SP580 Security Policy
Version: 1.03

Document Modification

Version	Author	Date	Description
V1.00	lianjiazhi	20221010	Initial version
V1.01	Liushihua	20221104	1. Add reference documents, and tamper pictures. 2. Add the terminal authentication type, description, terminal usage scenario, and PCI authentication version. 3. Correct some grammar and spelling errors. 4. Modify the KEY Table in “4.6 Key Management”.
V1.02	lianjiazhi	20230301	Modify contents according to PCI v6.1
V1.03	lianjiazhi	20230817	Update the pictures to actual pictures in Section 2.1. Eliminate the errors in Section 2.3.

Content

1. Purpose

This document involves the secure use of the SP580, including information about key-management responsibilities, administrative responsibilities, functionality, identification, and environmental requirements.

The device is approved as a hand-held PED product under PCI PTS v6.1 requirements.

The PCI PTS POI version for the device assessment is v6.1. And any deviation from the approved usage of the device will result in invalid approval of PCI PTS POI.

2. General Description

2.1 Product Introduction

Product Name: SP580
Appearance:

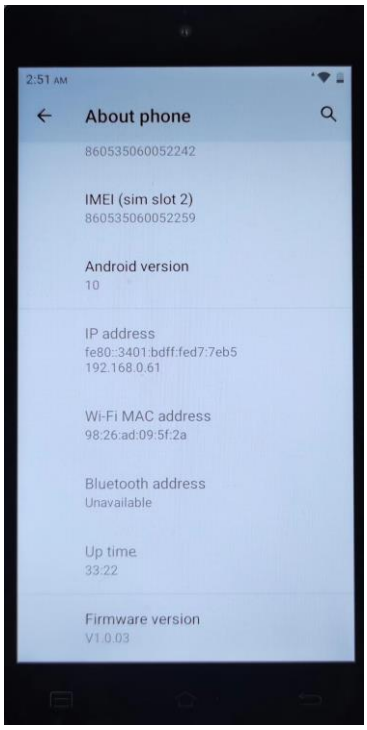
2.2 Product Type

The SP580 has been approved by PCI as a smart PED POS and does not provide a privacy shield. The device is a smart POS terminal for financial transactions. It is hand-held and used in an attended environment. It has LCD, Touchscreen, Security Magnetic Reader, IC Card Reader, Contactless Card Reader, Printer, SD card slot, SAM card slot, SIM card slot, Camera, Speaker, Power button, USB port, WIFI, Bluetooth and Cellular (2G/3G/4G).
The device uses a touch panel for PIN entry.

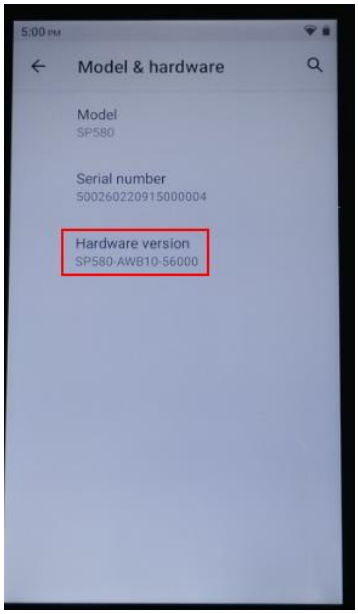
2.3 Identification

The SP580 is a smart POS device. To identify the device, please check the equipment according to the following steps:

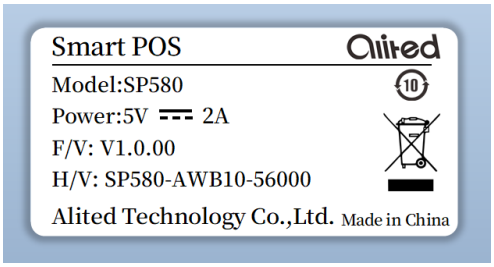
1. Check the software and hardware version of the device, as shown in the picture below: The software version can be checked after powering on the device, click "About phone" to view the firmware version number (Firmware version).



2. On the “About phone” screen, tap “Model & hardware” to view the terminal model and hardware version.



3. The SP580 has been approved by PCI as a PED, and it is used as a handheld device or equipment accessory. Below is the sample for the label on the back side of the device.



Hardware Version

The hardware version format is
SP580-x0010-x6xxx,
SP580-xW010-x6xxx,
SP580-x0B10-x6xxx and
SP580-xWB10-x6xxx, which is showing in the figure below.

S	P	5	8	0	-	x	0/W	0/B	1	0	-	x	6	x	x	x
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17

The explanation of each digit is below:
7th, 8th and 9th digits are used for different communication: 4G, Wi-Fi and Bluetooth.
13th digit is used for 4G module version, Asia/EMEA/North America, Memory Size.
15th, 16th and 17th digits are used for customization, casing color and silkscreen.

Firmware version

The firmware version format is V1.x.xx, shown in the figure below

V	1	.	x	.	x	x
1	2	3	4	5	6	7

The explanation of each digit is below:
4: The major version number for non-security-related software changes
6: The minor version number for non-security-related software changes
7: The revision number for non-security-related software changes

2.4 Device Functions

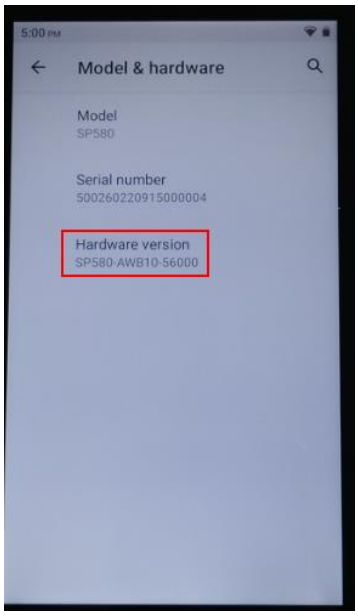
SP580 is a smart POS terminal, and it is designed as a secure PED terminal and provides a more convenient, versatile secure payment.

3. Installation and User Guidance

3.1 Initial Inspection

1. Check the packing and make sure all of them are intact. If one of them was broken or damaged, refuse to accept and sign, and inform the express company to be responsible for the loss.
2. You can look out for the tampered information on the LCD to check if the device is tampered. If tampered with, please contact the authorized service or vendor.
3. Check the tamper-evident label of each package with the device to make sure the label is not ripped off or broken. If one of them was broken or damaged, open the package to check whether the device exists. Then refuse to accept or sign, inform the express company to be responsible for the loss, and ask the vendor if there is any product that has been opened and lost.
4. After making sure the package of the product is well, sign the acceptance receipt. The responsibilities for the product will be transferred to the merchant.
5. Open the box of the device, and check the integrity of the device:
   ① Check the tamper-evident label is not ripped off or broken.
   ② Check the outward appearance is the same as the picture below:

   ③ Check the device including the model and logo is intact.



④ Check the hardware version is labeled on the backside of the device, and the software version is shown after powering on the device.

⑤ Check the accessories are complete, such as the adapter, data line, operation manual including precautions & security use and so on.

⑥ Check the screen if there are any suspicious coverings.

3.2 Installation

Document [2] includes how to install the equipment. Equipment needs to be used in a good environment. Check to confirm the temperature, humidity, clean lines and the power supply are in the reasonable range. Check there are no other sources of interference around the device, like a strong magnetic field and so on. Make sure the device works in a good environment.

3.3 Environmental Conditions

The ranges of operating temperature, voltage and humidity of the SP580 are shown as below.

Environment Factor	Minimum Value	Nominal Value	Maximum Value
Voltage		5V	
Working Temperature	-10°C		50°C
Storage Temperature	-20°C		80°C
Working Humidity	20%		90%

Storage Humidity	5%		95%

3.4 Communications and Security Protocols

The communication interfaces and protocols used by the device are shown in the tab:

Interface	**Protocols**
Cellular (2G/3G/4G)	PPP, TCP, UDP, IP, DHCP, ICMP, TLS v1.2
WIFI	ARP, TCP, UDP, IP, DHCP, ICMP, TLS v1.2
Bluetooth	Bluetooth 4.2 (Bluetooth BR/EDR Mode 4 Level 4 and BLE Mode 1 Level 4)
USB	The device has a Type-C USB port which supports USB OTG.

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

3.5 Configuration Settings

Step 1.
Enter the sensitive service for the first time: Passwords of “Key download manager” must be modified after powering on for the first time.
Log in with the default password first, and then the administrator must re-set a valid password to replace the default password so that the device can be used continuously. Two manager’ passwords are needed to input correctly, then the device can be run into key-loading status when the device runs for the first time. The device gets to login attempts at entering the correct password, if this value is reached, the device will be locked.
Note:
The default passwords of “key download manager A and B” are “00000000”.
Besides, the new passwords cannot be the same to the default passwords and to each other. After two “key download manager” logging in, the device can download the transport key (KBPK) from the secure network. The transaction keys must be downloaded into the device when the device runs for the first time. The TMK can only be downloaded after the KBPK is downloaded.

Step 2.
When it does not run for the first time, the device goes to the normal state. In normal state, the functions include transactions and entering system menu. The system menu contains the functions of loading the transaction keys, changing the password, and checking the version.

Step 3.
After the device was shipped out, and has not yet been installed in the merchant, the device should be sent to the acquirer to do the key initialization and replace the

authentication and transport keys which were loaded by the vendor before shipment. The loading of keys must be done under dual key download manager control. Only inputting two key download manager passwords correctly, can enter the status of downloading keys.

There is a time limit of 15 minutes for the whole key-loading process. If the key-loading is not finished in 15 minutes, the device will return to the normal status. And if wrongly input the passwords over five times, the device will be locked and provide no service. After finishing the key initialization, the device will be installed in merchant to be used.

Step 4.
The detailed step of downloading keys is as follows:
When downloading the clear-text keys to SP580 device, two key download manager passwords should be input firstly, and then download the keys into the device.

4. Operation and Maintenance

4.1 Periodic Inspection

The device must be inspected every day as follows:
1. Environment checking
Check the temperature, humidity, cleanliness and power supply are in a reasonable range. Check there are no other sources of interference around the device, like a strong magnetic field and so on. Make sure the device works in a good environment.

2. Device checking
Check the hardware, serial cable and the body of the device especially the IC card slot whether there has any illegal matter. Make sure the case and whole device are intact. Please refer to the figure below for normal ICC slot state.

3. Overlay detection
Check the screen for any suspicious coverings.

4.2 Self-Test

The device must perform a self-test at startup, and then perform at least once every 12 hours.

The self-test includes:
- Check the integrity and authenticity of the firmware
- Check the integrity and authenticity of the application
- Check the integrity and authenticity of the key

The device 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 fails in a secure manner. When the device goes to the "Lock" mode, all the stored keys are removed as well. The merchant must return the device to a vendor for the repair. Self-test is not initiated by an operator. Every time the device powers up or reboots every 12 hours, the memory will be re-initialized.

If any of the above checks fails, the device will be disabled in a secure manner. In this case, please contact the supplier center.

4.3 Patching and Updating

Patching and Updating Update and/or patch to the firmware, software and configuration parameters can be installed into the device. And both local and remote updates and/or patch downloading are supported. Any security-related update and/or patch loaded into ALITED terminals must be signed using an RSA certificate.

If the signature of the update and/or patch cannot be authenticated, the update and/or patch will be rejected and not be installed. For the secure operation of the device, it is recommended to use the latest versions of the released firmware and software.

4.4 Roles and Responsibilities

The customers of the vendor are acquirers. The vendor sells devices to the acquirer and provides maintenance and technique support. Acquirer sells devices to the end-users and services to the end-users. Vendor, acquirer and end-users play different roles in operating the device as shown below:

	Role	Operations
Acquirer	Administrator	Access to devices sensitive services
End User	Operator	Performs payment transactions
Vendor	Maintainer	Repairs the device and handles devices with tamper events

4.5 Passwords and Certificates

The administrator's passwords must be modified after powering on the device for the first time. Log in with the default password first, and then the administrator must re-set a valid password to replace the default password so that the device can be used continuously. Two administrators' passwords are needed to input correctly, then the device can be run into key-loading status when the device runs for the first time. The administrator gets five login attempts at entering the correct password, if this value is reached, the device will be locked, and can't run in ten seconds.
The devices do not need any change of certificate.

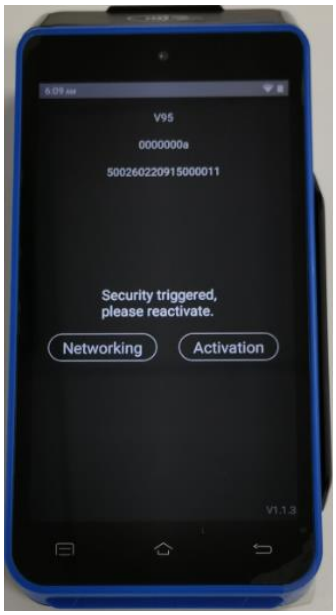
4.6 Tamper Response

Tamper Trigger Events

- Front case removal.
- Back case removal.
- Physical penetration on all sides of the device.
- Temperature is >115℃ or <-45℃.
- Button cell voltage is >4.2V or <2.1V.
- Stored sensitive data authentication failed during the Self-test.

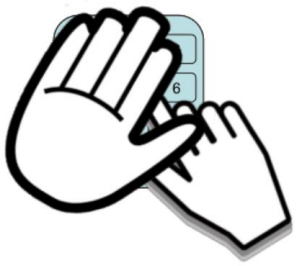
In the tamper event, the device will turn into the locked status and display a warning message. No other signal is used to indicate that the terminal has tampered. There will be no further transaction function performed on the device.

If the device is in tampered status, the user must contact the device maintenance or authorized center immediately, remove it from service and keep it away from the potential illegal investigation.



4.7 PIN Entry

The device is a hand-held device, and it does not provide a physical Privacy Shield additional, but it is required to provide cardholders with the necessary privacy during PIN entry. The device will prompt some messages to remind the cardholder to block the view of the keyboard with the body or free hands.
For example:



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

Method	Observation Corridors				
	Cashier	Customer in Queue	Customer Elsewhere	On-Site Cameras	Remote Cameras
With stand	No Action Needed	No Action Needed	No Action Needed	Out of sight of the cameras	Out of sight of the cameras
Without stand	Block the view of cashier by body	Block the view of other customers by body	Block the view of other customers by body	Out of sight of the cameras	Out of sight of the cameras
Customer Instruction	Remind the customer to shield PIN	Keep a distance	Keep a distance	Out of sight of the cameras	Out of sight of the cameras

4.8 Firmware Update

Customers can download the latest firmware by OTA. Then, the service will detect the remote server if there is a new firmware version under good network condition. Additionally, we use the TLSv1.2 protocol to transmit data when it updates. During the TLS handshake process, POS terminal will authenticate the server and the server will authenticate the device's client. After the mutual authentication is approved, a secure channel will be established to ensure the security of the data in the downloading process. When the download is complete, the integrity of the downloaded firmware will be checked by RSA2048-SHA256. After the firmware is downloaded, old firmware in the terminal will immediately verify whether the signature is legal. Any non-signed firmware will be considered unauthorized, and cannot be updated. Terminal type information is already contained in firmware, and firmware will also choose whether it could work in the existing terminal. If the terminal type is not compatible, the firmware will not be updated. When firmware update is completed, restart the device again, and a new firmware version will be shown.

Note:
Only the firmware codes that have been authorized for release should be signed.

Firmware update uses SHA-256 in combination with RSA 2048 bits for authentication and signature verification. The signature and verification mechanism ensures the authenticity and integrity of the firmware that is loaded into the device.

4.9 Decommissioning

Permanent removal

When the device is no longer used, it can be decommissioned and removed from service. And all the key material used to encrypt any sensitive data must be erased by rendering the device to tamper.

Temporary removal

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

Decommissioning

To decommission the device permanently, the merchants or users should disassemble the device to make it tampered with and erase all payment keys. Then merchants or users should return the device to the acquirer or vendor.

5. Security

5.1 Software Development Guidance

During the software development, the following steps must be implemented:

1. Software development/programming according to the requirement;
2. After the software development, developer must take a functional test (self-test);
3. Code review, audit, and digital signature;
4. Undergo a full testing (detailed test);
5. If some bugs are found, the tester will feed back to the relevant developer to fix up;
6. The software can be released to production when passing the test.

5.2 TLS Security Protocol

OP applications development

For OP application development please refer to document [4] and the compliance with PCI PTS, the following points need to take attention.

1. The client must authenticate the CA certificate and client certificate.

2. The cipher suite of the server to which terminal connects should be as secure as TLS_RSA_WITH_AES_128_GCM_SHA256 or more secure.

3. The server to which terminal connects should be configured to require Client Authenticate.

4. Use TLS v1.2 or higher.

5. Application developers must use SHA-256 on top of the security protocol when it is being used for security functionality. Application developer can get the security guidance from vendor.

SSL/TLS

The BoringSSL is customized by the vendor and all weak cipher suites are removed from the device. The device only supports the cipher suites as PCI PTS required. The device supports TLS v1.2. TLS v1.0 and TLS v1.1 are inherently weak and they are not recommended.

The device does not support SSL.

5.3 Signing

The manufacturer supports RSA2048-SHA256 for application authentication. Application can be updated and downloaded into the device in a cryptographically authenticated way.
1. Developers use a trusted development environment to generate public and private key pairs;
2. Generate a certificate request file and send it to the vendor over a secure network;
3. The manufacturer shall review the applicant according to the approval process, and only after the approval can the developer be granted a certificate;
4. The manufacturer uploads the certificate to the certificate management system;
5. The developer downloads the certificate to the terminal and restarts it;

When downloading the application, the device will authenticate the signature of the application, only after authenticate successfully the application can be installed.
For firmware, the firmware is signed and verified by RSA2048/RSA4096 and SHA256 algorithm. The unsigned or incorrectly signed firmware will be rejected by the device.

5.4 Account Data Protection

Below are SRED functions implemented by the device. Please refer to document [4] when developing SRED functions.

- The account data should be encrypted by the TDK (TDES 192 bits, AES 192 bits) or DUKPT_FUTURE_KEY (TDES 128/192 bits, AES 128/192 bits).
- The device doesn't support the pass-through of clear-text account data using techniques such as whitelisting.
- The device doesn't support the disablement (turning off) of SRED functionality.

5.5 Algorithm Supported

SP580 supports the following cryptographic algorithms:
- TDES (128bits, 192bits)
- AES (128bits, 192bits)
- SHA-256
- RSA (signature verification, mutual authentication, 2048/4096 bits)
- ECC (P-224, P-256, P-384, P-521)

5.6 Key Management

The device supports the following key management methods:

Master/Session Key

This method uses a hierarchy of master key (TMK) and session keys (PIK, MAK and TDK). The session keys are distributed under the protection of TMK. These keys can be replaced by the same methods whenever compromise is known or suspected.

DUKPT

This method uses a unique key for each transaction and prevents the disclosure of any past keys used by the transaction-originating device.

The use of the POI with unapproved key management systems will result in incompliance with PCI PTS POI security requirements.

KEY Table:

Key Name	Purpose/Usage	Algorithm	Size (bit)	Generated by	Form Factor Loaded to Device In
KEK	The encryption and protection of all terminal keys, it is the basis of the whole terminal security.	AES	192	Vendor	Randomly generated by SP.
KBPK	The key used to encrypt TMK and IPEK during network transmission.	AES	192	Vendor	Randomly generated by KMS and downloaded to the device under dual control in the safe room.
TMK	Encryption working key (PIK, MAK, TDK) for transmission to the device. The device supports multi-group TMK, and the index of TMK is 0-9.	TDES/AES	128/192	Acquiring	Loaded into the device after encrypted by KBPK, and then stored through KEK encryption.
MAK	Message Authentication. The device supports multi-group MAK and the index of MAK is 0-9.	TDES/AES	128/192	Acquiring	Loaded into the device after encrypted by TMK.
TDK	Account data encryption. The device supports multi-group TDK, and the index of TDK is 0-9.	TDES/AES	192	Acquiring	Loaded into the device after encrypted by TMK.
PIK	Encryption of online PIN. The device supports multi-group PIK, and the index of PIK is 0-9.	TDES/AES	128/192	Acquiring	Loaded into the device after encrypted by TMK.
IPEK	Used to derive DUKPT_FUTURE_KEY.	TDES/AES	128/192	Acquiring	Loaded into the device after encrypted by KBPK, and then stored through KEK encryption.

DUKPT_FUTURE_KEY	Used to encrypt PIN, Identification of messages and encrypt account data after DUKPT divergence.	TDES/AES	128/192	Device	Generated dynamically during the transaction.
AUTH_SP_BOOT_KEY	SP Security startup firmware boot signature authentication.	RSA	2048	Vendor	The public key of Vendor.
AUTH_SP_APP_KEY	SP boot Checks the SP framework.	RSA	2048	Vendor	The public key of Vendor.

5.7 Key Loading

The key-loading techniques supported by the device fall into the following two categories.

- Injecting clear-text secret or private keys from a key loader,
- Symmetric encrypted keys injection

Dual control:

The key loading process is strictly authorized and controlled by at least two persons. Identification and authentication are performed first to make sure they are the right operator for the key loading.

7-12 bytes of password are used in the key loader to authenticate the operator.

5.8 Key Replacement

There are symmetric master keys used in the device, for some security reasons, like the crack technique is improved day by day. Once the keys are cracked by the hacker, the device is not secure anymore. So, the keys saved in the device must have a life cycle, usually a year for symmetric master keys. Another case: 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, the key must be replaced with a new key immediately.

To replace the key through external selection, the key index and key type must be specified, and only the key with the same index can be replaced.

6. Acronyms

Abbreviation	Description
PCI	Payment Card Industry
PTS	PIN Transaction Security
PIN	Personal Identification Number
DES	Data Encryption Standard
TDES	Triple Data Encryption Standard
KMS	Key Management System

7. References

[1] PCI_PTS_POI__DTRs_v6-1_Final.pdf

[2] SP580 operating instructions.docx

[3] SP580 SDK Documentation.docx

[4] Application Development Guidance.docx