AF70

Security Policy

Version 1.00

Beijing Shenzhou Security Pay Technology Co., Ltd.

Dec 2018

Version Control

Revision	Date	Description of updates
1.00	2018/12/25	Document creation

TABLE OF CONTENTS

1. Introduction

This Security Policy document addresses the proper of secure manner use of the AF70 terminal, in order to meet the security requirements of the Payment Card Industry (PCI).

The use of the device in an unapproved method, as described in the security policy, will violate the PCI PTS approval of the device.

2. References

[1] ANS X9.24 Part 2: 2006, Retail Financial Services Symmetric Key Management Part 2: Using Asymmetric Techniques for the Distribution of Symmetric Keys

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

[3] ISO 9564-1, Financial services — Personal Identification Number (PIN) management

[4] ISO 9564-2, Banking — Personal Identification Number management and security

[5] X9 TR-31 2010, Interoperable Secure Key Exchange Key Block Specification for Symmetric Algorithms and security —

Part 1: Basic principles and requirements for PINs in card-based systems

Part 2: Approved algorithms for PIN decipherment.

3. Device Identification

Device description

AF70 terminal is a new generation of traditional POS products. This device is designed for financial transaction in an attended environment, and as a hand-held device, it provides display screen with 320*240 resolution, SIM card readers, IC card reader (ICCR), magnetic card reader (MSR), contactless card reader, integrated high-speed printer and camera.

Appearance

Please check whether the appearance of AF70 is the same as follow:

Figure 2-1

AF70 provides the following functions to meet the requirement of different scenarios.

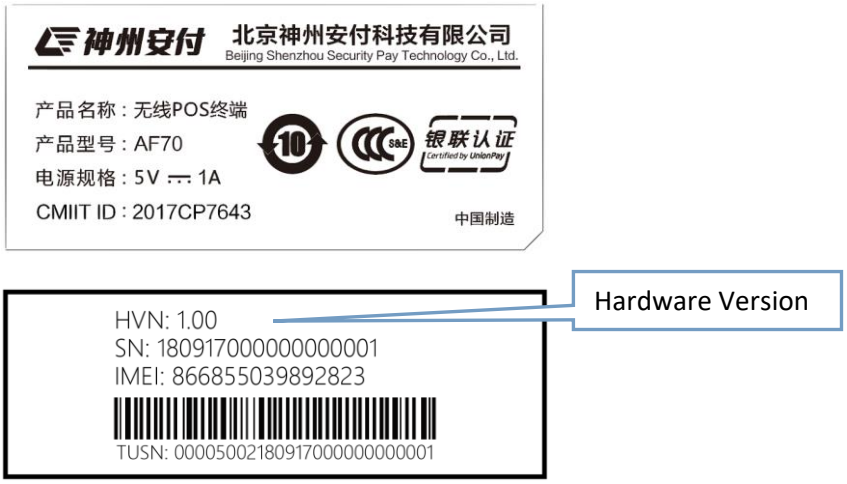
Configuration	Description
Barcode	1D barcode

	2D barcode
communication	USB
	Bluetooth
	GPRS
Camera	30w pixels fixed focus camera

Terminal label

User can identify the approved device through the methods as below:

- Check the device name and type on the label of the device, which should not be modified by anyone after manufactory.
- Check the product label which is adhere on the back side of AF70, reading machine type, working voltage and currency, barcode and product number, etc.
  User can check the labels of the device with the picture below as an example:



Version information

To examine the version of the device, user can enter home menu, then select “1-Show Version”, the hardware, firmware version information will be shown below on screen or shown during starting up.

4. Secure Guidance

Security Inspection

When receiving the device via shipping, the merchant or user will be informed to inspect before use for a transaction to make sure:

- The labels covered on screw holes are not broken.
- The device case has never been opened or destroyed, if doubt, please reject to use it and ask vendor for help.
- The device information, such as name, type, firmware and hardware version, meets the requirements of PCI PTS POI.
- Power on the device, please check if any tamper warning message is shown on the screen.

This checking routine is applied to shipment or periodicity checking. Also, a user manual is provided with the device, in which the user will be told how to view the serial number, logo and version and how to use the device securely.

Secure Settings

The devices are functional when received by the merchant or acquirer. No security related settings need to be setup by the end user in order to meet security requirements.

Force to Update

The administrator's passwords for security sensitive services are forced to be updated at the first time logging on the terminal.

Secure Environment

This device is designed to be used in an attended environment.
Power Supply: 3.8V
Operating Temperature: 0°C - 50°C
Storage Temperature: -10°C - 70°C
Operating Humidity: 10% - 90% noncondensing
Storage Humidity: 5% - 95% noncondensing

Personal data privacy

AF70 is designed to be a hand-held device. It's recommended that:

- The cardholders should use their body to prevent peeping from their back or their free hand to block the view of keypad during entering PIN.
- Make sure the cardholder keeps at a certain distance from others on check sand.
- Make sure no unsecure device such as video camera towards the keypad.

Additionally, acquirer, administrator, and merchants have to make sure to enter their PIN safely.

5. Device Secure Maintenance

Decommissioning/Removal

- Permanent removal

  If device is permanently decommissioned from the service, it can be done by disassembling of device to lead it into tampered status, then any operation of device will be forbidden, and all sensitive data will be erased immediately.

- Temporary removal

  If the device is out of service temporarily, all sensitive data is kept and protected by battery power supply. No operations of changing state of device are needed.

Periodic Inspection

The merchant or acquirer must visually inspect the terminal when received via shipping and inspect periodically after the device is deployed to ensure that:

- The merchant or acquirer should daily check that the terminal was not destroyed or installed a suspicious bug. Make sure the devices are the approved ones.
- There is no evidence of unusual wires that have been connected to any ports of the terminal.
- Hardware version and firmware version on terminal label or screen are consistent with the approved HW and FW version.
- There is no open case evidence visible via checking the case or the labels in screw holes.
- The merchant or acquirer should also check that the installation/maintenance operations are performed by a trusted person.

6. Hardware Security

Tamper event

Any physical penetration will be considered as a tamper event and all the tamper trigger events are shown below:

- Back case removal.
- Physical penetration on all the sides of the device.
- Logical tamper because of improper use (administrator's password error count exceeded and self-test failed, etc.).
- The temperature goes out of specified ranges.
- Supply voltage of Button Battery is out of specified ranges.

Tamper response

If the device detects tamper event, the tamper mechanisms will activate, all keys and other sensitive data will be cleared and make the device unusable and display the tamper information on the screen.

The operators, merchants and users can easily detect a tampered device when,

- A warning message 'PED TAMPERED!' is displayed on the screen.
- The device will go out of service, no transaction can be performed since keys are cleared.

If the device is tampered state, the user must contact the device maintenance personnel immediately for help.

Environment Conditions and Environmental Failure Protection

The environmental conditions of operation of the device are specified in chapter 4.1.

The security of the device is not compromised by altering the environmental conditions. Subjecting the device to temperature or operating voltages out of the scope does not alter the security.

7. Software Security

Software Development Guide

The AF70 POS device provides security communication interface which is compliant with PCI requirement. The application developer should strictly comply with the development manual. The developer also must accept training course before development activity starting and respect the coding rules and best practices during the whole development stage.

Software Update

Updates and patches can be loaded in the device. When downloading or updating firmware, software, application, it needs authentication. AF70 terminals only accept updates and patches with legitimate and correct signature. The device will reject to load and save any unauthenticated updates and patches. Any security related firmware changes will cause firmware version update. For more update procedure, the user can refer to the <AF70 user manual> document.

Firmware Configuration

The updates and release changes cannot and do not affect the secure configuration of the firmware. The firmware remains in minimal configuration.

Firmware Authentication

This device implements asymmetric cryptographic algorithm for firmware and software authentication. RSA algorithm with 2048bits key is used for signature verification and SHA256 algorithm is used to calculate the digest of firmware.

Any updates loaded into AF70 terminal must be signed with RSA-2048 bits private key which is only controlled by Shenzhou Security Pay Company. If the authentication fails, the updates will not be loaded. In that case, new authorized updates will be needed to be downloaded into the device.

Please refer to <Shenzhou Security Pay Loader Operation Guide> for the detail information about updates loaded.

Self-Checking

The self-checking of device contains following items.

- Power on check

When the system powers on, it will check the firmware in a certain order to verify their integrity and legitimacy.

- Check key during key reading

During key reading, the key will be checked. If the key integrity or legitimacy fails in the checking procedure, the battery-backup key will be cleared and regenerated, and all other keys will be cleared.

- 24 hours check

The device will reboot every 24 hours to re-initialize the RAM. After power on, self-tests is performed to verify validity of firmware and keys. If any error detected, sensitive data will be erased.

8. Key Management

Design and Techniques

AF70 implements different types of key management techniques:

- DUKPT: a key management techniques based on a unique key for each transaction as specified in [2].
- Master Key/ Session Key: a method using a hierarchy of keys. The session keys are unique per transaction as specified in [2].
- Fixed Key: a key management technique based on a unique key for each terminal as specified in [2].

List of Supported Algorithms

AF70 terminal supports the following secure algorithms:

- RSA: Signature verification, 2048 bits.
- SHA256: Integrity verification
- TDES: Data encryption/decryption, 128/192 bits.
- AES: Data encryption/decryption, 128/192 bits.

List of Keys

AF70 terminal key management complies with ANSI X9.24 key management rule strictly. Each key has only one pure and only one value. When the terminal is suffering from attacking, the keys are erased.

Key Name	Pure/ Usage	Algorithm	Size(Bits)	Storage
SEK	System KEK	AES	192	Secure unit
TLK	Key for loading other TDES Key	TDES	128/192	Cipher-text in flash
Master Key	Key encryption for session keys loading	TDES	128/192	Cipher-text in flash
PIN Key	Encryption key for plaintext PIN Block	TDES	128/192	Cipher-text in flash
MAC Key	Encryption key for MAC generation	TDES	128/192	Cipher-text in flash
Decryption	Decryption key for data	TDES	128/192	Cipher-text

Key				in flash
Encryption Key	Encryption key for data	TDES	128/192	Cipher-text in flash
Account data Key	Encryption key for account data	TDES	192	Cipher-text in flash
Serial number Key	Encryption key for terminal serial number	TDES	128/192	Cipher-text in flash
DUKPT Initial Key	Initial DUKPT keys	TDES	128	Cipher-text in flash
DUKPT future Key	Encryption key for PIN Block encryption	TDES	128	Cipher-text in flash
AES PIN Key (TPKA)	Encryption key for plaintext PIN Block	AES	128/192	Cipher-text in flash

Key injection

AF70 terminal can be injected key by a local secure KLD, and it doesn't support remote key loading. Dual-control and split knowledge techniques are used to manage the key loading procedure in a secure room of acquirer.

- Only both administrator A and B input correct password can enter loading process.
- Initial plain-text loading keys which are divided into two full-length key components should be loaded into the device by two different persons. Each person is required to input his key component into the device separately.

Key Replacement

Whenever the original key is known or suspected and whenever the time is deemed feasible to determine the key by exhaustive attack elapses, the terminal will be demanded mandatorily to replace or inject the new keys before it can be used as a normal device which can process PIN transaction.

9. Secure System Management

System Administration

The device uses dual-control technology to protect sensitive services. Only if both of administrator A and administrator B input correct password, sensitive services can be entered and used.

The device is functional when received by the merchant or acquirer and the default passwords for sensitive function management should be changed mandatorily when using this device for the first time.

Roles and services

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

- Administrators

System sensitive functions, such as change password, key inject, set time and format PED. Only the vendor authorized administrators have access to them under dual controls.

- End Users

The end users can process the PIN-based transaction.

10. Development Guidance

AF70 implements the necessary security measures and functions to meet PCI security requirements. For payment or other security related applications, we vendor has provided <AF70 Application Development Manual> document to the developers, which provides safety-related development guidance such as follows:

- Application development process
- Application development environment
- Coding standards and good practices
- Payment application security standard

AF70 does not support SRED. The device cannot be connected to a tablet or mobile phone. Any such user will violate the approval of the device.

For OP Module: SSL/TLS protocol is known inherently weak and we vendor have already removed these inherently weak codes. AF70 only supports TLS1.2 version which contains higher security.