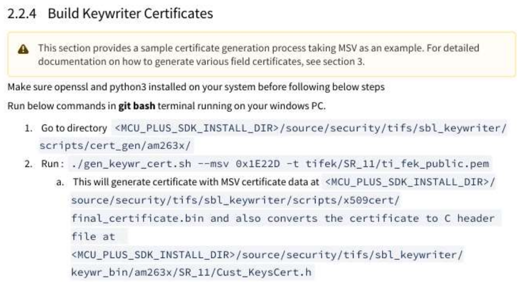
Security - eng ver

Friday, January 24, 2025 3:49 PM



2.2.4 Build Keywriter Certificates

> ⚠ This section provides a sample certificate generation process taking MSV as an example. For detailed documentation on how to generate various field certificates, see section 3.

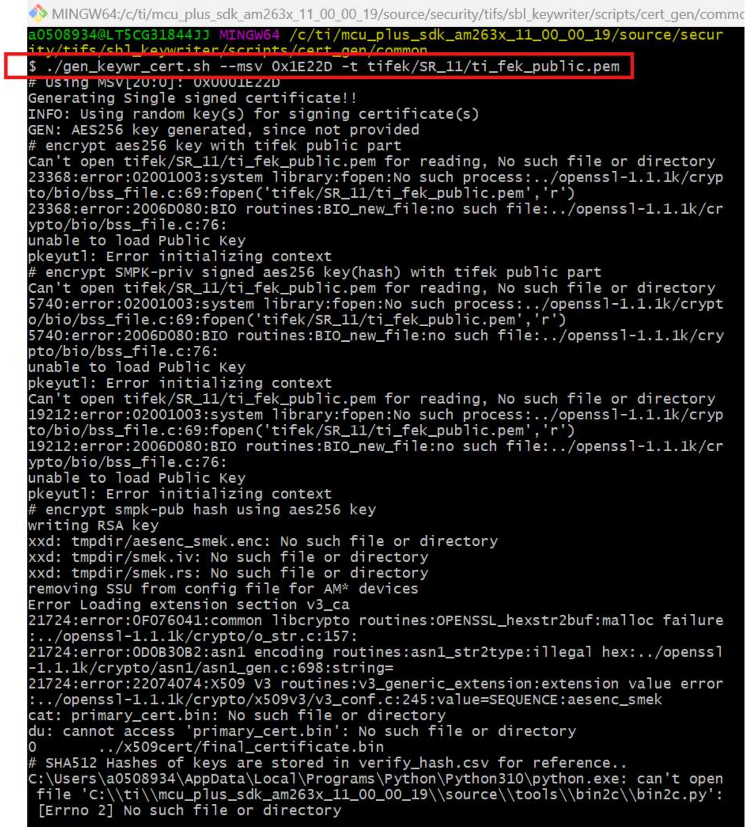
Make sure openssl and python3 installed on your system before following below steps

Run below commands in **git bash** terminal running on your windows PC.

1. Go to directory `<MCU_PLUS_SDK_INSTALL_DIR>/source/security/tifs/sbl_keywriter/scripts/cert_gen/am263x/`
2. Run : `./gen_keywr_cert.sh --msv 0x1E22D -t tifek/SR_11/ti_fek_public.pem`
    a. This will generate certificate with MSV certificate data at `<MCU_PLUS_SDK_INSTALL_DIR>/source/security/tifs/sbl_keywriter/scripts/x509cert/final_certificate.bin and also converts the certificate to C header file at <MCU_PLUS_SDK_INSTALL_DIR>/source/security/tifs/sbl_keywriter/keywr_bin/am263x/SR_11/Cust_KeysCert.h`

Problem 1: The directory of step_1 is incorrect, there is only cert_gen/common, there is no cert_gen/am263x

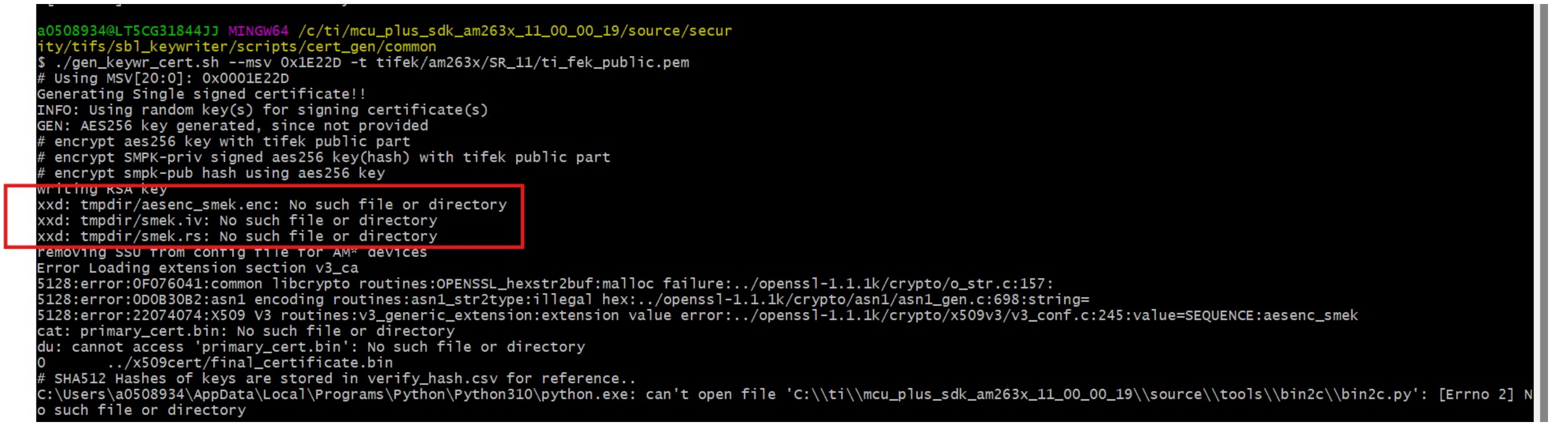
Fixed the path based on above assumption, and run the commands in step 2, I have the following error output.



MINGW64:/c/ti/mcu_plus_sdk_am263x_11_00_00_19/source/security/tifs/sbl_keywriter/scripts/cert_gen/commc

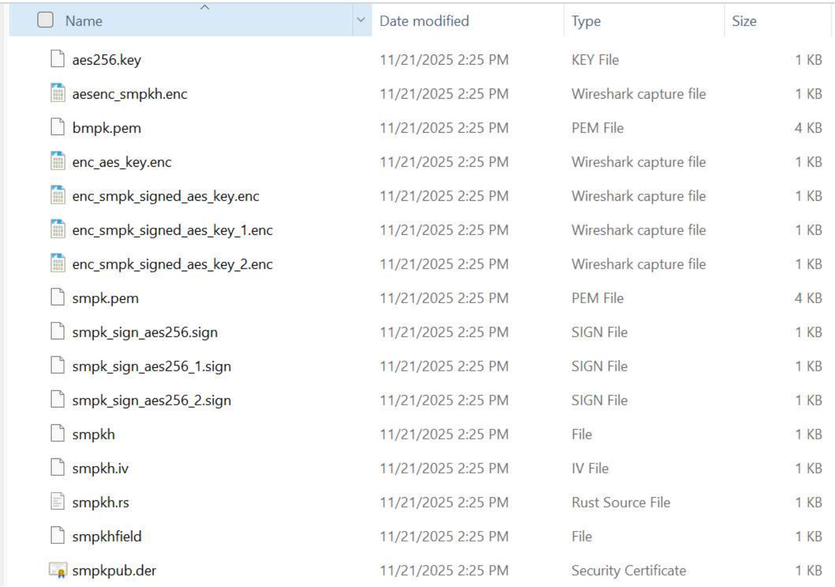
```
a0508934@LT5CG31844JJ MINGW64 /c/ti/mcu_plus_sdk_am263x_11_00_00_19/source/secur
ity/tifs/sbl_keywriter/scripts/cert_gen/common
$ ./gen_keywr_cert.sh --msv 0x1E22D -t tifek/SR_11/ti_fek_public.pem
# Using MSV[20:0]: 0x0001E22D
Generating Single signed certificate!!
INFO: Using random key(s) for signing certificate(s)
GEN: AES256 key generated, since not provided
# encrypt aes256 key with tifek public part
Can't open tifek/SR_11/ti_fek_public.pem for reading, No such file or directory
23368:error:02001003:system library:fopen:No such process:../openssl-1.1.1k/cryp
to/bio/bss_file.c:69:fopen('tifek/SR_11/ti_fek_public.pem','r')
23368:error:2006D080:BIO routines:BIO_new_file:no such file:../openssl-1.1.1k/cr
ypto/bio/bss_file.c:76:
unable to load Public Key
pkeyutl: Error initializing context
# encrypt SMPK-priv signed aes256 key(hash) with tifek public part
Can't open tifek/SR_11/ti_fek_public.pem for reading, No such file or directory
5740:error:02001003:system library:fopen:No such process:../openssl-1.1.1k/crypt
o/bio/bss_file.c:69:fopen('tifek/SR_11/ti_fek_public.pem','r')
5740:error:2006D080:BIO routines:BIO_new_file:no such file:../openssl-1.1.1k/cry
pto/bio/bss_file.c:76:
unable to load Public Key
pkeyutl: Error initializing context
Can't open tifek/SR_11/ti_fek_public.pem for reading, No such file or directory
19212:error:02001003:system library:fopen:No such process:../openssl-1.1.1k/cryp
to/bio/bss_file.c:69:fopen('tifek/SR_11/ti_fek_public.pem','r')
19212:error:2006D080:BIO routines:BIO_new_file:no such file:../openssl-1.1.1k/cr
ypto/bio/bss_file.c:76:
unable to load Public Key
pkeyutl: Error initializing context
# encrypt smpk-pub hash using aes256 key
writing RSA key
xxd: tmpdir/aesenc_smek.enc: No such file or directory
xxd: tmpdir/smek.iv: No such file or directory
xxd: tmpdir/smek.rs: No such file or directory
removing SSU from config file for AM* devices
Error Loading extension section v3_ca
21724:error:0F076041:common libcrypto routines:OPENSSL_hexstr2buf:malloc failure
:../openssl-1.1.1k/crypto/o_str.c:157:
21724:error:0D0B30B2:asn1 encoding routines:asn1_str2type:illegal hex:../openssl
-1.1.1k/crypto/asn1/asn1_gen.c:698:string=
21724:error:22074074:X509 V3 routines:v3_generic_extension:extension value error
:../openssl-1.1.1k/crypto/x509v3/v3_conf.c:245:value=SEQUENCE:aesenc_smek
cat: primary_cert.bin: No such file or directory
du: cannot access 'primary_cert.bin': No such file or directory
0       ../x509cert/final_certificate.bin
# SHA512 Hashes of keys are stored in verify_hash.csv for reference..
C:\Users\a0508934\AppData\Local\Programs\Python\Python310\python.exe: can't open
 file 'C:\\ti\\mcu_plus_sdk_am263x_11_00_00_19\\source\\tools\\bin2c\\bin2c.py':
 [Errno 2] No such file or directory
```

Problem 2: SR_11 folder is under tifek/am263x/, not directly under tifek/
Fixed the command as
./gen_keywr_cert.sh --msv 0x1E22D -t tifek/am263x/SR_11/ti_fek_public.pem
and run again, I have the below error output



```
a0508934@LT5CG31844JJ MINGW64 /c/ti/mcu_plus_sdk_am263x_11_00_00_19/source/secur
ity/tifs/sbl_keywriter/scripts/cert_gen/common
$ ./gen_keywr_cert.sh --msv 0x1E22D -t tifek/am263x/SR_11/ti_fek_public.pem
# Using MSV[20:0]: 0x0001E22D
Generating Single signed certificate!!
INFO: Using random key(s) for signing certificate(s)
GEN: AES256 key generated, since not provided
# encrypt aes256 key with tifek public part
# encrypt SMPK-priv signed aes256 key(hash) with tifek public part
# encrypt smpk-pub hash using aes256 key
writing RSA key
xxd: tmpdir/aesenc_smek.enc: No such file or directory
xxd: tmpdir/smek.iv: No such file or directory
xxd: tmpdir/smek.rs: No such file or directory
removing SSU from config file for AM* devices
Error Loading extension section v3_ca
5128:error:0F076041:common libcrypto routines:OPENSSL_hexstr2buf:malloc failure:../openssl-1.1.1k/crypto/o_str.c:157:
5128:error:0D0B30B2:asn1 encoding routines:asn1_str2type:illegal hex:../openssl-1.1.1k/crypto/asn1/asn1_gen.c:698:string=
5128:error:22074074:X509 V3 routines:v3_generic_extension:extension value error:../openssl-1.1.1k/crypto/x509v3/v3_conf.c:245:value=SEQUENCE:aesenc_smek
cat: primary_cert.bin: No such file or directory
du: cannot access 'primary_cert.bin': No such file or directory
0       ../x509cert/final_certificate.bin
# SHA512 Hashes of keys are stored in verify_hash.csv for reference..
C:\Users\a0508934\AppData\Local\Programs\Python\Python310\python.exe: can't open file 'C:\\ti\\mcu_plus_sdk_am263x_11_00_00_19\\source\\tools\\bin2c\\bin2c.py': [Errno 2] N
o such file or directory
```

The three files the script is looking for does not exist in the tmpdir. Nevertheless, this is should be a temporary folder as the name suggests, there might be some access issue in the git bash.



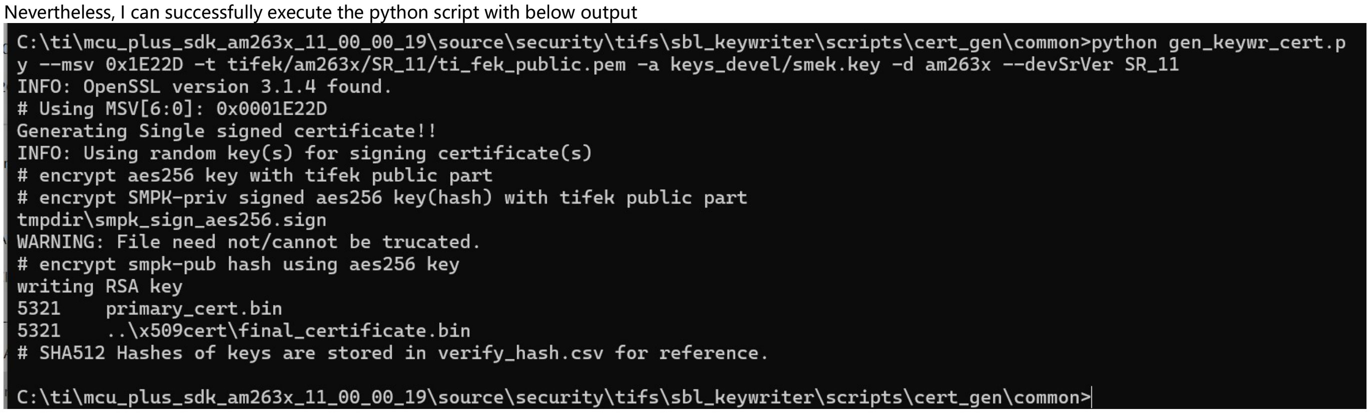
Name	Date modified	Type	Size
aes256.key	11/21/2025 2:25 PM	KEY File	1 KB
aesenc_smpkh.enc	11/21/2025 2:25 PM	Wireshark capture file	1 KB
bmpk.pem	11/21/2025 2:25 PM	PEM File	4 KB
enc_aes_key.enc	11/21/2025 2:25 PM	Wireshark capture file	1 KB
enc_smpk_signed_aes_key.enc	11/21/2025 2:25 PM	Wireshark capture file	1 KB
enc_smpk_signed_aes_key_1.enc	11/21/2025 2:25 PM	Wireshark capture file	1 KB
enc_smpk_signed_aes_key_2.enc	11/21/2025 2:25 PM	Wireshark capture file	1 KB
smpk.pem	11/21/2025 2:25 PM	PEM File	4 KB
smpk_sign_aes256.sign	11/21/2025 2:25 PM	SIGN File	1 KB
smpk_sign_aes256_1.sign	11/21/2025 2:25 PM	SIGN File	1 KB
smpk_sign_aes256_2.sign	11/21/2025 2:25 PM	SIGN File	1 KB
smpkh	11/21/2025 2:25 PM	File	1 KB
smpkh.iv	11/21/2025 2:25 PM	IV File	1 KB
smpkh.rs	11/21/2025 2:25 PM	Rust Source File	1 KB
smpkhfield	11/21/2025 2:25 PM	File	1 KB
smpkpub.der	11/21/2025 2:25 PM	Security Certificate	1 KB

For the above error, I tried the python script instead of the .sh script. For the python script I run it with windows console instead of git bash.

I used the below command:
python gen_keywr_cert.py --msv 0x1E22D -t tifek/am263x/SR_11/ti_fek_public.pem -a keys_devel/smek.key -d am263x --devSrVer SR_11

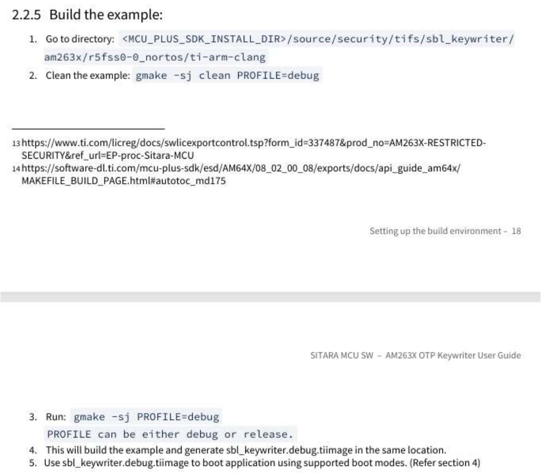
(PS: I tried to refer to the command mentioned in section 3.2.1, however, it's missing -d parameter, path for -t is correct like previously said)

Nevertheless, I can successfully execute the python script with below output



```
C:\ti\mcu_plus_sdk_am263x_11_00_00_19\source\security\tifs\sbl_keywriter\scripts\cert_gen\common>python gen_keywr_cert.p
y --msv 0x1E22D -t tifek/am263x/SR_11/ti_fek_public.pem -a keys_devel/smek.key -d am263x --devSrVer SR_11
INFO: OpenSSL version 3.1.4 found.
# Using MSV[6:0]: 0x0001E22D
Generating Single signed certificate!!
INFO: Using random key(s) for signing certificate(s)
# encrypt aes256 key with tifek public part
# encrypt SMPK-priv signed aes256 key(hash) with tifek public part
tmpdir\smpk_sign_aes256.sign
WARNING: File need not/cannot be trucated.
# encrypt smpk-pub hash using aes256 key
writing RSA key
5321    primary_cert.bin
5321    ..\x509cert\final_certificate.bin
# SHA512 Hashes of keys are stored in verify_hash.csv for reference.

C:\ti\mcu_plus_sdk_am263x_11_00_00_19\source\security\tifs\sbl_keywriter\scripts\cert_gen\common>
```

I assumes this means the x509 is generated correctly. Next, I continued to follow the guide and build the key writer appliaction



2.2.5 Build the example:

1. Go to directory: `<MCU_PLUS_SDK_INSTALL_DIR>/source/security/tifs/sbl_keywriter/am263x/r5fss0-0_nortos/ti-arm-clang`
2. Clean the example: `gmake -sj clean PROFILE=debug`

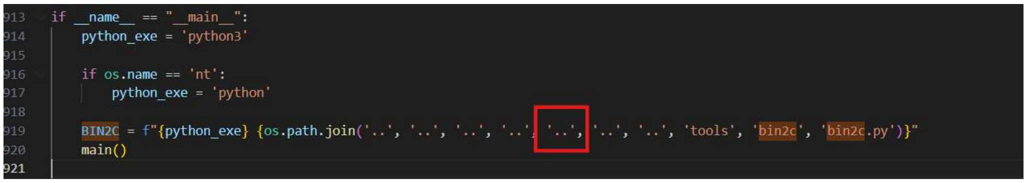
[13] https://www.ti.com/licreg/docs/swlicexportcontrol.tsp?form_id=337487&prod_no=AM263X-RESTRICTED-SECURITY&ref_url=EP-proc-Sitara-MCU

[14] https://software-dl.ti.com/mcu-plus-sdk/esd/AM64X/08_02_00_08/exports/docs/api_guide_am64x/MAKEFILE_BUILD_PAGE.html#autotoc_md175

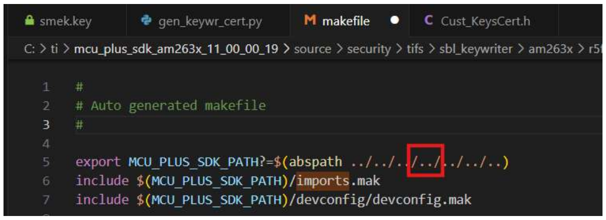
3. Run: `gmake -sj PROFILE=debug`
   `PROFILE can be either debug or release.`
4. This will build the example and generate sbl_keywriter.debug.tiimage in the same location.
5. Use sbl_keywriter.debug.tiimage to boot application using supported boot modes. (Refer section 4)

Again, there is path errors for three items:

1. Import.mak
2. Include path
3. Path for bin2c, I fixed them as below

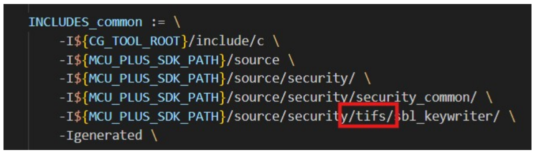


```
if __name__ == "__main__":
    python_exe = 'python3'

    if os.name == 'nt':
        python_exe = 'python'

    BIN2C = f"{python_exe} {os.path.join('..', '..', '..', '..', '..', '..', '..', 'tools', 'bin2c', 'bin2c.py')}"
    main()

```



smek.key
gen_keywr_cert.py
makefile
Cust_KeysCert.h
C: > ti > mcu_plus_sdk_am263x_11_00_00_19 > source > security > tifs > sbl_keywriter > am263x > r5

```
#
# Auto generated makefile
#

export MCU_PLUS_SDK_PATH?=$(abspath ../../../../../../..)
include $(MCU_PLUS_SDK_PATH)/imports.mak
include $(MCU_PLUS_SDK_PATH)/devconfig/devconfig.mak
```



```
INCLUDES_common := \
    -I${CG_TOOL_ROOT}/include/c \
    -I${MCU_PLUS_SDK_PATH}/source \
    -I${MCU_PLUS_SDK_PATH}/source/security/ \
    -I${MCU_PLUS_SDK_PATH}/source/security/security_common/ \
    -I${MCU_PLUS_SDK_PATH}/source/security/tifs/sbl_keywriter/ \
    -Igenerated \
```

With that, I can compile the example successfully