VICTORY ELECTRIC VKR 626

Security Policy

Version: 1.1

Content

0. Document change

Version	Author	Date	Description
V1.0	Tangdy	2021-08-30	Initial version
V1.1	Tangdy	2022-01-24	Add the description of Handheld devices in chapter 3.6 and some other supplement.

1. Purpose

This document is to provide a security policy which addresses basic information for users (merchants, acquirers) to use the device in a secure manner, including information on secure feature implementation, key-management details, administrative responsibilities, device functionality, product identification and user guidance. The use of any method not listed in this security policy will invalidate the PCI PTS POI V6.0 approval of the device.

2. General description

2.1 Product name and appearance

Figure 1 shows the appearance of VKR 626.
The product name is visible on the label at the back side. The product name shall not be covered by a sticker or modified by merchant.

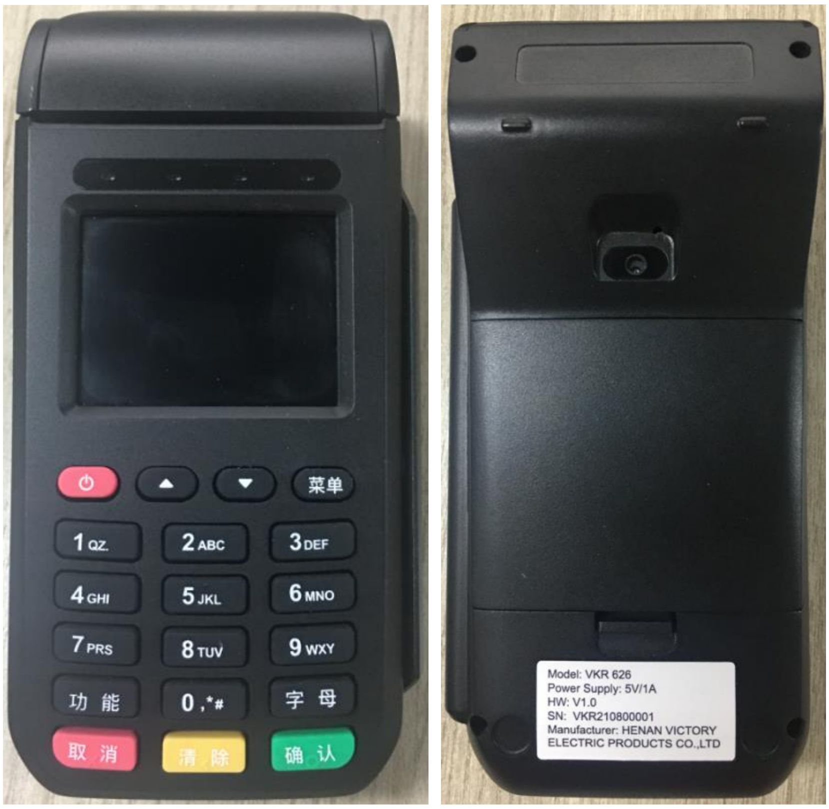


Figure 1 VKR 626

2.2 Product type

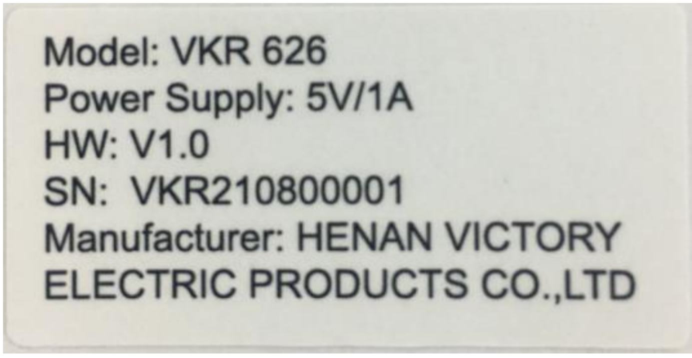
The device is a handheld terminal designed to process online and offline transactions in an attended environment.
It provides display, PIN entry, IC card reader (ICCR), MSR, CLTS, Printer, cellular, WIFI, USB interface.

The approval class of VKR 626 is Stand-alone POS terminal under PCI PTS v6.0 requirement, and it's designed to process financial transactions in an attended environment.
The use of the device in an unapproved method will violate the PCI PTS approval of the device.

2.3 Identification

Hardware Version: V1.0

The product hardware version is visible on the label at the back side of the device (See figure2). The label shall not be taken off, altered or covered in any way.

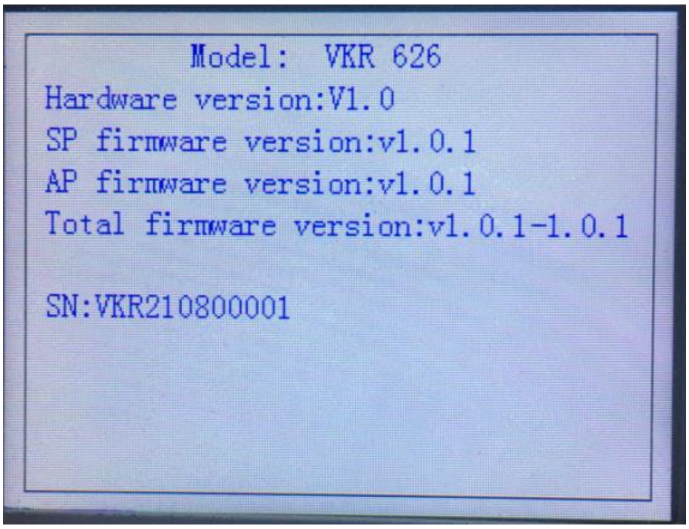


Model: VKR 626
Power Supply: 5V/1A
HW: V1.0
SN: VKR210800001
Manufacturer: HENAN VICTORY
ELECTRIC PRODUCTS CO.,LTD

Figure 2 label

Firmware Version: V1.0.1-1.0.1

The version information can be retrieved with operations below.
1. Power on the device.
2. After the system initializing and automatic self-test, run into the application list.
3. Press the 'MENU' button to enter system menu. Then the screen will show the default system menu.
4. Select "Terminal Info", the version will be shown on screen:
Hardware Version (shown as "Hardware version:" and same as the label at the backside of device)
Firmware Version (shown as "Total firmware version:")
Serial Number:
Select "Terminal Info", the SN will be shown on screen (shown as 'SN:' and same as the label at the backside of device).



```
Model:  VKR 626
Hardware version:V1.0
SP firmware version:v1.0.1
AP firmware version:v1.0.1
Total firmware version:v1.0.1-1.0.1

SN:VKR210800001
```

Figure 3 Terminal Info

3. Installation and user guidance

3.1 Initial inspection

In order to make sure the product received is exactly the same as what is specified, the acquirer or merchant must check the product according to below tips.

1. Check if the origin that providing the VKR 626 device is authorized, if not authorized, please reject.

2. Check if the device's name, firmware, hardware version is meet the approved identification number of PCI PTS POI in the website (www.pcisecuritystandards.org).

3. Check if the appearance of VKR 626 is altered, if found some trace, please reject the device.

4. Check if something overlay on the keypad area in order to prevent overlay attack.

5. Check if the ICC card slot has wire out or something that suspicious, if so, reject the device.

6. Check if the Magcard reader slot has other reader or some bug, if found, reject the device.

To further inspect and use the received device, please check carefully of the following aspect described in the rest of this section.

3.2 Installation

The terminal must be used in an attended environment.
The terminal should be kept away from the direct sunlight, high temperature, humidity or dusty places. The terminal should also be kept away from the complex environment of electromagnetic radiation to prevent interference or damage to the device.

3.3 Environmental conditions

The environmental conditions to operate the device are specified in the below condition.

Working Environment:

Temperature: 0℃～50℃(32°F～122°F)

R.H.: 10%～90%(non-condensing)

Storage Environment:

Temperature:－20℃～70℃(-4°F～158°F)

R.H.:5％～95％ (non-condensing)

Power Supply: DC 5.0V---2A

Environmental protection features:
Temperature sensor: -45±10℃~100±10℃(-49±18℉~203±18℉)

Main voltage sensor: 2.0±0.1V~3.7±0.1V

Failed to comply with the condition above will trigger the device's environmental protection mechanisms.
The security of the device is not compromised by altering the environmental conditions (e.g. place the device outside the stated operating range temperature or operating voltages).

3.4 Communications and security protocols

The device supports Cellular, WIFI communication for transaction purpose.

The device supports USB communication as virtual serial port; one Type C USB Port is provided.

The device supports TLS v1.2 security protocol for TCP/IP security communication, include WIFI (ARP), Cellular (PPP), IP, DHCP client. Mutual authentication is provided by TLS v1.2.

3.5 Configuration settings

The device is configured and set by administrator before deployed in the field, includes the sensitive configuration settings.

No security sensitive configuration settings are necessary to be tuned by the end user to meet security requirements. And also, there is no security default value that needs to be updated by the end user.

3.6 Handheld devices

The device is a handheld device that support SRED encryption.

4. Operation and Maintenance

4.1 Periodic Inspection and maintenance

The user should conduct the following daily inspection:

(1) Inspect the appearance of device to make sure it is the right product.

(2) Inspect whether the IC card reader’s slot has, wire out, untoward obstructions or suspicious objects at the opening;

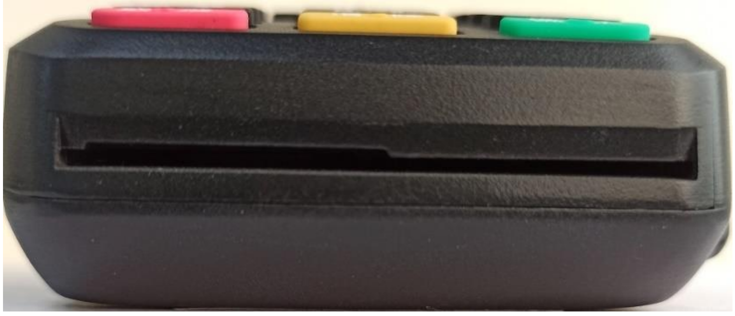


Figure 4 View of the ICC slot

(3) Inspect whether the MSR card slot has an additional card reader and other inserted bugs;

(4) Inspect whether the product appearance has been changed, such as the display, keypad area and so on.

(5) Check if the firmware version is correct.

(6) Observe whether there are any visual observation corridors, and deter them by body or other shields.

(7) Power on the device and check if the firmware runs well. As the start-up will inspect the hardware security, authenticity and integrity of firmware.

Such checks would provide warning of any unauthorized modifications to or substitution of the terminal.

Devices, which are detected as disabled through the system of requirement, must not be used without further investigation of the causes of the tamper. Users are advised to seek technical support from their terminal service partners or directly from Vendor.

4.2 Self-Test

The device will perform self-test upon start-up and every 24 hours. Periodical self-test is done by automatically reboot. This reboot period is count once the device is powered on.

The self-test includes:

- Firmware and application integrity and authenticity check

- Keys correctness check

- Hardware security status check

If any of the above check fails, the device will be disabled in a secure manner. In this case, please contact the supplier center.

4.3 Roles and responsibilities

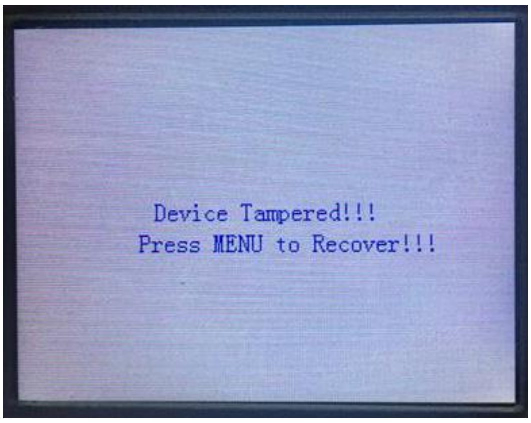
Roles	**Responsibilities**
Vendor	1. Sign customer public key 2.Repair device and unlock the device if tampered
Acquirer	1. Organize the third party to develop application program 2.Download customer public key, master keys, DUKPT initial key and application
End user	Perform transaction

4.4 Passwords and certificates

There is no security related default value that is necessary to be changed before operating the device. The device does not include any certificate for testing purpose after being manufactured.

4.5 Tamper response

In the event of tamper detection, the device will turn into the DISABLED state. The device will therefore be locked and no further secure function can be performed on it.



Device Tampered!!!
Press MENU to Recover!!!

Figure 5 Tamper Prompt

If the device is in tampered state, the user must contact the device maintenance immediately, remove it from service and keep it away from potential illegal investigation.

4.6 Privacy shield

The device is designed to be used on hand therefore the device does not contain a privacy shield. The device is compliant to the character of handheld device as required by PCI_PTS_POI_DTRs_v6 Appendix A 1.2.

The customer should care to cover the key area with his (or her) hands and body during PIN entry. In this way, the keypad area will not be seen except by the user and the PIN is protected from being revealed, as shown in Figure 6.

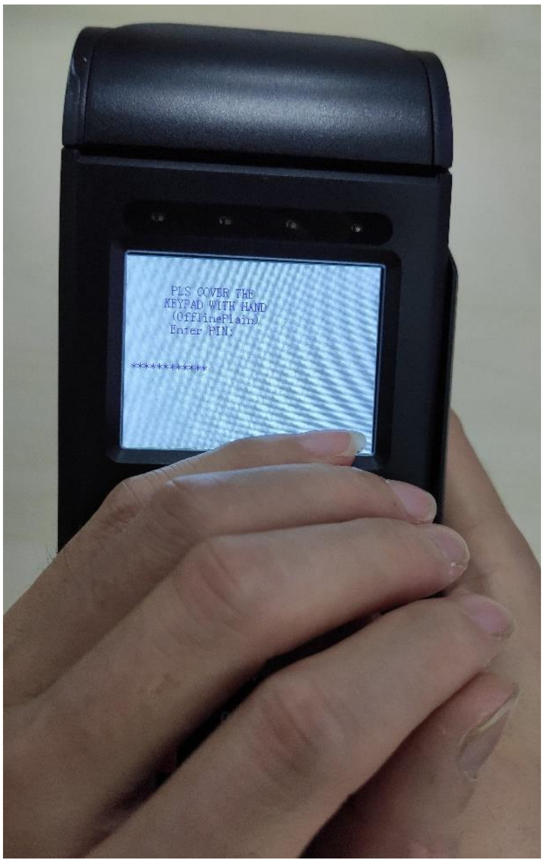


Figure 6 PIN Entry

It is recommended to enter PIN as following ways:

1. Make sure the cardholder hold the device on hand during PIN entry.
2. Make sure the cardholder keeps a distance from others on the check stand.
3. Indicate user to use his body or free hand to block the view of keypad through guidance message or logo.
4. Make sure no video camera towards the keypad.
5. Remind the cardholder to examine if anyone is looking at the keypad before PIN entry.

4.7 Patching and updating

Update and/or patch to the firmware, software can be installed into the device. And local update and/or patch downloading is supported.
Any security related update and/or patch loaded into terminals must be signed using vendor's firmware sign key. If the signature of the update and/or patch cannot be authenticated, the update and/or patch will be rejected and not be installed.
For the secure operation of the device, it is recommended to use the latest versions of the released firmware and software.

4.8 Decommissioning/Removal

Devices destined for permanent decommissioning must undergo a secure decommissioning process before they are finally disposed of, in order to ensure no sensitive information remains in them. Device decommissioning does not require any sensitive tool or service. Terminal administrators shall force a HW tamper condition by opening the casing of the device to ensure no sensitive information is recoverable from the device. Additional best practices, such as explicitly wiping all data in the device may also be implemented in a non-secure area, as they are not based on sensitive services.

For the temporary removal, there is no need to change the state of the device, as all the keys are still protected safely with the main board battery power supply.

5. Security

5.1 Software Development Guidance

The terminals implement the necessary security measures and functions to provide compliance with the PCI security requirements for authenticated applications.

Develop an application base on the device and ensure compliance, please follow the application programming guide and the SDK [2] Linux application programming guide , and the secure software development guide [3] Secure software development guide and OP secure software development guide [4] OP secure software development guide that the VKR provided, prepare the develop environment, install the compiler, refer to the demo and study how to use all the API provided to operate corresponding function module.

The device does not allow unauthorized or unnecessary functions.

5.2 SSL

The device does not support SSL, only TLSv1.2 was implemented.

5.3 Singing

The sign tool provided by VKR is used to sign user application and vendor firmware. The sign tool administrators perform signing process under dual control.
Application and firmware update uses SHA-256 in combination with RSA 2048 bits for authentication and signature verification.

Application is verified by the firmware before it is loaded and executed. If the verification fails, application can't be loaded into device and executed. The signature and verification mechanism ensures the authenticity and integrity of the application that is loaded into device.

5.4 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/AES encryption.
The firmware of device doesn't support white listing for the pass-through of clear-text account data. For more details, please refer to [3] Secure software development guide.

5.5 Algorithms Supported

The device supports the following algorithms:

- TDEA (128 bits/192 bits)
- AES (128 bits/192 bits/256 bits)
- RSA (2048 bits)
- SHA (256 bits)
- ECC (in support with NIST P-256 and P-521)

5.6 Key Management

- **Master/Session key (TDEA/AES)**

This method uses a hierarchy of Master keys and Session Keys.
The Master keys are distributed through key loading device. The Session Keys are distributed under the protection of Master Keys. These keys can be replaced by the same methods whenever compromise is known or suspected.

- **DUKPT (TDEA)**

This method uses a unique key for each transaction, and prevents the disclosure of any past keys used by the transaction-originating device.

The use of the POI with unapproved key management systems may result in incompliance with PCI PTS POI security requirement.

5.7 Key Table

RSA public keys

Key name	**Size(bits)**	**Algorithm**	**Usage**
APP_AUK	2048	RSA	Public key for application authentication
FRW_AUK	2048	RSA	Public key for firmware authentication
RPK（root public key）	2048	RSA	Public key for user public key authentication
Server_AUK	2048	RSA	Public key for server authentication during tamper recovery

Symmetric keys

Key name	**Size(bits)**	**Algorithm**	**Usage**
AES_MMK	256	AES	Used to encrypt/decrypt all other keys stored inside the device’s internal flash
Master Keys (TMK/AES_TMK)	192 256	TDEA AES	To load encrypted session keys
PIN Keys (TPK/AES_TPK)	128/192 128/192/256	TDEA AES	PIN encryption for PINBLOCK format 0,3,4
MAC Keys (TAK/AES_TAK)	128/192 128/192/256	TDEA AES	MAC Calculation and Encryption
Data Keys (TDK/AES_TDK)	128/192 128/192/256	TDEA AES	Transaction Data encryption/decryption
Cardholder Data Keys (TCHDK/AES_TCHDK)	192 128/192/256	TDEA AES	Exclusively used for Account data (PAN) encryption / decryption
DUKPT Initial Keys	128	TDEA	Used as IPEK to derive all DKUPT future keys

5.8 Key Loading

The terminal does not support manual cryptographic key entry.
The terminal supports local key injection by using a SCD under dual control and split knowledge in a secure environment.

5.9 Key Replacement

Whenever the compromise of the key is known or suspected and whenever the time deemed feasible to determine the key by exhaustive attack elapses, the key must be removed or replaced with a new key.

6. Acronyms

Abbreviation	Description
VKR	Vendor VICTORY ELECTRIC’s name
AES	Advanced Encryption Standard
ECC	Elliptical Curve Cryptography
TDEA	Triple Data Encryption Algorithm
SHA	Secure Hash Algorithm
RSA	Rivest-Shamir-Adelman Algorithm
CLTS	Contactless Module
ICC	Integrated Circuit Card
MSR	Magnetic-Stripe Reader
DUKPT	Derived Unique Key Per Transaction
PIN	Personal Identification Number
TLS	Transport Layer Security

7. References

[1] ANS X9.24 - 1: 2017, Retail Financial Services Symmetric Key Management Part 1: Using Symmetric Techniques

[2] Linux application programming guide

[3] Secure software development guide

[4] OP secure software development guide