**DUKPT Operation Manual**

V1.0.6



Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Description | Author |
| 1.0.0 | 9th Jan, 2020 | First version | Iris Wang |
| 1.0.1 | 13th Jan, 2020 | Add the introduction | Iris Wang |
| 1.0.2 | 15th Jan, 2020 | Add the log module | Iris Wang |
| 1.0.3 | 18th Mar, 2020 | Version update | Iris Wang |
| 1.0.4 | 22th Apr, 2020 | Added BDK component setting | Iris Wang |
| 1.0.5 | 14th May, 2020 | Added Config、MKEK Inject operation  Added operation of SN imported. | Iris Wang |
| 1.0.6 | 3th Jun, 2020 | Added selection function of 3DES length | Iris Wang |

**DUKPT Operation Manual**

Table of Contents

[Introduce 3](#_Toc42092817)

[Master POS 3](#_Toc42092818)

[1.CONFIG---Merchant config 5](#_Toc42092819)

[2.MKEK INJECT 6](#_Toc42092820)

[3.IMPORT AUTH CODE（preset condition） 7](#_Toc42092821)

[4.BDK ADMIN---Add BDK（INN） 9](#_Toc42092822)

[5.BDK ADMIN---Add BDK（KSN） 10](#_Toc42092823)

[6.BDK ADMIN---Remove BDK 11](#_Toc42092824)

[7. CARD ADMIN---Change PIN 12](#_Toc42092825)

[8. CARD ADMIN---Change Card name 13](#_Toc42092826)

[9. CONFIG---LOG 14](#_Toc42092827)

[10. CONFIG---export the log file 15](#_Toc42092828)

[11. Card expiration check 16](#_Toc42092829)

[Target POS 17](#_Toc42092830)

[1.IPEK INJECTION 17](#_Toc42092831)

# Introduce

Master POS

Master Pos mainly uses DUKPT key management technology to ensure that a unique key is used for each transaction process. In addition, it uses an irreversible key conversion algorithm, which makes it impossible to crack the previous transaction key from the current transaction data information. Master pos main job is to export the IPEK to the target pos using KEK and the target pos public key encryption.

Target POS

Target Pos is based on the idea of DUKPT key distribution and uses 3DES encryption method to import KEK from the Host. During the IPEK injection process, the relevant information of the target pos are transmitted to the master pos through the serial port. The master pos returns the encrypted IPEK to the target pos. The target pos is decrypted by the RSA private key firstly, and then decrypted by KEK. IPEK is stored in the security chip

Introduction of a set of cards

|  |  |  |
| --- | --- | --- |
| Card | Num | Comments |
| Manager card | 2 | 1.Config (such as set Customer ID、 set BDK component group number, set DIY KSN switch、Set Inject timeout time)；  2.Import SN  3.MKEK download；  4.Delete BDK |
| Supervisor card | 2 | Used to add BDK |
| Operator card | 2 | Used to inject IPEK |

# Master POS

|  |  |
| --- | --- |
| Parameter | Comments |
| DIY KSN | Customize KSN ON: you can customize KSN;  OFF: customize INN data in KSN; |
| CUSTOMER ID | used to distinguish customers |
| HOST IP / PORT | Used to download MKEK in a safe room |
| TIMEOUT (s) | Used for timeout when downloading MKEK in a secure room to establish a communication link. |
| INJECT TIMEOUT (s) | IPEK injection time custom setting, default 120s. |
| BDK COMPONENT | used to control the number of groups of input BDK components, that is set to 2, 3; |

A screenshot of a cell phone

Description automatically generated A screenshot of a cell phone

Description automatically generated

A screenshot of a cell phone

Description automatically generated A screenshot of a cell phone

Description automatically generated

## 1.CONFIG---Merchant config

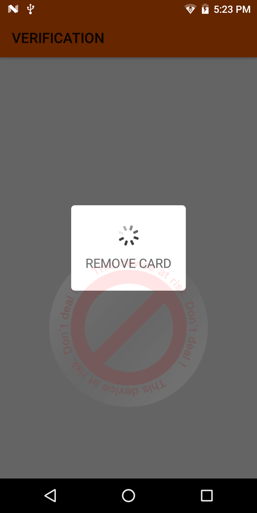
* Click the config module, Enter the config page,
* Click the setting module, then insert the manager card, Input password, Then Remove the card.
* Turn on the KSN switch.
* Config the customer id, click ‘OK ‘button, then click ‘confirm’ button, config success.

A screenshot of a cell phone

Description automatically generated A screenshot of a cell phone

Description automatically generated A screenshot of a cell phone

Description automatically generated

 A screenshot of a cell phone

Description automatically generated A screenshot of a cell phone

Description automatically generated A screenshot of a cell phone

Description automatically generated

## 2.MKEK INJECT

* Click the MKEK inject module, we insert Manager card and input PIN, then remove the card, MKEK will be downloaded automatically.
* Click the MKEK inject button again, we can see MKEK has been downloaded.

A screenshot of a cell phone

Description automatically generated A screenshot of a cell phone

Description automatically generated A screenshot of a cell phone

Description automatically generated

A screenshot of a cell phone

Description automatically generated A screenshot of a cell phone

Description automatically generated A screenshot of a cell phone

Description automatically generated

## 3.IMPORT AUTH CODE（preset condition）

* Click the ‘CONFIG’ icon, enter the config page.
* Click the ‘IMPORT AUTH CODE’ icon, we insert Manager card and input PIN, then remove the card, enter the server page.
* Click the ‘off ‘button and access the service address show. Open the web page on PC and upload the given SN document. Click the upload button.
* Check that the SN of the Target POS has been imported successfully and display the list of SN on Master POS.
* Note that the given SN document can’t be read or written in any way.
* Click the delete button in the upper right corner to delete SN of the Target POS.

**Note：PC and the master POS must be in the same network environment**

A screenshot of a cell phone

Description automatically generated A screenshot of a cell phone

Description automatically generated A screenshot of a cell phone

Description automatically generated

A screenshot of a cell phone

Description automatically generated A screenshot of a cell phone

Description automatically generated A screenshot of a cell phone

Description automatically generated

 A screenshot of a cell phone

Description automatically generated

A screenshot of a cell phone

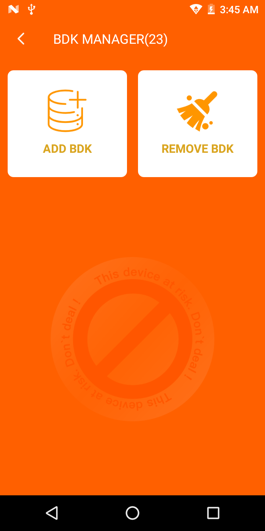
Description automatically generated A screenshot of a cell phone

Description automatically generated

## 4.BDK ADMIN---Add BDK（INN）

* Click the ‘BDK Admin’ icon, enter BDK manager page.
* Click the ‘Add BDK’ icon, then insert supervisor card and enter the password, remove card after verification successfully. This step needs double-checked.
* Choose 3DES length. Input BDK name、Index、IIN and two/ three Components, confirm each component.
* Add BDK successfully and click the ‘confirm’ button.
* If the Index has been occupied, we can use supervisor card to overwrite this index.

A screenshot of a cell phone

Description automatically generated  A screenshot of a cell phone

Description automatically generated A screenshot of a cell phone

Description automatically generated

A screenshot of a cell phone

Description automatically generated A screenshot of a cell phone

Description automatically generated A screenshot of a cell phone

Description automatically generated

A screenshot of a cell phone

Description automatically generated A close up of a keyboard

Description automatically generated A screenshot of a cell phone

Description automatically generated

## 5.BDK ADMIN---Add BDK（KSN）

* Click the ‘BDK Admin’ icon, enter BDK manager page.
* Click the ‘Add BDK’ icon, then insert supervisor card and enter the password, remove card after verification successfully. This step needs double-checked.
* Choose 3DES length. Input BDK name、Index、KSN and two/three Components, confirm each component.
* Add BDK successfully and click the ‘confirm’ button.
* If the Index has been occupied, we can use supervisor card to overwrite this index.

A screenshot of a cell phone

Description automatically generated A picture containing food

Description automatically generated A screenshot of a cell phone

Description automatically generated A screenshot of a cell phone

Description automatically generated

A screenshot of a cell phone

Description automatically generated A screenshot of a cell phone

Description automatically generated A screenshot of a cell phone

Description automatically generated A screenshot of a cell phone

Description automatically generated

A screenshot of a cell phone

Description automatically generated A screenshot of a cell phone

Description automatically generated A screenshot of a cell phone

Description automatically generated A screenshot of a cell phone

Description automatically generated

## 6.BDK ADMIN---Remove BDK

* Click the ‘BDK Admin’ icon, enter the DBK manager page.
* Click the ‘Remove BDK’ icon, all added BDKs are displayed in the list, choose the BDK you want to delete.
* Insert supervisor card and verification, then remove the card.
* This page will pop up the confirm message, click ‘delete’ button, the BDK will be deleted.

A screenshot of a cell phone

Description automatically generated  A screenshot of a cell phone

Description automatically generated A screenshot of a cell phone

Description automatically generated

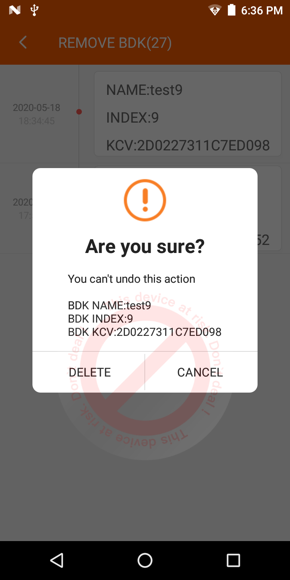
A screenshot of a cell phone

Description automatically generated A screenshot of a cell phone

Description automatically generated A screenshot of a cell phone

Description automatically generated

A screenshot of a cell phone

Description automatically generated  A screenshot of a cell phone

Description automatically generated

## 7. CARD ADMIN---Change PIN

* Click the ‘Card Admin’ icon.
* Insert the card you want to change your password and verify successfully.
* Click the ‘Change PIN’ button, enter new password and confirm. A pop-up message prompts that the modification was successful.

A screenshot of a cell phone

Description automatically generated A screenshot of a cell phone

Description automatically generated A screenshot of a cell phone

Description automatically generated

A screenshot of a cell phone

Description automatically generated A screenshot of a cell phone

Description automatically generated A screenshot of a cell phone

Description automatically generated

## 8. CARD ADMIN---Change Card name

* Click the ‘Card Admin’ icon.
* Insert the card you want to change your card name and verify successfully.
* Click the ‘change Name’ button, enter name you want to change. A pop-up message prompts that the modification was successful.
* Insert this card again to check its name has been changed.

A screenshot of a cell phone

Description automatically generated A screenshot of a cell phone

Description automatically generated A screenshot of a cell phone

Description automatically generated A screenshot of a cell phone

Description automatically generated

A screenshot of a cell phone

Description automatically generated A screenshot of a cell phone

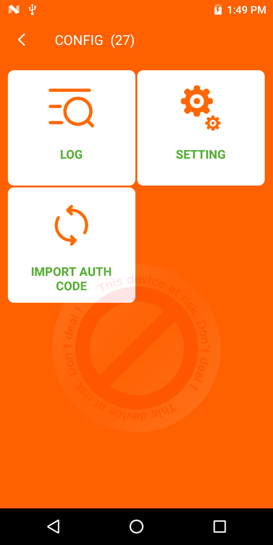
Description automatically generated

## 9. CONFIG---LOG

* Click the ‘CONFIG’ icon, enter the config page.
* Click the ‘LOG’ icon, enter log list page. This page records the log of all daily operations
* Click the date, enter the log details page. This page records the log of the day’s operations.

.

A screenshot of a cell phone

Description automatically generated  A screenshot of a cell phone

Description automatically generated A screenshot of a cell phone screen with text

Description automatically generated

## 10. CONFIG---export the log file

* Click the ‘CONFIG’ icon, enter the config page.
* Click the ‘IMPORT AUTH CODE’ icon, we insert Manager card and input PIN, then remove the card, enter the server page.
* Click the ‘off ‘button and access the service address shown. Enter the address in the browser, replace the web with logs. And go to the log download page.
* Click on the you want to view, and the log will be successfully exported.

A screenshot of a cell phone

Description automatically generated A screenshot of a cell phone

Description automatically generated A screenshot of a cell phone

Description automatically generated

A screenshot of a cell phone

Description automatically generated

## 11. Card expiration check

* Click the ‘Card Admin’ icon.
* Insert the card you want to check card expiry date and verify successfully.
* Check the card expiry date.
* If the card has expired, you need to replace it.

A screenshot of a cell phone

Description automatically generated A screenshot of a cell phone

Description automatically generated A picture containing device

Description automatically generated

# Target POS

# 1.IPEK INJECTION

* Connect the Target POS and Master POS with a serial cable we provide.
* Open Master POS and click ‘IPEK Injection’ icon, insert operator card and verify successfully. Select an added BDK and go to IPEK Inject page and accept USB access.
* Open Target POS and click ‘IPEK Injection’ icon, enter IPEK download mode and accept USB access.
* Click the ‘Start’ button of the Master Pos, the Master POS will receive request and ask operator to confirm SN of the connected Target POS, Click the ‘Enter’ button.
* IPEK will be Injected successfully.
* Connect the next Target POS with a serial cable we provide and repeat step 3 through 5 to inject IPEK again.

Target Pos figure:

A screenshot of a cell phone

Description automatically generated A screenshot of a cell phone

Description automatically generated A screenshot of a cell phone

Description automatically generated A screenshot of a cell phone

Description automatically generated

A screenshot of a cell phone

Description automatically generated A screenshot of a cell phone

Description automatically generated

Master POS figure:

A screenshot of a cell phone

Description automatically generated A screenshot of a cell phone

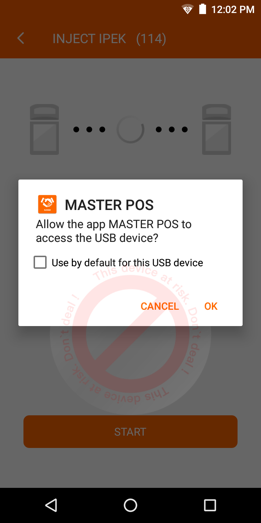
Description automatically generated A screenshot of a cell phone

Description automatically generated A screenshot of a cell phone

Description automatically generated

A screenshot of a cell phone

Description automatically generated A screenshot of a cell phone

Description automatically generated  A screenshot of a cell phone

Description automatically generated

A screenshot of a cell phone

Description automatically generated A screenshot of a cell phone

Description automatically generated A screenshot of a cell phone

Description automatically generated A screenshot of a cell phone

Description automatically generated

Connection figure:

A close up of a computer

Description automatically generated