



CASTLES TECHNOLOGY

SATURN1000 EFT-POS Terminal

User Manual

Confidential

Version 1.2

Oct. 2018

Castles Technology Co., Ltd.

6F, No. 207-5, Sec. 3, Beixin Rd., Xindian District,
New Taipei City 23143, Taiwan R.O.C.

<http://www.castech.com.tw>

WARNING

Information in this document is subject to change without prior notice.

No part of this publication may be reproduced, transmitted, stored in a retrieval system, nor translated into any human or computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual, or otherwise, without the prior written permission of **Castles Technology Co., Ltd.**

All trademarks mentioned are proprietary to their respective owners.

Revision History

Version	Date	Descriptions	Author
1.0	May.25, 2018	Initial creation.	John
1.1	Oct.04, 2018	Modify setup description	Aloha
1.2	Oct. 16, 2018	1. Add ch3.1 Main Screen 2. Add ch3.6 Settings 3. Modify ch4.1 from APK signing to File signing 4. Add CAP Generator Header Type in ch4.1	John

Contents

1. Introduction.....	5
2. Hardware Setup.....	6
2.1. Parts of the Terminal	6
2.2. Insert Battery	9
2.3. Insert SAM Card	10
2.4. Insert Paper Roll.....	11
2.5. Insert GSM SIM Card	12
2.6. Insert Memory card.....	13
3. Basic Operation	14
3.1. Main Screen	14
3.2. System Panel	15
3.3. Loader	18
3.4. Test Utility.....	20
3.3.1 APP Info.....	21
3.3.2 UI Test.....	22
3.3.3 Card Test	24
3.3.4 System Test.....	25
3.5. POS Demo	27
3.6. Setting	32
4. Secure File Loading.....	35
4.1. File Signing.....	35
4.2. CAP file loading.....	38
5. Key Injection	40
5.1. Preparation.....	40
5.2. Enter Key Injection AP.....	41
5.3. Inject Initial Key (KEK)	42
5.4. Generate TR31 Key Block	43
5.5. Inject Working Key.....	44
5.6. Information	46
5.7. Injected Key for Transaction AP.....	47

1. Introduction

This document provides a guideline for operating and configuring Castles SATURN1000 terminal.

The scope of this document includes setting up the terminal, basic operation, application lifecycle, and some advanced features.

2. Hardware Setup

2.1. Parts of the Terminal

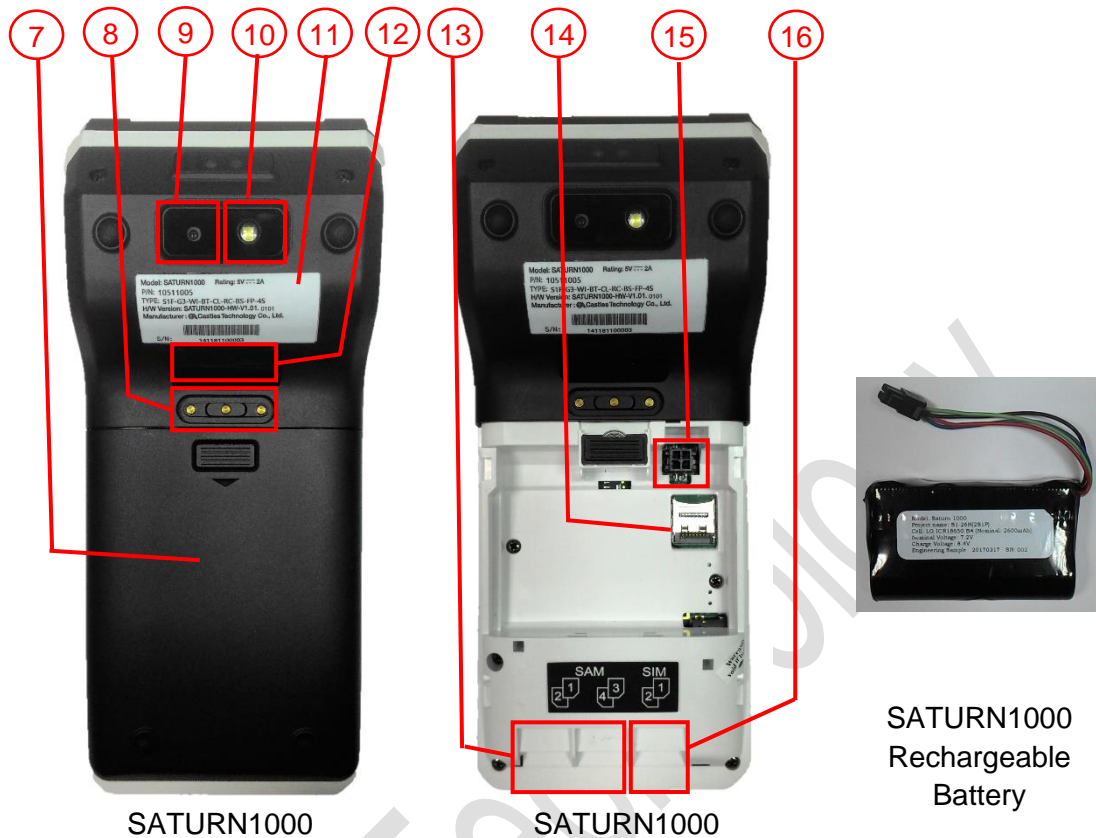
Front



- 1. Paper Roll Box
- 2. LCD Display (5.5")
- 3. Smart Card Reader
- 4. Magnetic Stripe Reader

- 5. Fingerprint identification area
- 6. Contactless Card Landing Zone

Rear



- 7. Rechargeable Battery Cover
- 8. The connector of charger cradle
- 9. Rear camera (500 MP)
- 10. Photo-flash
- 11. Product label
- 12. Scan button
- 13. SAM slots 1-4
- 14. Micro SD card slot
- 15. Battery connector
- 16. GSM SIM card slots 1-2
- 17. Barcode scanner (Front Camera)



Left side



18. Power Button

19. Micro USB slot

20. LED indicator

Green Light: External power source connecting

Red Light: Battery Charging function activated

21. Microphone

22. Headphone jack

23. Speaker

2.2. Insert Battery



Step 1: Press down the button and remove the battery cover.

Step 2: Insert the battery into the compartment.

Step 2-1: Mount the latches on the battery inner cover.

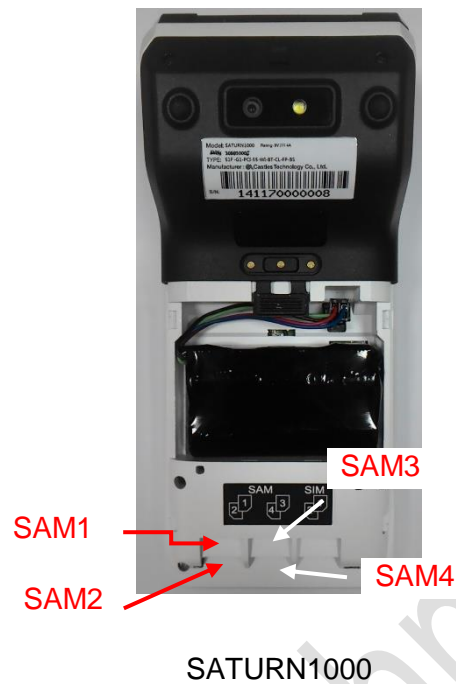
Step 2-2: Install the battery and plug in the contact point.

Step 2-3: Setup the upper side of battery inner cover to the correct position.
(The wires should be outside of the battery inner cover.)

Step 3: Reverse the operation of step 1 to install the battery cover.

Note: Please confirm the battery is installed before power on the terminal.

2.3. Insert SAM Card



Step 1: Remove battery cover / back cover

Step 2: Insert SAM card into desire slot.



SAM 1 & 3:

Gold contact is on the upper side of the card and facing down.



SAM 2 & 4:

Gold contact is on the upper side of the card and facing up.

Step 3: Reverse the operation of step 1 to install the battery cover.

2.4. Insert Paper Roll



Step 1: Pull up paper roll box handle.

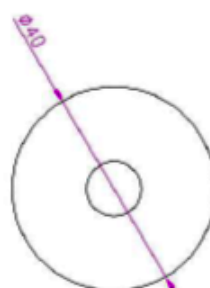
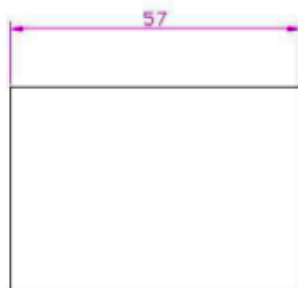
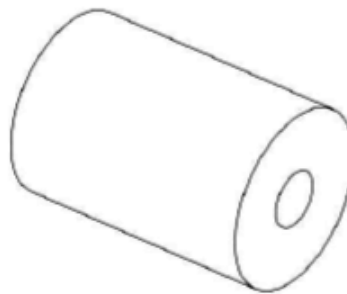
Step 2: Open paper roll cover gently.

Step 3: Insert paper roll as direction shown.

Paper specification

Width: 57mm

Outside diameter: 40mm



2.5. Insert GSM SIM Card



SATURN1000

Step 1: Remove battery cover / back cover

Step 2: Open SIM socket and insert GSM SIM card into desire slot.



SIM 1:

Gold contact is on the upper side of the card and facing down.

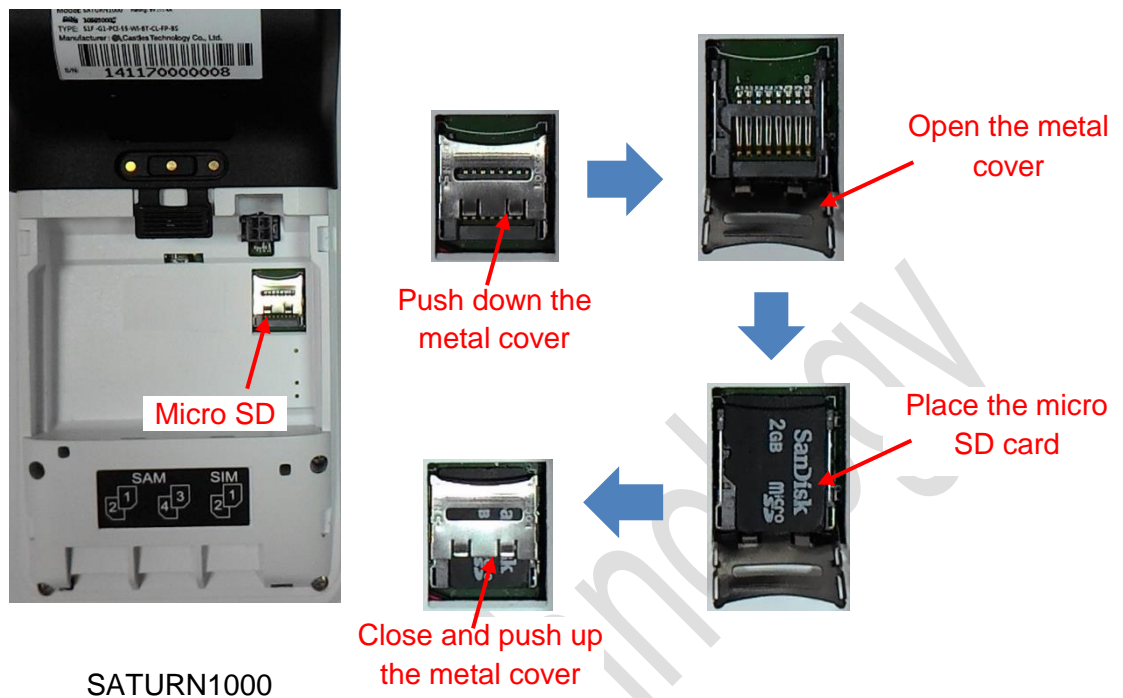


SIM 2:

Gold contact is on the upper side of the card and facing up.

Step 3: Reverse the operation of step 1 to install the battery cover.

2.6. Insert Memory card



Step 1: Remove battery cover / back cover

Step 2: Place Micro SD memory card.

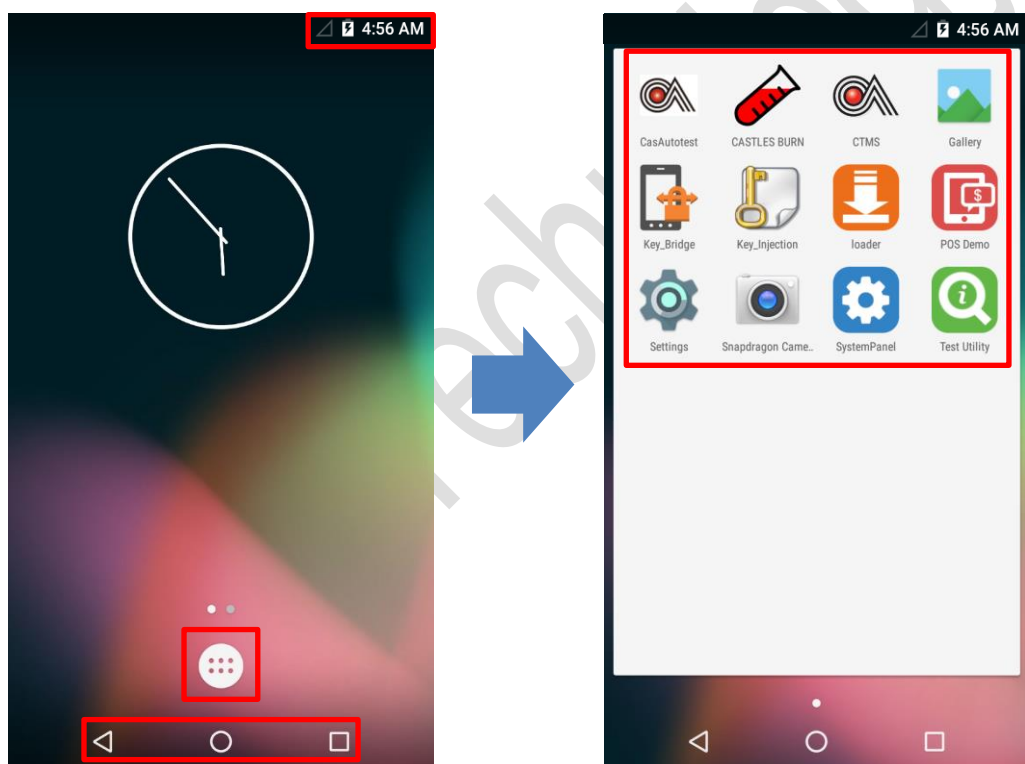
Step 3: Reverse the operation of step 1 to install the battery cover.







3. Basic Operation

Once the power is on in normal status, the terminal will enter Launcher if no default application selected. All user applications are listed in the launcher. Users can click on an application and run the application. Castles provide applications “System Panel”, “loader”, “Test Utility” and “POS Demo” for development use.

3.1. Main Screen

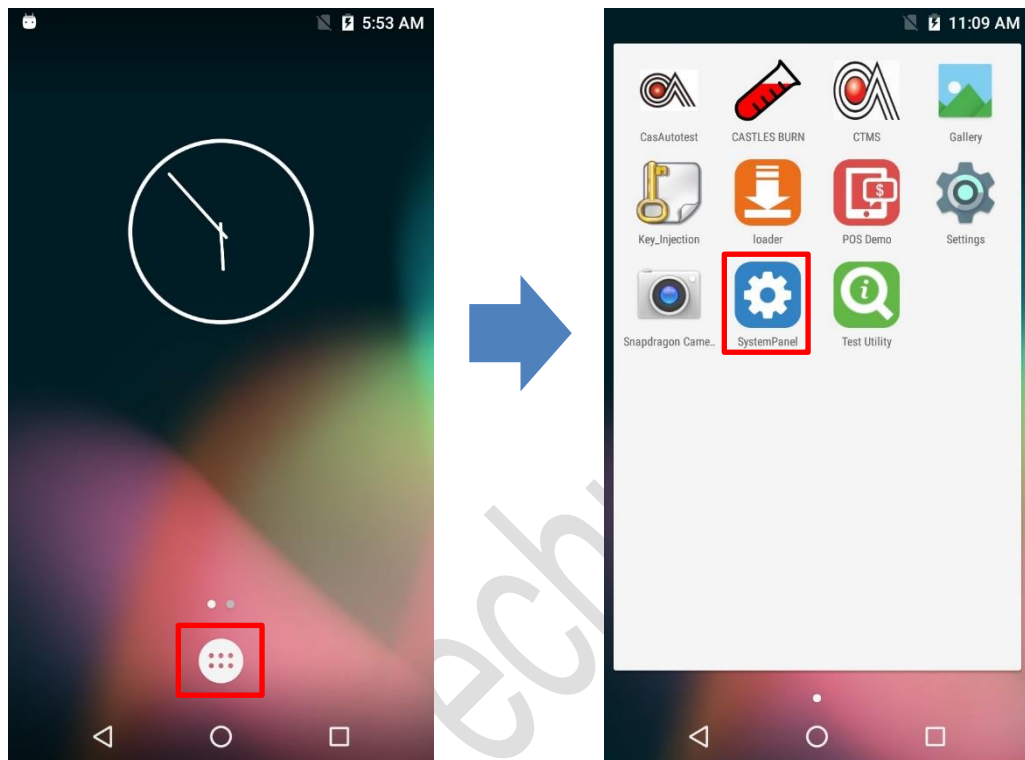
On the terminal, it provides some features for developers, and also have the simple symbols let users know the feature situation (e.g. internet, battery... etc.)



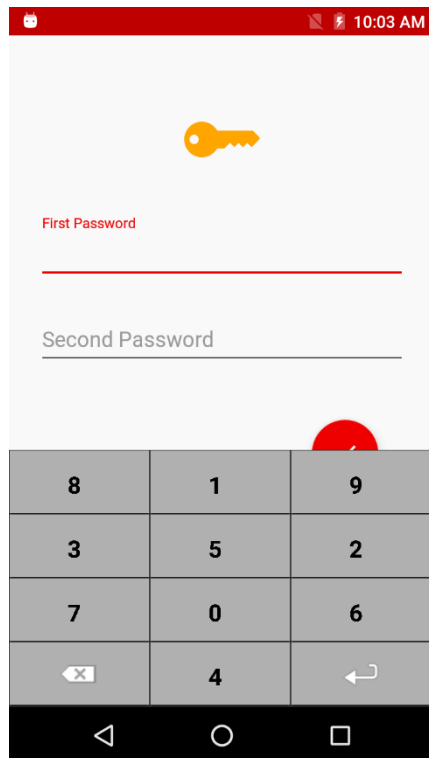
-  : APP menu
-  : GPRS signal
-  : Battery level
-  : Back to previous
-  : Back to Main screen
-  : View executed applications

3.2. System Panel

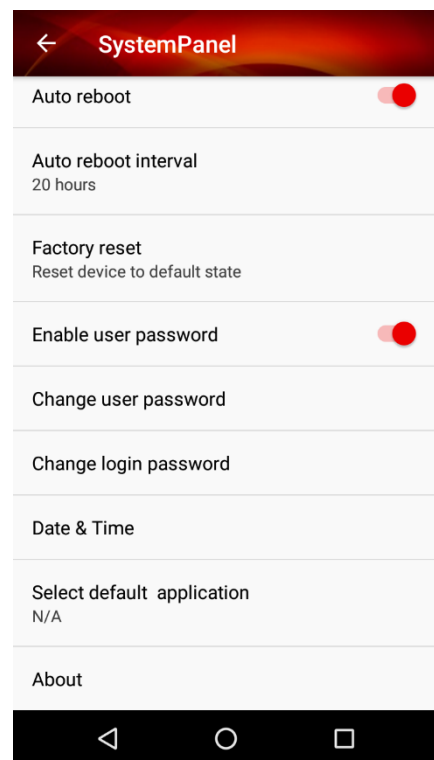
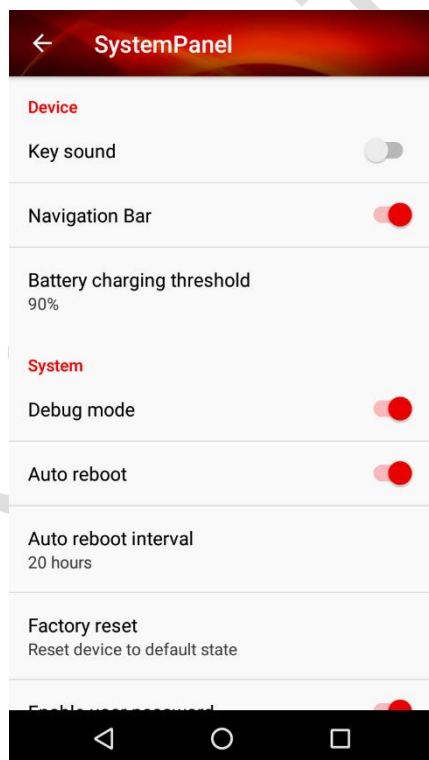
The developer can use the system panel to set system settings and check system versions.



- Click on [App menu].
- Click on [SystemPanel].



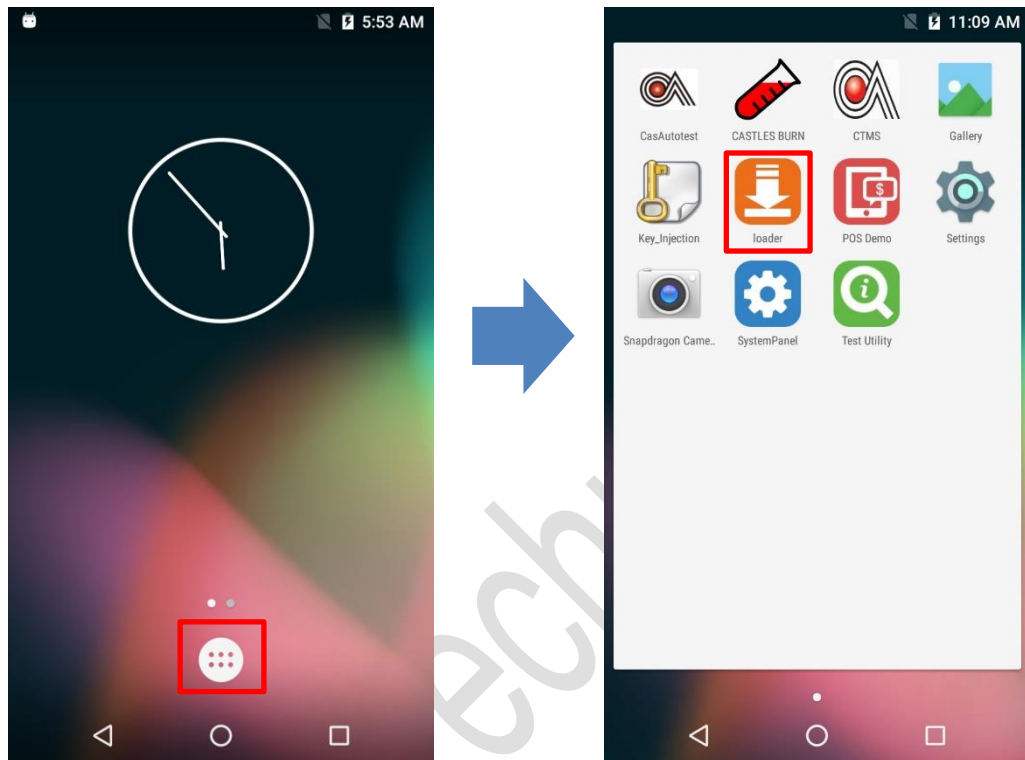
- Use random number keypad to enter the default password '00000000' to both of first password and second password.



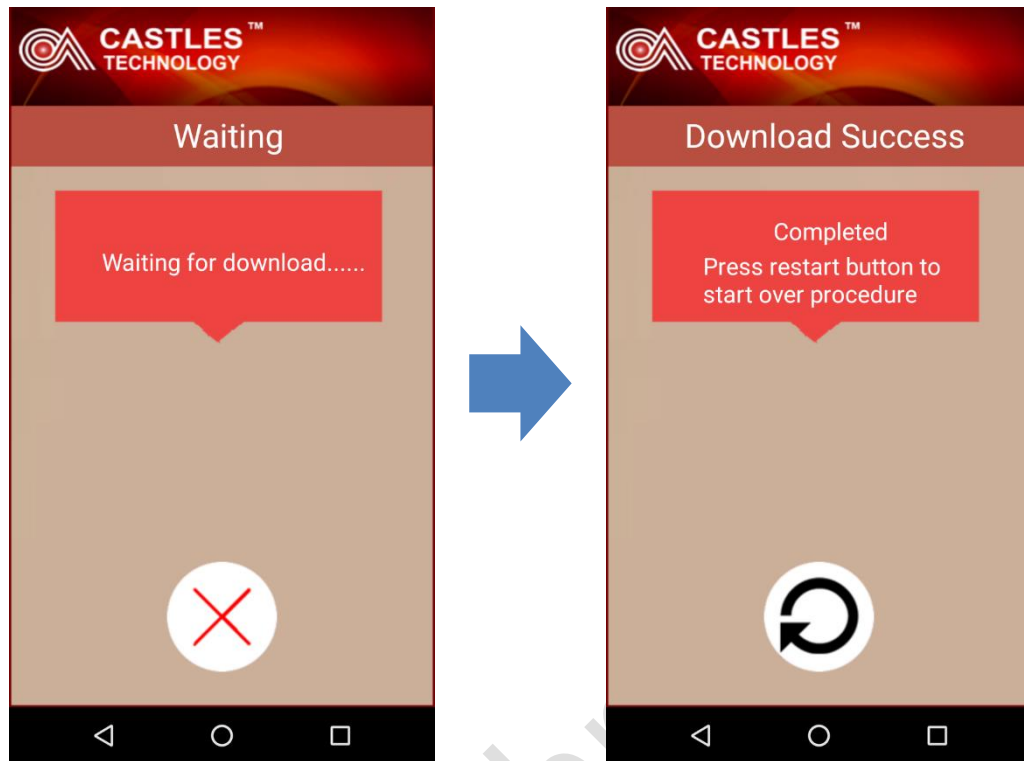
- Key Sound: Enable or disable the key sound function. (Currently only support to EMV pin code input.)
- Navigation Bar: Enable or disable this function will show or hide the navigation bar at the bottom.
- Battery charging threshold: Battery will start charging when the battery capacity is lower than setting threshold.
- Debug mode: Enable or disable the adb (Android Debug Bridge) function. (After enabling this function, please reboot the terminal at once.)
- Auto reboot: Enable or disable the auto reboot function.
- Auto reboot interval: select the auto reboot interval.
- Factory reset: Reset the terminal to factory default setting.
- Enable user password: Enable or disable the user password function for entering default AP.
- Change user password: Change the user password. (default 00000000)
- Change login password: Change System Panel login password. (default 00000000)
- Date & Time: Set date and time.
- Select default application: Select the default application which will autorun after system boot up.
- About: Show system versions.

3.3. Loader

Download user application, or update Android system and kernel modules firmware.



- Click on [App menu].
- Click on [loader].

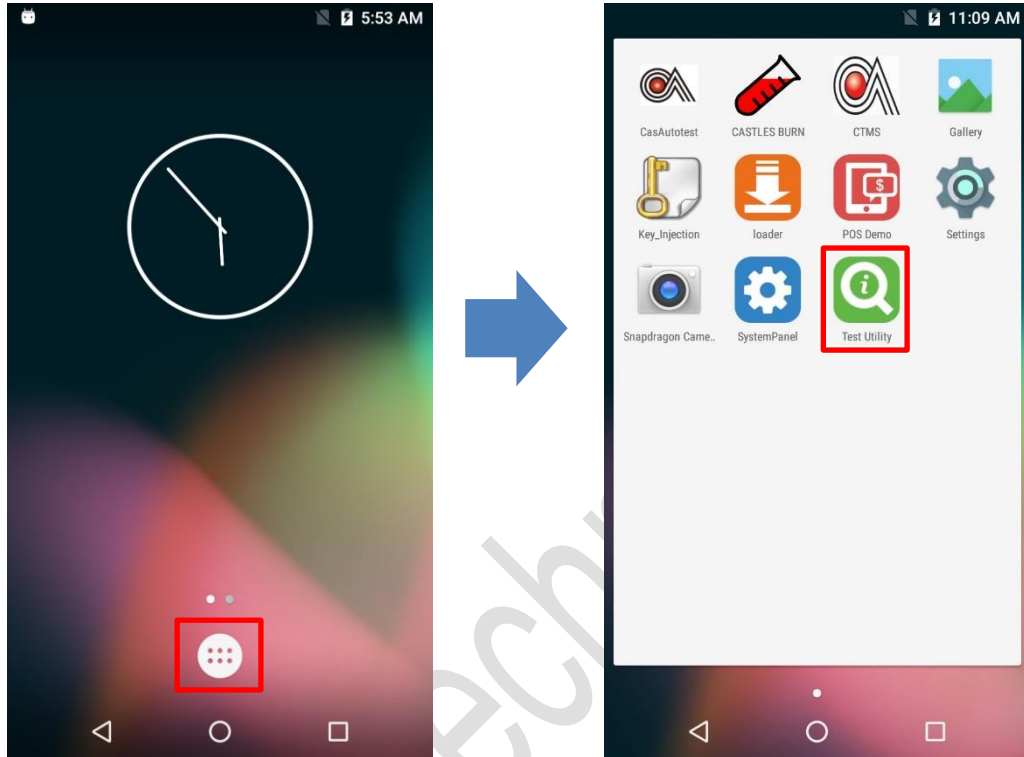


- The screen will show “Waiting for download”.
- If download successes, the screen will display completed information.

Notice: If cannot run this tool or download fail, please check the debug mode in “SystemPanel”, it should be set to disable.

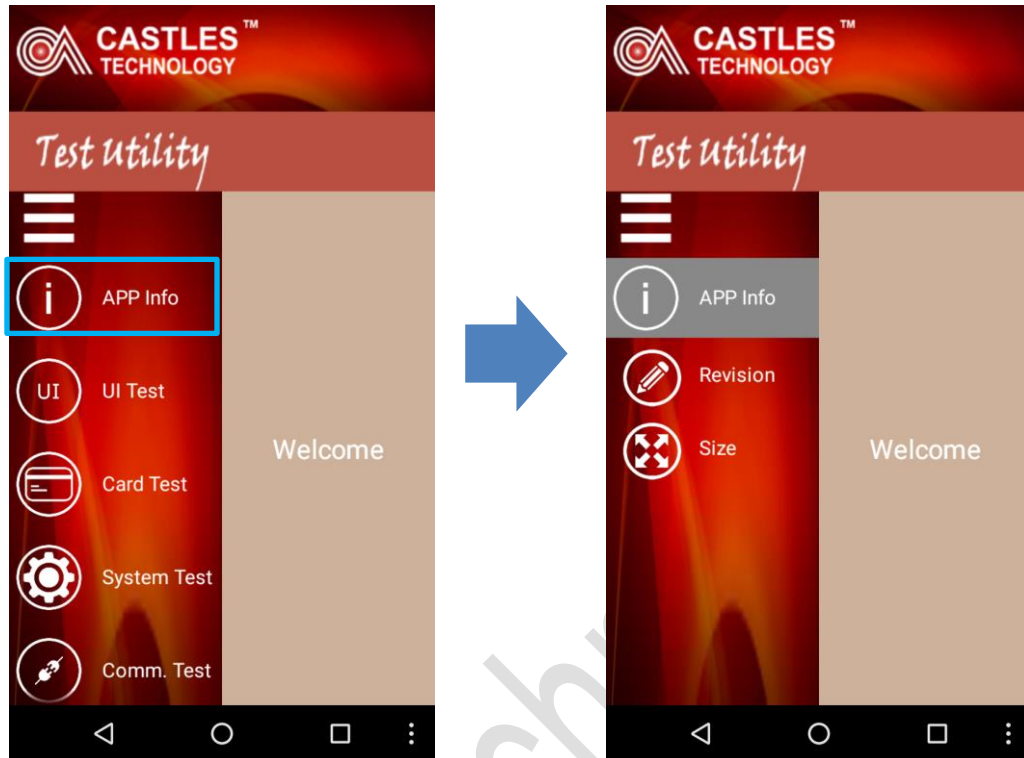
3.4. Test Utility

Diagnose terminal hardware components.



- Click on [App menu].
- Click on [Test Utility].

3.3.1 APP Info



- Click on [APP Info].
- Revision: Display the Android OS version.
- Size: Display the memory size info.

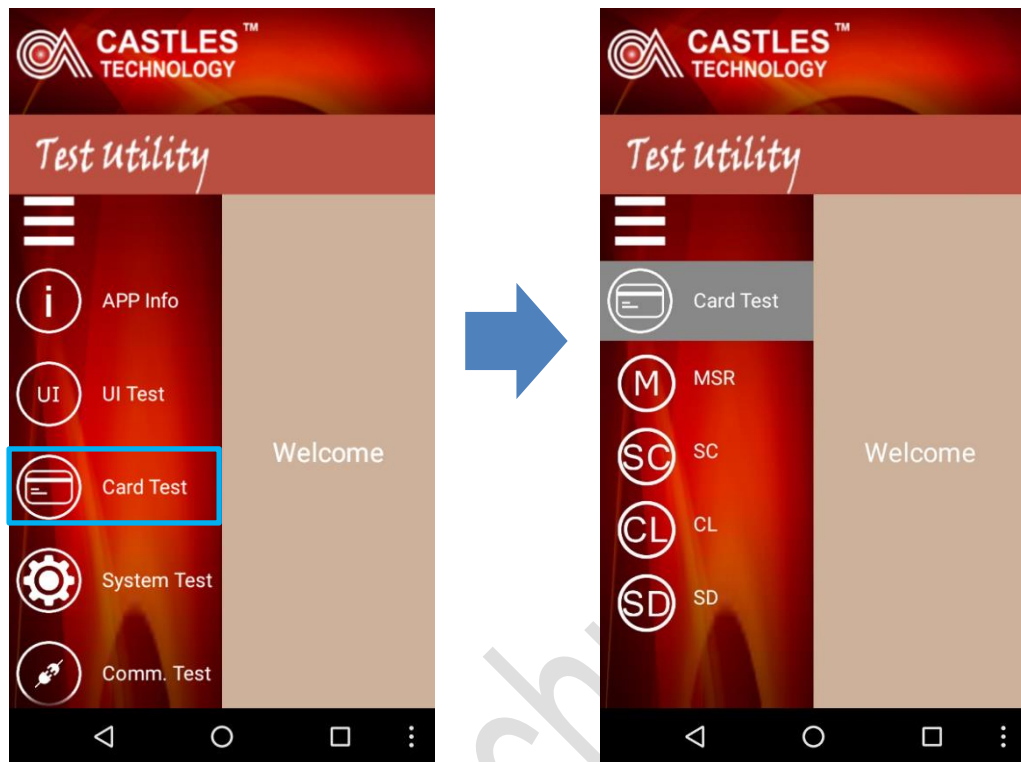
3.3.2 UI Test



- Click on [UI Test].
- LCD: Diagnose the LCD display function.

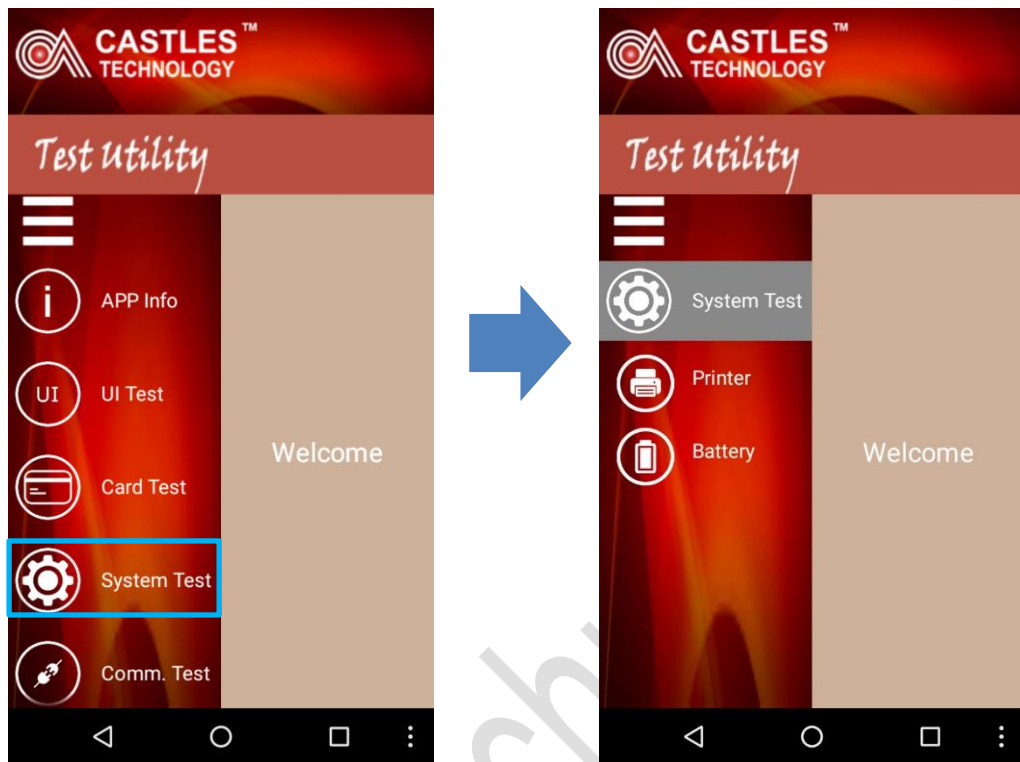
- LED: Diagnose the rear side LED function.
- Backlight: Diagnose the brightness of the backlight.
- RTC: Get system RTC info.
- Speaker: Diagnose the speaker function.
- Touch: Diagnose the touch function.
- Camera: Diagnose the rear camera function.
- Finger Print: Diagnose the fingerprint function.

3.3.3 Card Test



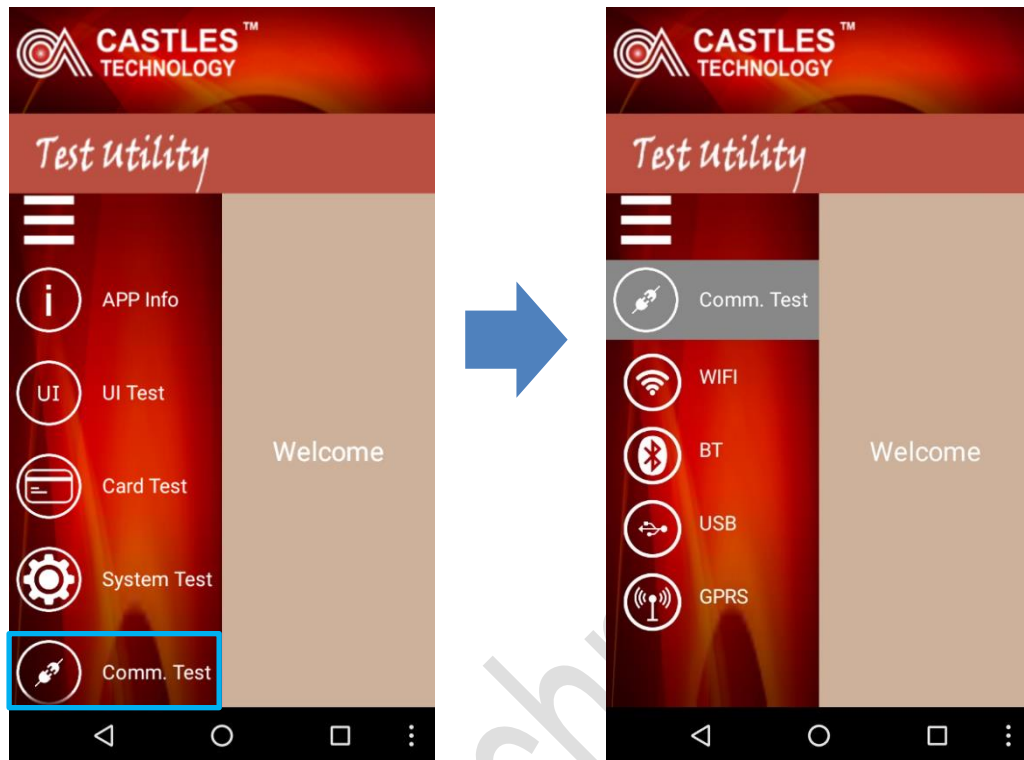
- Click on [Card Test].
- MSR: Diagnose the MSR function.
- SC: Diagnose the Smart Card function.
- CL: Diagnose the Contactless Card function.
- SD: Diagnose the SD card function.

3.3.4 System Test



- Click on [System Test].
- Printer: Diagnose the Printer function.
- Battery: Get the Battery operation info.

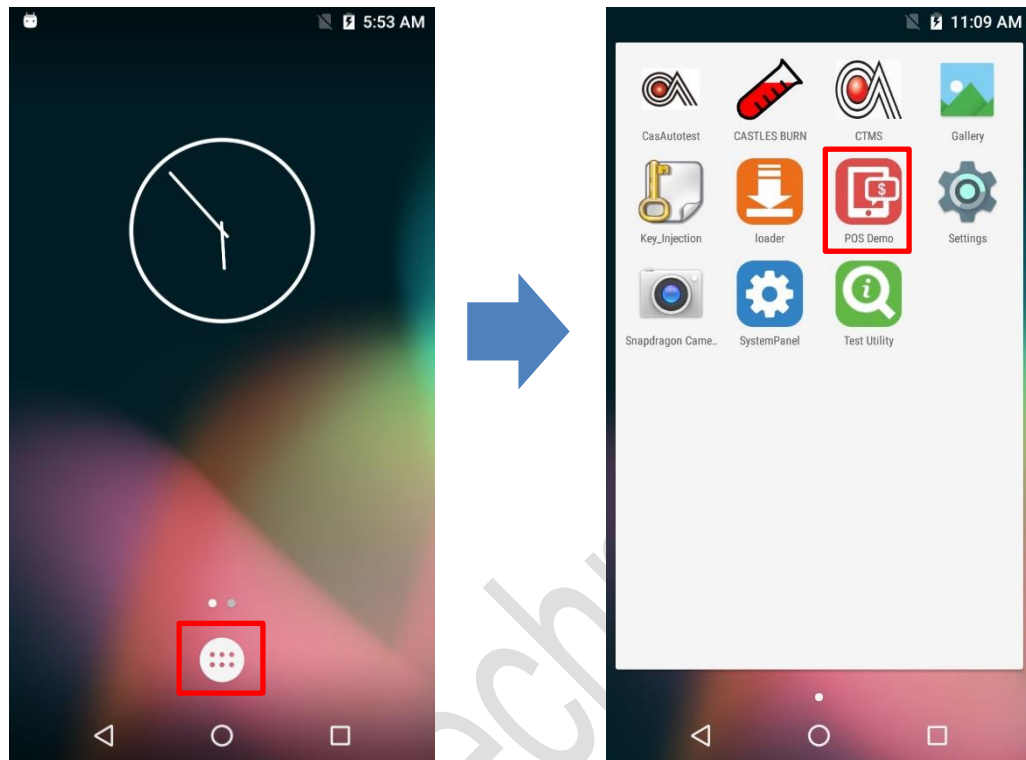
3.3.5 Communication Test



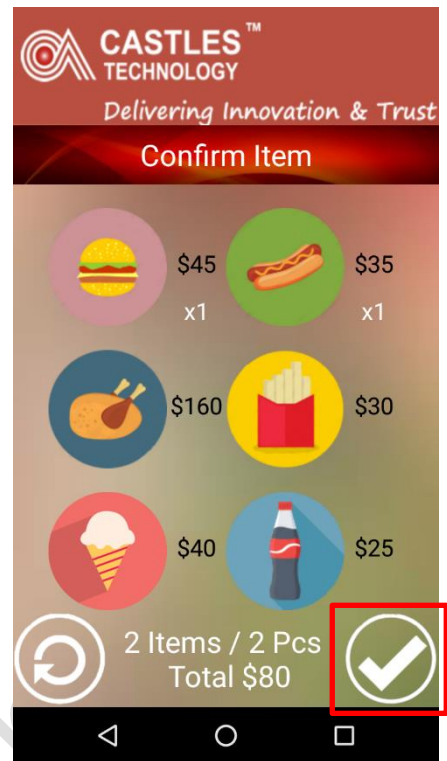
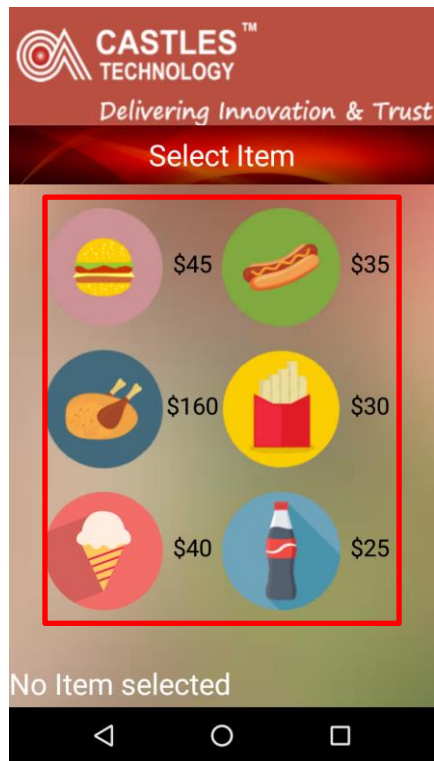
- Click on [Comm. Test].
- WIFI: Diagnose the WIFI function.
- BT: Diagnose the BT function.
- USB: Diagnose the USB function.
- GPRS: Diagnose the GPRS function.

3.5. POS Demo

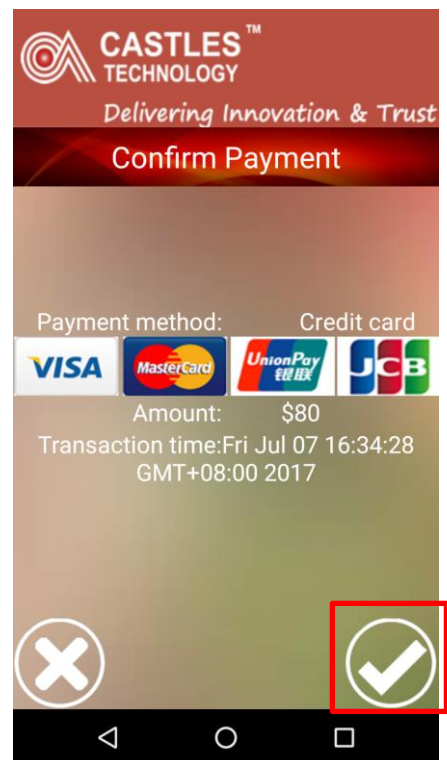
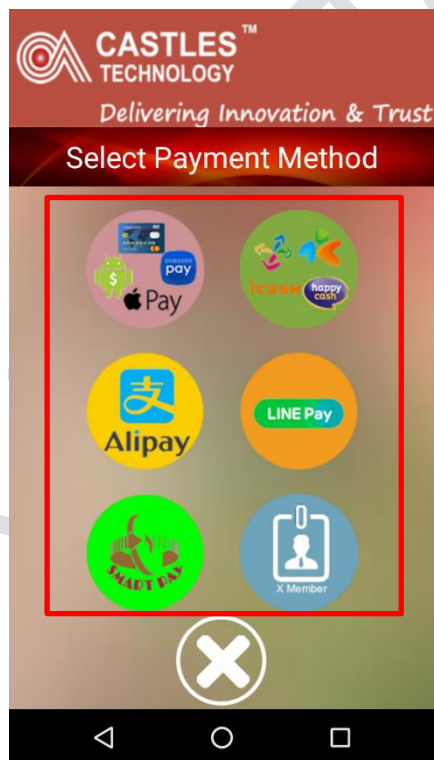
Test EMV/EMVCL function and demo use.



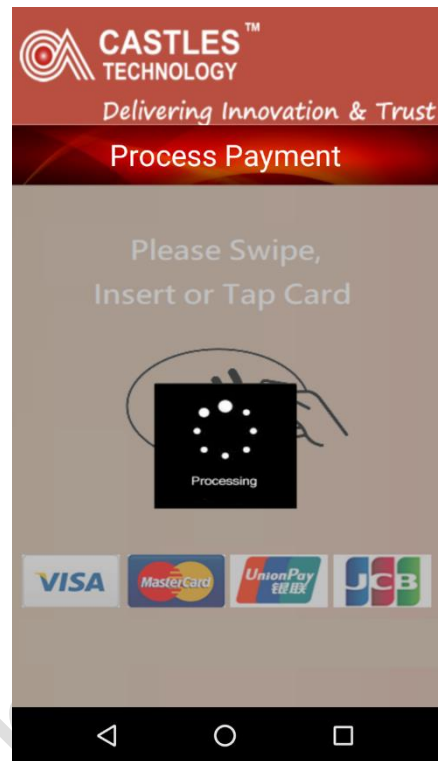
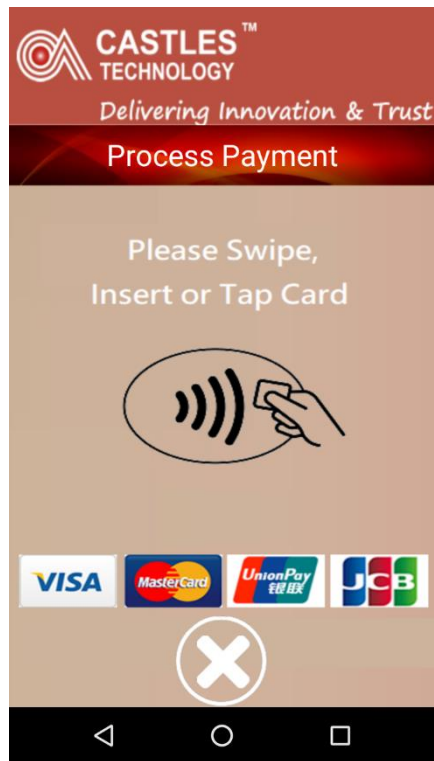
- Click on [App menu].
- Click on [POS Demo].



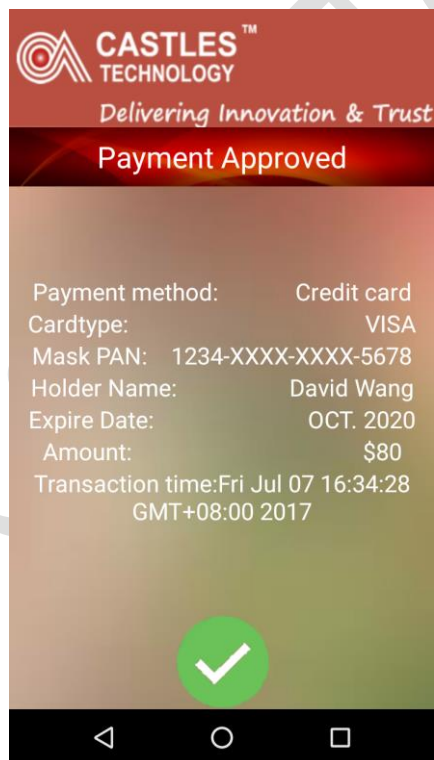
- Select items.
- Confirm items.



- Select payment method.
- Confirm Payment.

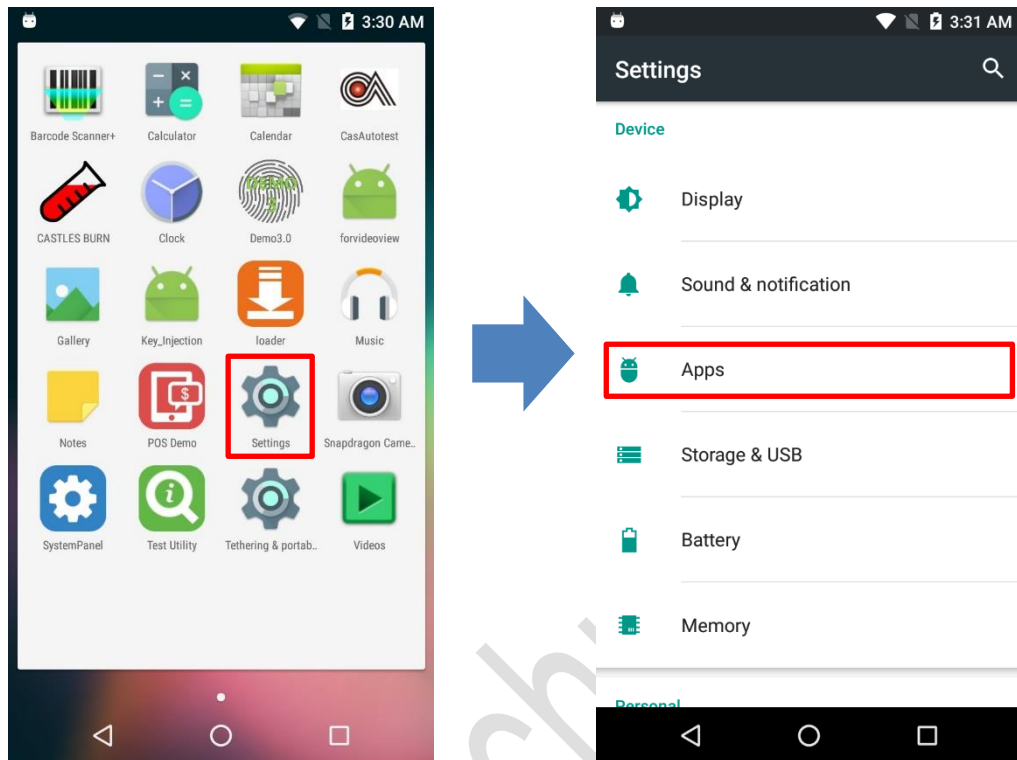


- Waiting Swipe, insert or tap card.
- Process payment.

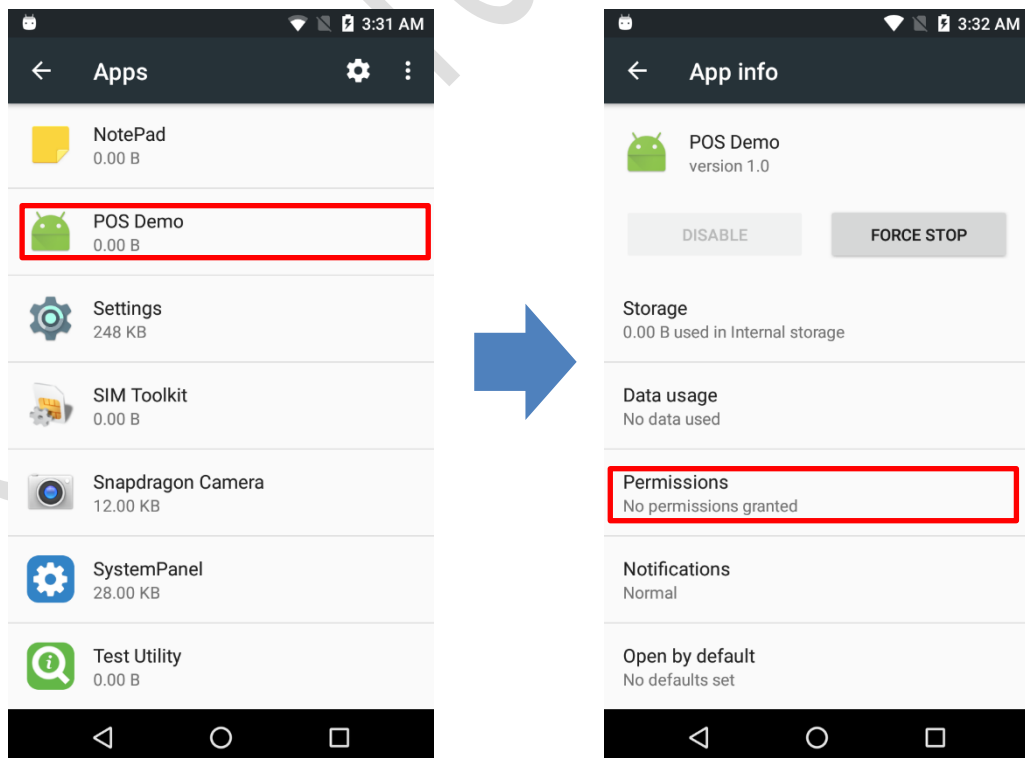


- Payment approved.
- Print receipt.

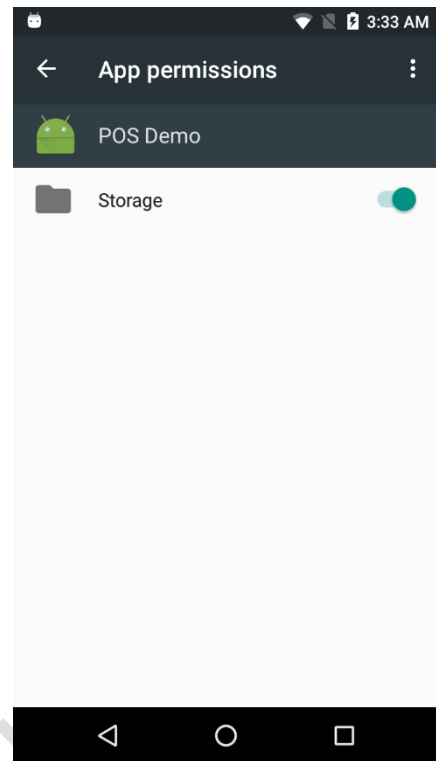
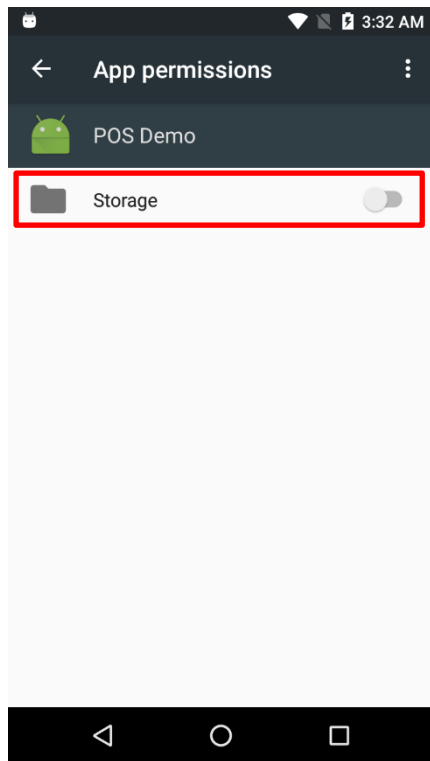
If print receipt fails, please check the permission of “storage”, it needs to be set to enable. The steps to check the permission is shown as below.



- Click on [Settings].
- Click on [Apps].



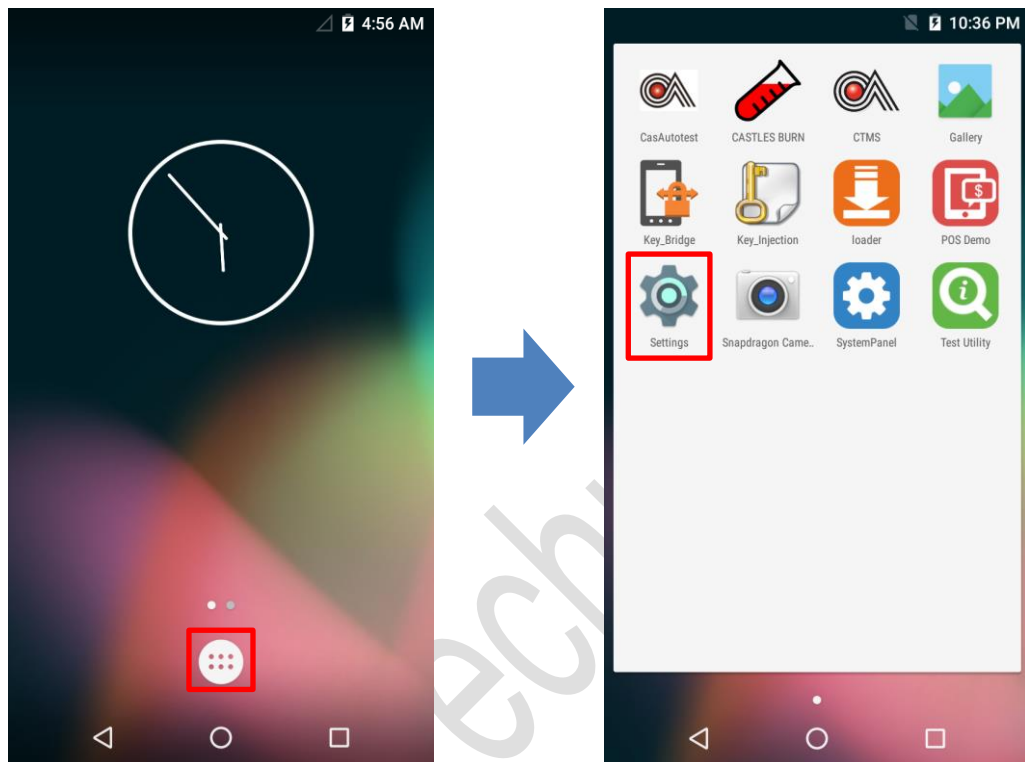
- Click on [POS Demo].
- Click on [Permissions].



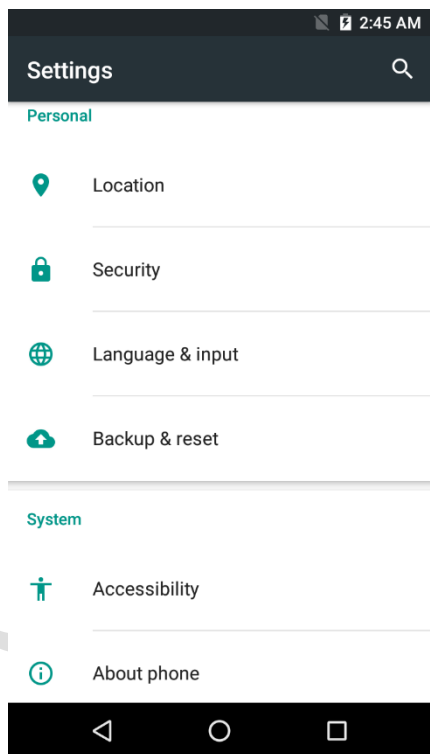
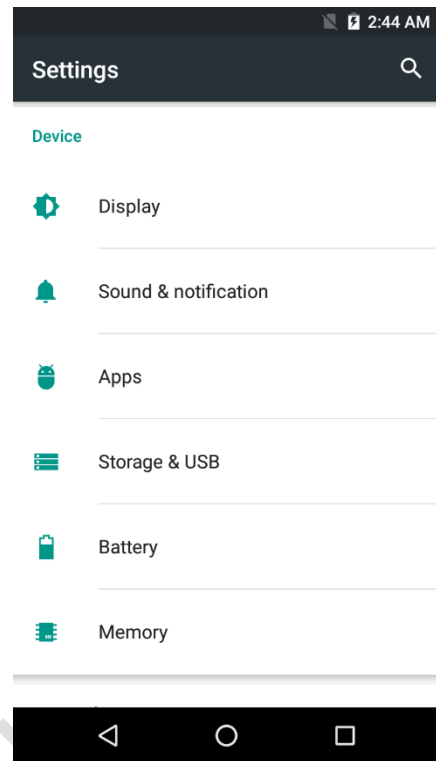
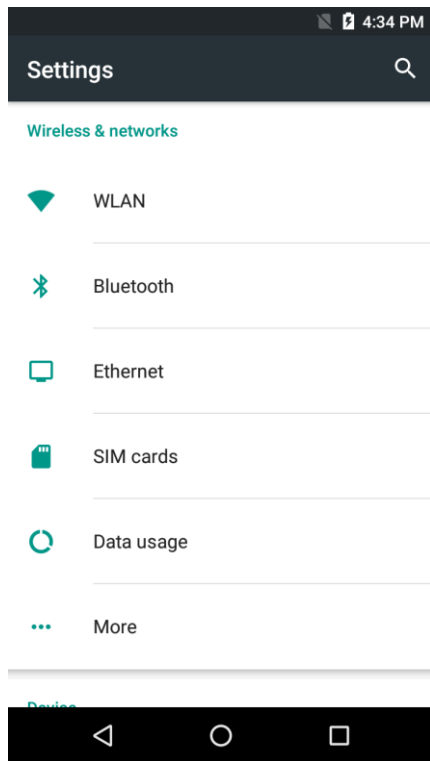
- Enable "Storage".

3.6. Setting

View/set the wireless & network, device configure, personal configure, system information on the terminal.



- Click on [App menu].
- Click on [Setting]



- WLAN: View available networks list and connection.
- Bluetooth: Search the Bluetooth device around and connection.
- Ethernet: Set USB OTG Ethernet configuration.
- SIM cards: Set the SIM card configure.

- Data usage: Check the data usage history of applications.
- More: The other settings for wireless & networks.
- Display: Set the display screen configuration.
- Sound & notification: Set the sound volume and notification ringtone.
- Apps: Management all of applications on the terminal.
- Internal storage: View the used size for the storage space.
- Battery: Check the battery voltage usage/charging status.
- Memory: Check the memory used status.
- Location: View the application requested location history.
- Security: Set the terminal security configuration.
- Language & input: Set the display languages and keyboard input methods.
- Backup & reset: Backup the terminal data.
- Accessibility: The accessibility feature configuration.
- About phone: View the phone information.

- Note: Saturn1000 device only support non Just work parsing devices, the Bluetooth device must support security PIN code to connect.
For Bluetooth Smart (LE) Secure Connections, it support three association models shown below.

1. Just Works :

As implied by the name, this method just works. No user interaction is required. This method is typically used by devices without display and keypad. This method provides no man in the middle (MITM) protection.

Headphones / Headsets was designed for the situation where at least one of the pairing devices has neither a display nor a keyboard for entering digits

2. Passkey Entry:

This method may be used between a device with a display and a device with numeric keypad entry (such as a keyboard), or two devices with numeric keypad entry. In the first case, the display is used to show a 6-digit numeric code to the user, who then enters the code on the keypad. In the second case, the user of each device enters the same 6-digit number. Both of these cases provide MITM protection.

3. Out of Band (OOB):

Out of band is a flexible option for developers that allows you to define some of your own pairing mechanisms, so the security level depends on out of band protection capability. This method provides no man in the middle (MITM) protection.

4. Secure File Loading

Castles implemented an interface in terminal named User Loader (ULD) to provide secure file loading to system memory. The Loader only applies to download the “CAP” file for the user application and the kernel firmware.

The loading process is secure by signing the files using ULD Key System.

4.1. File Signing

For convert the file to “CAP” file, Castles provides a tool named “CAPGen” to perform this task.

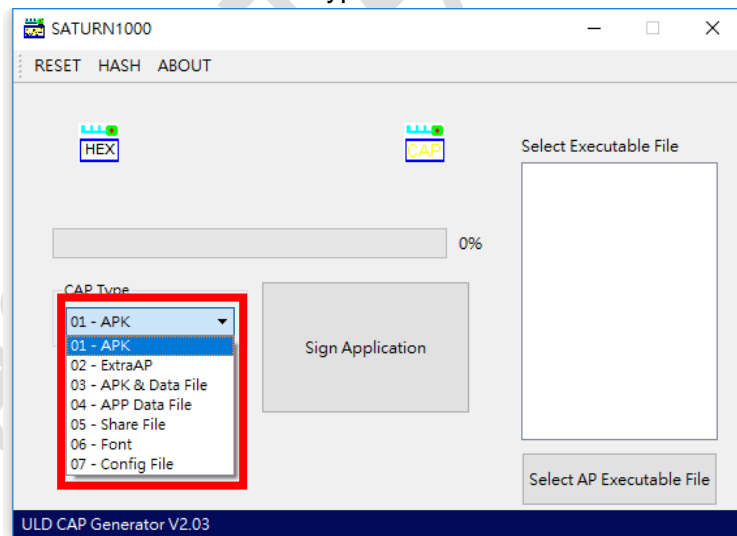
The CAPGen is located at:

C:\Program Files (x86)\Castles\SATURN1000\tools\CAPG (Evaluation Version)\

- Run CAPGen.exe

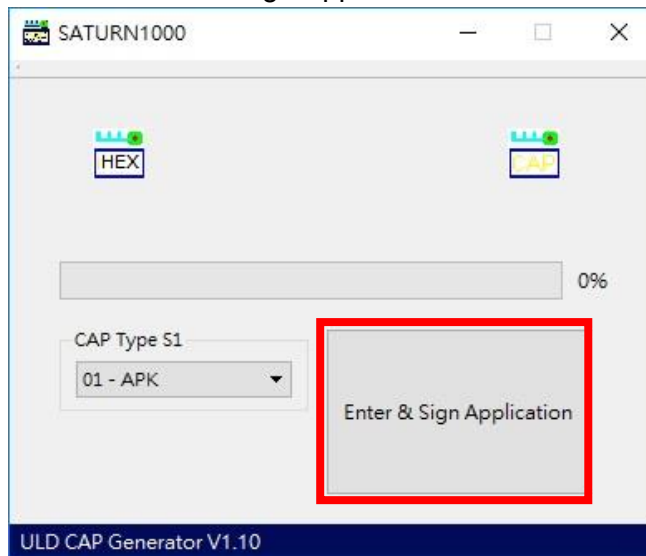


- Select the correct CAP Type from the list

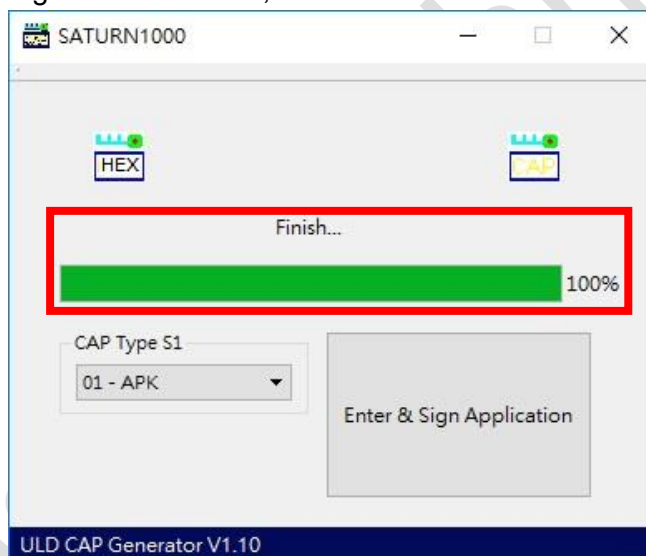


- 01- APK (For Android APK)
- 02- ExtraAP (For Secure Module files)
- 03- APK & Data Files (For Android APK and AP's data file)
- 04- APP Data Files (For dedicated Android AP's data file)
- 05- Share files (For file can be accessed by all APs)
- 06- Font (For Fonts Files)
- 07- Configuration file (For Castles Configuration Files)

- Click on “Enter & Sign Application” to browse files.



- If generate success, the tool will show “Finish...”.



- The output file will be in a set. A “mci” file with one or more “CAP” files. CAP file contents the signed file binaries, where MCI file contains the list of CAP files.



App.CAP



App.mci

Note: If the user would like to load multiple sets of the signed file, only need to create a new file with the extension of “mmci”. Then put the file path of the “mci” file to the “mmci” file just like the “mci” file contains the file path of the “CAP” files.



MultiApp.mmci

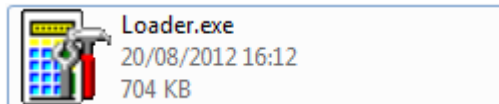
4.2. CAP file loading

The “ULD Download Utility” is a tool which provided by Castles Technology. It's the formal way to download the “CAP” file to the terminal.

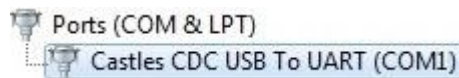
The Loader is located at:

C:\Program Files (x86)\Castles\SATURN1000\tools\Loader

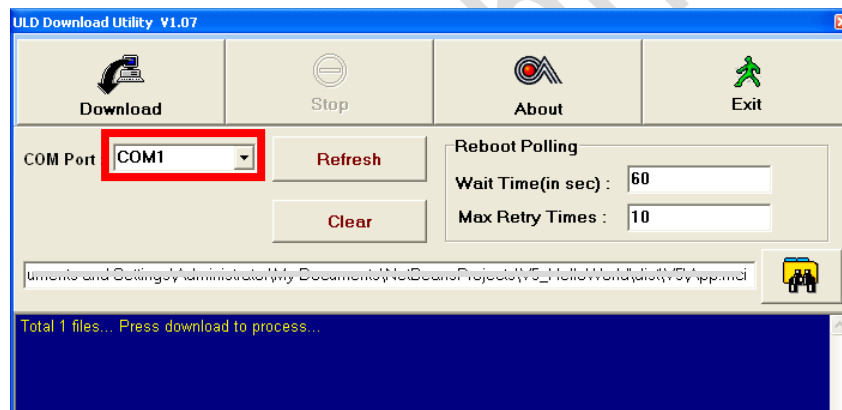
- Run Loader.exe



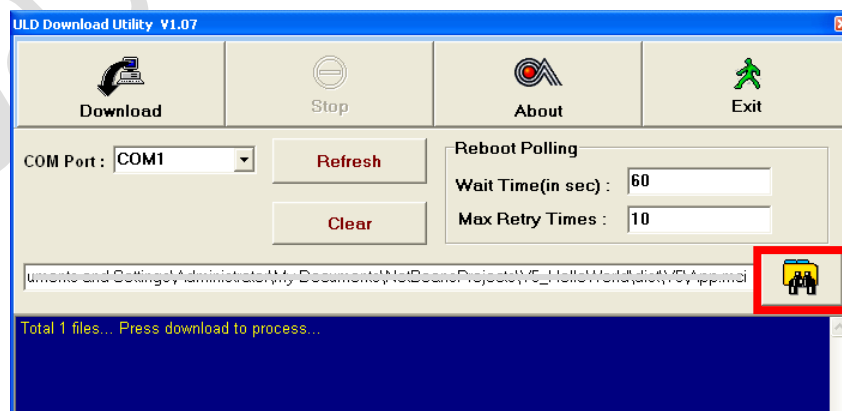
- Check the terminal com port in Device Manager.



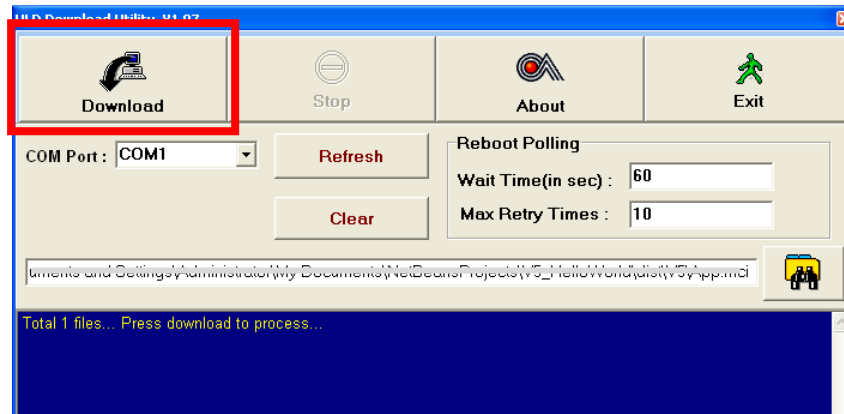
- Select COM port.



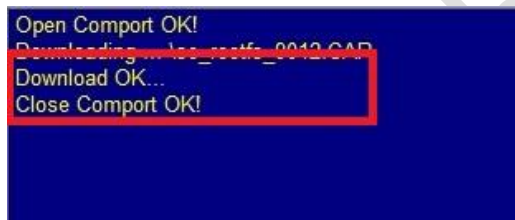
- Browse and select mci file or mmci file



- On terminal side, please refer to the chapter “**3.2 Loader**” to set the terminal in the status of waiting for download.
- Press “Download” button to start the download.



- After download finish, the log screen will show “Download OK...” as the following picture.





5. Key Injection

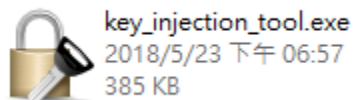
This chapter describes how to use key injection tool to load keys into the terminal. Key injection tool is used during the user testing phase.

5.1. Preparation

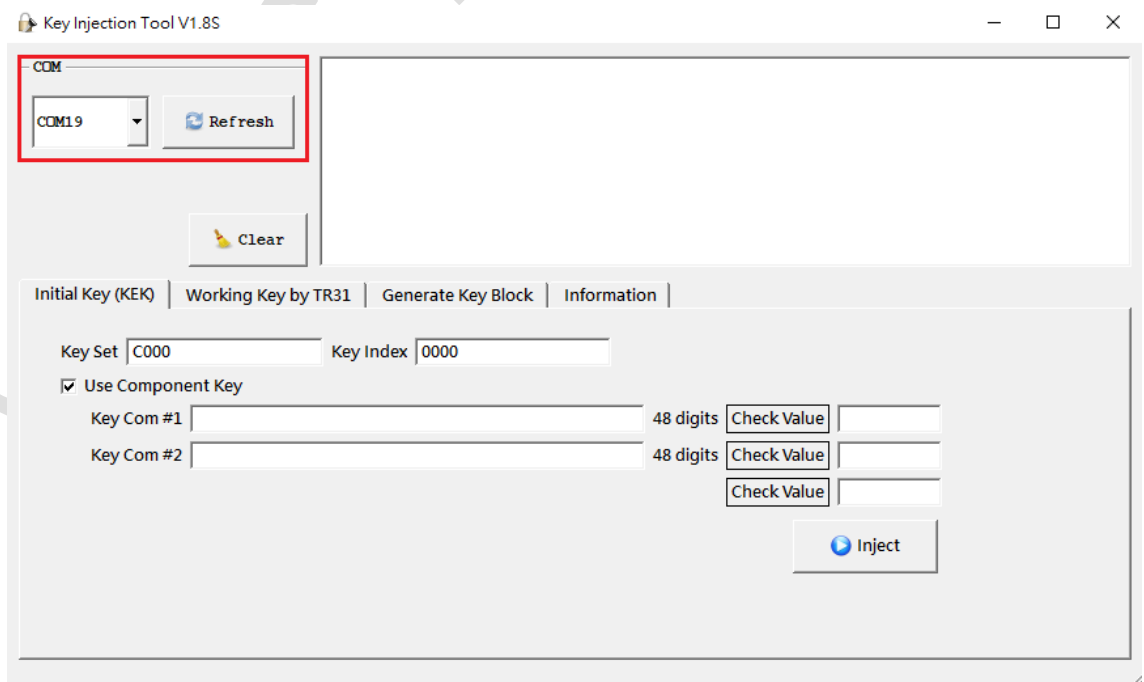
1. Disable terminal debug mode (set by SystemPanel).
2. Connect terminal to PC via USB and PC will have an additional COM port.
3. The terminal should be recognized as Castles CDC USB to UART (debug mode disable) instead of Qualcomm HS-USB Diagnostics 9091 (debug mode enable).

 Castles CDC USB To UART (COM19)
 Qualcomm HS-USB Diagnostics 9091 (COM21)

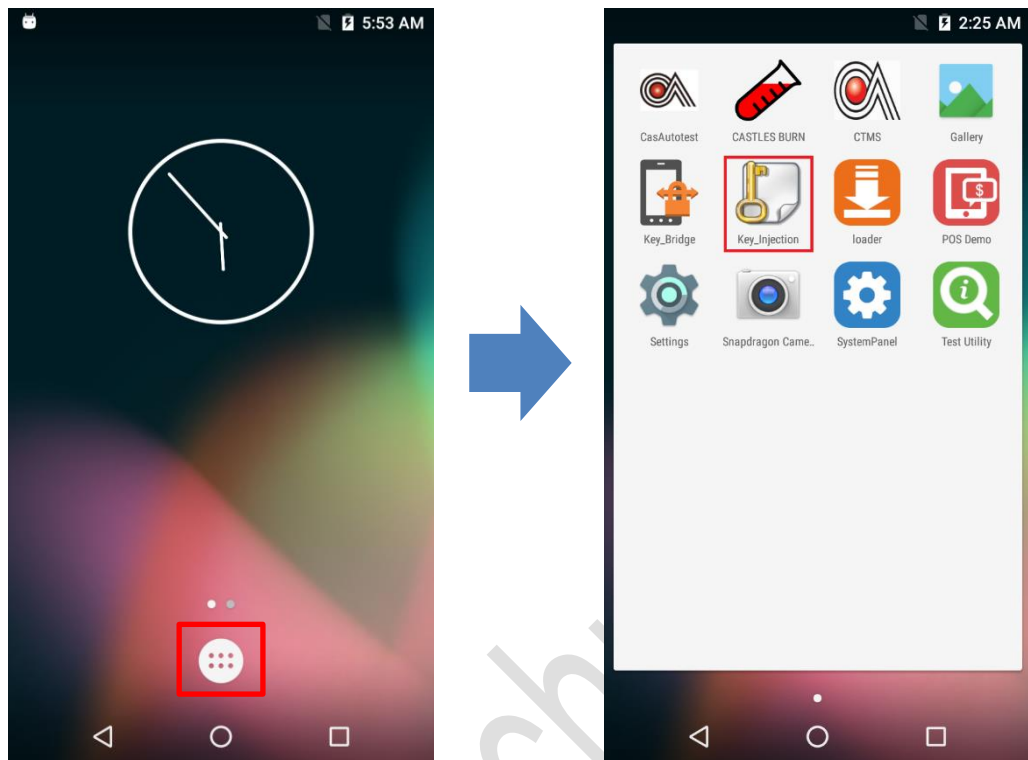
4. Run key_injection_tool.exe on PC.



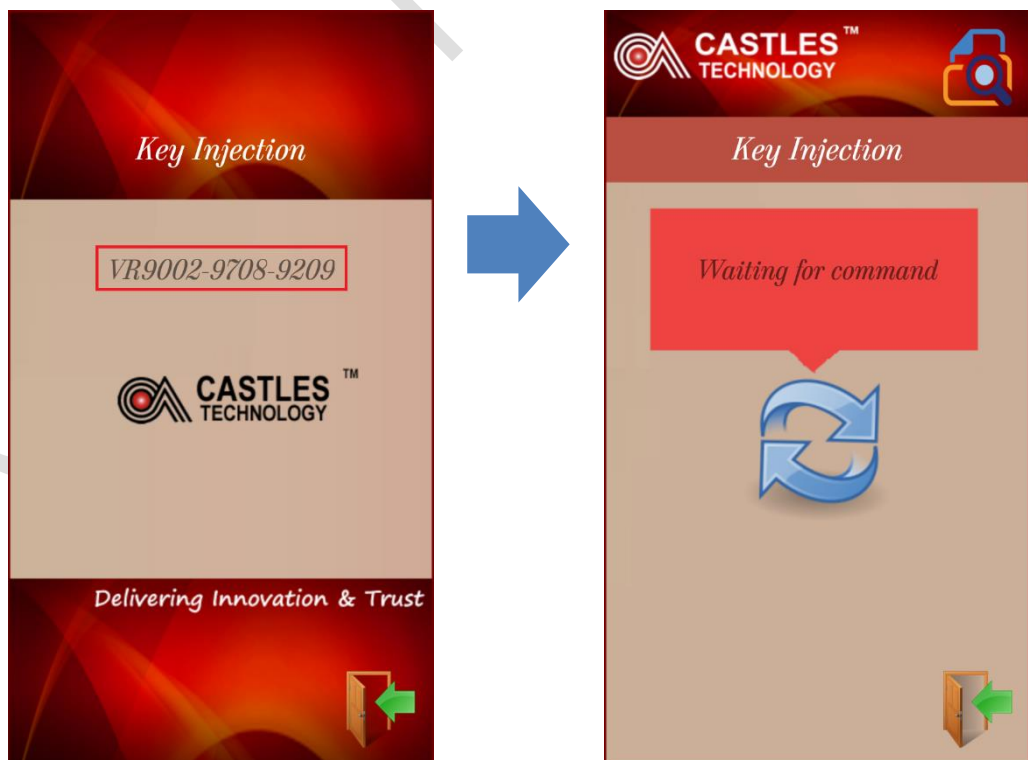
5. Choose the corresponding COM port.



5.2. Enter Key Injection AP



- Click on [App menu].
- Click on [Key_Injection]



- The welcome screen will show AP version.
- Terminal will show "Waiting for command" for the first time injection.

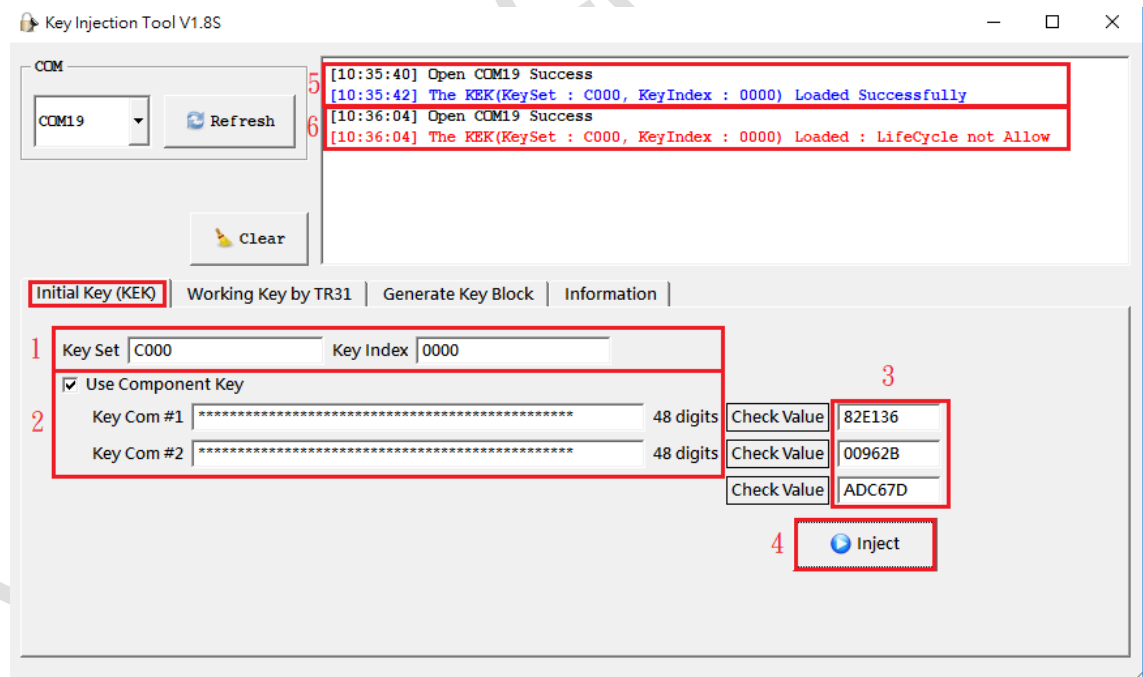
5.3. Inject Initial Key (KEK)

At the beginning, there is no key existing in the terminal. The first key for the terminal is a KEK, loaded in plain-text, used for encrypted working key loading based on TR31 block binding method.

On Initial Key (KEK) page.

1. Input Key Set (default C000) and Key Index (default 0000).
(Key Set ranging from C001 to CFFF, Key Index ranging from 0000 to FF00)
2. Input Key Value or Key Com#1 and Com#2 for the component key.
(Value should be 32 or 48 digits, ranging from 0 to F (Hex))
3. Confirm if the “Check Value” (3 bytes) is correct as you expect.
4. Press “Inject” button to inject key into terminal.
5. If successfully be loaded, the tool will show “Loaded Successfully”.
6. KEK can only be loaded once, then tool shows “Loaded LifeCycle not Allow”.

In case of KEK need to be reloaded, please perform “Factory Reset” in System Panel



5.4. Generate TR31 Key Block

This tool provides the function “Generate TR31 Key Block” to make user easy to generate TR31 key block during their testing phase.

On Generate Key Block page.

1. Input Key Value or Key Com#1 and Com#2 (same in Initial Key page)
2. Select Working Key Type and Working Key Attribute.
3. Input Working Key Value.
(For key type 3DES, value should be 32 or 48 digits, ranging from 0 to F(Hex)
For key type 3DES-DUKPT, value should be 32 digits, ranging from 0 to F(Hex))
4. Input KSN if using 3DES-DUKPT
(Value should be 20 digits, ranging from 0 to F (Hex))
5. Press “Generate” button.
6. The TR31 key block will be shown on the screen as below.

Key Injection Tool V1.85

COM: COM19 Refresh Clear

Initial Key (KEK) | Working Key by TR31 | **Generate Key Block** | Information

1 TR31 Key Block

2 KEK Com #1 48 digits Check Value 82E136

3 KEK Com #2 48 digits Check Value 00962B

4 Working Key 48 digits Check Value ADC67D

5 KSN 00 digits Check Value 0F2FCF

Working Key Type 3DES

Working Key Attr. PIN Encrypt

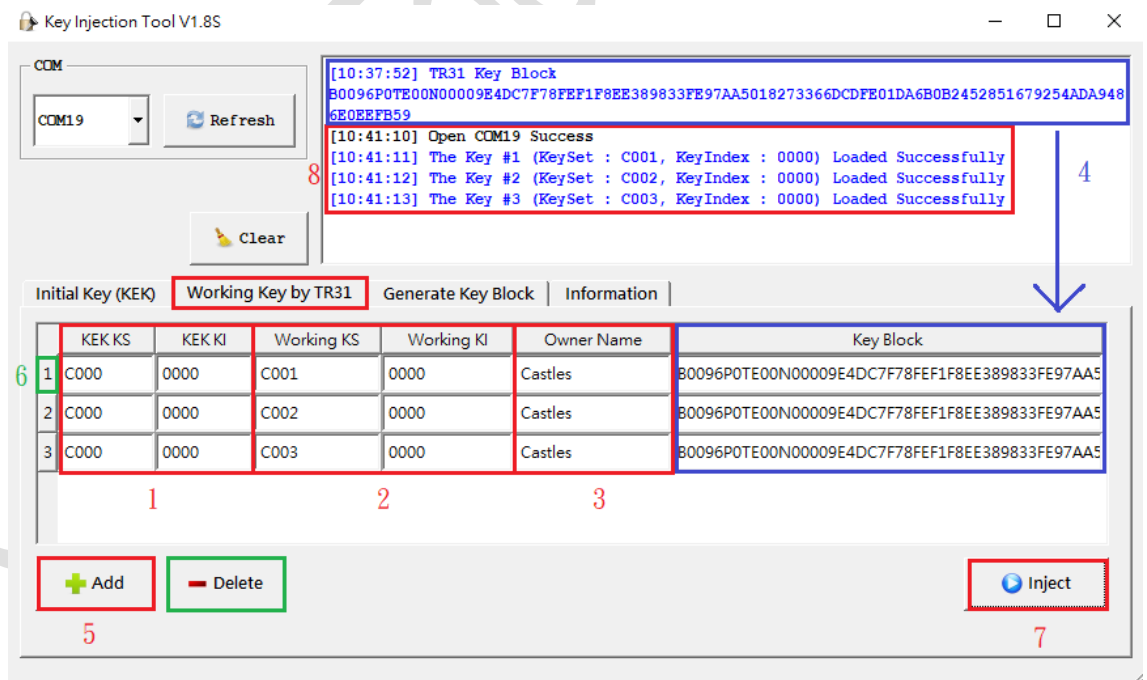
6 [10:37:52] TR31 Key Block
B0096P0TE00N00009E4DC7F78FEF1F8EE389833FE97AA5018273366DCDFE01DA6B0B2452851679254ADA948
6E0EEFB59

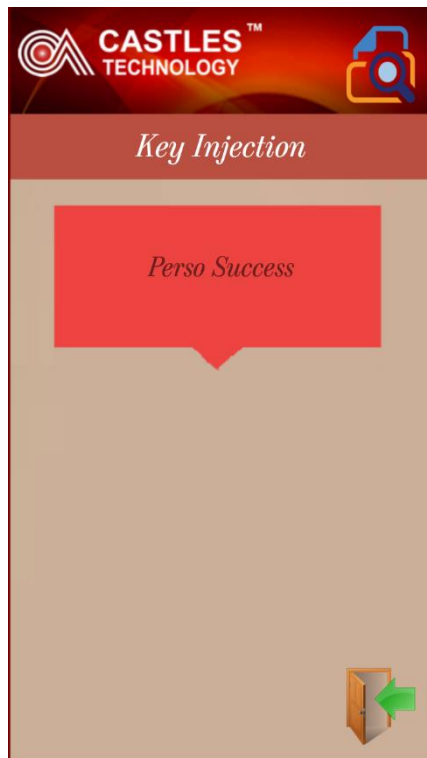
5.5. Inject Working Key

After KEK loading, the user can inject their working keys (WK), such as PIN key, data encryption key in ciphered text and TR31 key block format.

On Working Key by TR31 page.

1. Input KEK Key Set (default C000) and KEK Key Index (default 0000).
2. Input Working Key Set and Working Key Index.
(Key Set ranging from 0001 to BFFF, Key Index ranging from 0000 to FF00)
3. Input Owner name.
(The application name corresponding to the name input to CAP Generator)
4. Input Key Block
(If this is generated by tools, you can copy like the example below.)
5. For adding new input key, press "Add" button.
6. For deleting input key, select item number, and press "Delete" button.
7. Press "Inject" button to inject all the encrypted key(s) into the terminal.
8. If successfully be loaded, the tool will show "Loaded Successfully".
9. Key can only be loaded once, then tool shows "Loaded LifeCycle not Allow".





- After working key loading finished, the terminal is no longer allowed to perform key injection and it will show "Perso Success".
- In case working key need to be reloaded, please perform "Factory Reset" in System Panel.

5.6. Information

This page allows the user to access terminal information and key information.

On information page.

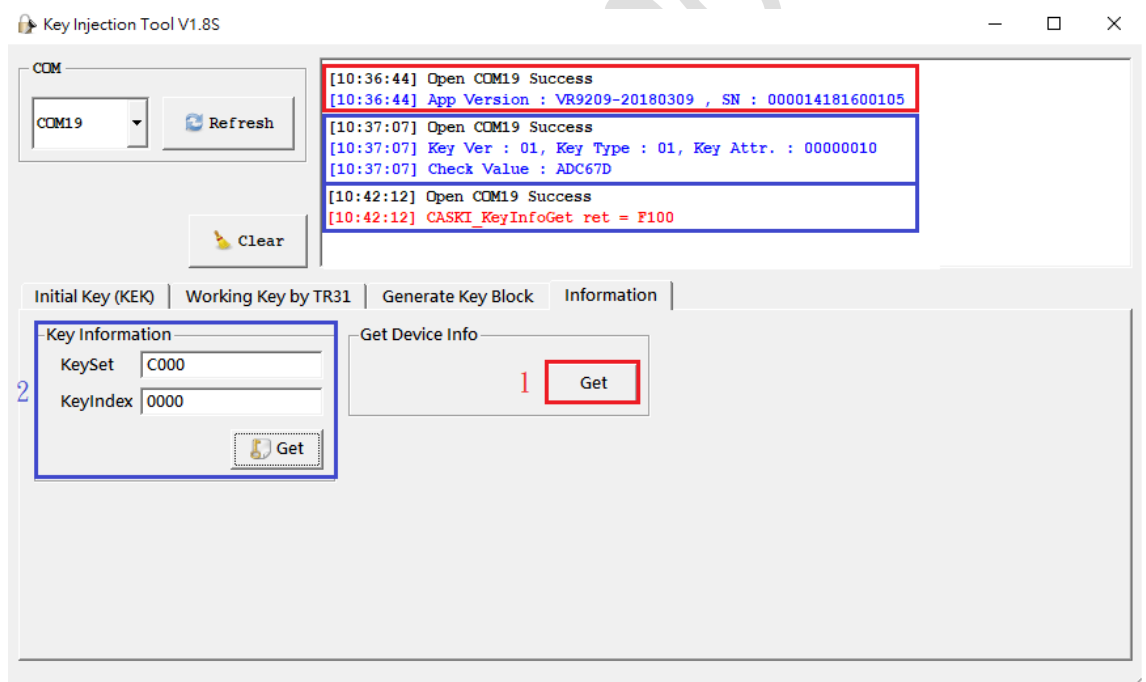
For Get Device Info

1. Press “Get” button to get app version and terminal serial number.

For Key Information

2. Input Key Set and Key Index. Then press “Get” button to get key version, key type, key attribute and key check value.

Key information can be only accessed before working key injection finished.
(Before terminal shows Perso Success on screen). It will shows ret = F100
after working key injection finished.



5.7. Injected Key for Transaction AP

For Castles SATURN1000 terminal, every transaction AP must use injected key for encryption and decryption data after API initialize.

This can be done by calling following APIs.

```
mentry.setEncryptInfo(meSecureInfo);    //manual entry
msr.setTracksEncryptInfo(msrSecureInfo);
emv.secureDataEncryptInfoSet(secureInfo);
emvcl.secureDataEncryptInfoSet(emvclSecureInfo);
```

SecureInfo parameters need to be set related to injected keys. Below are default parameters for all Castles sample AP, please modify based on your setting.

```
secureInfo.keyType = (byte)2;           //dukpt key
secureInfo.cipherKeySet = 0xC002;
secureInfo.cipherKeyIndex = 0x0000;
```

Take EMV as example:

```
Log.d(TAG, "EMV SecureDataEncryptInfoSet
*****");
EMVSecureDataInfo secureInfo = new EMVSecureDataInfo();
secureInfo.version = 2;
secureInfo.keyType = (byte)2;           //dukpt key
secureInfo.cipherKeySet = 0xC002;
secureInfo.cipherKeyIndex = 0x0000;
secureInfo.cipherMethod = 0x01;        //00:ecb 01:cbc
secureInfo.checksumType = 0;
secureInfo.ICVLen = 8;                 //required if cbc
secureInfo.ICV = new byte[8];
intRtn = emv.secureDataEncryptInfoSet(secureInfo);
if(intRtn != 0){
    str = "EMV secureDataEncryptInfoSet Fail, Rtn: " + String.format("0x%08X",
intRtn);
    Log.d(TAG, str);
    //str += "\n";
    ui_ShowLog(str);
}
else{
    Log.d(TAG, " EMV secureDataEncryptInfoSet OK");
}
```

~ END ~