Renesas RA Family

RA AWS Cloud Connectivity on CK-RA6M5 with Cellular– Getting Started Guide

Introduction

This document provides instructions for running AWS cloud connectivity Application Project on CK-RA6M5 using cellular interface.

Applies to:

- RA6M5 MCU Group

Required Resources

To build and run the MQTT/TLS application example, the following resources are needed.

Development tools and software

- e^2 studio ISDE v23.4.0 or later (renesas.com/us/en/software-tool/e-studio)
- Flexible Software Package (FSP) v4.4.0 (renesas.com/us/en/software-tool/flexible-software-package-fsp)

Hardware

- Renesas CK-RA6M5 kit (renesas.com/ra/ck-ra6m5)
- PC running Windows® 10 and an installed web browser (Google Chrome, Internet Explorer, Microsoft Edge, Mozilla Firefox, or Safari)
- Micro USB cables (included as part of the kit. See *CK-RA6M5 User's Manual*).

Prerequisites and Intended Audience

This application note assumes that the user is adept at operating the Renesas e^2 studio IDE with Flexible Software Package (FSP). If not, we recommend reading and following the procedures in the *FSP User's Manual* sections for 'Starting Development' including 'Debug the Blinky Project'. Doing so enables familiarization with e^2 studio and FSP and validates proper debug connection to the target board. In addition, this application note assumes prior knowledge of MQTT/TLS and its communication protocols and knowledge of cellular modems.

The intended audience is users who want to develop applications with MQTT/TLS modules using Cellular modules on Renesas RA6 MCU Series.

Note: If you are a first-time user of e^2 studio and FSP, we highly recommend you install e^2 studio and FSP on your system in order to run the Blinky Project and to get familiar with the e^2 studio and FSP development environment before proceeding to the next sections.

Note: This Application Project and Application Note can guarantee to work only with FSP v4.4.0.

Prerequisites

1. Access to online documentation available in the Cloud Connectivity References section
2. Access to latest documentation for identified Renesas Flexible Software Package
3. Prior knowledge of operating e^2 studio and built-in (or standalone) RA Configurator
4. Access to associated hardware documentation such as User Manuals, Schematics, and other relevant kit information (renesas.com/ra/ck-ra6m5)).

Contents

1. Importing, Building, and Loading the Project

1.1 Importing

This project “aws_ck_ra6m5_cellular_app” can be imported into the e^2 studio using the instructions provided in the RA *FSP User’s Manual*. See Section *Starting Development > e2 studio ISDE User Guide > Importing an Existing Project into e^2 studio ISDE.*

1.2 Building the Latest Executable Binary

Upon successfully importing and/or modifying the project into e^2 studio IDE, follow the instructions provided in the RA *FSP User's Manual* to build an executable binary/hex/mot/elf file. See Section *Starting Development > e2 studio ISDE User Guide > Tutorial: Your First RA MCU Project > Build the Blinky Project.*

1.3 Loading the Executable Binary into the Target MCU

The executable file may be programmed into the target MCU through any one of three means.

1.3.1 Using a Debugging Interface with e^2 studio

Instructions to program the executable binary are found in the latest RA FSP User Manual. See Section *Starting Development > e2 studio ISDE User Guide > Tutorial: Your First RA MCU Project > Debug the Blinky Project.*

This is the preferred method for programming as it allows additional debugging functionality available through the on-chip debugger.

Follow the instructions for programming the board and proceed to section 1.4.

1.3.2 Using J-Link Tools

SEGGER J-Link Tools such as J-Flash, J-Flash Lite, and J-Link Commander can be used program the executable binary into the target MCU. Refer to User Manuals UM08001 and UM08003 on www.segger.com. Use the `.srec` or `.hex` file in Application Project to program the board and proceed to section 1.4.

1.3.3 Using Renesas Flash Programmer

Renesas Flash Programmer provides usable and functional support for programming the on-chip flash memory of Renesas microcontrollers in each phase of development and mass production. Use the .srec or .hex file in the Application Project folder to program the board and proceed to section 1.4.

1.4 Connection Settings and Deviation

Reset the board assembly associated with this application note to the default electrical jumper settings as specified in the *CK-RA5M5 User’s Manual* before proceeding with the next set of instructions.

Note: For this Cellular based cloud connectivity application project and application note, the user is required to connect the RYZ014A PMOD module to the connector (J5 – PMOD2) on the board.

1.5 Powering up the Board

To connect power to the board, connect the USB cable to the CK-RA6M5 board’s J14 connector (USB_DEBUG) and the other end to the PC USB port. Connect the second USB Cable to J20 (USB SER) connector of the CK-RA6M5 board and other end to the second USB Port of the PC (This will be the Console Port for Application). Users are required to use the Command Line Interface (CLI) to configure and run the Application.

Then run the debug application, with the following instructions.

1.5.1 Power-on Behavior

Upon successful configuration and downloading of the image to the target RA MCU, the following behavior should be observed upon application of power, as indicated in the Quick Start Example project on the website at renesas.com/ra/ck-ra6m5:

1. The power LED on the RA MCU target assembly lights up.

2. The J-Link LED will be blinking based on the activity when it is connected.
3. The User LEDs (BLUE, GREEN, RED) are used to indicate the status of the application from the start of initialization to continuous status of running.

2. Running the Application Project

Note**:** The steps indicated below are applicable for Window OS only. The project is not supported on Mac OS or Linux.

To run the application project, users are required to

- Activate the Modem and SIM using the Launch Pad portal using the IMEI and ICCID info.
  Note: The details for getting IMEI and ICCID info are described in the following steps.

2.1 Connecting the Board to the Serial port Console of the PC

1. On the host PC, open Windows Device Manager. Expand **Ports (COM & LPT)**, locate **USB Serial Device (COMxx)** and note down the COM port number for reference in the next step.

   Note: USB Serial Device drivers are required to communicate between the CK-RA6M5 board and the terminal application on the host PC.

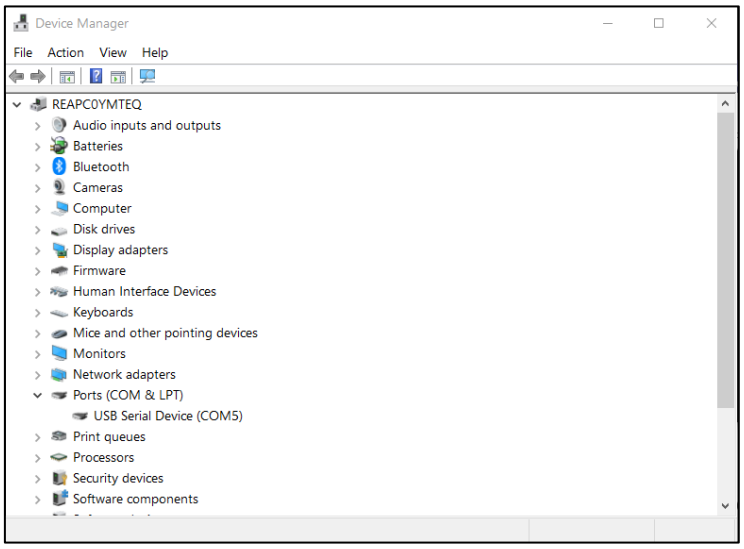

Figure 1. USB Serial Device in Windows Device Manager

2. Open Tera Term select **New connection** and select **Serial** and **COMxx: USB Serial Device (COMxx)** and click **OK**.

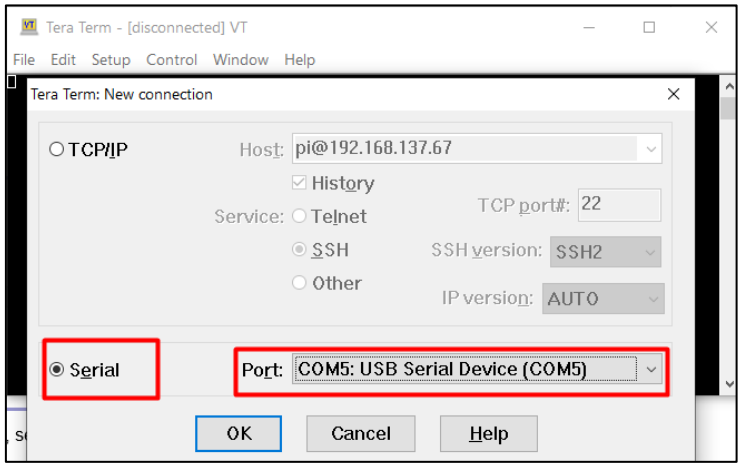

Figure 2. Selecting the Serial Port on Tera Term

3. Make sure Tera Term selects the black background, if not configure it from **Setup > Window** and make the following selections.

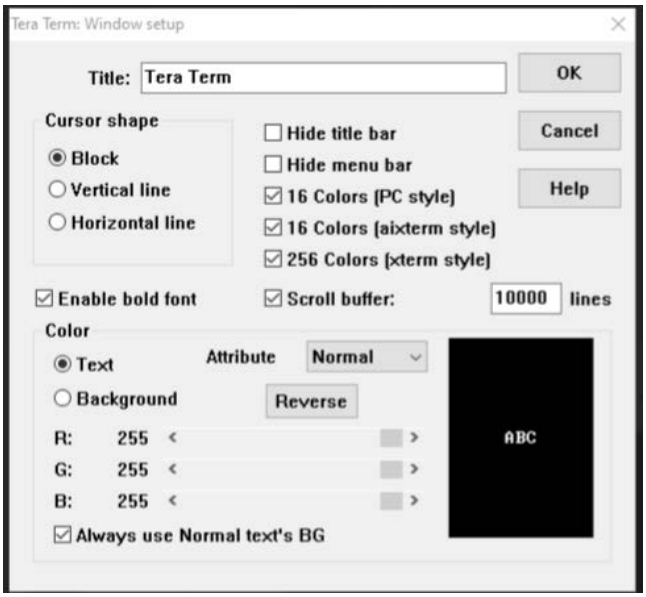

Figure 3. Configuring the Black Background for Serial Port on Tera Term

4. Also using the setup menu pull-down, and select terminal, on the terminal setup select **New-line Receive** as **AUTO**.
5. Using the **Setup** menu pull-down, select **Serial port…** and ensure that the speed is set to **115200**, as shown below.

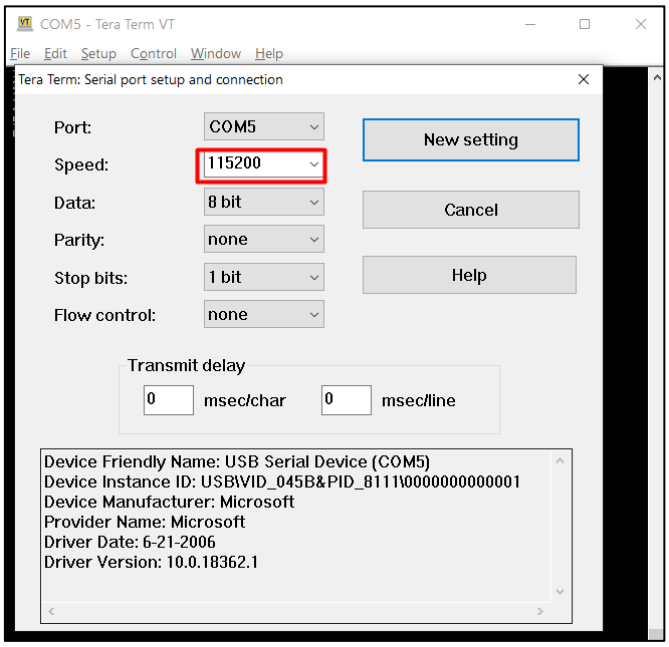

Figure 4. Select 115200 on the Speed Pulldown

6. Complete the connection. The Configuration CLI Menu will be displayed on the console as shown below.
   Note: Please reset the board by pressing the S1 user switch if the menu is not displayed.

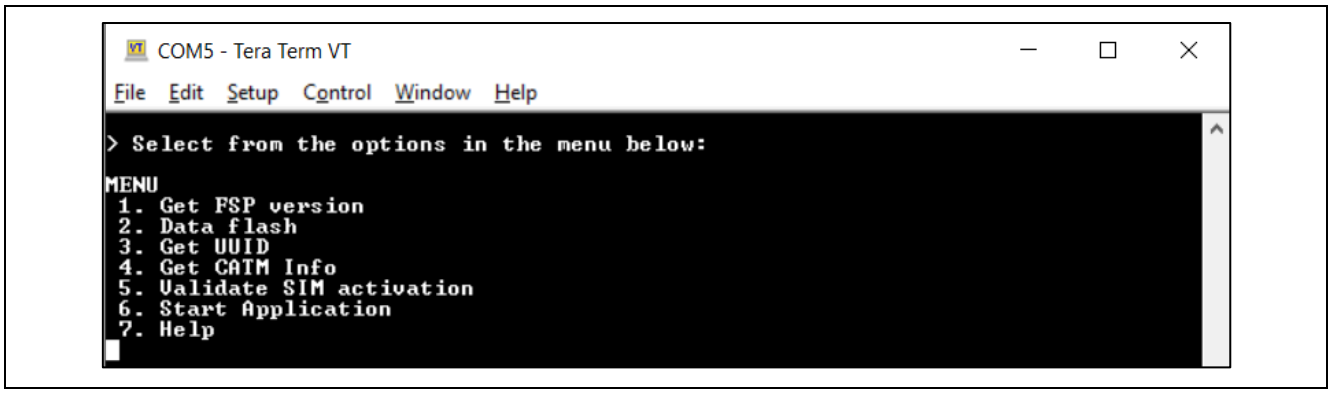

Figure 5. Main Menu

7. In the CLI shown in the preceding screenshot, choose the number to select the commands. For example, when you press **1**, the FSP version of the application is displayed as shown below. At any point of time, press the space bar to return to the previous menu.

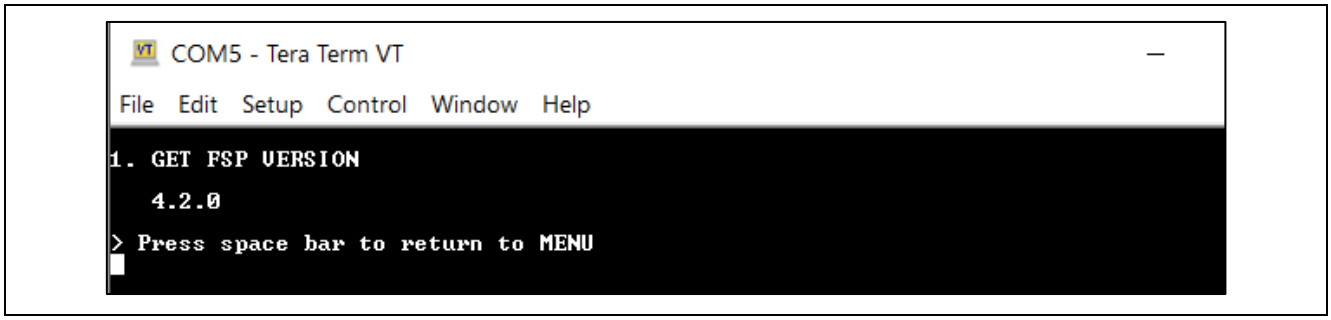

Figure 6. FSP Version Information

2.2 Getting the SIM and Modem Information for Activation

1. Press **4** to display **CAT-M Information**. This menu will communicate with the RYZ014A PMOD module to obtain the ICCID value needed for activating the SIM card. Upon success, the IMEI and ICCID values will be displayed on the terminal screen. The program will continue to attempt to communicate with the RYZ014A PMOD module until it has successfully connected or timed out. After obtaining the ICCID value, go to Truphone https://www.truphone.com/connectit/ to activate the SIM card (see section **2.3 Activating a SIM card).**

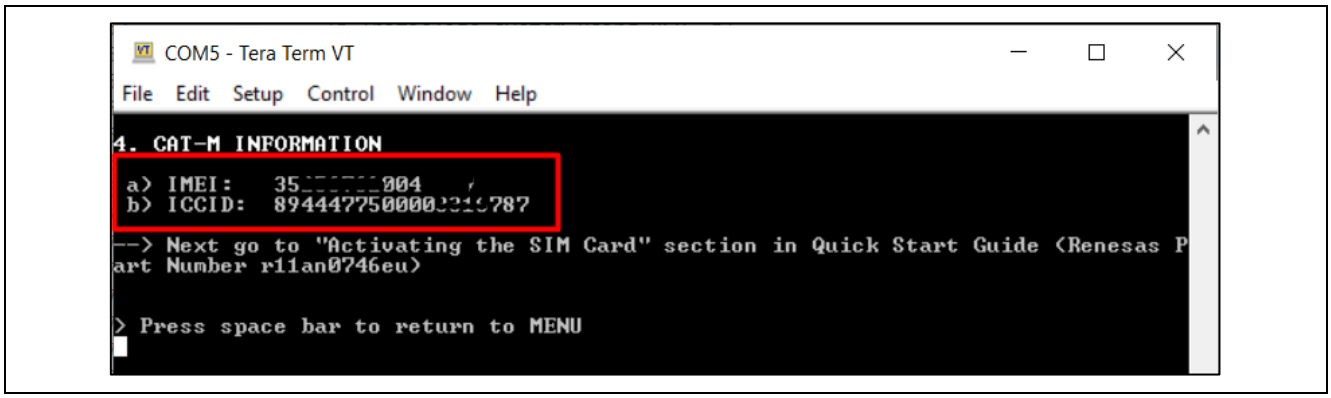

Figure 7. CAT-M Information

2.3 Activating a SIM card

To activate the included SIM card, please visit the Truphone SIM Activation platform at truphone.com/connectit and use the following steps:

1. On the Business page, click **Start activation** button under **IoT SIM Activation.**

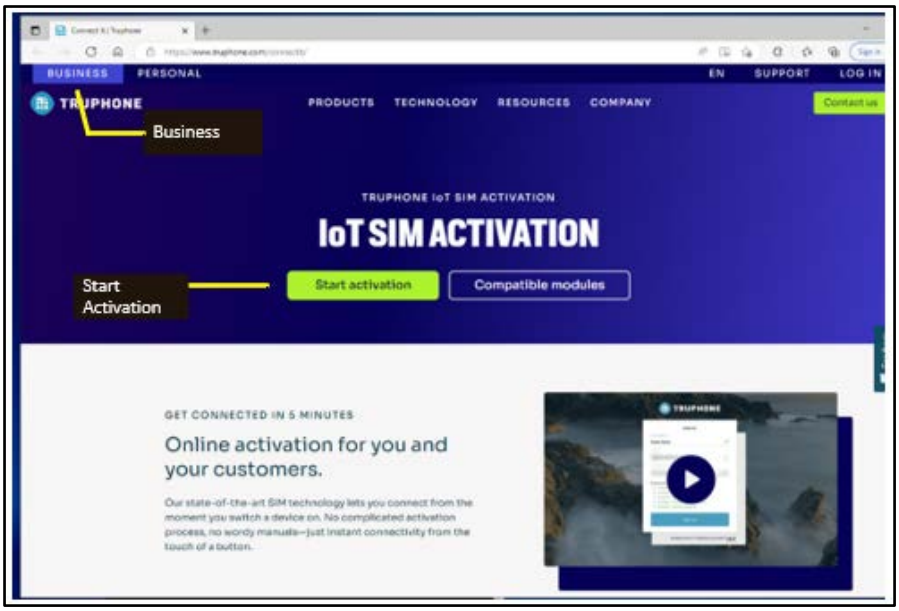

Figure 8. Activating the SIM card

2. Create a new Truphone Account by selecting **Sign up** (next to **Don't have an account yet?**) and fill-in your full name, Email, and a password. Then Click **Sign up** to create a new account.
3. Select **Personal** as the account type.
4. Select **Get Started**.
5. Verify your email by entering the activation code sent to your email account.
6. Complete the **Profile information** form – then select **Create account**.
7. Select **Activate SIMS** to Activate your individual SIM by **ICCID** and **PUK** found on the SIM Card packaging.
8. Enter the **ICCID** value obtained from the **Running the RYZ014A PMOD example project** section. See the **ICCID** value in **Figure 7. CAT-M Information.** Fill other fields as needed.
9. You will receive email confirmation when the SIM Card activation is complete.
10. Ensure the SIM card is inserted in the RYZ014A PMOD. From the Console **Main Menu 5, Validate SIM activation** to verify that the SIM card is activated.
    The SIM card should be activated on the Truphone SIM Activation platform after 15 minutes and can be validated on the Tera Term terminal as shown in . The time for the SIM Card to be activated by Truphone can vary depending on their system demand. In most cases, if PING Response fails, wait a few more minutes and repeat **Menu 5 Validate SIM activation.**

Disclaimer

The activation steps above are provided by SIM Provider Truphone. They are the most current at the time of publishing this application note. If you need help activating your SIM Card, contact Truphone support iot.truphone.com or Contact Support | Truphone.

If you have a SIM card from any other provider then contact the technical support for that provider.

For any other issue that cannot be resolved please contact Renesas Support at Technical Support.

Note: The SIM card Provider for the Application project is Truphone. If you use any other SIM Card provider you must change the Access Point Name required for the SIM Card Provider in your global region. Failure to do so could result in the RYZ014A not connecting to the Cellular network.

To set the Access Point Name (APN) for SIM Card provider other than Truphone

The APN is set in the Application project in /src/cellular_setup.c

See `#define CELLULAR_APN "iot.truphone.com"  /* APN : Truphone SIM Card */`

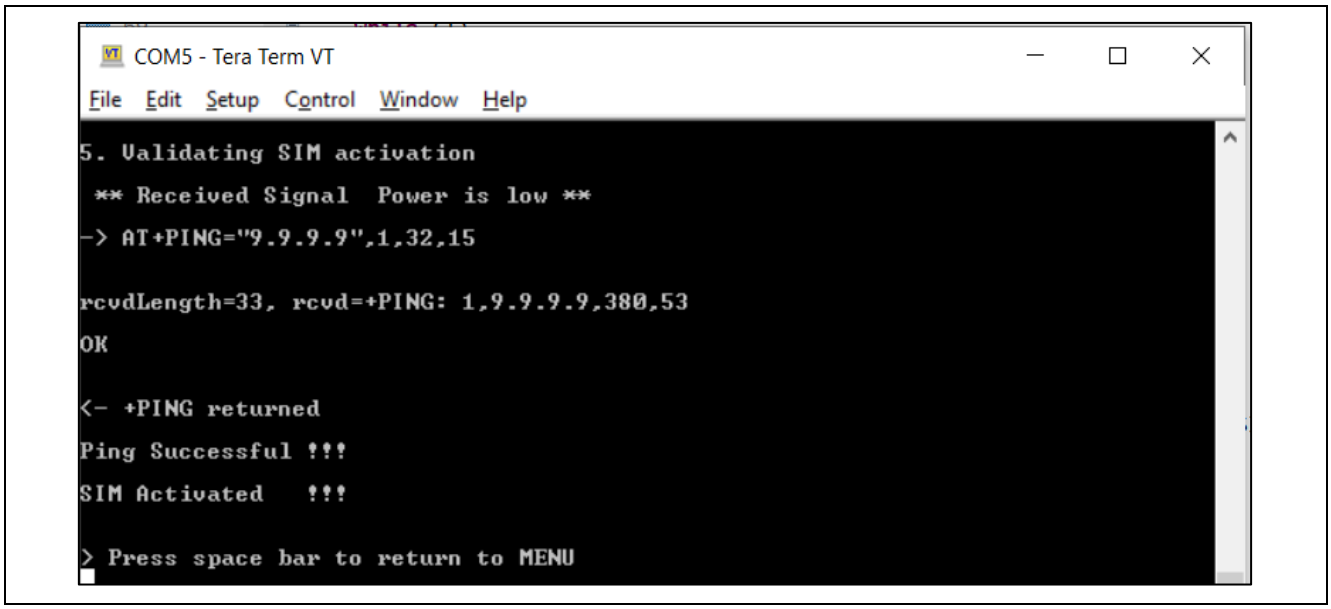

Figure 9. Validating SIM Activation – SIM Card Active

2.4 Getting the UUID Information of the Board

1. Press **3** from the **Main Menu** to display the board UUID. This command obtains the UUID information of the board and displays it on the console as shown in the screenshot below. You will need this information for registering to the Renesas AWS Cloud Dashboard.

Figure 10. Getting Board UUID Information

2.5 Registering to Renesas AWS Cloud Dashboard

AWS dashboard for Renesas CK-RA6M5 cloud kit is custom designed to visualize the data of all the sensors on the cloud kits. The dashboard connects to AWS IoT services through AWS IoT core and enables users to utilize the cloud services to full potential.
To allow users to experience a hassle free first experience of the cloud kits, every cloud kit will be credited with $10 USD AWS credits upon registration.
The dashboard can be accessed at https://renesas.cloud-ra-rx.com/

2.5.1 Sign up

After establishing the access of the RA & RX kit to kit-associated AWS sub account, where all necessary infrastructure will be provisioned, each user should sign up:

1. Go to the https://renesas.cloud-ra-rx.com/
2. If you don't have an account, click on the **Sign up** button. You are directed to the **Sign up** page.

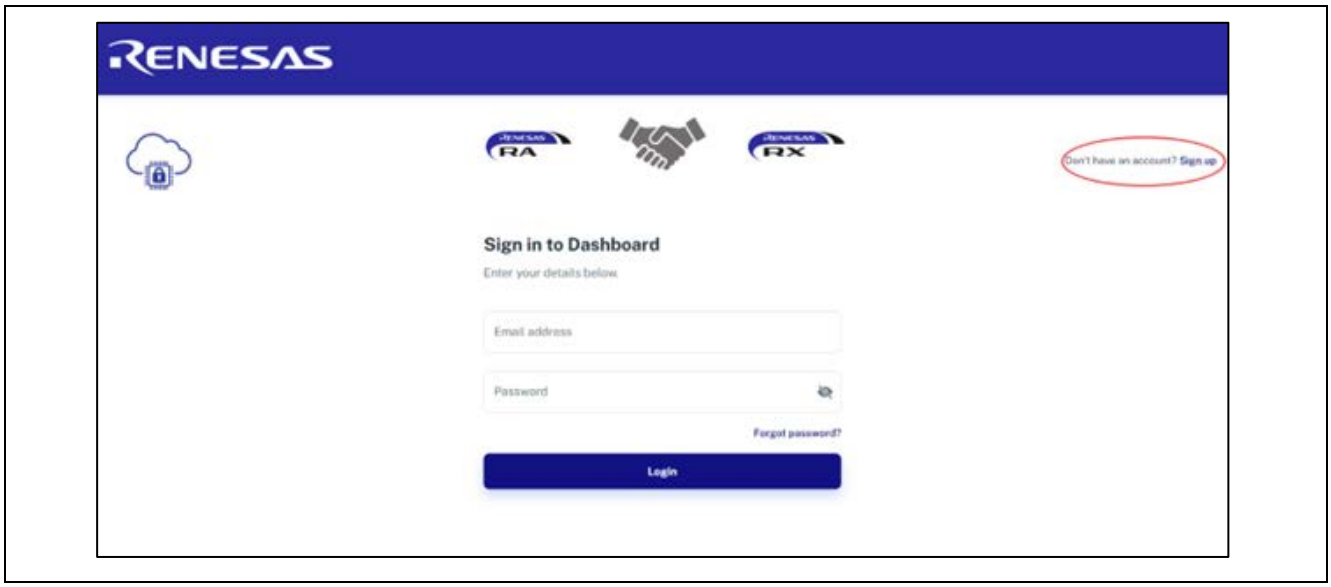

Figure 11. Creating Account

3. Enter your first name, last name, email address and password and press on the button **Register**.

Figure 12. Registering Information

The rules for a valid first name and last name:

- Length Constraints: Minimum length of 2. Maximum length of 24.
- Information must be entered in English or another Latin character-based language.

The rules for a valid email address:

- The address must be a minimum of 6 and a maximum of 64 characters long.
- All characters must be 7-bit ASCII characters.
- There must be one and only one @ symbol, which separates the local name from the domain name.
- The local name can't contain any of the following characters: whitespace, " ' ( ) < > [ ] : ; , \ | % &
- The local name can't begin with a dot (.)
- The local name can’t contain double Plus, for example: account+rnss+alpha@domain.com
- The domain name can consist of only the characters [a-z],[A-Z],[0-9], hyphen (-), or dot (.)
- The domain name can't begin or end with a hyphen (-) or dot (.)
- The domain name must contain at least one dot.

The rules for a valid password:

- The password must be a minimum of 8 and maximum of 64 characters long.
- Password must contain at least one uppercase character, one lowercase character, one number, one special character: ! # $ % & * ? @.

4. Verification code will be sent to your email. Enter the code and press on the button **Send**. You are redirected to the **Register Device** page.

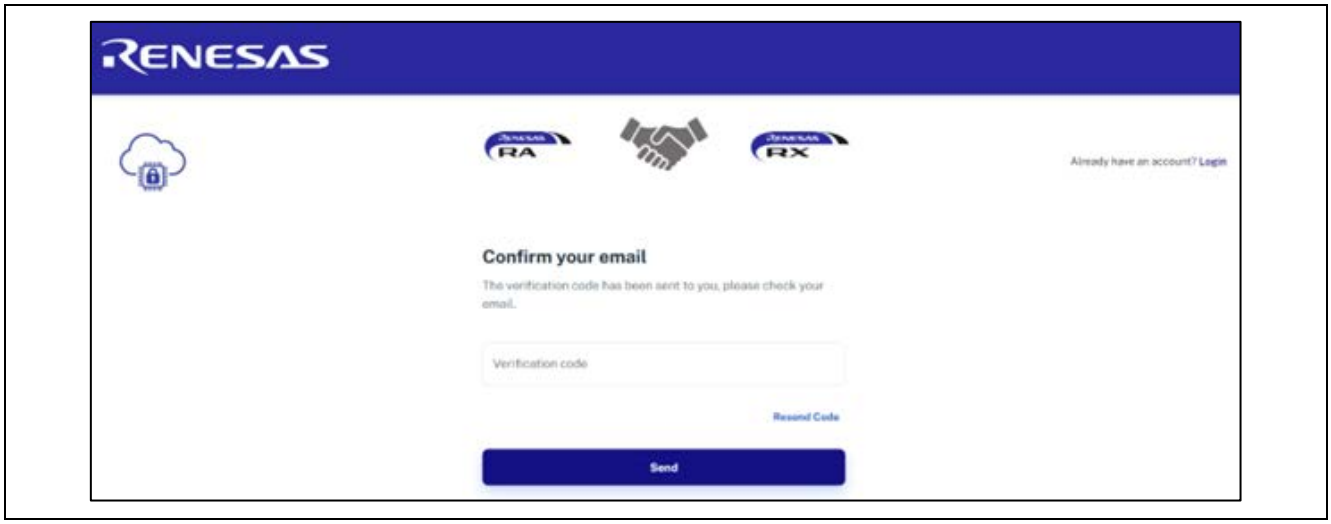

Figure 13. Confirming Email

If you do not receive an email with the code, please click on **Resend Code**.

5. Enter the UUID of the kit to complete the registration process. UUID is the unique ID of your board. Refer to “CK-RA6M5 AWS Application Project” for steps for obtaining the UUID of the kit.
   Note: Only 1 device will be assigned to an account.

Figure 14. Registering Device

6. The registration page indicates that the device registration is in progress.

Figure 15. Device Registration in Progress

7. After the sub account is registered, it is provisioned.

Figure 16. Sub Account Registration

8. Wait for the buttons **Download Certificate** and **Go To Dashboard** turn available on the registration page. This process may take up to **1 hour** for device provisioning to complete.

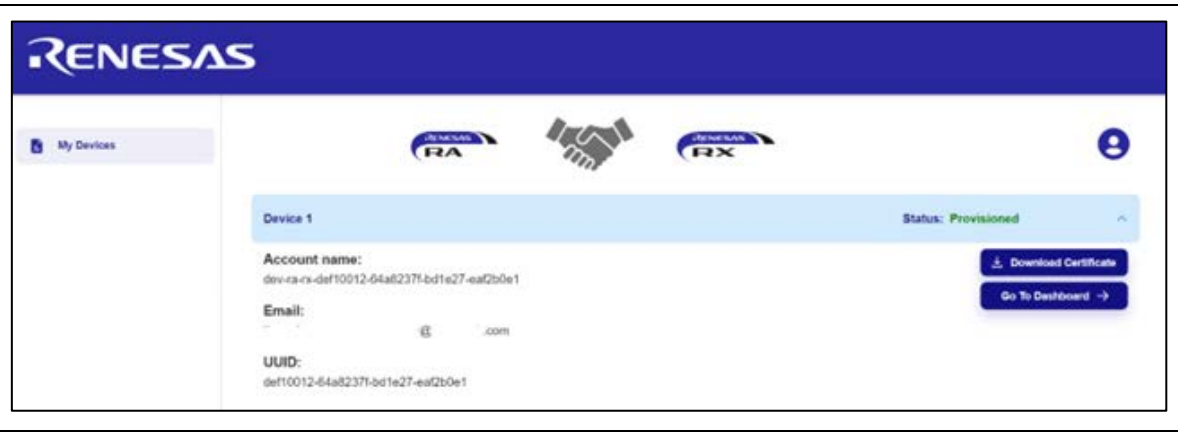

Figure 17. Completing Device Provisioning

2.5.2 Sign in

If you have already registered on our web portal, you need to Sign in entering your email and password.

2.5.3 Forgot password

1. Click **Forgot password** on **Sign in to Dashboard** page. You are directed to the **Restore Password** page.

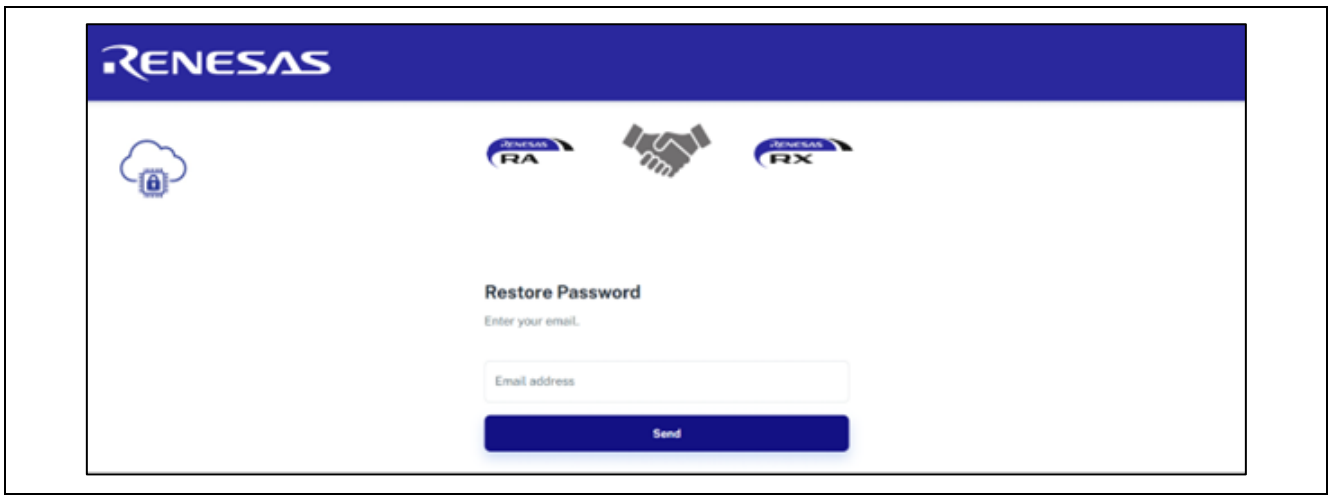

Figure 18. Restoring Password 1

2. Enter your email and click on the button **Send**.

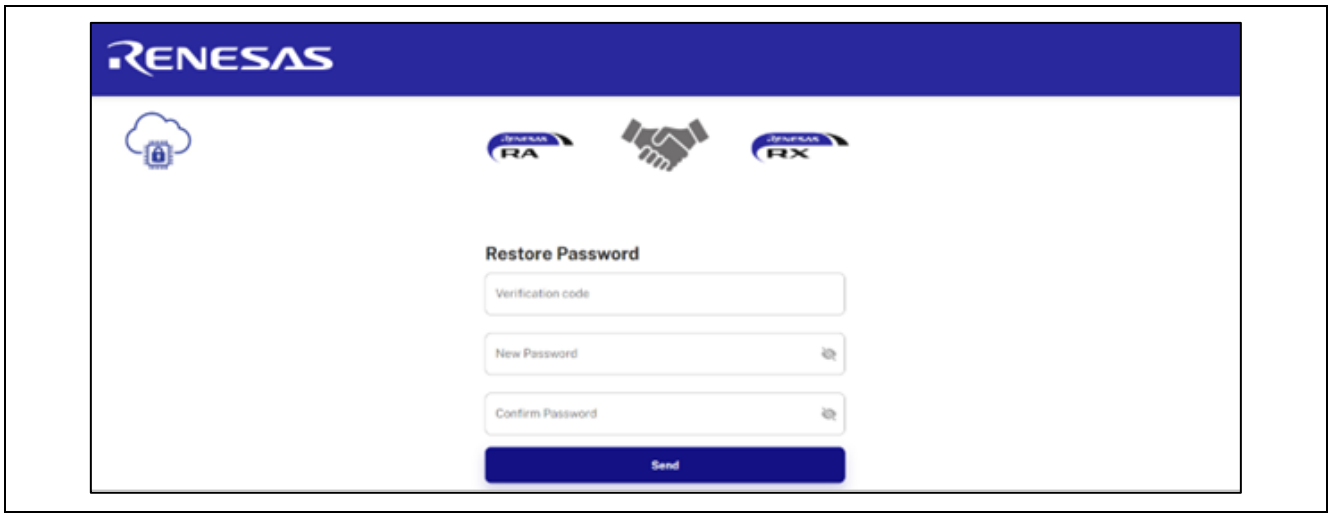

Figure 19. Restoring Password 2

3. You should receive a verification code to your email.
4. Enter the code, your new password and confirm it.
5. To end the process, press on the button **Send**.

2.5.4 Profile page

To see your profile page:

1. Click on your user's picture - top right. Select Profile.

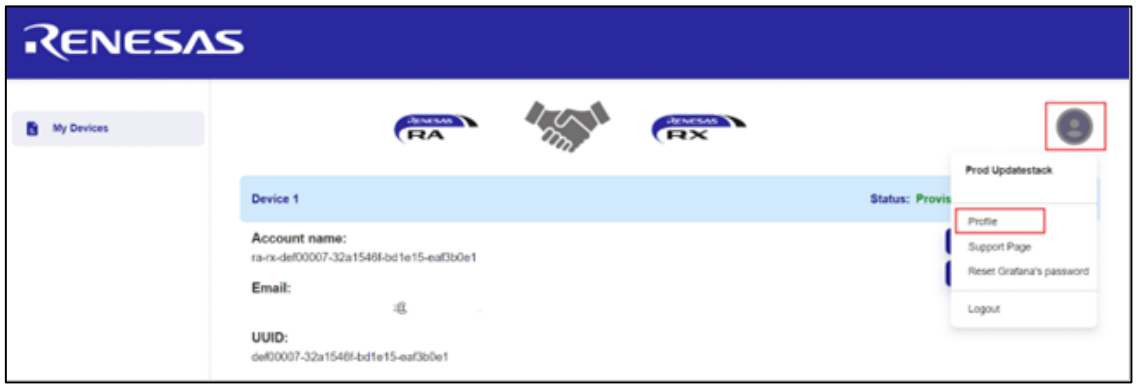

Figure 20. Selecting Profile

2. You are redirected to the Profile page.

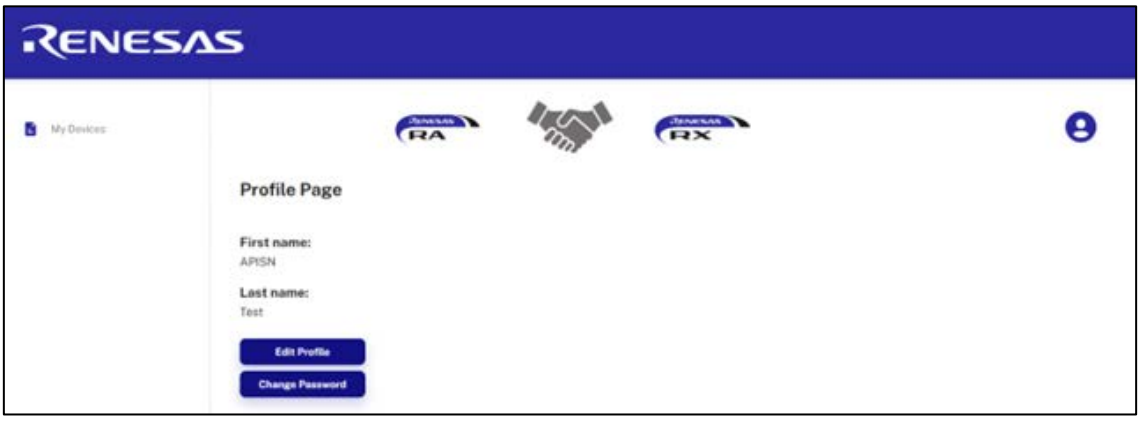

Figure 21. Profile Page

On the page you can edit your profile:

A. Press on the button Edit Profile.
B. Change your First name and Last name.
C. Press on the button Send.
D. Your Account Name is updated.

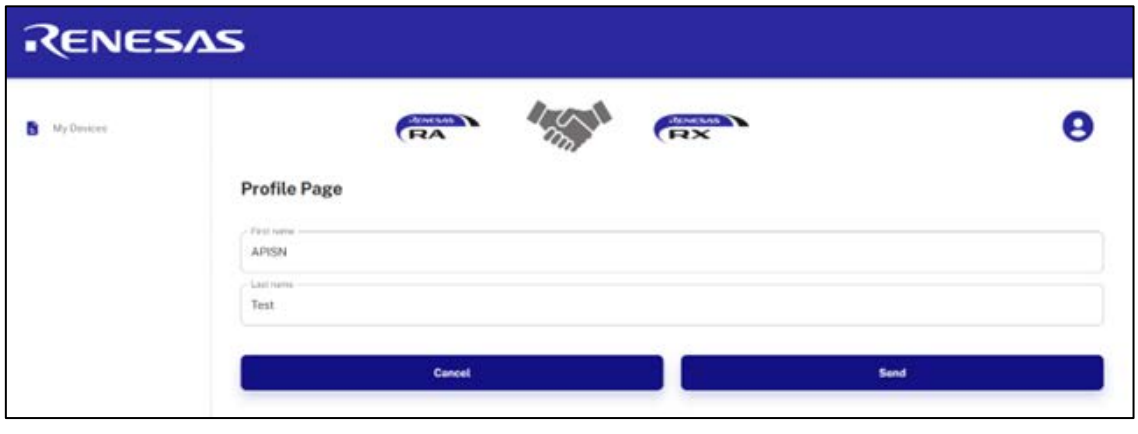

Figure 22. Updated Profile Page

Also, you can change your password, the rules for a valid password have been mentioned above:

A. Press on the button Change Password.
B. Enter your Old Password.
C. Enter your New Password.
D. Confirm your New Password and press the button Send.
E. Your password is updated.

Figure 23. Changing Password on Profile Page

2.5.5 Support page

To see your support page:
Click on your user's picture - top right. Select Support page.

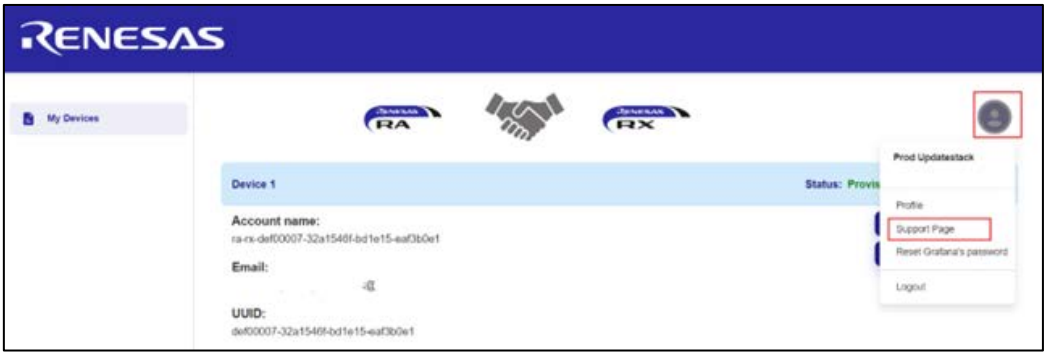

Figure 24. Selecting Support Page

Figure 25. Support Page

2.5.6 AWS Invitation Letter

Wait for 'Invitation to join AWS Single sign-on' email to activate the account. It could take up to 10 min to receive this email. Accept the invitation. **Please, pay attention this invitation will expire in 7 days.**

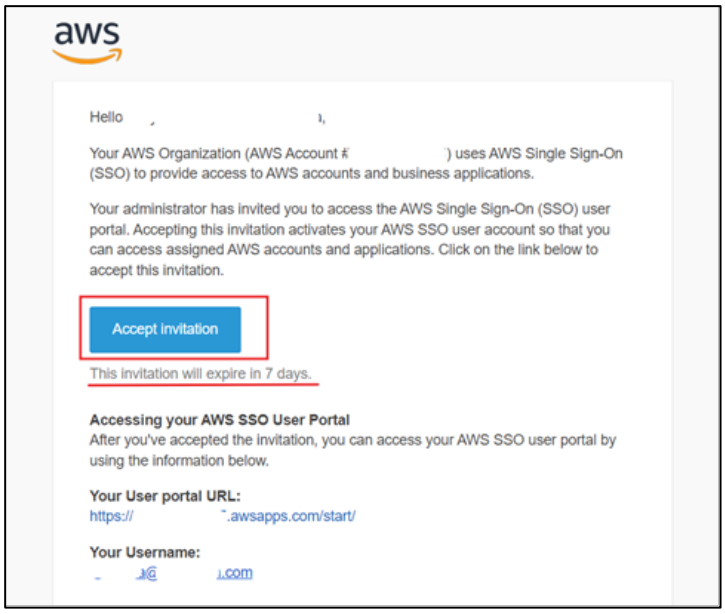

Figure 26. AWS Invitation Letter

Note: Save the invitation email for future, it may be required to access the AWS account.

2.5.7 AWS Sign up and Sign in

After accepting the invitation, you are redirected to AWS Sign up page:

1. Enter a new password and confirm.
2. Click the button Set new password.

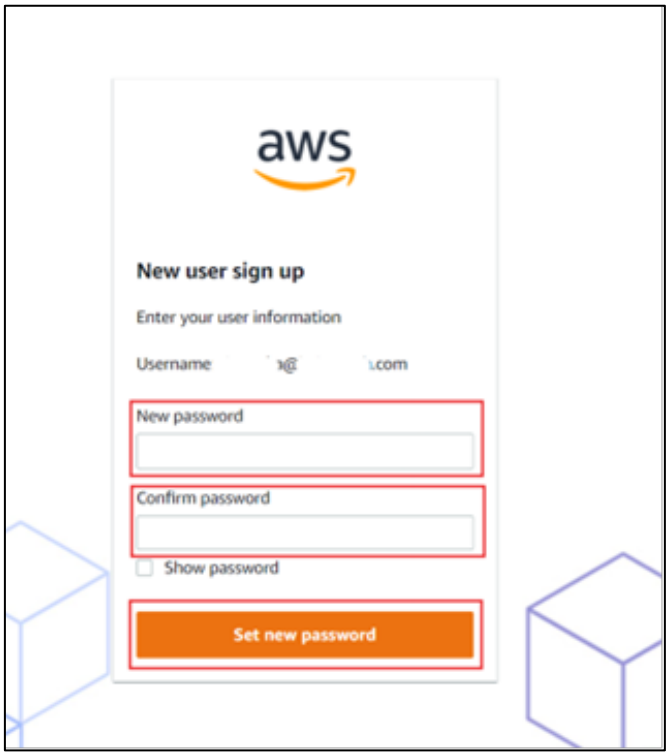

Figure 27. AWS Sign up Page

3. You are redirected to the **AWS Sign in** page.
4. Enter your username and Press on the button **Next**. **Please, pay attention our username is mentioned in the invitation letter**.

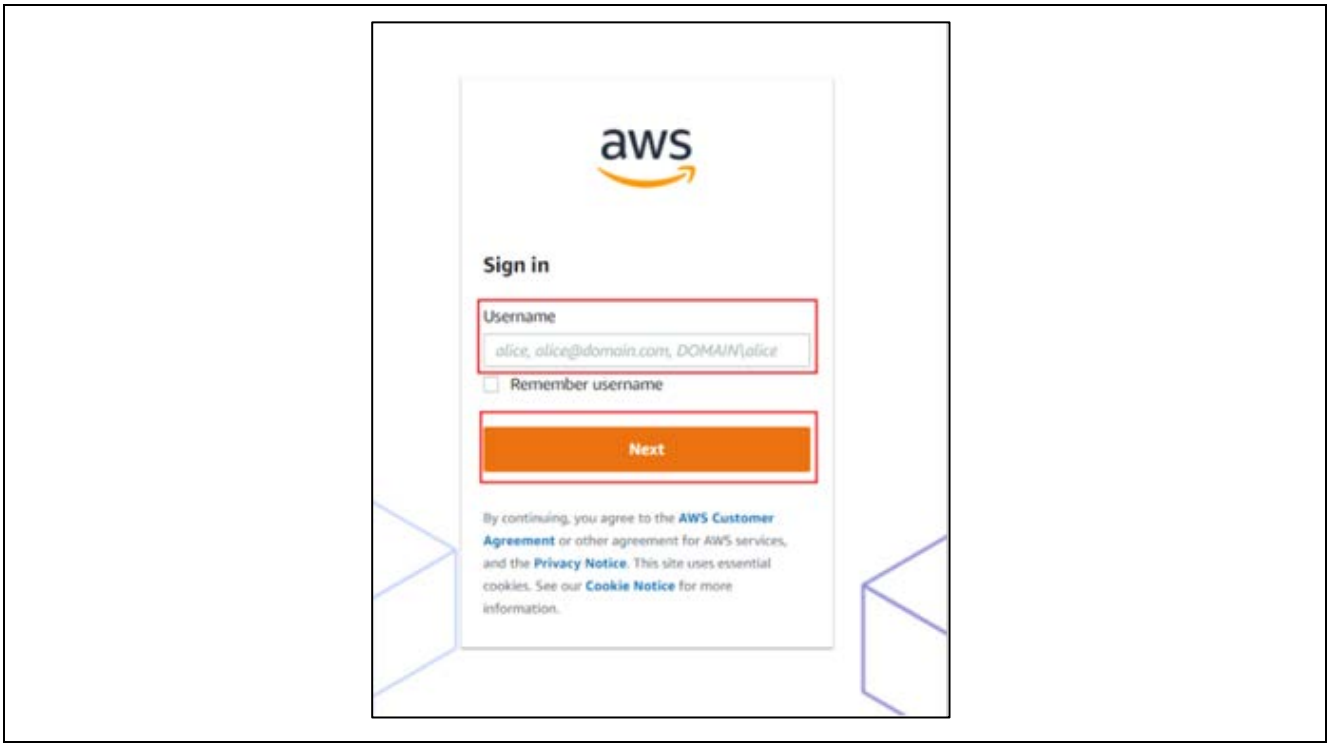

Figure 28. Entering Username

5. Enter your password and press on the button **Sign in**.

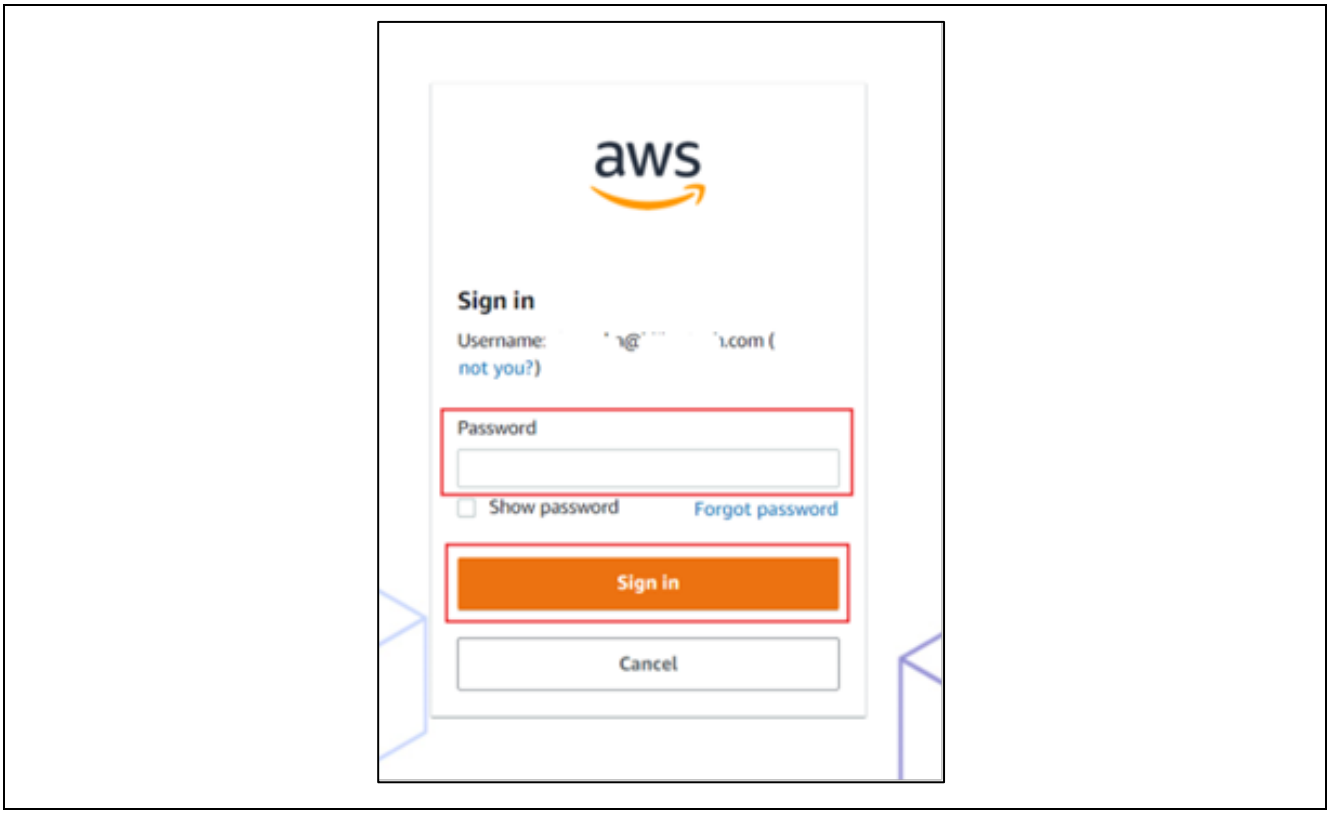

Figure 29. Signing into AWS

2.5.8 Single Sign-On

After login you are redirected to **Single Sign-On** page:

A. Click on AWS Account.
B. Click on your Account Name.
C. You can enter your AWS sub account by clicking on the Management console link.

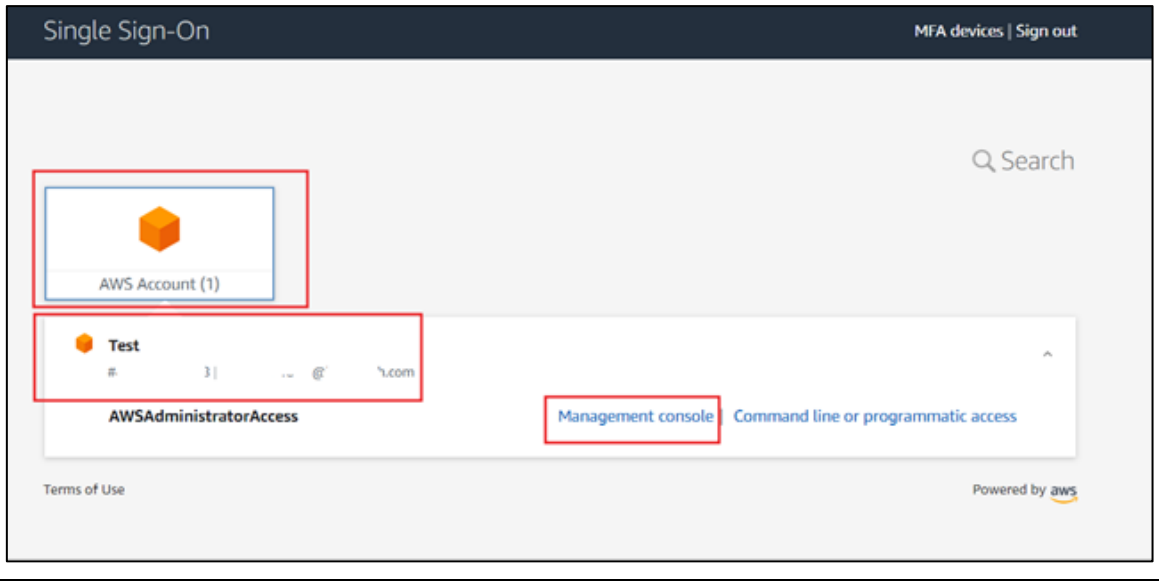

Figure 30. Single Sign-On Page

2.5.9 Sub Account Policy

After the sub account is provisioned, the following AWS resources will be available to you:

- EC2
- IoT Core
- S3
- Billing Dashboard

2.5.10 Downloading the Certificate

Click on the **Download Certificate** button to download the credentials, **certs.zip** file.

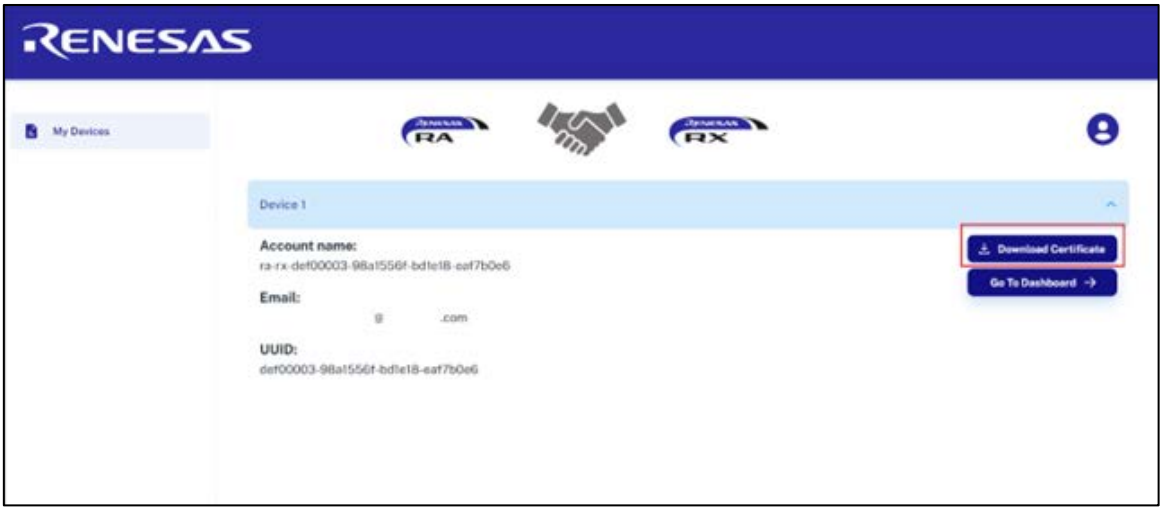

Figure 31. Downloading the Certificate

2.6 Storing the Device Certificate, Key, MQTT Broker Endpoint, and IoT Thing Name

Device Certificate, Device Private Key, MQTT Broker Endpoint, and IOT Thing name need to be stored in the data flash for the application to work.

1. Press **2** on the **Main Menu** to display **Data Flash** related commands as shown in the following screenshots. This sub menu has commands to store, read, and validate the data.

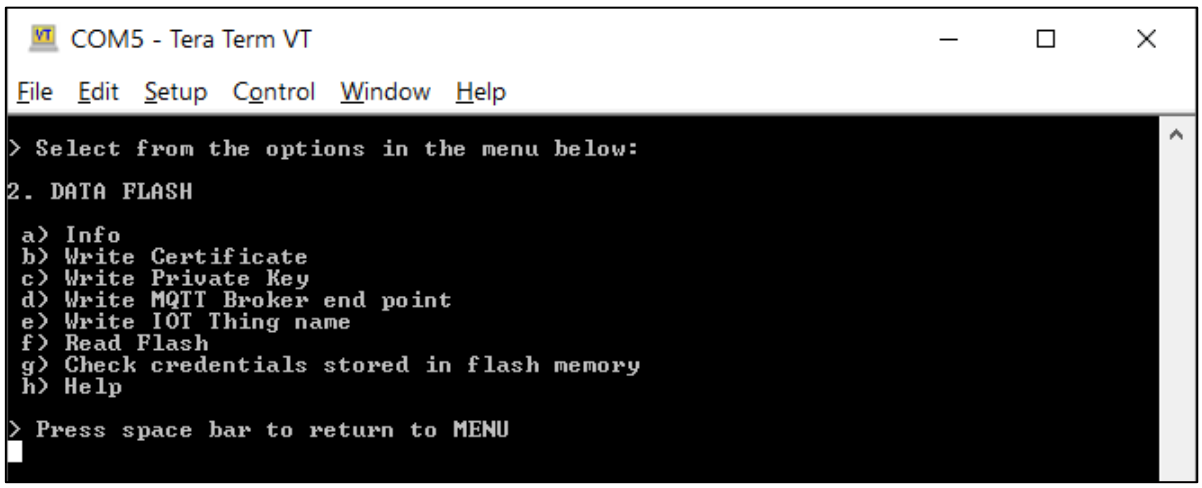

Figure 32. Data Flash related Menu and Commands

2. To store the **Device Certificate**, press the option **b** and Click the **File** tab of the Tera Term and **Send File** option and choose the device certificate file '`xxxxxcertificate.pem.crt`' from the downloaded `certs.zip` file in section 2.5.10.

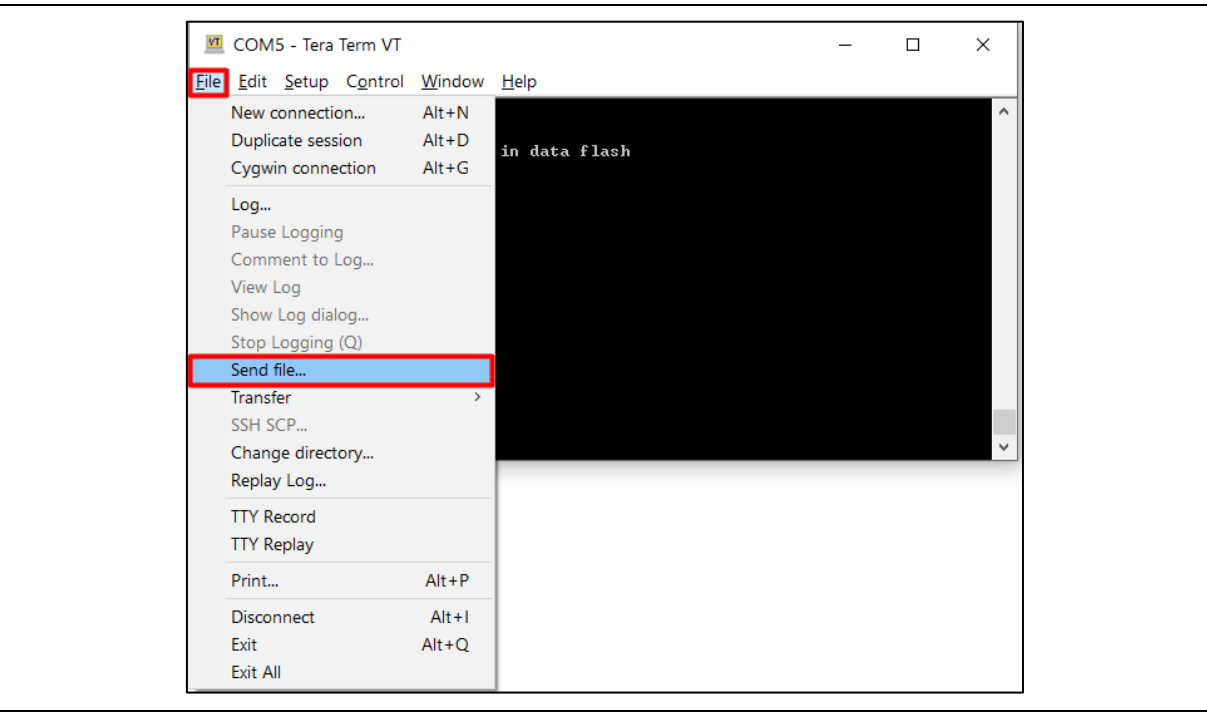

Figure 33. Accessing the Device Certificate

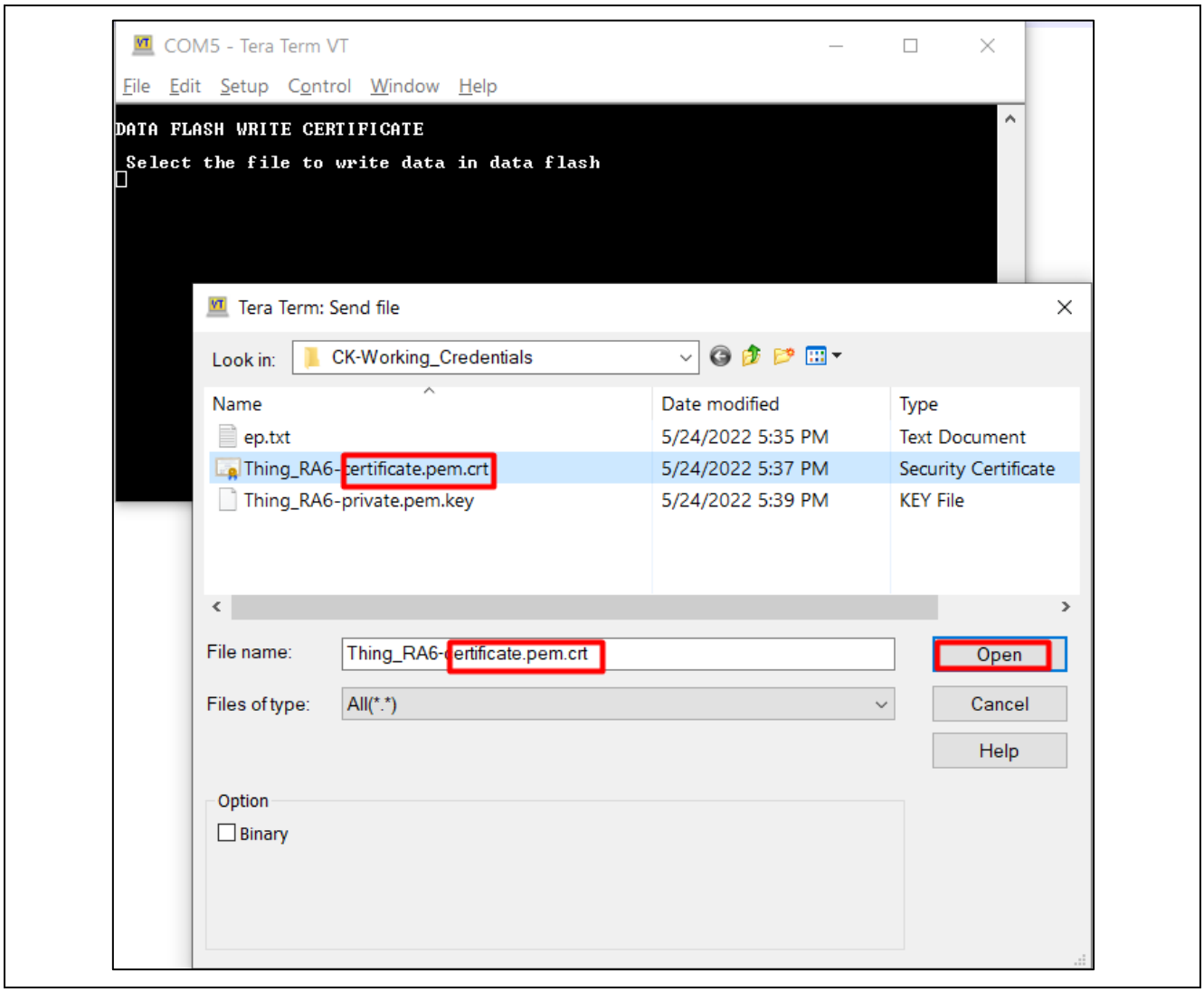

Figure 34. Downloading the Device Certificate into the Data Flash

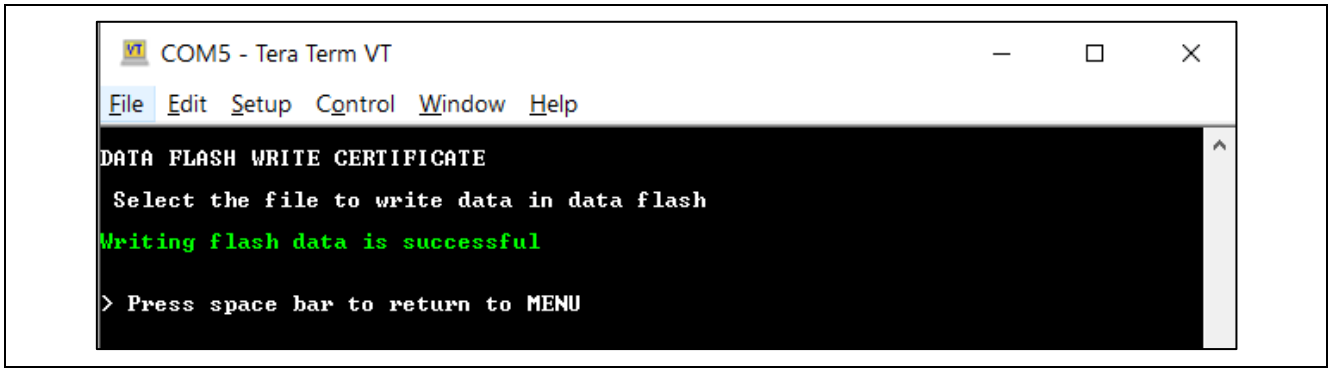

Figure 35. Status of the Downloaded Device Certificate into the Data Flash

3. To store the **Device Key,** press option **c** and click the **File** tab of the Tera Term. Select the **Send File** option and choose the Device Key "`xxxxxxxprivate.pem.key`" from the downloaded **certs.zip** file in section 2.5.10.
4. To store the MQTT Broker end point**,** copy the end point string `xxxxxxxxxx3ku-ats.iot.us-east-1.amazonaws.com` from the **iot-json.dat** file in **certs.zip** file. Press option **d** and click the **Edit** tab of the Tera Term and **Paste<CR>**. Verify and confirm the valid string and press **OK.**
   Note: Make sure to NOT copy the double quotes when copying the MQTT Broker end point.

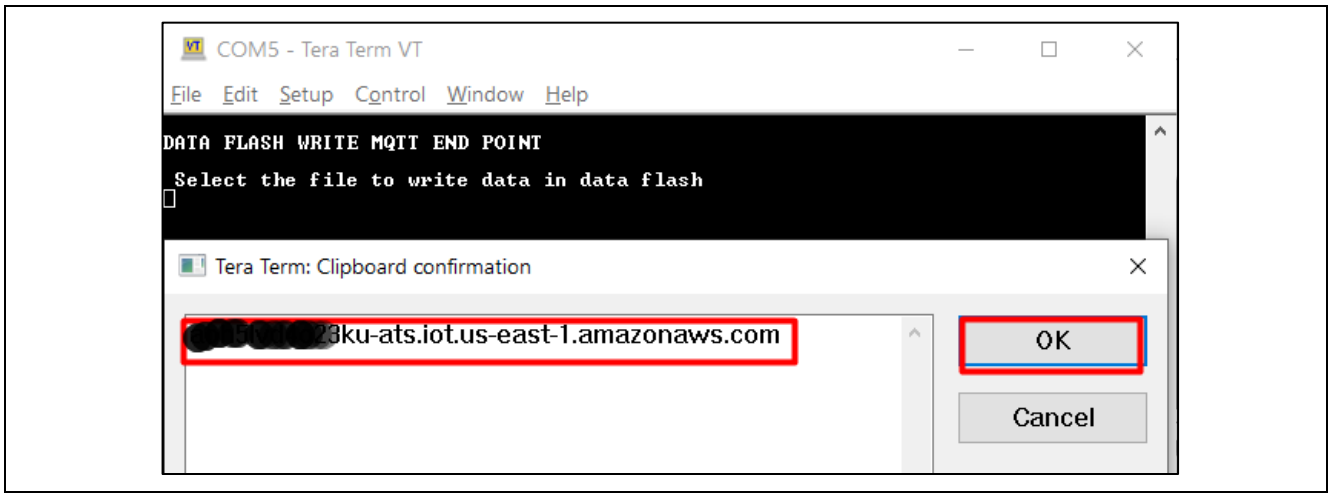

Figure 36. Storing the MQTT Endpoint into the Data Flash

5. To store the IOT Thing Name, copy the Thing Name string xxxxxxxx-5736xxxx-xxxxxxxx-4e4bxxxx from the **iot-json.dat** file in **certs.zip** file in section 2.5.10. Press option **e** and click the **Edit"** tab of the Tera Term and **Paste<CR>**. Verify and confirm the valid string and press **OK.**
   Note: Make sure to NOT copy the double quotes when copying the Thing Name.

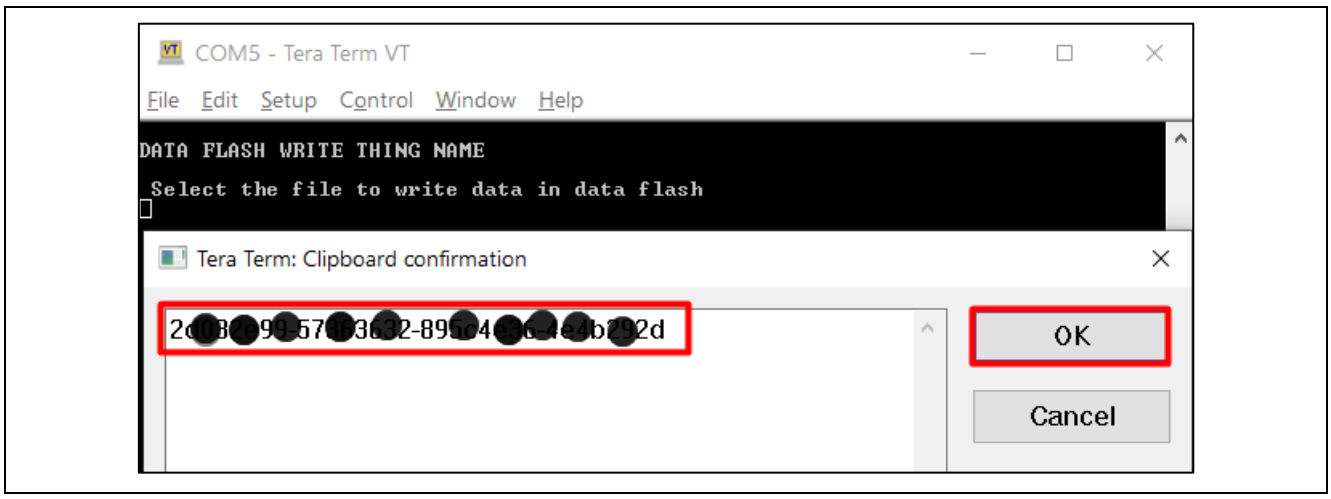

Figure 37. Storing the MQTT Endpoint into the Data Flash

6. Press option **f** and **g** to read and validate the stored information in the data flash. Press the space bar to go to the previous menu.

   Note: Validation of the stored data is very limited and validates minimum set of data points. Users are required to input the valid data to the flash obtained from the Dashboard for the proper working of the application.

2.7 IoT Cloud Configuration and Connecting to AWS IoT

Sign in to Renesas AWS dashboard at https://renesas.cloud-ra-rx.com/login using an email account that has NOT signed up for AWS account previously.

Note: It is important to sign up with an email that is not used previously to open an AWS account since the dashboard creates a new AWS account linked to the email address.

Note: Store the invitation email for future, it may be required to access the AWS account.

Note: For Ethernet Applications, firewalls in the network may prevent connectivity to AWS IoT. Configure the network to allow access to the MQTT Port 8883.

2.8 Starting the Application

After activating the SIM card, registering to the Dashboard, and configuring the required Cloud credentials via the CLI, the application is ready to run. Press option **6** to start the application. The application prints a Welcome screen along with the status of validating the Cloud credentials data present in the data flash as shown below.

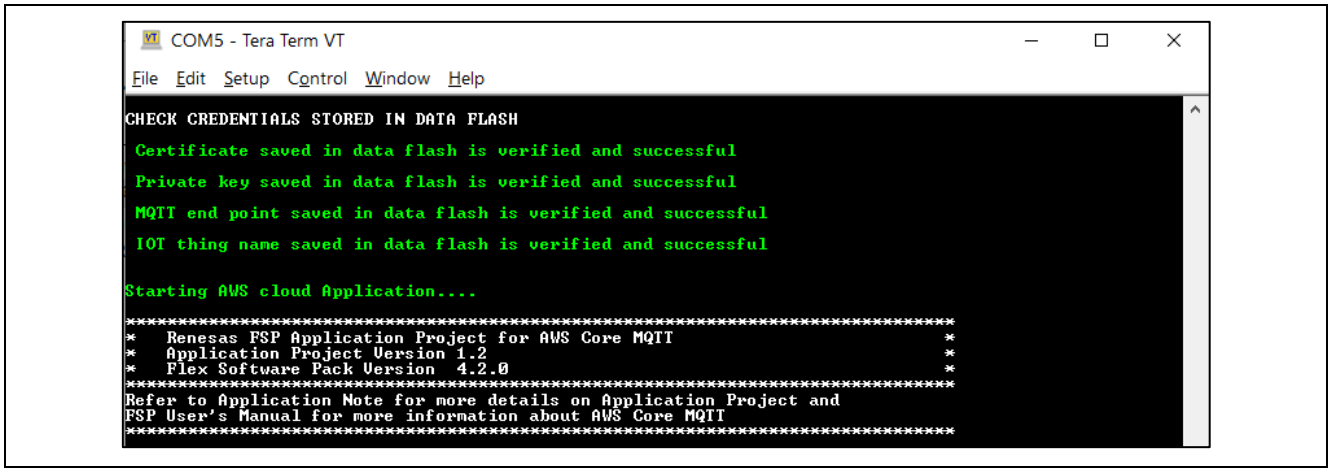

Figure 38. Welcome Screen on the Console

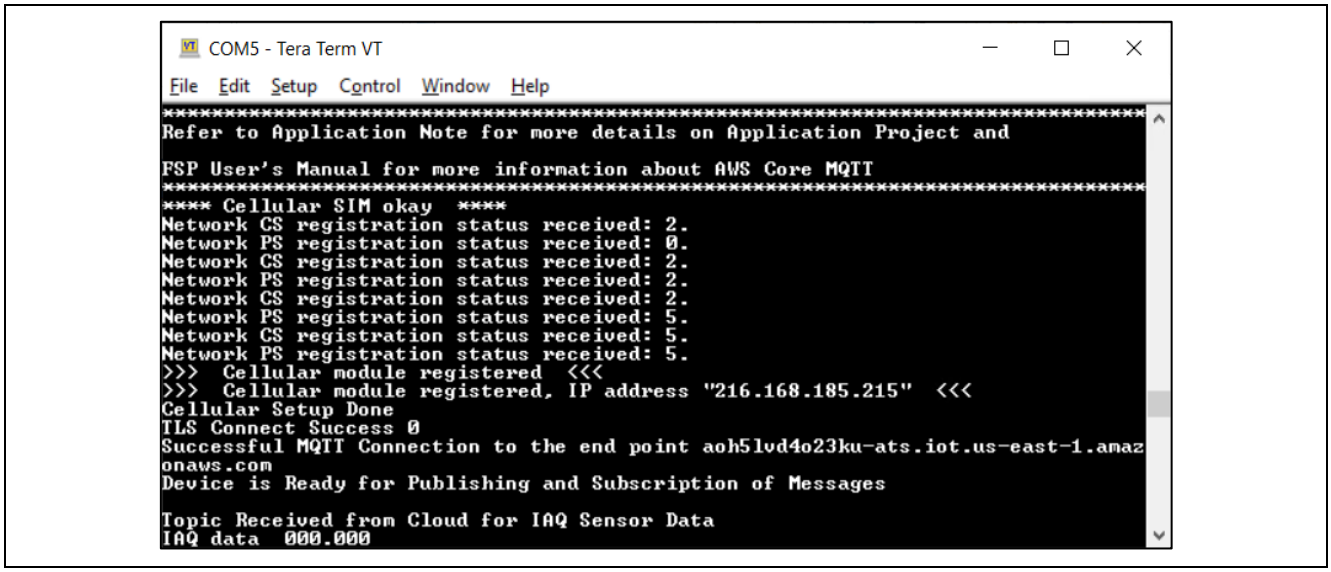

Figure 39. Connecting to the Network and AWS IoT

2.9 Verifying the Application Project from the Renesas Dashboard

Renesas AWS dashboard can be accessed from renesas.cloud-ra-rx.com by clicking on **Go to Dashboard**.

Note: Users will have access to Grafana dashboard only when the device is provisioned, and the device status is "Active".

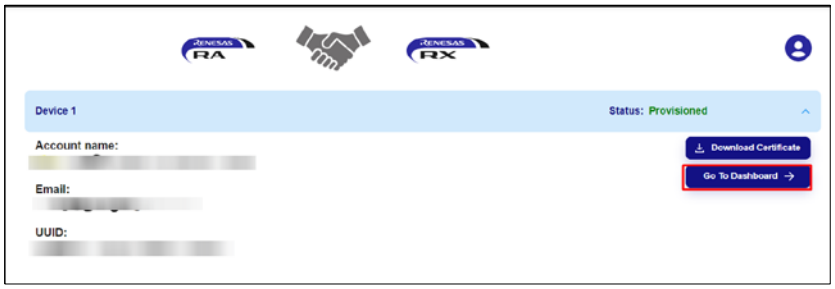

Figure 40. Accessing Renesas AWS Cloud Dashboard

First time users will access the dashboard with credentials **“admin” for both username and password** and will be directed to change the password.

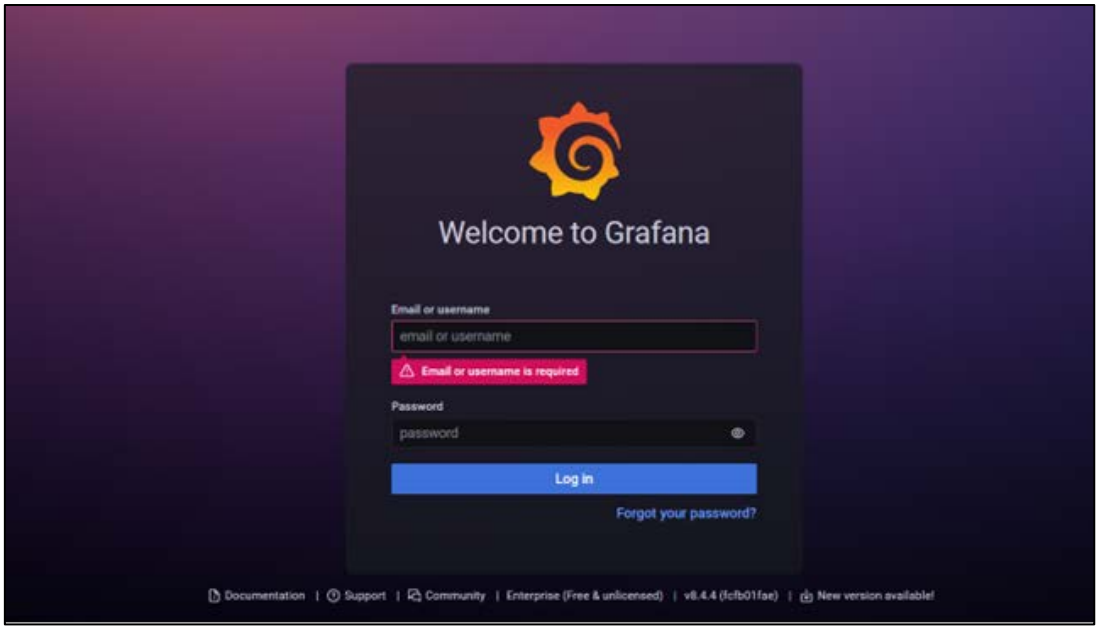

Figure 41. Welcome to Grafana Screen

Click **Skip** to access the dashboard.

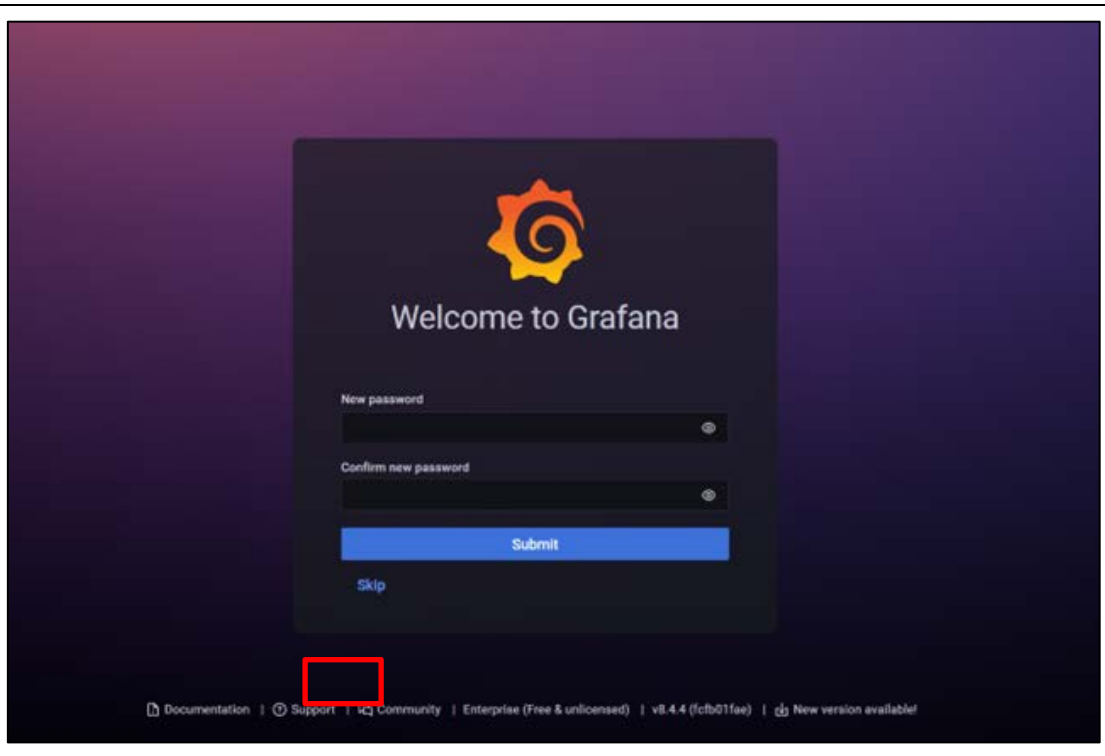

Figure 42. Skipping Grafana Screen to Access Dashboard

On the Renesas dashboard page, the sensors data can be viewed by clicking on the “arrow” next to each of the sensor data tabs. Allow up to 60 seconds for the data to be displayed on the dashboard. If the data is not updated as expected, refresh the page.

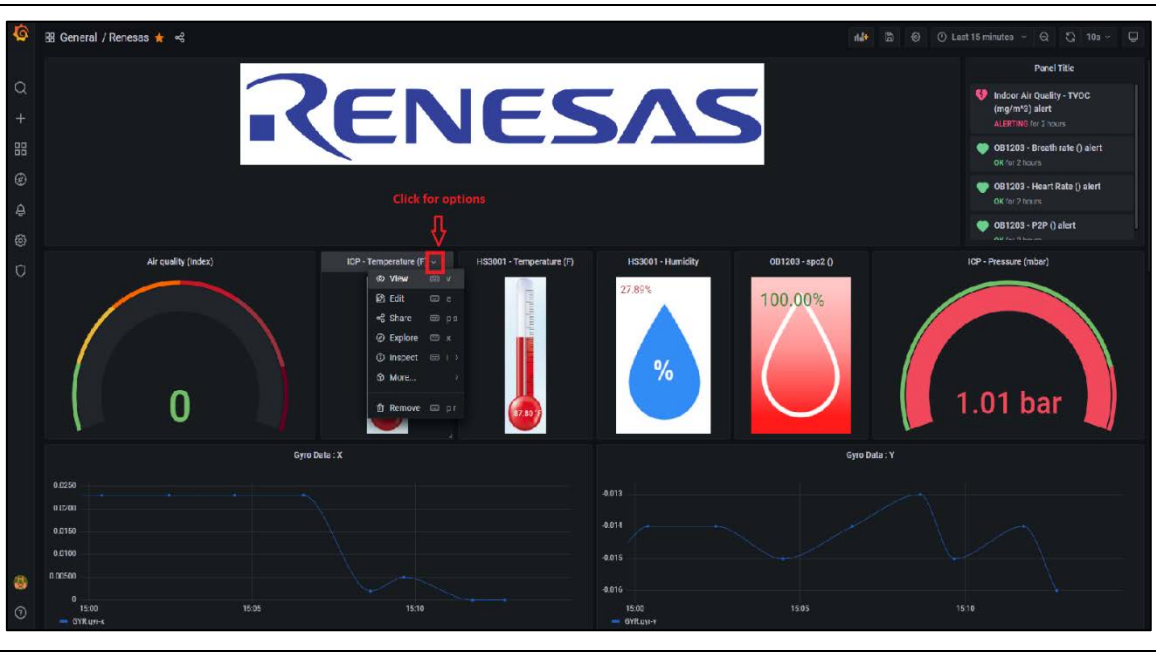

Figure 43. Renesas AWS Cloud Dashboard

3. Dashboard Types

Depending on the sensors, you can choose one of the dashboard types: Renesas 9-Axis sensor or Renesas. Click on **Renesas** option.

Figure 44. Renesas AWS Cloud Dashboard Types

Choose Renesas 9-Axis sensor.

Figure 45. Renesas 9-Axis Sensor

4. Sensor Data for Cloud Kits

The Grafana dashboard displays the following Data from sensors:

Table 1. Sensor Data from Grafana Dashboard

Sensor	Data
HS3001- Humidity and Temperature Sensor	Temperature, F
	Humidity, %
ZMOD4410- Indoor Air Quality Sensor	Etoh, ppm
	ECO2- Estimated Carbon dioxide, ppm
	TVOC - Total Organic Compounds, mg/m^3
OB1203 - Heart Rate, Blood Oxygen Concentration, Pulse Oximetry, Proximity, Light and Color Sensor	SPO2, %
	HR(Heart Rate), bpm(beats per minute)
	RR (Respiration Rate), breaths per minute
	P2P
ICP-10101 - Barometric Pressure and Temperature Sensor	Temperature, F
	Barometric Pressure, mbar
ICM-20948 Motion Tracking Sensor	Acc values, unit: g
	Gyro Data, unit: dps (degrees per sec)
	Mag Data, unit: mT
OAQ – Outdoor Air Quality	OAQ, ppm

5. Alerting and Anomaly Detection

Grafana alerts are a way to send notifications when a metric crosses a threshold that has been configured. By default, the dashboard has thresholds for the following sensors:

- OB1203-SPO2: SPO2 above 90, SPO2 below 90
- HS3001 - Temperature, F:
  - Temperature – Cold: below 65
  - Temperature – Warm: within range from 65 to 85
  - Temperature – Hot: above 85

Figure 46. Sensor Status Feedback

Sensor status feedback is sent to the device which is indicated by the LEDs.

6. Renesas AWS Dashboard

For further details on Renesas AWS dashboard types, dashboard quarantine and activation, and dashboard customization, refer to AWS Dashboard for CK-RA6M5 and CK-RX65N Application Note.

7. Sensor Stabilization Time

Table 2. Sensor Stabilization Time

Sensor Name	When Powered Up First Time	After Soft or Hard Reset
ZMOD4410 IAQ	Up to one hour	Up to one minute
ZMOD4510 OAQ	Up to 24 hours	Up to two hours
OB1203	Up to one minute (after placing a finger on the sensor, it may take up to 60 seconds to sense data)	Up to 10 seconds (after placing a finger on the sensor, it may take up to 60 seconds to sense data)
HS3001	Up to one minute	Up to 10 seconds
ICP	Up to one minute	Up to 10 seconds
ICM	Up to one minute	Up to 10 seconds

Note: Stabilization time of sensor provided above is from the point of sensor initialized.

8. Known Issues

- This section talks about the known FSP and tool related issues. More details can be found at the link: https://github.com/renesas/fsp/issues.
- Dashboard with Microsoft edge browser does not work properly with Google Chrome browser.

9. Debugging

Enable the **USR_LOG_LVL (LOG_DEBUG)** macro in the application project for additional information for debugging.

9.1 SIM Card Activation Problem

- If the SIM activation fails, verify that the ICCID number and PUK numbers are correctly entered when activating the SIM card on Truphone IoT SIM activation platform truphone.com/connectit
- If **Menu 5 Validate SIM activation** PING response returns a Ping Failed condition, it can take up to 15 minutes or longer for the card to be activated after performing **Activating the SIM Card** to obtain LTE Network access. In this case, wait at least 15 minutes (or longer) and repeat **Menu 5 Validate SIM activation**.
- SIM cards cannot be activated more than once. To verify whether the SIM card has already been activated, please monitor and manage your SIMs on the Truphone IoT Connectivity Management Platform or contact Truphone support through iot.truphone.com by logging into your account.
- If **Menu 5 Validate SIM activation** PING response continues to return Ping Failed condition, first check the external antenna is connected securely to the RYZ014A PMOD and try again. The CSQ Network Signal Quality (RSSI) could be too low to connect. If the RSSI is 99 then check external antenna is connected. It may be possible that no Cell Network Signal could be detected in your area. An RSSI reading with RSSI = 15 or less indicates marginal or poor reception.

  CSQ Network Signal Quality (RSSI) [99 = No Cell Signal] = 15, Marginal Signal Quality

  It may be necessary to move the CK-RA6M5 with PMOD to a different location to improve the Network Signal Quality (RSSI) to get an RSSI value in the range of 16 to 98.
- If **Menu 5 Validate SIM activation** continues to fail, verify that the APN is set for the Global Region where the RYZ014A PMOD is trying to connect. The APN setting and LTE Band List depends on your Global Region and the SIM card provider.

  `To set the Access Point Name (APN) for SIM Card provider other than Truphone`

  The APN is set in the Application project in `/src/cellular_setup.c`

  See `#define CELLULAR_APN "iot.truphone.com"  /* APN : Truphone SIM Card */`

- For all other SIM card issues that cannot be resolved with these troubleshooting steps, contact Truphone support through iot.truphone.com by logging into your account.

10. Troubleshooting

To validate the functionality of the sensor data, run the Quick Start Example Project as described in the *CK-RA6M5 Quick Start Guide*.

Website and Support

Visit the following vanity URLs to learn about key elements of the RA family, download components and related documentation, and get support.

CK-RA6M5 Kit Information	renesas.com/ra/ck-ra6m5
RA Cloud Solutions	renesas.com/cloudsolutions
RA Product Information	renesas.com/ra
RA Product Support Forum	renesas.com/ra/forum
RA Flexible Software Package	renesas.com/FSP
Renesas Support	renesas.com/support

Revision History

Rev.	Date	Description	
		Page	Summary
1.00	Mar.15.23	—	Initial release
1.01	May.08.23	—	Added support for FSP v4.4.0.

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/.