PD/VS

Vanstone Electronic Co., Ltd.

——User manual

A75 Security Policy

MAY. 2021

Version 1.00

Document Revisions

Version	Date	Document Changes
V1.00	2021/05/14	Document created

TABLE OF CONTENTS

1. Instruction

This Security Policy provides guidance for the proper and secure usage of Payment Card Industry (PCI) PIN Transaction Security (PTS) Approved Point of Interaction version 6.0 devices A75.

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.

2. Product Overview

A75 is approved as handheld PED in an attended environment under PCI-PTS 6.0 requirements. The terminal is a new smart payment POS device based on android system, and designed for financial transaction as a hand-held device which consists of large capacity memory, large LCD touch screen with 1280*720 resolution, TF card slot, PSAM card slots, SIM card slots, MSR, ICC reader, CTLS reader, integrated high-speed printer, two high resolution cameras and GPS. Please check whether the appearance of A75 is the same as follow:

Figure 2-1

A75 provide function as much as possible, to meet a variety of application scenarios, user can see the following form:

Function	Description
Barcode	1D barcode
	2D barcode
Wireless communication	2G/3G/4G
	GPS
	WIFI
	Bluetooth
Other communication	USB
Camera	5 Megapixel rear camera
	2 Megapixel front camera

3. Device Identify

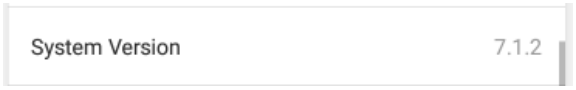
3.1 Identify the approved device

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

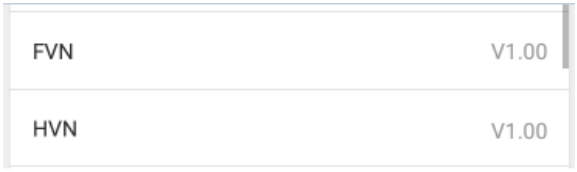
- The device name and type are visible on the label of the device, which should not be modified by anyone after leaving the factory.
- User can check the product label that stick on the back of A75, reading machine type, working voltage and currency, barcode and product number, etc. Please see picture below as an example:

3.2 Version information

To examine the version of the device, we can launch ”Setting”, then “Information”, next “About ”, the version info will be shown below for android:



And hardware, firmware version is also shown below:



The hardware version on the nameplate is affixed to the rear case, and user also can see it from ‘HVN’ item.

4. Secure Guidance

4.1 Secure Use Environment

This device is designed to be used in an attended environment.

Power Supply: 3.6V

Operating Temperature: -20°C - 50°C

Storage Temperature: -20°C - 60°C

Operating Humidity: 0% - 90% noncondensing

Storage Humidity: 0% - 95% noncondensing

Tamper temperature: -35°C-105°C(out of the ranges)

Tamper voltage: 1.82V~3.85V(out of the ranges)

4.2 User Guide

When the device is received, the merchant or user will be informed to inspect before use for a transaction to make sure:

1. The labels covered on screw holes are not broken.
2. The device case has never been opened or destroyed, if doubt, please reject to use it and ask vendor for help.
3. All information such as name, type, and firmware and hardware version of the device meets the requirements of PCI.
4. Power on the device, then please check if any tamper warning message is shown on the screen.

This checking routine is applied to shipment or periodicity checking. Also, a user manual is provided with the device, in which the user will be told how to view the serial number, logo and version and how to use the device securely.

4.3 PIN Entry Guide

A75 is a hand-held device without a privacy shield, and it's recommended that the cardholders should use their body to prevent peeping from their back or their free hand to block the view of keypad during entering PIN. In this way, the numeric area of the keypad will not be seen except the user to make cardholder PIN spying infeasible.

Additionally, acquirer, administrator, and merchants have to make sure to enter their PIN safely.

	Observation Corridors				
Method	Cashier	Customers in Queue	Customers Elsewhere	On-Site Cameras	Remote Cameras
Customer Instruction	Used the body or free hand to block the view of the cashier and the device.	Used the body or free hand to block the view of other customers and device.	Used the body or free hand to block the view of other customers and device.	Do not operate within view of cameras.	Do not operate within view of cameras.

4.4 Device Periodically Checking

The merchant or acquirer must visually inspect the terminal when received via shipping and daily check after the device is deployed to ensure that:

(1) The merchant or acquirer should check that the terminal was not destroyed or installed a suspicious bug. Make sure the 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 screen are consistent with the approved hardware version and firmware version, and user also can see hardware version on the terminal label.

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

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

(6) The merchant or acquirer should check if the ICC reader slot is damaged, such as abrasion, painting and other machining marks, and if there is any suspicious object like lead wire over ICC reader slot, or any unknown object inside IC card. If these suspicious circumstances are found, please stop using the device immediately and contact the vendor to confirm if the device has been tampered. Please refer to section “2.Product Overview” for more information about device appearance.

(7) The merchant or acquirer should check if the MSR slot is damaged, such as abrasion, painting and other machining marks, and if there is any suspicious object like lead wire over MSR slot, or any unknown object. If these suspicious circumstances are found, please stop using the device immediately and contact the vendor to confirm if the device has been tampered.

(8) Check that there is no something overlay on the touchscreen in order to prevent overlay attack.
(9) Check that the device is not in tamper state. Please refer to section “6.1 Tamper trigger events”.

4.5 Decommissioning/Removal

If device leave service temporarily, all sensitive data are kept and protected by battery power supply, no any operations for change state of device are needed.
If device is permanently decommissioned from the service, it can be done by disassembling of device to lead it into tampered status, then any operation of device will be forbidden, and all sensitive data will be erased immediately.

5. Key Management

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

5.1 Key Management Techniques

A75 implements different types of key management techniques:

1) DUKPT: a key management techniques based on a unique key for each transaction as specified in [1].
2) Master Key/ Session Key: a method using a hierarchy of keys. The session keys are unique per transaction as specified in [1].

5.2 Algorithm Support

A75 terminal supports the following secure algorithms:

Algorithm	**Size (BITS)**
SHA256	N/A
TDES	128/192
AES	128/192/256
RSA	2048
ECC	224/256/384/521

5.3 Key Table

A75 terminal key management complies with ANSI X9.24 key management rule strictly. Each key has only one pure and only one value. When the terminal is suffering from attacking, the keys are erased.

RSA public key

Key Name	Purpose/Usage	Algo-rithm	Size(bits)	Storage
CF_PUK	Verify firmware signature of BOOT	RSA	2048	Vendor public key, and stored in OTP area.
MF_PUK	Verify firmware signature of VOS	RSA	2048	Vendor public key, and hardcoded into BOOT.

Symmetric Key

Key Name	Purpose/Usage	Algo-rithm	Size(bits)	Storage
SEK	Encryption for all other keys	AES	256	Secure unit
TLK	KBPK for TMK and DUKPT key loading.	TDES	128/192	Cipher-text in Flash
TMK	KBPK for TPK, TAK,TDK, TEK and TCK key loading.	TDES	128/192	Cipher-text in Flash
TPK	Encryption key for plain-text PIN Block.	TDES	128/192	Cipher-text in Flash
TAK	Encryption key for MAC generation.	TDES	128/192	Cipher-text in Flash
TDK	Decryption key for data.	TDES	128/192	Cipher-text in Flash
TEK	Encryption key for data.	TDES	128/192	Cipher-text in Flash
TCK	Encryption key for account data from MSR, ICCR or CTLS reader.	TDES	192	Cipher-text in Flash
TNK	Encryption key for terminal unique serial number.	TDES	128/192	Cipher-text in Flash
TIK	Initial TDES DUKPT Key for DUKPT Future Key.	TDES	128	Cipher-text in Flash
TLKA	KBPK for TMKA and AES DUKPT key loading.	AES	128/192/256	Cipher-text in Flash

TMKA	KBPK for TPKA, TAKA,TDKA, TEKA and TCKA key loading.	AES	128/192/256	Cipher-text in Flash
TPKA	Encryption key for plain-text PIN Block.	AES	128/192/256	Cipher-text in Flash
TAKA	Encryption key for MAC generation.	AES	128/192/256	Cipher-text in Flash
TDKA	Decryption key for data.	AES	128/192/256	Cipher-text in Flash
TEKA	Encryption key for data.	AES	128/192/256	Cipher-text in Flash
TCKA	Encryption key for account data from MSR, ICCR or CTLS reader.	AES	128/192/256	Cipher-text in Flash
TNKA	Encryption key for terminal unique serial number.	AES	128/192/256	Cipher-text in Flash
TIKA	Initial AES DUKPT Key for DUKPT Derivation Key.	AES	128/192/256	Cipher-text in Flash

5.4 Key Download

A75 terminal can be injected key by KLD, and it doesn't support remote key loading. Dual-control and split knowledge techniques are used to manage the key loading procedure in a secure room of acquirer.

1) Only both administrator A and B input correct password can enter loading process.
2) Initial plain-text loading keys which are divided into two full-length key components should be loaded into the device by two different persons. Each person is required to input his key component into the device separately.

5.5 Key Replacement Policy

Whenever the original 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 or inject the new keys before it can be used as a normal device which can process PIN transaction.

5.6 System Administration

The device uses dual-control technology to protect sensitive services. Only if both of administrator A and administrator B input correct password, sensitive services can be entered and used.

The device is functional when received by the merchant or acquirer and the default passwords for sensitive function management should be changed mandatorily when using this device for the first time.

6. Tamper detection and response

6.1 Tamper trigger events

Any physical penetration will be considered as a tamper event and all the tamper trigger events are shown below:

1) Back case removal.
2) Physical penetration on all the sides of the device.
3) Logical tamper because of improper use (administrator's password error count exceeded and self-test failed, etc.).
4) The temperature goes out of specified ranges(-35°C-105°C).
5) Supply voltage of Button Battery is out of specified ranges(1.82V~3.85V).

6.2 Tamper response

If the device detects tamper event, the tamper mechanisms will activate, all keys and other sensitive data will be cleared and make the device unusable and display the tamper information on the screen.

The operators, merchants and users can easily detect a tampered device when,

- ✓ A warning message is displayed on the screen, and no other reminders to users such as LED, buzzer.
- ✓ The device will go out of service, and no transaction can be performed since keys are cleared.
- ✓ When restarts, the device will display the tamper state on the screen and wait to recover from tamper state.

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.

6.3 Environment Conditions and Environmental Failure Protection

The environmental conditions of operation of the device are specified in chapter 4.1.
The security of the device is not compromised by altering the environmental conditions. Subjecting the device to temperature or operating voltages out of the scope does not alter the security.

7. Software Security

7.1 Software Development Guide

The device provides some secure communication interfaces that complies with PCI standards. The application developer should strictly comply with the development manual. The developer also must accept training course before development activity starting and respect the coding rules and best practices during the whole development stage.

7.2 Software Update

Updates and patches can be loaded in the device. When downloading or updating firmware, software, application, it needs authentication. A75 terminals only accept updates 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. For more update procedure, the user can refer to the <A75 user manual> document.

7.3 Firmware Configuration

The updates and release changes cannot and do not affect the secure configuration of the firmware. The firmware remains in minimal configuration.

7.4 Firmware Authentication

This device implements asymmetric cryptographic algorithm for firmware, software, application authentication. RSA algorithm with 2048bits key is used for signature verification and 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 Vanstone. And the firmware authentication is executed by signature verification using corresponding public key of Vanstone.

Before firmware running every time, their integrity and validation will also be checked. If failed, firmware will not be loaded. In that case, new authorized firmware will be needed to be downloaded into the device.

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

7.5 Self-Checking

The self-checking of device contains following items.

(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 when reading

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 become invalid.

(3) 24 hours check

The device will reboot every 24 hours to re-initialize the RAM. After power on, self-tests is performed to verify validity of firmware and keys. If any error detected, sensitive data will be erased.

8. System Administration

8.1 Configuration Settings

The devices are functional when received by the merchant or acquirer. No security related settings need to be setup by the end user in order to meet security requirements.

8.2 Default Value Update

The administrator's passwords for security sensitive services are forced to be updated at the first time logging on the terminal.

9. Roles and Services

The roles that supported by the terminal are defined as follows.

- Administrators

System sensitive functions, such as change password, key inject, set time and format PED. Only the vendor authorized administrators can access to them under dual control and split knowledge.

- End Users

The end users can process the PIN-based transaction.

10. Development Guidance

A75 implements the necessary security measures and functions to meet PCI security requirements. For payment or other security related applications, we vendor has provided <A75 Application Development Security Guidance> document to the developers, which provides safety-related development guidance such as follows:

- Application development process

- Application development environment
- Coding standards and good practices
- Payment application security standard
- Account data protection

For SRED Module: A75 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 application cannot display any plaintext account data on the screen or output any plaintext account data to network through any communication channel.

For OP Module: SSL protocol is known inherently weak and we vendor has already removed these inherently weak codes. A75 only supports TLS1.2 version which contains higher security. The device doesn't support Bluetooth Low Energy and doesn't support "Just Works" pairing option. The device supports Bluetooth V4.2 security mode 4 level 4. Any insecure communication options are not allowed.

11. 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] A75 User Manual v1.0 – May 2020.

[7] ANSI X9.24-3-2017,Retail Financial Services Symmetric Key Management Part 3: Derived Unique Key Per Transaction.

[8] ASC+X9+TR+31-2018,Interoperable Secure Key Exchange Key Block Specification .