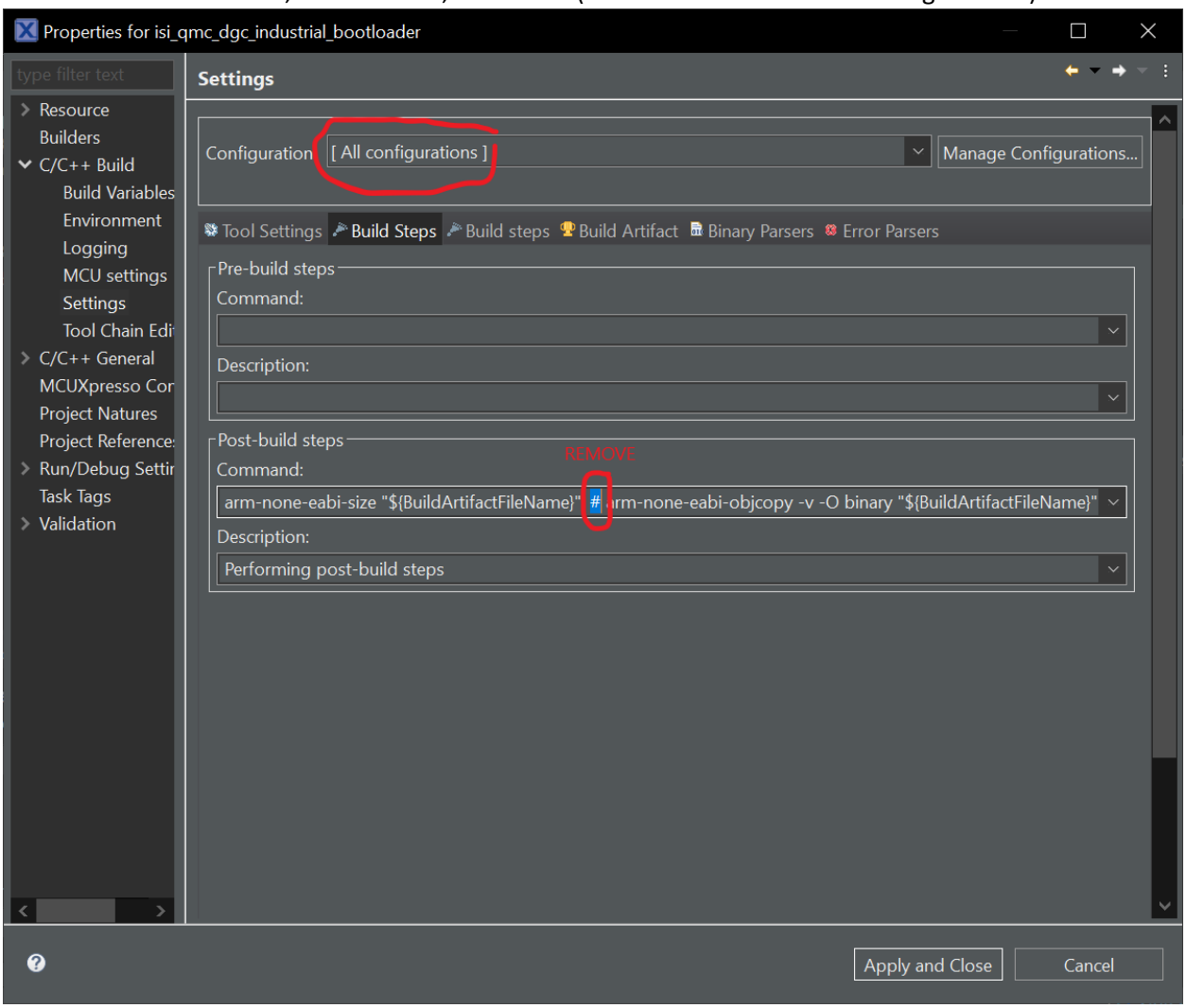
How To Program QMC2G main FW along with SBL

1. Open the QMC2G project in MCUXpresso.
2. Open the project properties window for the CM7 and Bootloader projects, go to *Properties > C/C++ Build > Settings > Build Steps* and remove the **#** symbol in front of *arm-none-eabi-objcopy*, so that *.bin file creation, needed later, is enabled (make sure to do it for all configurations):



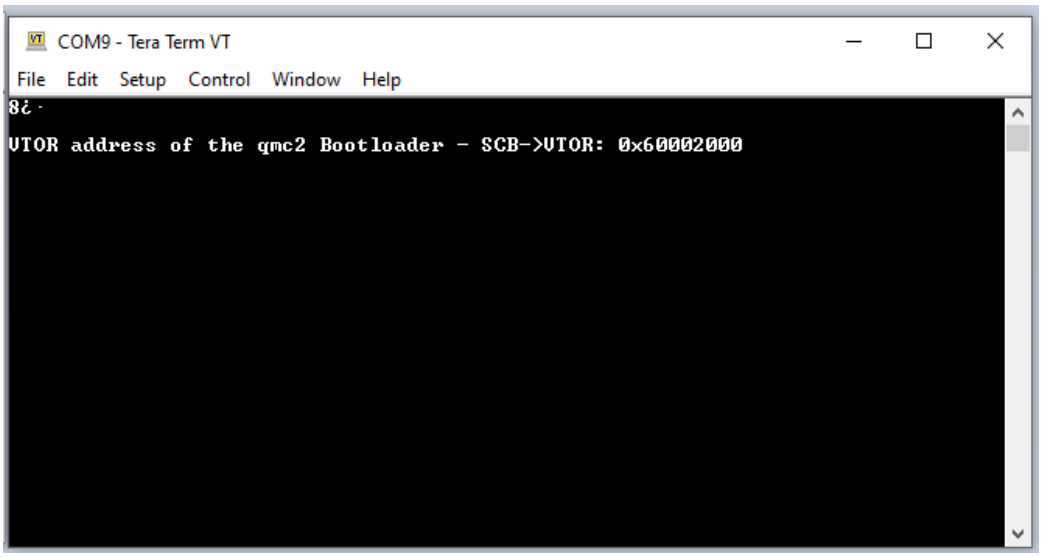
3. Compile the **isi_qmc_dgc_industrial_bootloader** project using **Debug_Non_Secure** or **Debug (Secure)** target.
4. Next, compile the CM4 and then the CM7 project using **Debug_SBL** targets.
5. Go into the **"tools"** folder located at the application sw pack directory, which contains two batch files.
    a. **blhost_usb_cmd_xip_app.bat –** programs the board with both the main FW and SBL with disabled security.
    b. **blhost_usb_cmd_xip_app_secure.bat –** programs the SBL with enabled security and all essential fuses + PUF KeyStore. The main FW will be programmed by SBL from SD card.

6. **Edit the paths on lines 74 and 75 in blhost_usb_cmd_xip_app.bat and on line 108 in blhost_usb_cmd_xip_app_secure.bat to point to your project binaries correctly.**

blhost_usb_cmd_xip_app.bat

As this script does not use any of the security features, no provisioning is needed. The binaries can be programmed directly.

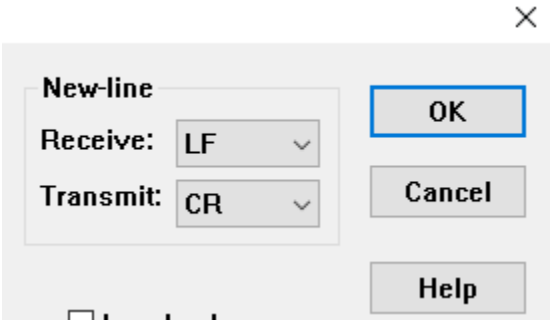
1. Configure the switch SW4 on the daughter card to SDP mode (1-ON/2-OFF/3-OFF/4-OFF).
2. Connect micro-USB cable into J3 on the daughter card and press reset(SW2).
3. Execute the **blhost_usb_cmd_xip_app.bat.**
4. Configure the switch SW4 on the daughter card to Boot from fuses mode (1-OFF/2-OFF/3-OFF/4-OFF).
5. Reconnect the micro-USB cable to the J48 on the digital board.
6. Power up the board if needed.
7. Use an application to establish serial communication for both COM ports (115200).
8. Press reset button on daughter card (SW2) and after 5 seconds you should see similar prints on both consoles:



COM3 - Tera Term VT

File Edit Setup Control Window Help

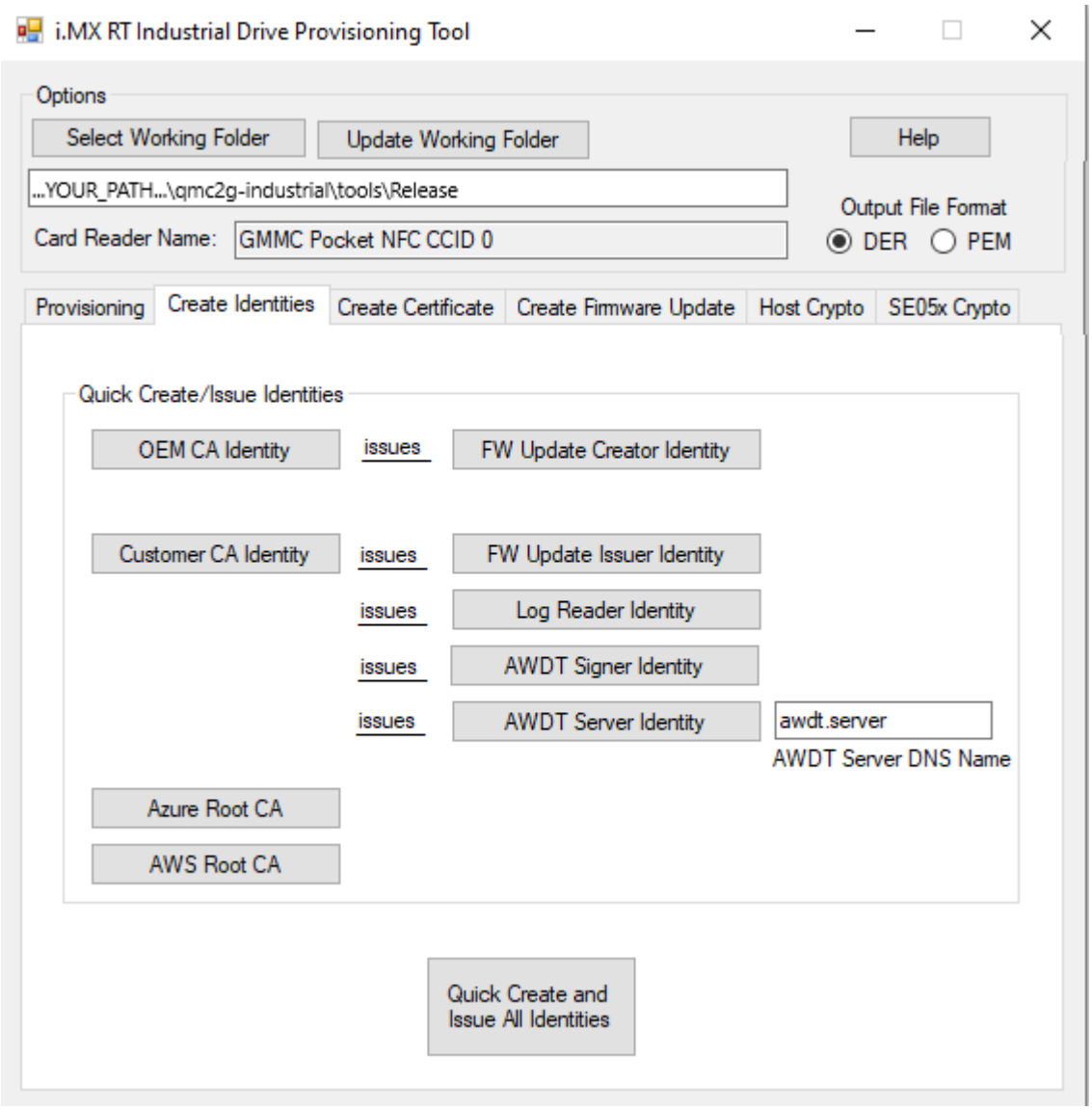
```
QMC2G code started
Rootclock:52MHz
Rootclock:264MHz
Starting GPT timer(400f8000), frequency: 11718
INIT            0.000000000 api    genavb_init                    : NXP's GenAV
B/TSN stack version 4_0_3-dirty (Built Sep 13 2021 14:20:44)
INIT            0.000000000 freertos hw_avb_timer_init            : hw_timer_
init done
INIT            0.000000000 freertos hw_clock_init                : rate: 240
00000, period: 100000000, mult(to ns): 699050667, shift(to ns): 24, mult(to cycl
es): 103079215, shift(to cycles): 32
INIT            0.000000000 freertos hw_clock_register            : hw clock
id: 1 registered
INIT            0.000000000 freertos hw_timer_register            : hw_timer(
20246B04) of clock id: 1 registered
INIT            0.000000000 freertos hw_timer_register            : hw_timer(
20246B28) of clock id: 1 registered
INIT            0.000000000 freertos hw_timer_register            : hw_timer(
20246B4C) of clock id: 1 registered
INFO            0.000000000 freertos hw_avb_timer_register_device : dev(20246
D78) , ref clock 24000000 Hz, min delay cycles 240
INFO            0.000000000 freertos gpt_hw_timer_set_period      : gpt_dev (
20246D58) set period 125(us), 3000(cycles)
INIT            0.000000000 freertos gpt_init                     : gpt_init
```



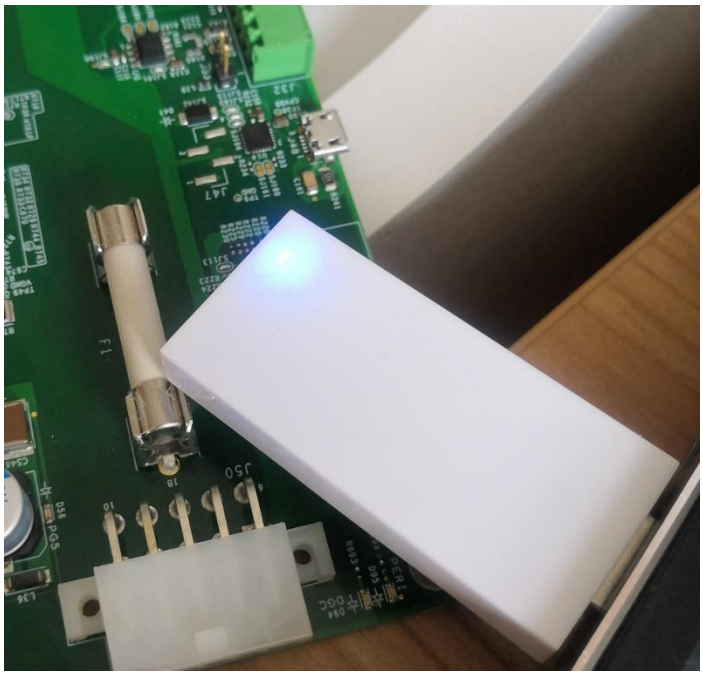
blhost_usb_cmd_xip_app_secure.bat

This utilizes the security features of the SBL, which require additional steps. The Main FW will be programed by the SBL from a mini-SD card. Provisioning of the security assets into the SE must be done via an NFC reader.

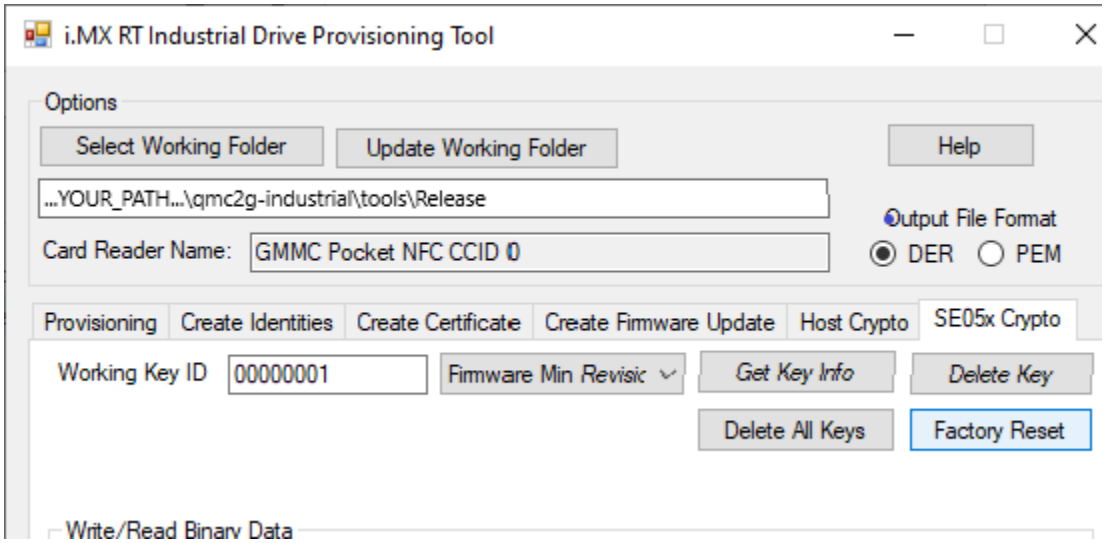
1. Power off the QMC2G HW to enable provisioning via NFC.
2. Insert the NFC reader into your PC and let it install. After successful installation the LED will be blinking red/blue/white color.
3. Go into the **“tools”** folder located at **root** directory and unzip the **“Qmc2gProvisioningTool.zip”** file to **“tools/Release”** folder. **Password is “123”.**
4. Run the tool **“Qmc2gProvisioningTool.exe”.** All files will be placed on taken from the Working folder. You can change the working folder according to your preference (Need to copy image_enc.exe into your customized working folder).
5. Go to the “Create Identities” tab and press “Quick Created and Issue all Identities” All generated content will be placed into your working folder.



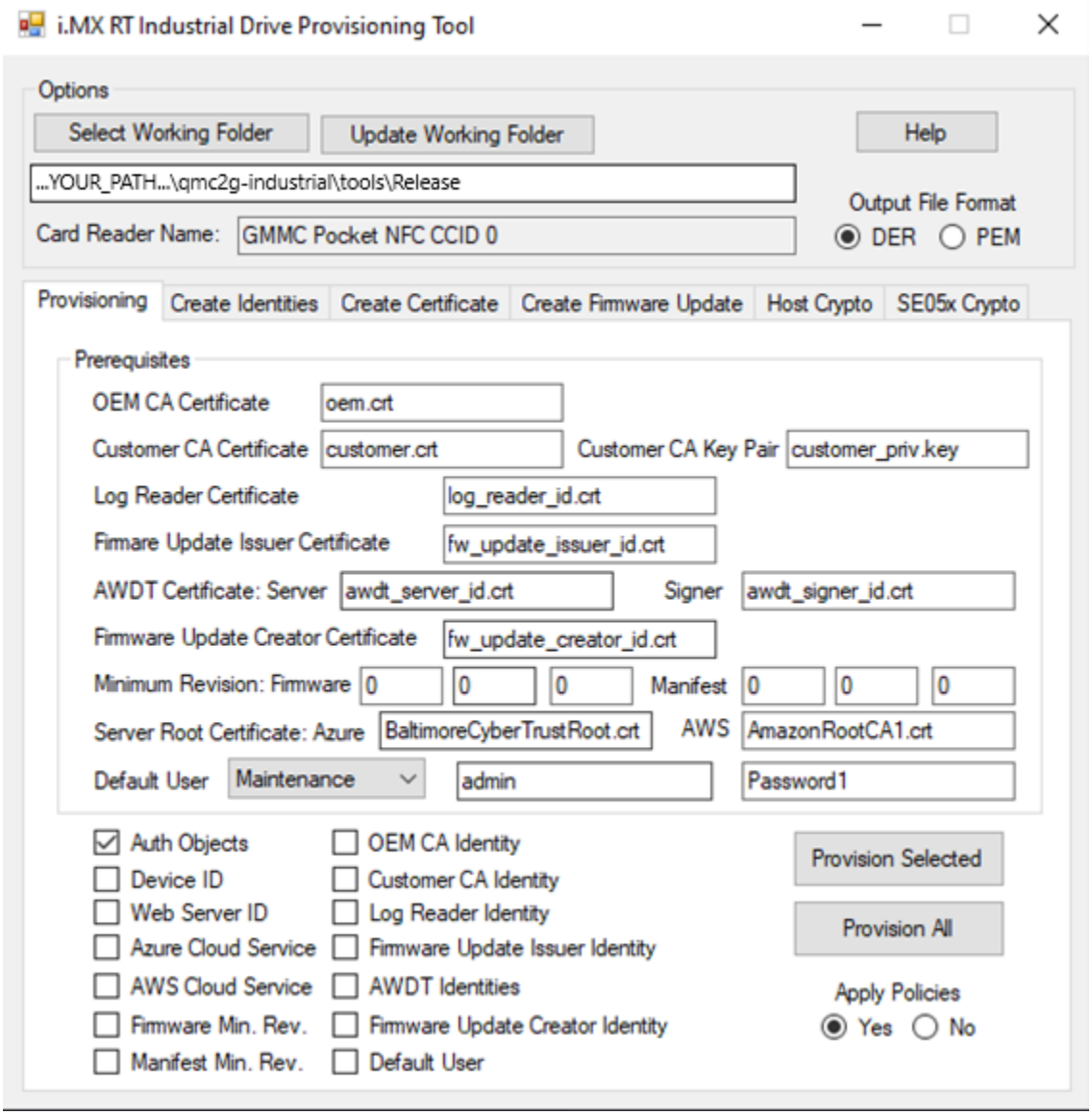
6. Go to the **"SE05x_Crypto"** tab.
7. Take the unpowered Digital board and place the board by the NFC antenna below the NFC reader. The LED color will change to white once a connection is established.



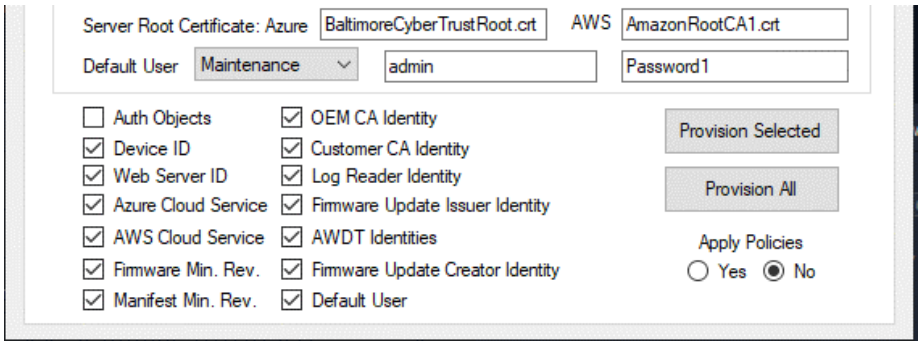
8. In the provisioning tool press the Factory reset button while having the NFC Reader connected the Secure element on the Digital Board.



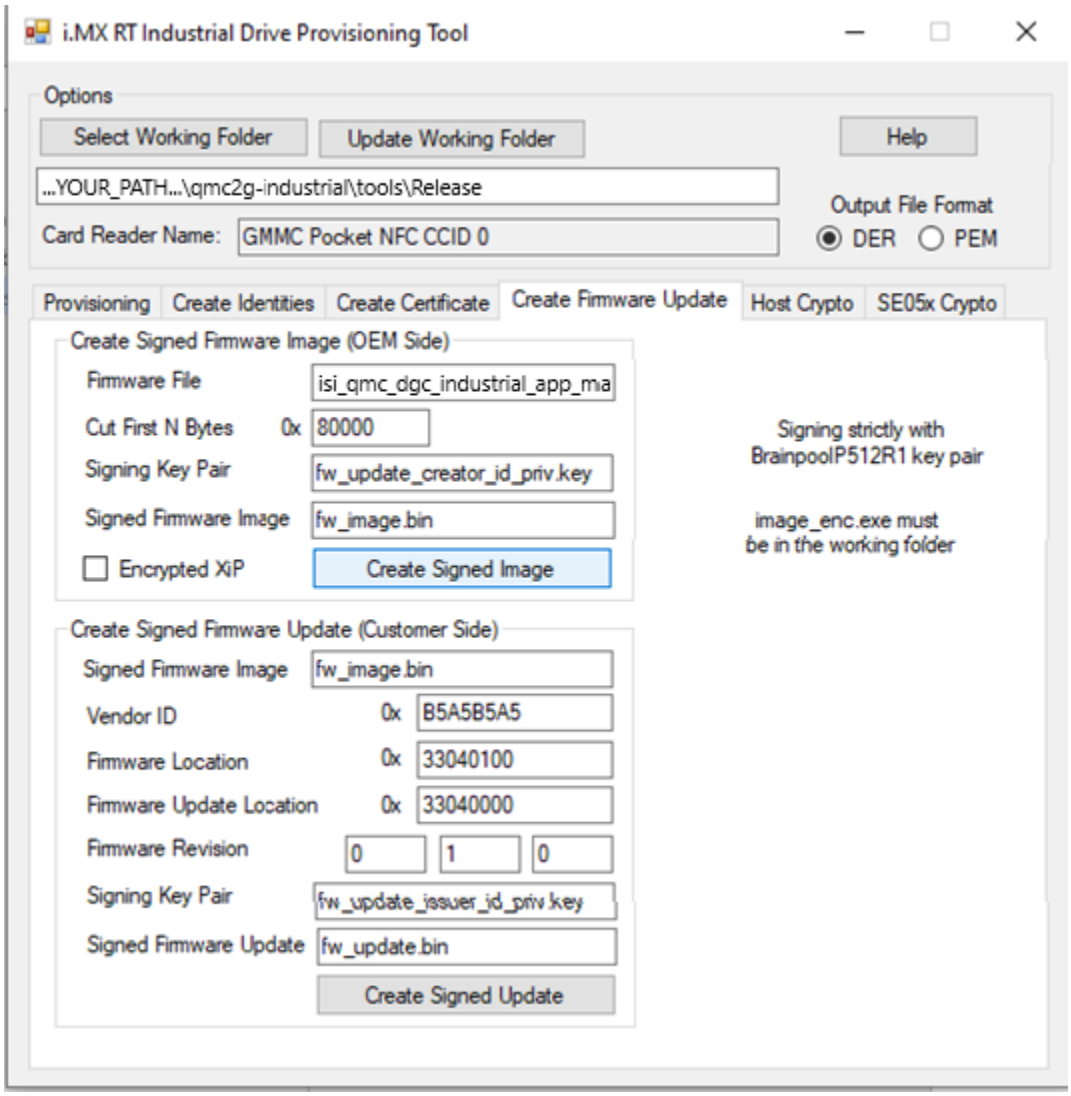
9. Go to the “Provisioning” tab to finally provision the SE with security assets. The provision steps must be done in the steps as policies for secure objects have not been fully defined yet.
10. Apply Policies using the “Yes” radio button and select “Auth Objects”. Press “Provision Selected” button while having the NFC Reader connected the Secure element on the Digital Board.



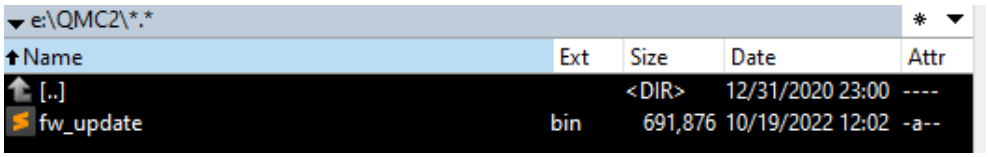
11. Deselect “Auth Objects” and set Apply Policies to “NO”.
12. Select all remaining checkboxes.
13. Press Again “Provision Selected” button while having the NFC Reader connected the Secure element on the Digital Board. It takes few seconds to complete the operation.



14. Secure element on the Digital board is provisioned. Secure FW update image can be generated.
15. Copy the “isi_qmc_dgc_industrial_app_master_cm7**Debug_SBL**\ **isi_qmc_dgc_industrial_app_master_cm7.bin**” into your Provisioning Tool working folder where all security assets were generated.
16. Go into the “Create Firmware Update” tab.
17. Deselect “Encrypted XiP” as we do not use this feature for now.
18. Increase Manifest firmware revision. It must be greater than minimum Manifest revision configured during the provisioning step (default 0.0.0).



19. Press **“Create Signed Image”** button.
20. Press” **“Create Signed Update”** button.
21. Copy the resulting **“fw_update.bin”** from your working folder onto mini-SD card in the folder **“QMC2”**



e:\QMC2*.*

Name	Ext	Size	Date	Attr
[..]		<DIR>	12/31/2020 23:00	----
fw_update	bin	691,876	10/19/2022 12:02	-a--

22. Insert the SD card into Daughter card SD memory slot(below battery).
23. Provisioning Tool can be closed.
24. Configure the switch SW4 on the daughter card to SDP mode (1-ON/2-OFF/3-OFF/4-OFF).
25. Connect micro-USB cable into J3 on the daughter card and press reset(SW2).
26. Execute the **blhost_usb_cmd_xip_app_secure.bat. The script programs all essential fuses, PUF keystore and secure version of SBL.**
27. Configure the switch SW4 on the daughter card to Boot from fuses mode (1-OFF/2-OFF/3-OFF/4-OFF).
28. Reconnect the micro-USB cable to the J48 on the digital board.
29. Power up the board if needed.
30. Use an application to establish serial communication for both COM ports (115200).
31. Press reset button on daughter card (SW2) and after 5 seconds you should see similar prints on both consoles:

```
VTOR address of the qmc2 Bootloader - SCB->VTOR: 0x60002000

Info: SDCARD is inserted!
sss    :INFO :atr (Len=35)
                01 A0 00 00      03 96 04 03      E8 00 FE 02      0B 03 E8 00
                01 00 00 00      00 64 13 88      0A 00 65 53      45 30 35 31
                00 00 00
App    :INFO :Reading binary data at 0x0000001D
App    :INFO :Device is commissioned !
Device is commisioned! Policy AES key is present.
SCP03 key generation successful!
SCP03 KeyStore programming successful!
SCP03 Keys reconstructed successfully!
sss    :INFO :atr (Len=35)
                01 A0 00 00      03 96 04 03      E8 00 FE 02      0B 03 E8 00
                01 00 00 00      00 64 13 88      0A 00 65 53      45 30 35 31
                00 00 00
App    :INFO :Erasing binary data at 0x0000001D
App    :INFO :Device is commissioned !
AES key was errased sucessfully!
SNVS LP GPR Init successful!
sss    :INFO :atr (Len=35)
                01 A0 00 00      03 96 04 03      E8 00 FE 02      0B 03 E8 00
                01 00 00 00      00 64 13 88      0A 00 65 53      45 30 35 31
                00 00 00
App    :INFO :SE05x Read State Successfully!!!
App    :INFO :Following is the SE05x Read State status
App    :INFO :SE05x Lock State = 0x2  i.e. SE05x is Unlocked!!!
App    :INFO :SE05x Restrict Mode = 0x0  i.e. No Restriction is applied for object creation!!!
App    :INFO :SE05x Platform SCP Request = 0x2  i.e. Platform SCP is not required for Communication
sss    :INFO :atr (Len=35)
                01 A0 00 00      03 96 04 03      E8 00 FE 02      0B 03 E8 00
                01 00 00 00      00 64 13 88      0A 00 65 53      45 30 35 31
                00 00 00
App    :INFO :Reading binary data at 0x00000001
App    :INFO :Reading binary data at 0x00000002
No Request from Main FW.
New FW update detected!

**********************************

Copy data from SDcard to STORAGE.!

**********************************
sss    :INFO :atr (Len=35)
                01 A0 00 00      03 96 04 03      E8 00 FE 02      0B 03 E8 00
                01 00 00 00      00 64 13 88      0A 00 65 53      45 30 35 31
                00 00 00
App    :INFO :Do Verify
App    :INFO :digest (Len=64)
                C8 67 B6 26      79 59 2B 58      81 53 4B A4      F8 8E 56 55
                A6 44 40 82      DC 16 30 91      E5 B9 39 0A      25 3B 27 82
                88 50 88 6E      BF 76 31 13      14 E3 8E 77      D6 19 A8 43
                1A FF 5B A3      AE 21 52 D7      B1 D3 5E 25      11 6D 0C 11
App    :INFO :signature (Len=135)
                30 81 84 02      40 39 48 FB      4E 34 4B FB      25 11 E8 14
                D6 16 81 F0      84 8D E0 9B      03 33 4F A8      F0 EF 16 D7
                43 DC A4 FC      20 38 A1 40      D5 96 F0 43      94 D9 F1 D5
                FD C8 3C CB      89 A4 0C 57      BB 8C 61 9A      CA 90 5A BB
                6C 5B 49 17      7F 02 40 10      DD A9 FC 3B      62 C0 10 07
                B6 40 73 90      03 99 5D 3B      5C AB 49 3E      4C 05 47 7E
                29 4F 8F EF      AE 0E A0 81      1C ED 44 B2      91 26 C1 22
                CA 46 90 8E      60 1D F7 60      89 EB 8F C6      2D 13 0A 2A
                FD 9D 24 04      4F 76 C0
App    :INFO :Verification Successful !!!
sss    :INFO :atr (Len=35)
                01 A0 00 00      03 96 04 03      E8 00 FE 02      0B 03 E8 00
                01 00 00 00      00 64 13 88      0A 00 65 53      45 30 35 31
                00 00 00
sss    :WARN :Object id 0x2 exists
App    :INFO :Injecting binary data at 0x00000002
App    :INFO :Reading binary data at 0x00000002
FW Update completed!
sss    :INFO :atr (Len=35)
                01 A0 00 00      03 96 04 03      E8 00 FE 02      0B 03 E8 00
                01 00 00 00      00 64 13 88      0A 00 65 53      45 30 35 31
                00 00 00
App    :INFO :Do Verify
App    :INFO :digest (Len=64)
                F2 83 EA C7      FB 97 1A D9      14 22 D3 21      9F 2F E6 E1
                0A E7 05 F6      5C B9 68 4A      22 99 EC F2      66 A6 A2 C0
                80 A1 2A 6B      23 CD 63 61      09 64 16 38      B9 40 46 F8
                3C BB 31 0A      DB F6 EF E0      9A FC 6E BA      67 1F 25 05
App    :INFO :signature (Len=135)
                30 81 84 02      40 21 FD 69      BA 33 84 C8      D0 80 36 20
                0D 46 B9 E5      9A FE 0D B3      AB 6C 32 C6      FA C3 70 39
                F6 3E F4 49      B6 09 19 20      57 7F EF 8D      E5 07 E9 D1
                BE 29 9F C9      EB 0A 97 56      07 7B C3 2E      F4 9D 76 78
                F2 B1 44 54      90 02 40 30      E2 77 06 15      FE 03 6F 62
                03 79 72 06      E3 22 F1 C9      4A 67 F1 6F      F3 D8 B8 AB
                C0 77 D7 43      FB D0 6D 25      EC B7 8E 9B      D7 C7 B1 30
                96 46 49 E5      85 33 77 08      A7 72 F1 61      B7 29 42 2B
                16 1F F1 EA      A4 69 1F
```

```
QMC2G code started
Rootclock:52MHz
Rootclock:264MHz
Mutex init ok. Configuration.
Read flash chksum fail. Using defaults. Configuration.
DataloggerTask create OK. Datalogger.
INIT            0.000000000 api    genavb_init                      : NXP's GenAVB/TSN stack version 4_0_3-dirt
(Built Sep 13 2021 14:20:44)
INIT            0.000000000 freertos hw_avb_timer_init              : hw_timer_init done
INIT            0.000000000 freertos hw_clock_init                  : rate: 24000000, period: 100000000, mult
o ns): 699050667, shift(to ns): 24, mult(to cycles): 103079215, shift(to cycles): 32
INIT            0.000000000 freertos hw_clock_register              : hw clock id: 1 registered
INIT            0.000000000 freertos hw_timer_register              : hw_timer(20246C5C) of clock id: 1 regis
red
INIT            0.000000000 freertos hw_timer_register              : hw_timer(20246C80) of clock id: 1 regis
red
INIT            0.000000000 freertos hw_timer_register              : hw_timer(20246CA4) of clock id: 1 regis
red
INFO            0.000000000 freertos hw_avb_timer_register_device   : dev(20246ED0) , ref clock 24000000 Hz,
n delay cycles 240
INFO            0.000000000 freertos gpt_hw_timer_set_period        : gpt_dev (20246EB0) set period 125(us),
00(cycles)
INIT            0.000000000 freertos gpt_init                       : gpt_init : registered AVB HW timer(2024
00) channel: 0, prescale: 1
ERR             0.000000000 freertos gpt_init                       : gpt_init : failed to register GPT media
lock recovery
INIT            0.000000000 freertos __port_init                    : port(0): 2024939C
INIT            0.000000000 freertos enet_qos_init                  : port(0) enet(0) ptp clock: 200000000 Hz
core clock: 240000000 Hz num TX queue: 5, num RX queue: 4
INIT            0.000000000 freertos hw_clock_init                  : rate: 1000000000, period: 3b9ac9ffc4653
0, mult(to ns): 1, shift(to ns): 0, mult(to cycles): 1, shift(to cycles): 0
INIT            0.000000000 freertos hw_clock_register              : hw clock id: 2 registered
INIT            0.000000000 freertos hw_timer_register              : hw_timer(20247524) of clock id: 2 regis
red
INIT            0.000000000 freertos hw_timer_register              : hw_timer(20247548) of clock id: 2 regis
red
INIT            0.000000000 freertos hw_timer_register              : hw_timer(2024756C) of clock id: 2 regis
red, pps support
INIT            0.000000000 freertos _os_clock_init                 : clock ID: 0 success, flags: 0
ERR             0.000000000 freertos _os_clock_init                 : clock ID: 1 has no hw clock
ERR             0.000000000 freertos _os_clock_init                 : clock ID: 2 has no hw clock
ERR             0.000000000 freertos _os_clock_init                 : clock ID: 3 has no hw clock
ERR             0.000000000 freertos _os_clock_init                 : clock ID: 4 has no hw clock
ERR             0.000000000 freertos _os_clock_init                 : clock ID: 5 has no hw clock
ERR             0.000000000 freertos _os_clock_init                 : clock ID: 6 has no hw clock
ERR             0.000000000 freertos _os_clock_init                 : clock ID: 7 has no hw clock
INIT            0.000000000 freertos _os_clock_init                 : clock ID: 8 success, flags: 1
INIT            0.000000000 freertos _os_clock_init                 : clock ID: 9 success, flags: 0
ERR             0.000000000 freertos _os_clock_init                 : clock ID: 10 has no hw clock
ERR             0.000000000 freertos _os_clock_init                 : clock ID: 11 has no hw clock
ERR             0.000000000 freertos _os_clock_init                 : clock ID: 12 has no hw clock
ERR             0.000000000 freertos _os_clock_init                 : clock ID: 13 has no hw clock
INIT            0.000000000 freertos _os_clock_init                 : clock ID: 14 success, flags: 4
ERR             0.000000000 freertos _os_clock_init                 : clock ID: 15 has no hw clock
ERR             0.000000000 freertos _os_clock_init                 : clock ID: 16 has no hw clock
INFO            0.000000000 freertos net_qos_map_traffic_class_to_hw_ : port(0) num tc: 5, num sr: 2, num hw qu
es: 5
INFO            0.000000000 freertos net_qos_map_traffic_class_to_hw_ : num hw queues: 5, num cbs: 2
INFO            0.000000000 freertos net_qos_map_traffic_class_to_hw_ : tc(0)->hw_queue_id: 0, flags: 2, hw que
 prop: 1
INFO            0.000000000 freertos net_qos_map_traffic_class_to_hw_ : tc(1)->hw_queue_id: 1, flags: 2, hw que
 prop: 1
INFO            0.000000000 freertos net_qos_map_traffic_class_to_hw_ : tc(2)->hw_queue_id: 2, flags: 2, hw que
 prop: 1
INFO            0.000000000 freertos net_qos_map_traffic_class_to_hw_ : tc(3)->hw_queue_id: 3, flags: 1, hw que
 prop: 2
INFO            0.000000000 freertos net_qos_map_traffic_class_to_hw_ : tc(4)->hw_queue_id: 4, flags: 1, hw que
 prop: 2
INFO            0.000000000 freertos hw_timer_request               : hw_timer(20246CA4)
```