Security Policy for i90 Terminal

V1.0.1

2023-09-20

SZZT ELECTRONICS CO.,LTD

1 Introduction

This Security Policy provides guidance for the proper and secure usage of PCI PTS POI v6.2 devices i90.

The use of the device in an unapproved method, which is not described in this document will violate the PCI PTS approval of the device.

1.1 History

Version	Date	Author	Comment
V1.0.0	2023-08-04	Lianguangping	Initial version
V1.0.1	2023-09-20	Lianguangping	Modified section 5

2 References

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

[2] ANSI X9.24 Par2: 2016, Retail Financial Services Symmetric Key Management Part 2: Using Asymmetric Techniques for the Distribution of Symmetric Keys

[3] ANSI X9.143-2022: Retail Financial Services Interoperable Secure Key Block Specification

[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.

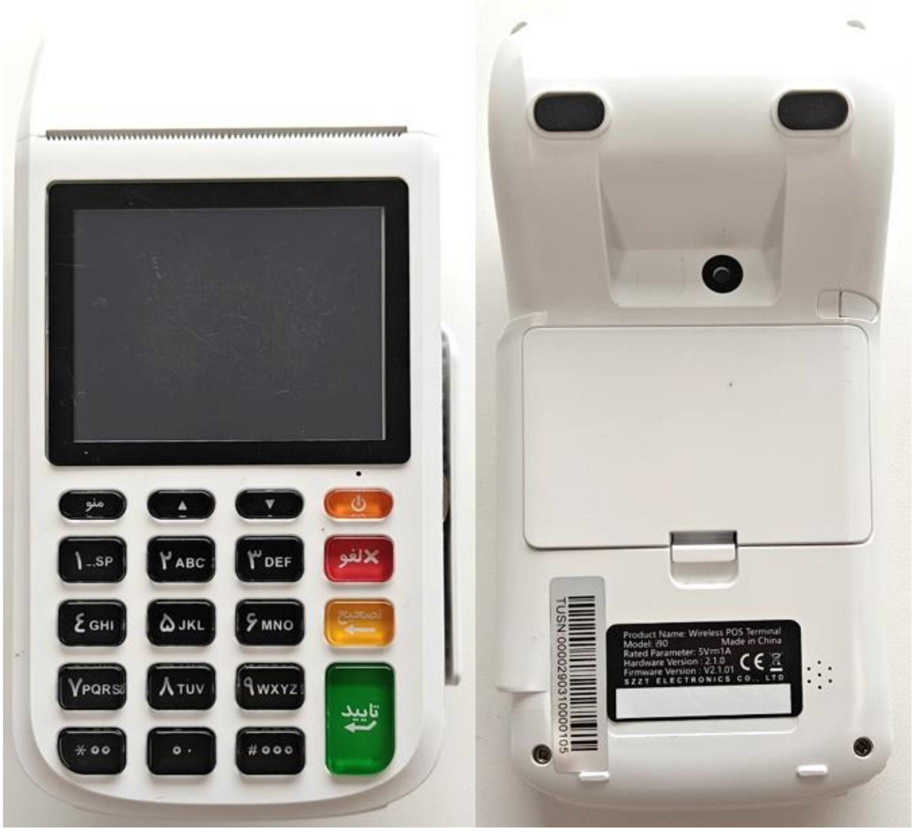
[6] PCI_PTS_POI_DTRs_v6.2_Final.pdf

[7] POS Terminal APIs.docx

[8] SSL Security Protocol Usage Guide.docx

3 Product Overview

The device intended to be used as a handheld PED in the attended environment under PCI PTS v6.2 requirements. The device is a new smart payment terminal, and provides LCD, buzzer, physical keypad, PSAM card, SIM card, IC card reader (ICCR), MSR, contactless reader, camera, USB, Cellular, Wi-Fi, printer. Please check whether the appearance of i90 is the same as follow:



3.1 Communication Methods and Security Protocols

The following describes the communication methods and protocols available in the device.

Function	Description
Wireless communication	Cellular(2G/4G), protocols: TLS V1.2, TCP, UDP, DHCP, ICMP, PPP, IP
	Wi-Fi, protocols: TLS V1.2, TCP, UDP, DHCP, ICMP, ARP, IP
Security protocol	TLS V1.2
Other communication	USB

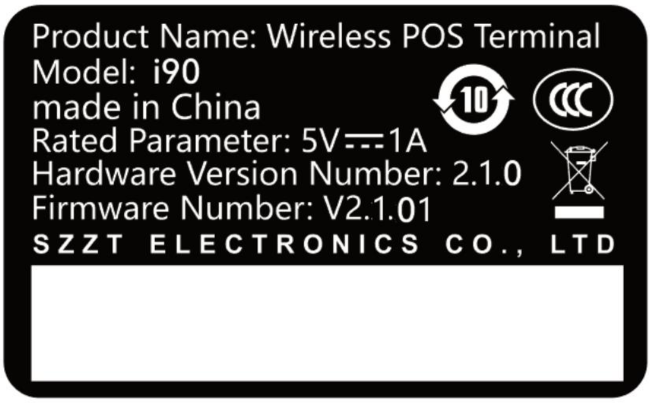
Use of any method not listed in the policy invalidates the device approval.

3.2 Device Identify

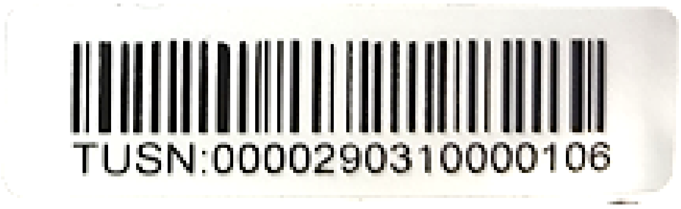
User can identify the approved device through the methods as below:

(1) Press the power button to power on the device, and you can see the LED lights up, indicating that the machine is powered on. Waiting for a period of time, it will enter the menu. Go to menu (3.Term Information), and you can see many version information such as firmware, etc.

(2) User can check working voltage, hardware version and product number, etc. Please see below picture as an example:



Product Name: Wireless POS Terminal
Model: i90
made in China
Rated Parameter: 5V⎓1A
Hardware Version Number: 2.1.0
Firmware Number: V2.1.01
SZZT ELECTRONICS CO., LTD



TUSN:0000290310000106

The merchant or acquirer must visually inspect the terminal when received via shipping, as it is described in the user manual.

For example, the merchant or acquirer should inspect the terminal to ensure that:

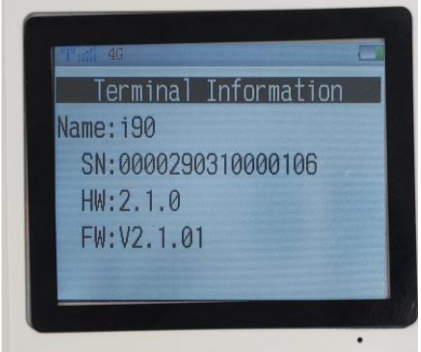
- There is no evidence of unusual wires that have been connected to any ports of the terminal.
- There is no shim device in the slot of the ICC acceptor

3.3 Terminal Information

The hardware versions is 2.x.x The “x” variable at 3rd position stands non-security related hardware option for device camera pixel and the “x” variable at 5th position stands non-security related hardware option for communication module.

The firmware version is V2.x.xx The “x" variable at 4th position stands for non-security related software option for camera driver and the “xx" variables at 6th to 7th position stand for non-security related software option for communication module driver.

To examine the version of the device, we can launch “3.Term Information" -> “Terminal Information” the version info is shown below:



Terminal Information

Name:i90

SN:0000290310000106

HW:2.1.0

FW:V2.1.01

The hardware version on the nameplate is affixed to the rear case.

Hardware Number	2	.	x	.	x
	1	2	3	4	5
3	The character stands for camera pixel, as described below: 0.400 thousands pixels 1.300 thousands pixels 2.200 thousands pixels 3.100 thousands pixels 4.None				
5	The character stands for communication module, as described below: 0.support 4G+2G+WIFI 1.support 4G+WIFI 3.support 4G+2G 4.support only WIFI 5.support only 4G				

Firmware Number	V	2	.	x	.	x	x
	1	2	3	4	5	6	7
4	The character stands for camera driver, as described below: 0.400 thousands driver 1.300 thousands driver 2.200 thousands driver 3.100 thousands driver 4.None						
6-7	The character stands for communication module driver, as described below: 01. 4G+2G+WIFI 02.support 4G+WIFI 03.support 4G+2G 11.support only WIFI 12.support only 4G						

4 User Guide

The merchant or user will be informed to check:
(1) If the labels on screw holes are well;
(2) If the device case had ever been opened or destroyed;
(3) If the IC and MSR reader appear suspicious object.

Also, the user will be told how to view the serial number, logo and version. This checking routine is applied for shipment or periodicity checking.

4.1 Device Designed for Handheld

The i90 is a handheld POS device. There are some features which a handheld device should own:
(1) With a battery which can be charged when necessary.
(2) Can enter low-power mode when necessary.
(3) The battery cover is designed for handheld, which conform to human engineering design.
(4) The weight and size are designed for handheld standard.

4.2 Roles of Device

The roles that supported by device are administrator and normal user.

(1) Administrator. Each device has two administrators. The two administrators are responsible for managing the sensitive services of device. Only if both of the administrators input correct password, sensitive services including change password, load key and KBPK loading can be accessed.

(2) Normal user. The normal users have no access to sensitive services of device.

They can only use device to do normal financial transaction.

4.3 PIN Entry Guide

The i90 is a handheld device, and the consumer has to face the device to obscure other people's external observations when entering the password.

The operator should be in the following locations:

- When the cardholder enters the password, it is necessary to take into account that others have inadvertently photographed it with the camera.
- Cardholders must consider whether there will be a mirror or some reflective material when entering the password.

4.4 Secure Use ICC

To make sure IC card reader being used securely, the merchant will be informed to note the following cases:

(1) Check whether the IC card reader opening has suspicious line. If it has, please stop using the device and inform the manufacture.

(2) Check whether IC card is inserted smoothly. If there is foreign object blocking the card or the card can’t be inserted normally, please stop using and inform the manufacture.

(3) Check whether the shell of IC card reader interface is integral. If its surface has traces of damage, please stop using and inform the manufacture.

4.5 Secure Use MSR

To make sure MSR being used securely, the merchant will be informed to note the following cases.

(1) Check whether the MSR slot has suspicious line. If yes, please stop using the device and inform the manufacture.

(2) Check whether swipe card smoothly. If no, please stop using and inform the manufacture.

(3) Check if there is any addition beside the MSR from the hollow slot. If yes, please stop using and inform the manufacture.

4.6 Device Periodically Checking

The merchant or acquirer should inspect the terminal when the device received via shipping and every day to ensure that:

(1) The merchant or acquirer should check that the terminal was not destroyed or installed a suspicious bug. Make sure the used devices are the approved ones.

(2) There is no evidence of unusual wires that have been connected to any ports of the terminal.

(3) Hardware version and firmware version on terminal label or screen are consistent with the approved HW and FW version.

(4) There is no open case evidence visible via checking the case or the labels in screw holes.

(5) There is no suspicious thing appear in ICC and MSR reader.

(6) The merchant or acquirer should also check that the installation/maintenance operations are performed by a trusted person.

(7) The merchant or acquirer should inspect whether the product appearance has been changed to avoid overlay, such as the display, physical keypad area and so on.

(8) The merchant or acquirer should check if the terminal is triggered. The tamper response, please refer to section “8.1 Tamper Response”.

5 Key Management

5.1 Key Management Techniques

The device implements key management techniques:

Master Key/Session Key: a method using a hierarchy of keys. The session keys are unique per device.

Use of the terminal with a key-management system other than mentioned above will invalidate any PCI approval of the terminal.

Note: Using any other key-management will invalidate the PCl approval. The device is designed to support cryptographic method as required from PCl.

5.2 Algorithm Support

The i90 terminal supports the secure algorithm as following:

· TDES (128bits, 192bits)
. AES (128bits, 256bits,)
· RSA-2048
· SHA (256bits, 512bits)
. ECC (p-256, P-521)

5.3 Key Table

Name	**Purpose / Usage**	**Algorithm**	**Size (Bits)**
Symmetric Key			
Root Key (RootKey)	Encrypt Data For Store	AES	256
KBPK	Protect For key loading	AES	256
Main Key (TMK)	Encrypt Work Key	AES	128
PIN Key (PINK)	Encrypt PIN Block	TDES/AES	128 for TDES and 128 for AES
MAC Key (MACK)	Calculates Mac Value of The Transaction Message	TDES	128
PAN Key (PANK)	Encrypt Account Data	TDES	192

5.4 Key Download

The device uses the following key loading method:
1. Clear-text key components through the physical keypad.
2. Symmetric encrypted keys
3. The device does not support remote key loading.

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

5.5 Key Replacement Policy

Whenever the stored 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 the keys or inject the new keys before it can perform PIN transaction as normal.

6 System Administration

6.1 Configuration Settings

The device is functional when received by the merchant or acquirer. No security related configuration settings need to be tuned by the end user in order to meet security requirements.

6.2 Default Value Update

In the device, the default password used for dual control will be forced to be changed when the device is received by the acquirer.

7 Software Security

7.1 Software Development Guide

The POS device provides security communication interface obey Compliance with PCI requirement. The developer should strictly comply with the document [7]. Document [7] also provides guidance for SRED development. The developer also must accept training course before development activity starting and respect the coding rules and best practices during the whole development stage. 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) Signature

For SRED Module, the i90 works in encrypting mode and doesn’t support pass-through of clear-text account data. Any plaintext account data are not allowed to transfer to outside of the device, which means the firmware cannot display any plaintext account data on the screen or output any plaintext account data to network through any communication channel.

For use of open protocol, the developer must respect the document [8]. It is important to note that SSL3.0, TLS1.0, TLS1.1 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 non-financial use. In addition, we strongly recommend a server should disable SSL protocol, and select TLS1.2 or higher instead. To make it more secure, mutual authentication is recommended.

7.2 Firmware Authentication

This device implements asymmetric cryptographic algorithm for firmware authentication. RSA algorithm with 2048bits key is used for signature verification and SHA512 or SHA256 algorithm is used to calculate the digest of firmware.

The firmware is signed by RSA-2048 bits private key which is only controlled by vendor. And the firmware authentication is executed with signature verification using corresponding public key of vendor.

The certificate and signature of the firmware code are verified. The certificate and signature are based on couples of RSA keys.

7.3 Software Update

Updates and patches can be loaded in the device. When downloading or updating firmware, it needs authentication. The i90 only accepts update package 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.

7.4 Self-Checking

(1) Power on check

When the system powers on, it will check the firmware in a certain order to verify their integrity and legitimacy.

(2) Check key before using

When reading key, the key will be checked. If the key integrity or legitimacy checked fail in the checking procedure, the battery-backup key will be cleared and regenerated, and all the other keys will be cleared.

(3) 6 hours check

The device will reboot every 6 hours to re-initialize the RAM. After powering on, self-test is performed to verify validity of firmware and keys. If any error detected, sensitive data will be erased.

8 Product Hardware Security

8.1 Tamper Respond

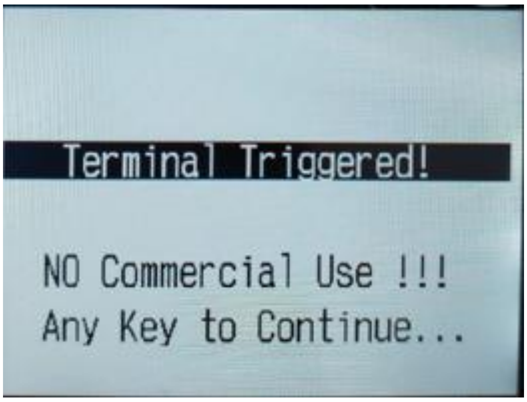
Tamper trigger event

1. Front case removal;
2. Back case removal;
3. Physical penetration on all the sides of the device;
4. MSR removal;
5. Temperature is >115℃ or <-45℃;
6. Security chip voltage is outside of range, approximately < 2.0V or > 4.3V;
7. Stored sensitive data authentication failed during the self-test.

A merchant or acquirer can easily detect a tampered terminal when:

- Warning message is displayed on the screen.
- Can’t do any transaction.

Any physical penetration will result in tamper event. This event causes the activation of tamper mechanisms that make the device go out of service.



Terminal Triggered!

NO Commercial Use !!!
Any Key to Continue...

There are two separate modes in which the device can be:

- Activated mode: The device is fully operational.
- Locked mode: The device is tampered, not operational and needs reactivation after maintenance and security checks.

When the device is in tamper state, the operators or merchants should ask vendor maintenance personnel for help to recover device from tamper state or send back this device to vendor.

8.2 Re-inject Key

After device detects tamper event, it will be tampered.
Only if the terminal is returned to the original factory, it can be released from self-destruction and download the key again.
For how to inject key please refer to chapter 5.4.

8.3 Environment and Operational Conditions

This device is designed to be used in an attended environment.
Working temperature range: 0℃～50℃.
Working humidity range: 10%～90%.
Storage temperature range: -20℃～70℃.
Storage humidity range: 5％～95％.
Input voltage: DC 5V.

Terminal should stay away from all sources of heat, to prevent vibration, dust, moisture and electromagnetic radiation.

8.4 PIN Confidentiality

The i90 is a hand-held PED device without a privacy shield, and it is required to provide cardholders with necessary privacy during PIN entry process. The device needs some methods to protect PINs during PIN entry. For example, the device will demonstrate a safe PIN-entry process how to securely enter the PIN, and this message will remind cardholder that he can use his own body or his free hand to block the view of physical keypad.

The following table shows the combinations of methods that must be used to protect the cardholders' PIN during PIN entry.

Method	Observation Corridors				
	Cashier	Customer Queue	Customer Elsewhere	On-Site Cameras	Remote Cameras
Check stand	Customer positions PED.	Customer positions PED.	Customer positions PED.	Do not operate within view of cameras.	Do not operate within view 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.

8.5 Decommissioning/Removal

When the device is no longer used for permanent decommissioning reason, the device needs to erase all the key materials on it. It can be done by directly opening the casing of the device to make it tampered. Even though someone reassembles the device, it still cannot work as its all keys have been erased automatically and it will warn exception because of the tamper triggered by disassembling.

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 main board hardware tamper mechanism.