Urovo Technology Corporation Limited

i9000S

PCI PTS POI Security Policy

2019.07.11

V1.3

Revision declaration

Version	Author	Date	ChangeLog
V1.0	WX.Cheung	2019.04.17	Document Created
V1.1	WX.Cheung	2019.05.24	Add Tamper Condition
V1.2	WX.Cheung	2019.07.08	Update the description of Security chapter
V1.3	WX.Cheung	2019.07.11	Add the description of USB interface

Contents

1 Purpose......4
2 General description......4
2.1 Product Name and Appearance......4
2.2 Product Type......5
2.3 Identification......6
3 Installation and User Guidance......6
3.1 Initial Inspection......6
3.2 Installation......6
3.3 Environmental Conditions......6
3.4 Communications and Security Protocols......7
3.5 Configuration Settings......7
3.6 Unattended Installation......7
3.7 Handheld devices......7
4 Operation and Maintenance......8
4.1 Periodic Inspection......8
4.2 Self-Test......8
4.3 Roles and Responsibilities......8
4.4 Passwords and Certificates......9
4.5 Tamper Response......9
4.6 Privacy Shield......10
4.7 Patching and Updating......11
4.8 Decommissioning......11
4.9 Removal Detection......12
5 Security......12
5.1 Software Development Guidance......12
5.2 SSL......13
5.3 Signing......13
5.4 Account Data Protection......13
5.5 Algorithms Supported......13
5.6 Key Management......14
5.7 Key Loading......14
5.8 Key Replacement......15
6 Acronyms......15
7 References......15

1 Purpose

This document describes the security policy for developers and users to ensure the proper use of devices in a secure manner including information about key-management, FW & SW security features, device functionality, environmental requires.

The device compliance with PCI PTS POI v5.1. The use of the device in an unapproved method, which is not described on the security policy, will violate the PCI PTS approval of the device.
The device is intended to be used as a handheld POS in an attended environment and it can’t be used in an unattended environment.

2 General description

2.1 Product Name and Appearance

To identify the i9000S device, validate the appearance as follow:

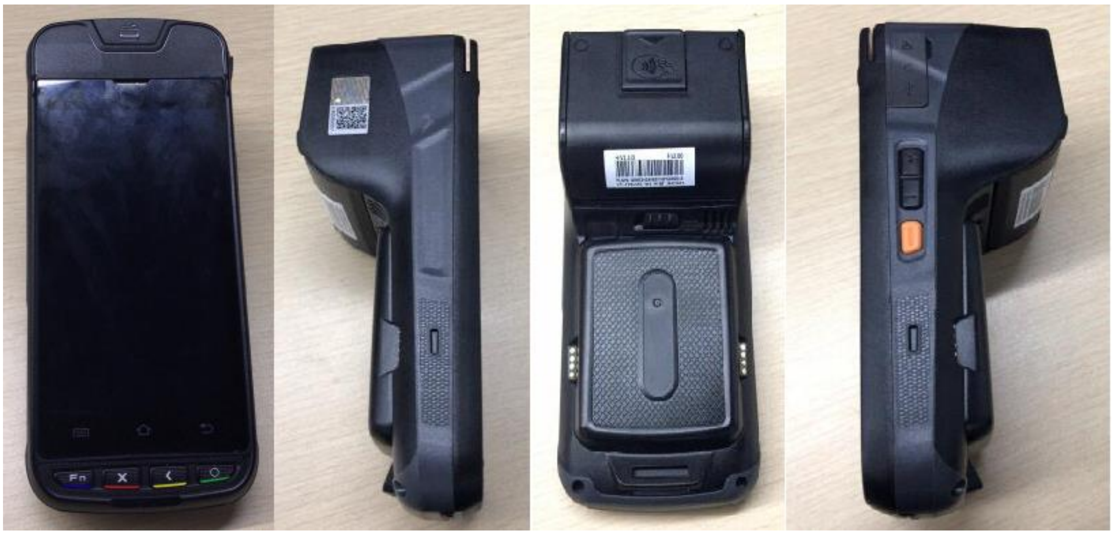
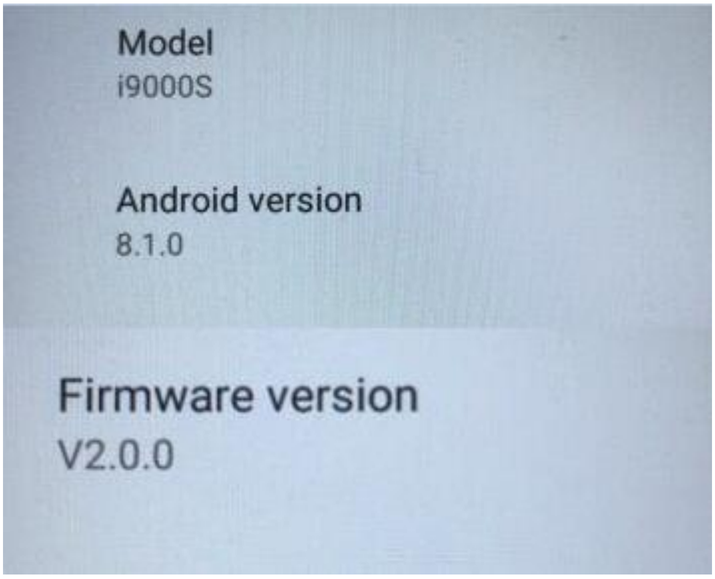


Figure 1 Product Appearance

The device model name is i9000S, which can be found on settings application in system like the picture below:



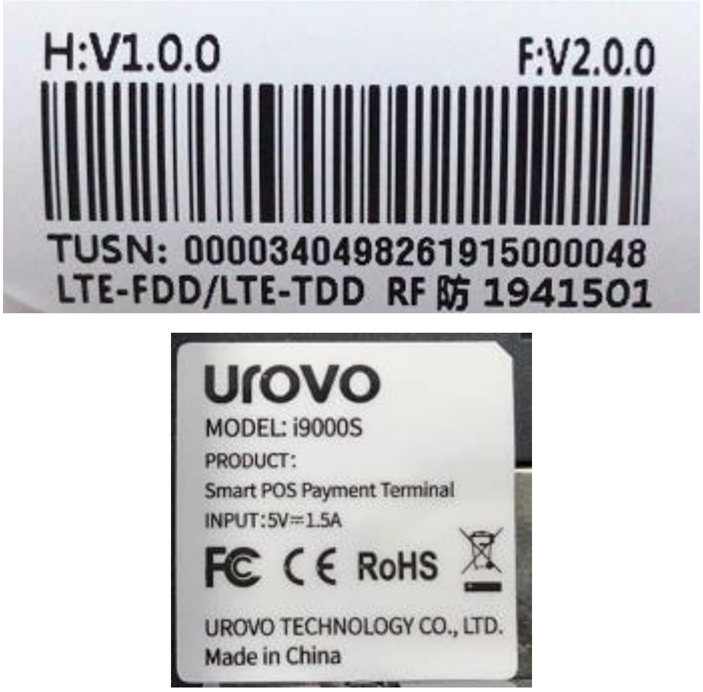
Model
i9000S

Android version
8.1.0

Firmware version
V2.0.0

Figure 2 Version Information

Hardware version printed in the label attached to the rear casing like the picture below:



H:V1.0.0 F:V2.0.0
TUSN: 0000340498261915000048
LTE-FDD/LTE-TDD RF防1941501

urovo
MODEL: i9000S
PRODUCT:
Smart POS Payment Terminal
INPUT:5V⎓1.5A
FC CE RoHS
UROVO TECHNOLOGY CO., LTD.
Made in China

Figure 3 Product Label

2.2 Product Type

The device is a stand-alone handheld POS terminal for financial transactions. The device is forbidden to use in an insecure environment, otherwise it will violate the PCI PTS approval of the device.

The device provides touch screen keypad, LCD, IC card reader(ICCR), magnetic card reader(MSR), contactless card reader(CTLS), thermal printer, USB and the wireless communication(such as 2G/3G/4G, Wi-Fi, Bluetooth). And it can deal with diversified financial transactions.

2.3 Identification

The hardware version is printed on a label at the back of the device, as shown in Figure 3.
The software version can be checked after power on and located on “Setting” -> “About Device” -> “Firmware Version” and the version information will be as shown in Figure 2.

3 Installation and User Guidance

3.1 Initial Inspection

The following inspection should be performed when the devices are received via shipping.

Inspect whether the devices delivery source information matches to one of the trust site from vendor.
Inspect whether the quantity matches to the delivery information.
Inspect whether the devices information (product name, serial number etc.) matches to the delivery information.
Inspect whether any signs of tamper on the cartons, boxes, and/or the devices.
If anything found abnormally during inspection, please contact the vendor or authorized center immediately.

3.2 Installation

The device is designed to be portable and does not need any installation.
The device should stay away from all source of heat, to prevent from vibration, dust, moisture and electromagnetic radiation (including computer screen, motor, security facilities etc.).

3.3 Environmental Conditions

The environmental conditions to operate the device are as follows.

Working Environment	Temperature: 0℃～50℃(32℉～120℉)
	R.H.: 10%～90%(non-condense)

Storage Environment Temperature:－20℃～70℃(-4℉～158℉)
R.H.:5%～95% (non-condense)

The tamper conditions of device as follows:
Tamper temperature: CPU temperature lower than -30℃ or higher than 100℃.
Tamper voltage: voltage of Battery Backup Login lower than 2.0V or higher than 3.8V.

3.4 Communications and Security Protocols

	Interface	Protocols
Communication	Wi-Fi	TCP, UDP, DHCP Client, ICMP, SSL/TLS, IP Stack.
	Bluetooth	Classic Bluetooth
	Cellular	TCP, UDP, DHCP Client, PPP, SSL/TLS, IP Stack.
	USB	USB

Tabel 1 Communications and Protocols

The terminal supports TLS v1.2 security protocols for TCP/IP security communication, including Wi-Fi and Cellular, Mutual authentication is provided by TLS v1.2.
Use of any method not listed in the policy will invalidate any PCI approval of the terminal.

3.5 Configuration Settings

No security sensitive configuration settings are necessary to be tuned by the end user to meet security requirements.

3.6 Unattended Installation

The device is intended to be used as a handheld POS in the attended environment.

3.7 Handheld devices

The device is intended to be used as a handheld POS in the attended environment. The document [8] guides acquirers PIN entry device support SRED encryption.

4 Operation and Maintenance

4.1 Periodic Inspection

The user should daily check that the keypad is firmly in place. Such checks would provide warning of any unauthorized modification to the terminal, and other suspicious behavior of the terminal. The merchant or acquirer should also check that the installation/maintenance operations are performed by a trusted person.

- Inspect the appearance of device to make sure it is the right product:
- Inspect whether the IC card reader’ s slot has untoward obstructions or suspicious objects at the opening:
- Inspect whether the MSR card slot has an additional card reader and other inserted bugs:
- Inspect whether the product appearance has been changed, such as the display, keypad area and so on, to ensure that it is free of rogue overlays;
- Check if the firmware version is correct:
- Observe whether there are any visual observation corridors, and deter them by body or other shields:
- Power on the device and check if the firmware runs well. As the startup will inspect the hardware security, authenticity and integrity of firmware.

If you find these suspicious circumstances, please stop using the device immediately and contact the customer service to confirm if the device has been tampered.

4.2 Self-Test

Self-tests are performed upon startup/reset. The device will perform self-test upon startup and also every 24 hours. Periodical self-test is done by automatically reboot. This reboot period is count up once the device is powered on. Self-tests are not initiated by an operator but automatically implemented by the firmware code.

4.3 Roles and Responsibilities

Below Table shows different roles and responsibilities:

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

Table 2 Roles and Responsibilities

4.4 Passwords and Certificates

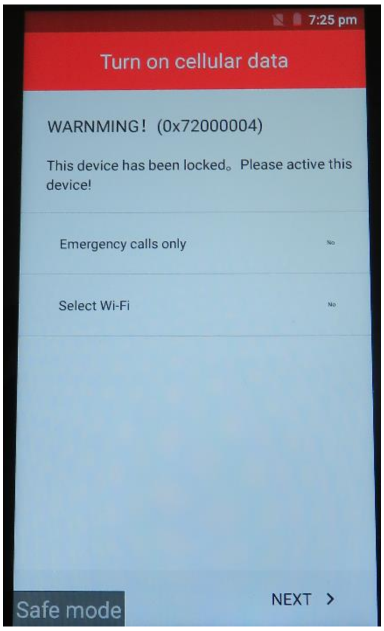
Acquirer is forced to change all passwords when receiving the device and keep passwords safely.

- Verify default password;
- Select the menu of “modify password”;
- Set new password follow tips;
- New password must different default rulers and different from default or old values.

Acquirer shall download certificates use KLD (Key Loading Device).

4.5 Tamper Response

The device contains tamper mechanisms that will trigger when a physical penetration attempt of the device is detected or the logic anomalies was occurred. The device will be locked in the event of tamper detection and the merchant or acquirer can easily detect a tampered terminal.
The device shows a dialog to notify that “The Device is Lock” like Figure 4. Operator can’t do any security function under this situation until re-activation operation of the device. If the device is in tampered state, the user must contact the device maintenance immediately, remove it from service and keep it away from potential illegal investigation.



Turn on cellular data

WARNMING！ (0x72000004)

This device has been locked。 Please active this device!

Figure 4 Tamper Prompt

4.6 Privacy Shield

The device is designed to be used on hand and the device does not contain a privacy shield. It is required to provide cardholders with the necessary privacy during PIN entry. For example, the device will demonstrate a safe PIN-entry process how to entry PIN. This message reminds cardholder that he/she can use his/her body or their free hand to block the view of keypad.

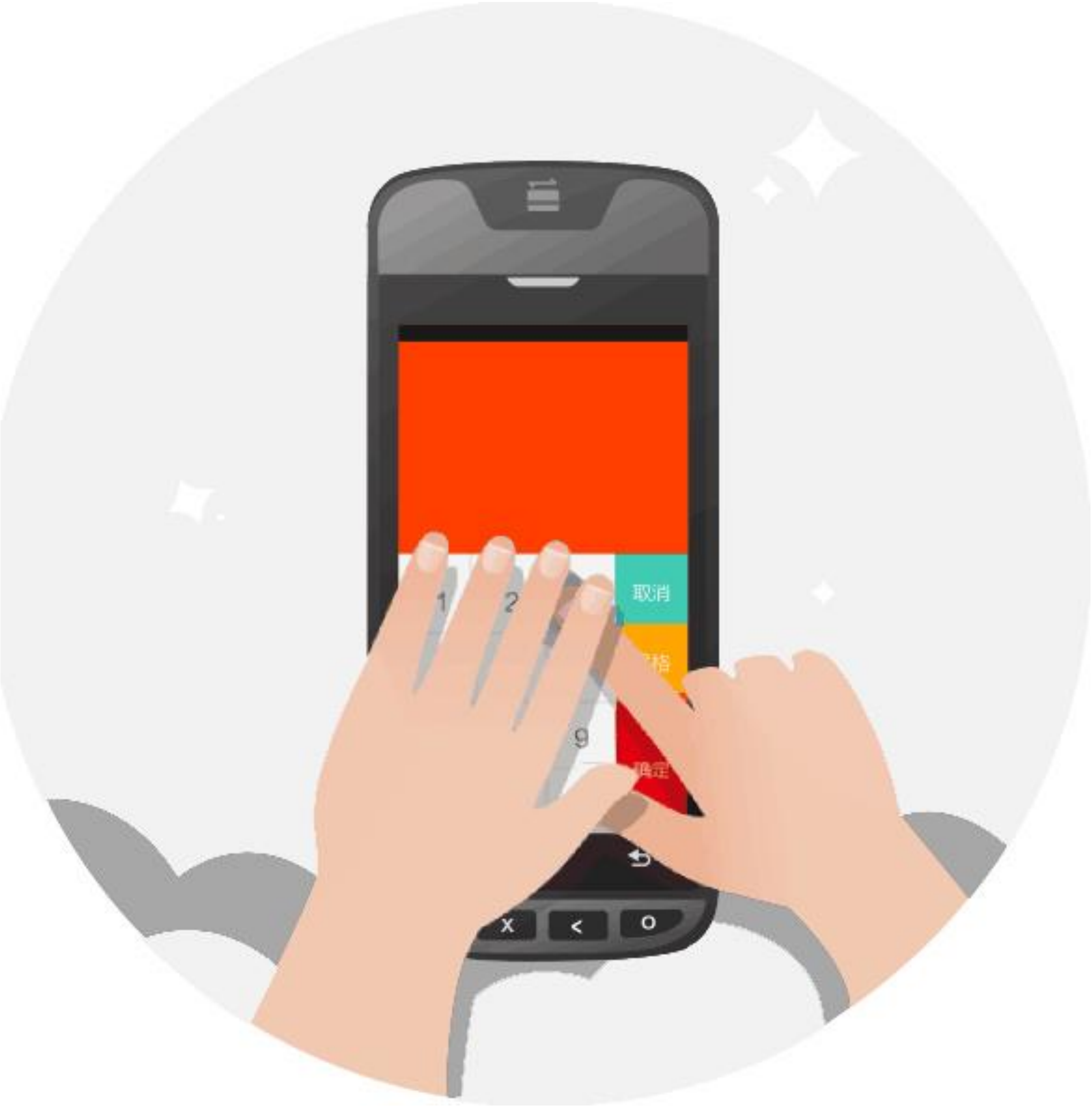


Figure 5 Safe PIN Entry Logo Example

4.7 Patching and Updating

The device supports both local and remote methods of updating or patching the SW. Updates and patches can be loaded into the device just only they are authenticated successfully. If the authenticity is not confirmed, the updates or patches will be rejected.
For the updating procedures, please refer to document [7].

4.8 Decommissioning

When the device is no longer used for permanent decommissioning reason, the administrator of the device needs to gather the device and then erase all the key materials on it. It can be done by directly opening the casing

of the device to make it tampered.
For the temporary removal, there is no need to change the state of the device, as all the keys are still protected safely by the battery power supply.

4.9 Removal Detection

The device does not support this feature.

5 Security

5.1 Software Development Guidance

When developing applications, the developer must respect the security guidance described in the document [8], document [10] and document [11]. During the software development, the following steps must be implemented:

1. Code Review.
2. Security review and audit
3. Module test
4. Source code management and version control
5. Software test
6. Release policy

For use of open protocol, the developer must respect the SSL security guidance, Bluetooth Security Guide and Wi-Fi Security Guide that described in the document [8] and document [11]. The device supports SSLv2, SSLv3, TLSv1.0, TLSv1.1 and TLSv1.2 of SSL/TLS security protocols. It is important to note that SSLv2, SSLv3, TLSv1.0 and TLSv1.1 are inherently weak and should be removed, but considering these versions still exist in the world, in order to be compatible, we temporarily keep them for being used in non-financial applications.

In addition, we strongly recommend a server should disable SSL protocol, and select TLSv1.2 or higher version. To make it more secure, mutual authentication is recommended. The device does not support Bluetooth Low Energy and does not support “Just Works” pairing option. The device supports security mode 4. Any insecure communication options are not allowed.

For the SRED, account data can be protected by TDK/MACK. The firmware of the device does not support the pass-through of clear-text account data using techniques such as whitelisting. For more details please refer to document [8], document [10] and document [11].

5.2 SSL

The device selects TLSv1.2 or higher version, and it only supports the cipher suites as PCI PTS required.

5.3 Signing

Application is authenticated before being to install and run. The device rejects the illegal application to install and run which was authenticated failed. The details about digital signature algorithms are as follows:

- SHA256 is used to compute the digest of firmware.
- RSA 2048bits key is used for signature verification.

Application/Firmware code has been reviewed by two or more experts and have been tested strictly before release to avoid hidden functions and vulnerabilities then addition the firmware signature while released.
That is, the firmware was signed by the vendor, and the application was signed by acquirer. They all use 2048 bits RSA private keys, with the SHA 256 as digest computing algorithm. And vendor’ s RSA private keys for signature are under the control of the vendor and the private key of acquire are controlled by acquirer.

5.4 Account Data Protection

The device does not support whitelisting functions, and not allow clear-text account data output the device; also it always provides SRED functionality and does not support the disablement (turning off) of SRED functionality. The account data is protected by TDK (TDES 192bits in Table 3.

5.5 Algorithms Supported

The device includes the following algorithms:

- Triple DES (128bits/192bits)
- RSA (Signature verification, 2048 bits)
- SHA256
- AES (128bits)

5.6 Key Management

The device support various type of key management techniques:

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

Using of the terminal with a key-management system other than these three ones above will invalidate any PCI approval of the terminal.

The Keys are specified as follow:

Key Name	Purpose/Usage	Algorithm	Sizes(bits)
TMK	Terminal master key which are used to encrypt/decrypt PINK,MACK,TDK	TDES	128/192
PINK	Pin encryption key.	TDES	128/192
MACK	Mac calculation key	TDES	128/192
TDK	Account data encryption key	TDES	192
FIXK	Fixed PIN encryption key	TDES	192
IPEK	DUKPT initial key used to generate the DUKPT future keys.	TDES	128
DUKPT PEKs	Used to calculate PIN encryption key	TDES	128
AESK	Used for encryption PIN block with Format4	AES	128

5.7 Key Loading

The initial keys mainly include listed below:

- TMK
- Fixed Key
- Initial DUKPT Key

It is recommended to load the initial keys as following ways:

The initial keys are loaded to the device under dual control and knowledge split by KLD in a secure environment.

5.8 Key Replacement

Whenever compromise of the key is suspected or known and whenever the time deemed feasible to determine the key by exhaustive attack elapses, the key must be removed or replaced with a new key. If the device is compromised, all keys will be erased, please send the device to authorized center for technique analysis and reloading new keys.

6 Acronyms

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

7 References

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

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

[3] X9 TR-31 2010, Interoperable Secure Key Exchange Key Block Specification for Symmetric Algorithms

[4] ISO 9564-1, Financial services-Personal Identification Number (PIN) management and security - Part 1: Basic principles and requirements for PINs in card‐based systems

[5] ISO 9564-2, Banking-Personal Identification Number management and security Part 2: Approved Algorithms for PIN encryption.

[6] PCI_PTS_PO__DTRs_v5-1.pdf

[7] i9000S Logical solution.doc

[8] Secure software development guide.doc

[9] Urovo_SmartPOS_Digital_Signature_System.doc

[10] Urovo Smart POS API.pdf

[11] OP secure software development guide.doc