secure boot

**Before using,please kindly read follow ,thank you:**

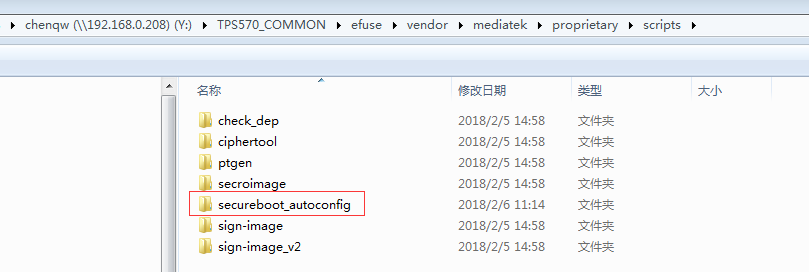
**\* Once the signature burning tool is enabled to burn firmware, only the same signature can be used to burn the firmware ! ! !**

**\* This file and burning tool are important, please keep it properly ! ! !**

**1、**Copy the “secureboot\_autoconfig” under the source directory to

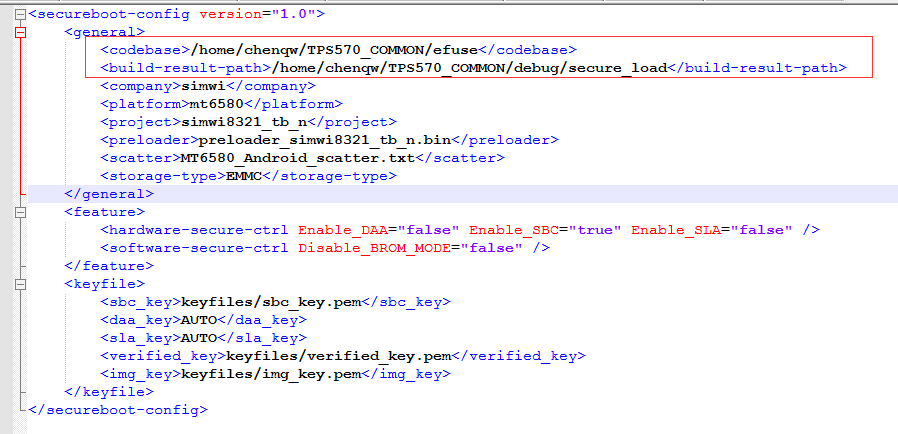
the “vendor/mediatek/proprietary/scripts/” directory.

Following is the source directory used by me.



**2、**Firstly, modify the “configuration.xml” under the “secureboot\_autoconfig” directory according to the source path.

The red part as below is the part that needs to be changed according to its own source code:



Explanation:

<sbc\_key> <verified\_key> <img\_key> specifies the corresponding key value path as

“Configuration.xml” file in the “keyfiles” directory in the same directory。

**3、Key file generation**

Note: I create a new “keyfiles” directory in the “code base” directory to save the key file.

chenqw@ubuntu208:~/TPS570\_COMMON/efuse$ mkdir keyfiles

chenqw@ubuntu208:~/TPS570\_COMMON/efuse$ openssl genrsa -out keyfiles/sbc\_key.pem 2048

chenqw@ubuntu208:~/TPS570\_COMMON/efuse$ openssl genrsa -out keyfiles/verified\_key.pem 2048

chenqw@ubuntu208:~/TPS570\_COMMON/efuse$ openssl genrsa -out keyfiles/img\_key.pem 1024

This generated three possible files:

“img\_key.pem”、 “sbc\_key.pem”、 “verified\_key.pem”.

Replace this three files in “vendor/mediatek/proprietary/scripts/secureboot\_autoconfig/keyfiles/”

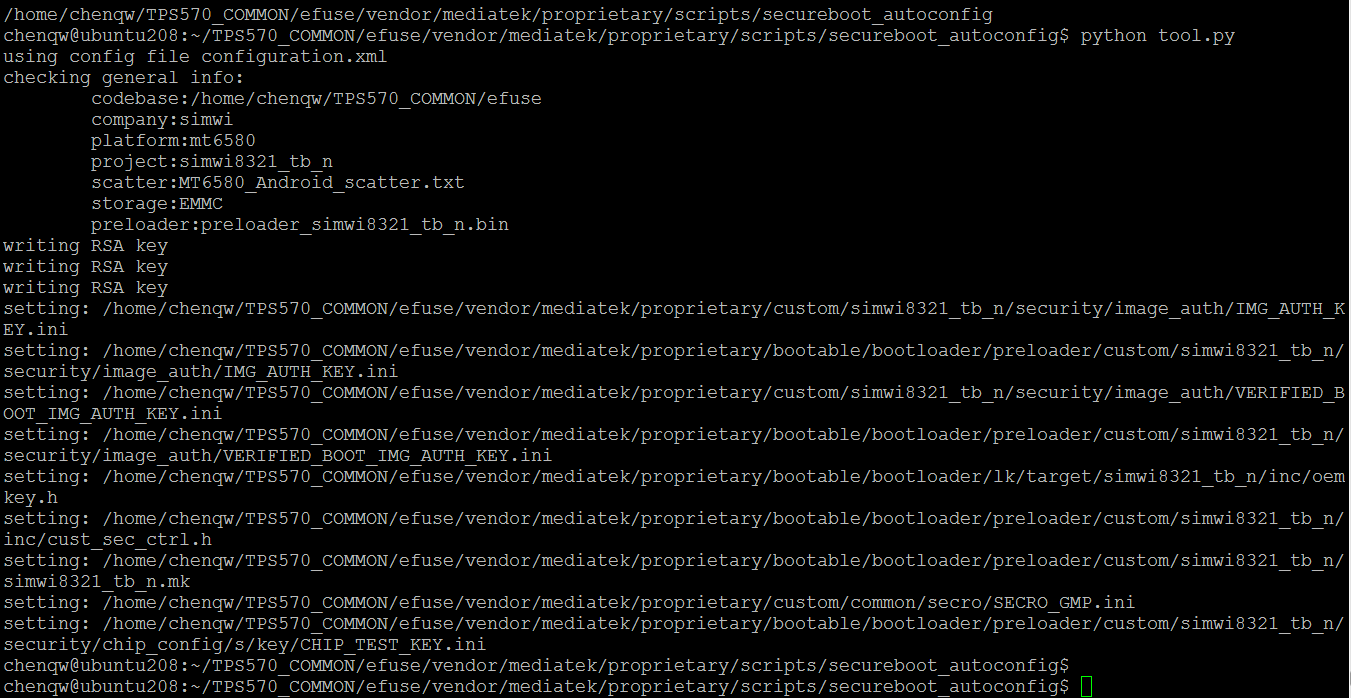
If you use the default key value, skip the whole third step.

**4、Generate a signature file**

Enter the “vendor/mediatek/proprietary/scripts/secureboot\_autoconfig/” directory and execute: “python tool.py” command, ex:

chenqw@ubuntu208:~/TPS570\_COMMON/efuse/vendor/mediatek/proprietary/scripts/secureboot\_autoconfig$ python tool.py

Following is the signature file generated screenshot:



Generated signature file:

vendor/mediatek/proprietary/custom/simwi8321\_tb\_n/security/image\_auth/IMG\_AUTH\_KEY.ini

vendor/mediatek/proprietary/custom/simwi8321\_tb\_n/security/image\_auth/VERIFIED\_BOOT\_IMG\_AUTH\_KEY.ini

vendor/mediatek/proprietary/bootable/bootloader/preloader/custom/simwi8321\_tb\_n/security/chip\_config/s/key/CHIP\_TEST\_KEY.ini

**Special attention:**

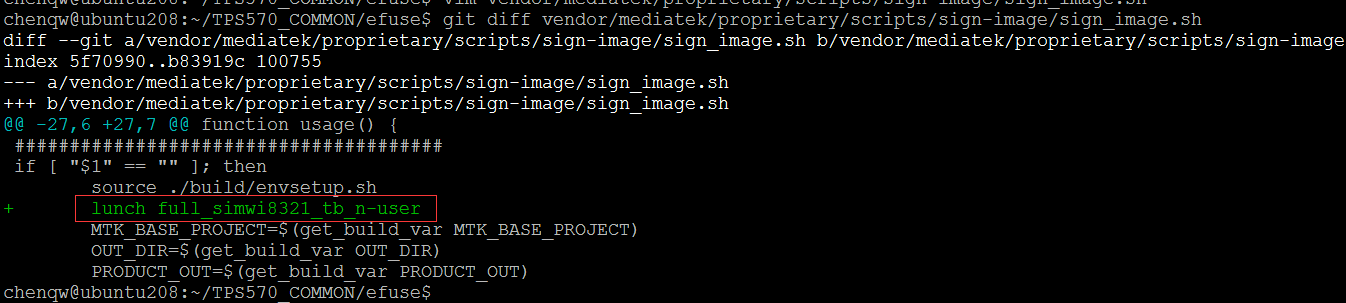
Please keep the “key” file produced in the third step and the “signature file” generated in the fourth step properly. This is a correspondence. Once an error occurs, it will lead to serious consequences such as unsigned or incorrect signature.

**5、Modify the “sign\_image.sh” script**

“Vendor/mediatek/proprietary/scripts/sign-image/sign\_image.sh”

Add “Lunch full\_simwi8321\_tb\_n-user”after “source ./build/envsetup.sh”.

As below:



**6、 Compile the firmware**

chenqw@ubuntu208:~/TPS570\_COMMON/efuse$ source build/envsetup.sh

chenqw@ubuntu208:~/TPS570\_COMMON/efuse$ lunch full\_simwi8321\_tb\_n-user

chenqw@ubuntu208:~/TPS570\_COMMON/efuse$ make -j12 2>&1 | tee android.log

chenqw@ubuntu208:~/TPS570\_COMMON/efuse$ sh vendor/mediatek/proprietary/scripts/sign-image/sign\_image.sh

If you need to compile firmware with OTA function, compile OTA before “sh sign\_image.sh”.

chenqw@ubuntu208:~/TPS570\_COMMON/efuse$ make otapackage

1. **Sign the tool**

①Unzip the“Customization\_Kit\_buildspec.zip” package in the tool.

 ②Copy “dummy\_K2 bin” file in vendor/mediatek/proprietary/scripts/secureboot\_autoconfig/tempfile/dummy\_

k2.bin to“Customization\_Kit\_buildspec\custom\security\usbdl4enduser

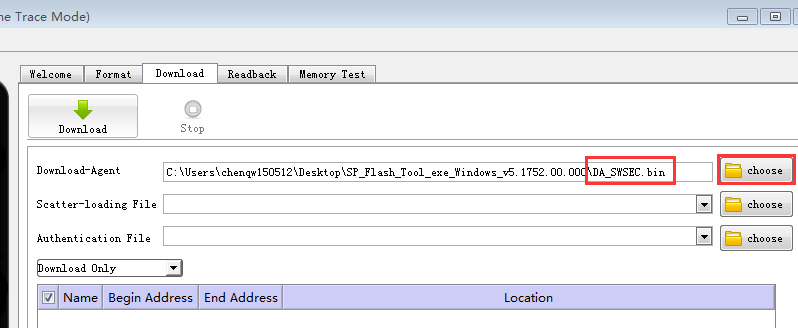
\_dummy\”

③Execute “sig.bat” and “package.bat” in “Customization\_Kit\_buildspec” in order, and then will generate a “CustomDAbin” folder in the “Customization\_Kit\_buildspec” directory.

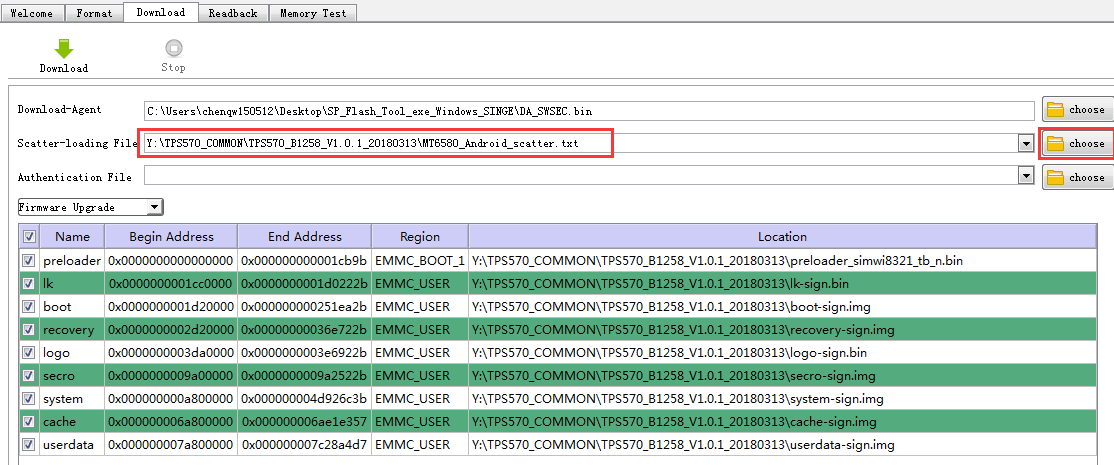
④ Unzip the “SP\_Flash\_Tool\_exe\_Windows\_v5.1752.00.000.zip” file in the “tools” and replace the “DA\_PL.bin DA\_SWSEC.bin MTK\_AllInOne\_DA.bin” in CursorDAbiin(mentioned in last step ).

**8、Download**

Open the “SP\_Flash\_Tool\_exe\_Windows\_v5.1752.00.000” tool and select the “DA\_SWSEC.bin” file as shown in the picture:



Select the firmware which need to be download.



Completed up to here..........