DS50 Smart Tool Operation Guide

Version: V1.00

Version update record

No	VER	DATE	REVISION	AUTHOR	AUDITOR
1	V1.00	2024-12-10	Initial release	HGJ	FYM

Catalogue

1 Summary

The Smart Tool Kit is a windows tool developed by SUNYARD, mainly used to maintain the products developed and produced by SUNYARD: S20/S60/S60P, its main functions include: Download File, key/cert, File signature, Terminal Maintenance and Write/Check SN.

The main interface of the tool is shown as follows:
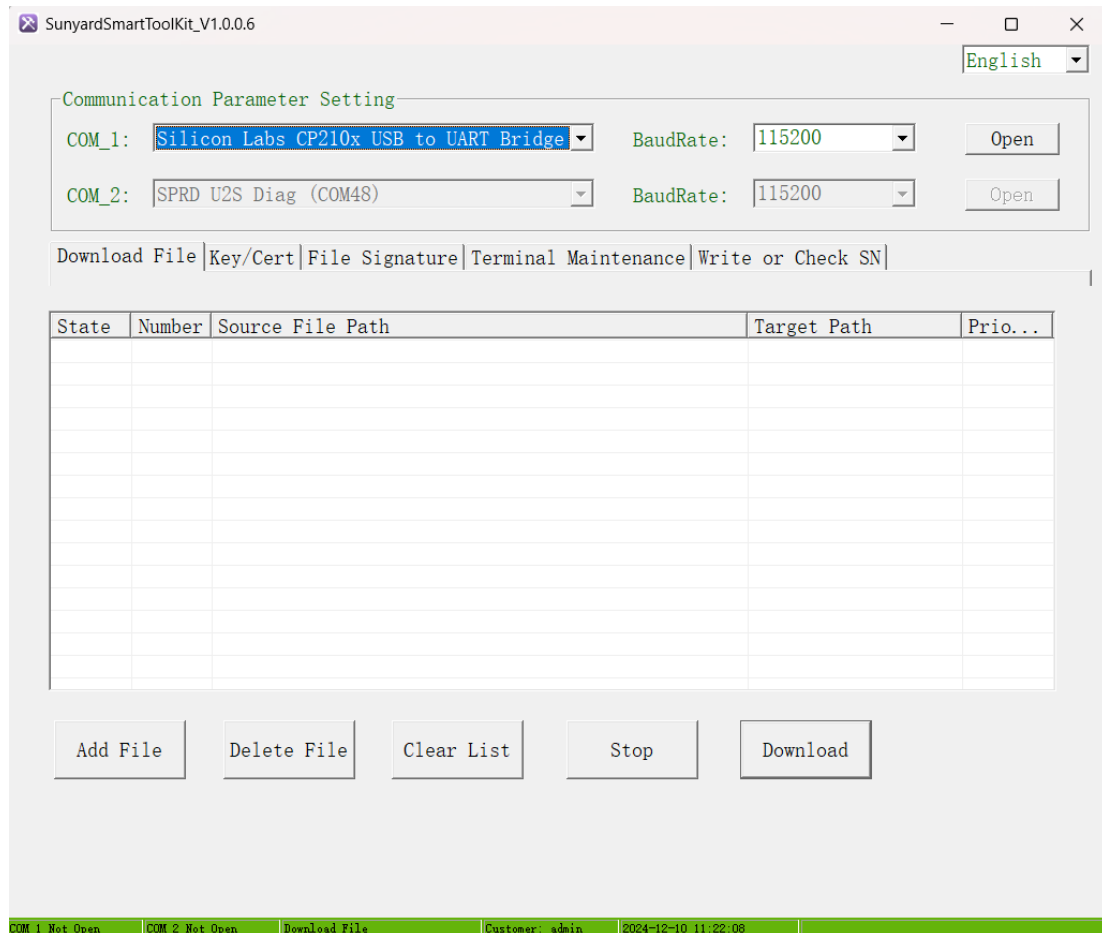
2 Communication Port Settings

The communication method of this tool is serial port communication. Please ensure that the driver for the POS terminal has been installed before use.
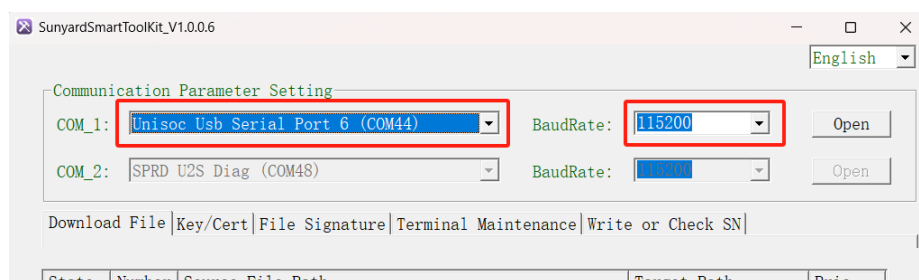
The driver installation for each POS terminal is different. Please refer to the corresponding operation manual.

2.1 DS50 Driver Installation
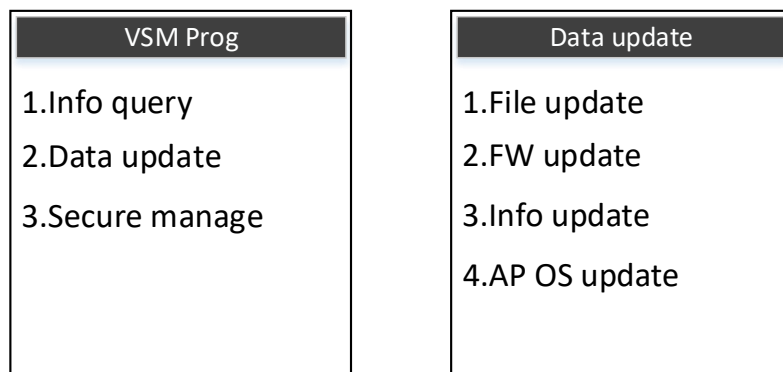
● **Driver**

Install the driver: S20_module_usb_driver

Note: Please select Computer Management (Local)->System Tools->Device Manager->Port (COM&LPT)-> Unisoc
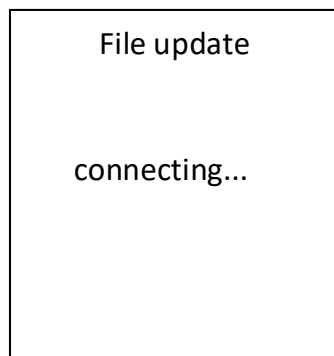
Usb Serial Port 6, BaudRate set to 115200.

3 DS50

Press and hold the [0] key before turning on the power. Press the power button to start the device and enter the vendor's security management login interface. The login password is "520182". After logging in, you will enter the vendor's security management interface. Press [2] to enter the data update interface, and then select [1] or [2] based on the file you need to download. Insert the USB drive, open the SunyardSmartToolKit.exe download tool on your PC, select the desired download file, and click "Start Download" to begin the download process.
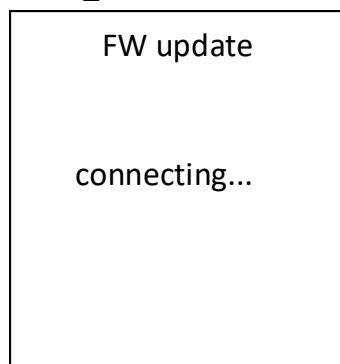
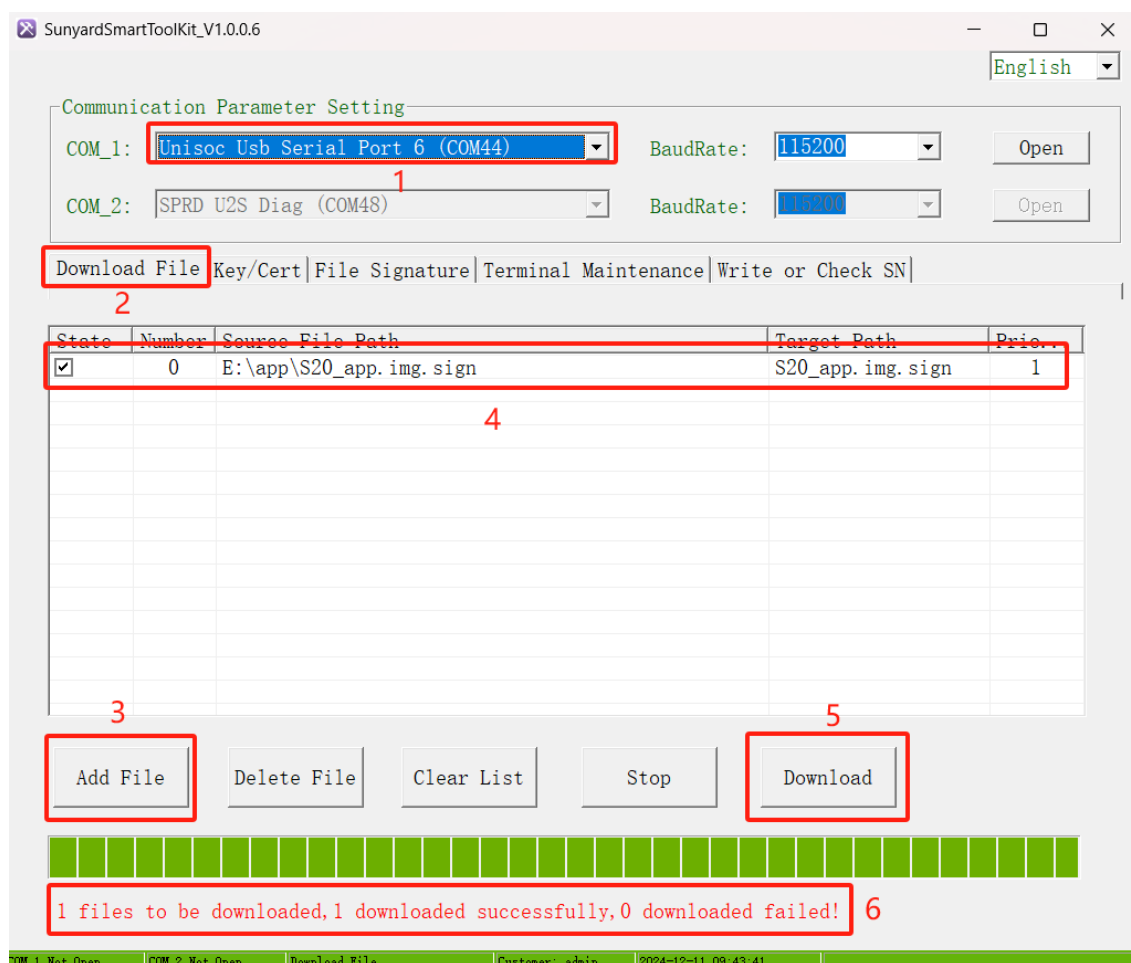The terminal interface is shown in the following figure:

VSM Prog
1.Info query
2.Data update
3.Secure manage

Data update
1.File update
2.FW update
3.Info update
4.AP OS update

1. Application, app.crt or resource file download:

File update
connecting...

2. S20_core.bin download:
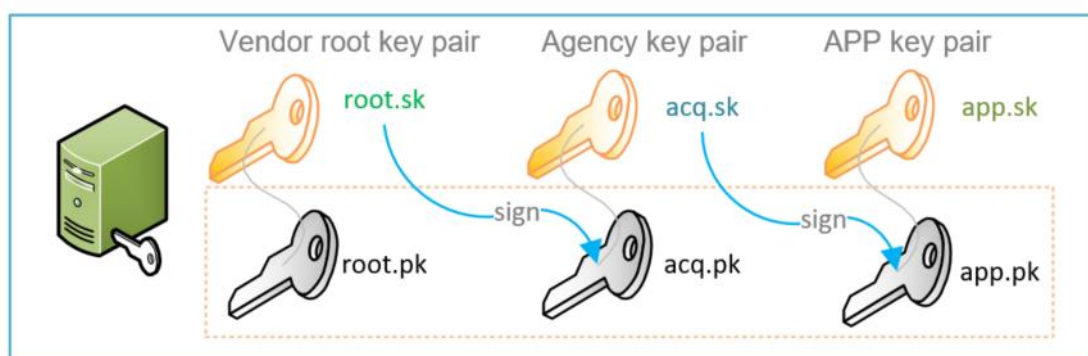
FW update
connecting...

The application download operation interface is as follows:

4 Key/Certificate

The tool SunyardSmartToolKit.exe can be used to generate RSA public and private key pairs and issue certificates (Temporarily only supports S20).
The solution about Key/Certificate is as follows:

The Agency need to generate one pairs of public and private keys：Acq.sk & Acq.pk.
The App need to generate one pairs of public and private keys ：App.sk & App.pk.
Note:
The ACQ key pair is generated by SUNYARD by default and is pre-installed in the terminal before shipment.
If you have a need to generate it yourself, please contact SUNYARD.
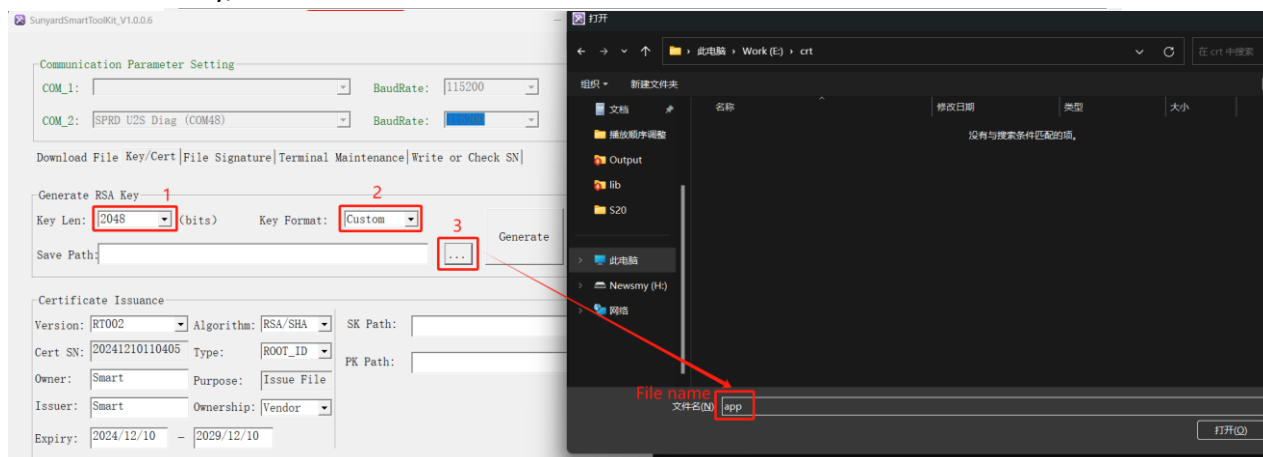1. The acq.crt or app.crt is generated by SUNYARD, please send acq.pk or app.pk file to SUNYARD Technology.

2. The app.crt need to be downloaded into the machine before download app.

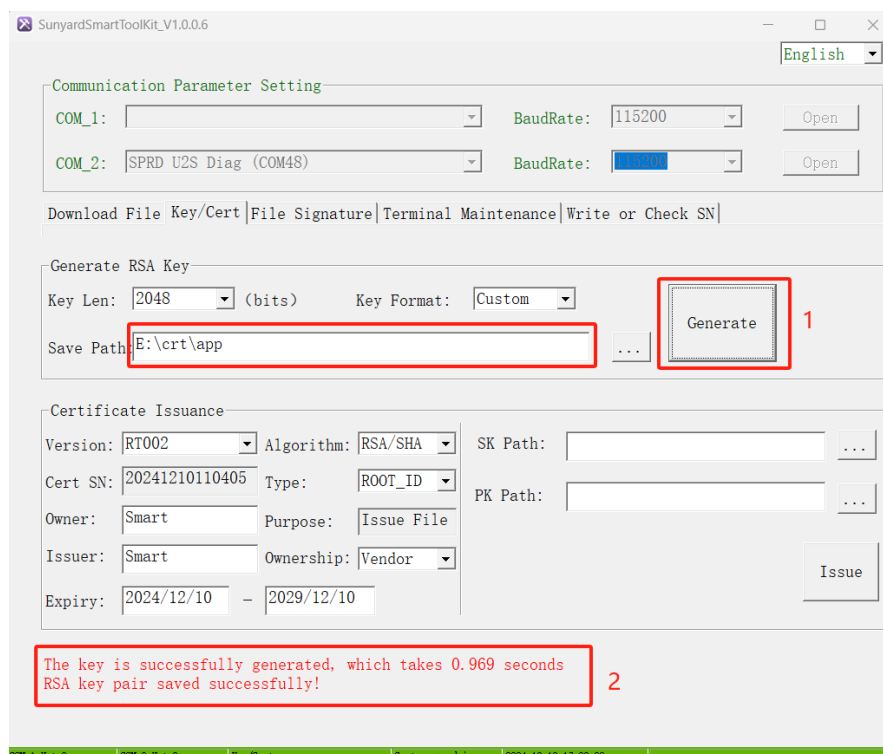The Key/Certificate relevant process is shown in the figure below:

4.1 Generate RSA key pair
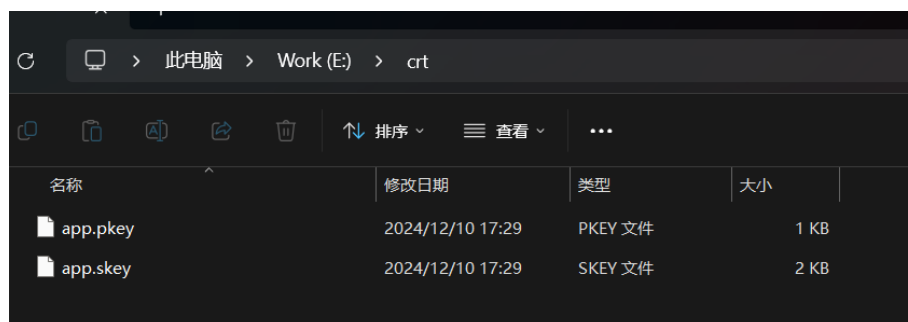
Step 1: Enter the Key/Cert menu.

Step 2: Select the key save path, enter key file name (**Note:** no suffix, and file name customization).

Step 3: Click the "Generate" button.

Step 4: The pkey & skey files are generated and can be found in the corresponding directory.

4.2 Certificate Issue

This step is currently completed by the manufacturer.

5 File Signature

After the application development is completed, the machine needs to use the corresponding certificate to sign the application file in the production mode, and only the signed file can be downloaded (Temporarily only supports S20).

- **File Signature**
  - ➢ **File Type**: S20_app.img
  - ➢ **Custom ID**: Item code, 5 digits
  - ➢ **APP Ver**: App Version, 4 digits
  - ➢ **Skey Path:** app.sk file path

➤ **File Path:** App file path that needs to be signed
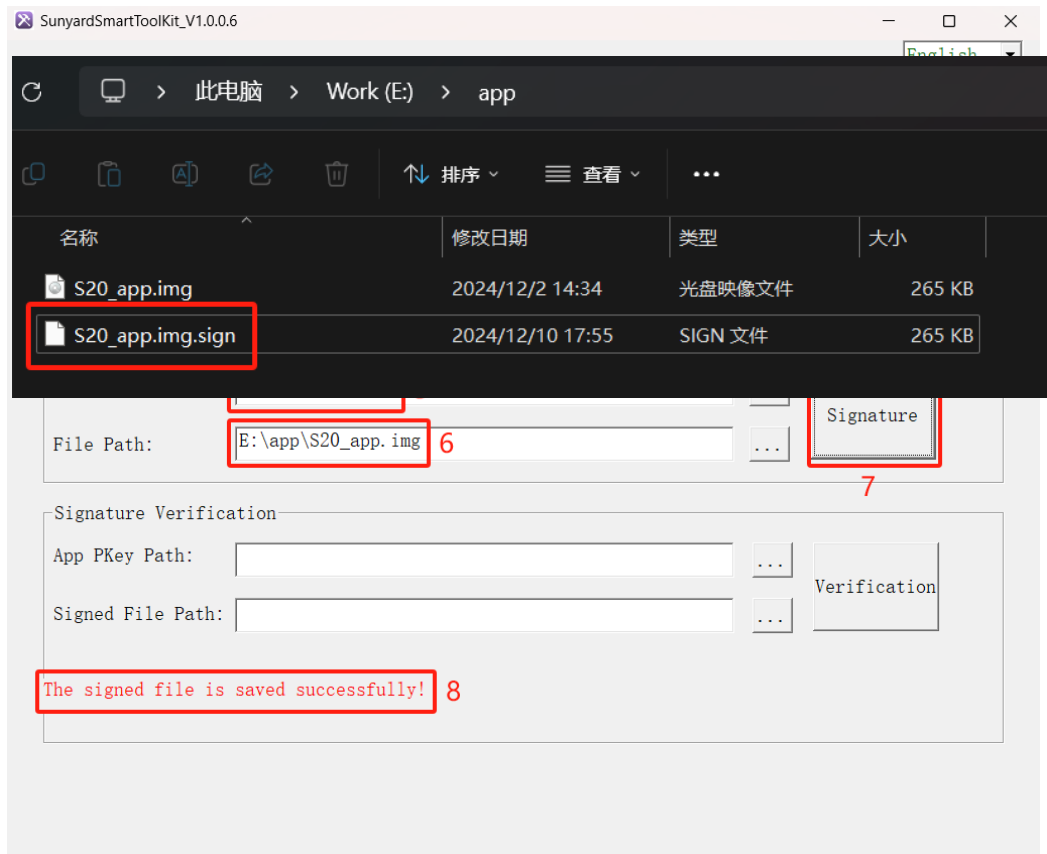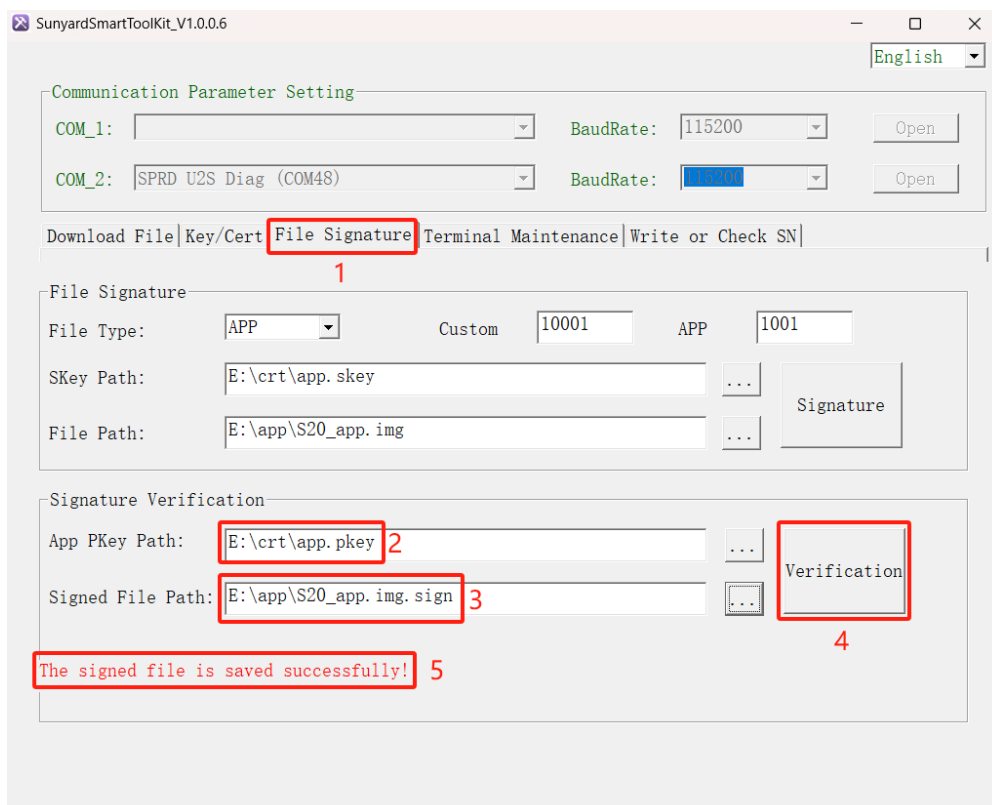

After the file is signed successfully.

After the application file is signed, you can use app.pk to verify the signature.

● **Signature Verification**

➤ **App PKey Path:** app.pk file path

➤ **Signed File Path:** app signature file path

6 Terminal Maintenance

When the terminal has triggered the screen lock, it needs to be unlocked. Press and hold the [0] key before turning on the power. Press the power button to start the device and enter the vendor's security management login interface. The login password is "520182". After logging in, you will enter the vendor's security management interface, select "2. Terminal Unlock". You can perform the unlock operation on this interface.
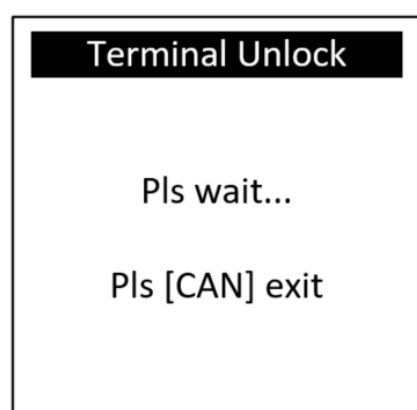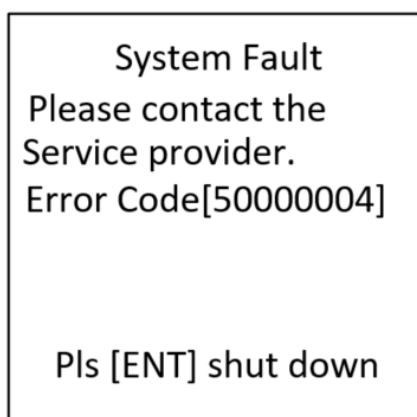
The application download operation interface is as follows:
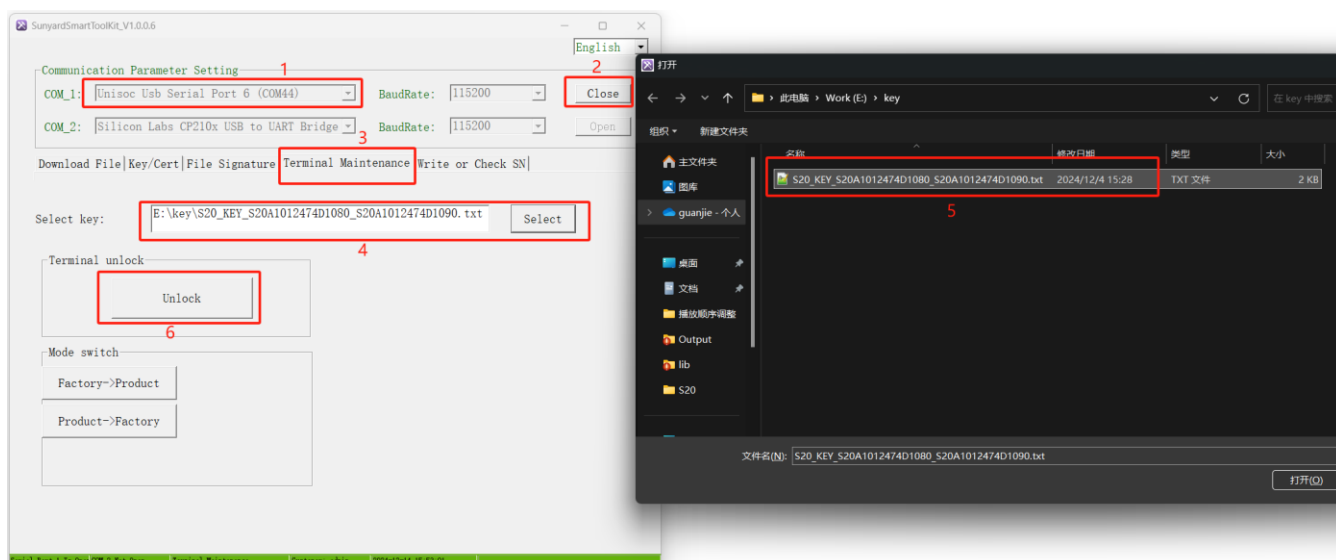
Note: The key file for authentication keys is provided by the manufacturer.

The unlocking is successful as shown in the following figure:
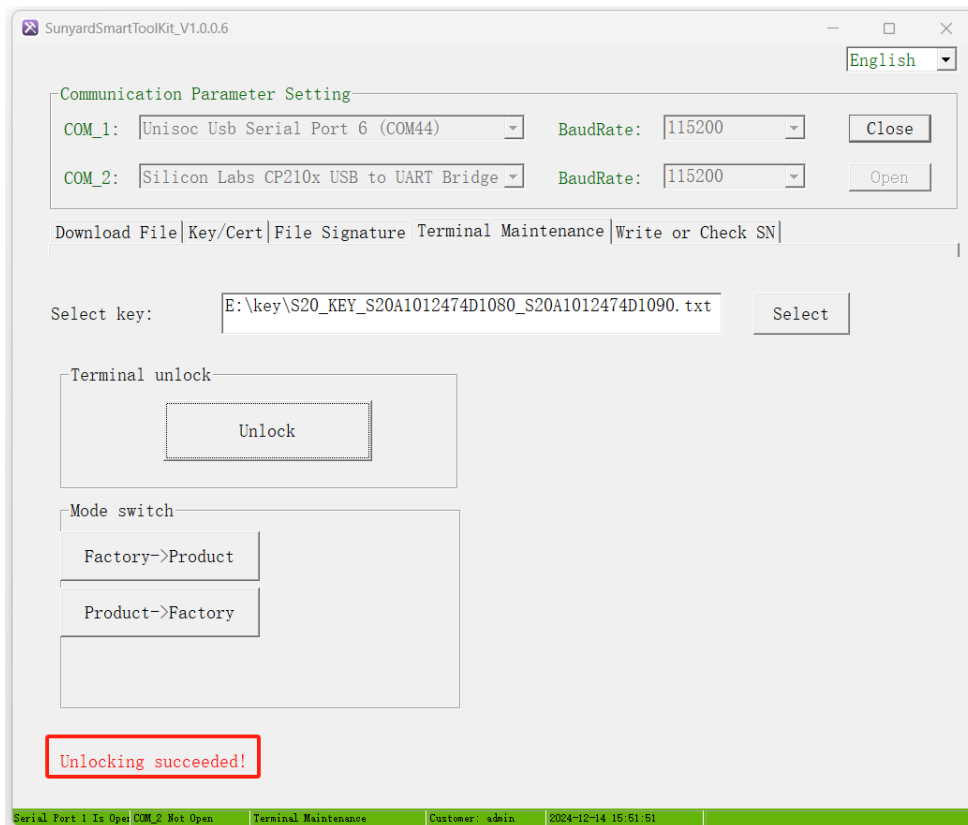
Abbreviations

SN   Terminal Serial Number

POS   Point of Sales

FW   Firmware

HW   Hardware

VSM   Vendor System Manage