AF820
Security Policy

Version 1.00

Beijing Shenzhou Anfu Technology Co., Ltd.

Jun 2024

Version Control

Revision	Date	Description of updates
1.00	2024/06/08	Document creation

Contents

1. Purpose

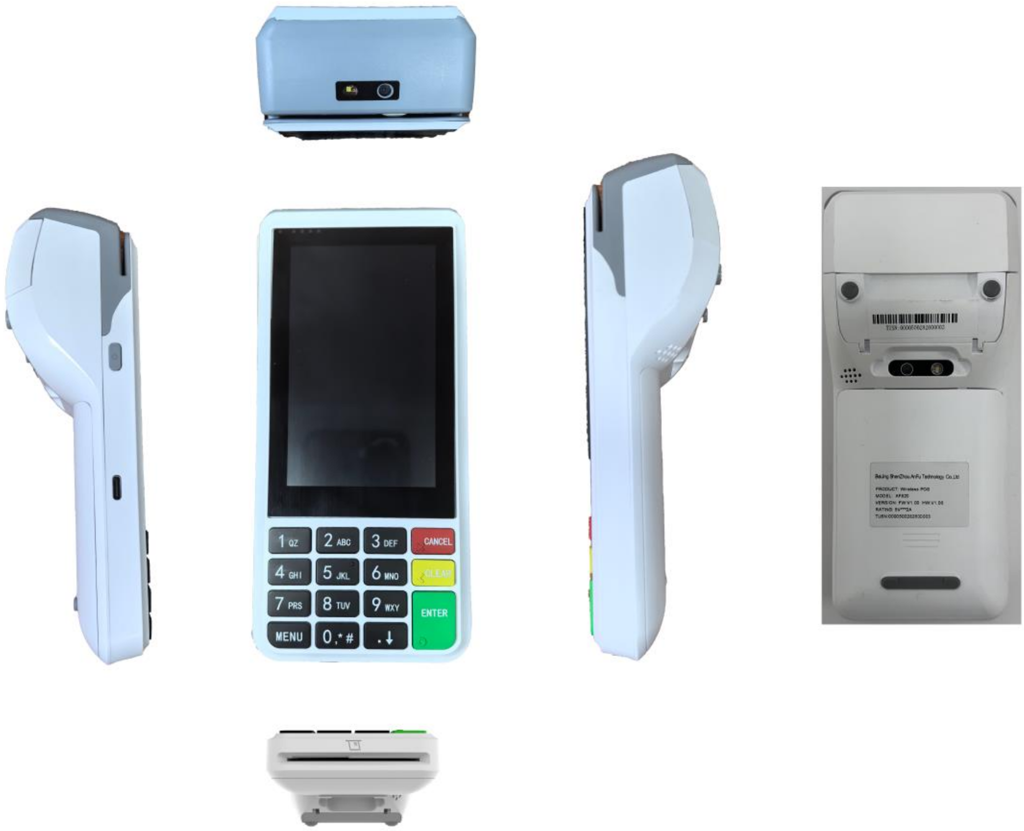
The device is assessed for PCI PTS POI v6.2. This Security Policy document addresses the proper of secure manner use of the AF820 terminal, in order to meet the security requirements of the Payment Card Industry (PCI).

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 Model Name and Appearance

The device model name is AF820.



2.2 Product Type

Terminal AP1 is a new generation of POS products. This device is designed for financial transaction in an attended environment, and used as a hand-held PED device.

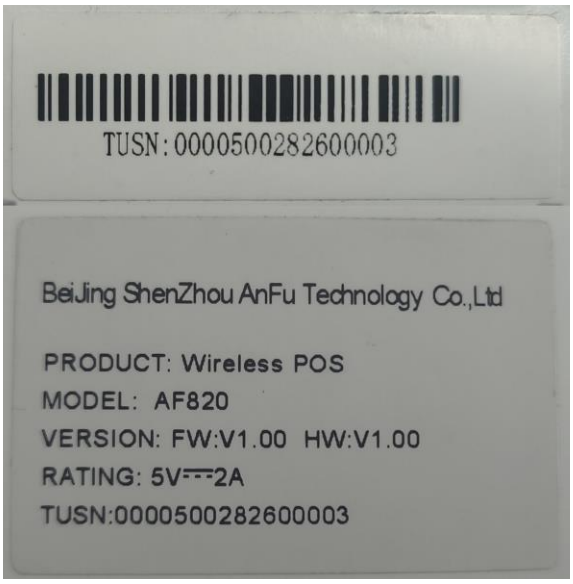
2.3 Identification

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

- Check the device model name on the label of the device, which should not be modified by anyone after manufacturing.
- Check the product label which is adhere on the back side of AF820, reading model name and serial number, etc.

The hardware version is V1.00 and the firmware version is V1.xx.

User can check the label of the device with the picture below as an example:

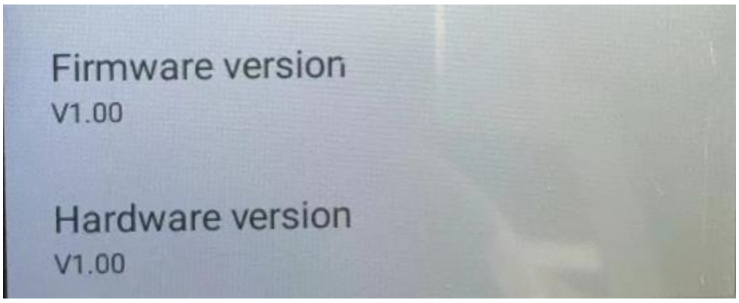


TUSN:0000500282600003

BeiJing ShenZhou AnFu Technology Co.,Ltd

PRODUCT: Wireless POS
MODEL: AF820
VERSION: FW:V1.00 HW:V1.00
RATING: 5V⎓2A
TUSN:0000500282600003

To examine the version of the device, user can enter setting application, then select "About device", the hardware, firmware version information will be shown below on screen. The picture below as an example:



Firmware version
V1.00

Hardware version
V1.00

Version definition as follows:
Hardware Version Number Description:
V1.00

Firmware Version Number Description:
V1.xx
The role of "x" is the version of non-secure parts, such as bug fixes and vulnerability fixes.

2.4 Device functions

The AF820 is a handheld PED terminal. It provides Physical Keypad, Power Button, LCD display, Touch Panel, TF card slot, two SIM card readers, IC card reader(ICCR), magnetic card reader (MSR), contactless(CTLS) card reader, two Cameras, Printer, USB, Wi-Fi, Cellular (2G/3G/4G), Bluetooth, GPS, Buzzer, Speaker, PSAM card slot, Power button and Charge ports. It is designed for portable and handheld use without a privacy shield, and the device can be shielded by the body when in use. The power system is based on a DC 5.0V power supply or battery and the communications to the external world are based on Wi-Fi, USB, Bluetooth and Cellular (2G/3G/4G).

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 anti-tear 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.
- Power on the device, 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 and version and how to use the device securely.

3.3 Environmental Conditions

This device is designed to be used in an attended environment.
Power Supply: 5V
Cell battery Tamper voltage.
High: 4.5±0.15V
Low: 2.0V±0.15V
Operating Temperature: 0°C - 50°C
Storage Temperature: -10°C - 70°C
Operating Humidity: 10% - 90% noncondensing

Storage Humidity: 5% - 95% noncondensing
Tamper temperature:
High: 100±10°C
Low: -35±5°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, PPP, IP, ICMP, TCP, UDP, DHCP, HTTP, DNS and TLSv1.2), and Wi-Fi (ARP, IP, ICMP, TCP, UDP, SCTP, DHCP, HTTP, DNS and TLSv1.2).

The device supports TLSv1.2 security protocol for TCP/IP security communication.

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

The device supports Bluetooth v5.2 with BR/EDR mode 4 level 4 and BLE, BLE only supports mode 1 level 4, and Justwork mode is disabled

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.

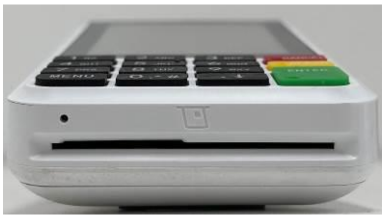
4. Operation and Maintenance

4.1 Periodic Inspection

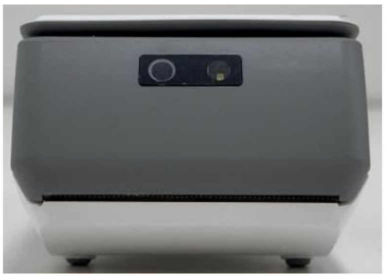
The merchants or acquirers should daily check as what described below:

- 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 whether the physical keypad being covered in order to avoid an 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 cannot 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.

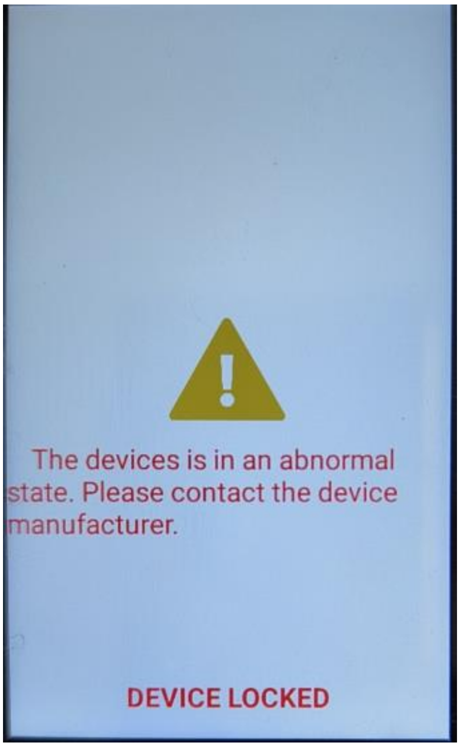
The device does not include any certificate for testing purpose after manufacture.

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 ‘The devices is in an abnormal state. Please contact the device manufacturer’ and ‘DEVICE LOCKED’ are displayed on the screen.
- There is no other prompt warning except LCD display.
- The device will go out of service and no transaction can be performed since keys are cleared.
- There is no any other prompt for device tamper response.



The devices is in an abnormal state. Please contact the device manufacturer.

DEVICE LOCKED

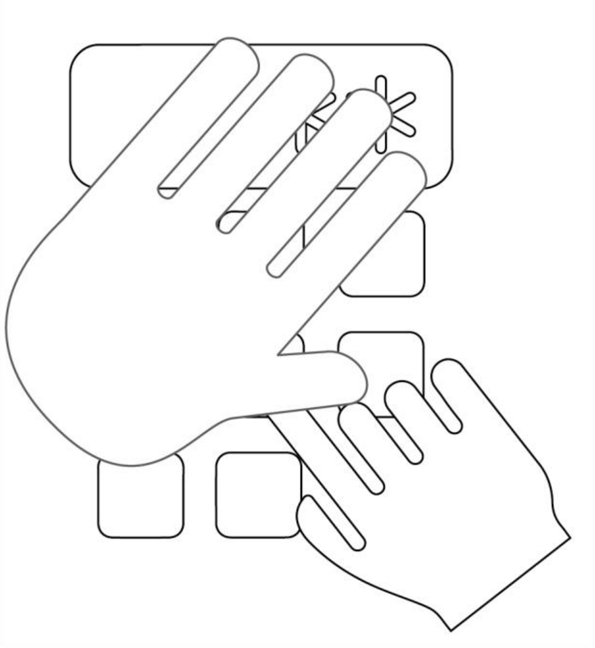
If the device is in the tampered state, the user must contact the device maintenance personnel immediately for help.

4.6 Privacy Shield

AF820 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, end user, and vendor 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 from the cashier. Use signage to	Position unit between customer and the next in cue.	Used the body to block the view of other customers	Do not install within view of cameras.	Do not install within view of cameras.

	block cashiers view.		and the device.		
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. AF820 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 software, the developer must respect the guidance described in the document [8] and document [9] to compliant with PCI security requirement. Please refer to document [8] when developing SRED function and document [9] when developing Open Protocol function.

The following steps must be implemented：

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

5.2 TLS

SSL protocol is known inherently weak and the device AF820 does not support SSL. AF820 only supports TLSv1.2 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 AF820 terminal must be signed with RSA-2048 bits private key which is only controlled by Shenzhou Anfu Technology 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 gotten 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 using techniques such as whitelisting.
The device does not allow the disablement of SRED functionality.

5.5 Algorithms Supported

AF820 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

AF820 implements different types of key management techniques:

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

AF820 terminal key management complies with ANSI X9.24 key management rule strictly. Each key has only one purpose and unique key value. When the terminal is suffering from attacking, the keys will be erased.

Key Name	Purpose	Algorithm	Size
KBPK	Protect X9.143 key block	AES	256Bits
Master Key	Key encryption for session keys Loading	TDES	128/192Bits
		AES	128/192/256Bits
PIK	Encryption key for clear-text PIN Block	TDES	128/192Bits
		AES	128/192/256Bits
MAK	Encryption key for MAC generation	TDES	128/192Bits
		AES	128/192/256Bits
TDK	Encryption key for account data	TDES	192Bits
		AES	128/192/256Bits
IPEK	Initial DUKPT keys	TDES	128Bits
		AES	128/192/256Bits
PEK	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.

- Symmetric encrypted keys injection

AF820 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, Retail Financial Services Symmetric Key Management Part 1: Using Symmetric Techniques
[2] ANSI X9.24 Part2, Retail Financial Services Symmetric Key Management Part 2: Using Asymmetric Techniques for the Distribution of Symmetric Keys
[3] ANS X9.24 Part 3, Retail Financial Services Symmetric Key Management Part 3: Derived Unique Key Per Transaction
[4]ANSI X9.143, Retail Financial Services Interoperable Secure Key Block Specification
[5] ISO 9564-1, 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, v6.2-January 2023
[7] User Manual
[8] Security Application Development Guidance
[9] Open Protocol Implementation Guidance