| Document Number | Classification |
| --- | --- |
| DTK-DOC-ADC-001 | Public |
| **Rev.** | DTK, Inc. |
| C00 | |

# DTKAuthClient Instructions

## V1.0



**DTK Confidential**

# Revision History

| Version | Author | Date | Description |
|---|---|---|---|
| V1.0 | Junping.wang | 2025/1/15 | Initial version |
| | | | |

# Content

# 1. Apply for a TAMS system account

## 1.1 Account application method

Step 1: Send an email to TAMS terminal authorization management system to apply for a legal login account;

Step 2: After successful application, you will receive the following email message;

Dear test,

Welcome to TAMS! Please log in to the system using the following information.

TAMS website: https://ams.dreamtek-global.com:7989

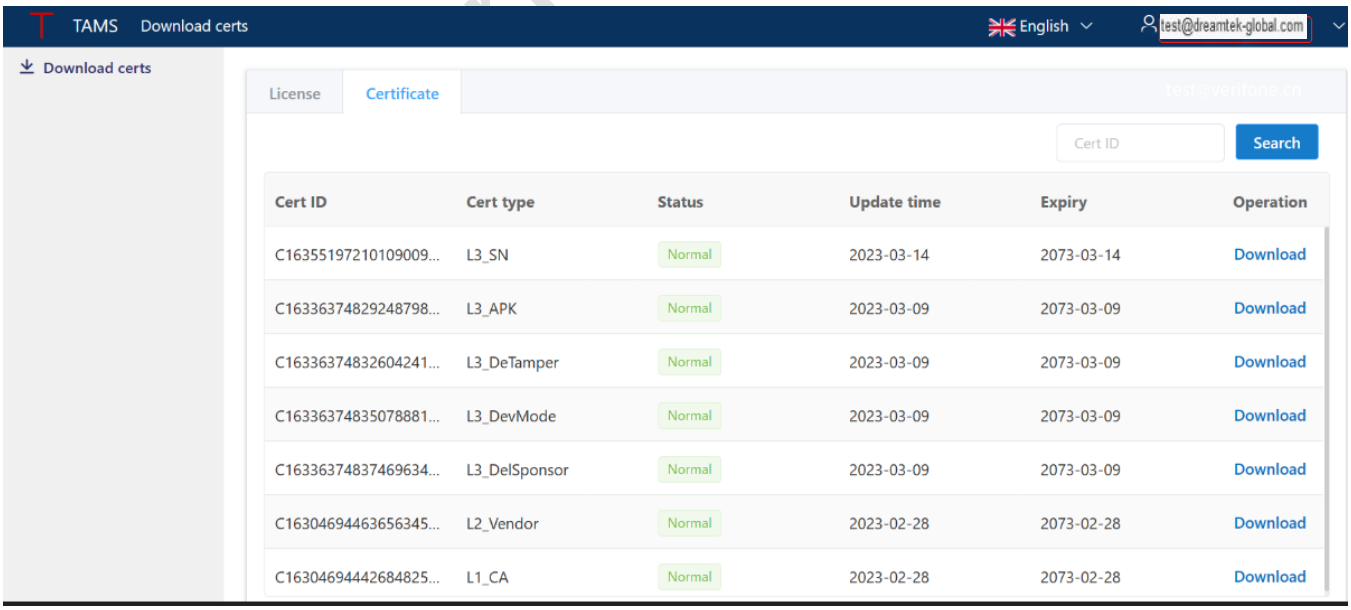
user name: test@dreamtek-global.com

password: sd9RVm338

Please change your password after the first login.

Thank you for using TAMS!
TAMS team

Step 3: Log in to TAMS according to the TAMS URL, user name and password in the red box in the picture in Step 2. The test user is taken as an example in the figure above. The successful login interface is shown below;

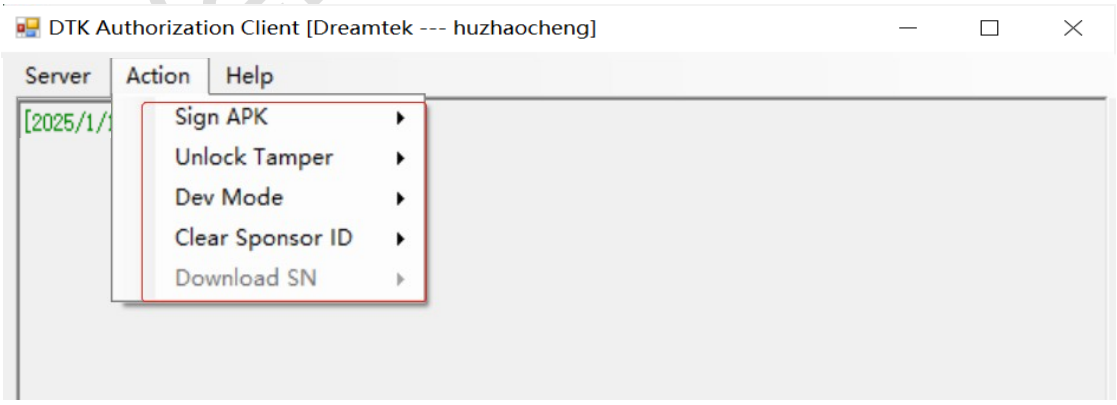


# 2.Introduction to the DTKAuthClient.exe tool

## 2.1 Introduction to Tool Interface

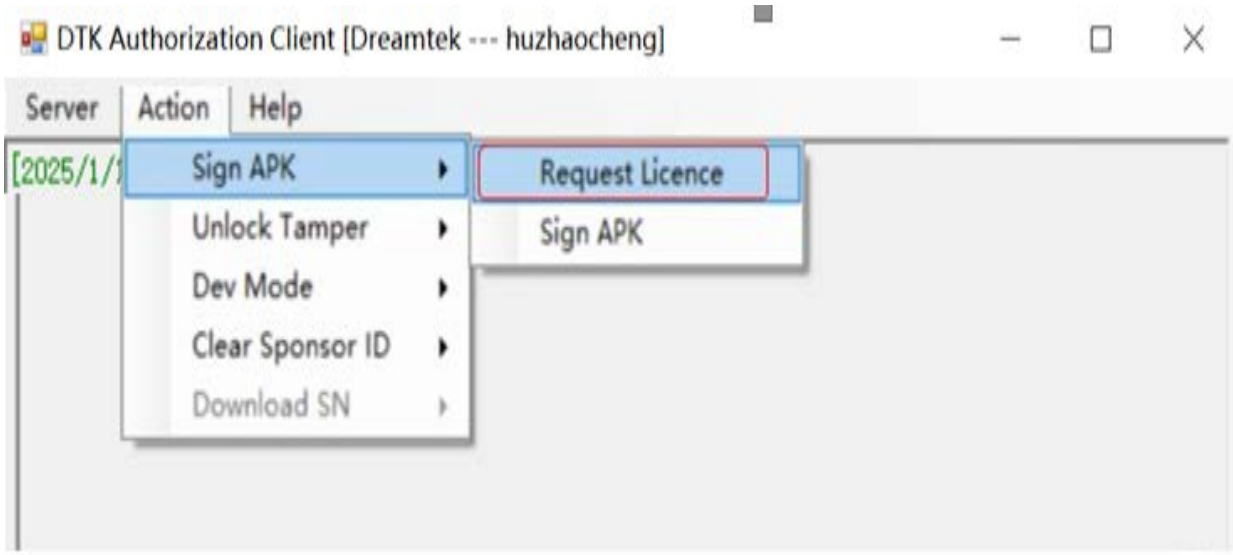

Step 1: Click the "Server" drop-down list to perform the "Logon" and "Exit" operations of the tool. You can log in successfully by using the correct account and password applied.


Step 2: The "Action" function can only be used normally after successful login. Click "Action" to select the option to be operated, as shown in the following figure:



## 2.2 Request licence

You need to apply for permission separately before using each function in the "Action", and you need to apply for permission first when using each function. This section takes the application of "Sign APK" as an example, and the application method for other functions is the same:




Step 1: Click "Request Licence" as shown above to complete the licence application, and wait for the review personnel after the application;

Step 2: Open TAMS and click "License" to view the approved license, as shown below:

| Application ID | Status | Approver | Remaining limit | Approved daily limit | Expiry | Approval time | Application time | Operation |
|---|---|---|---|---|---|---|---|---|
| snWrite202... | Approved | Mei Xiang | 9993 / 10000 | 0 / 100 | 2026-03-11 | 2023-03-14 | 2023-03-14 | Download |

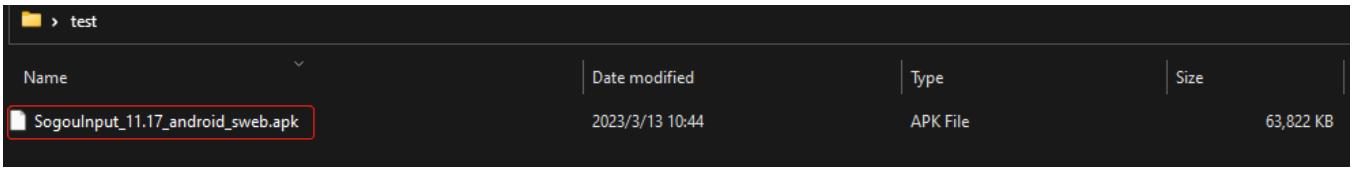
## 2.3 Function introduction under Action

Before operating the functions in the Action, it is necessary to apply for the license separately. After the application is completed, login to TAMS and download the approved license certificate and put it into the same root directory as DTKAuthClient.exe. The certificate is shown in Section 2.2.

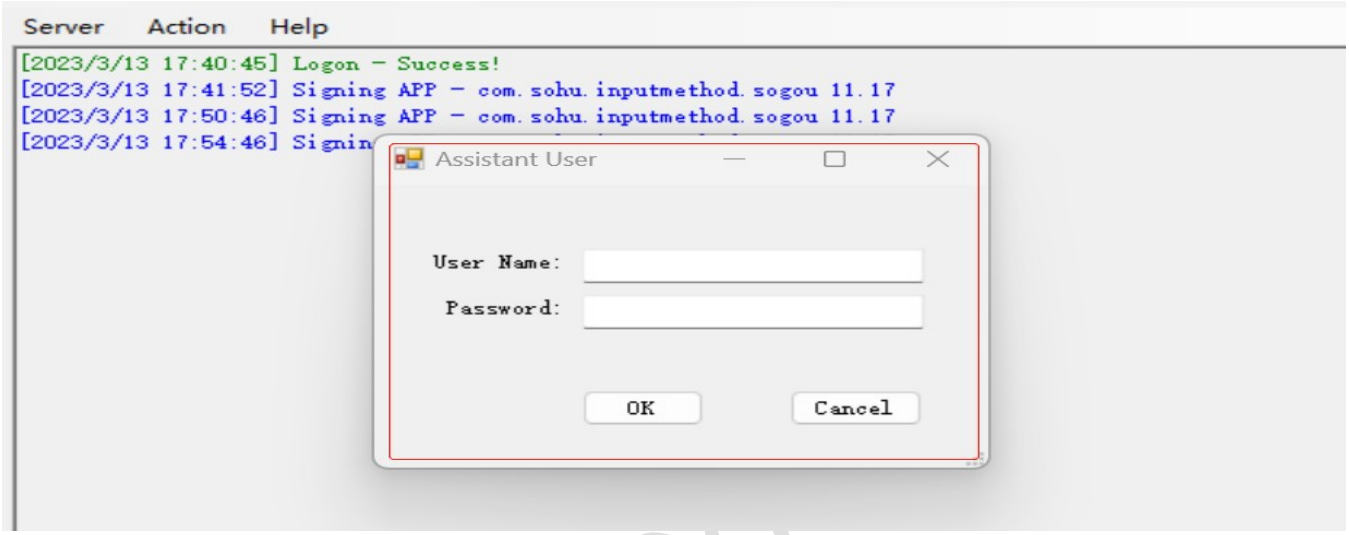
### 2.3.1 Sign APK Function

Since only APKs that have been verified and signed can be installed on devices, APKs need to be signed before installation. This section takes Sogou input method as an example to introduce:

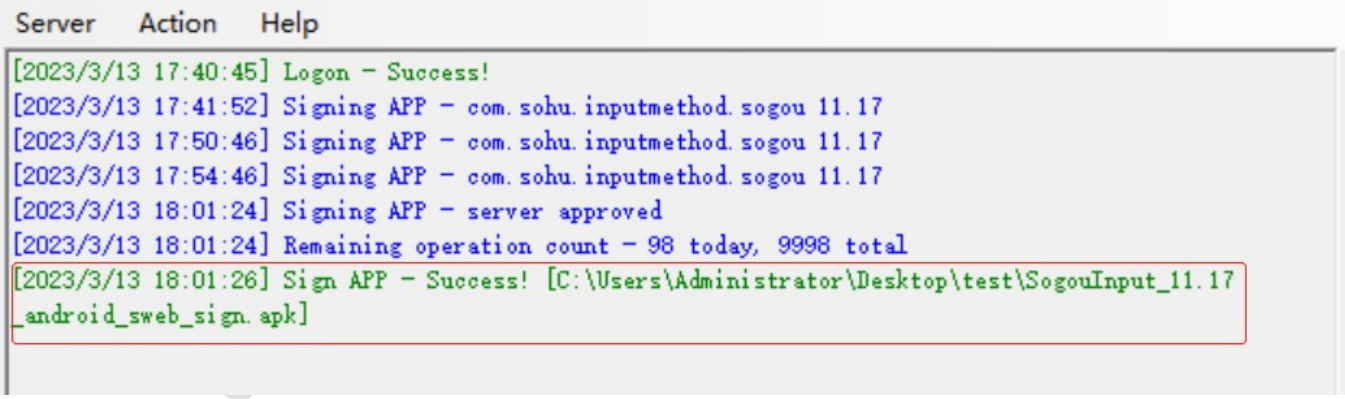
Step 1: Click Sign SPK in "Sign SPK" under "Action" to select the signed Sogou input method APK application, as shown below:



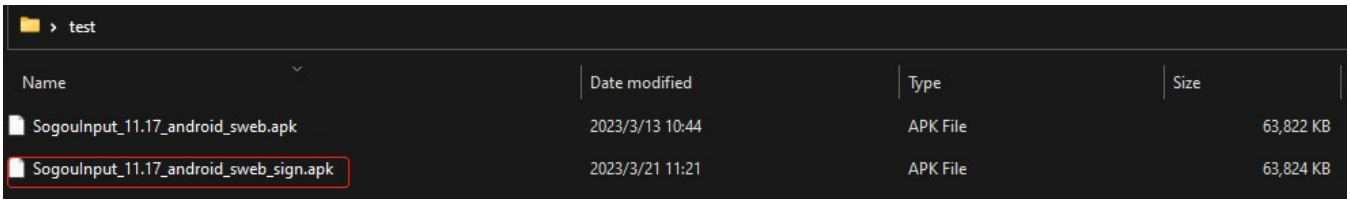

Step 2: Select "SogouInput_11.17_android_sweb.apk" and click the open button in the above image. The "Assistant User" user confirmation will pop up, as shown below:




Step 3: The username and password in the above picture need to use the secondary account of the same institution for login confirmation. Enter the correct username and password and click "OK" to generate the signed APK file. The path of the signed APK is shown below:



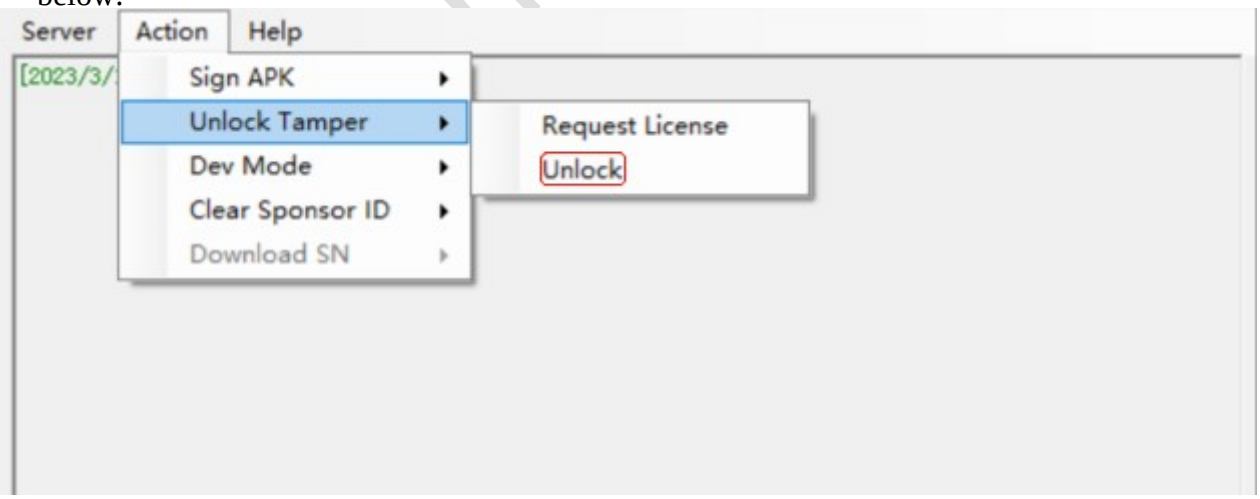

Step 4: "SogouInput_11.17_android_sweb_sign.apk" is the signed APK file, as shown in the following figure:



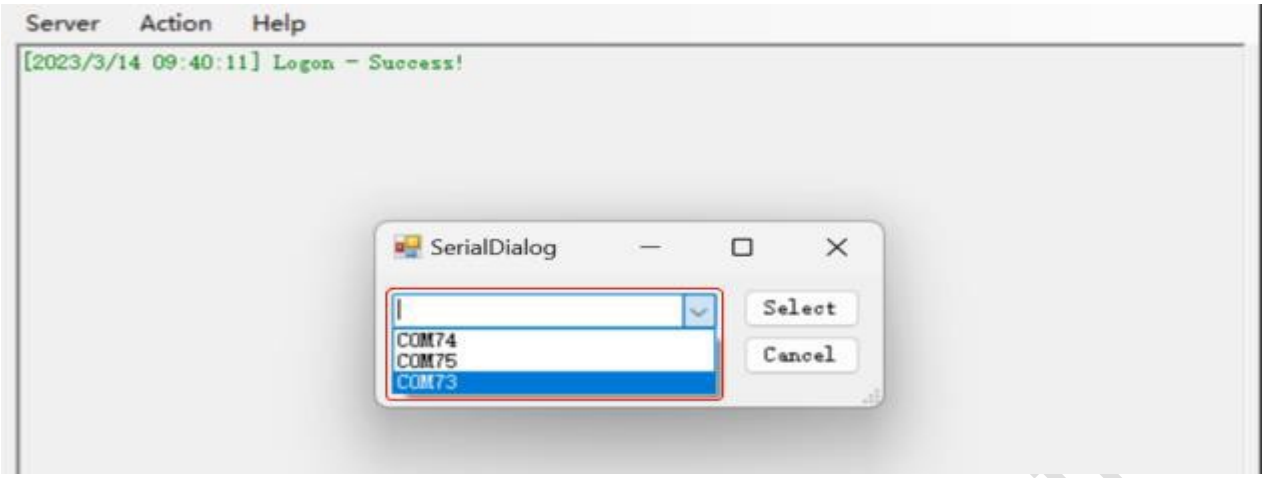
## 2.3.2 Unlock Tamper Function

This section describes how to use the "DTKAuthClient.exe" tool to unlock the triggered tamper. This section takes the key authentication failure as an example, and other trigger unlocking is the same.
Step 1: After tamper is triggered, the devices screen is displayed as follows:

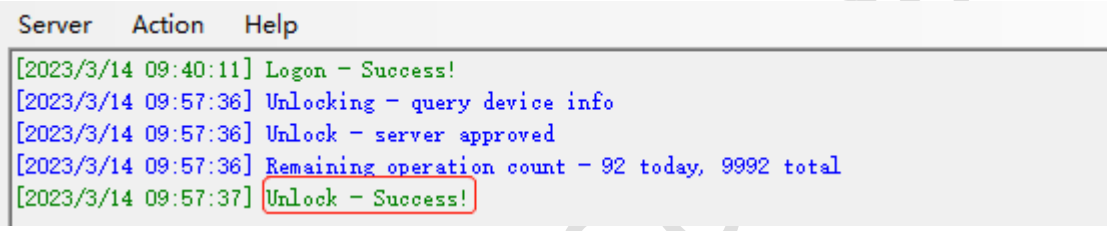

1. Step 2: Connect the Devices to the PC through the data cable, then log in to "DTKAuthClient.exe" and select the "Unlock" option in the "Unlock Tamper" of the Action drop-down list, as shown below:




Step 3: Click the "Unlock" button in the above figure to enter the port selection list in the following figure, and select the "DTK Smart POS COM(S1)" port, which can be confirmed by checking the "Port" in the "Device Manager" of the local PC.



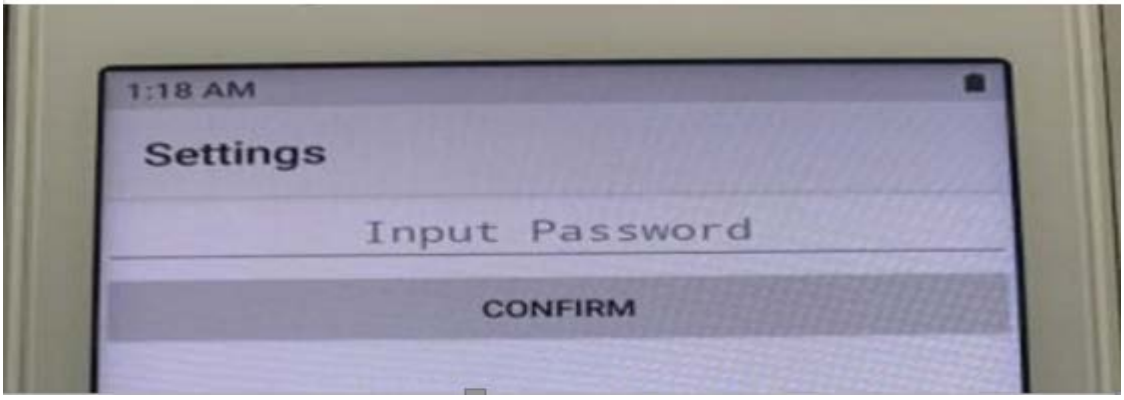

Step 4: Select the correct port and click "Select" to complete tamper unlocking. The result printed by the host computer is as follows:



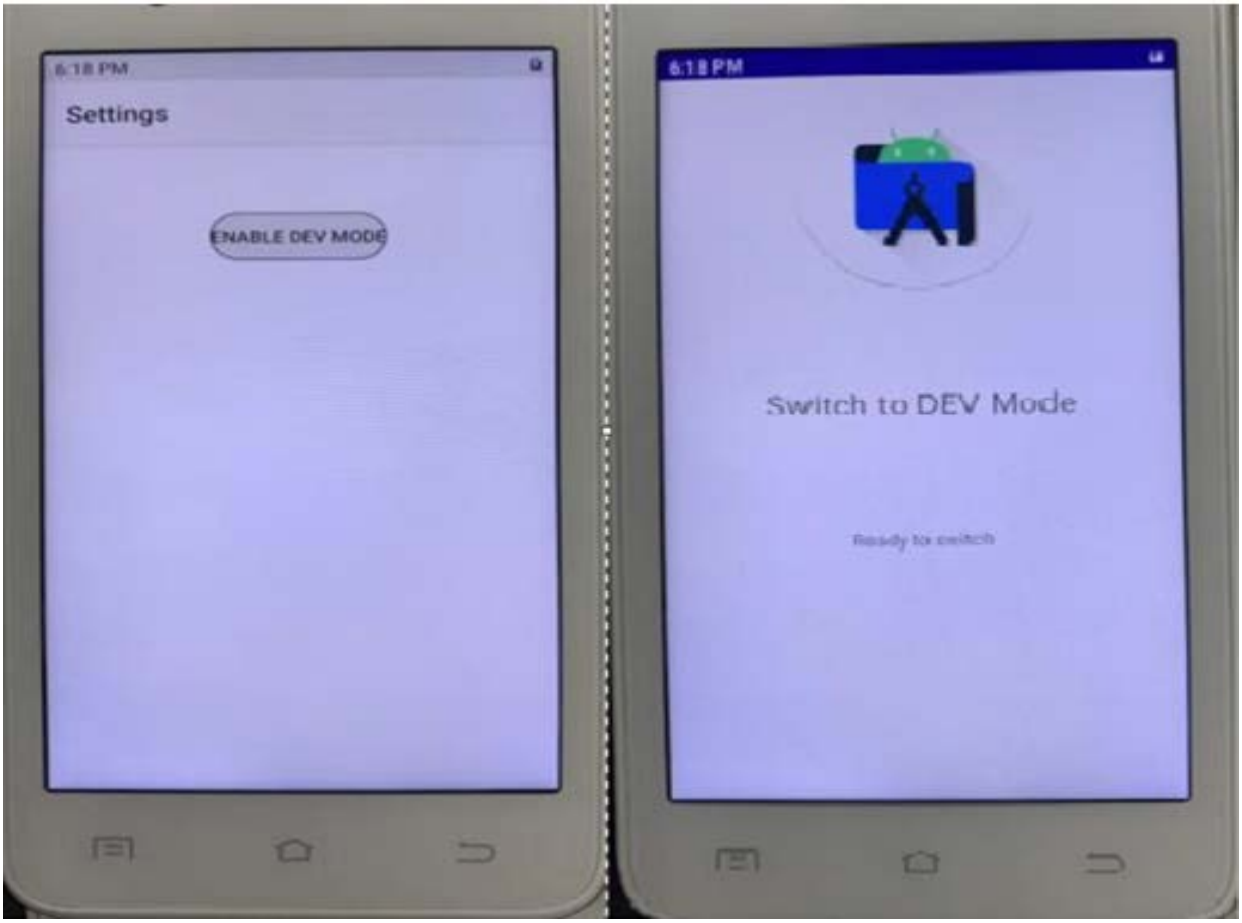

## 2.3.3 Dev Mode Function

The Devices physical buttons are shown below

Step 1: Open Devices flight mode and touch "left right middle middle left left right" in the physical button in the above picture successively in order to open the verification interface as shown below


1:18 AM
Settings
Input Password
CONFIRM

Step 2: Enter the password "Z6C6831v" in the above figure to enter the "ENABLE DEV MODE" as shown below on the left. Click "ENABLE DEV MODE" to enter the "Switch to DEV Mode" interface as shown below on the right:



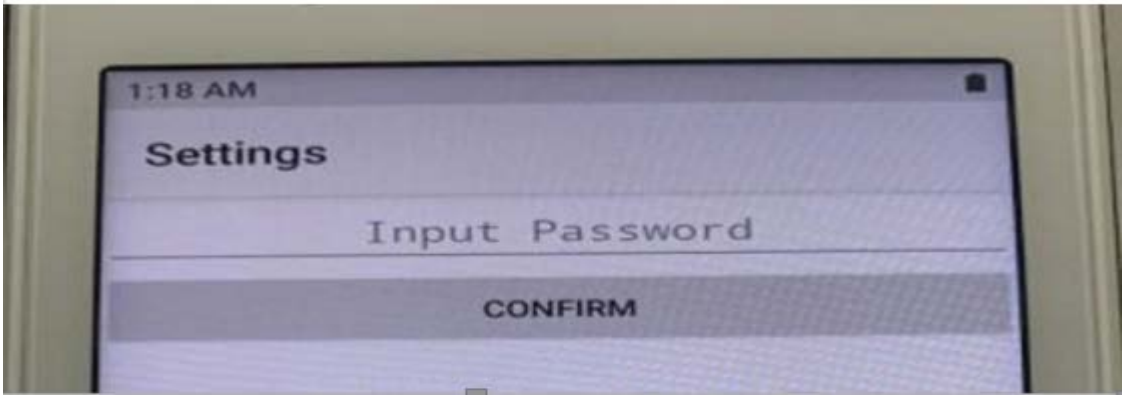

Step 3: Connect the Devices to the PC through the data cable, then log in to "DTKAuthClient.exe", select the "Switch to DEV mode" option in the "DEV mode" of the Action drop-down list, as shown below:

Step 4: Click "Switch to DEV Mode" in the figure above to enter the port selection interface and select the port of "DTK Smart POS COM(S1)". This port can be confirmed by checking the "Port" in the "Device Manager" of the local PC.


Step 5: Select the correct port and keep the devices screen constant state, otherwise the operation will fail. Click "Select" in the figure above to complete the developer mode switch, as shown below


## 2.3.4 Clear Sponsor ID Function

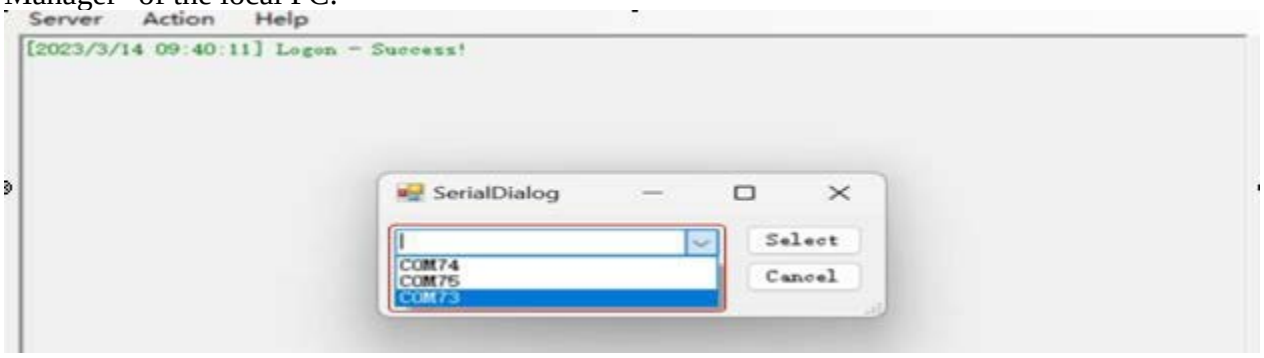
Step 1: Open devices flight mode, and continuously touch "left right middle middle left left right" in the devices physical button in order to open the verification interface as shown below:



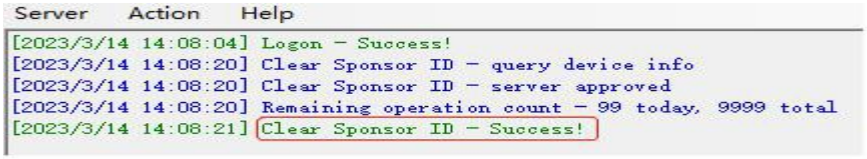

Step 2: Enter the password "Z166831" in the above image and you will see the pre-installed application of the devices. Select "Clear Sponsor" to enter the "Clear Sponsor ID" screen, as shown below:

Step 3: Connect the devices to the PC through the data cable, then log in to "DTKAuthClient.exe", select the "Clear Sponsor ID" option in the Action drop-down list, as shown below:


Step 4: Click "Clear Sponsor ID" in the figure above to enter the port selection interface, and select the port of "DTK Smart POS COM(S1)". This port can be confirmed by checking "Port" in the "Device Manager" of the local PC.



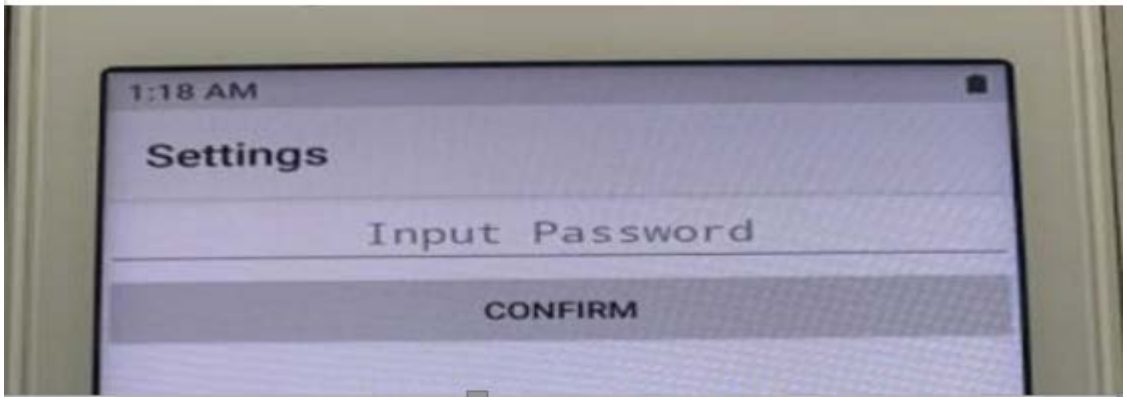
Step 5: Click "Select" in the figure above to clear the Sponsor ID. After clearing, the result is shown below:



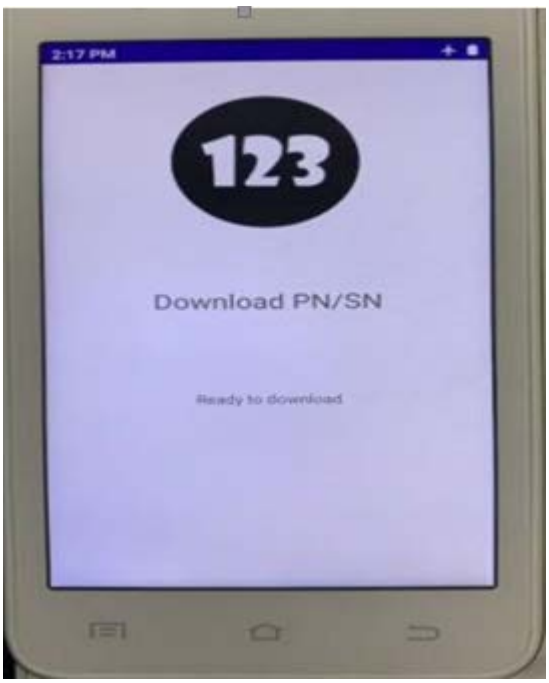


## 2.3.5 Download SN Function

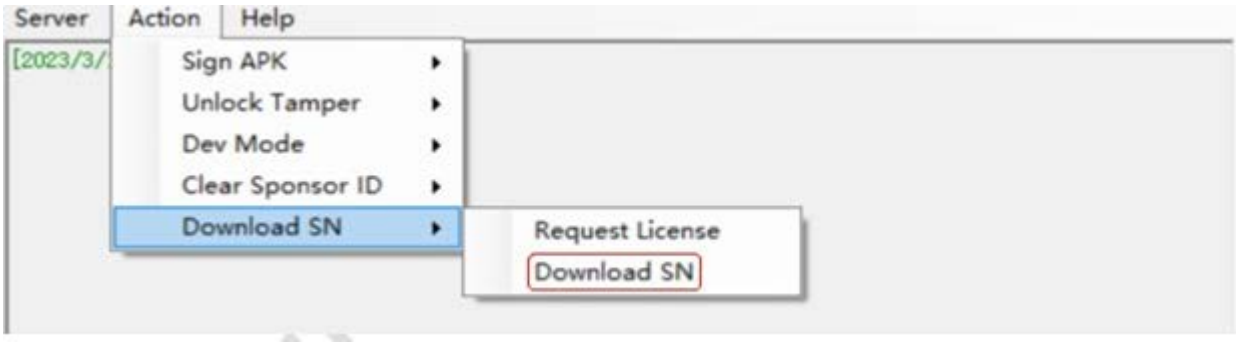
Step 1: Open X990mini Flying Moss, and continuously touch "left right middle middle left left right" in the X990mini physical button in order to open the verification interface as shown below:



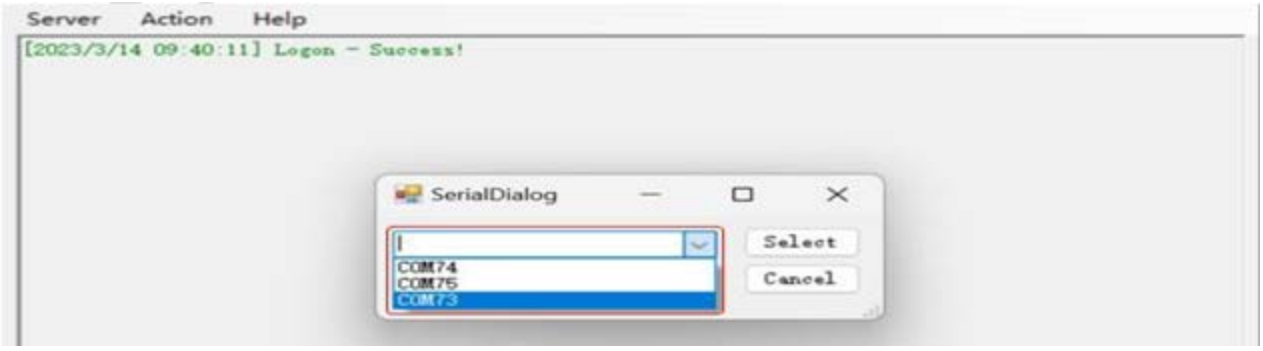
Step 2: Enter the password "Z166831" in the figure above to see the pre-installed application of the devices after successful verification. Select "SN Download" to enter the "Download PN/SN" interface, as shown below:



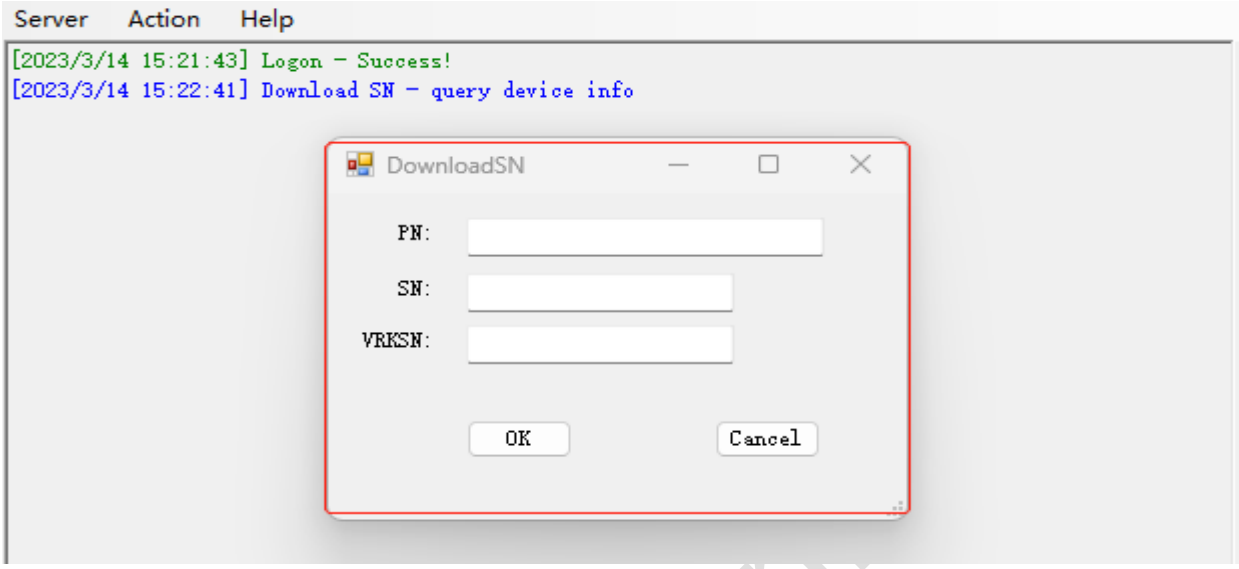

Step 3: Connect the devices to the PC through the data cable, then log in to "DTKAuthClient.exe" and select the "Download SN" option in the "Download SN" Action drop-down list, as shown below:




Step 4: Click "Downlaod SN" in the figure above to enter the port selection interface, and select "DTK Smart POS COM(S1)" port. This port can be confirmed by checking "Port" in "Device Manager" of the local PC .

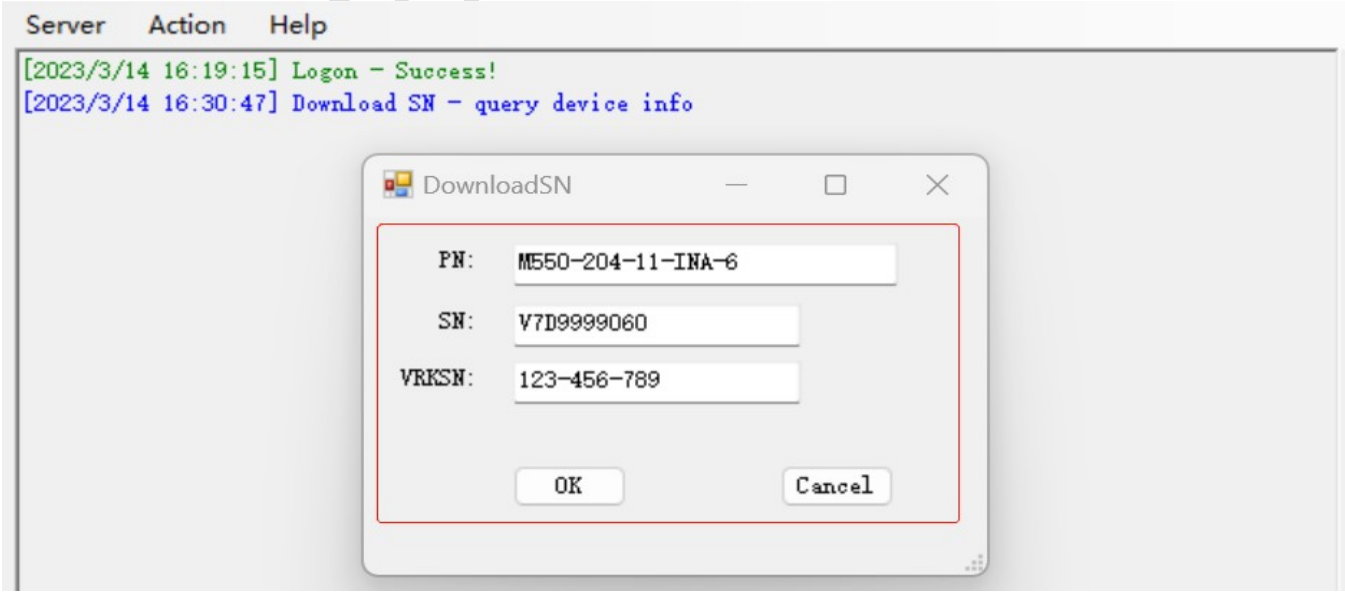

Server
Action
Help
[2023/3/14 09:40:11] Logon - Success!
SerialDialog
COM74
COM75
COM73
Select
Cancel

Step 5: Select the correct port and keep the devices screen constant, otherwise the operation will fail. Click "Select" and the PN\SN\VRKSN input interface will pop up, as shown in the following figure




Step 6: The interface for input PN\SN\VRKSN information in the above figure is shown below:

Note: The PN format is: 4-3-2-3-1 character format;
SN format is: 9 characters starting with V;
The VRKSN format is: 3-3-3 character format.



Step 7: Click "OK" to finish writing SN\PN. The pictures before and after writing are shown below. The left is the picture without writing SN\PN, and the left is the picture after writing SN\PN. Open Devices "setting" and click "About terminal" to enter "configuration info" to see SN\PN related information: