C90 Financial POS Security Policy

FILE NAME	**C90 Financial POS Security Policy**		
CLASS	PUBLIC	FILE NO.	S-PO-A001

No	VER	DATE	REVISION	AUTHOR	AUDITOR
1	V1.00	2021-06-10	Initial release	CYQ	GHZ
2	V1.01	2021-08-19	Fix known problems	CYQ	GHZ
3	V1.02	2021-09-27	Add a description of Key Loading Policy	CYQ	GHZ
4	V1.03	2021-11-08	Update pictures and labels	CYQ	GHZ
5	V1.04	2021-11-24	Modify the time description of self-test and some description.	CYQ	GHZ
6	V1.05	2022-04-14	Modify the content of table in section "1.1 Product Overview".	CYQ	GHZ

Contents

Abstract

This document is used to guide users and developers utilizing the security features more properly.

This document complies with the current security standards. Use of the device in an unapproved method will violate the PCI PTS v6.0 approval of the device.

Reference

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

[2] ANSI X9.24 Par2: 2016, Retail Financial Services Symmetric Key Management Part 2: Using Asymmetric Techniques for the Distribution of Symmetric Keys

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

[4] C90 Financial POS Terminal Logical Security Specification V1.00.docx

[5] Software Development Control Program

[6] Firmware Development Coding Rules Specification

[7] C90 Financial POS terminal Open Protocol Security Specification V1.00

[8] ASC+X9+TR+31-2018

1 Introduction

1.1 Product Overview

C90 POS device is approved as handheld PED device and used in an attended environment. It provides the functions listed in the following table. The evaluated version of the terminal is PCI PTS v6.0.

Function configuration can be found:

Configuration	Function
Card	IC card
	CTLS
	MSR
Scanner	Scan 1D barcode
	Scan 2D barcode
Touch Screen	Not for PIN entry For non-security related operation
LCD	LCD 2.8 inch for display
Communication	Cellular (2G/3G/4G)
	Bluetooth
	Wi-Fi
	Micro USB
Printer	Thermal Printer
Keypad	Physical Keypad

The pictures are shown as below:

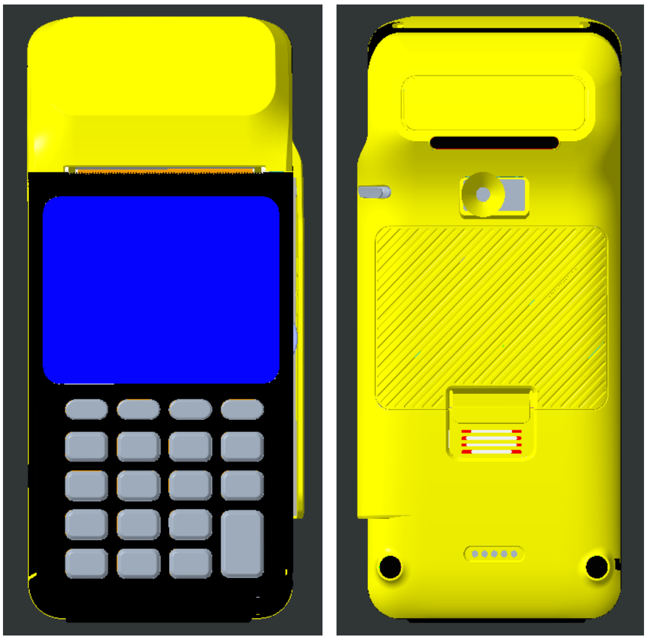


Figure 1.1 – C90 Front and back

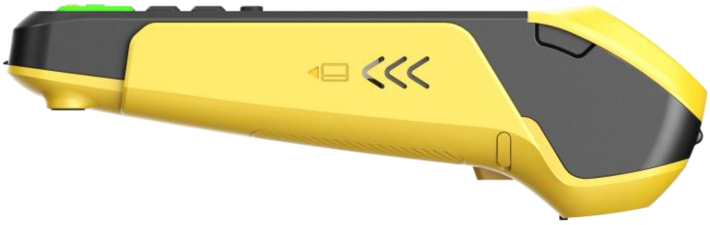


Figure 1.2 – C90 Side

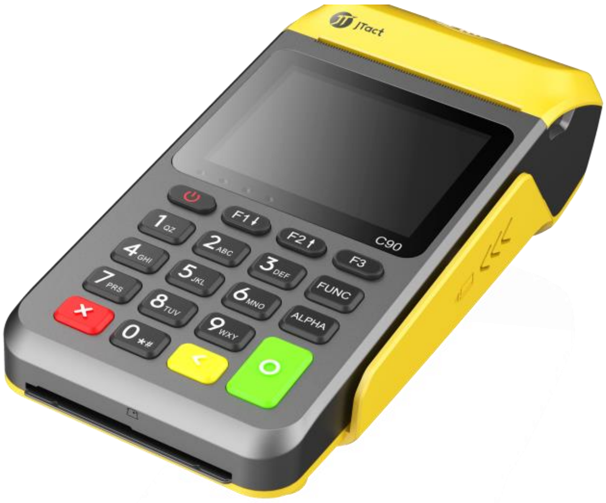


Figure 1.3 – C90 ICC Slot

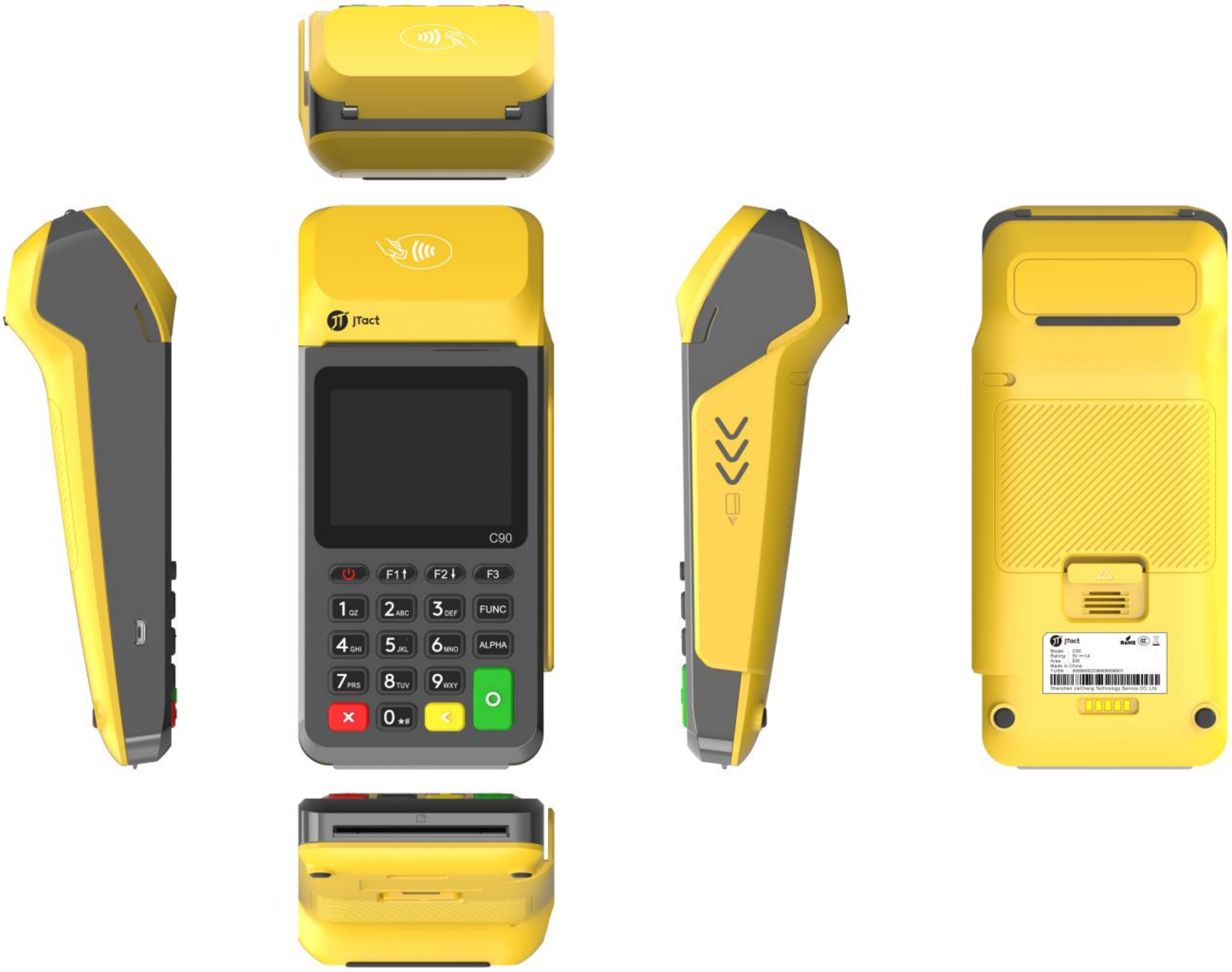
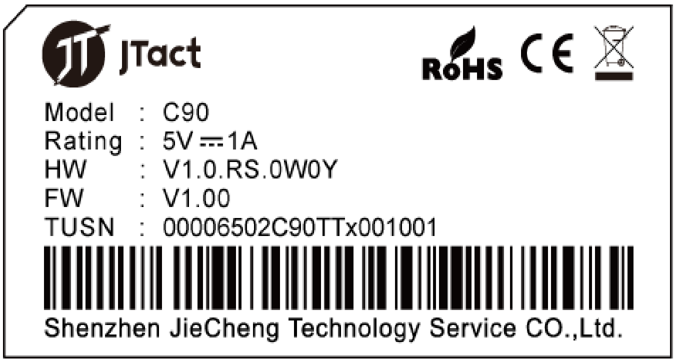


Figure 1.4 – Hexagonal view of C90

1.2 Product Identification

The product name and hardware version are printed on a label on the device. The HW version can be identified from this label. Please see below picture.



JTact

RoHS CE

Model : C90
Rating : 5V⎓1A
HW : V1.0.RS.0W0Y
FW : V1.00
TUSN : 00006502C90TTx001001

Shenzhen JieCheng Technology Service CO.,Ltd.

Figure 1.5 – C90 Product Identification

The firmware version can be retrieved by using the software menu. User can enter “Vendor management” -> “Version info” find the FW version is V1.00.

1.3 Communication methods and protocols

Communication methods: USB, Cellular (2G/3G/4G), Wi-Fi, Bluetooth
Communication protocols: TCP/IP, SSL/TLS, PPP, ICMP, ARP, UDP, DHCP
Use of any method not listed in the policy invalidates the device approval.

2 Guidance

This chapter mainly introduces how to use this device securely. Use of any method not listed in the policy will invalidate the device approval.

2.1 Check Device

User should check all items when receives the device at the first time. The items along with the device include a battery, a power supply, and a copy of user guide specification.
Before using the device, user needs to check if it is genuine and ready for use. If anything is lacking or damaged, user should contact with the vendor for inspection, refund or exchange.

2.2 Power

User should take out and check the power supply in a packaging box, and put the DC plug into the power socket, as shown in figure 2.1:

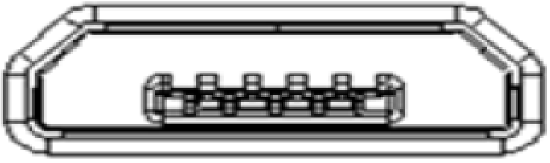


Figure 2.1 – C90 Power socket

Specification of power supply:
Input: 100 to 240V AC, 50 Hz /60Hz
Output: 5V 2A

2.3 Environment

The device is designed to be used in an attended environment.
The device can only be used normally under a specific environmental condition. When the device detects an abnormal condition, a tamper event will happen and all the sensitive data will be cleared.

2.4 Input PIN

C90 is a handheld PED device which supports physical keyboard and the device is without privacy shield. It’s also recommended that the customer should be advised to take care that that he is not overlooked when entering his PIN code. And user should use his own body or free hand to prevent others peeping at the PIN information.

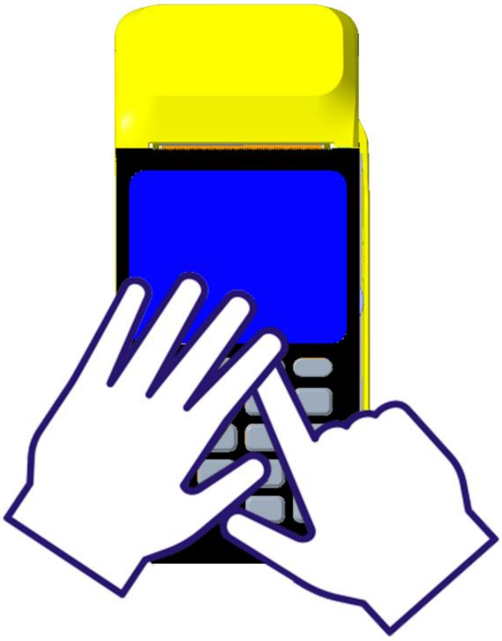


Figure 2.2 – Input PIN

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 the view of cameras.	Do not install within the view of cameras.
Without stand	Use signage and body to block the view.	Use signage and body to block the view.	Use signage and body to block the view.	Do not install within the view of cameras.	Do not install within the view of cameras.

2.5 Period Detection

The merchant or acquirer should check that the device is not destroyed or installed a suspicious bug once a day. The merchant or acquirer must visually inspect the device when received via shipping. The merchant or acquirer should inspect the device to ensure that:

- The used device is the approved one and there is no overlay.
- There is no suspicious wire being connected to any ports of the device.
- There is no visible open case evidence via inspecting the device shell or the labels in screw holes.
- There is no suspicious thing appearing in ICC and MSR.
- The installation/maintenance operations are performed by a trust person.
- The checking routines are applied.
- For the inspection of ICC and MSR card slots, please refer to the picture of device in section 1.1
- Refer to section 3.1 for the handling of device tamper.

2.6 Handle Fault

The merchant or acquirer should always concern the status of the device being used. Once the device is locked or displays abnormally, it cannot be used for PIN transactions. When a tamper event occurs, the device must be inspected by the vendor. Users are advised to contact with vendor for further and detail secure inspection.

2.7 Process Decommissioning Device

If the device would be decommissioned permanently from service and no longer in use. The security staff will gather the device and erase all the key information. This can be done by taking the device apart to make it tampered or using a dedicate tool to delete all the sensitive information. Then these device will be transported back to JC factory for disassembling and recycling.

If the device requires a temporary removal, it is unnecessary to change the state of the device due to all the sensitive information in the device are still under the protection of physical and logical protection mechanism.

3 Hardware Security

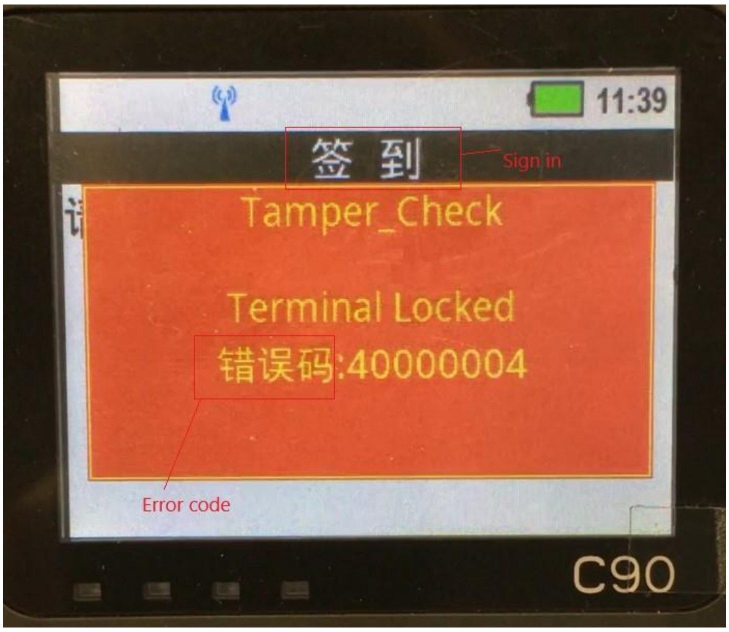
The device will be triggered when a physical penetration attempt is detected. And it contains anti-detected mechanism to protect the device from being attacked.

3.1 Deal with Tamper

A merchant or acquirer can easily find a tamper event in the device. When it is being tampered, the device will display a prompt and be locked. There is no other sound or light warning. When the device is locked all the sensitive data will be immediately erased and none of them can be used again.

Any tamper event happened will make the device out of normal service. The device has 2 separate modes as below:

- Activated mode: the device is fully operational.
- Freezing mode: the device has been tampered. Under this mode the device cannot be operated and requires reactivation after maintenance and security checks. The merchant must stop using the device and contacts the vendor to return the device. The vendor will check the device in a secure room.



签 到

Tamper_Check

Terminal Locked

错误码:40000004

Figure 3.1 — Example of tamper-message

The Chinese characters mean that the terminal has locked. Error code: 40000004.

3.2 Environmental Failure Protection

The security of the device is not compromised by altering the environmental conditions (e.g. the temperature or operating voltages outside the stated operating range does not alter the security). The environmental conditions, that will cause environmental failure-protection mechanisms to trigger, are shown below

Tamper	Name	Min	Typical	Max
SD(signal detection)	Circuit input low level	-	-	0.3Voltage of Battery
	Circuit input high level	0.7Voltage of Battery	-	-
TD(temperature detection)	TD High	95℃	105℃	115℃
	TD Low	-45℃	-38℃	-35℃
VD(voltage detection)	VD High	3.9 V	4.0 V	4.1 V
	VD Low	1.8 V	1.9 V	2.0 V

3.3 Environment and Operational Conditions

Power Supply: DC 5V
Operating Temperature: 0°C ~ 50°C
Storage Temperature: -20°C ~ 70°C
Operating Humidity: 10% ~ 90% noncondensing
Storage Humidity: 5% ~ 95% noncondensing.

4 Software Security

4.1 Software Development Guidance

On the one hand, the developer must accept training course before development. On the other hand, the developer must respect the coding rules and practice during the whole development stage.
When developing applications, the developer must respect the security guidance described in the Reference [5]
During the software development, the following steps must be implemented:

- Code Review.
- Security review and audit
- Module test
- Source code management and version control
- Software test
- Signature

Reference [5], [6] and [7] document can provide more details.

4.2 Update Firmware and Software

Updates and patches can be loaded in the device. They are cryptographically authenticated by the device. If the authenticity is not confirmed, the update or patch will be rejected.
Prompts updates are security related and any security related firmware changes will cause firmware version update.
Note that tampered device will appear to be disabled, and will not allow for software and firmware running even if they are authentic. The device only supports local mode to update firmware and software through AP.

4.3 Authenticate Firmware and Software

This device implements asymmetric cryptographic algorithm for firmware authentication. RSA algorithm with 2048-bits 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 JC. And the firmware authentication is executed by signature verification using corresponding public key of JC.

Before firmware and application running every time, their integrity and validation will also be checked. If failed, the device will not work correctly.

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

4.4 Application Review

The application managers must implement a full source code review to make sure that the application does not have one of following behaviors:

- PIN entry prompt while the keypad digit is displayed in plain-text.
- Not using the correct security mechanism and APIs recommended in the user guidance for PIN entry.
- Any application running on the device obtain the whole track data plaintext and related key.

It is recommended that the application source code review and signing process is executed by at least two persons and that an audit log is recorded for future trace back.

4.5 Self-Test

Self-test is routinely executed upon start up or resetting every time. This checking is also performed periodically (23 hours) during the period of normal use. This test is not initiated by an operator. Like firmware, certificate and tamper will be tested.

4.6 Signature Mechanism

JC use a signature system based on web server technology to sign and manage all files. RSA algorithm with 2048-bits key is used for signature verification and SHA256 algorithm is used to calculate the digest of firmware. This system implements a serial of important functions such access control, permission management, file signature, log management and etc.

A pair of signature operators will be granted and permitted to login this system and do signature operation. Only both of them are identified by the system (through entry respective passwords successfully) during a window time, they can use the signature function to sign firmware or application.

During the whole signature process, private key always remains in the encryption machine and never be exported. Only signed file will be output to outside. Certainly, any operation trace will be recorded by this system to make it more secure.

4.7 SRED

The terminal supports the SRED function and must use a key of appropriate length. Account data and related key buffer must be cleared after use or exit transaction immediately. The firmware of device doesn’t support whitelisting for the pass-through of clear-text account data; also it always provides SRED functionality and doesn’t support the disablement (turning off) of SRED functionality.

4.8 OP

This device supports OP function, which uses SSL3.0 and TLS1.2 security protocols. WLAN supports 2.4/5 GHz band, which use the 802.11a/ B/G/N protocol. No password connect function is disabled in WLAN. Bluetooth supports Bluetooth 3.0. Bluetooth supports mode 4 level 3, Bluetooth BLE and JUST WORK mode are disabled in Bluetooth. The device supports cellular networks, including 2G, 3G and 4G. The TCP/IP protocol stack is implemented by the communication module itself, and the version is IPv4.The developer must respect the SSL security guidance. SSL is inherently weak and should be removed, but considering that SSL server is still in use in the world, to keep compatible, we temporarily maintain SSL as non-financial applications for use. In addition, our SSL only runs as a client, so we strongly recommend that the server disable the SSL protocol and choose TLS1.2 or higher.
Reference [7] document can provide more details.

5 System Administration

5.1 Configuration Settings

The device is functional when it is received by the merchant or acquirer. No security sensitive configuration settings are necessary to be tuned by the end user to meet security requirement.

5.2 Default Value Update

The device does not include any certificates for testing purposes 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 PSW1 is “88888888”, the other default value of PSW2 is “99999999”, and is enforced to be re-set a valid PSW before first time using.
PSW modifying at “SstS->Change PWD”. 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 ten times limits for the PSW input, if wrong input over ten times, the sensitive service cannot be accessed for two hours.

6 Key Management

6.1 Key Management Techniques

C90 device implements different types of key management techniques.

- **Master Key/Session Key**: a method using a hierarchy of keys.
- **DUKPT**: a key management technique based on a unique key for each transaction

Use of the POI with different key-management systems will invalidate any PCI approval of this POI

6.2 MK/SK

An acquirer's MK/SK hierarchy is used in the device. TMK is used to encrypt session keys transferred. The session keys can be divided into three types: TPK (PIN Encryption Key), TAK (MAC Calculating Key) and TDK (Data encryption Key).

6.3 DUKPT KEY

Acquirer downloads initial key in the secure room. Then it will generate 21 future keys under the ANSI X9.24 future key generate algorithm. The key is used as TPK (Pin Encryption Key).

6.4 Cryptographic Algorithms

C90 POS device can support the secure algorithm as following:

- TDES(128 bits and 192 bits)
- AES(128bits, 192bits, 256bits)
- SHA-256(digest signature, 256 bits)
- RSA-2048(signature verification, 2048 bits)
- ECC(P-256 and P-521)

6.5 Key Introduction

The transaction related keys are classified as following description. These transaction keys are controlled and generated by the acquirer.

All keys loaded into the device can't be obtained from external or exported to external by any way. These keys only can only be used for the intended purpose via the interface or commands provided by the device.

Key Name	Purpose/Usage	Algorithm	Size(Bits)	Storage
TMK	Master Key. Use to protect TPK/TAK/TDK	TDES	128/192	Secure Unit
		AES	128/192/256	
TPK	PIN Encryption Key. Used to encrypt PINBLOCK	TDES	128/192	Secure Unit
		AES	128/192/256	
TAK	MAC Calculating Key. Used to calculate MAC value	TDES	128/192	Secure Unit
		AES	128/192/256	
TDK	Data Key. Used to encrypt account data.	TDES	128/192	Secure Unit
		AES	128/192/256	
TTK	Transmission Key. Use to protect TMK	TDES	128/192	Secure Unit
		AES	128/192/256	
IPEK	Used to generate Future DUKPT Key	TDES	128	Temporary buffer
Future DUKPT Key	Online PIN Encryption. Used to encrypt online PINBLOCK	TDES	128	Secure Unit

6.6 Key Loading Policy

This device supports both remote and local key loading. For each remote key loading, mutual authentication should be executed between POS device and Key Management Center firstly. Specific tools complied with key management requirements shall be used for key injection.

The RSA key pairs are generated in an encryption equipment and these public keys are signed by proper secret keys. These operations are controlled by secure manager and happened in a secure room. Dual control and split knowledge mechanism are mandatory during this process. Reference [6] document can provide more details.

Initial keys should be loaded into the device by two trust persons using an authentic key loading dedicated tool in secure environment.

In MK/SK system, the working keys loaded into the device in the form of cipher, under the protection of master key.

Device support the ANSI TR-31 Key Derivation Binding Method. In MK/SK system and DUKPT system, the keys loaded into the device protected by TR-31 key block.

6.7 Key Replacement Policy

Key should be replaced with a new key 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, as defined in NIST SP 800-57-1. If a tamper event has happened, the device is asked to make secure inspection and sent to Key Authorization Center to inject new key again.

7 Roles and Services

The device provides sensitive services which can only be accessed by secure manager through identity authentication.

Acquirer: Update keys.

Device-user: Use app to transaction; Business interaction.

Vendor: Update Firmware and Software.