Security Policy for V72 Terminal

V1.02

2019-9-27

VANSTONE CO., LTD

1 Introduction

This document is to provide the basic security policy for Vanstone device, which guides users and developers to use security features properly.
This document complies with the PCI PTS v5.1.

1.1 History

Version	Date	Author	Comment
V1.00	2019-6-24	Vanstone SZ R&D department	Initial version
V1.01	2019-8-23	Vanstone SZ R&D department	Modify description
V1.02	2019-9-27	Vanstone SZ R&D department	Modify description

2 References

[1] X9 TR-31 2010, Interoperable Secure Key Exchange Key Block Specification for Symmetric Algorithms

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

[3] ANSI X9.24 Par2: 2006, Retail Financial Services Symmetric Key Management Part 2: Using Asymmetric Techniques for the Distribution of Symmetric Key

[4] ISO 9564-2, Banking-Personal Identification Number (PIN) management and security Part 2: Approved algorithms for PIN encipher

[5] PCI PTS v5.1

[6] MH1903 datasheet v1.1

[7] NFC Interface MH1608

[8] VTT024QVA03NTP-V1

[9] SZZE20181225

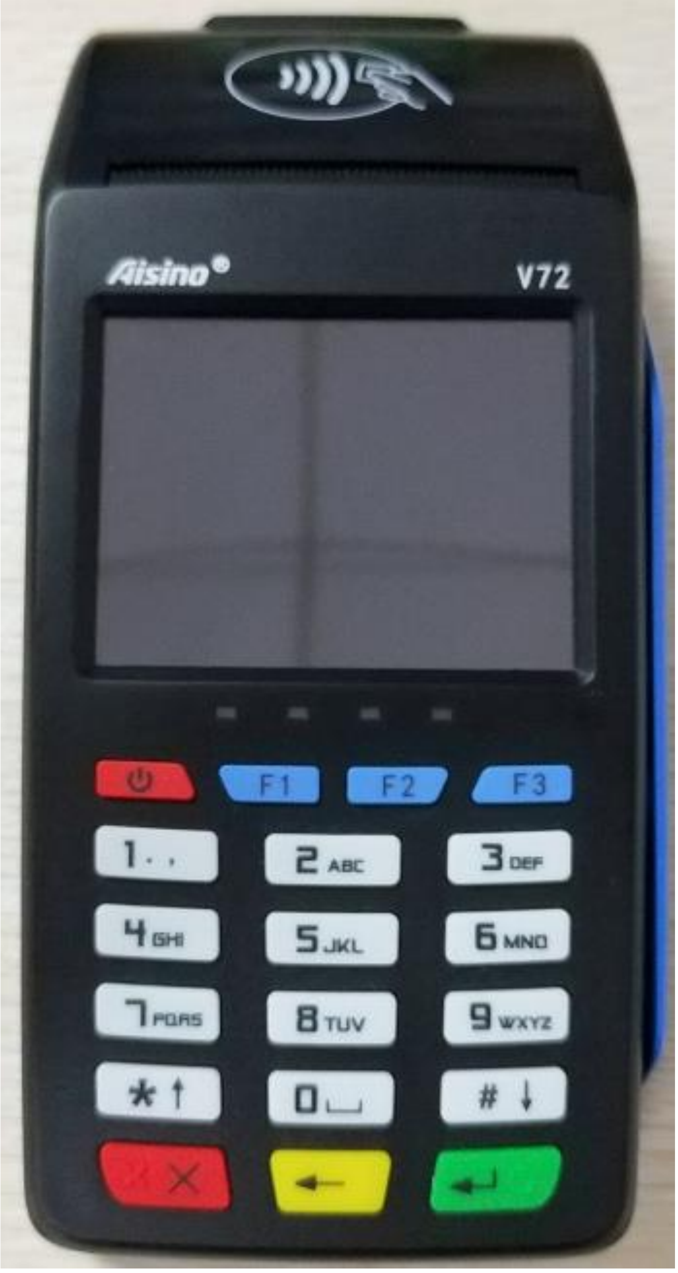
[10] C873 datasheet

3 Product Overview

V72 is a hand-held terminal for financial transactions in an attended environment. Use of the device in an unapproved method will violate the PCI PTS 5.1 approval of the device.

It provides physical keypad, IC card reader (ICCR), security magnetic reader (MSR), display, contactless reader, Printer, USB, GPRS, 3G/4G and Wi-Fi communications.

The communication protocol used include UDP, TCP and TLSv1.2.



Aisino
V72

Aisino
V72

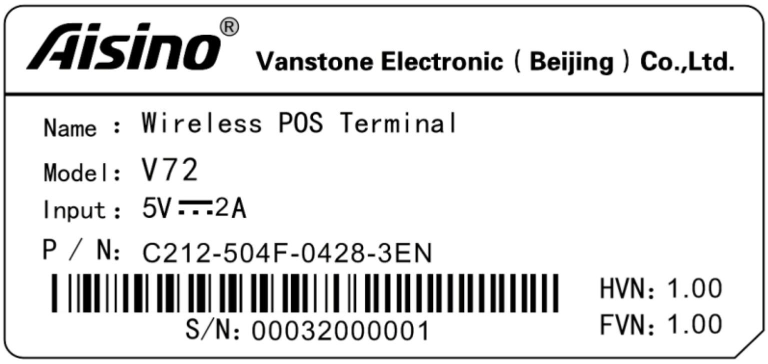
4 Device Identification

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

(1) Press the power button for 3 seconds to power on the device, please see the LED lights up, which indicate that the machine is powered on. Wait for a period of time, it will enter the APP menu.

Press the Cancel button to go to the system menu page, please see the terminal version number and other information.

(2) User can check the product label which is printed machine type, work voltage, barcode, hardware version and product number, etc. Please see below picture as an example:



Aisino® Vanstone Electronic（Beijing）Co.,Ltd.

Name : Wireless POS Terminal

Model: V72

Input: 5V⎓2A

P / N: C212-504F-0428-3EN

S/N: 00032000001

HVN: 1.00

FVN: 1.00

FVN Version：V1.0x.

The ‘x’ stands for non-security related software upgrades. Bug fixed, not related for security.

HVN Version：V1.0x.

The ‘x’ stands for non-security related hardware changes. Component supplier changes.

5 User Guide

The merchant or user will be informed to check if the labels on screw holes are well, if the device case had ever been opened or destroyed, if the IC and MSR reader appear suspiciously. Also, the user will be told how to view the serial number, logo and version. This checking routine is applied for shipment or periodicity check.

5.1 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 manage the sensitive services of device. Only if both administrators input correct password they can access sensitive services include change password, load key, clear key and set RTC time, etc.
2. Normal user. The normal users have no access to sensitive services of device. They can only use device to do normal financial transaction.

5.2 PIN Entry Guide

V72 is a handheld device, 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.

5.3 Secure Use ICC

To ensure the securely of IC card, the merchant must check the product according to below tips.

(1) Check whether the IC card open 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 body block 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 interface is integral. If its surface has traces of

damage, please stop using and inform the manufacture.

5.4 Secure Use MSR

To ensure the securely of MSR, the merchant must check the product according to below tips.

(1) Check whether the MSR guide 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 guide. If yes, please stop using and inform the manufacture.

(4) Check if MSR guide is destroyed. If yes, please stop using and inform the manufacture.

5.5 Device Periodically Check

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

(1) The merchant or acquirer should check that the terminal is 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. Please check if there is any overlay on 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 check the case or the labels in screw holes.

(5) Any suspicious objects internal and ICC slot.

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

6 Key Management

6.1 Algorithm Support

V72 terminal supports the secure algorithm as follow:

Algorithm	Key Length (BITS)	Remark
SHA256	N/A	Integrity verification
3DES	128/192	Data encryption/decryption
AES	128/192	Data encryption/decryption
RSA	2048	Data encryption/decryption, sign and verify sign

6.2 Key Table

The device implements different types of key management techniques:

Fixed Key: a key management technique based on a unique key for each terminal as specified in [3].

Master Key/Session Key: a method using a hierarchy of keys. The session keys are unique per transaction as specified in [3].

DUKPT: a key management technique based on a unique key for each transaction as specified in [3].

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

All keys in these three key management techniques are stored under the protection of key encryption key.

Each key has only one purpose and only one value. When the terminal is suffer from attack, the key are erased, which make the device more security. Please see below the key table in which will describe the key number, key type, key length and the storage status when tamper event happened.

Key Name	Purpose/ Usage	Algorithm	Size(Bits)	Destroyed By	#Slots	Unique to (describe)
SEK	Encryption for all other keys	AES	192	Battery off, and device tampered	1	Device

TLK	KBPK for TMK, fixed, and DUKPT key loading	AES	192/128	When SEK is lost	1	Device
PMK	Encryption of PK and data	AES	192	Battery off, and device tampered	1	Device
TMK	KBPK for TPK, TAK, TDK, TEK and TCK key loading	TDEA/ AES	TDEA :192 AES:128	When SEK is lost	100 X 10	Device
TPK	Encryption key for plaintext PIN Block	TDEA/ AES	TDEA :192 AES:128	When SEK is lost		Device
TAK	Encryption key for MAC generation	TDEA/ AES	TDEA :192 AES:128	When SEK is lost		Device
TDK	Decryption key for data	TDEA/ AES	TDEA :192 AES:128	When SEK is lost		Device
TEK	Encryption key for data	TDEA/ AES	TDEA :192 AES:128	When SEK is lost		Device
TCK	Encryption key for account data from MSR, ICCR or contactless reader.	TDEA/ AES	TDEA :192 AES:128	When SEK is lost		Device
fTPK	Fixed encryption key for plaintext PIN Block	TDEA/ AES	TDEA :192 AES:128	When SEK is lost		Device
fTAK	Fixed Encryption key for MAC generation	TDEA/ AES	TDEA :192 AES:128	When SEK is lost		Device
fTDK	Fixed encryption key for MAC generation	TDEA/ AES	TDEA :192 AES:128	When SEK is lost		Device
fTEK	Fixed decryption key for data	TDEA/ AES	TDEA :192 AES:128	When SEK is lost		Device
fTCK	Fixed encryption key for account data from MSR, ICCR or contactless reader.	TDEA/ AES	TDEA :192 AES:128	When SEK is lost		Device
DUKPT Initial Keys	Unique encryption key for PIN Block or MAC encryption	TDEA/ AES	128	When SEK is lost	10X 10	Device
DUKPT Future Keys	Unique encryption key for PIN Block or MAC encryption	TDEA/ AES	128	Erased after DukptGetPin or DukptGetMac	21 per key	Device

6.3 Key Download

The TLK is downloaded in the sensitive service of the V72 POS terminal, and other work keys are injected through the security PC tool. It doesn’t support remote key loading.
We use dual control and split knowledge to protect the key download function.

For dual control technology, by the two custodians have to enter two dual control passwords through key loader device and then have access to key injection sensitive service to enter two key components of the terminal loading key.

For split knowledge, the two custodians enter a key component, and then the two key components XOR and get the final key. The key conforms to the PCI specification, and both key components cannot be all 0, even if the parity bit is not 0.

6.4 Key Replacement

The key replacement will be required in the follow cases:

1. The original key is known or suspected or stolen.
2. Whenever the time deemed feasible to determine the key by exhaustive attack elapses.
3. The key technology is outdate, or there is already a migration vulnerability.

6.5 Key Removal

After key injection into device successfully, there are two ways to removal the key installed. One is passively erased by firmware or hardware, like a tamper event happened. The other is actively cleared by secure administrator via dedicate tool, like repair on request or decommission event happened.

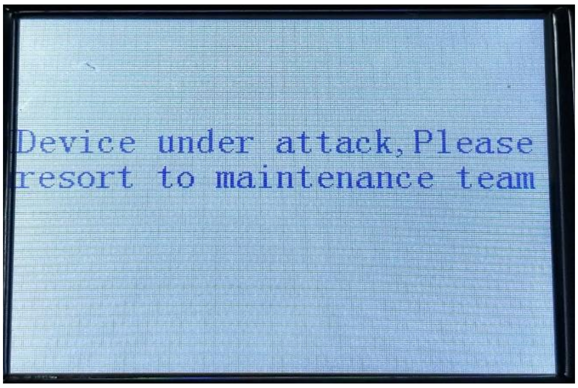
6.6 Sign mechanism

To make ensure the integrity and authenticity of information, V72 POS terminal uses sign mechanism. The algorithms used are RSA and SHA256. The RSA key length is 2048 bits. Firstly, we use SHA256 to calculate the HASH value of the information. Then we use RSA private key to sign this HASH value. At the end, we send out the signed files which have the encrypted HASH value to the original file.

7 Product Hardware Security

7.1 Tamper Response

When the device is triggered, the unlock message will be displayed on the screen and the buzzer will sound.



Device under attack,Please resort to maintenance team

If the device detects tamper event, it will clear the key used to protect other key within the device immediately, and then restart automatically.

7.2 Re-inject Key

After device detects tamper event and restarts, it will be locked. Under locked status, the device can’t run firmware and application until it is unlocked by unlocked tool which is provided by Vanstone. The unlocked tool is managed by Vanstone, other people has no access to the tool. The merchant needs to return the terminal to the factory.

If tamper event occurs, keys will be cleared. In this case, new key must be re-injected to the device before process PIN transaction. For how to inject key please refer to chapter 6.3.

7.3 Environment and Operational Conditions

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

USB Power Supply: 5V

Battery Supply: 3.6V

Operating Temperature: 0°C - 50°C

Storage Temperature: -20°C - 70°C

Tamper temperature: -40°C< or >100°C

Tamper voltage: 1.8V< or >4.1V

Operating Humidity: 10% - 90% noncondensing

Storage Humidity: 5% - 95% noncondensing.

8 Product Software Security

8.1 Software Development Guide

The developer must accept training course before development activity start and respect the code rules and best practices during the whole development stage.

When developed SRED application, the developer must respect the follow guidance:

(1) PAN data that is read from CTLS, MSR and ICC, it must be encrypted at once.

(2) No clear-text account data is outputted.

(3) SRED applications must be signed, and only applications with legal signatures can be downloaded into POS terminal.

When developed applications that use OP module to transmit transaction data, the developer must implement TLS secure protocol to protect the transaction data. SSL is inherently weak and should be removed unless required on an interim basis to facilitate interoperability.

The release process of application is as follow.

(1) Developer developed application, and perform self-test;

(2) Reviewer reviewed source code of application, and outputted a report to detail the issues found. Please note that code reviewer must be performed by a person who was not involved in the authorship of application code;

(3) Tester performed test for application, and outputted a report to detail the issues found. Please note that the tester must be performed by a person who was not involved in the authorship of application code;

(4) If all of above steps found no issues, the review report and test report will be sent to development administrator who will review the reports. If the development administrator confirmed the application is really OK, he will sign and release the application.

8.2 Firmware and Software Update

When download or update firmware or application, it needs authentication.

Before download firmware, each administrator must input his password. Then the download personnel can access the room and use the VANSTONE tool to download firmware or application. V72 POS terminals only accept firmware and software with legitimate and correct signature.

The application and firmware loading process does not need to be protected by any special way other than installation best practices. The device will reject to load and save any unauthenticated application and firmware.

Please note that tampered devices will be locked, and will not allow for software and firmware running even if they are authentic.

The vendor will ensure that after updated firmware the device still comply with PCI security requirements.

8.3 Firmware and Software Authentication

This device implements asymmetric cryptographic algorithm for firmware authentication use. 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 use corresponding public key of Vanstone.

The signature of the application and firmware code are verified. The signature are based on couples of RSA key.

8.4 Self-Check

The self-check of device contains follow items.

(1) Power on check.

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

(2) Check application before install.

Before install an application, its signature will be checked to verify its integrity and legitimacy. Only check successfully, the application can be install.

(3) Check key when read.

When read key, the key will be checked. If detect the key has been modified, all key will be cleared.

(4) 23 hours check

During running time, firmware, application and key are checked every 23 hours to ensure their integrity. Once detect firmware or application or key is modified, the key used to protect other key within the device will be cleared, and device will be locked.

9 System Administration

9.1 Configuration Setting

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.

9.2 Default Value Update

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

When use this device for the first time, the merchant or acquirer needs to download the key. Before download the key, the device will force the default passwords to be changed. The merchant or acquirer must follow the prompts step of the device to complete the password change.

10 Decommission

10.1 Permanent removal

When the device reaches its lifetime or any other reason for no longer use, the device administrator shall remove all the keying material that used to decrypt any sensitive data from the device, ensuring that the device is permanently decommissioned and removed from service. It can be done by directly disassemble the device to make the device tampered.

10.2 Temporary removal

If the device is temporarily decommissioned, all sensitive data are kept and protected by battery power supply, no any operations for change state of device are needed.