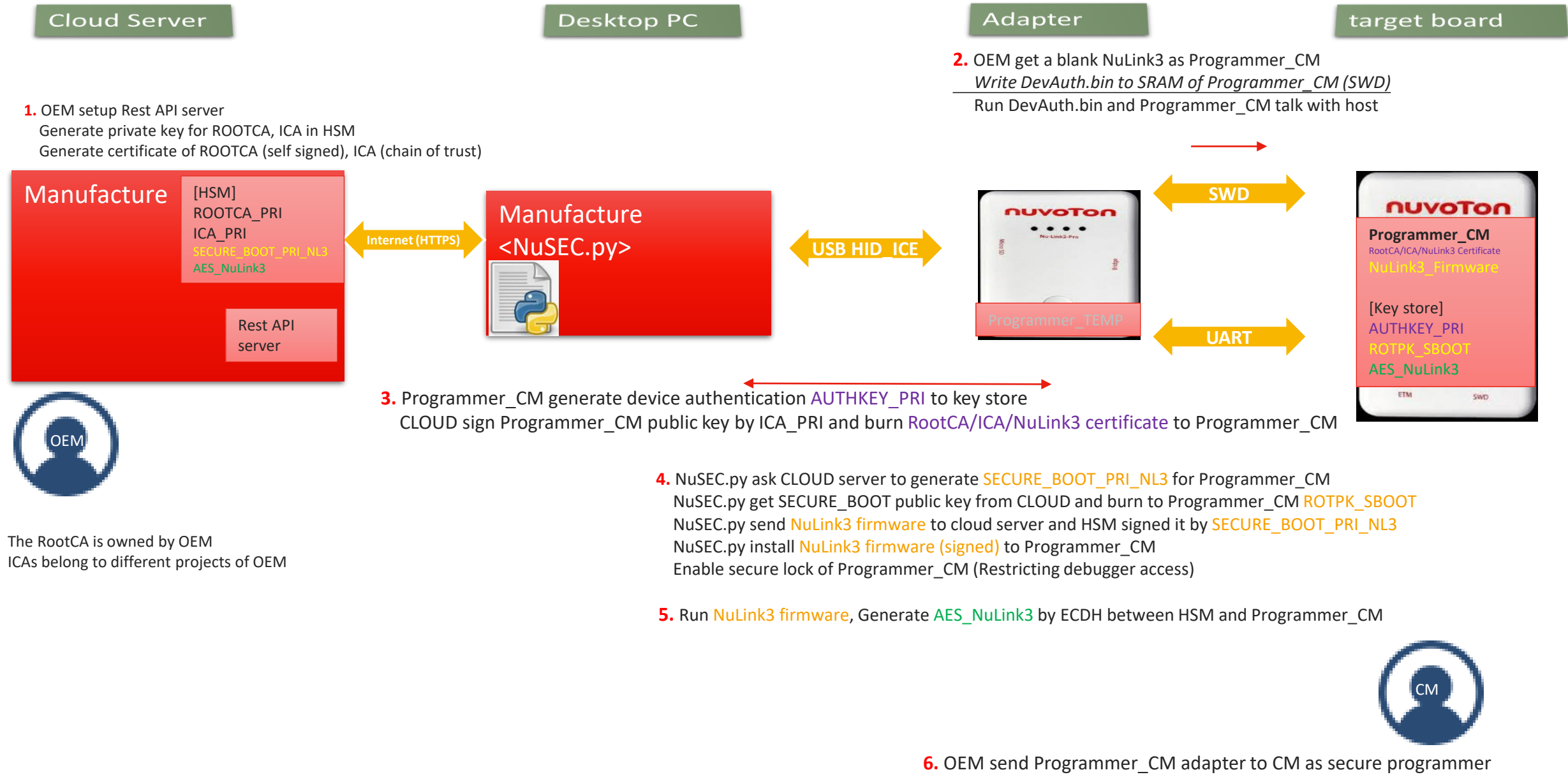


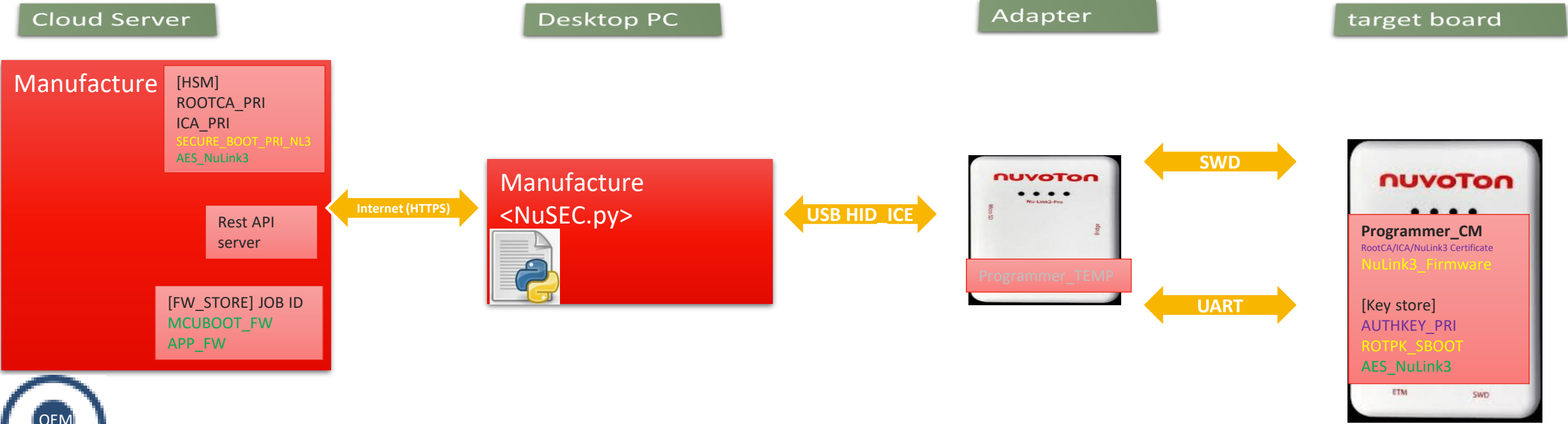
Manufacture stage



Prepare NuLink3 programmer for CM (In an OEM's secure environment)



EXPORT PROJECT for CM (by OEM)



7. OEM use PROJECT EXPORTER (function of NuSEC.py)
Generating a package for the CM, the package include:
- Production count
 - **JOB ID (AS A TOKEN)**
 - IDs to check (e.g. UID list provided by chip vendor)

8. Encrypt package by **AES_NuLink3**, OEM send encrypted package to CM
OEM upload target firmware (**MCUBOOT: BL2, APP_FW: BL3**) to FW_STORE server
Bind uploaded firmware with corresponding Job ID



9. OEM send encrypted package to CM by Email

Import OEM package (CM)

Cloud Server

Desktop PC

Adapter (NuLink3)

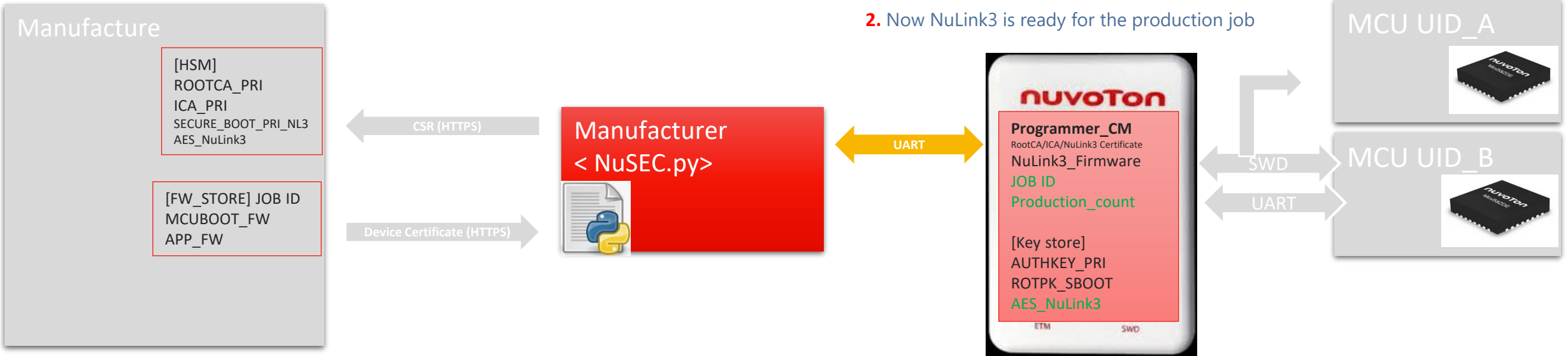
target board

0. CM use package importer function of NuSEC.py to import OEM package to NuLink3



1. The package is processed in NuLink3 SECURE ENVIRONMENT to ensure authenticity and integrity after transporting from OEM to NuLink3. The package is then decrypted (by AES_NuLink3) in NuLink3 SECURE ENVIRONMENT and **production_count/Job_ID/..** are programmed in the NuLink3

2. Now NuLink3 is ready for the production job



3. For each provision.
NuLink3 decrease the production count number
Read device UID and communicate with cloud server
Device authentication provision (the following slide)
Secure boot key provision and FW installation (the following slide)
Firmware installation will be rejected if device authentication fail

Device authentication key provision

Cloud Server

Desktop PC

Adapter (NuLink3)

target board

0. Trigger Mass Production flow by NuSEC.py, BLE/WIFI connect to Programmer_CM and it's the **start point** of target device provisioning procedure

2. Program NuLink3 Certificate, ROOTCA CERT (SWD)
Program DevAuth_MCU.bin to SRAM and run it (SWD)

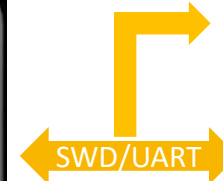
1. Programmer_CM "mutual TLS" with Cloud, from authentication to get SESSION KEY
https://builtin.com/sites/www.builtin.com/files/styles/ckeditor_optimize/public/inline-images/2_mutual-tls-tutorial.jpg

3. Generate private key and store it in key store

4. Target MCU send "pubkey+UID" to NuLink3
5. NuLink3 send CSR hash to Target MCU
6. Target MCU sign the CSR hash with private key of NuLink3

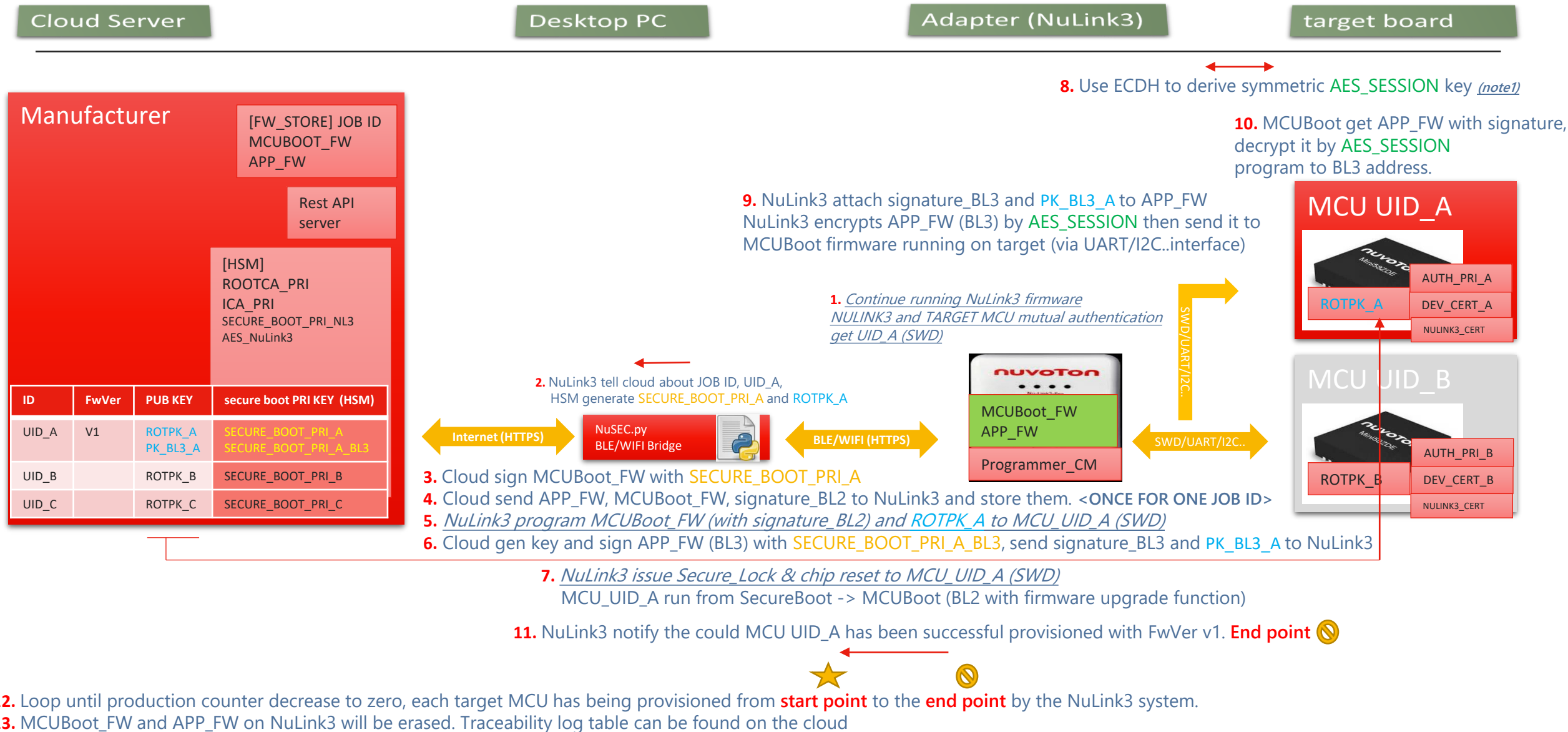
7. Send CSR (certificate signing request) to CLOUD

8. CLOUD verify signature, create device certificate DEV_CERT (UID, pubkey, ICA sign), and then provision it to the MCU

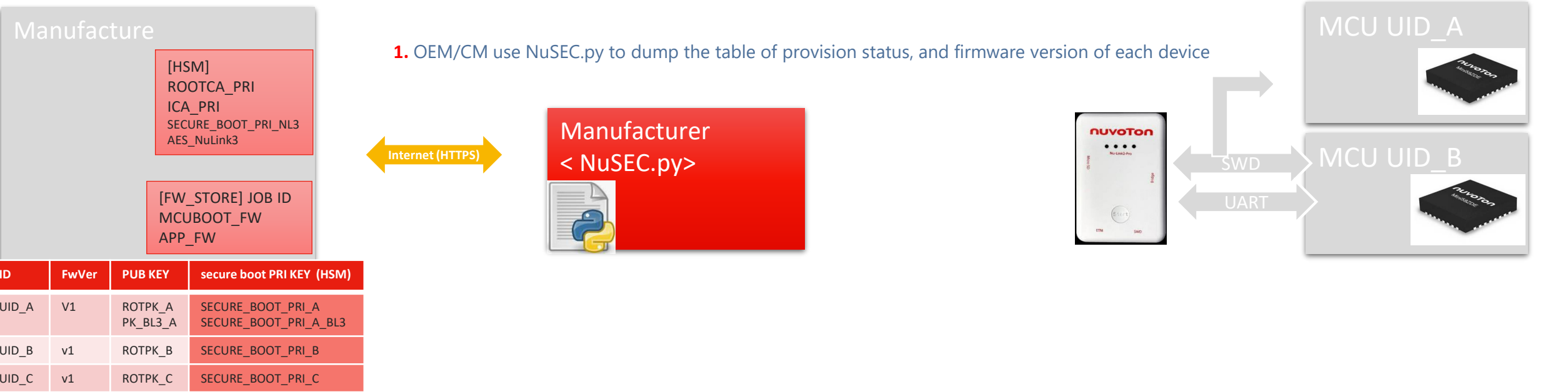


Public key: 512 bits (64B)
Unique ID: 128 bits (16B)
Certificate: 16000 bits (2000bytes)

Firmware attestation - secure boot key and FW install



Status report



Deployment stage



Device authentication

Cloud Server

Gateway

target board

Deployment

[HSM]
ROOTCA_PRI
ICA_PRI
SECURE_BOOT_PRI_NL3
AES_NuLink3

Rest API
server

[FW_STORE] JOB ID
MCUBOOT_FW
APP_FW

Gateway

ROOTCA_CERT
ICA_CERT

DEV_CERT_A
DEV_CERT_B

Chain of trust

UART/I2C/..

Challenge & response authentication (SPDM)

MCU UID_A

AUTH_PRI_A
DEV_CERT_A

RootCA CERT

MCU UID_B

AUTH_PRI_B
DEV_CERT_B

RootCA CERT

HTTPS

Device Certificate (HTTPS)

HTTPS

Device Certificate (HTTPS)

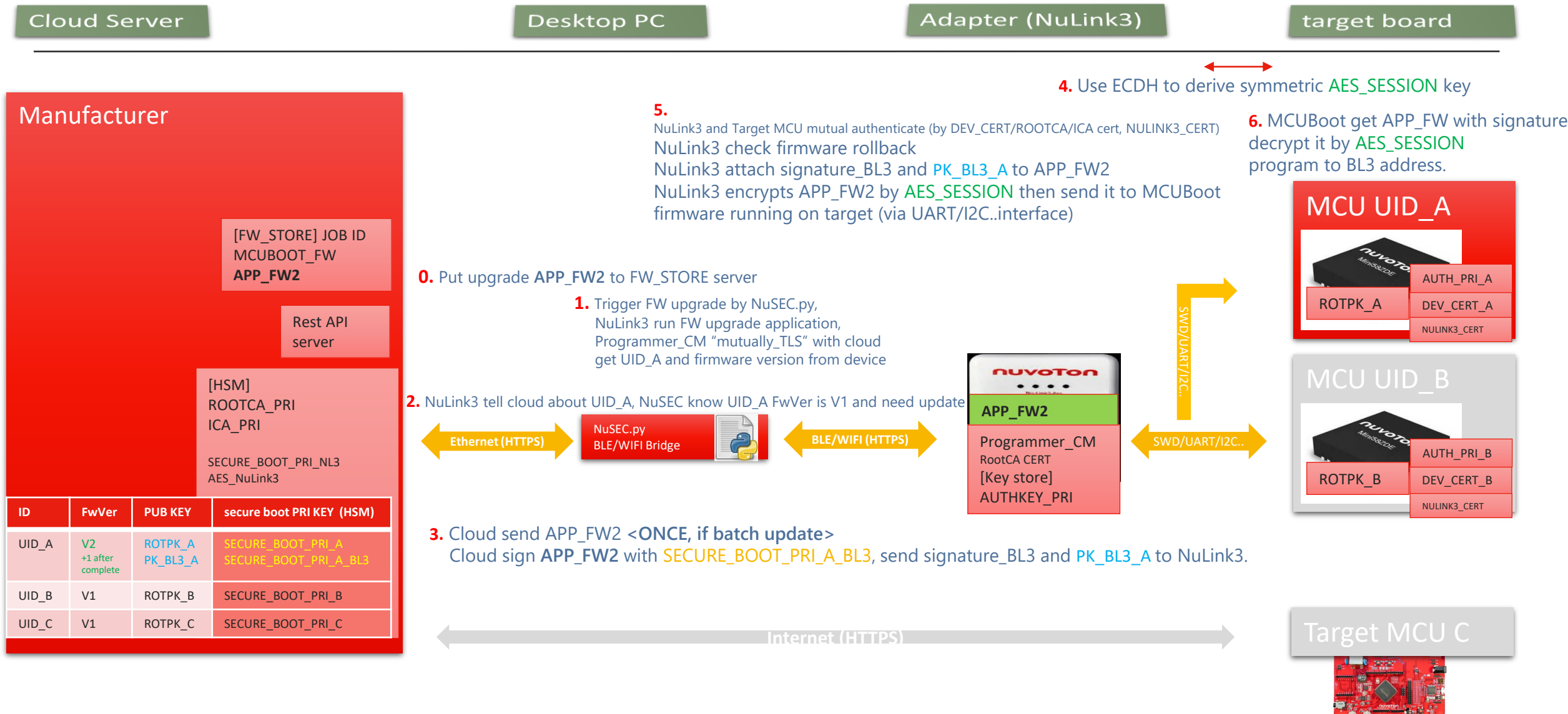
Challenge & response authentication (SPDM)

If devices are online:
Cloud can manage & track the issued,
expired, and revoked certificates

Maintenance stage



Firmware upgrade (NuSEC.py + NuLink3 bridge)



Firmware OTA upgrade (direct)

Cloud Server

Desktop PC

Adapter (NuLink3)

target board

Manufacturer

[FW_STORE] JOB ID
MCUBOOT_FW
APP_FW2

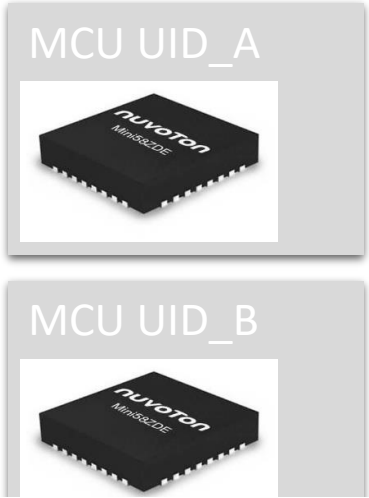
Rest API
server

[HSM]
ROOTCA_PRI
ICA_PRI

SECURE_BOOT_PRI_NL3
AES_NuLink3

ID	PUB KEY	secure boot PRI KEY (HSM)
UID_A	ROTPK_A PK_BL3_A	SECURE_BOOT_PRI_A SECURE_BOOT_PRI_A_BL3
UID_B	ROTPK_B	SECURE_BOOT_PRI_B
UID_C	ROTPK_C	SECURE_BOOT_PRI_C

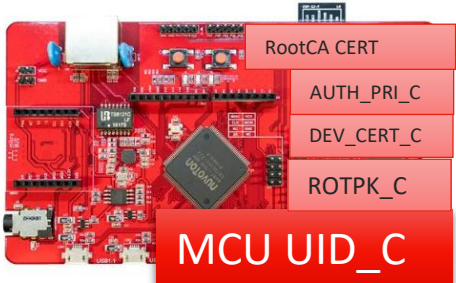
Put upgrade **APP_FW2** to FW_STORE server



MCUBoot get APP_FW with signature,
decrypt it by AES_SESSION
program to BL3 address.



Device and cloud do mutual_TLS and derive AES_SESSION
Cloud prevent firmware rollback
Cloud attach signature_BL3 and PK_BL3_A to APP_FW2
Cloud encrypts APP_FW2 by AES_SESSION then send it to MCUBoot



Decommission



Decommission

Cloud Server

Desktop PC

Adapter (NuLink3)

target board

Manufacturer

[FW_STORE] JOB ID
MCUBOOT_FW
APP_FW2

Rest API
server

[HSM]
ROOTCA_PRI
ICA_PRI

SECURE_BOOT_PRI_NL3
AES_NuLink3

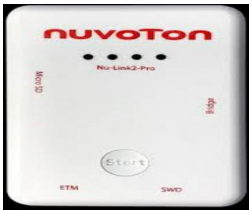
ID	Revoke cert
UID_A	
UID_B	revoked
UID_C	revoked

Decommission device

Internet (HTTPS)

NuSEC.py
BLE/WIFI Bridge

BLE/WIFI



SWD/UART/I2C

UART

MCU UID_A



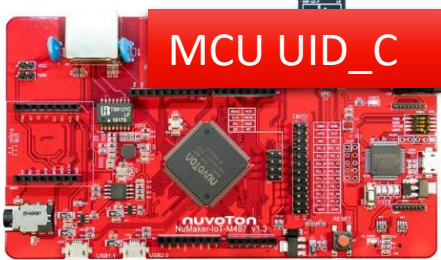
MCU UID_B



HTTPS

Decommission device

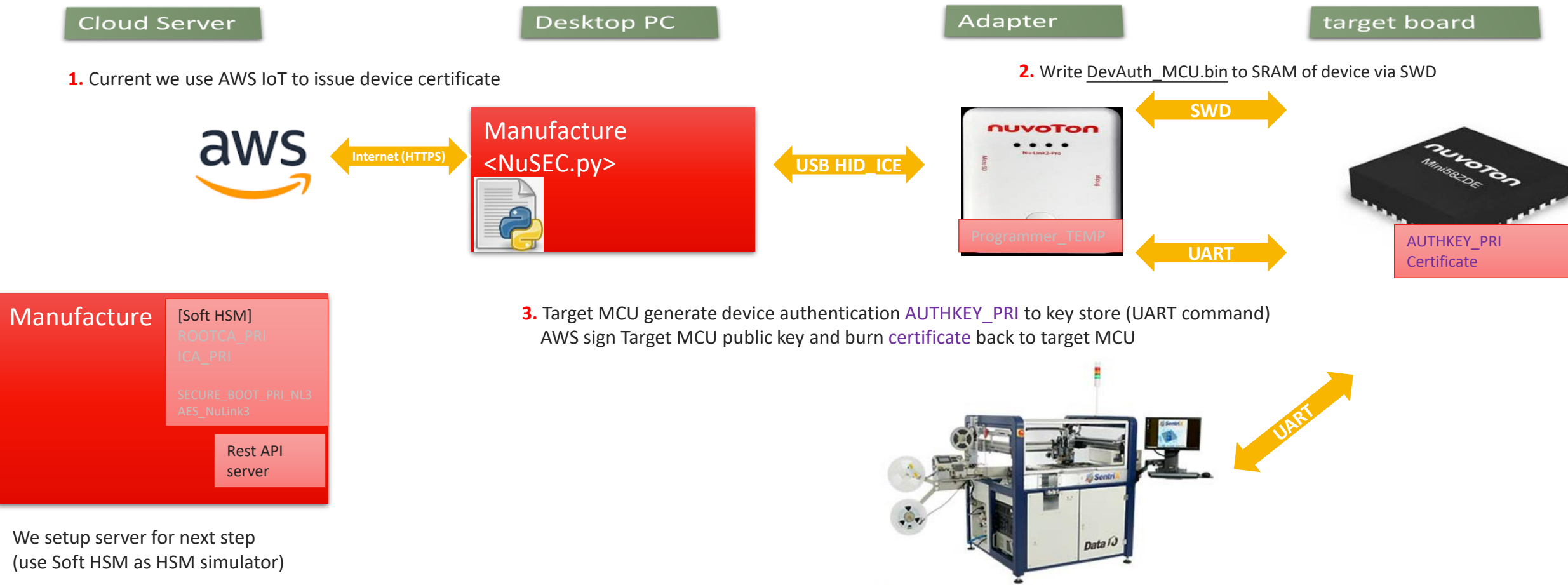
MCU UID_C



Current status



- Current status (Coworking with A008 JY33)
 - Device authentication: AWS <-> NuSEC.py <-> NuLink2 <-> (M2354,KM1M7C)



UART protocol of DevAuth_MCU.bin is standardized.
It can also communicates with other devices. (e.g. DATA IO)

Joy of innovation
nuvoTon

Thank You

Danke

Merci

ありがとう

Gracias

Kiitos

감사합니다

धन्यवाद

كل ارکش

הודות