Security Policy Manual

VERSION: 1.06A

For T1000

Revision Notes

Version	Date	Page(s)	Description	Updated by
1.00A	1 Mar, 2016		Initial Version.	Gary/Michael/Ho
1.01A	2 Jun, 2016		Added Section 7.9 label for safe pin entry	Jeff
1.02A	2 Jun, 2016		Added SRED	Gary
1.03A	12-Jul-2016		Update operating and storage conditions of the device	Patrick
1.04A	2 Aug, 2016		Updated Section 6.1 (Installation Environment)	Jeff
1.05A	3 Aug, 2016		Updated section 3 and 5.4 for software guidance document. Fixed alignment issue in section 5.5.	Gary
1.06A	6 Sep, 2016		Revise footer. Correct typo in section 5.6. Revise General Description.	Gary

Functions Definition and Abbreviation

DES = DES encrypt function in form DES(encryption KEY, DATA to be encrypted)

DES2 = DES decrypt function in form DES2(decryption KEY, DATA to be decrypted)

3DES = triple DES encrypt function in form 3DES(encryption KEY, DATA to be encrypted)

3DES2 = triple DES decrypt function in form 3DES2(decryption KEY, DATA to be decrypted)

owf = one way function in form of owf(KEY to be diversified, diversify DATA)

KVC = key verification code

TDES = triple DES

RSA = RSA encrypt function in form RSA(KEY,DATA to be encrypted)

Contents

1. APPLICATION 5

2. OBJECTIVE 5

3. REFERENCE DOCUMENT 5

4. GENERAL DESCRIPTION 5

5. APPEARANCE 6

5.1. SELF-TEST AND STARTUP SEQUENCE 10

5.2. FIRMWARE AND APPLICATIONS MAINTENANCE 10

5.3. FIRMWARE AND APPLICATIONS SIGNING / AUTHENTICATION 10

5.4. SOFTWARE DEVELOPMENT GUIDANCE 11

5.5. KEY MANAGEMENT 11

5.5.1. CRYPTOGRAPHIC ALGORITHMS 11

5.5.2. KEY TYPES / USAGES 12

5.5.3. KEY REPLACEMENT 12

5.5.4. KEY LOADING 12

5.6. ENVIRONMENTAL CONDITIONS THAT TRIGGER TAMPER MECHANISM 12

6. USER GUIDANCE/ INSTALLATION AND DAILY CHECKING ITEMS 13

6.1. INSTALLATION ENVIRONMENT 13

6.2. USAGE ROLES 13

6.3. CONFIGURATION SETTING 13

6.4. IC CARD SLOT CHECKING 13

6.5. CHECKING FOR TAMPER EVIDENCE 14

6.6. CHECKING FOR OVERLAY ATTACK 14

6.7. SYSTEM INITIAL SETUP FLOW 15

6.8. DECOMMISSIONING OF DEVICES 15

6.9. LABEL FOR SAFE PIN ENTRY 15

1. Application

This manual is to serve as the security policy information for R&D, Production, Sales & Marketing and Customer Service purpose.

This manual can only be applied to T1000.

2. Objective

The objective of this manual is to provide necessary security policy information for users to use the device. It addresses the proper use of the POI in a secure fashion, including information on key-management responsibilities, administrative responsibilities, device functionality, identification, and environmental requirements.

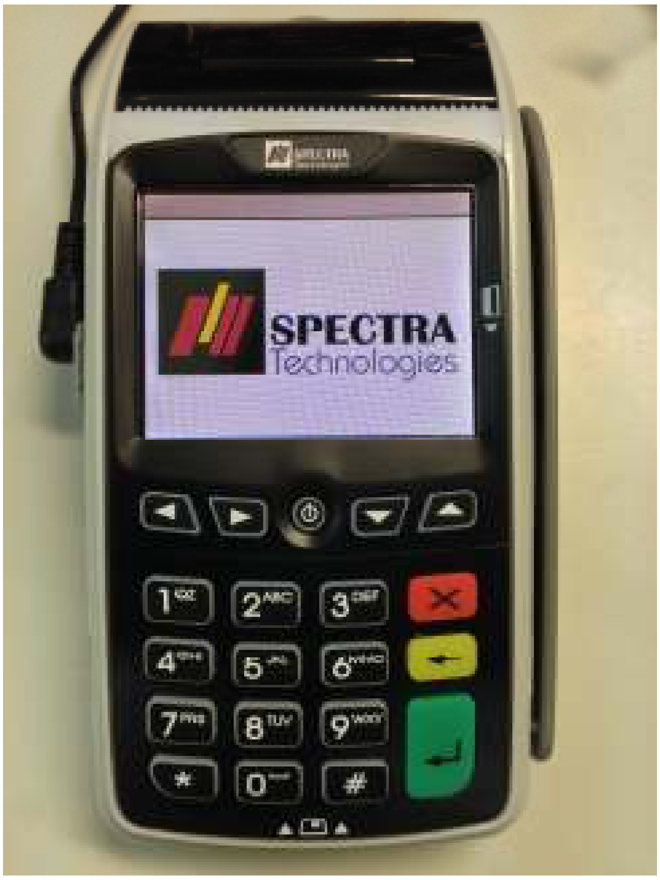
3. Reference Document

[1] T1000 PCI Evaluation Document
[2] T1000 OP Security Guidance
[3] T1000 Installation and Security Guide
[4] T1000 SRED Security Guidance
[5] T1000 Software Development Guidance

4. General Description

It is mobile/desktop POS terminal in an attended environment. It equips with TFT colour display, EMV compliant IC card reader, secure magnetic swipe card reader, printer, USB, Ethernet, modem, optional GPRS wireless communication.

5. Appearance



Environmental condition

Device Operating Temperature:	0-45 ℃
Relative Humidity :	0-85% non-condense
Device Storage Temperature:	-20-70 ℃
Rechargeable battery Storage Temperature :	-20 ~ 25 degree C
Relative Humidity:	0-85% non-condense

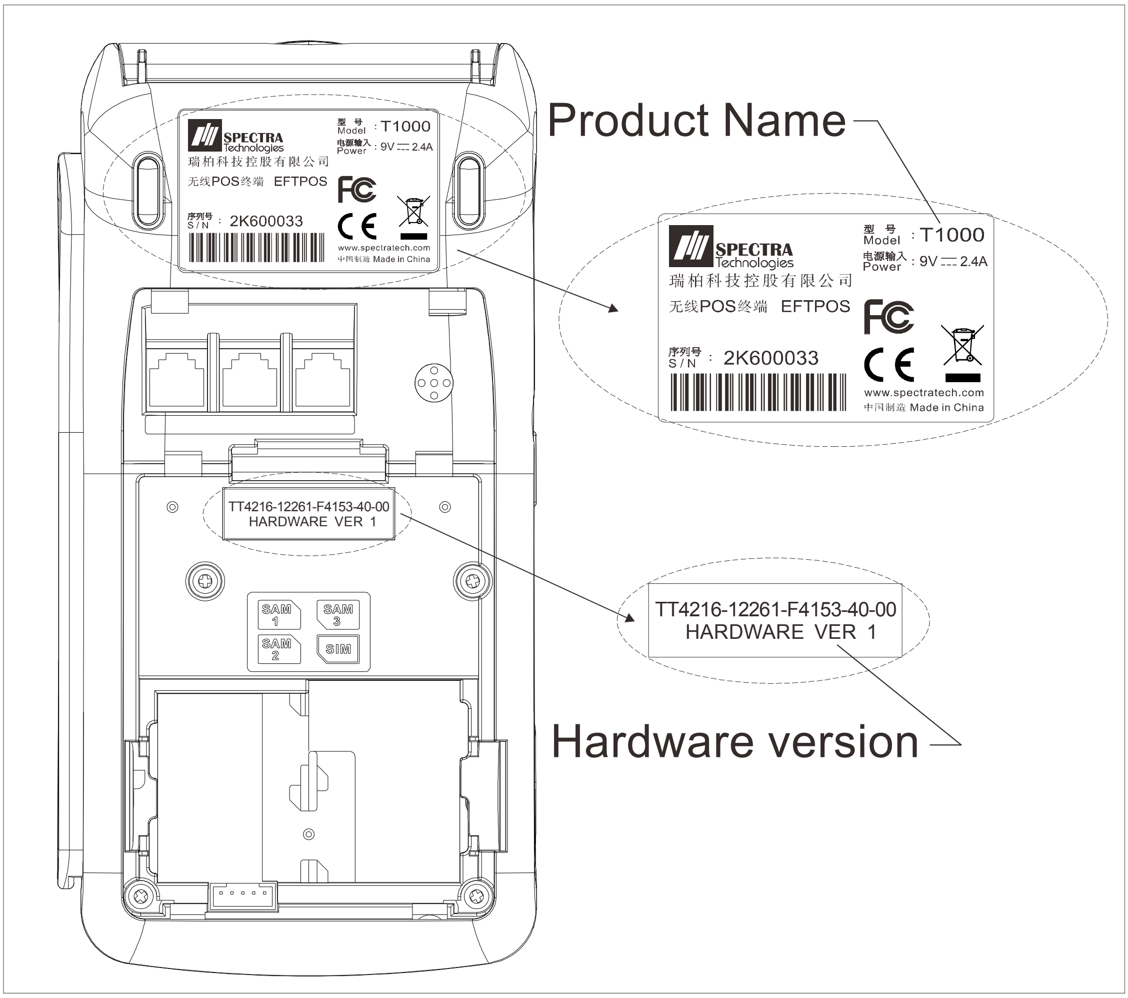
Power input: DC 9.5V/2.4A or USB 5V/1A

The security of the device is not compromised by changing the environmental condition stated above.

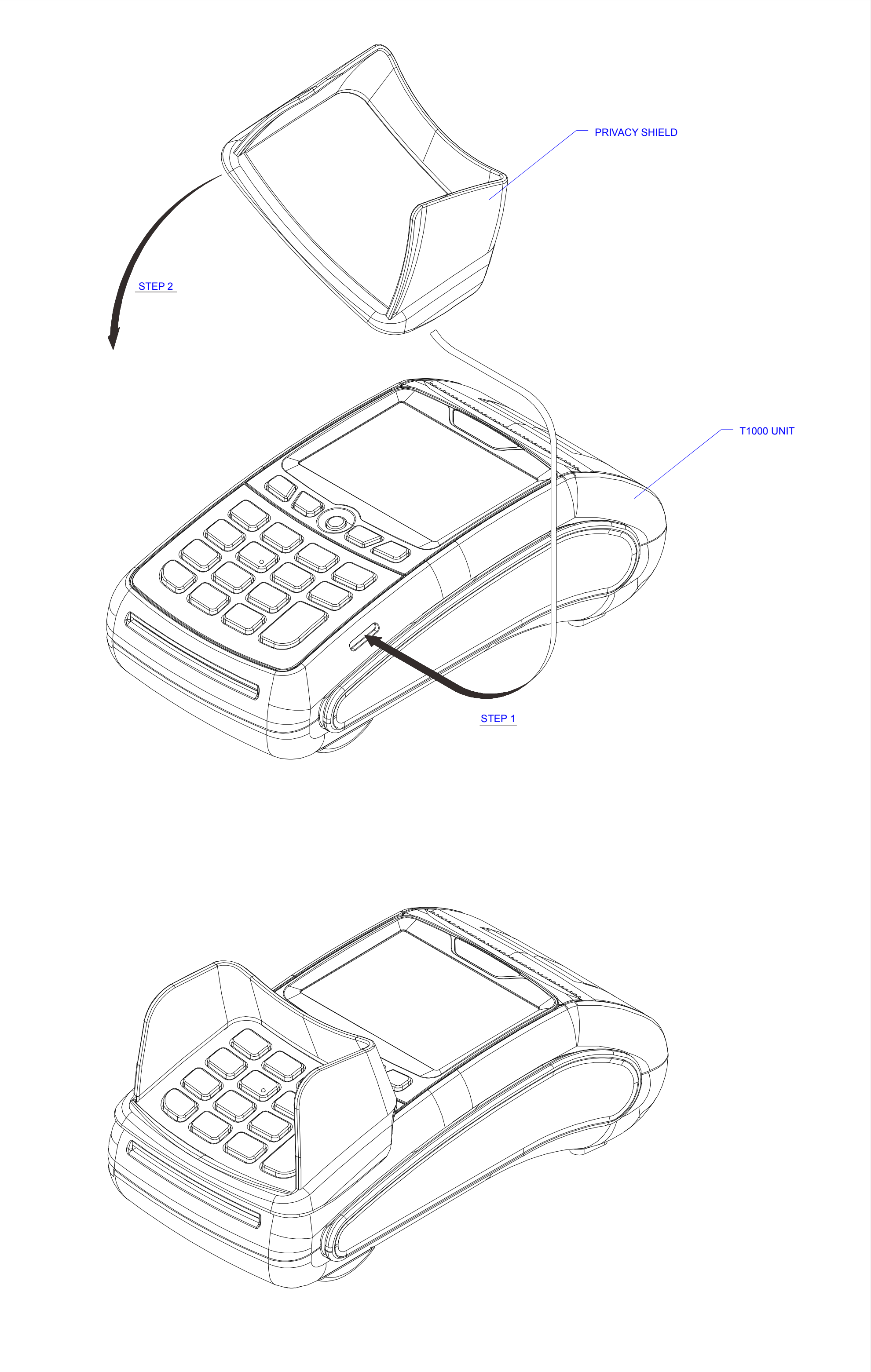
Open Box Checklist

- Product name – T1000
- Hardware version –TTxxxx-xxxxx-xxxx3-xx-xx

The “x” are not security related variables.
Please note that modification of a PCI approved platform that impacts platform security results in a change of platform identifier.



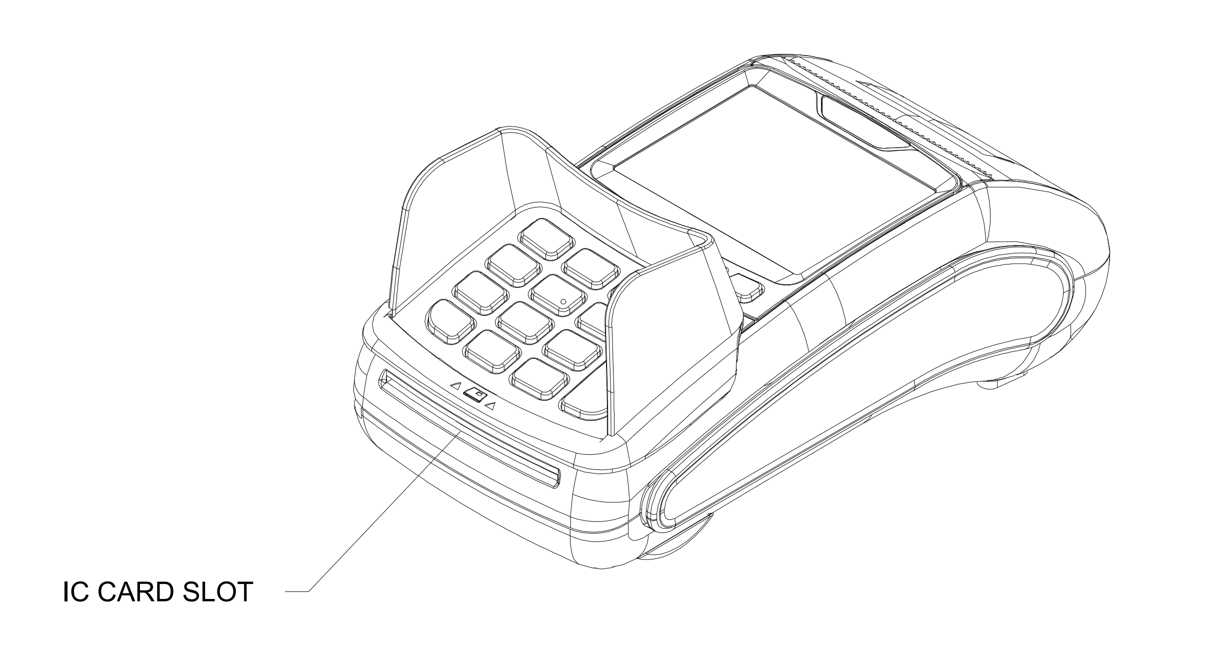
- Firmware version -
    - Power up T1000 to check Boot loader and System version and checksum.
- Application version -
    - Power up T1000 and press the keys described in document [3] one by one.
    - Press ‘2. SW LIST’ and then press ‘1. Application’ to check application version.
    - Press individual application number to check the application checksum.
- Equipped with privacy shield – Yes



T1000 UNIT WITH PRIVACY SHIELD INSTALLED

- Damage of Front or Rear Cabinet - No
- Suspicious object connected to the machine body - No
- Damage at the position of screw holes - No
- Damage of the keyboard - No
- Suspicious object such as overlay on keyboard surfaced - No

- Suspicious object near the IC card slot - No
- Damage near the IC card slot - No
- Wire running out of the slot – No



5.1. Self-test and Startup Sequence

Device will perform a self-test, which includes tamper detection, integrity verification and authenticity tests for the system firmware and applications upon start-up/reset and at least once per day to check whether the device is in a compromised state. No operator is required to initiate the self-test. More details are described in document [1].

5.2. Firmware and Applications Maintenance

Firmware and applications maintenance are under maintenance menu, which provides application update and delete functions. The device will perform cryptographically authentication during the maintenance process and only authenticated firmware, applications and patches can be updated. The loading process is described as below and please refer to document [3] for more details.

- Power up device and press the keys described in document [3] one by one.
- Enter the password prompted by the system.
- Press “1 SW DOWNLOAD” for application update or press “2. SW LIST’ and then press ‘1. Application’ for application maintenance.
- Enter the password prompted by the system.
- For application update, please use the authenticated program loader on PC to download the application to the device.
- For the application maintenance, press individual application number for maintenance.

The device also support the remote updates and the setup and loading processes are shown as below. More details can be found in document [3].

- Power up device and press the keys described in document [3].
- Setup the remote parameters described in document [3].
- Wait for finishing update process and restart the device.

5.3. Firmware and Applications Signing / Authentication

All applications have to be signed by the corresponding private key for authentication, their signatures will be verified using corresponding public key at system boot up and application download. The signature used is 2048 bits RSA with SHA-256.

In system boot up, if signature verification is not correct, system will be reset. During application download, if the signature is found not correct, signature error will be resulted and the application will not be saved. The signature will also be verified when the application is launched. If the signature verification is failure, application will be ignored.

The signature uses 2048 bits RSA with SHA-256 and the 2048 bits RSA key pair is controlled by Spectra.

More details can be found in document [1].

5.4. Software Development Guidance

The security details of HSM operations, memory organization, file system usage and program management are described in sections 1.17/1.4/1.9/1.8 of the document [1]. The system security and security data organization are also described in the document [1].

In addition, for the following list of supported protocols and services, a security guidance document for their usages, operations, APIs and configurations are described in document [2].
- Ethernet, PPP, TCP, UDP, IP, ICMP, ARP, TLS, DHCP, USB, UART, GPRS and Modem.

Please note that the device provides TLS v1.2 as a secured communication channel for financial applications to send data over the Ethernet, GPRS and modem. This protocol must be used when handling transaction data, or other sensitive data.

Besides, when developing SRED application, account data must be encrypted and masked, outputting of clear-text account data is not allowed. Details can be found in document [4].

The developers must follow the above guidance and document [5] when developing the related applications.

5.5. Key Management

The device supports different types of key management systems listed below. More details can be found in ANS X9.24.

Fixed Key: A method based on a unique key for each terminal.
Master/Session Key: The technique based on a hierarchy of keys. The master key is used to encrypt the session keys which is unique per transaction.
DUKPT: It is based on a unique key per transaction.

Please note that the use of the device with unapproved key-management systems will invalidate the PCI PTS approval.

5.5.1. Cryptographic Algorithms

The device includes the following algorithms:
- Triple DES (112 bits and 168 bits)
- AES (128/192/256 bits)
- RSA (Signature verification, 2048 bits)
- SHA-256 (Signature digest)

5.5.2. Key Types / Usages

Key	Usage	Algorithm	Size (Bits)
APSK	Public key for application signature verification	RSA	2048

Table 1: Public RSA keys

Key	Usage	Algorithm	Size (Bytes)
AFK	PIN encryption	TDES/AES	TDES: 24 AES: 24/32
AMSTMK	Key encryption key for AMSTPK	TDES/AES	TDES: 24 AES: 24/32
AMSTPK	PIN encryption	TDES/AES	TDES: 24 AES: 24/32
ADUKPTK	PIN encryption	TDES	16
ADEK	Account data encryption	TDES	24
Key encryption key	Key encryption	AES	32

Table 2: Triple DES keys

5.5.3. Key Replacement

Any key should be replaced with new key 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 technology must be review for every 2 years to see whether the key should be replaced with the new key to avoid exhaustive attack.

5.5.4. Key Loading

Before key loading of Fixed Key, Master/Session Keys (TMK/TPK) or DUKPT Key is allowed, IMEKs and MEK must be updated. Trustees have to enter the IMEK key pair into both PED and authenticated key injection host. Once is MEK is updated, key injection will be allowed. All the above sensitive functions are under dual password protection from 2 trustees. The key loading process must be performed in a secure environment.

5.6. Environmental conditions that trigger tamper mechanism

Temperature attack outside the range from -37℃ to +120℃

Voltage of VBATT outside the range from 2.1V to 3.8V. Or VDDIO voltage outside the range from 3.6V to 3.8V.

External supplied voltage higher than 5.5V may damage Buck mode DCDC and cause over voltage at VBATT and VDDIO. Therefore trigger the tamper mechanism.

6. User Guidance/ Installation and Daily Checking Items

6.1. Installation Environment

T1000 terminal must be installed in an attended environment only. It has been designed for both handheld and counter top usage. For handheld usage, only wireless connectivity is adopted. For counter top usage, wireless connectivity or both wireless and wired connectivity as backup purpose can be adopted.

6.2. Usage Roles

All terminals are delivered to end users in their active state that process the PIN base transaction normally. For system maintenance (e.g. application download, password modification), only authorized administrators can access to it, the system maintenance is protected by the system passwords. Besides, only authorized trustees can perform the key injection that protected by dual passwords control.

6.3. Configuration Setting

There are no security sensitive configuration settings and default values are required to be changed by the end user to meet security requirements except the passwords.

Each trustee will be given his corresponding initial password generator to generate the initial password for the agreed parse phrase. Either system or PED DLL will enforce those trusted people to change the initial passwords. Otherwise, no application can be run, all sensitive functions and external requests will be blocked by PED DLL, and all boot system sensitive functions will be inaccessible.

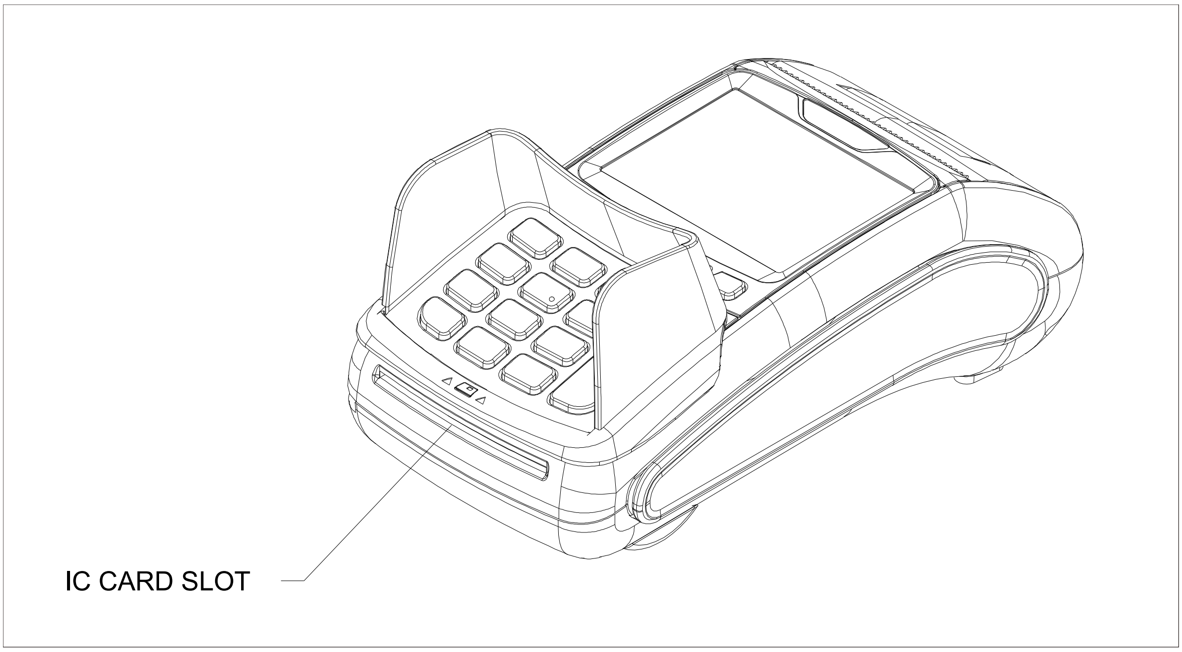
6.4. IC Card Slot Checking

In order to eliminate unauthorized capturing of IC card information, please perform checking everyday for unauthorized electronics within the IC card slot.

1. Check the entrance of the IC card slot carefully. Stop using the machine and report to the local agent when one of the followings is detected.
   - any suspicious object near the slot
   - any damage near the slot
   - any wire running out of the slot

2. Inspect the IC card slot with help of torch light. Stop using the machine and report to the local agent when any suspicious object such as thin film is stored inside the slot.

3. Insert the IC card slot with a test card. Stop using the machine and report to the local agent when the card insertion is obstructed abnormally.



6.5. Checking for Tamper Evidence

In order to eliminate unauthorized modification of the terminal unit, please perform the following checking everyday. This information is also described in document [3].

Check the Front and Rear Cabinet carefully. Stop using the machine and report to the local agent when one of the followings is detected.
- any damage of Front or Rear Cabinet
- any suspicious object connected to the machine body
- any damage at the position of screw holes
- system prompts the following “Terminal Tampered” message

```
*** Terminal ***
*** Tampered ***
    (XXXXX)
```

6.6. Checking for Overlay Attack

In order to eliminate unauthorized pin capturing by additional keyboard such as overlay, it is advised that checks are performed everyday. The guidance of checking is described in document [3].

6.7. System Initial Setup Flow

To setup the device when it is firstly started, the guidance for system setup, password management and application download procedures are describe in document [3].

6.8. Decommissioning of Devices

All sensitive data and keying material must be erased before decommissioning the device or removing it permanently from service. This can be done by disassembling the device and make it tampered.

6.9. Label for safe Pin Entry

Merchants should instruct cardholders to hold the machine at a position to deter visual observation by the cardholders' body during pin entering. The label has to be kept sticking onto the device any time for reminding safe PIN-entry process