

Security Policy Manual

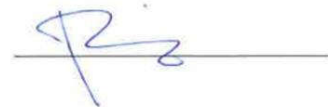
VERSION: 2.12

Model: T300

Issued Date : 22 May 2024

Prepared by : Kenneth

Approved by :



Distribution List			
R&D (Doc. Control)	General Manager	QA Manager	R&D (CD)
R&D (ME)	R&D (EE)	R&D (Testing)	Sales & Marketing
Customer Service	PD (Production)		

Revision Notes

Version	Date	Page(s)	Description	Updated by
2.00A	22 Aug 2017	14	Initial Version.	Gary/Kenneth/Mobile
2.01A	12 Sep 2017	14	Add touch LCD description in section Software Development Guidance.	Gary
2.02A	09 OCT 2017	14	Section 6.1 updated.	Kenneth
2.03A	11 OCT 2017	14	Section 5.0 updated.	Kenneth
2.04A	12 OCT 2017	15	Added Section 6.1.1	Kenneth
2.05A	20 OCT 2017	16	Hardware version & it's label changed in Section 5.0	Kenneth
2.06A	27 NOV 2017	17	Section 6.5 updated.	Kenneth
2.07A	26 Feb 2018	12	Section 5.6	Gary/Steven
2.08A	14 Mar 2018	7	Updated Open Box Checklist	Mobile
2.09A	9 April 2018	5 6	Section 4) General Description add secondary display description. Updated section 5) Appearance	Mobile
2.10A	10 Apr 2018	7 & 8 5-6 8	Update Hardware version label Update Section 5) Appearance Updated Open Box Checklist	Kenneth Mobile
2.11	21 Jan 2024	5	Renamed GPRS Wireless to cellular	Kenneth
2.12	26 Jan 2024	7 11	Update open box checklist Renamed GPRS to cellular	Kenneth
	29 Feb 2024	5-11	Update Section 4) General Description – update device description, photo, Hardware, and Firmware version.	Kenneth
	18 Apr 2024	1-19	Update logo of heading	Kenneth
	22 May 2024	5, 13	Remove bluetooth	Kenneth

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	12
5.2. FIRMWARE AND APPLICATIONS MAINTENANCE	12
5.3. FIRMWARE AND APPLICATIONS SIGNING / AUTHENTICATION	12
5.4. SOFTWARE DEVELOPMENT GUIDANCE	13
5.5. KEY MANAGEMENT	13
5.5.1. CRYPTOGRAPHIC ALGORITHMS.....	13
5.5.2. KEY TYPES / USAGES.....	14
5.5.3. KEY REPLACEMENT	14
5.5.4. KEY LOADING.....	14
5.6. ENVIRONMENTAL CONDITIONS THAT TRIGGER TAMPER MECHANISM	14
USER GUIDANCE/ INSTALLATION AND DAILY CHECKING ITEMS	15
5.7. INSTALLATION ENVIRONMENT	15
6.1.1 DEVICES INSTALLATION ENVIRONMENT FOR COUNTER TOP USAGE.....	15
5.8. USAGE ROLES	16
5.9. CONFIGURATION SETTING	16
5.10. IC CARD SLOT CHECKING	16
5.11. CHECKING FOR TAMPER EVIDENCE.....	17
5.12. CHECKING FOR OVERLAY ATTACK	18
5.13. SYSTEM INITIAL SETUP FLOW	18
5.14. DECOMMISSIONING OF DEVICES	19

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 T300.

2. Objective

The objective of this manual is to provide necessary security policy information for R&D Development, Production and customers. 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] T300 PCI Evaluation Document
- [2] T300 OP Security Guidance
- [3] T300 Installation and Security Guide
- [4] T300 SRED Security Guidance
- [5] T300 Software Development Guidance

4. General Description

The device is approved as PED product under PCI PTS 5.1 requirement.

It is POS terminal in an attended environment. It equips with primary TFT colour display, secondary mono display [it ONLY showing the amount to the customer. It will be off in payment stage.], EMV compliant IC card reader, secure magnetic swipe card reader, printer, USB, Ethernet, modem and cellular communication.

The use of the device in an unapproved method will violate the PCI PTS approval of the device

5. Appearance



Front view



T3-T-xxxxx-xx1xx-xxxx2-xx (with Contactless reader) (Previous Approved)



T3-F-xxxxx-xx1xx-xxxx3-xx (with Contactless reader & w/ Fiscal Memory & Customer LCD) (Delta version)

Environmental condition

Device Operating Temperature: 0 ~ 45 °C
Relative Humidity : 0~85% non-condense

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

Power input: USB 5V/1A
DC Jack 9V/1A

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

Open Box Checklist

- Product name – T300
- **Hardware Version**
 - T3-F-xxxxx-xx0xx-xxxx3-xx (without contactless reader & w/ Fiscal Memory & Customer LCD)
 - T3-F-xxxxx-xx1xx-xxxx3-xx (with contactless reader & w/ Fiscal Memory & Customer LCD)
 - T3-T-xxxxx-xx0xx-xxxx2-xx (without contactless)
 - T3-T-xxxxx-xx1xx-xxxx2-xx (with contactless)

The format of hardware version is:

With contactless reader

T	3	-	F	-	x	x	x	x	x	-	x	x	1	x	x	-	x	x	x	x	3	-	x	x
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

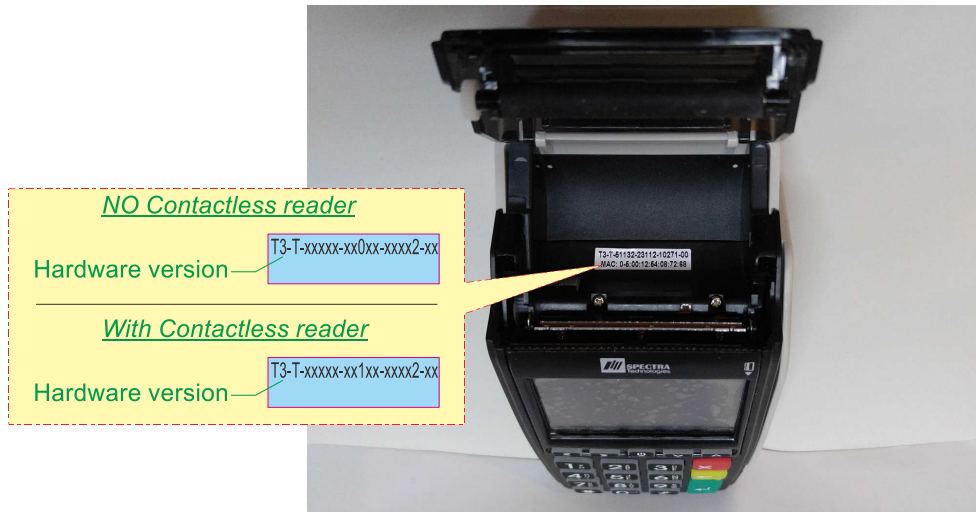
Without contactless reader

T	3	-	F	-	x	x	x	x	x	-	x	x	0	x	x	-	x	x	x	x	3	-	x	x
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

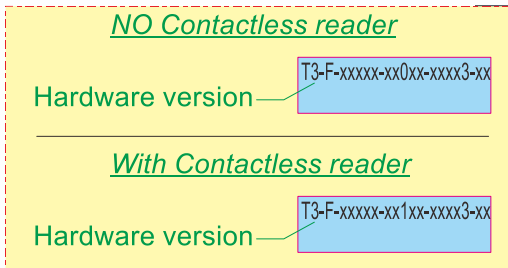
The “x” are not security related variables, the explanation of each digit is below:

- 6: Type of power adaptor
- 7: Keypad silkscreen language
- 8: Casing color
- 9: Stand pole
- 10: Battery capacity
- 12: Flash and SDRAM size
- 13: Codec and Touch panel
- 15: MSR and Smart card
- 16: SAM / SIM card
- 18-19: Cellular
- 20: Reserved
- 21: Ethernet and mode
- 24-25: Logo

Please note that modification of a PCI approved platform that impacts platform security results in a change of platform identifier.



For model with Fiscal Memory & customer display



- **Firmware version**

- Power up T300 to check Boot loader and System version and checksum.



Bootloader: 1.x.x

x: The version number for non-security-related software changes

System: 2.x

x: The version number for non-security-related software changes

- **Application version -**

- Power up T300 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. In order to deter the visual observation of PIN values as they are entered by the cardholder, the privacy shield must be used regardless of device being used as desktop or handheld PED.

PEDDLL 1.x

x: The version number for non-security-related software changes



- 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.

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 refers 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.

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, cellular 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, cellular 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].

For the device with touch LCD, the touch LCD must not be used for any PIN entry purpose.

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 key 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/AES 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

The environmental conditions outside which trigger a tamper condition are:

- Voltage (external): >3.6V and <1.59V
- Voltage (processor - VDDCore): > 1.31V and <1.08V
- Temperature (processor): >125°C and < -40°C

User Guidance/ Installation and Daily Checking Items

5.7. Installation Environment

T300 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.

6.1.1 Devices Installation Environment for Counter Top Usage

The following techniques can be employed to provide for effective screening of the PIN-entry keypad during the PIN entry process:

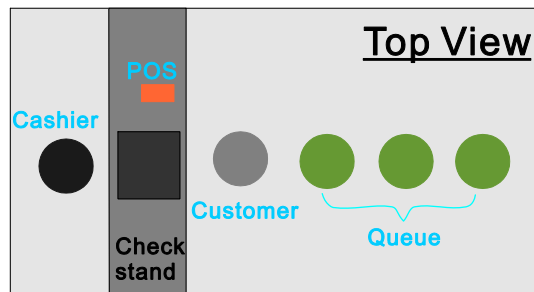
- Positioning of terminal on the cashier counter in such way as to make visual observation of the PIN-entry process infeasible. Examples include:
 - Visual shields designed into the cashier counter. The shields may be solely for shielding purposes, or may be part of the general cashier counter design, for example, used as selling area.
 - Position the device so that it is angled in such a way to make PIN spying difficult.
- Positioning of in-store security cameras such that the PIN-entry keypad is not visible.
- Instructing the cardholder regarding safe PIN-entry. This can be done with a combination of
 - Potentially, literature at the point of sale; and
 - A logo for safe PIN-entry process.

Sample Matrix of Observation Corridors and PIN Protection Methods

Method	Observation Corridors				
	Cashier	Customers in Queue	Customers Elsewhere	On-Site Cameras	Remote Cameras
Privacy Shield	High	High	High	Medium	Medium
Cashier Counter A	Medium	Medium	High	Low	Medium
Cashier Counter B	Medium	High	Medium	Low	High
Customer Instruction	High	High	High	High	High

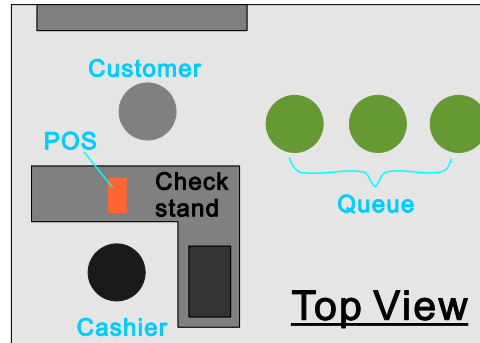


Cashier Counter A





Cashier Counter B



5.8. 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.

5.9. 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 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.

5.10. IC Card Slot Checking

In order to eliminate unauthorized capturing of IC card information, please perform checking every day 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.



5.11. Checking for Tamper Evidence

In order to eliminate unauthorized modification of the terminal unit, please perform the following checking every day. 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)
```

Checking tamper seals on the box and device

Security void label:



Device tamper sticker:



Gift box:



Outer carton box:



5.12. Checking for Overlay Attack

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

5.13. 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].

5.14. 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.