

# RKMS User Manual

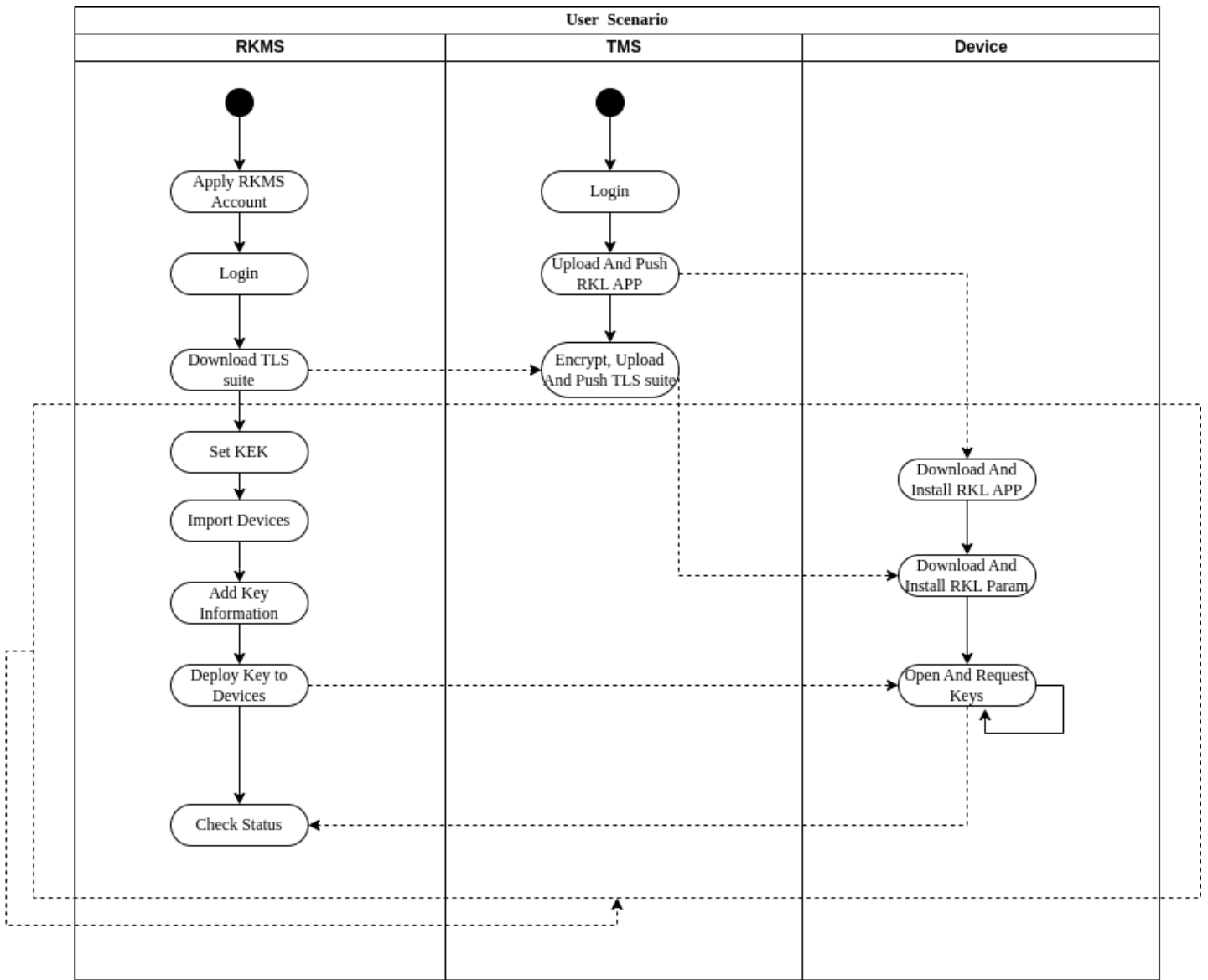
| Version | Author | Date       | Description       |
|---------|--------|------------|-------------------|
| 1.0     | Lizhou | 2023-08-04 | The first version |
|         |        |            |                   |
|         |        |            |                   |
|         |        |            |                   |
|         |        |            |                   |
|         |        |            |                   |
|         |        |            |                   |
|         |        |            |                   |
|         |        |            |                   |
|         |        |            |                   |

## 1. Introduction

The document describes how users use RKMS.

## 2. Usage Scenario

The general usage scenario diagram:

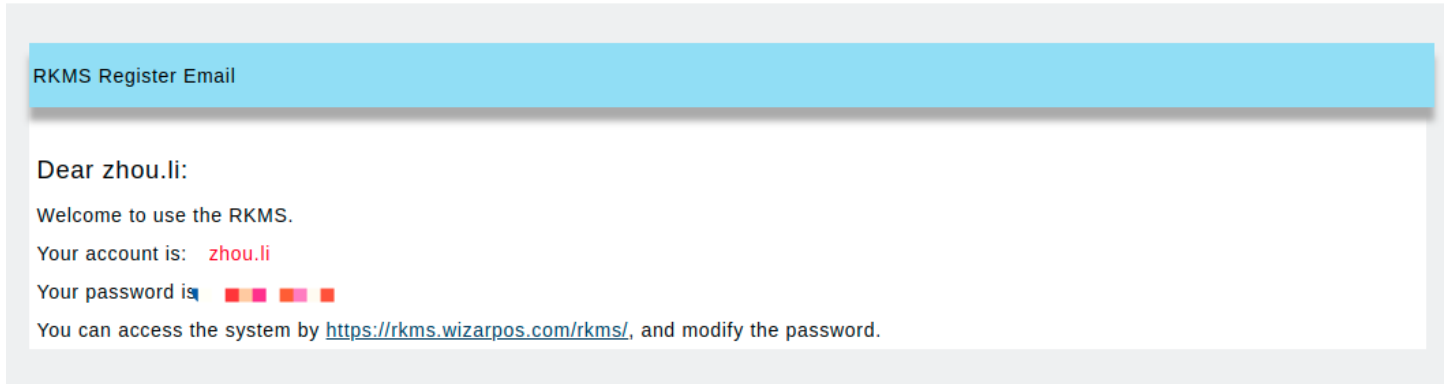


The above picture shows a general process and method that users use the RKMS.

- "Apply RKMS Account", please refer to chapter 2.1
- "Login", please refer to chapter 2.2
- "Download TLS Suite", please refer to chapter 2.3
- "Set KEK", please refer to chapter 2.4
- "Import Devices", please refer to chapter 2.5
- "Add Key Information", please refer to chapters 2.6 & 2.6.1 & 2.6.2
- "Deploy Key to Devices", please refer to chapter 2.6.3
- "Check Status", please refer to chapters 2.7 & 2.8

## 2.1 Apply Account

1. The users apply RKMS account information. The user information will be sent to user email.
2. The user checks the email and gets account information. An email like this:



The user can click the <https://rkms.wizarpos.com/rkms> link and access the RKMS.

Note:

Please modify the password when first logging into the system.

## 2.2 Login


The user login into the RKMS system with the user name and password

# Remote Key Management System

### Login

Name

Password

Captcha  

[Forget Password](#)

## 2.3 Download TLS Suite

The user can view the customer information, and download the TLS key suite.

The TLS key suite will be pushed to the terminal device. And the terminal device will create a secure connection to RKMS with the key suite and protect the terminal device and RKMS communication .

Then the user can open the RKMS client app, and request to inject the keys.

Customer List

Name  Email  Phone  [Search](#)

1

| Name          | Email                | Phone | Description   | Country | State    | Update Time         | #  |
|---------------|----------------------|-------|---------------|---------|----------|---------------------|--|
| wizarpos-test | zhou.li@wizarpos.com |       | wizarpos-test | China   | Shanghai | 2023-01-09 16:39:40 | <a href="#">Download SSL Key Suite</a> ▾ |

## 2.4 Manage KEK

KEK, the full name is Key Exchange Key, which is a cryptographic key. The KEK can be used to crypto the working key or KEK.

The user can manage the KEK, which is an encrypted key.

The user can view the KEK list.

KEK List

Name  [Search](#)

[Add](#)

1

| Name              | Description | Update Time         | #                      |
|-------------------|-------------|---------------------|------------------------|
| customer-root     |             | 2023-08-07 14:08:01 | <a href="#">Edit</a> ▾ |
| CUSTOMERTEST-ROOT |             | 2023-08-03 10:28:33 | <a href="#">Edit</a> ▾ |
| WIZARPOSTEST-ROOT |             | 2023-08-03 10:26:00 | <a href="#">Edit</a> ▾ |

On the page, users can click the "Add" button and add new KEK information:

## KEK Update

\* The fields with red border are required.

|                  |   |
|------------------|---|
| Name             | <input type="text" value="WIZARPOSTEST-ROOT"/>  |
| KEK Format       | <input type="text" value="AKB"/>  |
| Key Exchange Key | <input type="text" value="3kDNE000,L [redacted] D10&lt;br/&gt;5F4A3,8D195A0C2A38D4A1"/> |
| KCV              | <input type="text" value="E72B5F"/>   |
| Description      | <input type="text"/>  |

There are 2 key formats: AKB and TR31.

- AKB, Atalla Key Block, you can contact WizarPOS to get support and apply for it from MyHSM.
- TR31, a generally TR-31 format. The customer can generate 3 components by yourself, then there are 3 security officers separately send them to WizarPOS with 3 envelopes via 3 express companies. WizarPOS will input them into HSM in the security room by 3 security officers. The HSM will generate TR31, then export it from HSM.

When the key format is TR31, it will be different from AKB:

\* The fields with red border are required.

|                  |   |
|------------------|---|
| Name             | <input type="text" value="CUSTOMERTEST-ROOT"/>                  |
| KEK Format       | <input type="text" value="TR31"/>                               |
| Parent KEK       | <input type="text" value="WIZARPOSTEST-ROOT"/>                  |
| Key Exchange Key | <input type="text" value="C0088K1TR007...A0793D98C9AC228A909"/> |
| KCV              | <input type="text" value="3F8BA9"/>                             |
| Description      | <input type="text"/>  |

The parent KEK is the TR31 protected key.

Note: If the KEK is combined in the HSM of WizarPOS, WizarPOS will export TR31 KEK and can help customer input it to system.

## 2.5 Manage Devices

The user can view the terminal device list.

## Customer Device List

SN  Customer Name

First Previous (1-15/51 - 1/4) Next Last

| SN               | Customer   | Update Time         | Operator | #                                     |
|------------------|------------|---------------------|----------|---------------------------------------|
| WP20230Q20002429 | customer21 | 2023-08-04 16:50:07 | admin    | <input type="button" value="Edit"/> ▾ |
| WP20230Q20002428 | customer21 | 2023-08-04 16:50:07 | admin    | <input type="button" value="Edit"/> ▾ |
| WP20230Q20002427 | customer21 | 2023-08-04 16:50:07 | admin    | <input type="button" value="Edit"/> ▾ |
| WP20230Q20002426 | customer21 | 2023-08-04 16:50:07 | admin    | <input type="button" value="Edit"/> ▾ |
| WP20230Q20002425 | customer21 | 2023-08-04 16:50:07 | admin    | <input type="button" value="Edit"/> ▾ |
| WP20230Q20002424 | customer21 | 2023-08-04 16:50:07 | admin    | <input type="button" value="Edit"/> ▾ |
| WP20230Q20002423 | customer21 | 2023-08-04 16:50:07 | admin    | <input type="button" value="Edit"/> ▾ |
| WP20230Q20002422 | customer21 | 2023-08-04 16:50:07 | admin    | <input type="button" value="Edit"/> ▾ |
| WP20230Q20002421 | customer21 | 2023-08-04 16:50:07 | admin    | <input type="button" value="Edit"/> ▾ |
| WP20230Q20002420 | customer21 | 2023-08-04 16:50:07 | admin    | <input type="button" value="Edit"/> ▾ |

On the page, users can click the "Add Devices" button and add new devices information:

SN List

Description

The SN list format:

SN can be separated by commas(,)/semicolons(;)/spaces( )/line(\n) breaks.

## 2.6 Manage Keys

The RKMS supports 3 key types: DUKPT Key, Master key, Transport key.

### 2.6.1 View Keys

The user can view the key list.

Key List


| Name                       | Customer Name | Enabled    | Search |        |         |                     |          |        |
|----------------------------|---------------|------------|--------|--------|---------|---------------------|----------|--------|
| Add                        | Import        | 1          |        |        |         |                     |          |        |
| Name                       | Customer      | Type       | Slot   | Length | Enabled | Update Time         | Operator | #      |
| WP20230Q20002310-MasterKey | customer21    | Master Key | 0      | 32     | ● Yes   | 2023-07-21 16:39:23 | admin    | Deploy |
| WP20230Q20002309-MasterKey | customer21    | Master Key | 0      | 32     | ● Yes   | 2023-07-21 16:39:23 | admin    | Deploy |
| WP20230Q20002308-MasterKey | customer21    | Master Key | 0      | 32     | ● Yes   | 2023-07-21 16:39:23 | admin    | Deploy |
| WP20230Q20002307-MasterKey | customer21    | Master Key | 0      | 32     | ● Yes   | 2023-07-21 16:39:23 | admin    | Deploy |
| WP20230Q20002306-MasterKey | customer21    | Master Key | 0      | 32     | ● Yes   | 2023-07-21 16:39:23 | admin    | Deploy |
| WP20230Q20002305-MasterKey | customer21    | Master Key | 0      | 32     | ● Yes   | 2023-07-21 16:39:23 | admin    | Deploy |
| WP20230Q20002304-MasterKey | customer21    | Master Key | 0      | 32     | ● Yes   | 2023-07-21 16:39:23 | admin    | Deploy |
| WP20230Q20002303-MasterKey | customer21    | Master Key | 0      | 32     | ● Yes   | 2023-07-21 16:39:23 | admin    | Deploy |
| WP20230Q20002302-MasterKey | customer21    | Master Key | 0      | 32     | ● Yes   | 2023-07-21 16:39:23 | admin    | Deploy |
| dukpt-test3                | customer21    | DUKPT Key  | 0      | 32     | ● Yes   | 2023-03-30 13:28:12 | admin    | Deploy |

On the page, users can click the "Add" button and add new key information:



## Key Update

\* The fields with red border are required.

|                    |   |
|--------------------|---|
| Customer           | <input type="text" value="customer21"/>   |
| Name               | <input type="text" value="WP20230Q20002310-MasterKey"/>                             |
| Type               | Master Key <span>▼</span>   |
| Key Length         | <input type="text" value="32"/>   |
| Key Slot           | <input type="text" value="0"/>  |
| KEK                | Second-Level-KEK <span>▼</span>   |
| Key Info Algorithm | TR31 <span>▼</span>   |
| Key Info           |  |
| KCV                | <input type="text" value="FAD1FE"/>   |
| Description        | <input type="text"/>  |
| Enabled            | <input checked="" type="checkbox"/>   |

When the key type is DUKPT key, there will be KSN / DeviceID variable (Decimal) / Transaction Counter (Decimal), and does not have KCV.

|   |   |                             |                                |
|---|---|-----------------------------|--------------------------------|
| Name  | <input type="text" value="dukpt-test3"/>  |                             |                                |
| Type  | DUKPT Key <span>▼</span>  |                             |                                |
| Key Length  | <input type="text" value="32"/>   |                             |                                |
| Key Slot  | <input type="text" value="0"/>  |                             |                                |
| KEK   | Root KEK <span>▼</span>   |                             |                                |
| Key Info Algorithm  | TR31 <span>▼</span>   |                             |                                |
| Key Info  | <input type="text" value="C0072B0TB00E000056502CF3B132908E179FEB0EDF1FD43E8E0978629AFA6643E25513B4"/> |                             |                                |
| KSN (Hex)   | <input type="text" value="FFFF9876543210E000"/>   | DeviceID Variable (Decimal) | <input type="text" value="1"/> |
| Transaction Counter (Decimal)   | <input type="text" value="0"/>  |                             |                                |
| Description   | <input type="text"/>  |                             |                                |
| Enabled   | <input checked="" type="checkbox"/>   |                             |                                |
| <hr/>   |   |                             |                                |
| <input type="button" value="Cancel"/> <input type="button" value="Submit"/> <input type="button" value="Copy And New"/> |   |                             |                                |

Click the "Submit" button to submit the key information to the system.

The key information has 2 key formats: AKB and TR31.

- AKB, Atalla Key Block, you need to apply it from WizarPOS. And the applying process is like generating KEK.

- TR31, a generally TR-31 format. It's protected by KEK. The customer can generate it by themselves. Recommend use version C.

## 2.6.2 Import Keys

The user can import the keys of a batch also.

### Key Import

\* The fields with red border are required.

Customer

Type

Key Length

Key Slot

KEK

Key Info Algorithm

Key Info (.csv file)   
Format: Key, KCV, SN

Description

Enabled

The key file format:

The demo KEK:

|           |  |
|-----------|--|
| Clear Key | 55634E647CF9F2F10DA881E6AA3232285194D297657EE3D8   |
| TR31      | C0088K1TB00E0000027F76398A89E45EDB96DC1E96F41D66D9303B898866C7D6FCBBBD57330C9E82AE131994 |
| KCV       | FB9484   |

The working key format:

|           |  |
|-----------|--|
| Clear Key | EA58EF96B08BF9483910E6E1CC9B7C99BA702292B81DBD3B   |
| TR31      | C0088K1TB00E0000954F545F07782F75F94931F8D075C54146EE65389EDAFF1F9569C1C675F279542642F4FB |
| KCV       | 159A6A   |
|           |  |
| Clear Key | 3CF2CDCF9C614DA32B665BC19FFDC91AC60BE4B334B398E3   |
| TR31      | C0088K1TB00E0000A479350B91F721F2D5763B0E357036A685A070C0FAEC3134BAF6BF05F7744BFC177E32DD |
| KCV       | 47A912   |

```
1 # The line started with # is a comment line
2 # The encrypted key, KCV, SN
3 #
   C0072K1TB00E00007E8B9B5DA2AB70C68C9E9477FC805E5F62F622A67CFAB5FE16A885E1, FAD1FE
   ,WP20230Q20002310
```

The key supports 2 algorithms: AKB, TR31. We recommend use TR31.

### 2.6.3 Deploy Keys

When preparing the keys, then you can click the "Deploy" button to deploy the key to terminal devices.

Key List

Name  Customer Name  Enabled   1

| Name                       | Customer   | Type       | Slot | Length | Enabled                                  | Update Time         | Operator | #  |
|----------------------------|------------|------------|------|--------|--|---------------------|----------|--|
| WP20230Q20002310-MasterKey | customer21 | Master Key | 0    | 32     | <span style="color: green;">●</span> Yes | 2023-07-21 16:39:23 | admin    | <input type="button" value="Deploy"/> <input type="button" value="▼"/> |
| WP20230Q20002309-MasterKey | customer21 | Master Key | 0    | 32     | <span style="color: green;">●</span> Yes | 2023-07-21 16:39:23 | admin    | <input type="button" value="Deploy"/> <input type="button" value="▼"/> |
| WP20230Q20002308-MasterKey | customer21 | Master Key | 0    | 32     | <span style="color: green;">●</span> Yes | 2023-07-21 16:39:23 | admin    | <input type="button" value="Deploy"/> <input type="button" value="▼"/> |
| WP20230Q20002307-MasterKey | customer21 | Master Key | 0    | 32     | <span style="color: green;">●</span> Yes | 2023-07-21 16:39:23 | admin    | <input type="button" value="Deploy"/> <input type="button" value="▼"/> |
| WP20230Q20002306-MasterKey | customer21 | Master Key | 0    | 32     | <span style="color: green;">●</span> Yes | 2023-07-21 16:39:23 | admin    | <input type="button" value="Deploy"/> <input type="button" value="▼"/> |
| WP20230Q20002305-MasterKey | customer21 | Master Key | 0    | 32     | <span style="color: green;">●</span> Yes | 2023-07-21 16:39:23 | admin    | <input type="button" value="Deploy"/> <input type="button" value="▼"/> |

Deploy page:

## WP20230Q20002310-MasterKey - Deploy

Deploy Target  Devices  Group

Target

Please input the device SN list. Example: WP12345678901234, WP12345678901235,  
...

Force Deploy

When select the checkbox, if the device had a key on the same slot N, the old relation will be reset as invalid with no error notice.

Close

Submit

Note:

If the terminal device had a key in the same slot N, and did not select "Force Deploy", there would be an error when clicking the "Submit" button submit the form.

## 2.7 Check Status

The user can check the terminal device and key status in the system.

This page will show all the deploy records of keys and terminal devices.

Customer Device Status List

| SN               | Customer   | Key Name                   | Key Type   | Key Slot | Status  | Inject Time         | Update Time         | Operator | #                            |
|------------------|------------|----------------------------|------------|----------|---------|---------------------|---------------------|----------|------------------------------|
| WP20230Q20002310 | customer21 | WP20230Q20002310-MasterKey | Master Key | 0        | Success | 2023-08-04 16:12:26 | 2023-07-26 17:18:11 | admin    | <a href="#">Reset Status</a> |
| WP20230Q20002310 | customer21 | dukpt_key_test2            | DUKPT Key  | 0        | Success | 2023-07-25 11:00:21 | 2023-07-25 10:59:56 | admin    | <a href="#">Reset Status</a> |
| WP20230Q20002310 | customer21 | dukpt-test3                | DUKPT Key  | 0        | Invalid |                     | 2023-07-25 10:27:35 | admin    | <a href="#">Reset Status</a> |
| WP20230Q20002310 | customer21 | WP20230Q20002310-MasterKey | Master Key | 0        | Success | 2023-08-04 16:12:26 | 2023-07-21 17:02:41 |          | <a href="#">Reset Status</a> |
| WP20230Q20002323 | customer21 | dukpt-test3                | DUKPT Key  | 0        | Success | 2023-07-21 16:47:28 | 2023-07-21 16:42:46 | admin    | <a href="#">Reset Status</a> |
| WP20230Q20002323 | customer21 | dukpt_key_test2            | DUKPT Key  | 0        | Reset   | 2023-03-30 12:21:51 | 2023-07-21 16:42:48 | admin    | <a href="#">Reset Status</a> |
| WP20230Q20002323 | customer21 | Demo_Key                   | DUKPT Key  | 1        | Reset   | 2023-03-30 11:32:01 | 2023-07-21 16:42:57 | admin    | <a href="#">Reset Status</a> |
| WP20230Q20002323 | customer21 | Test_Master_Key            | Master Key | 1        | Reset   | 2023-03-28 09:34:49 | 2023-07-21 16:43:01 | admin    | <a href="#">Reset Status</a> |
| WP20230Q20002322 | customer21 | Test_Master_Key            | Master Key | 1        | Success | 2023-02-24 17:13:26 | 2023-02-24 17:13:16 | admin    | <a href="#">Reset Status</a> |
| WP17391Q20000041 | lipeng     | TestKey                    | DUKPT Key  | 0        | Reset   |                     | 2023-02-15 15:06:07 | admin    | <a href="#">Reset Status</a> |
| WP20230Q20002322 | customer21 | Demo_Key                   | DUKPT Key  | 1        | Success | 2023-02-24 17:13:25 | 2023-02-24 17:13:18 | admin    | <a href="#">Reset Status</a> |

There are 5 statuses: Init, Success, Failed, Reset, Invalid

- Init, the key and terminal device's first status. The terminal device can request and download the key in this status.
- Success, the terminal device downloaded and install the key successfully.
- Failed, the terminal device downloaded the key successfully but install failed.
- Reset, the terminal device can download and install this key again.
- Invalid, the terminal device can not download and install this key. Example, if a terminal device has a key A in slot 1 and it's Init status, then deploying a key B to this device in slot 1 also. The status of key A will be changed to Invalid.

## 2.8 Inject Report

The user can view all inject reports on this page. It will only show all success injecting.

## Inject Report List

|    |          |            |          |                        |
|----|----------|------------|----------|------------------------|
| SN | Customer | Date Begin | Date End | <a href="#">Search</a> |
|----|----------|------------|----------|------------------------|

[First](#)
[Previous](#)
[\(1-15/27 - 1/2\)](#)
[Next](#)
[Last](#)

| SN               | Customer   | Key Name                   | Key Type   | Key Slot | KSN                  | KCV    | KEK              | IP        | Inject Time         |
|------------------|------------|----------------------------|------------|----------|----------------------|--------|------------------|-----------|---------------------|
| WP20230Q20002310 | customer21 | WP20230Q20002310-MasterKey | Master Key | 0        |                      | FAD1FE | Second-Level-KEK | 127.0.0.1 | 2023-08-04 16:12:26 |
| WP20230Q20002310 | customer21 | dukt_key_test2             | DUKPT Key  | 0        | FFFF9876543210E00000 |        | Root KEK         | 127.0.0.1 | 2023-07-25 11:00:21 |
| WP20230Q20002310 | customer21 | dukt_key_test2             | DUKPT Key  | 0        | FFFF9876543210E00000 |        | Root KEK         | 127.0.0.1 | 2023-07-25 10:29:38 |
| WP20230Q20002310 | customer21 | WP20230Q20002310-MasterKey | Master Key | 0        |                      | FAD1FE | Second-Level-KEK | 127.0.0.1 | 2023-07-21 17:19:11 |
| WP20230Q20002323 | customer21 | dukt-test3                 | DUKPT Key  | 0        | FFFF9876543210E00000 |        | Root KEK         | 127.0.0.1 | 2023-07-21 16:47:28 |
| WP20230Q20002323 | customer21 | dukt-test3                 | DUKPT Key  | 0        | FFFF9876543210E00000 |        | Test KEK         | 127.0.0.1 | 2023-03-30 13:28:32 |
| WP20230Q20002323 | customer21 | dukt_key_test2             | DUKPT Key  | 0        | FFFF9876543210E00000 |        | Test KEK         | 127.0.0.1 | 2023-03-30 12:21:51 |
| WP20230Q20002323 | customer21 | Demo_Key                   | DUKPT Key  | 1        | FFFF9876543210E00000 |        |                  | 127.0.0.1 | 2023-03-30 11:32:01 |
| WP20230Q20002323 | customer21 | Demo_Key                   | DUKPT Key  | 1        | FFFF9876543210E00000 |        |                  | 127.0.0.1 | 2023-03-28 09:34:50 |
| WP20230Q20002323 | customer21 | Test_Master_Key            | Master Key | 1        |                      | 91FEF5 | Test KEK         | 127.0.0.1 | 2023-03-28 09:34:49 |
| WP20230Q20002323 | customer21 | Demo_Key                   | DUKPT Key  | 1        | FFFF9876543210E00000 |        |                  | 127.0.0.1 | 2023-03-21 17:45:28 |
| WP20230Q20002323 | customer21 | Test_Master_Key            | Master Key | 1        |                      | 91FEF5 | Test KEK         | 127.0.0.1 | 2023-03-21 17:45:27 |
| WP20230Q20002323 | customer21 | Demo_Key                   | DUKPT Key  | 1        | FFFF9876543210E00000 |        |                  | 127.0.0.1 | 2023-03-21 17:44:09 |
| WP20230Q20002323 | customer21 | Demo_Key                   | DUKPT Key  | 1        | FFFF9876543210E00000 |        |                  | 127.0.0.1 | 2023-03-21 17:37:21 |
| WP20230Q20002323 | customer21 | Demo_Key                   | DUKPT Key  | 1        | FFFF9876543210E00000 |        |                  | 127.0.0.1 | 2023-03-21 17:35:18 |