MOREFUN H9 Security Policy

Production Name: H9

Document Version: 0.1

Contents

1. Document Information

1.1. Evolution Follow-up

Revision	Type of modification	Date
0.1	Document creation	2022-03-15

1.2. Acronyms & Terms

Abbreviation	Description
N/A	Not Applicable
PED	PIN Entry Device
PIN	Personal Identification Number
RSA	Rivest Shamir Adelman Algorithm
TDEA	Triple Data Encryption Algorithm
SHA	Secure Hash Algorithm
MK/SK	Master Key/Session Key
MSR	Magnetic-stripe Reader
ICCR	Integrated-circuit card reader
SRED	Secure Reading and Exchange of Data
DUKPT	Derived Unique Key Per Transaction

1.3. Reference

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

[2] ANS X9.24 Part 2: 2016, Retail Financial Services Symmetric Key Management Part 2: Using Asymmetric Techniques for the Distribution of Symmetric Keys

[3] X9 TR-31 2018, 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] Morefun Security Software Development Lifecycle

[7] H9 Bilingual Manual

[8] OP secure user guidance.docx

1.4. Targeted Readers

This guideline is mainly intended for the following personnel:

- Those who deploy the H9 physical devices at the end-user site

  Execute the deployment of new H9 devices, for instance

  - Firmware update
  - Test before terminal deployment

- Administrator or outlet administrator

  Execute management and on-site guidance, i.e.

  - Key modification
  - Perform routine tests and terminal maintenance

2. Introduction

This Security Policy provides guidance for the proper and secure usage of Payment Card Industry (PCI) Payment Terminal Security (PTS) Approved Point of Interaction version 6.1 devices, such as the H9 terminal.

The security policy applies to all H9 terminals, which is PCI PTS version 6.1 POI approved. Any use of the device in an unapproved method will violate the PCI PTS approval of the device.

3. General Description

3.1. Product Overview

H9, is a handheld Point of Sales (POS) terminal device, which has integrated LCD Screen with physical keypad securities as PIN Entry Device(PED). And it also has integrated USB, Cellular(GPRS), Printer, ICCR, Contactless card reader and MSR reader. The device is used to process credit and PIN-based debit card transactions under an attended environment. This guideline constitutes the main information source of technicians, intended for the administrator and the site administrator to manage and deploy H9 devices.

3.2. Product Inspection

When the device is received via shipping, carefully inspect the shipping carton and its contents for possible tampering or damage.

1. Validate the authenticity of the sender by verifying the shipping tracking number and other information located on the product order paperwork.
2. Remove the H9 unit from the shipping carton.
3. Remove any protective plastic wrap and place the unit on a table or countertop.
4. Remove the clear protective film from the display.
5. Save the shipping carton and packing material for future repacking or moving the device.

3.3. Product Identification

Hardware Version: MF_HW_2.01 Firmware Version: MF_FW_2.01

To verify if your H9 product is PCI approved as a PED (PIN Entry Device), locate the PCI Id entification number at “Admin login->Firmware menu->Firmware Version”.

Go to the PCI Security Standards Council web site (www.pcisecuritystandards.org) and ver ify that the PCI Hardware Version matches the Hardware # on the list of Approved PIN T ransaction Security (PTS) Devices.

Figure 1: H9 Appearance

The product name and hardware version are printed on a label on the device.

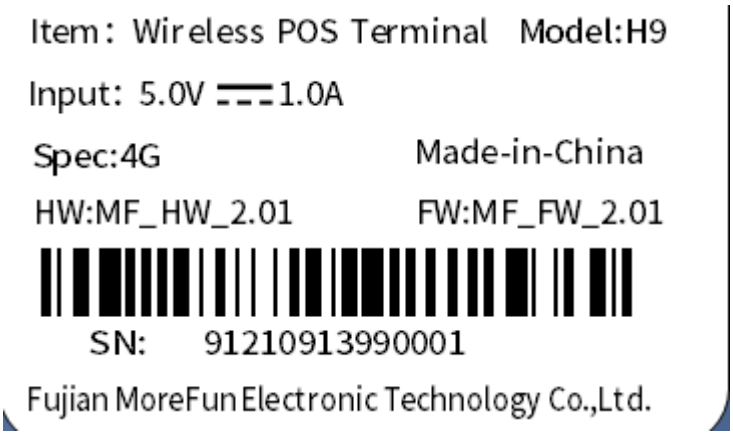


Figure 2: Device Label

4. Guidance

Before use and deployment, please read the [7] first, which introduces the precautions for device safety and use.

4.1. Periodic Inspection

The merchant or acquirer should daily check that the keypad is firmly in place. Such checks would provide warning of any unauthorized modification to the terminal, and other suspicious behavior of the terminal. And ensure that there is no overlay anomaly coverage.

Check daily whether the MSR card slot has an additional card reader and other inserted bugs.

Figure 3:MSR Slot

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

Figure 4: ICC Reader Slot

Check the terminal daily whether it has been tampered. When the terminal is triggered, the device displays a warning that the device is under attack, and without other messages.

Figure 5:Warning under attack

If you find these suspicious circumstances, please stop using the device immediately and notify the security personnel of your company and your local Morefun representative or service provider to confirm if the device has been tampered. Please send back for repair when tampered.

The terminal does not contain parts which can be repaired by users. Do not attempt to disassemble the terminal in any case.

4.2. PIN Confidentiality

The H9 device is a hand-held mobile device without Privacy Shield, and it is required to provide cardholders with the necessary privacy during transactions, especially PIN :

- Take the terminal to the cardholder to enter the password.
- Cover with body or hand when entering the password to prevent the password from being peeped.

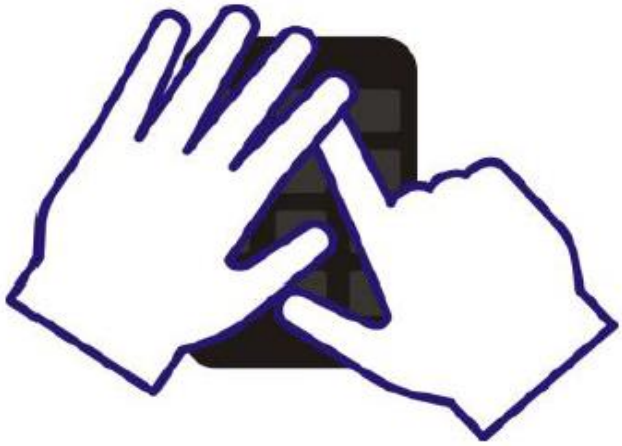


Figure 6: Safe PIN Entry Logo Example

The following table shows the combinations of methods that must be used when installing the terminal 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.

Note: The stand swivels to allow the cardholder to position the PED to optimize their viewing angle. If the stand will be used, you must include prompts in your application directing the cardholder to position the PED strategically to restrict the view of other.

Additionally, you may wish to implement the following to further increase security during PIN entry.

- Offer PIN security literature at the point of sale.
- Use signage to limit the view of the PED to just that of the cardholder.

4.3. Self-Test

The H9 device perform a self-test:

- when a device is powered on
- when the device restarts
- it will restart a self-test automatically every 23 hours

The following components will be tested during a self-test:

- Key field authenticity and integrity
- Tamper inspection
- Firmware authenticity and integrity inspection

During self test, there is no display avoid effecting normal display.

If the result of self test is safety, then complete the self test and no display.

If the result is fault, then prompt that “Figure5:Warning under attack” and the device is forbidden working.

4.4. Decommissioning/Removal

When the device is no longer used for permanent decommissioning reason, the administrator of the device needs to gather the device and then erase all the key materials on it. It can be done by directly dis-assemble the device to make it tampered.

For the temporary removal, there is no need to change the state of the device, as all the keys are still protected safely by the main board hardware tamper mechanism.

4.5. Management Security

- Perform a policy that requires all maintenance technicians accessing your store to log in and use certificates with their respective photos to verify their respective identity, and any technicians performing any work on PIN keypad and/or terminal will be accompanied by the store clerk during any work period.
- Execute a program, i.e. check the serial number of the terminal whenever the device starts or is powered on to ensure the device is not replaced. If the device is replaced, stop using the terminal and notify your Morefun customer relationship manager.
- Inspect the terminal visually every day to ensure that no foreign object is found in the smart card slot; make sure that no wire is led from the smart card slot.
- Develop a default response plan. This identifies the steps to be taken if a suspected violation occurs and who will execute each step. This plan needs the list of all personnel to isolate your payment system and all those who need to be informed. They include your local law enforcement authority, your acquiring bank, your processor, security assessor and your payment system provider.
- Keep track of terminals replaced in every store. Whether they are from the store inventory or sent to the store by maintenance technicians.

5. Product Hardware Security

In hardware security, physical tamper-proofing mechanism is designed that can prevent sensitive data against the leak and detection when the external environmental conditions and the operating conditions change.

When the device is under external attacks, such as drilling, laser, chemical corrosion, being uncovered etc., an attack detection mechanism will be triggered, All keys will be erased. These mechanisms ensure that sensitive data will not be leaked.

Terminal security shall not be affected by changes in environmental conditions. Its power and temperature range shall be within the specification range specified in the user manual. Beyond this range, the operating terminal will trigger tampering events and make the terminal stop executing the transaction and the display will show that the terminal has been tampered.

5.1. Temperature Humidity and Power

The following are the temperature and humidity specifications of H9 device:

- Operating temperature range: 0 ℃ ~ 40 ℃
- Humidity: 10% to 90% range(non-condense)
- Storage temperature range: -20 ℃ ~ 75 ℃
- Storage humidity range: 20% ~ 93% (non-condense)

Subjecting the H9 device to an extreme environmental condition will result in tampering event. Any temperature above 120℃ or below -40℃will result in tampering.

Specification of power supply:

- Battery: 5.0V DC

In addition, if the backup button battery voltage is beyond the range of 2.0 VDC~4.3 VDC, the device will be tampered.

6. Product Firmware Security

Only signed firmware can be updated to the device.

The Cryptographic algorithms utilized for signing are listed as below,

RSA 2048, used for signature verification.

SHA 256, used for calculating hash for data integrity.

The regular self-test mechanism ensures that firmware already downloaded into the device cannot be modified.

6.1. Software Development Guidance

The developer must respect the following security guidance.

- All payment-based firmware must be subject to formal review and security audit before sign-up and use.
- The reviewer must be an eligible individual not related to the author of the POI PED code.
- Code review must be managed by an auditable process that displays the review code with the security test already performed, it requires the sign-up of the personnel who executes code review and security test. Testers shall pay attention to any problematic programs occurring during the code review and security test period.
- Such a review must be subjected to such a review whenever the code changes.
- The firmware review must be performed according to the requirements of the PCI POI PED and the guideline listed in this document.

Authorized firmware must be signed before being published. The sign-up must be performed under the condition of dual control and knowledge segmentation.

Morefun provides Software programming guide to developers to develop applications compliant with PCI security requirement. Please refer to [6] when developing SRED applications.

The device does not allow unauthorized or unnecessary functions.

6.2. Communication Method 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(GPRS) communication methods.

OP applications development:

Development must respect the [8].

The following points need to take attention.

1. The client must authenticate the CA certificate and client certificate.

2. The cipher suite of the server which terminal connects should be as secure as

TLS_RSA_WITH_AES_128_CBC_SHA or more secure.

3. The server which terminal connects should be configured to require Client

Authenticate.

4. The server should disables SSL protocol, and the device does not support SSL. Use TLS v1.2 or higher.

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

6.3. SRED Security

The account data can be protected by MK/SK DEK (Data-encryption Key TDES 192bit or AES 128bit) and DUKPT Future Keys (TDES 192bit). After transaction or time out or other abort, the plain-text account data must be deleted immediately.

The device always provides SRED functionality and doesn't support the disablement (turning off) of SRED functionality.

The firmware of device doesn't support whitelisting for the pass-through of clear-text account data. For more details please refer to [6].

6.4. Vulnerability Detection and Follow-up Action

When new vulnerabilities, threats or bugs are detected via public resource or the customers, Morefun performs analysis to see if the new vulnerabilities, threats or bugs may impact on the H9 security. Morefun contacts PCI lab and gets consulted if there is a delta evaluation is necessary.

- If the vulnerabilities, threats or bugs impact on the H9 security, Morefun immediately informs customers of the vulnerabilities, threats or bugs analysis result via e-mail and send the patch to the customers.
- If Hardware change needs to be involved to fix the issue, customers should return their H9 devices to H9 manufacturing facility for the repair. When a new vulnerability occurs, H9's security team will send a vulnerability notification email to the customers (especially their security managers).
- Bug report contact with Morefun email: support@morefun-et.com

6.5. Firmware Update

When a new firmware version is released, Morefun will send an update notification email with the newly released firmware to the customers. The device supports both local and remote method of Firmware update.

The Procedure of update:

- The device receives the signature file.
- Decrypt the signature by using the corresponding public key, and capture the length and the SHA-256 of code data.
- According to the length, calculate the SHA-256 of code data. If the same, then update the firmware, otherwise discard the firmware and decline to update.

The format of the signature file of the Firmware is below:

256 bytes RSA signature	Code data

The frequency limited:

Only 4 times per hour, and don't exceed 15 minutes per time.

For example, if you download Firmware in 10:00, then you have only 3 times to update Firmware; if 4 times exhaust, you can update firmware until 11:00.

7. Key Management

H9 support the following key management methods:

- Master/Session Key

This method uses a hierarchy of Master Key and Session Key. The master key is distributed with 2 key components, then injected comply the principles of dual control and split knowledge. 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.

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

7.1. Cryptographic Algorithms

The device includes the following algorithms:

1. RSA(Signature verification, 2048 bits)

2. SHA-256

3. Triple DES

4. AES

5. ECC(in support with NIST P-256 and P-521)

7.2. Key Table

All keys store in the PED and the detail please refer to the key table.

Key name	Size (Bits)	Algorism	Purpose/ Usage	Store
MK/SK MK(Master Key)	192	TDES	Encryption of MK/SK PEK,MACEK,DEK	Manually entered into the TOE in 2 plain-text components Stored in cipher-text enciphered under the Root Key in flash
	128	AES		
MK/SK	192	TDES	PIN encipherment	Injected into the TOE in

PEK(PIN-encryption Key)	128	AES	for online PIN	cipher-text Stored in cipher-text enciphered under the Root Key in flash
MK/SK MACEK(MAC-encryption Key)	192	TDES	Message authentication	Injected into the TOE in cipher-text Stored in cipher-text enciphered under the Root Key in flash
	128	AES		
MK/SK DEK(Data-encryption Key)	192	TDES	Encryption of SRED Data	Injected into the TOE in cipher-text Stored in cipher-text enciphered under the Root Key in flash
	128	AES		
DUKPT IPEK	128	TDEA	Derive DUKPT future keys	Manually entered into the TOE in 2 plain-text components Delete after generating future keys
DUKPT Future keys	128	TDEA	Encrypt transaction data under DUKPT scheme	Derived from IPEK. Updated each time KSN is increased Stored in the SP internal Flash, encrypted by Root Key
APP_PUK	2048	RSA	Application authentication	AP internal flash
APP_OTA_PUK	2048	RSA	APP OTA package authentication	AP internal flash
FW_OTA_PUK	2048	RSA	Firmware OTA package authentication	AP internal flash
AP_PUK(AP Firmware Public Key)	2048	RSA	AP firmware authentication	SP internal flash

SP_PUK(SP Firmware Public Key)	2048	RSA	SP firmware authentication	SP internal flash
AP_ABI_PUK	2048	RSA	Authentication of ap boot1 image	SP internal flash
SP_SBI_PUK(SP Secure Boot Image Public Key)	2048	RSA	SP Secure Boot Image authentication	SP OTP
Root Key	192	AES	Encrypt keys	Stored plaintext in the SP CPU internal Battery-backed 512bits Secure Memory

7.3. Key Loading Policy

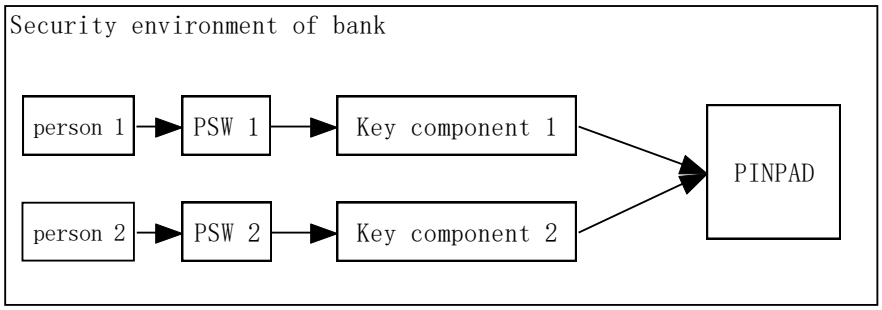
The key-loading techniques supported by the device fall into the following two categories.

- Clear-text key components through the keypad (MK/SK MK (Master Key), DUKPT IPEK),
- Symmetric encrypted keys injection (MK/SK PEK (PIN-encryption Key), MK/SK MACEK (MAC-encryption Key),MK/SK DEK(DATA-encryption Key)).

Manual key loading comply the principles of dual control and split knowledge.

Input key components from keypad Input two key components then XOR result in PINPAD. Before any key component input, you must input the corresponding PSW (password) and pass the password authentication. If input the PSW firstly, the value will be stored for the next authentication.

Please refer to the following figure:



method 1

When the device leaves the manufacture, all keys field are empty. The firmware can't export any key value, only support setup and use key. It will be unsuccessful if any downloaded key is the same to the existed key in the PINPAD.

- Key injection and management must be performed in a safe manner.
- Key component password, and other credentials must be managed under dual control and knowledge split to ensure that no one can use two credentials at the same time.
- Key management security objectives must comply with the PCI PIN transaction security requirements.
- Use of different key-management system than supported by the TOE will invalidate any PCI approval of this POI.
- Key exchange must be performed based on knowing all passwords or sensitive information or a suspected compromise.

7.4. Key Replacement

Any keys should be replaced with a new key value 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.

8. System Administration

8.1. Configuration Settings

The security functions are an inherent part of firmware functions. No security sensitive configuration settings are necessary to be tuned by the end user in order to meet security requirements.

8.2. Default Value Update

The device does not include any certificate for testing purpose after being manufactured.

There are two PSW – PSW1 and PSW2, which must be managed under dual control and split knowledge. PSW1 controls the key component 1 input, PSW2 controls the key component 2 input in the same key field. The default value of both PSW is all zeros, and is enforced to be re-set a valid PSW before first time using.

PSW modifying at “Settings->Set PSW”. The process must be in turn of Old PSW1> New PSW1> Old PSW2>New PSW2 , the PSW only be checked and modified after finishing the complete process, then the new value will be stored for the next verification. The new PSW cannot be the same to the old PSW and default PSW. There are five times limits for the PSW input, if wrong input over five times, the device will never access of key injection.

9. Roles and Services

The customers of MOREFUN are acquirer or Value Added Resellers (VAR). We also refer to VAR as acquirer directly. MOREFUN sells devices to VAR and provide technique and maintenance supports to VAR. VAR sells the devices to end users and provides services to their end user. MOREFUN，VAR and end users play different roles in operating the device. Below table shows different roles and operations:

	Role	Operation
VAR	Administrator	1.Change the default control password 2.Perform Key Loading 3.Perform firmware update
End user	Operator	Perform transaction
MOREFUN	Maintainer	1.Sign firmware 2.Repair device and unlock the device if tampered