AF60S Security Policy

Product Model： AF60S
Hardware Version： V1.1

Beijing Shenzhou Anfu Technology Co., Ltd

1. Document Information

1.1. Evolution follow-up

Revision	Type of modification	Date
V1.0	Creation	2018-12-01
V1.1	Details added	2019-03-01
V1.2	Modifications	2019-05-30

1.2. Acronyms

Abbreviation	Description
N/A	Not Applicable
PED	PIN Entry Device
PIN	Personal Identification Number
RSA	RSA Algorithm
TDES	Triple Data Encryption Standard
AES	Advanced Encryption Standard
SHA	Secure Hash Algorithm

1.3 Reference

[1] X9 TR-31 2010, 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 Par2: 2006, Retail Financial Services Symmetric Key Management Part 2: Using Asymmetric Techniques for the Distribution of Symmetric Keys
[3] ANSI X9.24-3-2017, Retail Financial Services Symmetric Key Management Part 3: Derived Unique Key Per Transaction
[4] ISO 9564-2, Banking —Personal Identification Number (PIN) management and security Part 2: Approved algorithms for PIN encipher
[5] Payment Card Industry PTS POI Derived Test Requirements, v5.1

2. 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. It is used to guide product users and developers utilizing the security features more properly. The PTS POI version of device assessed is V5.1.

3. Security Policy

3.1 Product Overview

AF60S POS terminal passes PCI PTS Evaluation as a pin entry device.
AF60S POS terminal is a hand-held device which supports the following interfaces:

- IC card reader (ICCR)
- Contact less card reader
- Magnetic card reader (MSR)
- Display screen (LCD)
- Micro USB port
- Buzzer
- Four LEDs
- Physical keypad

And this device supports the following protocol:

- Bluetooth

The operational and environmental conditions for which the device was designed.

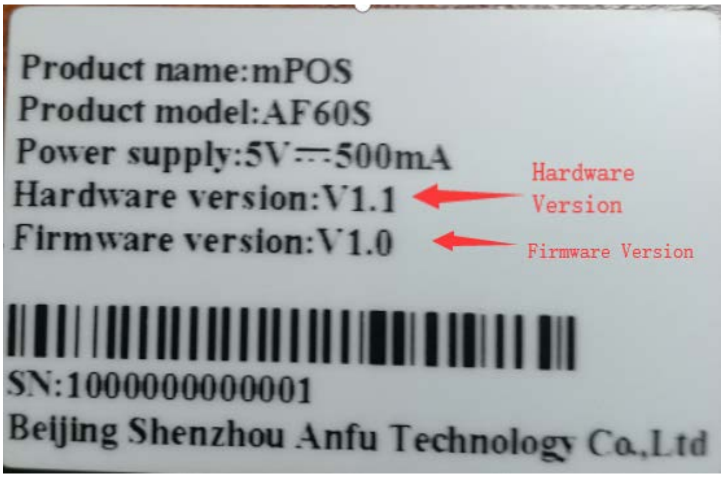
- Working Temperature: 0C° ~ 50C°
- Working R.H.: 5% ~ 90%(non-condense)
- Storage Temperature: – 20C° ~ 70C°
- Storage R.H.:5％ ~ 90％ (non-condense)
- Power Input: DC 5V

3.2 Hardware and Software Version

Hardware version and firmware version can be found on the label on the device and on the screen at the time of system start.

The application version can be found on the screen at the time of system start.

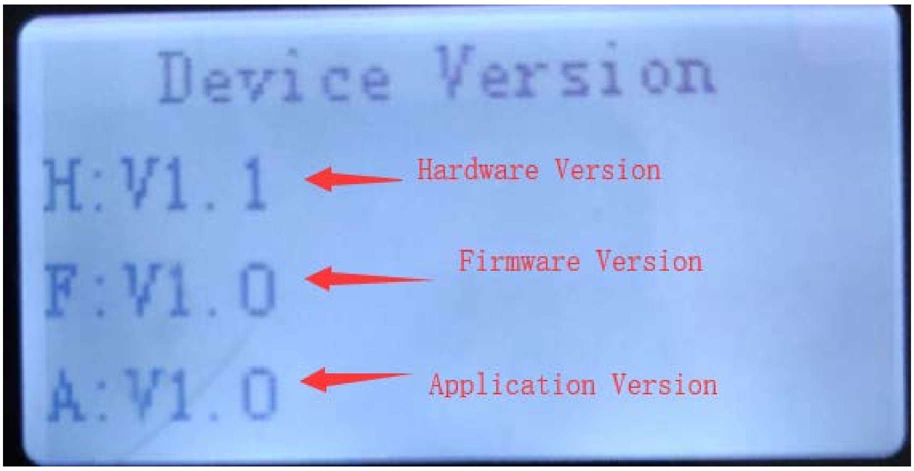
Hardware Version is V1.1 and Firmware Version is V1.0. They are printed on a label on the device.


Product name:mPOS
Product model:AF60S
Power supply:5V⎓500mA
Hardware version:V1.1
Firmware version:V1.0

SN:1000000000001
Beijing Shenzhou Anfu Technology Co.,Ltd

Hardware Version
Firmware Version

Hardware Version (V1.1), Firmware Version (V1.0) and Application Version (V1.0) are shown on the screen at the time of system start.



Device Version

H:V1.1

F:V1.0

A:V1.0

4. User Guidance

4.1 User Guide

The end user should check whether all components are intact when the device is received at the first time. There are one USB line and one copy of user guide specification along with AF60S terminal. Before using the device, user needs to check if it works well. It's recommended that the user asks the vendor for inspection, refunding or device exchanging when any problems are found.

The usage of the device must comply with the document. Otherwise, the device will violate PCI PTS authorization.

4.2 Secure Usage Environment

This device is designed to be used in an attended environment. Otherwise, the device will violate PCI PTS authorization.

Also, the device can only be used normally under a specific environmental condition. When the device detects an abnormal condition, a tamper event will happen and all the sensitive data will be cleared.

4.3 PIN Entry Guide

AF60S is hand-held mobile POS terminal. The PIN entry of the device only supports physical keypad. Before input the PIN, make sure the tip message on the LCD is about pin input. When pressing each PIN value, a Beep will be done by the device and a character "*" will be shown on the LCD. Block the keyboard with body.

4.4 Device Periodically Checking

The merchant or acquirer must inspect the terminal to ensure that the following measures are carried out.
Daily check whether the terminal is destroyed.
Daily check if the terminal is inserted by a malicious bug.
Daily check the terminal (including LCD, physical keypad, etc.) to ensure that it is free of rogue overlays.
No suspicious wires are connected to any ports.
HW and FW versions on terminal label or screen are consistent with the approved ones.
No open case evidence is found via checking the case or screw holes.
No suspicious thing appears around IC and MSR reader.
Installation and maintenance operations are performed by trusted persons.

4.5 Secure Use ICC

To make sure IC card being used securely, the merchant will be informed to note the following cases.
Check whether a suspicious wire is around IC card opening. If so, please stop using the device and inform the vendor for security inspection.
Check whether IC card is inserted smoothly. If not, please stop using it and inform the vendor for security inspection.
Check whether the shell of IC card interface is integral. If any damage evidence is found, please stop using it and inform the vendor for security inspection.

4.6 Secure Use MSR

To make sure MSR being used securely, the merchant will be informed to note the following cases.
Check whether a suspicious wire is around MSR guide. If so, please stop using the device and inform the vendor for security inspection.
Check whether swiping card is smooth. If not, please stop using it and inform the vendor for security inspection.
Check if there is any addition beside the MSR from the hollow guide. If so, please stop using it and inform the vendor for security inspection.
Check if MSR guide is destroyed. If so, please stop using it and inform the vendor for security inspection.

4.7 Dealing with Fault

The merchant or acquirer should always concern with the status of the device being used.

The device which displays abnormal information must not be used for PIN transaction any more without further inspection. Users are advised to contact with the vendor for further and detailed secure inspection.

4.8 Procedures for Decommissioning Device

Devices will be gathered by security personnel once they are decommissioned permanently. And all sensitive information will be erased. This can be done by taking apart the device to make it tampered or using a dedicated tool to delete all sensitive information actively. Then these devices are transported back to vendor factory for disassembling and recycle. If a temporary removal required, it is unnecessary to change the status of the device due to all sensitive information is still under the protection of physical and logical security mechanism.

4.9 Change Default Values

Before the devices being used, the password/password1/password2 must be reset. The default value of the password is “88888888”.

4.10 Personal Data Privacy

AF60S is designed to be a hand-held device. It’s recommended that:
The cardholders should use their body to prevent from being peeped from their back.
Use hand to block the view of keypad during PIN entry.
Make sure the cardholder keeps at a certain distance from others.
Make sure no detection device such as video camera is facing towards the keypad.
Additionally, acquirer, administrator, and merchants have to make sure to enter the PIN safely.

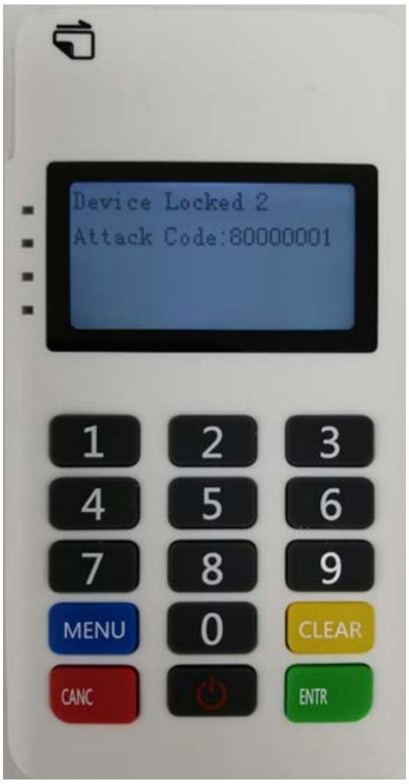
5. Hardware Security

5.1 Tamper Response Event

A merchant or acquirer can easily notice a tamper event happened in the terminal. A warning message will be displayed on the screen and the terminal is locked when tampered. Then all the sensitive data are erased. Any happened tamper event will make the device out of normal service. The device has 2 separate modes as below:

- Activated mode: Device is fully operational.
- Freezing Mode: Device is tampered and can’t be operated. It needs reactivation after maintenance and security checks.

The device must be sent back to the vendor for security checking and repairing when it is tampered.



5.2 Environmental Failure Protection

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 range does not alter the security). The device will get tampered when environmental conditions are out of range. Thus, all sensitive information will be cleared automatically and terminal turns into inoperable status.

The device is provided with voltage and temperature detection sensor, which ensures that the terminal is security from environmental conditions:

Backup battery low detect voltage set is 1.90V.

Backup battery high detect voltage set is 3.62V.

Temperature sensor low threshold set is -39C°.

Temperature sensor high threshold set is 109C°.

If the backup battery voltage is out of range, the internal sensitive information will be erased.

If the temperature is out of range, the internal sensitive information will be erased.

6. Software Security

6.1 Software Development Guide

The developer must accept training course before development activity starts and respect the coding rules and best practices during the whole development stage. Please refer to *Coding Specifications* for development guidance.

6.2 Firmware and Software

When downloading and updating software from local site, it needs signature authentication. The terminals only accept firmware and software with legitimate and correct signature. The software and firmware loading process does not need protection by any special way. The device will reject to load and save any unauthenticated software and firmware.

6.3 Firmware and Software Authentication

This device implements asymmetric techniques for firmware authentication. RSA algorithm with 2048 bits key is used for signature verification and SHA256 algorithm is used to calculate the digest of firmware. The firmware is signed by RSA-2048 bits private key which is only controlled by the vendor. And signature is verified by the corresponding public key. The terminal will check the integrity and validation of firmware and application when start-up every time. If failed, the terminal will stop working.

6.4 Key Checking

All keys stored in the terminal will be checked during being used every time. If failed, the keys are erased.

6.5 Self-Test

Self-test is routinely executed upon start-up or reset every time. This device reset is performed periodically (per 23 hours) during the period of normal use. This test is not initiated by an operator.

7. System Administration

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.

8. Key Management

8.1 Key Management Techniques

The AF60S terminal implements the key management techniques:

- Master Key/Session Key: A method using a hierarchy of keys. The session keys are unique per terminal.
- Fixed Key: A method using a fixed of keys. The session keys are unique per terminal.
- DUKPT: A method deriving unique keys per transaction. The initial DUKPT key is unique per terminal.

Use of the device with different key-management systems will invalidate any PCI approval of the device.

8.2 Cryptographic Algorithms

The device includes the following algorithms:

1. RSA (2048 bits)
2. SHA256
3. Triple DES (112bits/168bits)
4. AES (128bits/192bits/256bits)

8.3 Key Management

Key Name	Usage	Algorithm	Size (bits)	Storage
Fixed Pin Key	Encrypt PIN blocks	TDES/AES	TDES:168 AES:128/192/256	Flash
Fixed Mac Key	Generate or verify MAC of data blocks	TDES/AES	TDES:168 AES: 128/192/256	Flash
Fixed Data Key	Encrypted account data	TDES/AES	TDES:168 AES: 128/192/256	Flash
Main Key	Encrypt or decrypt session keys	TDES/AES	TDES:168 AES:128/192/256	Flash
Session Pin Key	Encrypt PIN blocks	TDES/AES	TDES:168 AES:128/192/256	Flash
Session Mac Key	Generate or verify MAC of data blocks	TDES/AES	TDES:168 AES:128/192/256	Flash
Session Data Key	Encrypted account data	TDES/AES	TDES:168 AES:128/192/256	Flash

Initial DUKPT Key	Derived working keys	TDES/AES	TDES:112 AES:128/192/256	Flash
Firmware PUK	For Firmware Verify	RSA	2048	Flash
Application PUK	For Application Verify	RSA	2048	Flash

8.4 Key Injection Method

This device supports key loading. Specific tools complied with key management requirements shall be used for key injection. These operations are controlled by secure manager and happened in a secure room. Dual control and split knowledge mechanism are mandatory during this process. Initial keys should be injected into the device by two trusted persons using the keypad in a secure environment. In MK/SK system, the working keys loaded into the device in the form of cipher, under the protection of main key.

8.5 Key Replacement

Any key should be replaced with a new key 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.

8.6 Key Removal

There are two ways to remove the keys installed. One is passive erasure by firmware or hardware, like when a tamper event happened. The other is actively clearing by security manager via dedicated tool, in case of repair or decommissioning.

9. Roles and services

The roles that supported by the terminal are defined as follows.

- **Administrators**
  System sensitive functions, such as password reset, key injection and system time setting. Only the vendor authorized administrators have access to them under dual controls.
- **End Users**
  The end users can process the PIN-based transaction.

10. Account Data

The account data will be encrypted by fixed data key or session data key or DUKPT data key. The TDES and AES algorithm will be used according with the key. The ECB and CBC mode will be used.

There is no white list or black list in the device.

The SRED cannot be closed.

11. Bluetooth Development Guide

The Bluetooth module must be set as “Pin Code” mode for paring.

If the Bluetooth module is unused, the software must power off the module.

If the device is not in a paring process, the Bluetooth module must be set invisible to Bluetooth host.

Every time paring with host, the software must be set a random paring code to the module.