all keys for decommissioning or tampering detected.

6 Device Maintenance

1. Decommissioning/Removal
    - 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.
    - 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.

    - Temporary removal

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

7 Vulnerability Detection and Follow-up Action

When new vulnerabilities, threats or bugs are detected via public resource or the customers, AMP performs analysis to see if the new vulnerabilities, threats or bugs may impact on the AMP 1200 security. AMP contacts PCI lab and gets consulted if there is a delta evaluation is necessary.

If the vulnerabilities, threats or bugs impact on the AMP 1200 security, AMP 1200 immediately informs customers of the vulnerabilities, threats or bugs analysis result via e-mail and send the patch to the customers. If Hardware change needs to be involved to fix the issue, customers should return their AMP 1200 devices to AMP 1200 manufacturing facility for the repair.

When a new vulnerability occurs, AMP’s security team will send a vulnerability notification email to the customers (especially their security managers).

Bug report contact with AMP email:
support@amobilepayment.com

8 Tamper Detection and Response

8.1 Tamper Trigger Events

- Front case removal
- Back case removal
- Physical penetration on all the sides of the device
- Temperature is > 90˚C or < -30˚C.
- Stored sensitive data authentication failed during the Self-test

8.2 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, you can contact your authorized service or AMP to maintain it