Urovo 优博讯®

领 跑 行 业 移 动 应 用

i9100_Security _Policy_01_20

V1.2

2017.10.09

Revision declaration

Version	Author	Date	ChangeLog
V1.0	WX.Cheung	2017.06.25	Document Created
V1.1	WX.Cheung	2017.08.03	Add AES description,SSL /TLS version and usage,OP usage.
V1.2	Max.luo	2017.10.09	Add MMK description

Reference

[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 encipherment
[6] PCI_PTS_POI_DTRs_v5_Sept_2016.pdf
[7] i9100 Logical solution.doc
[8] Secure software development guide[v1.0].doc
[9] Urovo_SmartPOS_Digital_Signature_System.doc
[10] Urovo Smart POS API v1.1.0.pdf
[11] OP secure software development guide[v1.3].doc

Table Of Contents

1. Introduction..5
2. General description..5
2.1 Functionality..5
2.2 Product Identification..6
2.2.1 Appearance..6
2.2.2 Version information..6
2.3 Communication Interfaces and Protocols..7
3 Guidance..7
3.1 Installation and Environment..7
3.3 Decommissioning/Removal..7
3.4 PIN Entry Confidentiality..7
3.5 Period Inspection..8
4 Hardware Security..9
4.1 Tamper Response..9
4.2 Environment Protection..9
5 Software Security..9
5.1 Software Development Guidance..9
5.2 Software Authentication/Signing..10
5.3 Software Update..10
5.4 Self-Tests..11
6 System Administration..11
6.1 Configuration Settings..11
6.2 Default Value Update..11
7 Key Management..11
7.1 Key Management Techniques..11
7.2 Cryptographic Algorithms..11
7.3 Key Table..12
7.4 Key Loading..14
7.5 Key Replacement..15
7.6 Key Lifetime..15
8. Roles and Services..15

1. Introduction

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 use of the device in an unapproved method, as describe 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 Functionality

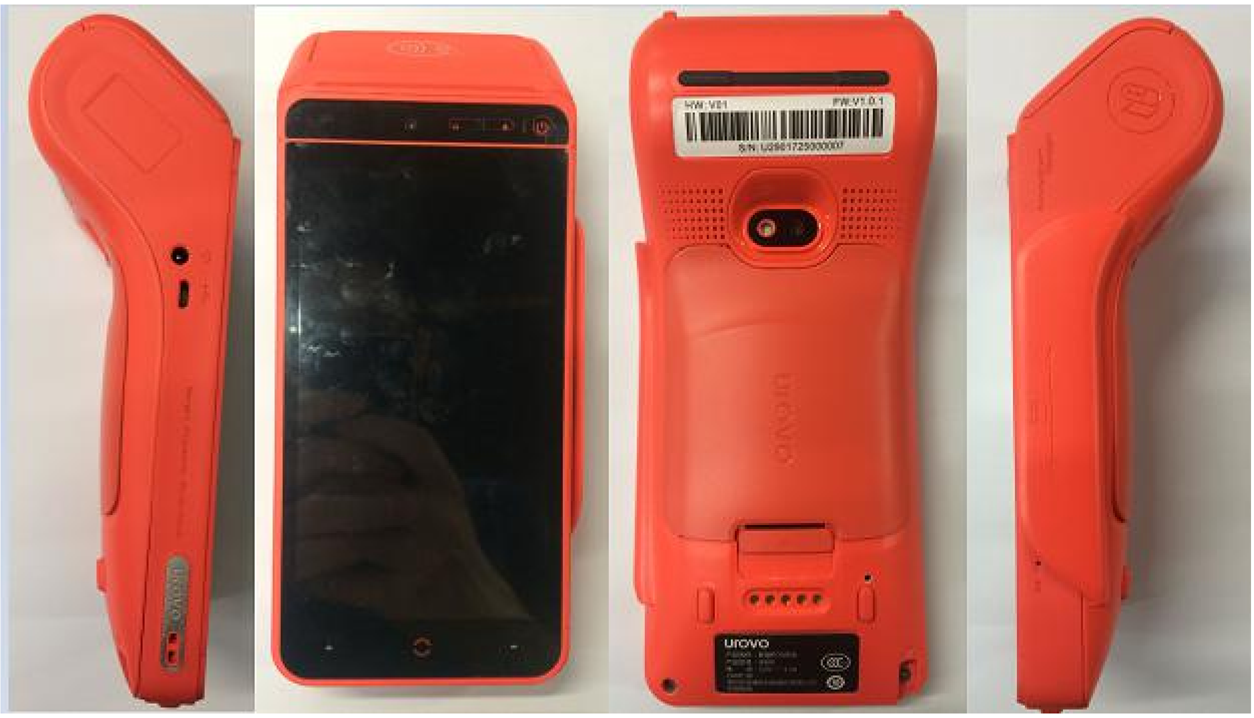
i9100 is a PIN entry device that can be used as the standard POS to undertake financial transactions, Performing the PIN entry, MAC calculation, Data Encryption/Decryption and some other functionalities provided.

The Device provides large capacity memory, large screen LCD touch operation, contactless card reader, ICCR, MSR, thermal printer, high-resolution camera, can choose various Cellular module, support multi-application management.

2.2 Product Identification

2.2.1 Appearance

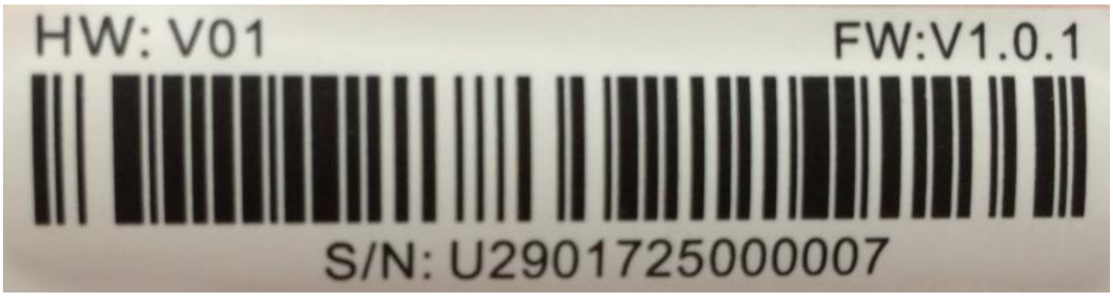
Please Check the appearance of i9100 is the same as follow that including the device information such like product name, hardware version printed in the label attached to the rear casing:



2.2.2 Version information

User should check if the firmware version consistent with the user manual.To retrieve detailed version information of i9100, please follow below operations.

1. Power up i9100,the device will stay on the main menu of firmware.
2. Press the “menu” button, Enter the correct password of Administration, and then click the “Version” item then see detail of Firmware version .
3. For the HW version which is printed in the label attached to the rear casing.



HW: V01 FW:V1.0.1

S/N: U2901725000007

2.3 Communication Interfaces and Protocols

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

The Terminal supports TLS v1.2 security protocols for TCP/IP security communication, including WIFI and Cellular, Mutual authentIcation is provided by TLS 1.2.

Use of any method not listed in the policy will invalidate any PCI approval of the terminal.

3 Guidance

3.1 Installation and Environment

Terminal should stay away from all sources of heat, to prevent vibration, dust, moisture and electromagnetic radiation (such as a computer screen, motor, security facilities etc.). The wireless terminal please pays attention away from electromagnetic radiation complex place when in use.

Be sure that terminal is used in a attended way.

The environmental conditions to operate the device are specified in the device’s specifications.

3.3 Decommissioning/Removal

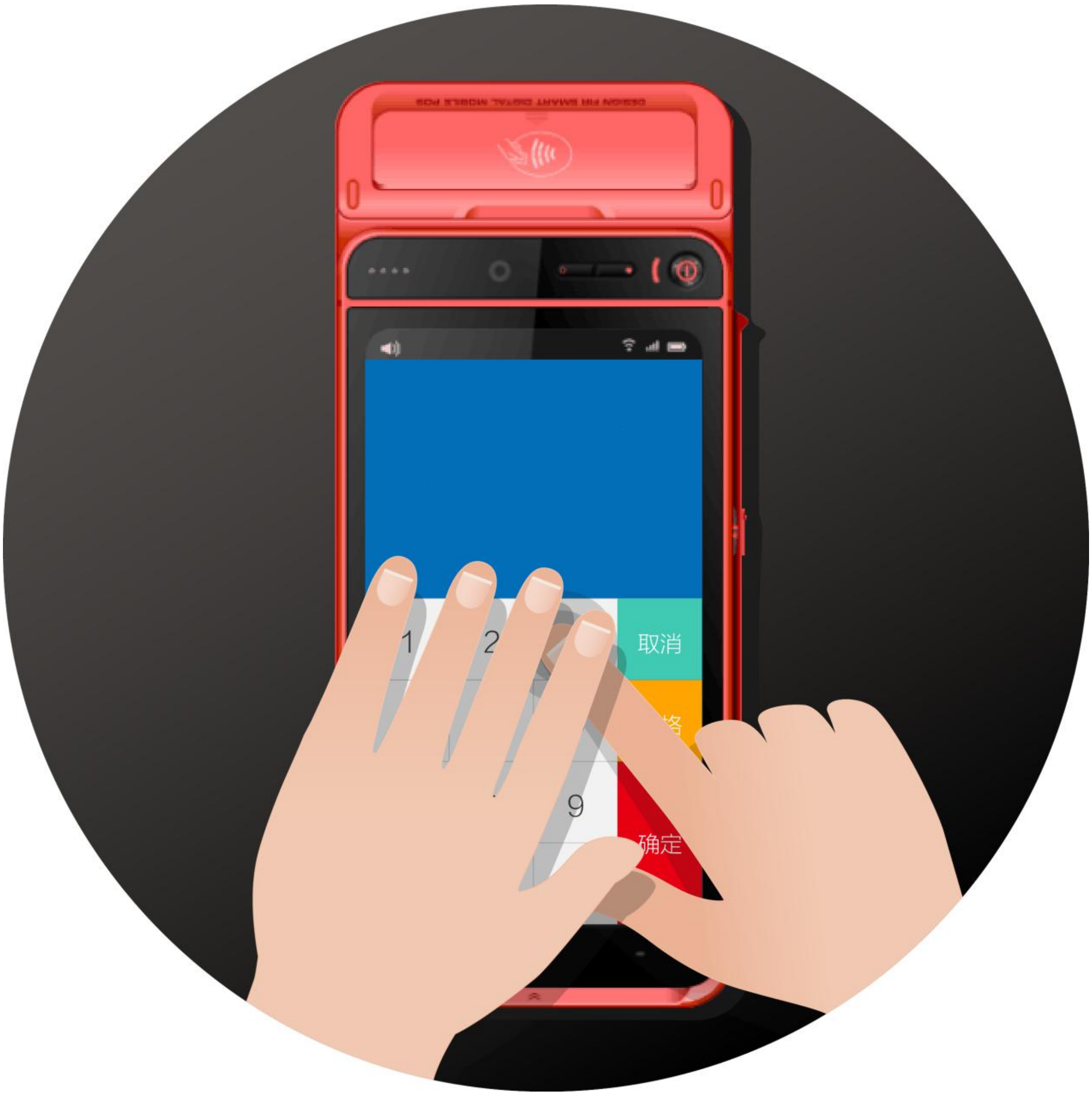
When the device is no longer used for permanent decommissioning reason, the administrator of the device needs to gather the device and then erase all the key materials on it. It can be done by directly opening the casing of the device to make it tampered.

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.

3.4 PIN Entry Confidentiality

I9100 is a Handheld devices, 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 can use his own body or their free hand to block the view of keypad.



Safe PIN Entry Logo Example

3.5 Period Inspection

The merchant or acquirer 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.

- 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 start up 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 with.

4 Hardware Security

4.1 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 lock 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”. Operator can’t do any security function under this situation until re-activation operation of the device..

4.2 Environment Protection

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)

5 Software 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] document[11]. The Device support SSLV2,SSLV3,TLSV1.0,TLSV1.1,TLSV1.2 of SSL/TLS security protocols and It is important to note that SSLV2,SSLV3,,TLS1.0,TLS1.1 are inherently weak and should be removed, but considering these version still exist in the world, in order to be compatible, we temporarily keep them for non-financial applications use.

In addition, we strongly recommend a server should disable SSL protocol, and select TLS 1.2 or higher instead. To make it more secure, mutual authentication is recommended. The device don’t support Bluetooth Low Energy and don’t support “Just Works” pairing option. The device support security mode 4. Any insecure communication options is not allowed.

For the SRED, account data can be protected by TDES/MACK.The Firmware of the device doesn’t 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 Software Authentication/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 algorithm 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 Urovo, and the application was signed by acquirer. They were both using the 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 Urovo and the private key of acquire are controlled by acquirer.

5.3 Software Update

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.

5.4 Self-Tests

Self-tests are performed upon start up/reset. The device will perform self-test upon start up 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.

6 System Administration

6.1 Configuration Settings

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

6.2 Default Value Update

There is no security default value(e.g. Admin password) that needs to be updated by the end user.

7 Key Management

7.1 Key Management Techniques

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.** a key management technique based on a unique key for each transaction as specified in [2].Use of the terminal with a key-management system other than these three ones above will invalidate any PCI approval of the terminal

7.2 Cryptographic Algorithms

The device includes the following algorithms:

- Triple DES
- RSA (Signature verification, 2048 bits)
- SHA256
- AES(Pin Block Format4, 128bits)

7.3 Key Table

Key Name	Purpose /Usage	Algorithm	Sizes(bits)	Generated by	Erasure	Save position	Number available / key slots (registers)
MMK	Protection of all keys stored in NVSRAM .	AES	128	TRNG on device.	Battery off, sensors Tamper Event	It is generated by MAX32555 boot, when first time running or a new boot downloaded (initialization of the device.). It is stored in the area of NVSRAM in the MAX32555.	One, unique to each device
PIN_MK	Master PIN key which are used to encrypt PIN Key.	TDES	128/192	Generated by acquirer in App-TRSM .	Be lost in case of MMK.	Downloaded under controlling of acquirer. It is encrypted by MMK, and stored in the internal flash of MAX32555.	150 sets per application
MAC_MK	Maste MAC keys which are used to encrypt MACK.	TDES	128/192	Generated by acquirer in App-TRSM	Be lost in case of MMK erased	Downloaded under controlling of acquirer. It is encrypted by MMK, and stored in the internal flash of MAX32555.	150 sets per application
DES_MK	Master	TDES	192	Generated	Be lost in	Downloaded	150 sets per

	Data keys which are used to encrypt DESK			by acquirer in App-TRSM	case of MMK erased	under controlling of acquirer. It is encrypted by MMK, and stored in the internal flash of MAX32555.	application
PINK	Pin encryption key.	TDES	128/192	Generated by acquirer	Be lost in case of MMK erased	Downloaded under controlling of acquirer. It is encrypted by MMK, and stored in the internal flash of MAX32555.	150 sets per application
MACK	Mac calculation key	TDES	128/192	Generated by acquirer	Be lost in case of MMK erased	Downloaded under controlling of acquirer. It is encrypted by MMK, and stored in the internal flash of MAX32555.	150 sets per application
DESK	Account data encryption key	TDES	192	Generated by acquirer	Be lost in case of MMK erased	Downloaded under controlling of acquirer. It is encrypted by MMK, and stored in the internal flash of MAX32555.	150 sets per application
FIXK	Fixed PIN encryption key	TDES	192	Generated by acquirer in App-TRSM	Be lost in case of MMK erased	Downloaded under controlling of acquirer. It is encrypted by MMK, and stored in the internal flash of MAX32555.	150 sets per application

IPEK	DUKPT initial key used to generate the DUKPT future keys.	TDES	128	Generated by KSN and IBDK in acquirer’s App-TRSM	Be lost in case of MMK erased	Downloaded under controlling of acquirer. It is encrypted by MMK, and stored in the internal flash of MAX32555.	1 sets per application
DUKPT Future Keys	Used to calculate PIN encryption key	TDES	128	Generated by DUKPT initial key in device	Be lost in case of MMK erased	Updated/Calculated from previous transaction keys and Transaction counter	One, unique to each transaction
DUKPT Pin Keys	Encryption of PIN block	TDES	128	Variant of future key	Be lost in case of MMK erased	Updated/Calculated from previous transaction keys and Transaction counter	One, unique to each transaction
AESK	Used for encryption PIN block with Format4	AES	128/192	Generated by acquirer in App-TRSM	Be lost in case of MMK erased	Downloaded under controlling of acquirer. It is encrypted by MMK, and stored in the internal flash of MAX32555.	150 sets per application

7.4 Key Loading

About key loading, we use App-TRSM to download firmware signature keys and application keys into device under dual control in secure room. The App-TRSM were placed in secure room, where only the administrators have the authority to enter into, when the device need to be downloaded keys, the administrators take it to secure room, and before use the App-TRSM to download the keys into device, the administrators’ password must be input right.

For the device, the firmware signature key loading is a sensitive service, there need mutual authentication between device and App-TRSM before loading key into device. Step as follows:

1、Do the mutual authentication between i9100 and App-TRSM.

2、then generate the PTK and TMACK used to encrypt the keys to be downloaded, and download the acquire keys from App-TRSM to device through serial communication.

Note:

1、All the session keys will generated by acquirer, and will be encrypted by the corresponding master keys when downloaded into device, for example, the PINK will be encrypted by PIN_MK, and all the application master keys are generated in App-TRSM, which is manually entered as plaintext components.

7.5 Key Replacement

The working keys must be update replaced with a new key every day. And whenever the compromise of the original key is suspected, even is explored and whenever the time deemed feasible to determine the key over exhaustive attack elapses.

7.6 Key Lifetime

There are symmetric master keys and asymmetric RSA keys used in the device, for some secure reason, like the crack technique is improved day by day, once the keys cracked by hacker, then the device is not security any more. So the keys saved in the device must have a life cycle, the recommended periods for different key types is as follow:

Private Signature Keys: 1~3 years;

Public Signature Keys: 3 years (2048 bits);

Symmetric Master Keys: about 1 year;

What is more, the OpenSSL was used in the device to generate RSA key pairs, and for mutual authentication before secure network communication, so if there is any bugs found in the OpenSSL, then the device must update the new OpenSLL library immediately.

8. Roles and Services

This device has three different modes:

- **Administrator mode**

  In this mode, the role has assigned to the acquirer management, which is in a secure manual to inject the initial key and force changing the default control password.

- **Normal mode**

  In this mode, the role has assigned to the normal use. That is the end users can use to the PIN entry normally.

- **Lock mode.**

  In this mode, the role has assigned to attack tampered, once the device suffered any tamper attack, this will cause the device into a locked manner. While the terminal device is disabled (in the Lock Mode), it must NOT be operate anymore. It' s recommend to look for the local technical supports.

The roles of device manufacturer, Acquirers, End users is as follow:

	Role	Operation
Acquirer	Administrator	1. Organize the third part to develop application program; 2. Download application and Acquirer Keys. 3. Access to device sensitive service.
End User	Operator	Perform transaction
Urovo	Maintainer	1. Sign Acquirer root certificate and initial key-load in factory. 2. Repair the device and unlock the device if tampered.