P63 Security Policy

Version	Author	Date	Description
V1.0	Leon	2019/03/30	Create

Table of Contents

1. Purpose

This document describes the security policy which addresses the proper use of P63 in a secure fashion including information on key-management responsibilities, administrative responsibilities, device functionality, identification and environmental requirements. Use of the device in an unapproved method will violate the PCI PTS V5.1 approval of the device.

2.General Description

2.1 Product Name: P63.

Figure 1: P63 appearance

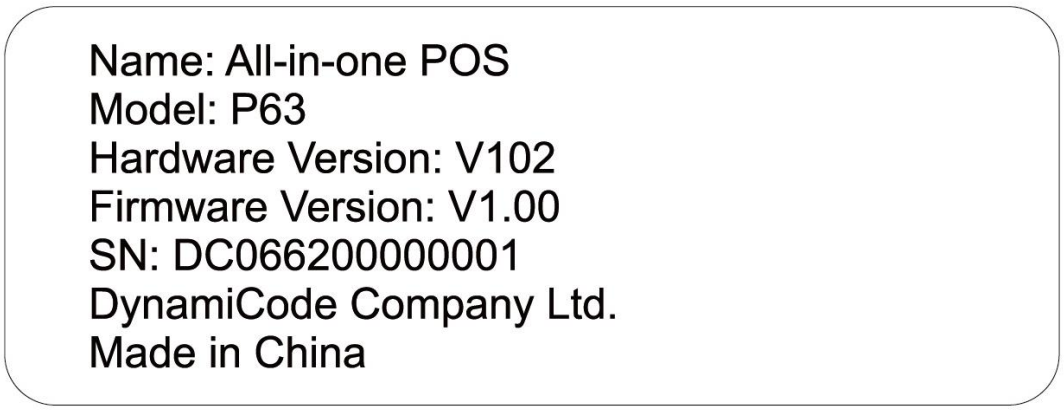

Figure 2: Label

2.2 Product Type:

P63 is a handheld payment device, which supports PIN entry, MAC calculation, and contact/contactless/magnetic stripe card transaction. The device supports Serial port (through USB connector) and 2G module for communication interfaces, and it is forbidden to be used in an unattended environment. Use with any method not listed in this document or put the device in an unattended environment will violate the PCI PTS approval of the device. The firmware system configurations are minimal and necessary to meet the security requirement. P63 is assessed for PTS POI v5.1. This product is mainly for indoor usage, and its target merchants are the restaurants, entertainment, chain stores, supermarkets, E-commerce and so on.

2.3 Identification:

Hardware version

Product model and hardware version are printed on a label attached on the back of the device as Figure 2 shows. The label should not be tore, covered or altered.

The Firmware version can be checked following steps below,

1. Power up P63 and get the main menu.
2. Press button '4' in the device keyboard to enter information mode.
3. You can see the Security Firmware version, as Figure 3

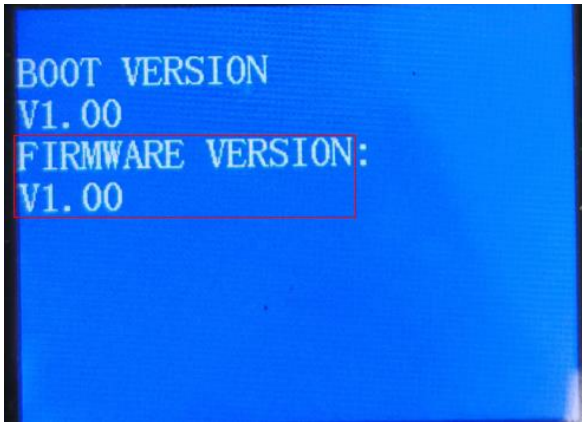

Figure 3: firmware version

3.Installation and User Guidance

3.1 Initial Inspection

The P63 is designed to be portable. When received via

shipping, the receiver must inspect the terminal following the procedures described in the vendor-provided guide documents.

An installation guide including the following information is provided with the device:

A. Equipment check list:

1) Device

2) Cable

3) Documents

B. Power supply and cable connected method information and the main characteristics of the device (i.e. temperature, humidity, voltage)

C. Security recommendations

D. Troubleshoot information of the device if it does not work.

Before installation, receiver should power on the device and check the information on LCD display to see if the device is tampered. If tampered, receiver should contact with the authorized service and reject the device if find any sign that the appearance of P63 is altered.

3.2 Installation

An installation guide including the following information is

provided with the device:

Equipment check list:

1) Device

2) Cable

3) Documents

All software is installed before delivering to end users. User can complete transaction with PIN entry normally.

3.3 Environment Conditions

Device is designed to be used in attended environment.

Operation Temperature: -10℃--+50℃

Operation Humidity: 10%--93%

Storage Temperature: -20℃--+70℃

Storage Humidity: 5%--95%

Power supply: DC 5V/0.5A

The security of device is not compromised by altering environmental conditions.

Device should be used in a safe environment including following features:

The trigger temperature of device: < -30℃ or > 90 ℃.

The trigger voltage for back up battery of the device: < 1.9V or > 3.7V.

Device will be tampered if any of above environmental conditions is out of range.

3.4 Communication and Security Protocols

The communication interfaces and protocols used by the device are shown in Table 1.

Interface	Protocol
2G Module	TCP/IP/ARP/TLS V1.2.
Micro USB Port	Provide serial port function， the interface is used for firmware/ application / prompts /keys download.

Table 1: communication interfaces

3.5 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 Device

As the handheld device, P63 does not support SRED. For this reason, no system is implemented to connect to a tablet or

mobile phone, and any such use will violate the approval of the device.

4.Operation and Maintenance

4.1 Routine examination

The merchant/acquirer must visually inspect the terminal device every day. Key points are listed below:

1. Inspect whether the IC card reader's slot has untoward obstructions or suspicious objects at the opening.
2. Inspect whether the MSR card slot has bypass magnetic head or other inserted bugs.
3. Inspect the product appearance to see whether it has been changed or any tamper evidence exists.
4. Power on the device, check if the firmware runs well. The self-test procedures every time it starts with will inspect the hardware, authenticity and integrity of firmware. Such checks will provide warning if find any unauthorized modifications and substitution of the terminal, or any suspicious behavior trying to get access to the terminal.
5. Check if firmware version is correct.
6. In order to prevent overlay attack, Please Check if any

external abnormal overlays put on the keyboard.

4.2 ICC checking guide

Before inserting card into ICCR, the device's status must be checked daily in bright environment, referring to the suggested steps below:

1. First check outer casing to ensure it is a normal product. It should have no modifications, no damage, no adhesive and no evidence of cutting ;
2. Check the card slot, there should be no suspicious wires connected to ICCR inside.
3. No shim should exist in the ICC slot.
4. When inserting card should meet no resistance or feel any loosing.
5. Card inserting direction is parallel with LCD plane.
6. If a card could not be inserted or could not reach the innermost of the card slot, unauthorized modification or substitution may occurs to the terminal.

4.3 Self-Test

P63 uses self-test to check firmware authenticity.

The self-test is performed:

1. Every time the device is powered up.

2. At least once every 24 hours.

P63 performs a complete self-test which includes P63 BOOT, P63 Firmware, P63 Application, stored keys, authenticity and any other sensitive properties tests to check whether the device is in a compromised state. If the result is fail, the device displays the tamper information on screen and it stops working in a secure manner. When the device goes to the "Compromised" mode, all the stored keys are removed as well. The merchant must return the device to DynamiCode for the repairing. Operators are not able to initiate the self-test.

RTC setting does not influence the periodic of self-test, because the self-test period depends on sys-tick interrupt.

4.4 Roles and Responsibilities

The customers of DC (DynamiCode Co.) are acquirers. DC sells devices to acquirers and provides technical support. Acquirer sells the devices to end users and provides services to them.

DC, acquirers and end users play different roles in operating the device. Table below shows the different roles and

operations:

Name Role Operation

Role		Operation
Acquirer	Administrator	The acquirer develops an application to call system SVC API to access sensitive data or perform sensitive service. This application controls the device to complete card reading, MAC calculation, PIN encryption, etc.
End user	Operator	Perform transaction
DC	Maintainer	1. Sign firmware in KMM and perform initial loading. 2. Sign customer public key. 3. Repair devices and unlock the device if tampered.

Table 2: Role and related operations

4.5 Passwords and Certificates

No passwords are used in the device, but there exist two sets of Certificates, Device certificate and CA certificate. These certificates are used for TLS communication.

When manufacturing in factory, P63 will upload device CSR to DynamiCode Server. After signed by DynamiCode Server, P63 will download Device certificate and CA certificate.

4.6 Tamper Response

The device contains tamper mechanism. In the event of tamper detection, the device will enter disable state. In the tampered/disabled state, the device clears the SEK and secret keys, and displays a warning message. Further use of the device is not possible. In the tamper event, the device will only display 'device tampered!' message without any other tamper warning. The following information could be seen on LCD display as Figure 4.

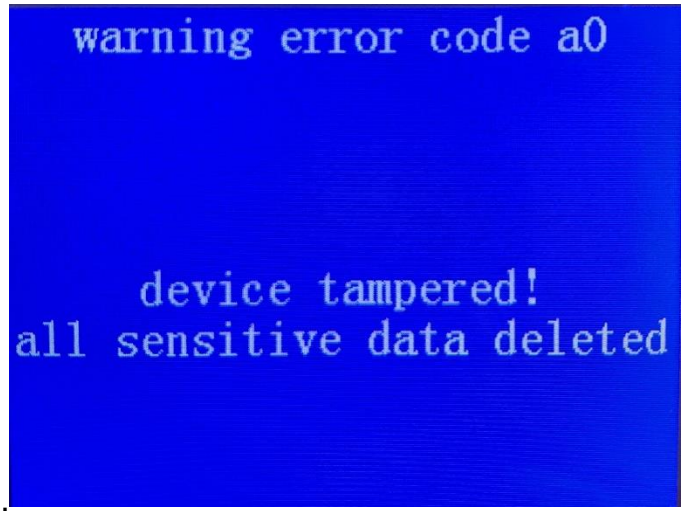

Figure 4: Tamper screen

When the device is in the tampered/disabled state, user should report to the terminal service partners or contact

manufacturer immediately.

4.7 Privacy Shield

When the user is going to enter the PIN, he (or she) will be told to follow security rules to protect this procedure. Security rules for this operation list as follows. User should cover the keypad area and LCD display with one of his (or her) hands during PIN entering.

In this way, the number area will not be observed by someone other than user. This can protect the user's PIN from leaking to others.

The vendor has added customer instructions into the cardholder user manual to instruct cardholder how to use another hand to prevent their PIN entering procedure from any directions.

Figure 5:

4.8 Patching and Updating

The device supports firmware updating through serial port by USB interface. A signature mechanism is introduced to check the authenticity of updating.

When the vendor releases a new version of software, the corresponding signature key must be used to sign the software bin file.

The device can be updated only after the dual control verification is passed. When download the software into

device, both binary file and signature file will be downloaded into device. The firmware download procedure is controlled by P63 BOOT. After downloading the binary file and signature file, P63 BOOT will check the integrity and legitimacy of the firmware, legal to save and illegal to refuse.

4.9 Decommissioning/Removal Detection

The device's lifetime is about five years. When the device is broken in the warranty period, it can be sent back to vendor for repair. If a device is used over five years, or it needs updating for some reason, a new device is required to replace the old one. Under this circumstance, the old device should be recycled in an environmentally friendly way.

Before the old device is abandoned, the sensitive information stored in the device should be cleared by unscrewing the casing of the device intentionally.

When the device requires temporary removal, there is no need to change the state of the device, as all the keys are still protected safely.

5.Security

5.1 Software Development Guidance

The application has no right to access any sensitive resource of device. If application wants to access sensitive data or performs sensitive service, it must call firmware SVC API.

To develop a firmware program which interfaces to the device, one must follow the steps as below:

Before trying to develop a program base on the device, one should read the firmware programming manual and the secure software development guide provided by vendor, 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.

After finishing the firmware/application development, the developer must submit the source code to the server and inform the software manager who will check and review the code according to the code review process to make sure no bug exists.

Then the developer should compile and build the firmware/applications and release it to test department until no problem is reported. Finally, a director will confirm the test

result, and the final version will be released by test department. Before loading the firmware/applications into device, the KMM must be used to sign the firmware or applications. After signing the firmware or applications by KMM, both the binary file and the signature file will be downloaded into the device. Only legal firmware or applications can be saved in device and run smoothly.

If a device in user's hand requires a new version of firmware, the device can be returned to vendor to make this updating. The steps list as follows:

Step	Description
1	Vendor releases a new version of firmware. vendor creates the signature for it.
2	Acquirer receives the notification of the updating and return devices to vendor.
3	Vendor receives the devices, collects them in the secure room by authorized person and downloads the new version firmware to the devices with a PC tool.
4	After completing download procedure for all the devices successfully, a full test will be done for the device. Then the devices will be sent back to the

	acquirer.

5.2 Signing

Boot/firmware/application run on P63 must be signed by legal signature key. The algorithms used in software authentication are RSA2048 & SHA256 algorithms.

MH1902 BOOT is integrated in SP's ROM area when SP is manufactured. DC_BOOT_PUK will be downloaded into SP's OTP which used to verify P63 BOOT's signature.

The KMM generates the signature for the P63 BOOT. P63 BOOT is signed with DC_BOOT_PVK by KMM. When the MH1902 BOOT starts, it uses DC_BOOT_PUK to verify the signature of P63 BOOT which is signed by DC_BOOT_PVK. MH1902 BOOT will start to run P63 BOOT only when the boot signature verification succeeds.

The KMM also generates the signature for P63 Firmware. P63 Firmware is signed with DC_FIRMWARE_PVK by KMM. When P63 BOOT starts, it uses DC_FIRMWARE_PUK to verify the signature of Firmware which is signed by DC_FIRMWARE_PVK. P63 BOOT will start to run P63 Firmware only when the firmware signature verification succeeds.

The KMM also generates the signature for P63 Application.

P63 Application is signed with ACQUIRER_APP_PVK by KMM. When P63 Firmware starts and operator select the application run on P63, firmware will use ACQUIRER_APP_PUK to verify the signature of P63 Application. P63 Firmware will start to run P63 Application only when the application signature verification succeeds.

5.3 Algorithms Supported

RSA2048

TDES128/TDES192

SHA256

AES256/AES128

5.4 Key Management

The device supports two key management methodologies,

1) MK/SK key (MK, PEK, MAK)

The technique based on a hierarchy of keys. Master Key is directly used to encrypt Session Keys.

2) Fixed Key (PEK_AES)

PEK_AES is unique for per terminal.

Note that use of other key management methods will violate the PCI PTS approval of the device.

The device supports 20 slots for symmetric keys.

Key generation:

The firmware signature keys and symmetric keys downloaded into P63 are generated or established (injected) by the KMM and saved in the KMM. The KMM will be placed in vendor and acquirer secure room where only authorized person can enter in and execute the step of key loading. The operation is under dual control management process, two administrators needed.

Keys in the device:

KEY TYPE	**Generate Method**	**Saving Mode**	**Saving Memory**
SEK	Generated by device TRNG	Plain Text	BPK area of MH1902.
TLK	Generated by acquirer	Encrypted by SEK.	Flash of MH1902
MK	Generated by acquirer	Encrypted by SEK.	Flash of MH1902
PEK	Generated by acquirer	Encrypted by SEK.	Flash of MH1902
PEK_AES	Generated by acquirer	Encrypted by SEK.	Flash of MH1902

MAK	Generated by acquirer	Encrypted by SEK.	Flash of MH1902

Table 3: Key Table

5.5 Key Loading

About key loading, the KMM is used to download keys (including TLK, MK, PEK, MAK and PEK_AES) into device under dual control process in secure room. The KMM was placed in secure room where only administrators have the authority to enter. When devices need loading keys, the administrators take them into secure room. Before using the KMM to download keys into devices, the administrators will need to login the system with right passwords.

Key saving

All symmetric keys of P63 will be saved inMH1902 Flash with cipher text form encrypted by SEK. Different kinds of keys with different values are saved in separately sector. All keys saved in the Flash of MH1902 are encrypted by SEK.

Key usage

The firmware signature keys are used to verify the integrity and legitimacy of firmware. The master keys are used to decrypt the work keys during key loading. The work keys are

used to encrypt PIN and calculate MAC value. For example, the PEK is used to encrypt the PIN data.

5.6 Key Replacement

Since the crack technique improves with time goes by, present key management method may not be secure at the all times. That's why the keys saved in the device must have a life cycle. One year is a usual life time for symmetric master keys used in device.

In another case, once the keys are known or suspected to be compromised, they must be replaced immediately.

New keys are from external selection, key index and key type must be specified. Only keys with the same index can replace each other.

5.7 SSL/TLS

The mbedTLS is customized by DynamiCode and all weak cipher suits are removed from device. P63 only supports the cipher suits as below:

TLS-RSA-WITH-AES-256-GCM-SHA256
TLS-RSA-WITH-AES-256-GCM-SHA384

Table 4: cipher suits

6. Acronyms

DC - DynamiCode Company Limited

AES - Advanced Encryption Standard

DES - Data Encryption Standard

IC - Integrated Circuit

LCD - Liquid Crystal Display

MAC - Message Authentication Codes

MSR - Magnetic Security Reader

OTA - Over-the-Air Technology

PAN - Primary Account Number

PCI - Payment Card Industry

PIN - Personal Identification Number

POI - Point of Interaction

PTS - PIN Transaction Security

MAC - encryption Key

TDEA - Triple Data Encryption Algorithm

TDES - Triple Data Encryption Standard

KMM - Key Management Machine

SVC - Supervisor Call

CSR – Certificate Signing Request