

Renesas RA Family

Establishing and Protecting Device Identity using SCE9 and Arm® TrustZone®

Introduction

This application note offers a general discussion on IoT security and offers a brief introduction to the security features offered by the Renesas RA Family MCUs with Arm® TrustZone® for Cortex-M technology support, including different key generation options.

The application example provided in this package uses the Secure Crypto Engine 9 (SCE9) module based on RA6M4 to generate a pair of ECC keys and uses a local CA to generate the device certificate based on the ECC public key. The ECC private key and the device certificate establish the MCU device identity which is unique to each MCU. The device private key is stored in data flash in wrapped format and the device certificate is stored in code flash which resides in secure partition of the device.

This application note enables you to effectively use the RA Family SCE9 modules and the Arm Mbed™ OS Crypto middleware in your own design. Upon completion of this guide, you will be able to add the RA Family Flexible Software Package (FSP) Mbed Crypto middleware and the SCE module to your own design, configure them correctly for the target application, and write code using the included application example code as a reference and efficient starting point.

Currently, this RA Family TrustZone® based Device Identity Application is implemented and tested on the EK-RA6M4. The software project can be easily migrated to other MCUs with SCE9 support using the same source code and memory map.

Required Resources

To build and run the RA Family Device Identity Application example, you need the following resources:

Development tools and software

- e² studio IDE v2025-04.1
- RA Family Flexible Software Package (FSP) v6.0.0
- SEGGER J-link® USB driver V8.44a

The above three software components: the FSP, J-Link USB drivers, and e² studio are bundled in a downloadable platform installer available on the FSP webpage at renesas.com/ra/fsp

- Visual Studio 2022 Community Version (<https://visualstudio.microsoft.com/downloads/>)
Only needed if user wants to customize the PC program. It is not needed to run the application project.

Hardware

- EK-RA6M4, Evaluation Kit for RA6M4 MCU Group (<http://www.renesas.com/ra/ek-ra6m4>)
- Test PC running Windows® 10 OS
- Two Micro USB cables

Prerequisites and Intended Audience

This application note assumes you have some experience with the Renesas e² studio IDE and RA Family Flexible Software Package (FSP). Before you perform the procedures in this application note, follow the procedure in the *FSP User Manual* to build and run the Blinky project. Doing so enables you to become familiar with the e² studio and the FSP and validates that the debug connection to your board functions properly. In addition, a prerequisite reading is chapter 3 of application note [Renesas RA Security Design with Arm® TrustZone® – IP Protection](#). The goal of reading this chapter is to understand the two different development models provided by Renesas Tooling for TrustZone® support. Furthermore, this application note assumes that you have some knowledge of cryptography and RA Family SCE9 features.

The intended audience are users who want to develop applications with SCE9 modules using Renesas RA Family MCUs with SCE9 support.

Contents

1. Introduction to IoT Security	3
1.1 Overview	3
1.2 Importance of Device Identity in an IoT Ecosystem	4
2. RA Family MCU Hardware Security Features	4
2.1 Arm® TrustZone®	5
2.2 Secure Crypto Engine 9	5
2.3 Flash Block Protection	5
3. Overview of Key Generation in RA Family MCUs	6
3.1 Key Wrapping	6
3.2 Key Generation in the Device	6
4. Device Identity Design Overview	6
5. Device Identity Application Example	7
5.1 Overview	7
5.2 Software Architecture Overview	7
5.3 Operational Overview	9
5.4 Securely Storing Device Identity	10
5.5 Non-Secure Callable APIs	11
6. Running the Device Identity Application Example	11
6.1 Importing and Building the Embedded Projects	11
6.2 Powering up the Board	16
6.3 Downloading and Verifying the Demonstration	16
6.3.1 Download the Secure Project and the Dummy Non-secure Project	18
6.3.2 Change the MCU Device Lifecycle State to NSECSD	20
6.3.3 Download the Non-Secure Project and Run the Application	21
6.3.4 Run the PC Application to Communicate with the MCU	22
6.4 Customizing the Application Project	23
6.4.1 Customize the PC Application	23
7. References	23
8. Known Issues and Limitations	23
9. Appendix	24
9.1 Glossary	24
10. Website and Support	25
Revision History	26

1. Introduction to IoT Security

This section provides an overview of IoT Security (in general) and covers the different aspects of the security features offered by RA Family MCUs.

1.1 Overview

A typical infrastructure for an operational IoT (Internet of Things) environment consists of the following:

- IoT Devices
- Cloud Server
- Device Management services
- Certificate Authority (CA)

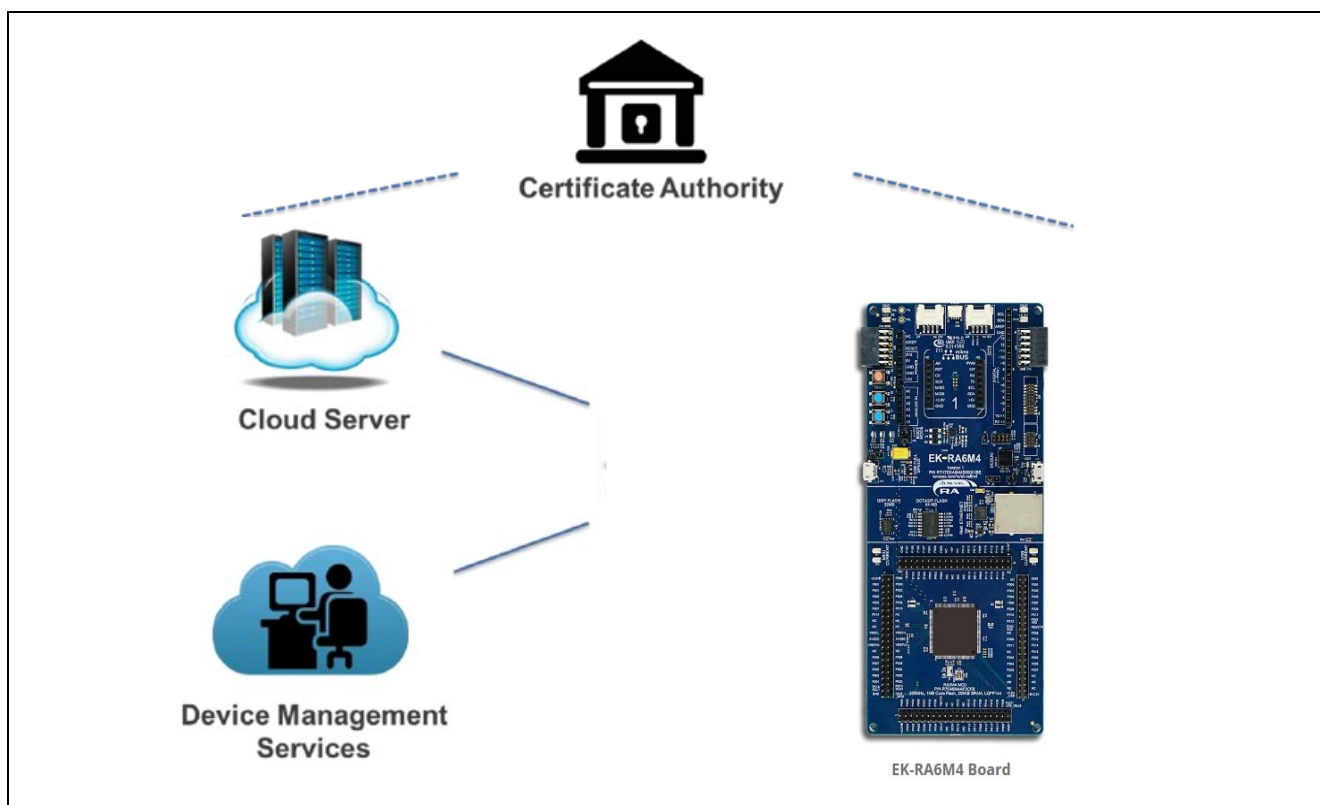


Figure 1. IoT Environment Overview

IoT Devices

An IoT Device is a piece of equipment with the mandatory capabilities of communication and the optional capabilities of sensing, actuation, data capture, data storage, and data processing. IoT devices can be in a secure or non-secure location and without any security safeguard, but all are prone to attack.

Cloud Server

A Cloud Server is a network server for cloud service providing everyday services and access to those devices. It is typically located in a highly secure and controlled data center.

Device Management Services

Device Management services offer a comprehensive suite of capabilities associated with managing and configuring IoT devices. The management service enables IoT customers of any size to have complete control over their devices and data. This includes (but is not limited to):

- Application Security
 - Device management solution that ensures your IoT devices' reliability, longevity, and interoperability in addition to providing trusted and useful data. The security entity used in the application security design includes Cloud Server keys/certificates.
- Device Management Security
 - Manage keys/certificates which identifies each unique IoT Device, which may involve Device key and certificate creation, update, and revocation.
 - Initial firmware deployment and subsequent firmware updates. Firmware contains a signature verifying its authenticity and may be encrypted.

Certificate Authority (CA)

An authorized and trusted entity that issues certificates as a service is commonly referred to as CA. Certificates are used to authenticate public keys and thus the devices that contain those keys. The process by which a certificate is generated for a key is a well-defined process that is part of your security scheme. A Certificate Authority can be public or private. If your devices are managed in a tight ecosystem (for example, devices for industrial settings), the CA will likely be private. If your devices are distributed through a consumer channel where the services and hardware are likely to be provided by different vendors (for example, surveillance cameras, thermostats, home security systems, and so forth), the CA will likely be a public CA.

1.2 Importance of Device Identity in an IoT Ecosystem

With the establishment of a strong device identity, IoT devices can be uniquely identified and authenticated when they are connected to ensure secure and encrypted communication between other devices, services, and users.

Strong IoT security can be achieved by providing the following foundations typically agreed upon by the industry. A well-designed Device Identity is the core to these foundations:

- Trust

When a device connects to the network, it must authenticate and establish trust between other devices, services, and users. Once trust is established, devices, users, and services can securely communicate and exchange encrypted data and information.
- Privacy

As more IoT devices connect, more data is generated, collected, and shared. This data can include personal, sensitive, and financial information that must be kept private and secured – often under regulatory compliance. A device identity can provide authentication and identification when the IoT devices are connected to one another.
- Integrity

Device integrity applies to both the devices and data being transmitted within the IoT ecosystem. The integrity of a device starts with proving it is what it says it is. With a strong unique device identity, it can be ensured that the devices are legitimate – reducing counterfeit products and protecting a company's brand. Data integrity is an often-overlooked requirement, but connected devices and systems rely on the authenticity and reliability of the information being transmitted.

2. RA Family MCU Hardware Security Features

RA Family TrustZone®-enabled MCUs enable hardware root-of-trust mechanisms by providing the ability to protect memory blocks. Using this capability, the protected memory can be accessed only by firmware located in memory regions designated as a secure memory region. These capabilities are provided by the Arm® TrustZone® and Renesas Flash Block Protection hardware feature. The contents of flash memory can be locked from future erase/write events using the Renesas Flash Block Protection. Memory protection features offered by RA Family MCU devices can be used for storing the secure boot code and device certificate/keys amongst other sensitive data which are vital for device identity application.

2.1 Arm® TrustZone®

RA TrustZone®-based MCUs incorporate an IDAU (Implementation Defined Attribution Unit) for TrustZone® region setup. The IDAU is set up prior to any application code execution and offers protection against boot-time attack during over-the-air or in-the-field update. There are 8 IDAU regions available in the RA MCUs with TrustZone® support.

The secure SRAM regions are protected from illegal read and write from non-secure region. The secure flash regions are protected from illegal read from non-secure region. For more detailed information on the TrustZone® IDAU region setup, please refer to the application projects in the reference section.

2.2 Secure Crypto Engine 9

The Secure Crypto Engine 9 (SCE9) is an RA Family MCU hardware peripheral that provides several security features, including NIST certified algorithms and support for cryptographic primitives. In addition, MCUs containing the SCE9 have a Hardware Unique Key (HUK), unique to every individual MCU, which is stored wrapped by the Hardware Root Key and MCU's unique ID. The HUK is never exposed outside SCE9 and will not work on any other MCU. The HUK is used for secure key storage only; it cannot be used for MCU device identity.

The RA Family TrustZone®-enabled MCUs support asymmetric cryptography as well as symmetric cryptography. Following is a diagram of the SCE9 features offered by these MCUs. When keys are generated on the MCU, they are always wrapped by the HUK and will only work on the MCU that generated the keys.

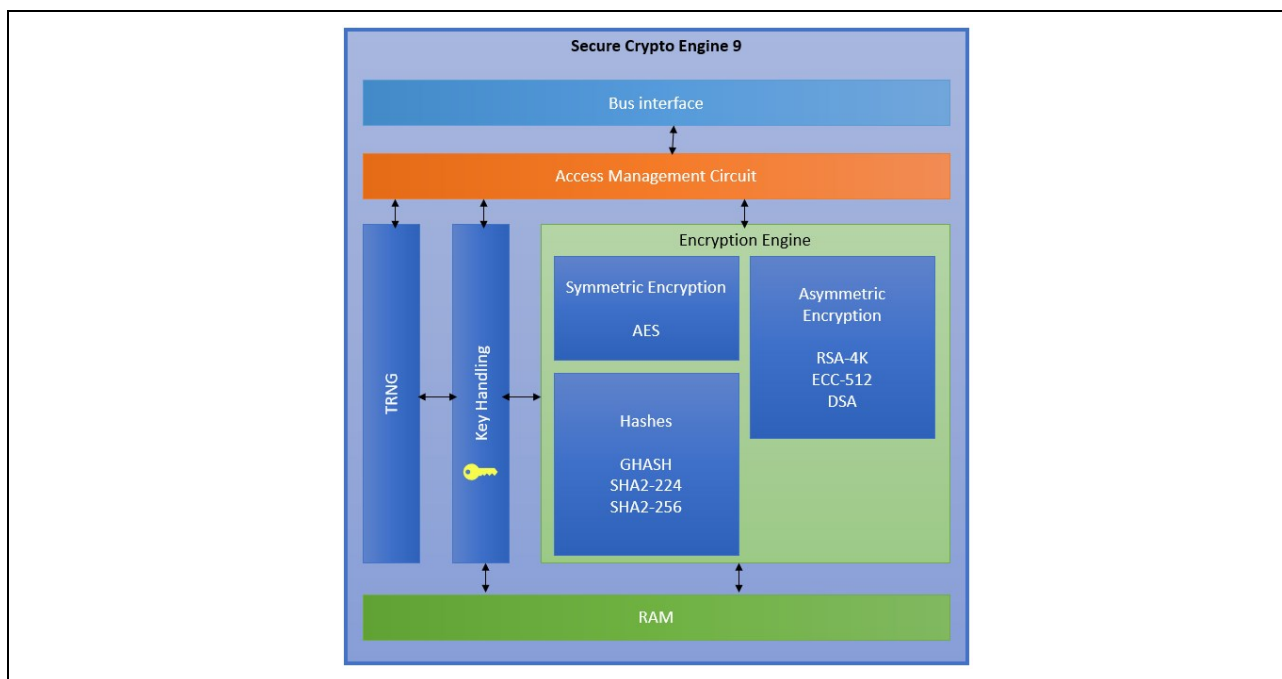


Figure 2. Secure Crypto Engine 9 Features

The SCE9 engine provided by RA Family devices is used by this application project in the following areas:

- Generate ECC key pairs (plaintext public and wrapped private key).
- Sign the challenge string using the ECC private key.

2.3 Flash Block Protection

The RA Family TrustZone®-enabled MCUs can provide temporary and permanent flash block locking for code and data flash Programming and Erasing (P/E) mode entry. The e² studio provides configuration options for a user to selectively prevent the erasure and programming of the intended flash block.

This flash block protection is not directly used in this application project. However, for use cases where the device certificate needs to be permanently locked down in the manufacturing stage, this can be used at compile time to compile the device certificate and operationally lock down the corresponding flash block at compile time to protect the secure code flash region from accidental erasure and reprogramming.

3. Overview of Key Generation in RA Family MCUs

3.1 Key Wrapping

Device keys generated inside the RA Family TrustZone®-enabled MCU using the SCE9 hardware module can only be generated as wrapped keys. Plaintext key can be injected from external sources and stored as wrapped keys in the MCU.

A wrapped key is a key that has been encrypted by the SCE, using a method that involves use of the MCU's HUK. Because this method requires the MCU's HUK to unwrap the key, the key can only be unwrapped by the same MCU that wrapped it. Therefore, key wrapping on RA Family MCUs is considered secure, as a wrapped key can only be used on the RA Family MCU on which it was generated, and it cannot be used outside of that MCU. As a result, the scalability of an attack can be substantially reduced.

Wrapped keys provide the following advantages:

- A wrapped key can only be used on the RA Family MCU on which it was generated.
- It cannot be moved to another RA Family MCU. If moved to another RA Family device, the original key cannot be recovered from the wrapped key and cannot be used with SCE9.

3.2 Key Generation in the Device

Key generation in the device is the common use case where the device-specific key is natively generated inside the RA Family MCU using the SCE module. To generate the device key using the RA Family Flexible Software Package (FSP), the Mbed™ Crypto module is used. The Mbed™ Crypto module implements PSA Crypto APIs which call the Secure Cryptographic Engine (SCE9) HAL module, which in turn drives the SCE IP on the device.

Mbed Crypto Module Features

The following key types can be generated using the services of the Mbed Crypto module using SCE9 hardware:

- RSA 2048-bit, 1024-bit standard format wrapped private keys.
- AES 128-bit, 192-bit and 256-bit wrapped keys for CBC, CTR, CCM, CMAC and GCM chaining modes.
- ECC 192-bit, 256-bit plaintext public keys and wrapped private keys.

This application generates ECC secp256r1 plain-text public key and wrapped private keys.

4. Device Identity Design Overview

This section explains how RA hardware and software features are integrated to create a unique device identity for each device.

Key Generation

The first step in creating a device identity is key generation. The keys can be either generated inside the RA Family MCU or they can be generated outside in a secure facility and injected into the RA device. Each methodology has its pros and cons. The decision must be made based on the customer use case.

Certificate Authority (CA)

Once the device keys are generated/injected, we need an entity that takes the public key from the key pair and issues associated digital certificates. A CA can be either public or private CA located in the cloud or in an on-premises CA (local CA), which would typically be hosted on a secure server.

Securing the Device Identity

Once the device identity is created and programmed on the RA Family device, it must be securely stored to prevent theft or tampering. Depending on what kind of end application the certificate is for, it may provide access to a controlled environment. If the device certificate is stolen, fraudulent access could occur. Therefore, the certificate must be securely stored.

Secure storage of the Device Identity can be achieved by using the Arm® TrustZone® and Renesas Flash Block Protection features offered by the RA Family MCU. These features configure a portion of internal code flash as secure partitions for both code and data.

- Code and data in secure partition are protected from access by non-secure code, non-secure peripheral and non-secure bus master channels (DMAC and DTC) based on Renesas RA Arm® TrustZone®-enabled MCU hardware features. A Secure Fault will be triggered for any violation.
- In addition, Renesas TrustZone®-enabled MCUs provides Device Lifecycle Management capabilities that can be used to disable debugger and serial programming access to the secure partitions.
- Access to secure region services is only possible via exposed non-secure callable API veneers, located in the Non-secure Callable region.
- The device certificate can be stored in the secure partition, which cannot be accessed or modified directly by any non-secure code running on the RA Family MCU.

5. Device Identity Application Example

5.1 Overview

The example application project accompanying this document demonstrates natively generating and storing the device identity information using the on-chip SCE9 modules available with the Renesas RA Family device. For demonstration purposes, this application uses a local Certificate Authority (CA) running on a Windows® PC to generate a signing key and root CA that will be used to sign the device certificate. USB-CDC is used as the primary communication interface between the EK-RA6M4 kit and the host console application running on the Windows PC.

5.2 Software Architecture Overview

The following figure shows the overall software architecture of the RA Family device identity application project. The light green blocks are components from FSP ecosystems: AWS FreeRTOS block is a component from AWS and the other light green background blocks PSA Cryptography API, Mbed™ Crypto lib, and littlefs are components from Arm®.

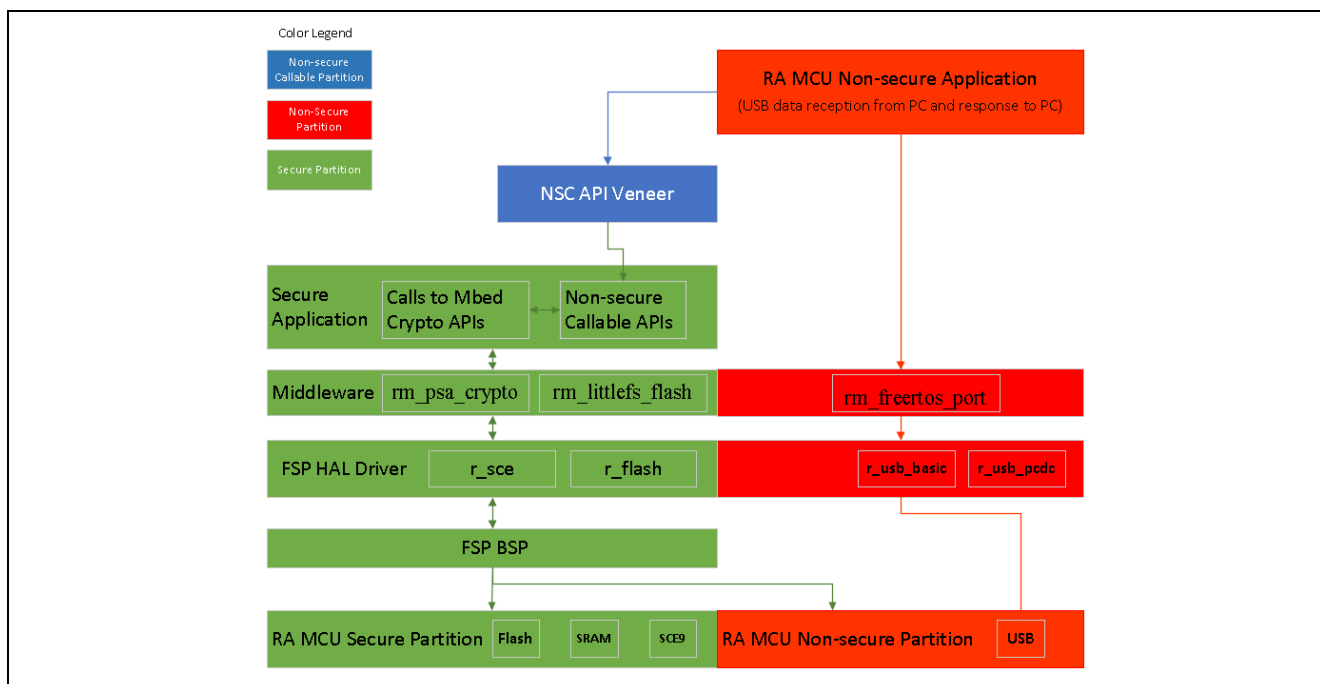


Figure 3. RA Device Identity TrustZone®-based Application Software Architecture

The major FSP software components of this application are:

- rm_psa_crypto and r_sce: for cryptographic operation.
- rm_littlefs_flash and r_flash: for ECC key pair (rm_littlefs) and device identity (r_flash) storage.
- r_usb_pcdc and r_usb_basic: for communication between PC and MCU.
- rm_freertos_port: multithreading framework for scalability.
- The application contains the following thread:
 - Main Thread

Main Thread

This is the main control thread which handles the following functions:

1. Incoming/outgoing USB data from and to PC.
2. Decoding the command and calling the appropriate command handler functions, which in turn handle the corresponding command functionalities.

The following commands are handled by the Main Thread:

- WRAPPED_KEY_REQUEST
- WRAPPED_KEY_CHALLENGE_RESP
- WRAPPED_KEY_CERT_PROGRAM

WRAPPED_KEY_REQUEST

This command is the first command issued from the local CA over USB to request the public key of the device. It is handled by the following API function: `handleWrappedKeyCreation()`.

This function handles the key generation using FSP Crypto modules. This application supports ECC Key pair generation. Once the key pair is generated, the plaintext public key is sent to the host application to be used for the device certificate generation.

The wrapped private key is stored internally in the data flash and will later be used for signing the challenge response.

WRAPPED_KEY_CHALLENGE_RESP

This command is issued after the PC-hosted local CA has received the device's public key. It is handled by the following API function: `handleCertChallengeResp()`.

The intention of this challenge request is to allow the target to prove its ownership of the device private key for the corresponding public key being certified.

This function handles the challenge response request sent by the host application. Once it receives the request, it signs the string sent as part of the request using the private key generated as part of WRAPPED_KEY_REQUEST command. The signed string is sent back to the host application for verification. Once the host application receives the signed string, it verifies the signature using the device public key extracted from the device certificate. When the signature validation is successful, the host application will send the device certificate to the device to be stored securely using Arm® TrustZone® and Flash Block Protection hardware feature.

WRAPPED_KEY_CERT_PROGRAM

This command is issued from the PC after successful challenge and response process between the PC and MCU. It is handled by the following API function: `handleCertProgram()`.

This function handles programming the device certificate received from the host application into the secure region of the internal code flash.

5.3 Operational Overview

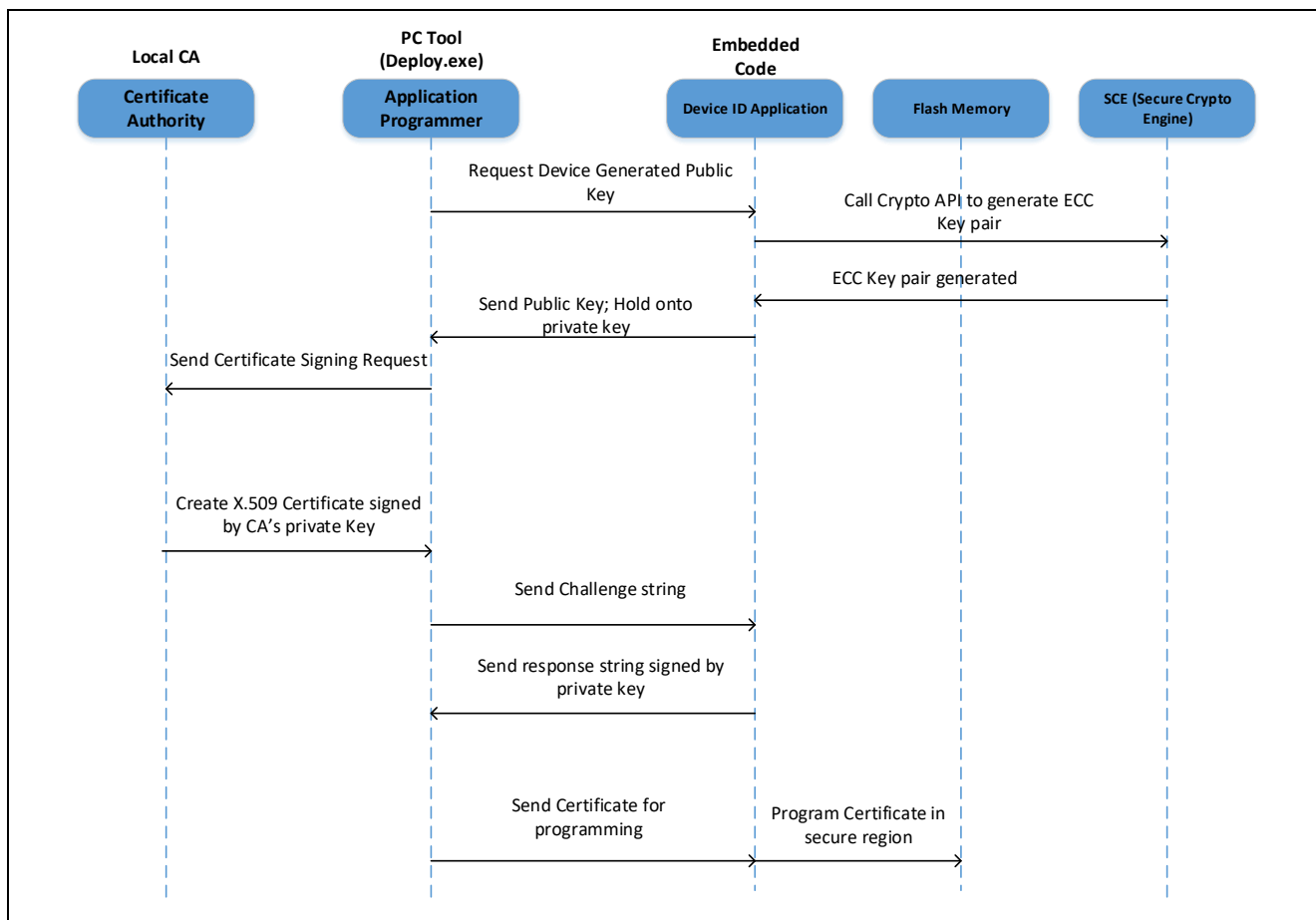


Figure 4. Operational Overview

This application project consists of two software projects:

- Embedded project running on the EK-RA6M4 kit.
- Host application running on Windows® 10 PC.

When power is supplied to the EK-RA6M4 kit, the firmware initializes the MCU and the underlying USB CDC stack that is used for communication with the host application running on the Windows PC. At end of initialization, the firmware waits for the USB device connect event. Once the user connects the kit to the Windows PC through a USB cable, the USB enumeration process occurs, and the USB CDC instance is created. At this stage, the firmware is waiting for the commands from the host application.

When the user runs the host utility on the Windows PC, it scans the available COM ports and opens the port to which the EK-RA6M4 kit is connected. Once the COM port is opened successfully, it generates a signing key and root CA certificate that will later be used to sign the device certificate. Now, the host application generates the WRAPPED_KEY_REQUEST command and sends it to the kit. On receiving this request, the embedded code running on the target kit generates device key pairs and sends out the public key to the host application. On the host application, it receives the public key from the device and generates a device certificate (signed by CA's signing key).

Before issuing the device certificate, the host application issues a challenge string to the device to prove that the device owns the private key. The embedded software, on receiving the challenge string, signs it using its private key and sends it back to the host application. The host application validates the signature using the device public key and if the validation is successful, the device certificate will be sent to the EK-RA6M4 kit to be securely stored using the Arm® TrustZone® and Renesas Flash Block Protection hardware feature.

5.4 Securely Storing Device Identity

The two pieces of information used to establish device identity and created as part of this application are as follows:

- Wrapped ECC private key
- Device certificate

These two pieces of information need to be securely stored inside the RA Family MCU using the Arm® TrustZone® and Renesas Flash Block Protection hardware features to avoid being accessed and modified. The private key generated as part of this application is already wrapped, so this example skips the step to securely store the device private key. However, in some cases, users may prefer to also store the wrapped key in a secure location to avoid it being misused in the device. This can be done using the same steps used to store the device certificate.

The following is the memory map of the current device identity application project.

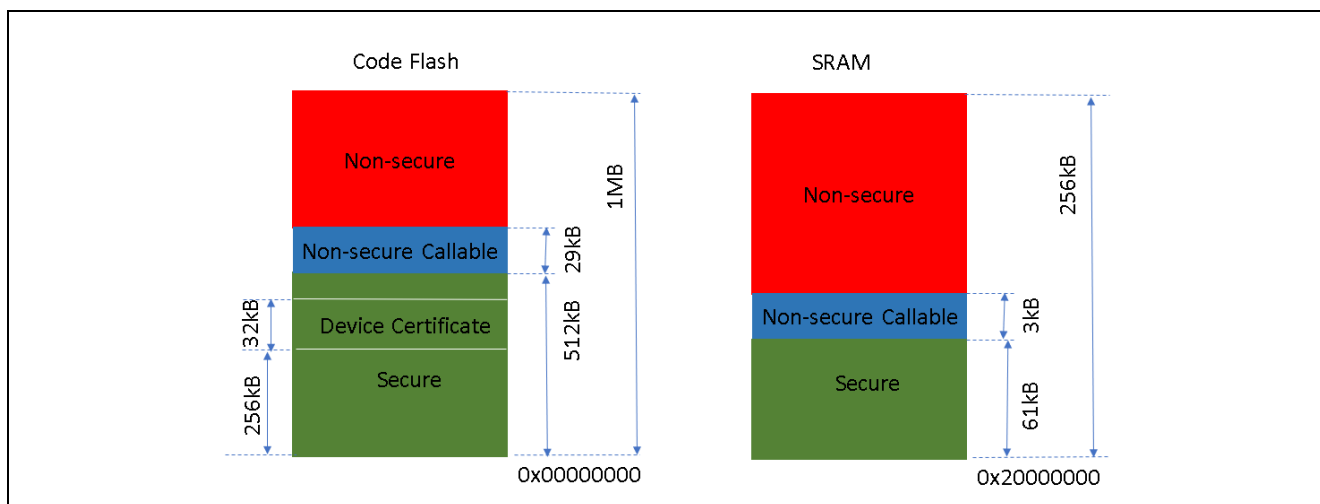


Figure 5. Memory Map used in the Application Project

The left side of Figure 5 shows the memory layout of the code flash in this application project. The right side of Figure 5 shows the memory layout of the SRAM in this application project.

The MCU operates in secure mode when executing code in the secure region or non-secure callable region. The Device Certificate is programmed in the flash block from 256 kB to 288 kB. The MCU operates in non-secure mode when executing code in the non-secure region. When executing in non-secure mode, the system cannot access information in the secure region.

The IDAU registers are set up such that the Mbed™ Crypto middleware and the LittleFS middleware are located in the TrustZone® secure partition as shown in Figure 4. Therefore, the Mbed™ Crypto module code which accesses the keys are protected from direct access from the non-secure partition. In addition, the FSP flash driver module (`r_flash_hp`) is mapped to the bottom portion of the secure SRAM (0x20000000). This protects the non-secure code from copying the flash routines for illegal flash operations.

Regarding the TrustZone® IDAU register setup, the e² studio automatically calculates the register setup after compiling the secure project. The IDAU registers are set up when the e² studio programs the MCU. Following is the summary of the setup for this application project displayed in the Debug Console when the e² studio programs the MCU.

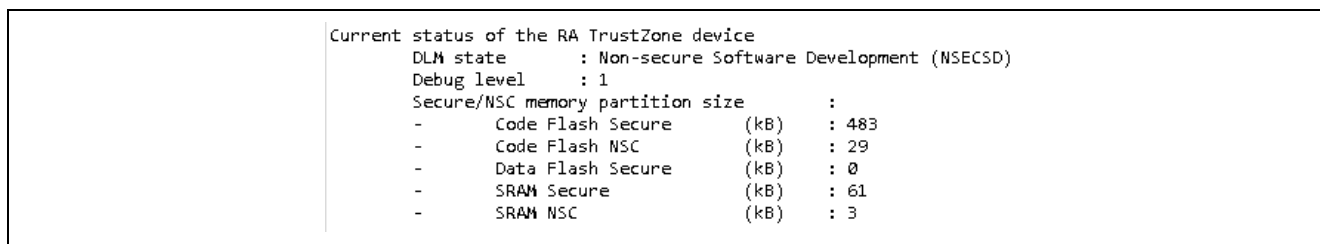


Figure 6. IDAU Setup

5.5 Non-Secure Callable APIs

There are two non-secure callable APIs that the non-secure code can call and activate the corresponding secure partition operations.

- The first non-secure callable receives one byte from the non-secure region and parses the received byte. Refer to `\embeddedCommon/src/framedProtocolTarget.c` for the definition of this function.

```
/* Handle a received byte of serial data */
BSP_CMSE_NONSECURE_ENTRY void fpReceiveByte(const uint8_t byte);
```
- The second non-secure callable returns secure region responses to non-secure region.

```
/* Provide response to Non-secure region */
BSP_CMSE_NONSECURE_ENTRY void share_with_ns(uint8_t *pBuffer, uint16_t *numBytes);
```

6. Running the Device Identity Application Example

6.1 Importing and Building the Embedded Projects

The embedded projects are included in the folder

`Establishing_and_Protecting_Device_Identity_using_SCE9_and_Arm_TrustZone\embedded`. The following instructions will show the user how to import these projects in their e² studio workspace.

First, open a new work space at

`\Establishing_and_Protecting_Device_Identity_using_SCE9_and_Arm_TrustZone`.

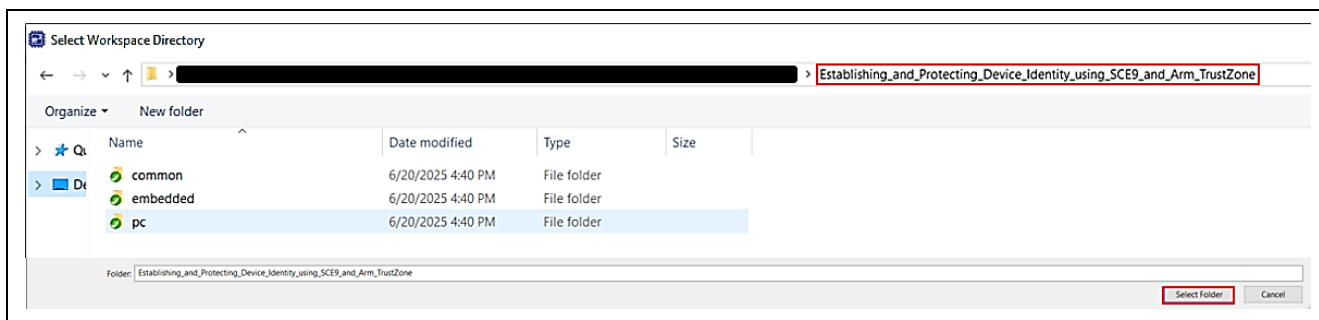


Figure 7. Open a new workspace

In the e² studio IDE, select **File -> Import... -> Existing Projects into Workspace**.

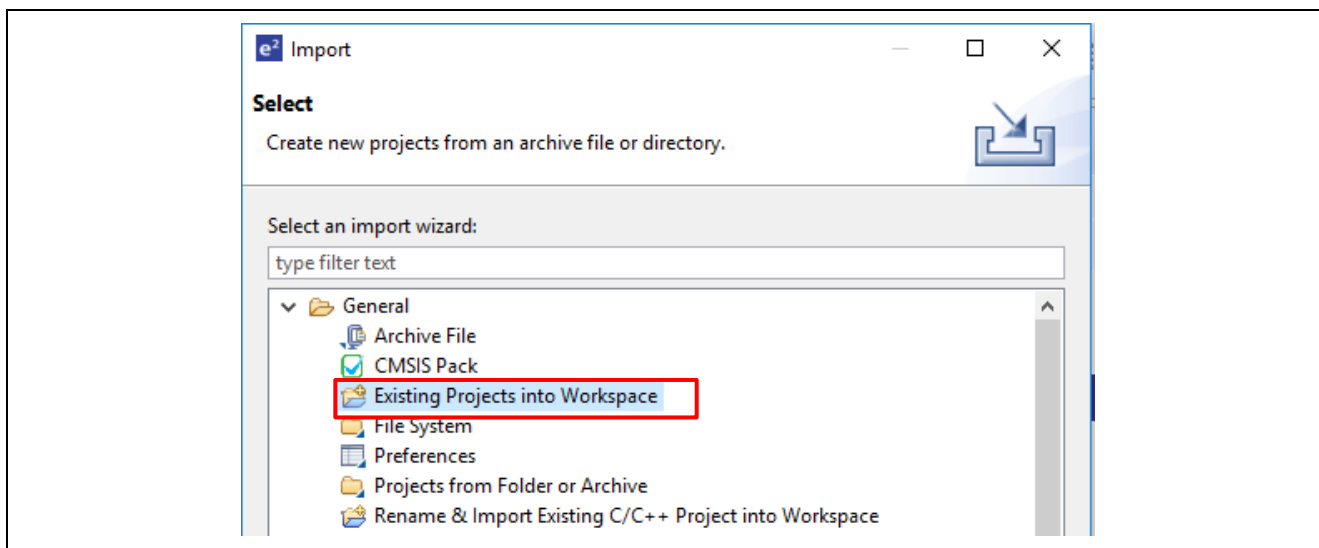


Figure 8. Choose to import “Existing Projects”

Browse to the folder shown in the **Select Root Directory** section:

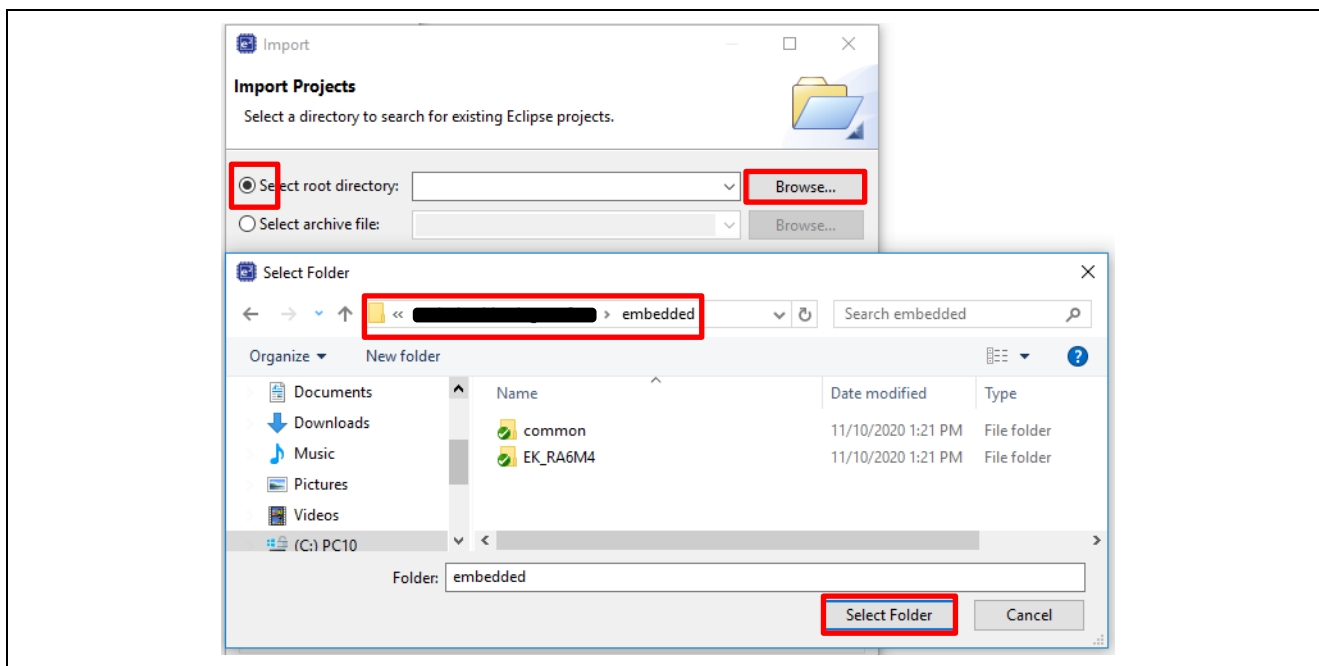


Figure 9. Select the “root directory”

DO NOT CHECK the “Copy projects into workspace” box. Import all projects as shown in the following figure.

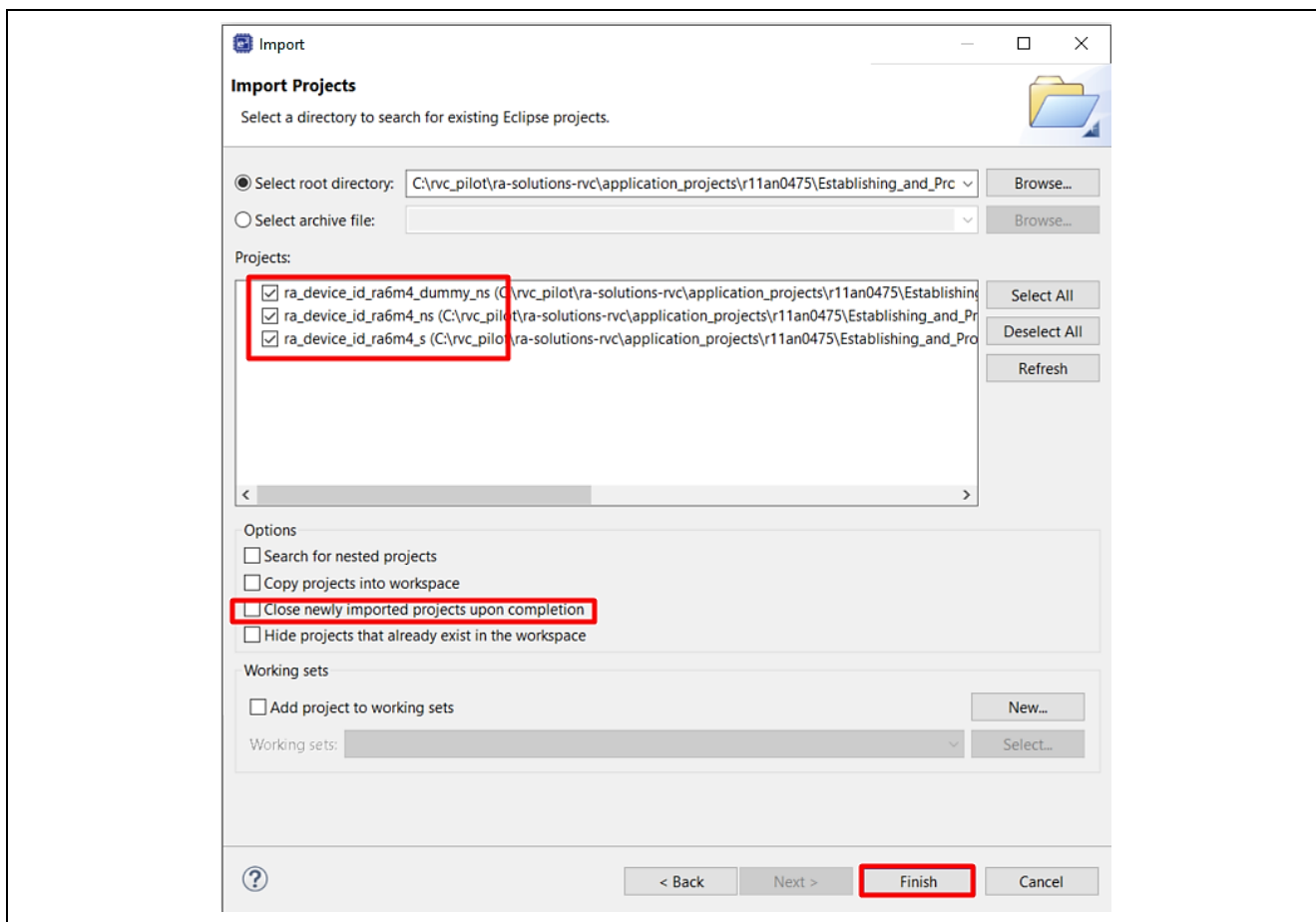


Figure 10. Selection for Importing the Embedded Project

There are three projects under the `\embedded\RA6M4` folder. The dummy non-secure project `ra_device_id_ra6m4_dummy_ns` is needed for a split project development model. In a split project development model, the secure project `ra_device_id_ra6m4_s` and the non-secure dummy project `ra_device_id_ra6m4_dummy_ns` are developed by the secure project development team, which is a different development team from the team that develops the non-secure project `ra_device_id_ra6m4_ns`. In addition, the secure project and a dummy non-secure project (whose linkage to the secure project is established with the Combined Development model) must be downloaded first before changing the MCU device lifecycle to NSECSD.

Follow the steps below to compile and download the application to the MCU. For more information on the definition of Split Project Development and Combined Project Development model, reference application project [Renesas RA Security Design with Arm® TrustZone® – IP Protection](#).

After importing the project, follow the steps below in sequence to compile the projects:

1. Expand project `ra_device_id_ra6m4_s` and double click `configuration.xml`. Once the RA configurator is opened, click **Generate Project Content** and then compile the project. It takes 1-2 minutes to compile the project. There are warnings from third-party software components.
2. Expand project `ra_device_id_ra6m4_dummy_ns` and double click `configuration.xml`. Once the RA configurator is opened, click **Generate Project Content** and then compile the project.
3. For the project `ra_device_id_ra6m4_ns`, follow the two steps below to compile the project:

- A. Update the matching secure bundle based on current project folder location. The secure bundle is linked as an absolute path. Right click on **ra_device_id_ra6m4_ns** project and select **Properties** as shown in Figure 11.

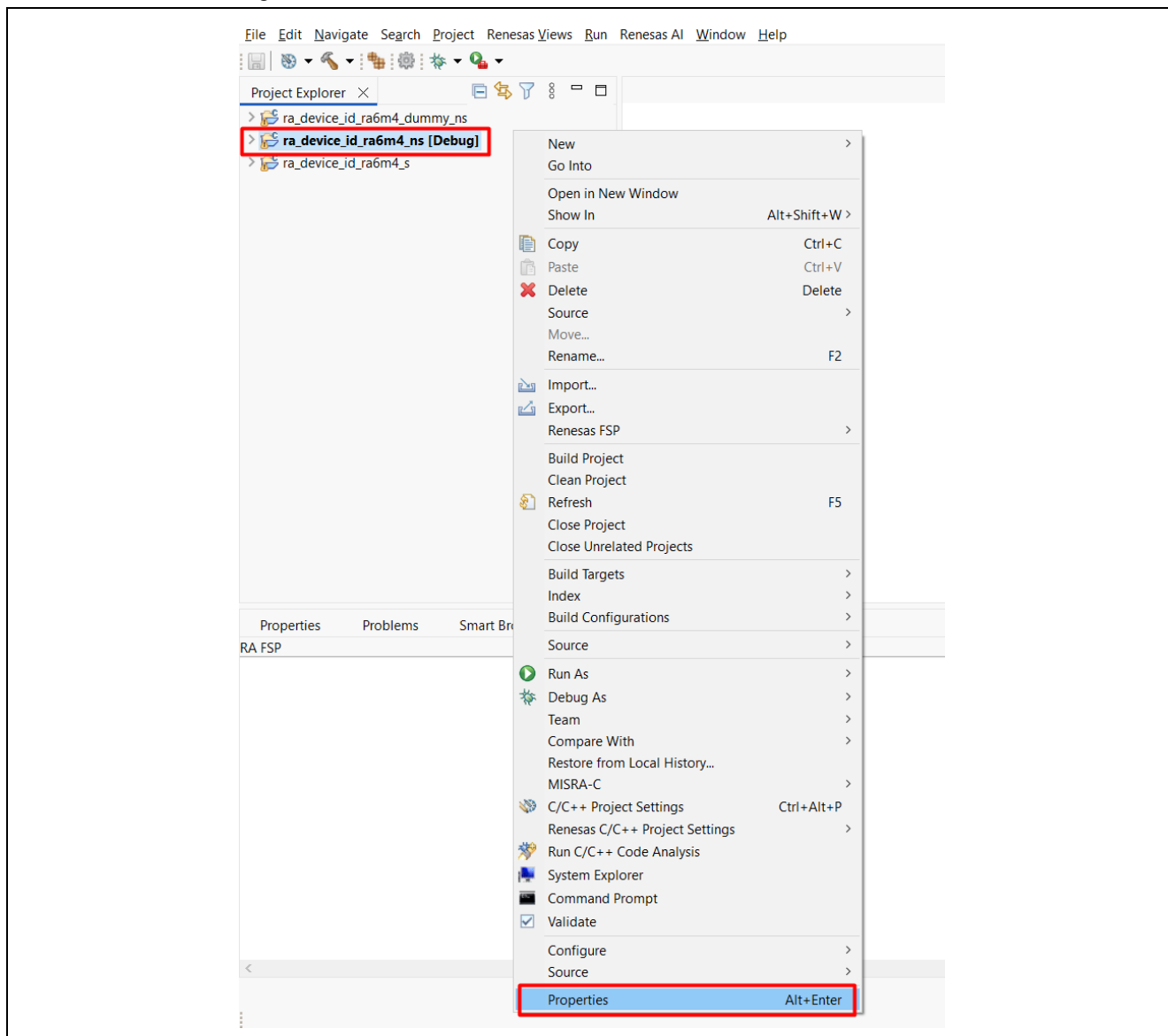


Figure 11. Open the Properties Menu

Navigate to the **Build Variables** configuration for **SecureBundle**.

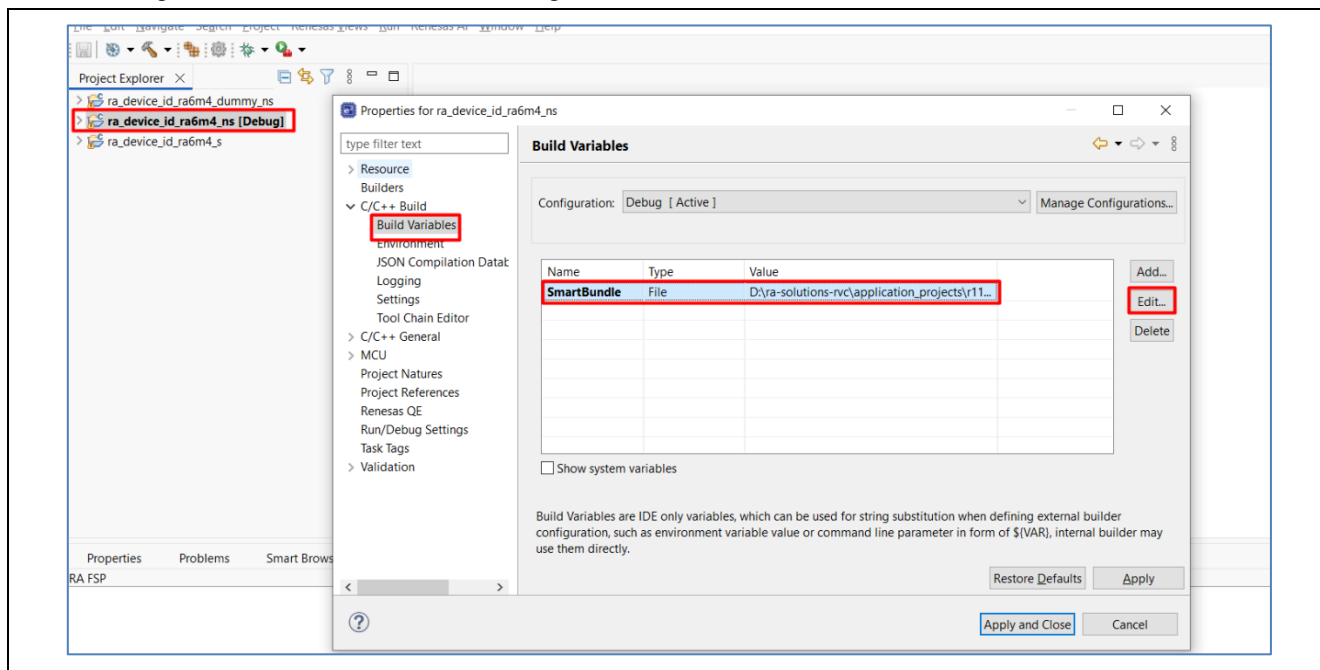


Figure 12. Edit the Build Variable “SecureBundle”

Next, click **Browse**, navigate to the folder where the **ra_device_id_ra6m4_s** project is located, then select **ra_device_id_ra6m4_s\Debug\ra_device_id_ra6m4_s.sbd**. Click **OK**.

Note: For the Split project development model, the non-secure project is linked to the secure project through the secure bundle file. The non-secure developer does not have access to the secure project source code. In a real-world use case, the **.sbd** file may be stored in any development folder. The user needs to manually select the secure bundle file.

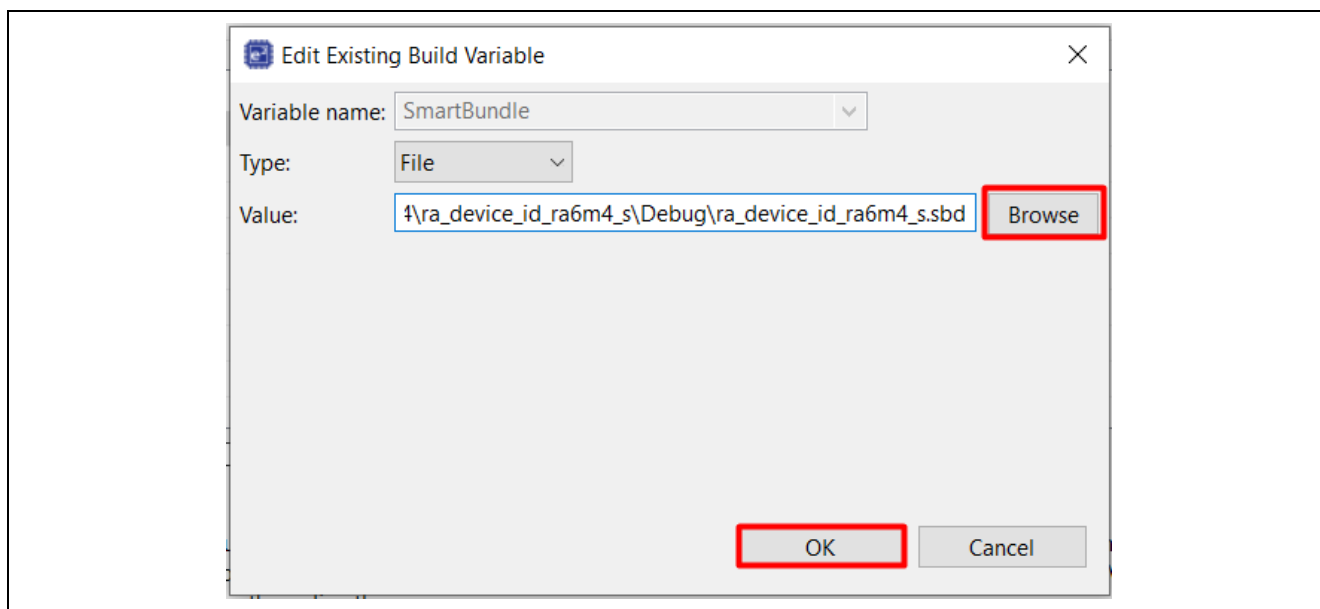


Figure 13. Select the Secure Bundle

Click **Apply and Close**.

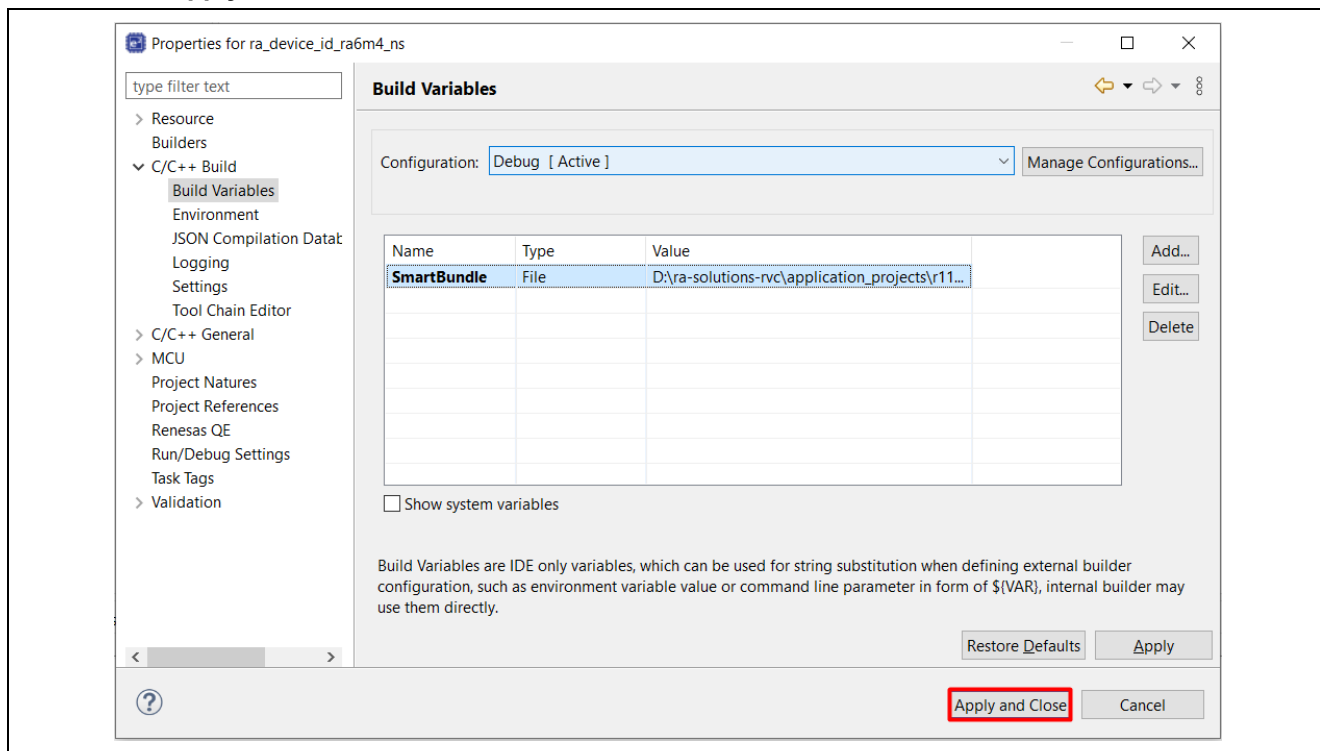


Figure 14. Finish Updating the Secure Bundle Linkage for the Non-secure Project

- B. Expand project `ra_device_id_ra6m4_ns` and double click `configuration.xml`. Once the RA configurator is opened, click **Generate Project Content** and then compile the project.

6.2 Powering up the Board

Follow the steps below to set up the hardware and jumpers to prepare debugging the system using the J-Link debugger:

- EK-RA6M4 jumper setting: J6 closed, J9 open. Other jumpers keep out-of-box setting.
- Connect J10 on EK-RA6M4 using a micro USB cable to the workstation to provide power and debugging capability using the on-board debugger.
- Connect J11 on EK-RA6M4 using a micro USB cable to the workstation to provide USB connection.

6.3 Downloading and Verifying the Demonstration

Once the projects are compiled and the EK-RA6M4 is connected to the development PC. We can follow below steps to download the projects.

Note: We advise that you read the Split Project Development Model explanation in chapter 3.2 Split Project Development in application note [Renesas RA Security Design with Arm TrustZone® – IP Protection](#) to understand why a dummy non-secure project (developed with Combined Project development model) needs to be downloaded with the secure project first.

Prior to downloading the application projects, it is recommended to check on the current Device Lifecycle State of the MCU. This can be achieved by using the Renesas Device Partition Manager which is integrated in e² studio.

Power cycle the board prior to working with the Renesas Device Partition Manager after a debug session if using J-Link as the connection interface. This is needed to transition to MCU Boot mode, so the Renesas Device Partition Manager can take control of the device via the SCI interface. For details on the hardware connections, please see section IDAU Registers in the FSP User's Manual.

1. Open the Renesas Device Partition Manager.

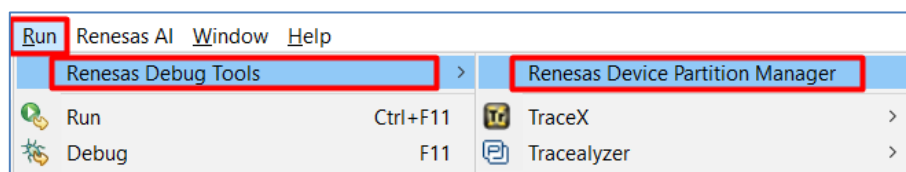


Figure 15. Open Renesas Device Partition Manager

2. Next, select **Read current device information** and click **Run**. If the device lifecycle is read as NSECSD or DPL, then you need to follow section **Initialize the MCU** to perform the initialization. **Initialize the MCU**

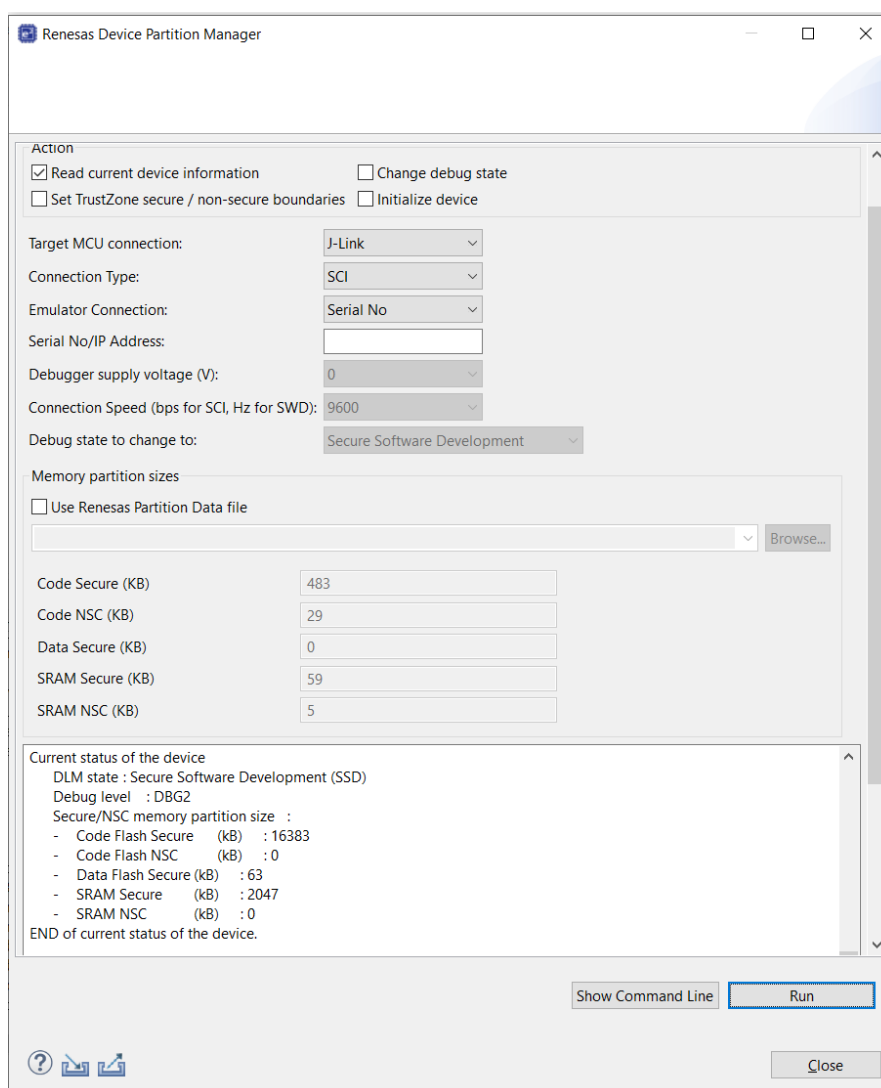


Figure 16. View the Current Device Lifecycle State

3. Initialize the MCU

This step is needed if the Device Lifecycle State is read as NSECSD or DPL. This step MUST be done after running the Device Identity projects included in this application project prior to running any other TrustZone® based application because the Device Lifecycle State will be in NSECSD after getting the project up and running.

Note: Flash content not permanently locked down will be erased during this process. This is particularly helpful if the device was previously used in NSECSD state or has certain flash block locked up temporarily.

Select **Initialize device back to factory default**, choose **J-Link** as the connection method and then click **Run**.

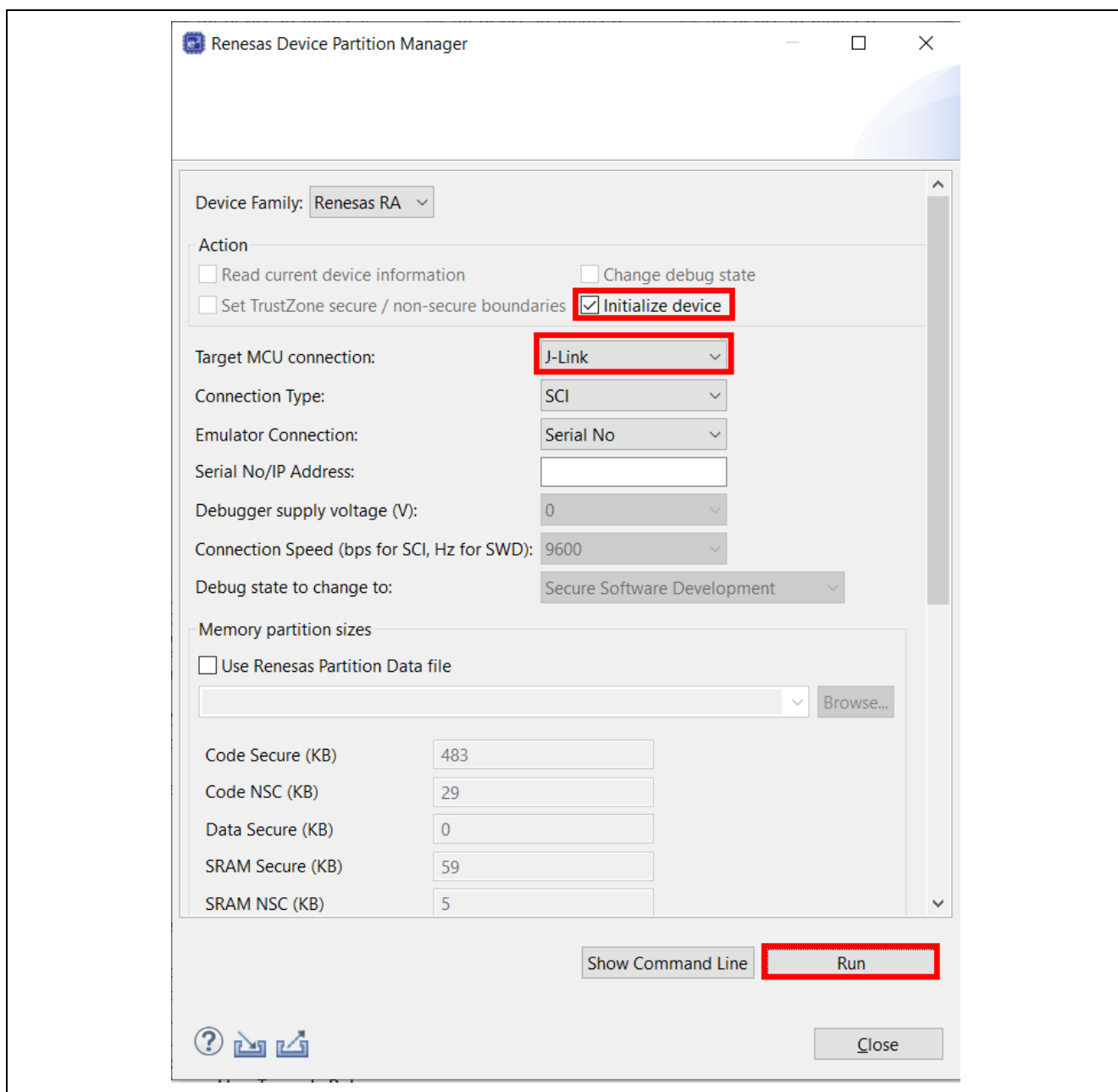


Figure 17. Initialize RA6M4 using Renesas Device Partition Manager

Power cycle the EK-RA6M4 after successfully initializing the device to SSD state by disconnecting both USB cable and reconnecting them to the development PC.

6.3.1 Download the Secure Project and the Dummy Non-secure Project

The dummy non-secure project is developed with the Combined Project Development Mode with the following features.

- It is debugged in the SSD state.
- It performs no real functionality (only while loop).
- It is used to create the conditions to allow debugging of the real Non-Secure Project (which is created with the Split Project Development model and can only be debugged under NSECSD state).

After the power recycle, right click on `ra_device_id_ra6m4_dummy_ns`, and select **Renesas GDB Hardware Debugging**.

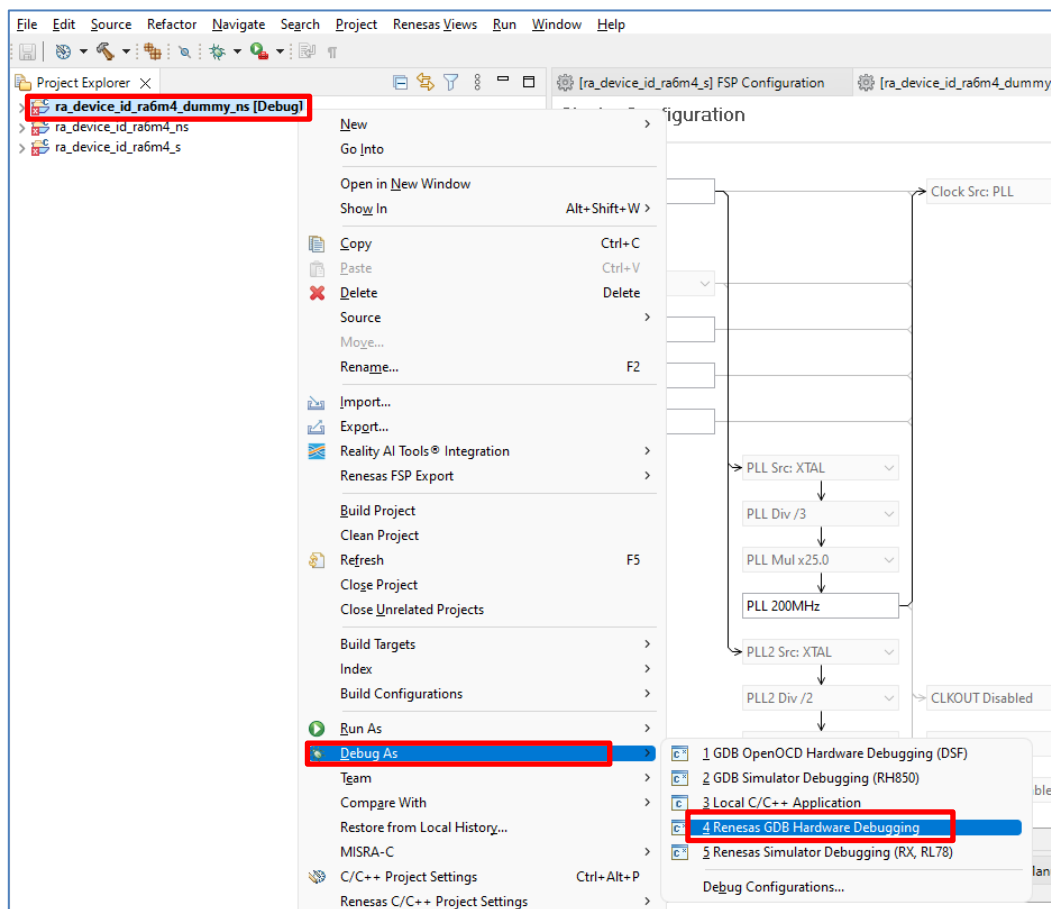


Figure 18. Download the Secure Project and Non-secure Dummy Projects

Click **Switch** if the following window pops up. Then click Resume  twice to run the project. At this point, the secure image and the dummy non-secure image are both downloaded.

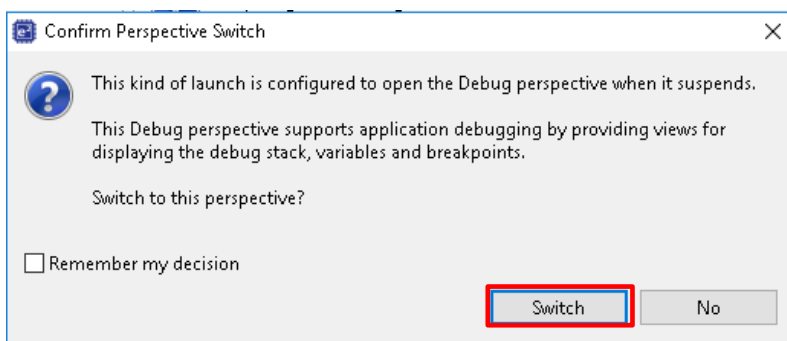
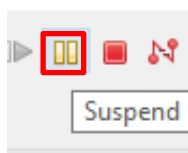
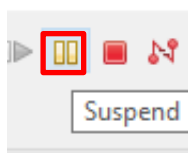


Figure 19. Select Switch to Debug perspective



Click Suspend button . The execution should be pointing to the `while (true);` loop in the dummy non-secure project. Click Stop/Terminate  to end the debug session.

6.3.2 Change the MCU Device Lifecycle State to NSECSD

Prior to this step, the MCU is running in SSD state where both secure and non-secure regions can be debugged. For security consideration, the MCU state can be transitioned to NSECSD state so only Non-secure regions can be debugged. For more understanding on the Device Lifecycle Management, please reference application note [Renesas Device Lifecycle Management Key Installation](#).

To change the Device Lifecycle State during development, we can use Renesas Device Partition Manager which is integrated with e² studio.

Power cycle the board prior to working with the Renesas Device Partition Manager after a debug session when using J-Link as connection interface. This is needed to transition to MCU Boot mode, so the Renesas Device Partition Manager can take control of the device via the SCI interface. For details on the hardware connections please reference section IDAU Registers in the FSP User's Manual.

Disconnect both USB cables from the development PC and then reconnect them to the PC.

Navigate to the **Run** tab in e² studio and select **Renesas Device Partition Manager**. Once the Renesas Device Partition Manager is opened, make the selections shown in Figure 20 and then click **Run**.

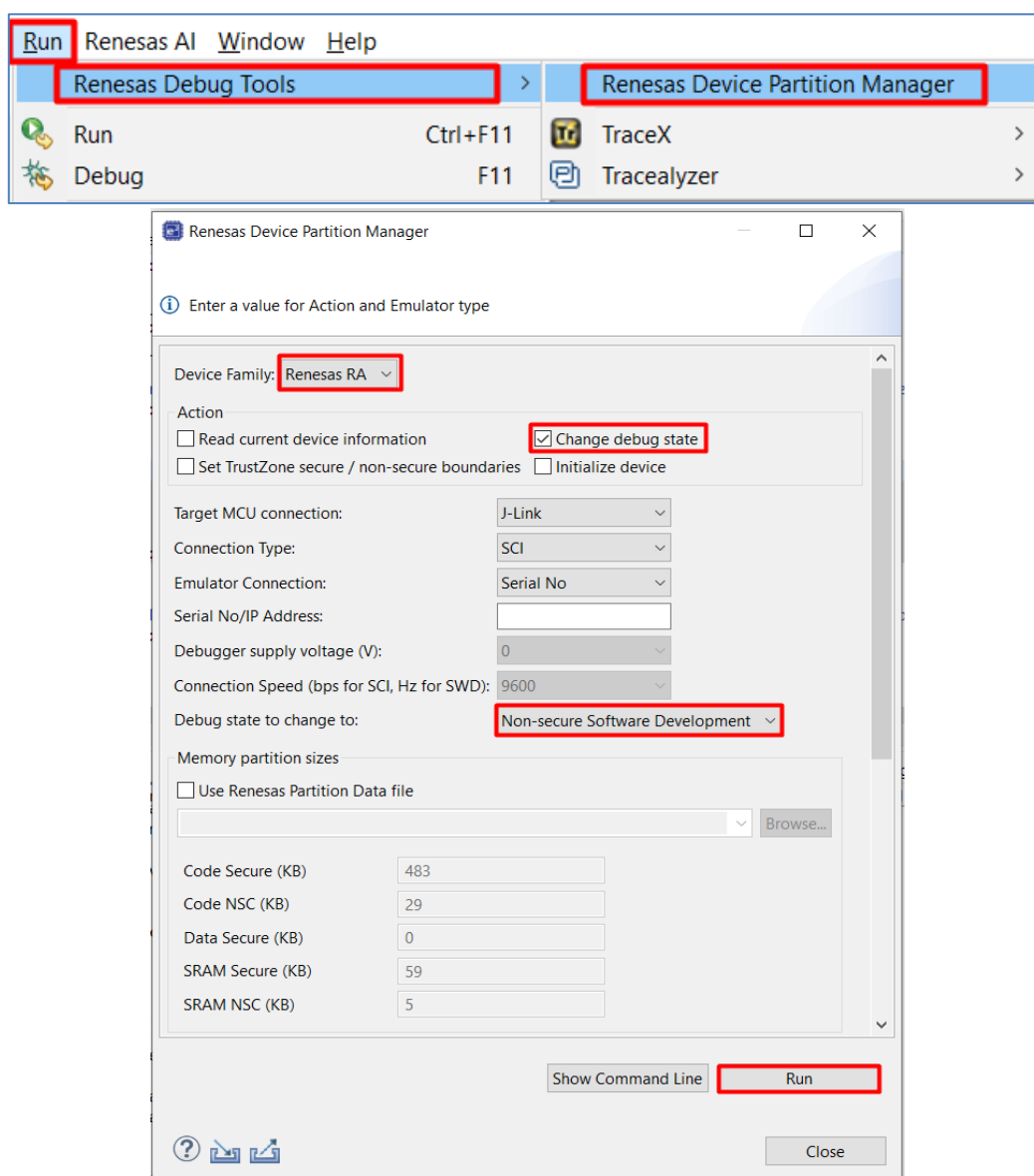


Figure 20. Open the Renesas Device Partition Manager

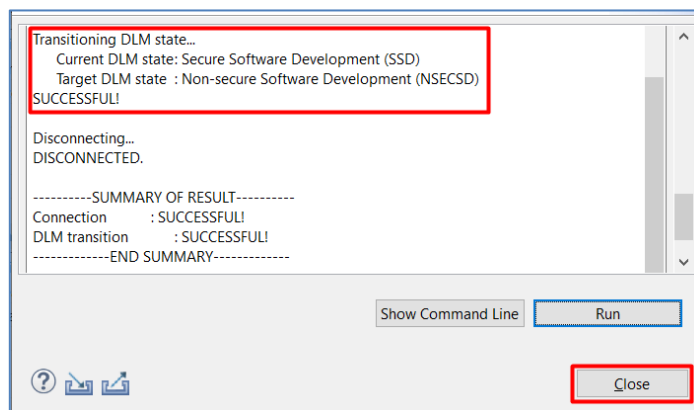


Figure 21. Successfully Transitioned to NSECS

Click **Close** to close the Renesas Device Partition Manager.

6.3.3 Download the Non-Secure Project and Run the Application

Right click on project `ra_device_id_ra6m4_ns` and select **Renesas GDB Hardware Debugging**. Note that this download will not touch the secure project content previously downloaded, but this Non-Secure project will overwrite the previously downloaded Dummy Non-Secure project. When the MCU starts execution, the secure project will transition to non-secure execution to this non-secure project which is being downloaded in this step.

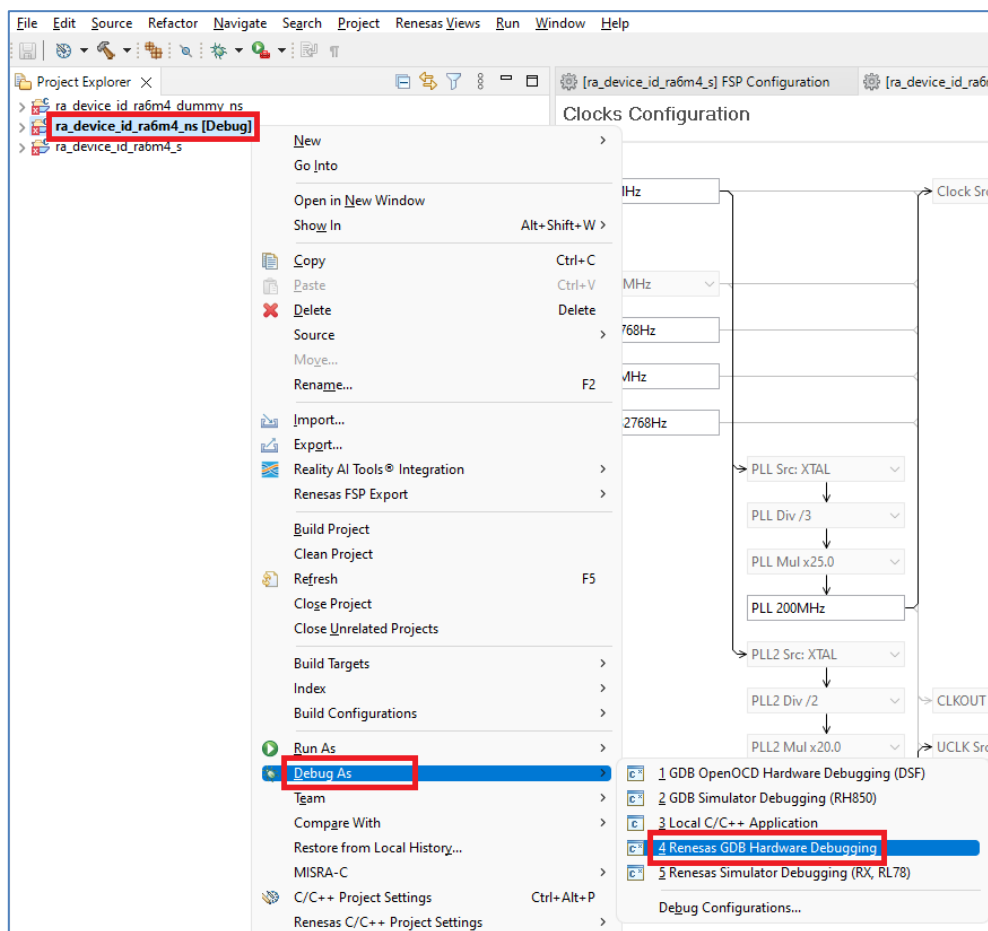


Figure 22. Debug the Non-secure Project with Secure Project Already Downloaded

Click Resume  twice to run the project.

6.3.4 Run the PC Application to Communicate with the MCU

To run the PC application, open the command window in your Windows PC and navigate to the folder where this application project is stored. The `deploy.exe` file will be located under the `Establishing_and_Protecting_Device_Identity_using_SCE9_and_Arm_TrustZone\pc\apps\deploy\Release` directory.

Before running the host application, open **Device Manager**, expand the **Ports (COM & LPT)** section, and identify the COM port number of your connected device, as shown in Figure 23.

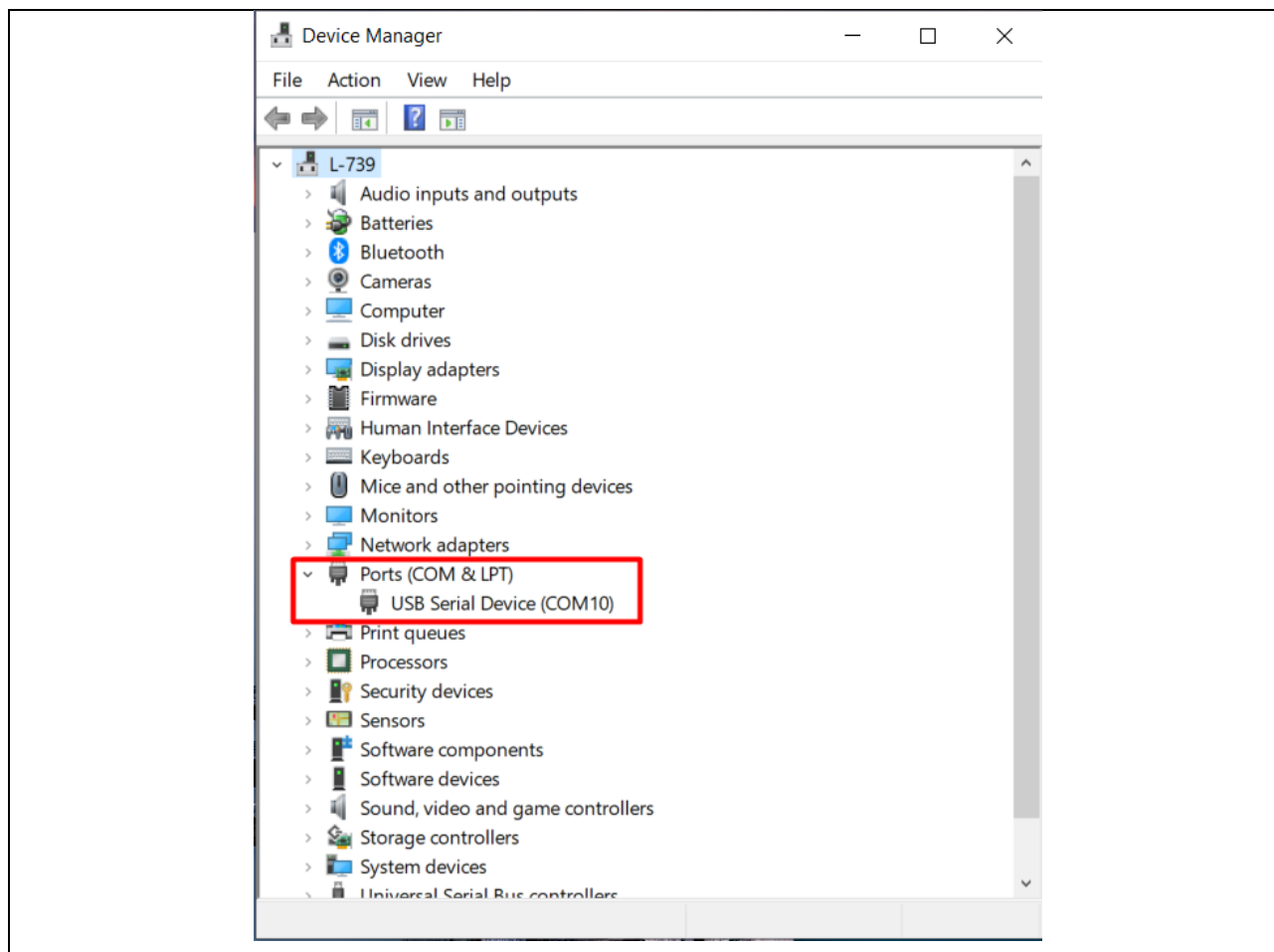


Figure 23. Identifying the COM Port in Device Manager

To run the host application, type the following command on the command window as shown below.

```
deploy.exe connect <COM port Number>
```



Figure 24. Host application console messages

At this stage, the host application communicates with the target through the USB-CDC communication interface. The user application does the following tasks as shown in section 5.3:

1. Scans for the USB COM port provided by the user. If it finds it, it opens the serial connection.
2. On successful serial connection, it issues the Generate Key command to the target kit.
3. On the device side, the ECC key pairs are generated using the SCE crypto modules. The public key is sent back to the host application.
4. The host application creates root CA and signing key to be used to sign the device certificate at the latter stage.
5. Generates a challenge/response string and sends it to the target kit.
6. On successful challenge/response, the host application will sign and send the device certificate to the device.
7. The device certificate will be securely stored in the internal code flash and protected by Arm® TrustZone®.

Note: After running this application project, user MUST follow section, Initialize the MCU

6.4 Customizing the Application Project

6.4.1 Customize the PC Application

To customize the PC application, first download the Visual Studio development environment using the software pointed out in the Required Resources section. Before compiling the project, retarget the project to use the Windows SDK installed on the development PC.

Next, compile the project and update as desired from this point onward.

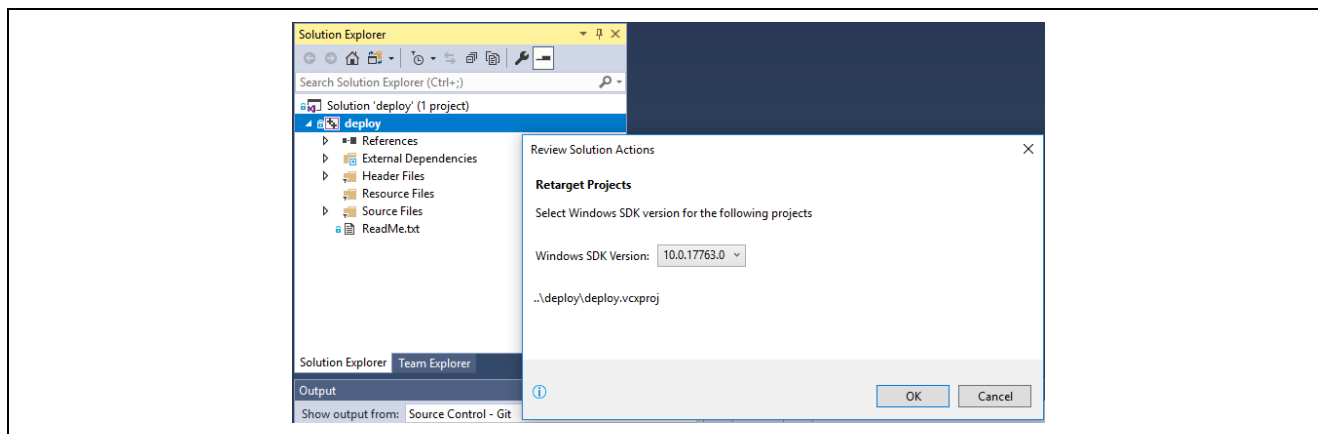


Figure 25. Retarget to the installed Windows SDK

7. References

Available on www.renesas.com:

- <https://github.com/renesas/fsp/releases>
- [Renesas RA Securing Data at Rest application project using TrustZone®](#)
- [Renesas RA Security Design with Arm TrustZone® – IP Protection](#)
- [Renesas Device Lifecycle Management Key Installation](#)

8. Known Issues and Limitations

The host application is tested only on Windows® 10 PC.

9. Appendix

9.1 Glossary

Term	Meaning
Certificate Authority (CA)	An entity that issues digital certificates according to policy-based rules. A CA could be public or private, located in the Cloud, or in the case of an on-premises CA, typically hosted on a secure appliance.
Device Certificate	Certificate uniquely identifying an individual device. It is digitally signed, asserting that the certificate comes from a known source and has not been modified, and that the device is trusted.
Root of Trust	Roots of trust are highly-reliable hardware, firmware, and software components that perform specific, critical security functions. (https://csrc.nist.gov/projects/hardware-roots-of-trust)
SCE	Secure Crypto Engine – A module in the MCU that provides for efficient, low-power cryptographic acceleration, TRNG (True Random Number Generation), creation and isolation of cryptographic keys.
PKI	Public Key Infrastructure – A set of roles, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates, which are typically used to manage secure identity via public key cryptography.
Key Pair	Asymmetric keys are generated in pairs – a public and private key. The private key is held in secret by only one party and can be used to assert that party's identity. The public key is freely distributed and is uniquely associated with the private key.
Secure Code	A function or group of functions that resides in a secure region of internal flash or internal SRAM, as defined and enforced by the TrustZone®. Please reference the Secure Data at Rest for RA Family to understand the access control of the Secure Code.
Non-Secure code	A function or group of functions that resides in a non-secure region of internal flash or internal SRAM. Please reference the Secure Data at Rest for RA Family to understand the access control of the non-Secure code.
Challenge String	Randomly generated string at the host application. This string is used by the host application to validate the ownership of the private key by the target.
Unique ID	An identification value, unique to each individual RA Family MCU, that is stored inside the MCU. The unique ID is used by the SCE when it wraps a key.

10. Website and Support

Visit the following URLs to learn about the RA family of microcontrollers, download tools and documentation, and get support.

EK-RA6M4 Resources	renesas.com/ra/ek-ra6m4
RA Product Information	renesas.com/ra
Flexible Software Package (FSP)	renesas.com/ra/fsp
RA Product Support Forum	renesas.com/ra/forum
Renesas Support	renesas.com/support

Revision History

Rev.	Date	Description	
		Page	Summary
1.0.0	Dec.02.20	-	Initial version
1.1.0	Jun.11.21	-	Updated to FSP v3.0.0. FSP MbedCrypto module is updated.
1.2.0	Aug.02.23	-	Updated to FSP v4.5.0.
1.3.0	Jun.03.24	-	Updated to FSP v5.2.0
1.4.0	Jul.21.25	-	Updated to FSP v6.0.0

General Precautions in the Handling of Microprocessing Unit and Microcontroller Unit Products

The following usage notes are applicable to all Microprocessing unit and Microcontroller unit products from Renesas. For detailed usage notes on the products covered by this document, refer to the relevant sections of the document as well as any technical updates that have been issued for the products.

1. Precaution against Electrostatic Discharge (ESD)

A strong electrical field, when exposed to a CMOS device, can cause destruction of the gate oxide and ultimately degrade the device operation. Steps must be taken to stop the generation of static electricity as much as possible, and quickly dissipate it when it occurs. Environmental control must be adequate. When it is dry, a humidifier should be used. This is recommended to avoid using insulators that can easily build up static electricity.

Semiconductor devices must be stored and transported in an anti-static container, static shielding bag or conductive material. All test and measurement tools including work benches and floors must be grounded. The operator must also be grounded using a wrist strap. Semiconductor devices must not be touched with bare hands. Similar precautions must be taken for printed circuit boards with mounted semiconductor devices.

2. Processing at power-on

The state of the product is undefined at the time when power is supplied. The states of internal circuits in the LSI are indeterminate and the states of register settings and pins are undefined at the time when power is supplied. In a finished product where the reset signal is applied to the external reset pin, the states of pins are not guaranteed from the time when power is supplied until the reset process is completed. In a similar way, the states of pins in a product that is reset by an on-chip power-on reset function are not guaranteed from the time when power is supplied until the power reaches the level at which resetting is specified.

3. Input of signal during power-off state

Do not input signals or an I/O pull-up power supply while the device is powered off. The current injection that results from input of such a signal or I/O pull-up power supply may cause malfunction and the abnormal current that passes in the device at this time may cause degradation of internal elements. Follow the guideline for input signal during power-off state as described in your product documentation.

4. Handling of unused pins

Handle unused pins in accordance with the directions given under handling of unused pins in the manual. The input pins of CMOS products are generally in the high-impedance state. In operation with an unused pin in the open-circuit state, extra electromagnetic noise is induced in the vicinity of the LSI, an associated shoot-through current flows internally, and malfunctions occur due to the false recognition of the pin state as an input signal become possible.

5. Clock signals

After applying a reset, only release the reset line after the operating clock signal becomes stable. When switching the clock signal during program execution, wait until the target clock signal is stabilized. When the clock signal is generated with an external resonator or from an external oscillator during a reset, ensure that the reset line is only released after full stabilization of the clock signal. Additionally, when switching to a clock signal produced with an external resonator or by an external oscillator while program execution is in progress, wait until the target clock signal is stable.

6. Voltage application waveform at input pin

Waveform distortion due to input noise or a reflected wave may cause malfunction. If the input of the CMOS device stays in the area between V_{IL} (Max.) and V_{IH} (Min.) due to noise, for example, the device may malfunction. Take care to prevent chattering noise from entering the device when the input level is fixed, and also in the transition period when the input level passes through the area between V_{IL} (Max.) and V_{IH} (Min.).

7. Prohibition of access to reserved addresses

Access to reserved addresses is prohibited. The reserved addresses are provided for possible future expansion of functions. Do not access these addresses as the correct operation of the LSI is not guaranteed.

8. Differences between products

Before changing from one product to another, for example to a product with a different part number, confirm that the change will not lead to problems. The characteristics of a microprocessing unit or microcontroller unit products in the same group but having a different part number might differ in terms of internal memory capacity, layout pattern, and other factors, which can affect the ranges of electrical characteristics, such as characteristic values, operating margins, immunity to noise, and amount of radiated noise. When changing to a product with a different part number, implement a system-evaluation test for the given product.

Notice

1. Descriptions of circuits, software and other related information in this document are provided only to illustrate the operation of semiconductor products and application examples. You are fully responsible for the incorporation or any other use of the circuits, software, and information in the design of your product or system. Renesas Electronics disclaims any and all liability for any losses and damages incurred by you or third parties arising from the use of these circuits, software, or information.
2. Renesas Electronics hereby expressly disclaims any warranties against and liability for infringement or any other claims involving patents, copyrights, or other intellectual property rights of third parties, by or arising from the use of Renesas Electronics products or technical information described in this document, including but not limited to, the product data, drawings, charts, programs, algorithms, and application examples.
3. No license, express, implied or otherwise, is granted hereby under any patents, copyrights or other intellectual property rights of Renesas Electronics or others.
4. You shall be responsible for determining what licenses are required from any third parties, and obtaining such licenses for the lawful import, export, manufacture, sales, utilization, distribution or other disposal of any products incorporating Renesas Electronics products, if required.
5. You shall not alter, modify, copy, or reverse engineer any Renesas Electronics product, whether in whole or in part. Renesas Electronics disclaims any and all liability for any losses or damages incurred by you or third parties arising from such alteration, modification, copying or reverse engineering.
6. Renesas Electronics products are classified according to the following two quality grades: "Standard" and "High Quality". The intended applications for each Renesas Electronics product depends on the product's quality grade, as indicated below.

"Standard": Computers; office equipment; communications equipment; test and measurement equipment; audio and visual equipment; home electronic appliances; machine tools; personal electronic equipment; industrial robots; etc.

"High Quality": Transportation equipment (automobiles, trains, ships, etc.); traffic control (traffic lights); large-scale communication equipment; key financial terminal systems; safety control equipment; etc.

Unless expressly designated as a high reliability product or a product for harsh environments in a Renesas Electronics data sheet or other Renesas Electronics document, Renesas Electronics products are not intended or authorized for use in products or systems that may pose a direct threat to human life or bodily injury (artificial life support devices or systems; surgical implantations; etc.), or may cause serious property damage (space system; undersea repeaters; nuclear power control systems; aircraft control systems; key plant systems; military equipment; etc.). Renesas Electronics disclaims any and all liability for any damages or losses incurred by you or any third parties arising from the use of any Renesas Electronics product that is inconsistent with any Renesas Electronics data sheet, user's manual or other Renesas Electronics document.
7. No semiconductor product is absolutely secure. Notwithstanding any security measures or features that may be implemented in Renesas Electronics hardware or software products, Renesas Electronics shall have absolutely no liability arising out of any vulnerability or security breach, including but not limited to any unauthorized access to or use of a Renesas Electronics product or a system that uses a Renesas Electronics product. RENESAS ELECTRONICS DOES NOT WARRANT OR GUARANTEE THAT RENESAS ELECTRONICS PRODUCTS, OR ANY SYSTEMS CREATED USING RENESAS ELECTRONICS PRODUCTS WILL BE INVULNERABLE OR FREE FROM CORRUPTION, ATTACK, VIRUSES, INTERFERENCE, HACKING, DATA LOSS OR THEFT, OR OTHER SECURITY INTRUSION ("Vulnerability Issues"). RENESAS ELECTRONICS DISCLAIMS ANY AND ALL RESPONSIBILITY OR LIABILITY ARISING FROM OR RELATED TO ANY VULNERABILITY ISSUES. FURTHERMORE, TO THE EXTENT PERMITTED BY APPLICABLE LAW, RENESAS ELECTRONICS DISCLAIMS ANY AND ALL WARRANTIES, EXPRESS OR IMPLIED, WITH RESPECT TO THIS DOCUMENT AND ANY RELATED OR ACCOMPANYING SOFTWARE OR HARDWARE, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE.
8. When using Renesas Electronics products, refer to the latest product information (data sheets, user's manuals, application notes, "General Notes for Handling and Using Semiconductor Devices" in the reliability handbook, etc.), and ensure that usage conditions are within the ranges specified by Renesas Electronics with respect to maximum ratings, operating power supply voltage range, heat dissipation characteristics, installation, etc. Renesas Electronics disclaims any and all liability for any malfunctions, failure or accident arising out of the use of Renesas Electronics products outside of such specified ranges.
9. Although Renesas Electronics endeavors to improve the quality and reliability of Renesas Electronics products, semiconductor products have specific characteristics, such as the occurrence of failure at a certain rate and malfunctions under certain use conditions. Unless designated as a high reliability product or a product for harsh environments in a Renesas Electronics data sheet or other Renesas Electronics document, Renesas Electronics products are not subject to radiation resistance design. You are responsible for implementing safety measures to guard against the possibility of bodily injury, injury or damage caused by fire, and/or danger to the public in the event of a failure or malfunction of Renesas Electronics products, such as safety design for hardware and software, including but not limited to redundancy, fire control and malfunction prevention, appropriate treatment for aging degradation or any other appropriate measures. Because the evaluation of microcomputer software alone is very difficult and impractical, you are responsible for evaluating the safety of the final products or systems manufactured by you.
10. Please contact a Renesas Electronics sales office for details as to environmental matters such as the environmental compatibility of each Renesas Electronics product. You are responsible for carefully and sufficiently investigating applicable laws and regulations that regulate the inclusion or use of controlled substances, including without limitation, the EU RoHS Directive, and using Renesas Electronics products in compliance with all these applicable laws and regulations. Renesas Electronics disclaims any and all liability for damages or losses occurring as a result of your noncompliance with applicable laws and regulations.
11. Renesas Electronics products and technologies shall not be used for or incorporated into any products or systems whose manufacture, use, or sale is prohibited under any applicable domestic or foreign laws or regulations. You shall comply with any applicable export control laws and regulations promulgated and administered by the governments of any countries asserting jurisdiction over the parties or transactions.
12. It is the responsibility of the buyer or distributor of Renesas Electronics products, or any other party who distributes, disposes of, or otherwise sells or transfers the product to a third party, to notify such third party in advance of the contents and conditions set forth in this document.
13. This document shall not be reprinted, reproduced or duplicated in any form, in whole or in part, without prior written consent of Renesas Electronics.
14. Please contact a Renesas Electronics sales office if you have any questions regarding the information contained in this document or Renesas Electronics products.

(Note1) "Renesas Electronics" as used in this document means Renesas Electronics Corporation and also includes its directly or indirectly controlled subsidiaries.

(Note2) "Renesas Electronics product(s)" means any product developed or manufactured by or for Renesas Electronics.

(Rev.5.0-1 October 2020)

Corporate Headquarters

TOYOSU FORESIA, 3-2-24 Toyosu,
Koto-ku, Tokyo 135-0061, Japan
www.renesas.com

Trademarks

Renesas and the Renesas logo are trademarks of Renesas Electronics Corporation. All trademarks and registered trademarks are the property of their respective owners.

Contact information

For further information on a product, technology, the most up-to-date version of a document, or your nearest sales office, please visit:
www.renesas.com/contact/.