AF930
Security Policy

Version 1.00

Beijing Shenzhou Security Pay Technology Co., Ltd.

Mar 2023

Version Control

Revision	Date	Description of updates
1.00	2023/03/25	Document creation

Contents

1. Purpose

The device is assessed for PCI PTS POI v6.1. This Security Policy document addresses the proper of secure manner use of the AF930 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. General Description

2.1 Product Name and Appearance

Please check whether the appearance of AF930 is the same as follow:

2.2 Product Type

AF930 terminal is a hand-held PED device. This device is designed for financial transaction in an attended environment, it provides touch screen, LCD, IC card reader(ICCR), magnetic card reader(MSR), contactless card reader(CTLS), the wireless communication (Cellular (2G/3G/4G), WIFI, Bluetooth), thermal printer, speaker, buzzer, LED, SAM card slot, TF card slot, earphone jack and camera.

2.3 Identification

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 AF930, reading machine type, working voltage and currency, barcode and product number, etc.

The hardware version is V1.00 and the firmware version is V1.00.
User can check the labels of the device with the picture below as an example:

To examine the version of the device, user can enter setting menu, then select “About device”, the hardware, firmware version information will be shown below on screen.

3. Installation and User Guidance

3.1 Initial 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, and please check if any tamper warning message is shown on the screen.

3.2 Installation

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.

3.3 Environmental Conditions

This device is designed to be used in an attended environment.
USB Power Supply: 5.0V
Operating Temperature: 0°C - 50°C
Storage Temperature: -10°C - 70°C
Operating Humidity: 10% - 90% noncondensing
Storage Humidity: 5% - 95% noncondensing
When the following conditions occur, the tamper detector will clear sensitive data information immediately:
Battery voltage VBAT rises above 3.7V±0.15V
Battery voltage VBAT falls below 1.9V±0.15V
On-chip temperature rises above approximately 100±10°C
On-chip temperature falls below approximately -30~-40°C

The security of the device is not compromised by altering the environmental conditions (e.g. setting the device to outside the stated operating ranges' temperature or operating voltages does not alter the security). If the temperature or voltage is out of the range of the environmental protection features above, the device will enter into the tamper state.

3.4 Communications and Security Protocols

The approved communication interfaces are USB, Cellular (2G/3G/4G, IP, ICMP, HTTP, DNS, DHCP, TCP, UDP, TLS, PPP), Bluetooth and Wi-Fi (IP, ICMP, HTTP, DNS, DHCP, TCP, UDP, TLS, ARP).

The device supports TLS security protocol for TCP/IP security communication.

The device support Bluetooth BR/EDR with mode 4 level 4, and BLE with mode 1 level 4.

The device supports Wi-Fi with WPA2/WPA3; WEP is not supported.

Use of any method not listed in the policy invalidates the device approval.

3.5 Configuration 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.

4. Operation and Maintenance

4.1 Periodic Inspection

The merchants or acquirers should daily check as what described below:

- Inspect that the terminal was not destroyed or installed a suspicious bug. Make sure the devices are the approved ones.
- Inspect whether the ICCR card slot to make sure that no any untoward obstructions or suspicious objects at the opening.

- Inspect whether the MSR card slot to make sure that no any additional card reader and other inserted bugs.

- Inspect whether the firmware version is correct; and power on the device to inspect whether the firmware runs well.
- Inspect whether the device is tampered refer to section 4.5 tamper response.
- Inspect that there is no something overlay on the touchscreen in order to prevent overlay attack.

4.2 Self-Test

The self-test is performed upon start-up or reset. In order to perform self-test periodically, the device will reboot automatically in 24 hours after it starts up.

The self-test includes:

- Hardware security status.
- Firmware integrity and authenticity.

Once any failures are detected in process of self-test, the device will display a prompt indicating tampered status. At this situation, the device will turn into inactivated mode and can not be used. It should be sent to the vendor or an authorized service center for repair.

4.3 Roles and Responsibilities

The following table shows different roles and responsibilities:

Role	Responsibility
Acquirer/Merchant	Download customer key
End user	Perform transaction
Vendor	Maintain the device

4.4 Passwords and Certificates

The device is functional when received by the merchant or acquirer and there is no security sensitive default value (e.g. admin password) that needs to be changed before operating the device.

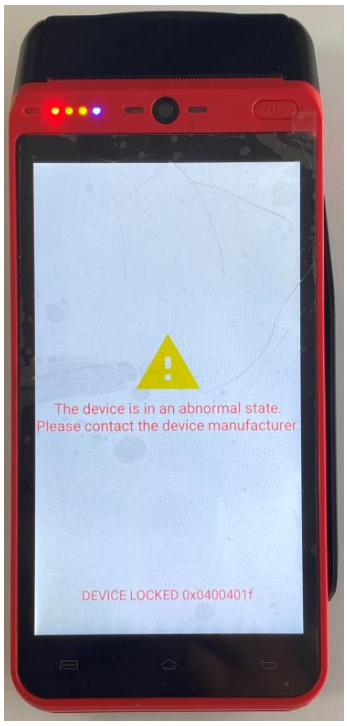
The device does not include any certificate for testing purpose after manufacture.

4.5 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 is displayed on the screen and the LEDs on the left will light.
- No other signal is used to indicate that the terminal has been tampered.
- The device will go out of service, and 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.

4.6 Privacy Shield

AF930 is designed to be a hand-held device without privacy shield. 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.

The following table shows the combinations of methods that must be used when installing the device to protect the cardholder's PIN during PIN entry.

Method	**Observation Corridors**				
	Cashier	Customer in Queen	Customer Elsewhere	On-Site Cameras	Remote Cameras
With Stand	No Action Needed.	Customer positions PED	No Action Needed.	Do not install within view of cameras.	Do not install within view of cameras.
Without stand	Position unit to face away	Position unit between	Used the body to	Do not install within view	Do not install within view

	from the cashier. Use signage to block cashiers view.	customer and the next in cue.	block the view of other customers and the device.	of cameras.	of cameras.
Customer Instruction	Used the body to block the view of the cashier and the device.	Used the body to block the view of other customers and the device.	Used the body to block the view of other customers and the device.	Do not operate within view of cameras.	Do not operate within view of cameras.

4.7 Patching and Updating

Updates and patches can be loaded in the device. When downloading or updating firmware, software, application, it needs authentication. AF930 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.

4.8 Decommissioning

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.

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.

5. Security

5.1 Software Development Guidance

When developing applications, the developer must respect the guidance described in the document to compliant with PCI security requirement. Please refer to document [8] when developing SRED application and document [9] when developing Open Protocol

application.

The following steps must be implemented：

- Security review and audit.
- Source code management and version control.
- Software test.
- Signature.

5.2 SSL/TLS

SSL protocol is known inherently weak and we vendor have already removed these inherently weak codes. AF930 only supports TLS1.2 version which contains higher security.

5.3 Signing

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 AF930 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.

5.4 Account Data Protection

Account data could be get through few ways: MSR, ICCR, and CTLS. The device will encrypt account data immediately regardless data entry from any way. The account data can be encrypted by MK/SK (TDES 192 bits or AES 128/192/256 bits) or DUKPT (TDES 128 bits or AES 128/192/256 bits).

The device does not support the pass-through of clear-text account data.
The device does not allow the disablement of SRED functionality.

5.5 Algorithms Supported

AF930 terminal supports the following secure algorithms:

- RSA (Signature verification, 2048bits)
- SHA-256 (Integrity verification)

- TDES (128/192Bits)
- AES (128/192/256Bits)
- ECC (P-256/P-384/P-521)

5.6 Key Management

AF930 implements different types of key management techniques:

- DUKPT: a key management technique based on a unique key for each transaction;
- Master Key/Session Key: a method using a hierarchy of keys. The session keys are unique per transaction.

AF930 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	Purpose	Algorithm	Size
KBPK	Protect TR-31 key block	AES	256Bits
Master Key	Key encryption for session keys Loading	TDES	128/192Bits
		AES	128/192/256Bits
PIN Key	Encryption key for plaintext PIN Block	TDES	128/192Bits
		AES	128/192/256Bits
MAC Key	Encryption key for MAC generation	TDES	128/192Bits
		AES	128/192/256Bits
Account data Key	Encryption key for account data	TDES	192Bits
		AES	128/192/256Bits
DUKPT Initial Key	Initial DUKPT keys	TDES	128Bits
		AES	128/192/256Bits
DUKPT future Key	DUKPT Encryption keys	TDES	128Bits
		AES	128/192/256Bits

Notes that use of the device with different key-management systems will invalidate any PCI approval of this device.

5.7 Key Loading

The key loading techniques supported by the device include the following category.
a. Clear-text key injection
b. Symmetric encrypted keys injection
AF930 terminal can be injected key by a local secure KLD after mutual authentication, and it doesn't support remote key loading. Dual-control and split knowledge techniques on the KLD are used to manage the key loading procedure in a secure room of acquirer.

5.8 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.

6. Acronyms

Abbreviation	Description
TDES	Triple Data Encryption Standard
AES	Advanced Encryption Standard
RSA	Rivest Shamir Adelman Algorithm
ECC	Elliptic Curves Cryptography
SHA	Secure Hash Algorithm
KLD	Key Loading Device
PCI	Payment Card Industry
PTS	PIN Transaction Security
POI	Point Of Interaction

7. References

[1] ANSI X9.24 Part 1:2017, Retail Financial Services Symmetric Key Management Part 1: Using Symmetric Techniques
[2] ANSI X9.24 Part2:2006, Retail Financial Services Symmetric Key Management Part 2: Using Asymmetric Techniques for the Distribution of Symmetric Keys
[3] ANS X9.24 Part 3:2017, Retail Financial Services Symmetric Key Management Part 3: Derived Unique Key Per Transaction
[4] X9 TR-31 2018, Interoperable Secure Key Exchange Key Block Specification for Symmetric Algorithms
[5] ISO 9564-1:2015, Financial Services – Personal Identification Number (PIN) management and security – Part 1: Basic principles and requirements for PINs in card-based systems
[6] PCI PTS POI Derived Test Requirements, v6.1 – March 2022
[7] Operating Manual
[8] Firmware Management Specification
[9] Open Protocol Security Guide