Security Policy for V73 Device

V1.03

2021-9-18

VANSTONE ELECTRONIC (BEIJING) 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.
The device is assessed for PCI PTS POI v6.0.

1.1 History

Version	Date	Author	Comment
V1.00	2021-2-24	Vanstone SZ R&D department	Initial version
V1.01	2021-4-23	Vanstone SZ R&D department	Add description
V1.02	2021-7-23	Vanstone SZ R&D department	Add description
V1.03	2021-9-18	Vanstone SZ R&D department	Adjust description

2 References

[1] X9 TR-31 2018, Interoperable Secure Key Exchange Key Block Specification for Symmetric Algorithms
[2] ANSI X9.24-1: Retail Financial Services Symmetric Key Management Part 1: Using Symmetric Techniques
[3] ANSI X9.24 Par2: 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 POI Derived Test Requirements v6.0

3 Product Overview

V73 device is designed for wireless POS terminal which consists of ICCR, CTLS, MSR, physical keypad, scanner and Type C USB.

The device is approved as a handheld PED under PCI PTS V6.0 requirement, and designed to be used in attended environment. Any use of the device in an unapproved method will violate the PCI PTS approval of the device.

Below are the pictures for V73 device with capacitive screen (the hardware version is V174-710-00):

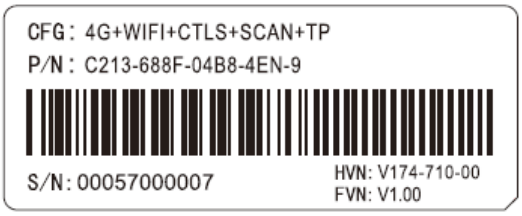

Below are the pictures for V73 device with resistive screen (the hardware version is V173-710-00):

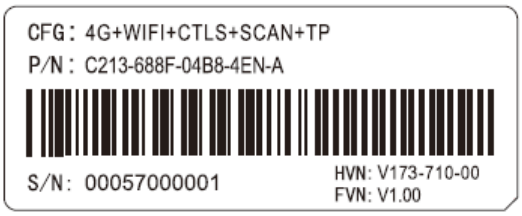
4 Device Identification

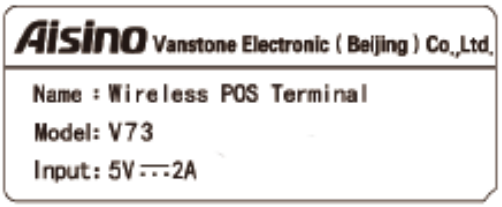
User can identify the approved device through the methods as below:

(1) Power on the device, enter the system menu and select "3. Version" to obtain software and hardware version information.

(2) User can check the product label which is printed with device model, working voltage, barcode, hardware version and product serial number, etc. Please see below picture as an example:







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. Also, the user will be told how to view the serial number, logo and version. This checking routine is applied for shipment or periodic 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 managing the sensitive services of device. Only if both administrators input correct password they can access sensitive services including 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 Privacy Shield and PIN Entry Guide

The device is designed to be used on hand and the device does not contain a privacy shield. We recommended that the user should care to cover the keypad area with his (or her) hands and body during PIN entry.

The following table shows the combinations of methods that must be used when installing the device to protect the cardholder's PIN during PIN entry.

Method	Observation Corridors				
	Cashier	Customer Queue	Customer Elsewhere	On-Site Cameras	Remote Cameras
With Stand	No Action Needed.	Customer positions PED.	No Action Needed.	Do not install within view of cameras.	Do not install within view of cameras.

Without stand	Position unit to face away from the cashier. Use signage to block cashiers view.	Position unit between customer and the next in cue.	Used the body to block the view of other customers and the device.	Do not install within view of cameras.	Do not install 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.

5.3 Secure Use ICC

To make sure IC card being used securely, the merchant will be informed to note the follow cases.

(1) Check whether the IC card 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 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 make sure MSR being used securely, the merchant will be informed to note the following cases.

(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 Checking

The merchant or acquirer must visually inspect the device when received it. The merchant or acquirer should daily inspect the device to ensure that:

(1) The merchant or acquirer should daily check that the device 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 device. Please check if there is any overlay on the device.
(3) Hardware version and firmware version on device 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) The merchant or acquirer should also check that the installation/maintenance operations are performed by a trusted person.
(6) Check the IC card slot refer to the guide of section “5.3 Secure Use ICC”.
(7) Check the MSR refer to the guide of section “5.4 Secure Use MSR”.

6 Key Management

6.1 Algorithm Support

Device supports the secure algorithm as follow:

Algorithm	Key Length (BITS)
SHA256	N/A
TDES	128/192
AES	128/192/256
ECC	256/521
RSA	2048

6.2 Key Table

Two types of key management techniques are supported, including Master/Session key and DUKPT. All keys in these two key management techniques are stored under the protection of key encryption key. Use of the POI with different key-management systems will invalidate any PCI approval of this POI.

- Master/Session Key This method uses a hierarchy of Terminal Loading Key, Master Key and Session Key. The highest level of Terminal Loading Key is distributed through the key loading device. The Master Key is distributed under the protection of Terminal Loading Key. The Session Key is distributed under the protection of Master Key. These keys can be replaced by the same methods whenever compromise is known or suspected.
- DUKPT This method uses a unique key for each transaction, and prevents the disclosure of any past keys used by the transaction-originating device.

Each key has only one purpose and only one value. When the device is suffering from attack, the keys 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	256	Battery off, and device tampered	1	Device
TLK	Protection key for TMK and DUKPT Initial Key loading	AES	128/ 192	When SEK is lost	1	Device
PMK	Encryption key for public keys	AES	192	Battery off, and device tampered	1	Device
TMK	The master key for TPK, TAK, TDK, TEK and TCK key	TDEA/ AES	192/ 128	When SEK is lost	100X 10	Device

TPK	Encryption key for plaintext PIN Block	TDEA/ AES	192/ 128	When SEK is lost	100X 10	Device
TAK	Encryption key for MAC generation	TDEA/ AES	192/ 128	When SEK is lost		Device
TDK	Decryption key for data	TDEA/ AES	192/ 128	When SEK is lost		Device
TEK	Encryption key for data	TDEA/ AES	192/ 128	When SEK is lost		Device
TCK	Encryption key for account data from MSR, ICCR or contactless reader	TDEA/ AES	TDEA: 192 AES: 192/ 128	When SEK is lost		Device
DUKPT Initial Keys	Used to derive DUKPT Future Keys	TDEA	192/ 128	Automatic clearing after derivation of DUKPT Future Keys	10X10	Device
DUKPT Future Keys	Unique encryption key for PIN Block or MAC encryption	TDEA	192/ 128	Erased after encryption	21 per key	Device

6.3 Key Download

The TLK is injected in the sensitive service of the POS device, and other keys are injected through the KLD device. 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 administrators to control the key download, only when the administrator A and administrator B, respectively, enter their own password and password verification are successful, the device can enable the key download function. If the password verification fails five consecutive times, the password function will be locked.
For split knowledge, the two administrators 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 following 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 outdated, or there is already a migration vulnerability.

In these cases, we will ask the merchant to replace or inject the new key before it can be used as a normal device which can process PIN transaction. The new key is injected via high secure channel (secure communication path) and stored by encrypted method.

6.5 Key Removal

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

6.6 Sign mechanism

To make ensure the integrity and authenticity of information, the POS device 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 lock message will be displayed on the screen. No other signal is used to prompt tamper.

If the device detects tamper event, it will clear the key used to protect other keys 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 device 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

Power Supply: DC 5V

Operating Temperature: 0°C ~ 50°C

Storage Temperature: -20°C ~ 70°C

Tamper temperature:

Low：Less than -35°C

High：High than 100°C

Cell battery Tamper voltage

High：3.85V

Low：1.90V

Operating Humidity: 10% ~ 90% noncondensing

Storage Humidity: 5% ~ 95% noncondensing.

7.4 Communication methods and protocols

The device supports USB communication. The device supports USB to virtual serial adapter. USB interface for download, de-trigger function, follow the standard USB protocol.

The device supports Cellular and Wi-Fi communication methods. The device supports Wi-Fi with WPA/WPA2; WEP is not supported.

The device supports TLS v1.2 security protocol for TCP/IP security communication.

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

8 Product Software Security

8.1 Software Development Guide

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

When developing SRED application, the developer must respect the following guidance:

(1) PAN data that is read from CTLS/ICCR/MSR, 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 device.

When developed applications that use OP module to transmit transaction data, the developer should implement TLS v1.2 secure protocol to protect the transaction data. The device support SSL, but 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 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 real OK, he will sign and release the application.

8.2 Firmware and Software Update

When downloading or updating firmware or application, it needs authentication. V73 devices only accept firmware and software with legitimate and correct signature. Legally verified firmware and applications will be required to be placed in the specified directory of the TF card, then through the corresponding TF card interface to download.

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 updating 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 using corresponding public key of Vanstone.
The signature of the application and firmware code are verified. The signature is based on couples of RSA key.

8.4 Self-Checking

The self-checking of device contains following 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 installed.
(3) Check key when reading
When reading key, the key will be checked. If detect the key has been modified, all key will be cleared.
(4) 22 hours check
During running time, firmware, application and key are checked every 22 hours to ensure their integrity. Once detect firmware or application or key is modified, the key used to protect other keys within the device will be cleared, and device will be locked.

8.5 Account Data Protection

The device always provides SRED functionality and doesn't support the disablement (turning off) of SRED functionality. For the SRED module, account data can be encrypted by TDES and AES encryption.
The firmware of device doesn't support whitelisting for the pass-through of clear-text account data.

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 are changed mandatorily when using 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 Decommissioning

If the device service date is expired or the user discovers that the device has been attacked (such as the device has traces of being attacked or the device is connected to an unknown object), the device needs permanent removal for decommissioning. Decommissioning the device causes it to be inoperable. To decommission the device, disassemble it by unscrewing the back thereby causing it to tamper. The tampered device must then be returned to the manufacturer.