Renesas RA Family

RA MQTT/TLS Azure Cloud Connectivity Solution - Cellular

Introduction

This application note describes IoT Cloud connectivity solutions in general and introduces you briefly to the IoT Cloud solution provider, Microsoft Azure. It covers the RA FSP MQTT/TLS module along with the Azure IoT SDK for embedded C, using Cellular connectivity.

This application project is built with the integrated Embedded Wireless Framework (EWF) and "Azure IoT SDK for Embedded C" package which allows small embedded (IoT) devices like Renesas RA family of MCUs RA6M3/RA6M4/RA6M5 to communicate with Azure IoT services.

The application example uses Azure IoT DPS (Device Provisioning Service) to provision, register the IoT device, and send and receive data to and from the development kit.

This application note enables you to effectively use the RA FSP modules in your own design with the FSP integrated Azure IoT SDK. Upon completion of this guide, you will be able to add the FSP modules to your own design, configure it correctly with Azure IoT SDK for the target application, and write code using the included application example code as a reference and efficient starting point. References to more detailed API descriptions and sample code, that demonstrates advanced usage of FSP modules are available in the *RA FSP Software Package (FSP) User's Manual* (see Next Steps and References section) and serve as valuable resources in creating more complex designs. Explaining the underlying operation of Azure IoT SDK for Embedded C is beyond the scope of this document. Users should refer to the documentation from Microsoft for education on topics related to Azure IoT SDK section: https://docs.microsoft.com/en-us/azure/iot-hub/iot-hub-devguide- sdks

In this release, the CK-RA6M5 kit is used for the application project.

Required Resources

To build and run the MQTT/TLS application example, you need:

Development Tools and Software

- e² studio version: v2023.4.0 or later
- RA Flexible Software Package (FSP) v4.4.0
- SEGGER J-Link® RTT viewer version: 7.84 or later
- Azure IoT explorer 0.14.13.0 or later (PC tool for validating the Cloud side). Download Link : Releases · Azure/azure-iot-explorer (github.com)
- Azure CLI 2.44 or later (Azure command-line interface is a set of commands used to create and manage Azure resources) Download Link: How to install the Azure CLI | Microsoft Learn
- Access to Azure Cloud Connectivity Portal (https://portal.azure.com/#home) to create IoT Devices (If you are new to Azure IoT)

Hardware

- Renesas CK-RA6M5 kit (CK-RA6M5 - Cloud Kit Based on RA6M5 MCU Group | Renesas)
- PC running Windows® 10, Tera Term console or similar application, and an installed web browser (Google Chrome, Internet Explorer, Microsoft Edge, Mozilla Firefox, or Safari).
- Micro USB cables
- Renesas LTE Cat-M1 Cellular IoT Module (Included in the CK-RA6M5 Kit) (RYZ014A - LTE Cat-M1 Cellular IoT Module | Renesas)

Prerequisites and Intended Audience

This application note assumes that you have some experience with the Renesas e^2 studio ISDE and RA FSP 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 e^2 studio and the FSP, and also validates that the debug connection to your board functions properly. In addition, this application note assumes you have some knowledge of MQTT/TLS and its communication protocols.

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: If you are new to Azure Internet of Things, we recommend you get started with Introduction the Azure IoT https://docs.microsoft.com/en-us/azure/iot-fundamentals/iot-introduction

Prerequisites

- Access to online documentation available for Azure in the Cloud Connectivity under References sections 5 and 6
- Access to latest documentation for identified Renesas FSP as referenced sections 5 and 6
- Prior knowledge of operating e^2 studio and built-in (or standalone) RA Configurator
- Access to associated hardware documentation such as User Manuals and Schematics

Using this Application Note

Section 1 of this document covers the General Overview of the Cloud Connectivity, Azure IoT Solution using IoT Central, and Azure DPS, MQTT and TLS Protocols and Device certificates and Keys used in the Cloud Connectivity.

Section 2 covers the modules provided by RA FSP to establish connectivity to Cloud service providers and the features supported by the module.

Section 3 covers the architecture of the reference application project, an overview of the software components included, and step-by-step guidelines for recreation using the FSP configurator. It also covers setting up the Azure IoT Hub, creating the self-signed certificates, storing the certificates in the flash using the application CLI.

Sections 4 covers Importing, building and running the Application project.

Note: We recommend that you operate with your own Microsoft Azure Cloud credentials and use your created Cloud configurations to run the application. The default sample configuration detailed in this project is for reference only and may have access issues to Azure since the application is communicating with a test account.

Note: For a quick validation using the provided application project, you can skip sections 1 to 2 and go to section 3 and 4 for instructions on setting up the Azure IoT Hub, creating the self-signed certificates, storing the certificates in the flash using the application CLI, and running the application project on the CK-RA6M5 board.

Contents

1. Introduction to Cloud Connectivity....4
1.1 Cloud Connectivity Overview 4
1.2 Microsoft Azure IoT Solution 5
1.2.1 Overview.... 5
1.2.2 IoT Hub and Device Provisioning Service 5
1.2.2.1 Azure IoT Hub and IoT Hub Device Provisioning Service (DPS) 5

1.2.3 Authentication Methods 6
1.2.3.1 X.509 6
1.2.3.2 Per-Device Key Authentication 6
1.3 MQTT Protocol Overview 7
1.4 TLS Protocol Overview 7
1.4.1 Device Certificates and Keys 8
1.4.2 Device Security Recommendations 8

2. RA FSP MQTT/TLS Cloud Solution 9
2.1 MQTT Client Module Introduction 9
2.1.1 Design Considerations 9
2.1.2 Supported Features 9
2.2 TLS Session Module Introduction 9
2.2.1 Design Considerations 9
2.2.2 Supported Features 10
2.3 Azure IoT Device SDK Module Introduction 10
2.3.1 Design Considerations 10
2.3.2 Supported Features 10

3. MQTT/TLS Application Example 11
3.1 Application Overview 11
3.2 Creating the Application Project using the FSP configurator 16
3.3 Install Azure CLI 24
3.4 Create an IoT Hub 25
3.5 Certificate Creation Process 27
3.6 View Device Properties 31
3.7 Set IoT Hub 32
3.8 Register an IoT Hub Device 35
3.9 Prepare the Device 36
3.10 Building and Running the Application 37
3.11 Download and Run the Project 37
3.12 Activating the SIM card 41
3.13 Storing Device Certificate, Host Name, Device ID 42
3.14 Send Device to Cloud Message 47
3.15 Send Cloud-to-Device Message 47

4. Importing, Building and Loading the Project 48
4.1 Importing 49
4.2 Building the Latest Executable Binary 49
4.3 Loading the Executable Binary into the Target MCU 49
4.3.1 Using a Debugging Interface with e^2 studio 49
4.3.2 Using J-Link Tools 49

4.3.3 Using Renesas Flash Programmer 49

5. Next Steps and References 49

6. MQTT/TLS References 49

7. Known Issues and Limitations 49

7.1 SIM Card Activation Problem 50

8. Website and Support 50

Revision History 51

1. Introduction to Cloud Connectivity

1.1 Cloud Connectivity Overview

Internet of Things (IoT) is a sprawling set of technologies described as connecting everyday objects, like sensors or smartphones, to the World Wide Web. IoT devices are intelligently linked together to enable newforms of communication between things and people, and among things.

These devices, or things, connect to the network. Using sensors, they provide the information they gather from the environment or allow other systems to reach out and act on the world through actuators. In the process, IoT devices generate massive amounts of data, and Cloud computing provides a pathway, enabling data to travel to its destination.

The IoT Cloud Connectivity Solution includes the following major components:

1. Devices or Sensors
2. Gateway
3. IoT Cloud services
4. End user application/system

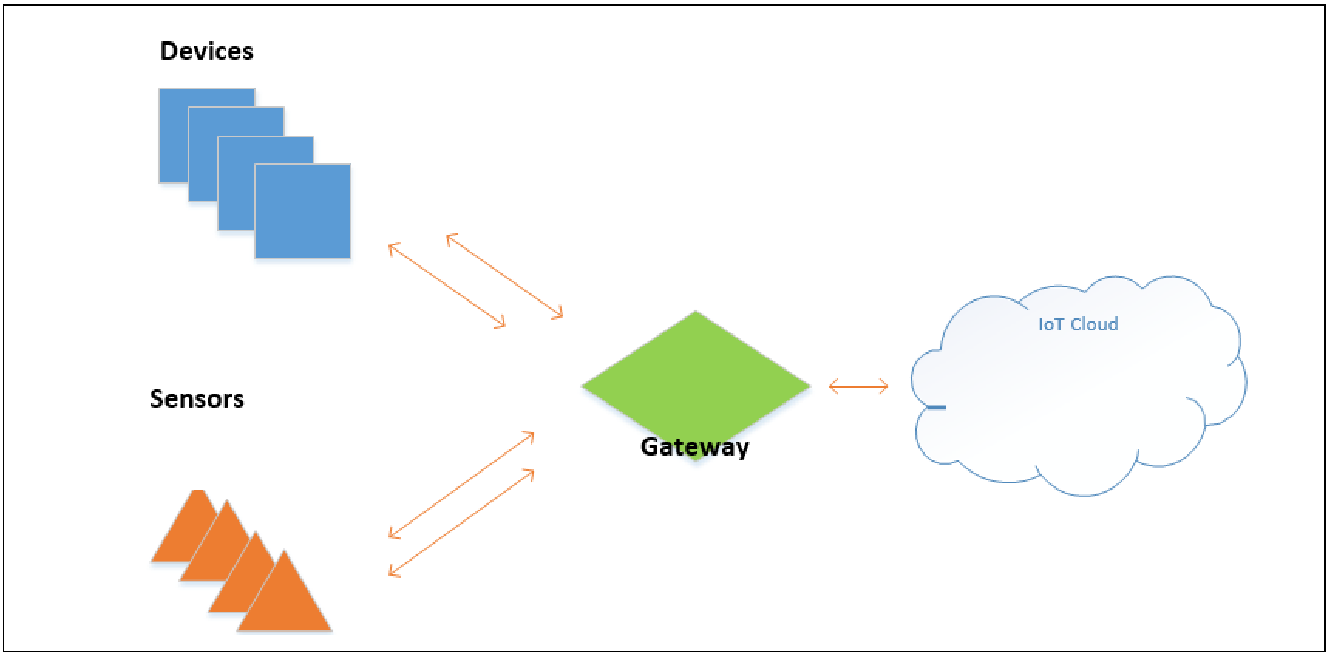

Figure 1. IoT Cloud Connectivity Architecture

Devices or Sensors

A device includes hardware and software that interacts directly with the world. Devices connect to a network to communicate with each other, or to centralized applications. Devices may connect to the Internet either directly or indirectly.

Gateway

A gateway enables devices that are not directly connected to the Internet to reach Cloud services. The data from each device is sent to the Cloud Platform, where it is processed and combined with data from other devices, and potentially with other business-transactional data. Most of the common communication gateways support one or more communication technologies such as Wi-Fi, Ethernet, or Cellular to connect to the IoT Cloud Service provider.

IoT Cloud

Many IoT devices produce lots of data. You need an efficient, scalable, affordable way to manage those devices, handle all that information, and make it work for you. When it comes to storing, processing, and analyzing data, especially big data, it is hard to surpass the Cloud.

1.2 Microsoft Azure IoT Solution

1.2.1 Overview

Microsoft's end-to-end IoT platform is a complete IoT offering so that enterprises can build and realize value from IoT solutions quickly and efficiently. Azure IoT Central solutions are used with backend support from the Azure IoT Hub Device Provisioning Service.

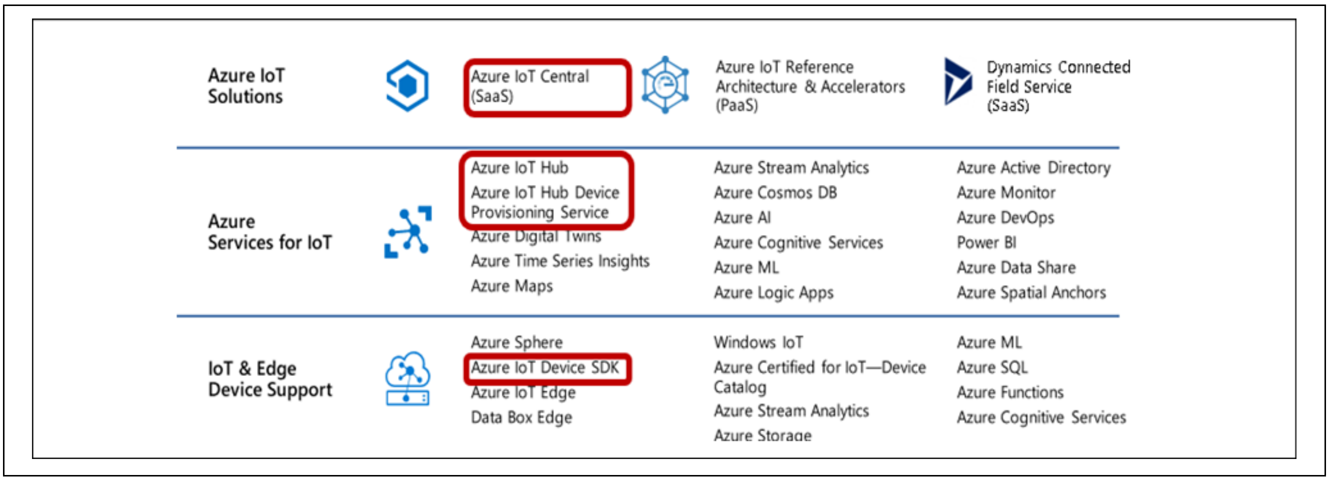

Figure 2. Microsoft Azure IoT Cloud Solution

1.2.2 IoT Hub and Device Provisioning Service

1.2.2.1 Azure IoT Hub and IoT Hub Device Provisioning Service (DPS)

IoT Hub provides built-in support for the MQTT v3.1.1 protocol. See the following webpage for more understanding of the IoT Hub and Device Provisioning Services (DPS):
https://docs.microsoft.com/en-us/azure/iot-dps/

(1) Device Provisioning Service

High-level sequence of events to connect a Device to IoT Hub:

1. After the device is manufactured, the device enrollment information is added to the DPS. This is the only manual step in the process.
2. At some point afterwards, which could be a day, or it could be several months, the device goes online and connects to DPS to find its IoT solution home.
3. DPS and the device go through an attestation handshake using the device enrollment info. DPS proves the device's identity.
4. DPS registers the device to IoT hub and populates the initial desired device state.
5. IoT Hub returns the connection info for the device.
6. DPS gives the device its IoT Hub connection info.

7. The device now establishes a connection with IoT Hub and retrieves its initial configuration from IoT Hub and makes any changes/updates, as needed.
8. The device starts sending telemetry to IoT Hub.

(2) Embedded C SDK

The Embedded C SDK, the newer addition to the Azure SDKs family, was designed to allow embedded IoT devices to leverage Azure services, like device to Cloud telemetry, Cloud to device messages, direct methods, device twin, device provisioning, and IoT Plug and play, all while maintaining a minimal footprint.

It allows full control over memory allocation and the flexibility to bring your own MQTT client, TLS, and Socket layers.

Written in C, this version of the SDK is optimized to be used on small and embedded devices with limited capabilities and resources.

The Azure IoT SDK is open source and published on GitHub (https://github.com/Azure/azure-sdk-for-c). This is also distributed with FSP version 4.4.0 and above.

1.2.3 Authentication Methods

Security is a critical concern when deploying and managing IoT devices. IoT Hub offers the security features described in the following sections.

1.2.3.1 X.509

The communication path between devices and Azure IoT Hub, or between gateways and Azure IoT Hub, is secured using the industry-standard Transport Layer Security (TLS) with Azure IoT Hub, authenticated using the X.509 standard.

To protect devices from unsolicited inbound connections, Azure IoT Hub does not open any connection to the device. The device initiates all connections.

1.2.3.2 Per-Device Key Authentication

Figure 3 shows authentication in the IoT Hub using security tokens.

Figure 3. Authentication using Security Tokens

1. The device prepares a shared access signature (SAS) token using the device endpoint, device id, and primary key (generated as part of the device addition to the IoT Hub).
2. When connecting to the IoT Hub, the device presents the SAS token as the password in the MQTT CONNECT message. The username content is the combination of device endpoint and device name along with the additional Azure defined string.
3. The IoT Hub verifies the SAS token and registers the device and connection is established.
4. IoT Hub provides Symmetric key for Data encryption.

   Note: The connection is closed when the SAS token expires.

1.3 MQTT Protocol Overview

MQTT stands for **Message Queuing Telemetry Transport**. MQTT is a Client Server publish-subscribe messaging transport protocol. It is an extremely light-weight, open, simple messaging protocol, designed for constrained devices, as well as low-bandwidth, high-latency, or unreliable networks. These characteristics make it ideal for use in many situations, including constrained environments, such as communication in Machine to Machine (M2M) and IoT contexts, where a small code footprint is required, and/or network bandwidth is at a premium.

An MQTT client can publish information to other clients through a broker. A client, if interested in a topic, can subscribe to the topic through the broker. A broker is responsible for authentication and authorization of clients, as well as delivering published messages to any of its clients who subscribe to the topic. In this publisher/subscriber model, multiple clients may publish data with the same topic. A client will receive the messages published if the client subscribes to the same topic.

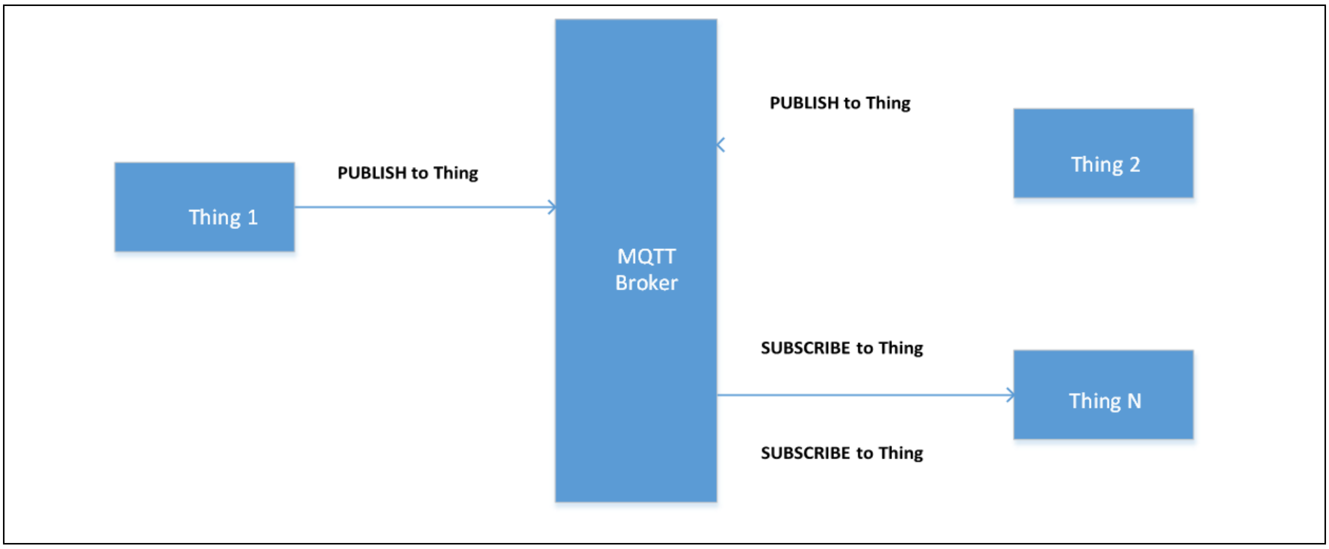

Figure 4. MQTT Client Publish/Subscribe Model

In the Pub/Sub model used by MQTT, there is no direct connection between a publisher and the subscriber.To handle the challenges of a Pub/Sub system, the MQTT generally uses quality of service (QoS) levels.

There are three QoS levels in MQTT:

- At most once (0)
- At least once (1)
- Exactly once (2)

At most once (0)

A message will not be acknowledged by the receiver or stored and redelivered by the sender.

At least once (1)

It is guaranteed that a message will be delivered at least once to the receiver. But the message can also be delivered more than once. The sender will store the message until it gets an acknowledgment in form of a PUBACK command message from the receiver.

Exactly once (2)

It guarantees that each message is received only once by the counterpart. It is the safest and the slowest QoS level.

1.4 TLS Protocol Overview

Transport Layer Security (TLS) protocol and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols that provide communications security over a computer network.

The TLS/ SSL protocol provides privacy and reliability between two communicating applications. It has the following basic properties:

Encryption: The messages exchanged between communicating applications are encrypted to ensure that the connection is private. A symmetric cryptography mechanism such as AES (Advanced Encryption Standard) is used for data encryption.

Authentication: A mechanism to check the peer's identity using certificates.

Integrity: A mechanism to detect message tampering and forgery ensures that connection is reliable. A Message Authentication Code (MAC), such as Secure Hash Algorithm (SHA), ensures message integrity.

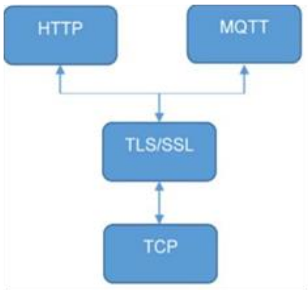

Figure 5. SSL/TLS Hierarchy

1.4.1 Device Certificates and Keys

Device certificates, public and private keys, and the ways they can be generated, are discussed in this section.

Security is a critical concern when deploying and managing IoT devices. In general, each of the IoT devices needs an identity before they can communicate with the Cloud. Digital certificates are the most common method for authenticating a remote host in TLS. Essentially, a digital certificate is a document with specific formatting that provides identity information for a device.

TLS normally uses a format called X.509, a standard developed by the International Telecommunication Union (ITU), though other formats for certificates may apply if TLS hosts can agree on a format to use. X.509 defines a specific format for certificates and various encodings that can be used to produce a digital document. Most X.509 certificates used with TLS are encoded using a variant of ASN.1, which is another telecommunication standard. Within ASN.1 there are various digital encodings, but the most common encoding for TLS certificates is the Distinguished Encoding Rules (DER) standard. DER is a simplified subset of the ASN.1.

Though DER-formatted binary certificates are used in the actual TLS protocol, they may be generated and stored in a number of different encodings, with file extensions such as `.pem`, `.crt`, and `.p12`. The most common of the alternative certificate encodings is Privacy-Enhanced Mail (PEM). The PEM format is a base-64 encoded version of the DER encoding.

Depending on your application, you may generate your own certificates, be provided certificates by a manufacturer or government organization, or purchase certificates from a commercial certificate authority.

Loading Certificates onto your Device

To use a digital certificate in your NetX™ Secure application, you must first convert your certificate into a binary DER format, and optionally convert the associated private key into a binary format, typically, a PKCS#1-formatted, DER-encoded RSA key. Once converted, it is up to you how to load the certificate and the private key on to the device. Possible options include using a flash-based file system or generating a C array from the data (using a tool such as xxd from Linux® with the -i option) and compiling the certificate and key into your application as constant data.

Once your certificate is loaded on the device, you can use the TLS API to associate your certificate with a TLS session.

1.4.2 Device Security Recommendations

The following security recommendations are not enforced by Cloud IoT Core but will help you secure your devices and connections.

- The private key of the device should be kept secret.
- Use the latest version of TLS (v1.2 or above) when communicating with IoT Cloud and verify that the server certificate is valid using trusted root certificate authorities.

- Each device should have a unique public/private key pair. If multiple devices share a single key and one of those devices is compromised, an attacker could impersonate all the devices that have been configured with that one key.
- Keep the public key secure when registering it with Cloud IoT Core. If an attacker can tamper with the public key and trick the provisioner into swapping the public key and registering the wrong public key, the attacker will subsequently be able to authenticate on behalf of the device.
- The key pair is used to authenticate the device to Cloud IoT Core and should not be used for other purpose or protocols.
- Depending on the device's ability to store keys securely, key pairs should be rotated periodically. When practical, all keys should be discarded when the device is reset.
- If your device runs an operating system, make sure you have a way to securely update it. Android Things provides a service for secure updates. For devices that don't have an operating system, ensurethat you can securely update the device's software if security vulnerabilities are discovered after deployment.

2. RA FSP MQTT/TLS Cloud Solution

2.1 MQTT Client Module Introduction

The NetX Duo MQTT Client module provides high-level APIs for a Message Queuing Telemetry Transport (MQTT) protocol-based client. The MQTT protocol works on top of TCP/IP and therefore the MQTT client is implemented on top of NetX Duo IP and NetX Duo Packet pool. NetX Duo IP attaches itself to the appropriate link layer frameworks, such as Ethernet, Wi-Fi, or Cellular.

The NetX Duo MQTT client module can be used in normal or in secure mode. In normal mode, the communication between the MQTT client and broker is not secure. In secure mode, the communication between the MQTT client and broker is secured using the TLS protocol.

2.1.1 Design Considerations

- By default, the MQTT client does not use TLS; communication is not secure between a MQTT client and broker.
- The RA FSP Azure RTOS NetX Duo IoT middleware module provides the NetX Duo TLS session block. It adds Azure RTOS NetX Secure block. This block defines/controls the common properties of NetX Secure.

2.1.2 Supported Features

NetX Duo MQTT Client supports the following features:

- Compliant with OASIS MQTT version 3.1.1 Oct 29, 2014. The specification can be found at http://mqtt.org/.
- Provides an option to enable/disable TLS for secure communication using NetX Secure in FSP.
- Supports QoS and provides the ability to choose the levels that can be selected while publishing the message.
- Internally buffers and maintains the queue of received messages.
- Provides a mechanism to register callback when a new message is received.
- Provides a mechanism to register callback when connection with the broker is terminated.

2.2 TLS Session Module Introduction

The NetX Duo TLS session module provides high-level APIs for the TLS protocol-based client. It uses services provided by the RA FSP Crypto Engine (SCE) to carry out hardware-accelerated encryption and decryption.

The NetX Duo TLS Session module is based on Azure RTOS NetX Secure which implements the Secure Socket Layer (SSL) and its replacement, TLS protocol, as described in RFC 2246 (version 1.0) and 5246 (version 1.2). NetX Secure also includes routines for the basic X.509 (RFC 5280) format. NetX Secure is intended for applications using ThreadX RTOS in the project.

2.2.1 Design Considerations

- NetX Secure TLS performs only basic path validation on incoming server certificates.
  Once the basic path validation is complete, TLS then invokes the certificate verification callback supplied by the application.

- It is the responsibility of the application to perform any additional validation of the certificate.
  To help with the additional validation, NetX Secure provides X.509 routines for common validation operations, including DNS validation and Certificate Revocation List checking.
- Software-based cryptography is processor-intensive.
  NetX Secure software-based cryptographic routines have been optimized for performance but depending on the capabilities of the target processor, performance may result in very long operations. When hardware-based cryptography is available, it should be used for optimal performance of the NetX Secure TLS.
- Due to the nature of embedded devices, some applications may not have the resources to support the maximum TLS record size of 16 KB.
  NetX Secure can handle 16 KB records on devices with sufficient resources.

2.2.2 Supported Features

- Support for RFC 2246 Transport Layer Security (TLS) Protocol Version 1.0
- Support for RFC 5246 TLS Protocol Version 1.2
- Support for RFC 5280 X.509 PKI Certificates (v3)
- Support for RFC 3268 Advanced Encryption Standard (AES) Cipher suites for TLS
- RFC 3447 Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version2.1
- RFC 2104 HMAC: Keyed-Hashing for Message Authentication
- RFC 6234 US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF)
- RFC 4279 Pre-Shared Key Cipher suites for TLS

2.3 Azure IoT Device SDK Module Introduction

The Azure IoT device SDK is a set of libraries designed to simplify the process of developing IoT applications for Azure Cloud to make sending and receiving messages easy from the Azure IoT Hub service. There are different variations of the SDK, each targeting a specific platform, but in this application note we will describe the Azure IoT device SDK for C.

The Azure IoT device SDK for C is written in ANSI C (C99) to maximize portability. This feature makes the libraries well suited to operate on multiple platforms and devices, especially where minimizing disk and memory footprint is a priority.

In this application note we will cover how to initialize the device library, send data to IoT Hub, and receive messages from it.

More details on the Azure IoT Device SDK can be found at the reference link The Azure IoT device SDK for C | Microsoft Docs.

2.3.1 Design Considerations

The Azure IoT Device SDK is integrated with FSP and is available for the customers to use. To add the SDK to the application, users are required to use the **Stacks** tab and select **Networking > Azure RTOS NetX Duo IOT Middleware.**

When the components are selected using the **Stacks** tab, and the project is created, the SDK and libraries can be seen under the `ra/microsoft/azure-rtos/netxduo/addons/azure_iot` and `ra/microsoft/azure-rtos/netxduo/addons/cloud` folders.

Note: In the following sections, step by step procedure of adding the Azure IoT middleware is explained in detail.

2.3.2 Supported Features

Table 1. IoT SDK Supported features

Features	Descriptions
Send device-to-cloud messages	Send device-to-cloud messages to IoT Hub with the option to add custom message properties.
Receive cloud-to-device messages	Receive cloud-to-device messages and associated properties from IoT Hub.

Features	Descriptions
Device twins	IoT Hub persists a device twin for each device that you connect to IoT Hub. The device can perform operations like get twin document and subscribe to desired property updates.
Direct methods	IoT Hub gives you the ability to invoke direct methods on devices from the Cloud.
Device Provisioning Service (DPS)	This SDK supports connecting your device to the Device Provisioning Service, for example, through individual enrollment using an X.509 leaf certificate.
Protocol	The Azure SDK for Embedded C supports only MQTT.
Retry policies	The Azure SDK for Embedded C provides guidelines for retries, but actual retries should be handled by the application.
IoT plug and play	IoT Plug and Play enables solution builders to integrate smart devices with their solutions without any manual configuration.

3. MQTT/TLS Application Example

3.1 Application Overview

This application project demonstrates the Renesas RA IoT Cloud Connectivity solution using the FSP and uses Microsoft® Azure as the Cloud provider. Cellular is used as the primary communication interface between the MQTT device and the Azure IoT Services.

The CK-RA6M5 kit acts as an MQTT node, connects to the Azure IoT service using MQTT/TLS protocol over the Cellular interface. The application periodically reads the on-board sensor values and publishes this information to the Azure IoT Hub. It also subscribes to a User LED state MQTT topic. You can turn the User LEDs ON/OFF by publishing the LED state remotely. This application reads the updated LED state and turns the User LEDs ON/OFF.

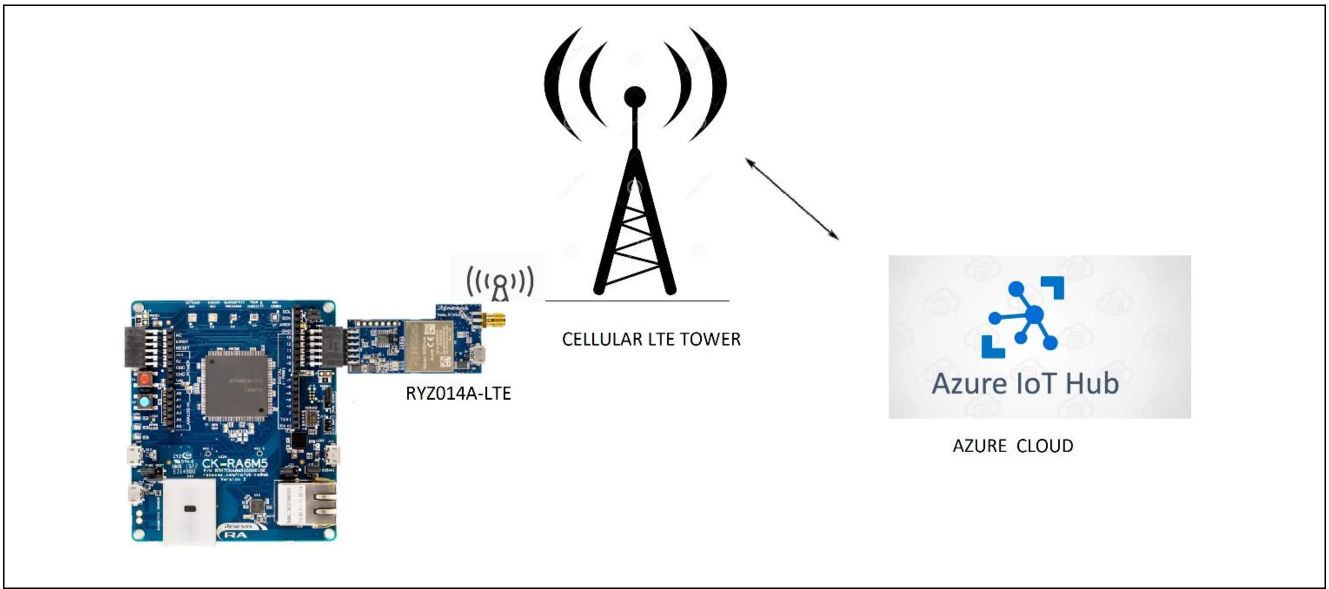

Figure 6. RA MQTT/TLS Application HW Connection Overview

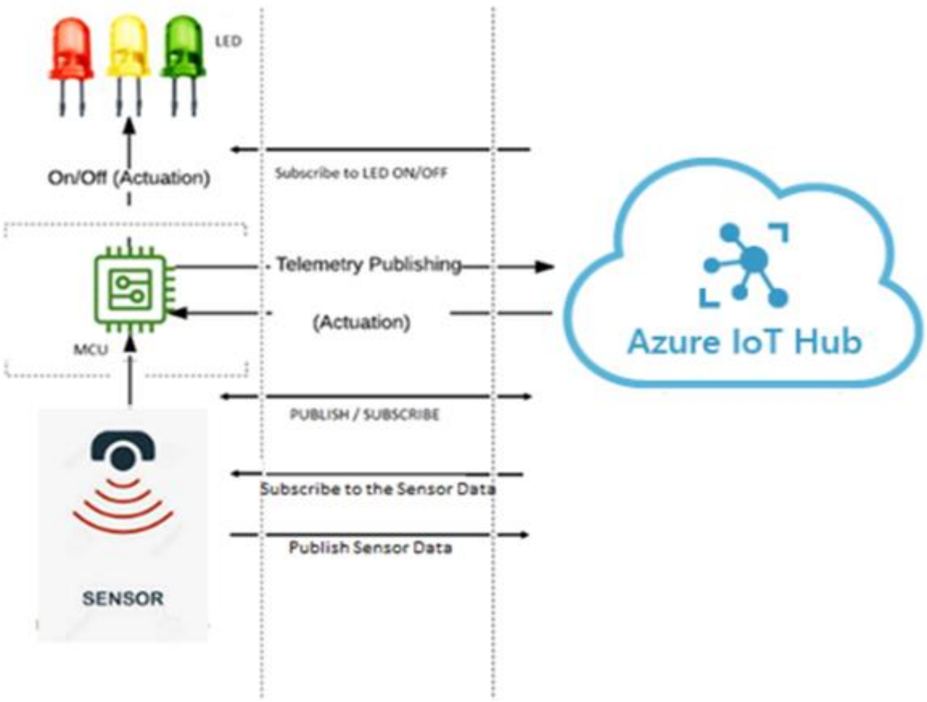

Figure 7. MQTT Publish/Subscribe to/from Azure IoT Central

The following files from this application project serve as a reference.

Table 2. Files Used in Application Project

No.	Filename	Purpose
1.	`src/application_thread_entry.c`	Contains initialization code and has the main thread used in Cloud Connectivity application.
2.	`src/common_init.h`	Contains macros, data structures, and functions prototypes used to initialize common peripherals across the project.
3.	`src/common_utils.c`	Contains data structures, and functions commonly used across the project.
4.	`src/common_utils.h`	Contains macros, data structures, and functions prototypes commonly used across the project.
5.	`src/Console_Thread_entry.c`	Contains the code for command line interface and flash memory operations.
6.	`src/ICM_20948.c`	Contains the code for the 9-Axis MEMS Motion Tracking™ Sensor
7.	`src/ICM_20948.h`	Contains the Data structure function prototypes for the 9-Axis MEMS Motion Tracking™ Sensor
8.	`src/ICP_10101.c`	Contains the code for Barometric Pressure and Temperature Sensor
9.	`src/ ICP_10101.h`	Contains the Data structure and function prototypes for Barometric Pressure and Temperature Sensor
10.	`src/ICP_Thread_entry.c`	Reading Barometric Pressure and Temperature data
11.	`src/HS3001_Thread_entry.c`	Contains Initializations for all sensors including Humidity and Temperature Sensor and Reading Temp-Humidity data
12.	`src/ICM_Thread_entry.`	Reading Accel Gyro Magnetometer Data

No.	Filename	Purpose
13.	src/OB_1203_Thread_entry.c	Contains the code for Heart Rate, Blood Oxygen Concentration, Pulse Oximetry, Proximity, Light and Color Sensor
14.	src/Oximeter.c	Contains data structures and functions used for the oximeter sensor
15.	src/Oximeter.h	Contains the Data structure and function prototypes for the oximeter sensor
16.	src/oximstruct.h	Contains the Data structure for the oximeter sensor
17.	src/r_typedefs.h	Contains the common derived data types
18.	src/RA_HS3001.c	Contains the code for the Renesas Relative Humidity and Temperature Sensor
19.	src/RA_HS3001.h	Contains function prototypes for Relative Humidity and Temperature Sensor
20.	src/RA_ZMOD4XXX_Common.c	Contains the common code for Renesas ZMOD sensors
21.	src/RA_ZMOD4XXX_Common.h	Contains the common data structure's function prototypes for the Renesas ZMOD sensors
22.	src/RA_ZMOD4XXX_IAQ1stGen.c	Contains the common code for the Renesas ZMOD Internal Air Quality sensors
23.	src/RA_ZMOD4XXX_OAQ1stGen.c	Contains the common code for the for the Renesas ZMOD Outer Air Quality sensors
24.	src/RmcI2C.c	Contains the I2C wrapper functions for the third-party sensors not integrated with FSP
25.	src/RmcI2C.h	Contains the I2C function prototypes for wrapper functions for the third-party sensors not integrated with FSP
26.	src/user_choice.h	Contains the Function prototypes for the Sensor and its user configuration for the different sensors and its data accessibility.
27.	src/usr_config.h	To customize the user configuration to run the application.
28.	src/usr_hal.c	Contains data structures and functions used for the Hardware Abstraction Layer (HAL) initialization and associated utilities.
29.	src/usr_hal.h	Accompanying header for exposing functionality provided by usr_hal.c.
30.	Src/cellular_setup.c	Contains data structures and functions used to operate the Cellular Module. This file is for Cellular Modem specific usage
31.	src/usr_network.c	Contains data structures and functions used to operate the NetX Duo TCP/IP and Cellular Module. This file is for Network-specific usage.
32.	src/usr_network.h	Accompanying header for exposing functionality provided by usr_network.c. This file is for Network-specific use.
33.	src/ZMOD4410_Thread_entry.c	Contains the code for indoor air quality sensor
34.	src/ sample_pnp_environmental_sensor_component.c	PNP Telemetry for HS3001 Temperature sensor data
35.	src/ sample_pnp_gas_component.c	PNP Telemetry for ZMOD4410 IAQ Sensor Data
36.	src/ sample_pnp_barometric_pressure_sensor_component.c	PNP Telemetry for ICP10101 Pressure Sensor data

No.	Filename	Purpose
37.	src/ sample_pnp_inertial_sensor_component.c	PNP Telemetry for ICM20948 Inertial Sensor data
38.	src/ sample_pnp_gas_oaq.c	PNP Telemetry for ZMOD4510 OAQ Sensor Data
39.	src/ sample_pnp_biometric_sensor_component.c	PNP Telemetry for OB1203 Biometric Sensor Data
40.	src/ZMOD4510_Thread_entry.c	Reading Outdoor Air Quality Data
41.	src/console_menu/console.c	Contains data structures and functions used to print data on console using UART
42.	src/console_menu/console.h	Contains the Function prototypes used to print data on console using UART
43.	src/console_menu/menu_flash.c	Contains data structures and functions used to provide CLI flash memory related menu
44.	src/console_menu/menu_flash.h	Contains the Function prototypes and macros used to provide CLI flash memory related menu
45.	src/console_menu/menu_kis.c	Contains functions to get the FSP version, get UUID and help option for main menu on CLI
46.	src/console_menu/menu_kis.h	Contains the Function prototypes and macros used to get fsp version, get uuid and help option for main menu on CLI
47.	src/console_menu/menu_main.c	Contains data structures and functions used to provide CLI main menu options
48.	src/console_menu/menu_main.h	Contains the Function prototypes and macros used to provide CLI main menu options
49.	src/console_menu/menu_catm.c	Contains functions to get to IMEI, ICCID and help option for main menu on CLI
50.	src/console_menu/menu_catm.h	Contains functions prototypes to get IMEI, ICCID and help option for main menu on CLI
51.	src/flash/ flash_hp.c	Contains data structures and functions used to perform flash memory related operations
52.	src/flash/ flash_hp.h	Contains the function prototypes and macros used to perform flash memory related operations
53.	src/I2C/i2c.c	Contains data structures and functions used for I2C communication
54.	src/I2C/i2c.h	Contains the Function prototypes and macros used for I2C communication
55.	src/ob1203_bio/KALMAN/kalman.c	Contains algorithm for Heart Rate, Blood Oxygen Concentration, Pulse Oximetry, Proximity, Light and Color Sensor sample calculations
56.	src/ob1203_bio/KALMAN/kalman.h	
57.	src/ob1203_bio/OB1203/OB1203.c	
58.	src/ob1203_bio/OB1203/OB1203.h	
59.	src/ob1203_bio/SAVGOL/SAVGOL.c	
60.	src/ob1203_bio/SAVGOL/SAVGOL.h	
61.	src/ob1203_bio/SPO2/SPO2.c	
62.	src/ob1203_bio/SPO2/SPO2.h	
63.	src/nx_azure_iot_cert.c	Azure IoT Interface code. These have the reference to the working sample implementation and other features such as Device Twin and Direct Method. These files can be used as reference for developing the application
64.	src/nx_azure_iot_cert.h	
65.	src/nx_azure_iot_ciphersuites.c	
66.	src/nx_azure_iot_ciphersuites.h	
67.	src/sample_azure_iot_embedded_sdk.c	
68.	src/sample_config.h	
69.	src/sample_device_identity.c	

No.	Filename	Purpose
70.	src/usr_app.c	Contains data structures and functions used to operate the user application functions.
71.	src/usr_app.h	Accompanying header for exposing functionality provided by usr_app.c.
72.	src/ base64_decode.c	Contains function used for BASE64 to Hex Conversion
73.	src/ base64.h	Contains function prototype used for BASE64 to Hex Conversion
74.	src/c2d_thread_entry.c	Contains data structures functions and main thread used in Cloud to Device message handling.
75.	src/hal_entry.c	Auto generated unused file for Non RTOS thing.
76.	commandRX_Thread_entry.c	Cloud to Device Commands reception
77.	uart_CATM.c	Contains code for the CATM info get for activation
78.	uart_CATM.h	Contains code for the CATM info get for activation

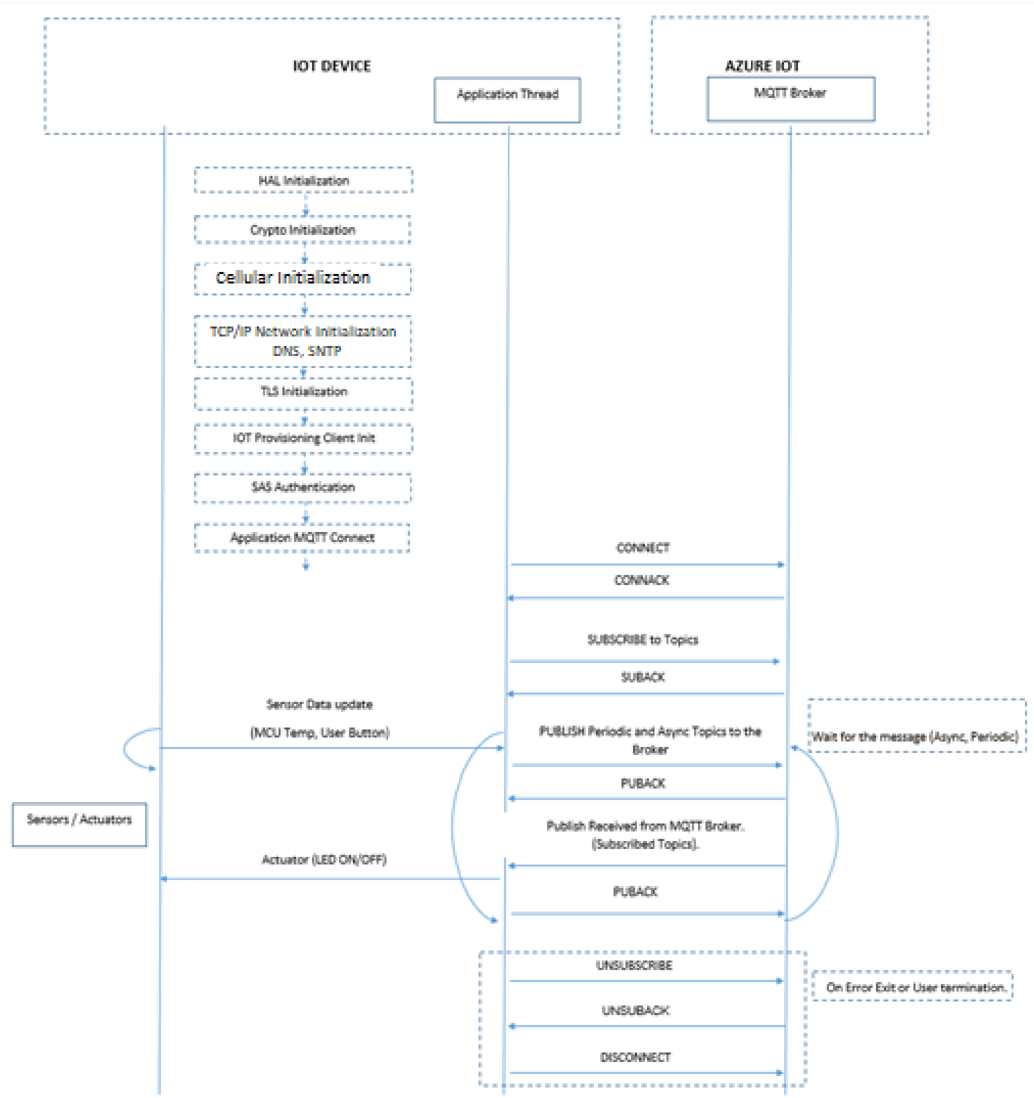

Figure 8. Application Example Implementation Details

3.2 Creating the Application Project using the FSP configurator

Note: Skip this section, if you are planning to import, build and run the project attached with this application note.

Complete steps to create the project from the start using the e^2 studio and FSP configurator. The following table shows the step-by-step process in creating the project. It is assumed that the user is familiar with the e^2 studio and FSP configurator. Launch the installed e^2 studio for the FSP.

Table 3. Step-by-step Details for Creating the Application Project

	Steps	Intermediate Steps
	Steps	**Intermediate Steps**
1	Project Creation:	**File → New → Renesas C/C++ Project → Renesas RA**
2	Project Template**:** Templates for Renesas RA Project	**Renesas RA C/C++ Project → Next**
3	e^2 studio - Project Configuration: Renesas RA C/C++ Project Project Name and Location	**Project Name (Name for the project of your choice) → Next**
4	**Device and Tools Selection**	
	Device Selection	**FSP Version: 4.4.0 (or higher)**
		Board: CK-RA6M5
		Device: R7FA6M5BH3CFC
		Language: C
5	**Toolchains**	**Toolchain: GNU ARM Embedded** (Default)
		Toolchain version: 10.3.1.20210824
		Debugger: J-Link ARM **→ Next**
6	**Project Type Selection**	**Flat (Non-TrustZone) Project** **→ Next**
7	**Build Artifact and RTOS Selection**	**Build Artifact Selection: Executable** **RTOS Selection: Azure RTOS ThreadX (v6.2.1+fsp4.4.0)** **→ Next**
8	**Project Template Selection**	**Azure RTOS ThreadX – Minimal → Finish**
9	**Clock**	**HOCO 20MHz →PLL Src:HOCO → PLL Div/2 →PLL Mul x20.0**
10	**Stacks** tab (Part of the **FSP Configurator**)	**Threads → New Thread**
11	Configure **Properties → Thread**	**Symbol: application_thread**
		Name: Application Thread
		Stack size (bytes):0x4000
		Priority: 3
		Auto start: Disabled
		Time slicing interval (ticks): 50
		Note: The stack size of the application thread needs to be a minimum of 0x1000 bytes or greater. This is the requirement for the NetX Duo Crypto use.
12	Adding the NetX IoT Middleware, SNTP Clients and Packet Pool to the Application Thread Keep the default names **g_dns0**, **g_sntp_client0**. The default configuration provided by the FSP configurator is used, so there is no need to change any of the specific configuration in the **Property** window.	
	Adding DHCP Client	
	New Stack	**Networking → Azure RTOS NetX Duo IoT Middleware**
	Adding Packet Pool for the NetX Duo DNS Client	Click on **Add NetX Duo Packet Pool → Use→ g_packet_pool0 Azure RTOS NetX Duo Packet Pool Instance**

	Steps	Intermediate Steps
	Adding NetX Duo Network Driver	Click on **Add NetX Duo Network Driver → New → Azure EWF NetX Duo Middleware**
	Configuring **Azure EWF interface on r_uart**	
	Common→	**Parameter checking →Enabled**
		Debug → Disabled
		Verbose Logging → Disabled
		EWF_LOG(…)→ Keep it Blank
	Configuring **g_uart0 UART (r_sci_uart)**	
	Common	**FIFO Support : Enabled**
		DTC Support: Disable
		Flow Control Support : Enabled
	Module g_uart0 UART (r_sci_uart)	**Baud → Baud Rate → 921600**
		Flow Control→ CTS/RTS Selection →Hardware CTS and Software RTS
		Software RTS Port → 04
		Software RTS Pin → 12
	Config Pins	**TXD0 : P411**
		RXD0 : P410
		CTS0: None
		CTSRTS0: P413
	Modifying the **BSP** tab → **Properties** → **RA Common** for Main stack and Heap Settings)	
	Property settings for **RA Common**	**Main stack size(bytes): 0x4000**
		Heap size (bytes): 0x4000
		Subclock Populated: Not Populated
13	Note: After the Azure IoT Middleware is added, the configurator reports following errors when youhover over the red Blocks. **Error: Hardware TCP/IP support must be enabled in NetX Duo.** **Error: Interface Capability must be enabled in NetX Duo.** **Error: NetX Duo Azure IoT Middleware Requires NetX Secure to be enabled.** **Error: NetX Duo Azure IoT Middleware Requires IP Packet Filter to be enabled.** **Error: NetX Duo Azure IoT Middleware Requires MQTT Cloud to be enabled.** **Error: A NetX Crypto Implementation must be added.** Note: To fix these errors, enable them as explained in the following steps	
	Enabled Hardware TCP/IP support	**Azure RTOS NetX Duo Common → Common → Common →TCP/IP Offload: Enable**
	Enable Interface capability	**g_packet_pool0 Azure RTOS NetX Duo Packet Pool Instance→ Common → Common→ Interface Capability: Enable**
	Enable the NetX Secure	**g_dns0 Azure RTOS NetX Duo DNS Client →Property → Common → MQTT → Client → NX Secure: Enable**
	Enable MQTT Cloud	**g_dns0 Azure RTOS NetX Duo DNS Client →Property → Common → MQTT → Client → Cloud Enable: Enable**
	Enable IP Packet Filter	**g_dns0 Azure RTOS NetX Duo DNS Client →Property → Common → Common → IP Packet Filter: Enabled**
	Add NetX Crypto Implementation	**Click on Add NetX Crypto SW Only or HW/SW Implementation →** **New → Azure RTOS NetX Crypto HW Acceleration**
	Enable the Extended Notify Support	**g_dns0 Azure RTOS NetX Duo DNS Client →Property → Common → Common →Extended Notify Support: Enabled**
14	NetX Secure Component is added from the HW Crypto perspective. IoT SDK also works with SW crypto. But in this application the HW Crypto Accelerators are used.	
	Configure Azure RTOS NetX Secure property values (Only values which changed from the default are shown here)	

	Steps	Intermediate Steps
	PSK Cipher Suite	**Enable**
	ECC Cipher Suite	**Enable**
	TLSv1.0	**Enable**
	TLSv1.1 Legacy Mode	**Enable**
	TLSV1.1	**Enable**
	TLSV1.3	**Disable**
	Server Mode	**Disable**
	Configure Azure RTOS NetX Crypto HW Acceleration property values (Only values which changed from the default are shown here)	
	Common→Hardware Acceleration→Public Key Cryptography (PKC)→ RSA→RSA	**Use Hardware**
	Common→Hardware Acceleration→Public Key Cryptography (PKC)→ RSA→RSA 3072 Verify/Encryption (HW)	**Enabled**
	Common→Hardware Acceleration → Public Key Cryptography (PKC) → RSA → RSA 4096 Verify/Encryption (HW)	**Enabled**
	Common→Hardware Acceleration → Public Key Cryptography (PKC) → RSA → RSA Scratch Buffer Size	**Disabled (HW)**
	Common-> Standalone Usage	**Use with TLS**
	Note: Increase the Stack size in the **BSP** tab to get rid of the error in configurator for NetX Crypto HW Acceleration	Refer to the Modifying the **BSP** tab → **Properties** → **RA Common** for (Main stack and Heap Settings) section in step 11 of this table Note: For crypto operation it is recommended to have a stacksize of 4K or more**.**
	Adding SNTP Client	
	New Stack	**Networking → Azure RTOS NetX Duo SNTP Client**
	Adding NetX Duo IP instance for SNTPClient	Click on **Add NetX Duo IP Instance →Use → g_ip0 NetX Duo IP Instance**
	Adding Packet Pool for the SNTPClient	Click on **Add NetX Duo Packet Pool →Use → g_packet_pool0 Azure RTOS NetX Duo Packet Pool Instance**
15	Increase the **Number of Packets in Pool**	
		Click on **g_packet_pool0 Azure RTOS NetX Duo Packet Pool Instance** **→ Properties window → Number of Packets in Pool**. Change from **16** to **50** (To allow enough buffer for the packets). This can be tuned based on the frequency and size
	Note: After adding the SNTP the configurator reports the following errors when you hover over the red Blocks. **Error: Maximum time adjustment (milliseconds) should be greater than unicast poll interval (seconds).** Note: To fix these errors, enable them as explained in the following steps	
	Reduce the starting poll interval forunicast update request (seconds)	**g_sntp_client0 Azure RTOS NetX Duo SNTP Client → Property → Common → SNTP → Client →Starting poll interval for unicast update request (seconds): 36**
16	Add Cloud to Device Processing Thread to the Application	
	Stacks tab (Part of the **FSP Configurator**)	**Threads → New Thread**

	Steps	Intermediate Steps
	Configure Thread Properties	
	Symbol	**c2d_thread**
	Name	**Cloud2Device Thread**
	Stack size	**2048 Bytes**
	Priority	**4**
	Auto start	**Disabled**
	Time slicing interval (ticks)	**25**
17	Adding the HAL Modules as required for the Application Project: Here, Timer0, External IRQ, 30-second periodic timer, respectively.	
	HAL/Common → New Stack	**Input → External IRQ Driver on r_icu**
	Property Settings for r_icu	**Name: g_sensorIRQ**
		Channel: 14
		Trigger: Falling
		Digital Filtering: Disabled
		Digital Filtering Sample Clock: PCLK/64
		Pin Interrupt Priority: Priority 12
		Callback: sensorOBIRQCallback
		Pins→IRQ14: (Navigate to IRQ14): P403
	HAL/Common Stacks → New Stack	**Timers → Timer, General PWM on r_gpt**
	Property Settings for r_gpt → **General**	**Name: g_timer2**
		Channel: 2
		Mode: Periodic
		Period: 1
		Period Unit: Milliseconds
	Interrupts:	**Callback: TimerCallback**
		Overflow/Crest Interrupt Priority:6
	HAL/Common Stacks → New Stack	**Timers → Timer, General PWM on r_gpt**
	Property Settings for r_gpt → **General**	**Name: gpt**
		Channel: 0
		Mode: Periodic
		Period: 1
		Period Unit: Seconds
	Interrupts:	**Callback: g_gpt_timer_cb**
		Overflow/Crest Interrupt Priority: Priority 10
18	Adding Azure RTOS Objects for the Application (Topic Queue needs to be created for the application – Message Queue)	
	Stacks Tab → Objects	**New Object → Queue**
	Property Settings for the Queue	**Name: Topic Queue**
		Symbol: g_topic_queue
		Message Size (Words): 16
		Queue Size (Bytes): 64
	Stacks Tab → Objects	**New Object → Mutex**
		Name: consolprint_mutex
		Symbol: consolprint_mutex
		Priority Inheritance: Disabled
19	Add HS3001 Sensor (Temperature and Humidity) Processing Thread to the Application	
	Stacks tab (Part of the **FSP Configurator**)	**Threads → New Thread**
	Configure Thread Properties	
	Symbol	**HS3001_Thread**
	Name	**HS3001_Thread**

	Steps	Intermediate Steps
	Stack size	**0x1000 Bytes**
	Priority	**4**
	Auto start	**Disabled**
	Time slicing interval (ticks)	**1**
20	Adding the HS300X Sensor Module to the HS3001_Thread	
	New Stack →	**Sensor → HS300X Temperature/Humidity Sensor**
	Config HS300X sensor→	Name: g_**hs300x_sensor0**
		Callback: **hs300x_callback**
	Note: This module requires an I2C peripheral, Add I2C by clicking on "Add I2C Communication Peripheral" → New → **I2C Master (r_iic_master)**	
	Module g_i2c_master0 I2C Master	**Rate: Fast Mode**
21	Add ZMOD4410 Sensor (IAQ) Processing Thread to the Application	
	Stacks tab (Part of the **FSP Configurator**)	**Threads → New Thread**
	Configure Thread Properties	
	Symbol	**ZMOD4410_Thread**
	Name	**ZMOD4410_Thread**
	Stack size	**2048 Bytes**
	Priority	**4**
	Auto start	**Disabled**
	Time slicing interval (ticks)	**1**
22	Adding ZMOD4XXX Gas Sensor Module to ZMOD4410_Thread	
	New Stack →	**Sensor → ZMOD4XXX Gas Sensor**
	Config ZMOD4XXX Properties→	**Add Requires ZMOD Libraries→ New→ZMOD4410 IAQ 1ST Gen**
		Add I2C Shared Bus→Use→g_comms_i2c_bus0 I2C Shared Bus
		Add IRQ Driver for Measurement →New→ External IRQ
	Module g_zmod4xxx_sensor0	**Name: g_zmod4xxx_sensor0**
		Comms I2C callback: zmod4xxx_comms_i2c0_callback
		IRQ Callbacks: zmod4xxx_irq0_callback
	Module g_i2c_master0 I2C Master	**Rate: Fast Mode**
	Config External IRQ→	**Name: g_external_irq0**
		Channel :4
		Trigger: Falling
		Pin Interrupt Priority:5
		Pins→IRQ04: (Navigate to IRQ04): P402
23	Add ICP-10101 Sensor (Barometric Pressure &Temperature) Processing Thread to the Application	
	Stacks tab (Part of the **FSP Configurator**)	**Threads → New Thread**
	Configure Thread Properties	
	Symbol	**ICP_Thread**
	Name	**ICP_Thread**
	Stack size	**2048 Bytes**
	Priority	**4**
	Auto start	**Disabled**
	Time slicing interval (ticks)	**1**
24	Adding I2C Communication Device (for ICP10101) into ICP_Thread	
	New Stack →	**Connectivity: I2C Communication Device**
	Config I2C Comm Device →	**Name: g_comms_i2c_device4**
		Slave Address:0x63

	Steps	Intermediate Steps
		Callback: ICP_comms_i2c_callback
	Add I2C Shared Bus→	**Add I2C Shared Bus→Use→g_comms_i2c_bus0 I2C Shared Bus**
	Module g_i2c_master0 I2C Master	**Rate: Fast Mode**
25	Add ICM-20948 (9 Axis MEMS) Processing Thread to the Application	
	Stacks tab (Part of the **FSP Configurator**)	**Threads → New Thread**
	Configure Thread Properties	
	Symbol	**ICM_Thread**
	Name	**ICM_Thread**
	Stack size	**2048 Bytes**
	Priority	**4**
	Auto start	**Disabled**
	Time slicing interval (ticks)	**1**
26	Adding I2C Communication Device (for ICM-20948) into ICM_Thread	
	New Stack →	**Connectivity: I2C Communication Device**
	Config I2C Comm Device →	**Name: g_comms_i2c_device5**
		Slave Address: 0x68
		Callback: ICM_comms_i2c_callback
	Add I2C Shared Bus→	**Add I2C Shared Bus→Use→g_comms_i2c_bus0 I2C Shared Bus**
	Module g_i2c_master0 I2C Master	**Rate: Fast Mode**
27	**Add ZMOD4510 Sensor (OAQ) Processing Thread to the Application**	
	Stacks tab (Part of the FSP Configurator)	**Threads → New Thread**
	Configure Thread Properties	
	Symbol	**ZMOD4510_Thread**
	Name	**ZMOD4510_Thread**
	Stack size	**2048 Bytes**
	Priority	**4**
	Auto start	**Disabled**
	Time slicing interval (ticks)	**1**
28	**Adding ZMOD4XXX Gas Sensor Module to ZMOD4510_Thread**	
	New Stack →	**Sensor → ZMOD4XXX Gas Sensor**
	Config ZMOD4XXX Gas Sensor Properties→	**Add Required ZMOD Libraries→ New→ZMOD4510 OAQ 1ST Gen**
		Add I2C Shared Bus→Use→g_comms_i2c_bus0 I2C Shared Bus
		Add IRQ Driver for Measurement→New→ External IRQ
	Module g_zmod4xxx_sensor1	**Name: g_zmod4xxx_sensor1**
		Comms I2C callback: zmod4xxx_comms_i2c1_callback
		IRQ Callbacks: zmod4xxx_irq1_callback
	Module g_comms_i2c_device2 I2C Communication Device (rm_comms_i2c)	**Name: g_comms_i2c_device2**
	Module g_i2c_master0 I2C Master (r_iic_master)	**Rate: Fast Mode**
	Config External IRQ→	**Name: g_external_irq1**
		Channel :15
		Trigger: Falling

	Steps	Intermediate Steps
		Pin Interrupt Priority:12
		Pins→IRQ15: (Navigate to IRQ15): P404
29	Add OB1203 (optical biosensor) Processing Thread to the Application	
	Stacks tab (Part of the **FSP Configurator**)	**Threads → New Thread**
	Configure Thread Properties	
	Symbol	**OB_1203_Thread**
	Name	**OB_1203_Thread**
	Stack size	**2048 Bytes**
	Priority	**2**
	Auto start	**Disabled**
	Time slicing interval (ticks)	**25**
30	Adding I2C Communication Device (for OB-1203) into **OB_1203_Thread**	
	New Stack →	**Connectivity: I2C Communication Device**
	Config I2C Comm Device →	**Name: g_comms_i2c_device3**
		Slave Address: 0x53
		Callback: comms_i2c_callback
	Add I2C Shared Bus→	**Add I2C Shared Bus→Use→g_comms_i2c_bus0 I2C Shared Bus**
	Module g_i2c_master0 I2C Master	**Rate: Fast Mode**
31	Add CLI Processing Thread to the Application	
	Stacks tab (Part of the **FSP Configurator**)	**Threads → New Thread**
	Configure Thread Properties	
	Symbol	**Console_Thread**
	Name	**Console_Thread**
	Stack size	**4096 Bytes**
	Priority	**4**
	Auto start	**Enabled**
	Time slicing interval (ticks)	**10**
32	Adding Uart to Console_Thread	
	New Stack →	**Connectivity: UART**
	Config Common →	**FIFO Support: Enable**
		DTC Support: Disable
		Flow Control Support: Enable
	Config General →	**Name: g_console_uart**
		Channel:5
		Data Bits:8bits
		Parity:None
		Stop Bits:1bit
	Config Baud→	**Baudrate: 115200**
	Config Interrupts →	**Callback: g_console_uart_callback**
	Config Pins →	**TXD: P501**
		RXD: P502
	Adding Flash to Console_Thread	
	New Stack →	**Storage: Flash (r_flash_hp)**

	Steps	Intermediate Steps
		Name: user_flash
		Data Flash Background Operation: Disabled
		Callback: flash_callback
		Flash Ready Interrupt Priority: Priority 6
		Flash Error Interrupt Priority: Priority 6
	Adding back door entry to the CATM1 module via the Uart to Console_Thread	
	New Stack →	**Connectivity: UART**
	Config Common →	**FIFO Support: Enable**
		DTC Support: Disable
		Flow Control Support: Enable
	Config General →	**Name: g_catm1_uart**
		Channel: 0s
		Data Bits:8bits
		Parity: None
		Stop Bits: 1bit
	Config Baud→	**Baudrate: 921600**
	Config Interrupts →	**Callback: catm1_uart_callback**
	Config Pins →	**TXD0 : P411**
		RXD0 : P410
		CTS0 : None
		CTSRTS0: P413
33	Add Cloud to Device Command Reception Thread to the Application	
	Stacks tab (Part of the **FSP Configurator**)	**Threads → New Thread**
	Configure Thread Properties	
	Symbol	**CommandRX_Thread**
	Name	**CommandRX_Thread**
	Stack size	**2048 Bytes**
	Priority	**4**
	Auto start	**Disabled**
	Time slicing interval (ticks)	**40**

The above configuration is a prerequisite to generate the required stack and features for the Cloud connectivity application provided with this app note. Once the **Generate Project Content** button is clicked, e^2 studio generates the source code for the project. The generated source code contains the required drivers, stacks, and middleware. The user application files must be added into the src folder.

For the validation of the created project, the same source files listed in the section 3, MQTT/TLS Application Example, Table 2, may be added. This is the quickest way to create and build the application without writing the code for the configuration created in the above section.

Note: After you follow instructions in section 3.2 to recreate the Application project using FSP configurator and add the src code to the project, the project is ready for building.

Note: If you get error while assigning PIN to External IRQ, go to **Pin Configuration** > **Pin Number** and select the IRQ function for that pin number, for example, for External IRQ channel number 4, you can select Function IRQ14 for pin number 4.

Note: As part of the manual creation of this project, you might encounter known issues/pin errors with the Pin configurator while selecting the peripherals. We recommended selecting the operation mode, disable/enable and select the pins. You can also refer to the attached project as working reference.

3.3 Install Azure CLI

To prepare Azure Cloud resources and connect a device to Azure, you can use Azure CLI. Azure CLI can be installed locally on your PC.

1. Azure CLI can be downloaded from the Microsoft site (https://docs.microsoft.com/en-us/cli/azure/install-azure-cli)
2. The installer name will be similar to `azure-cli-2.44.x.msi.` or later. Click on the installer and install shield will guide you through the installation process. Install it to your desired directory, for example `c:\AzureCLI`
3. Install the current release of the Azure CLI. After the installation is complete, you will need to close and reopen any active Windows Command Prompt or PowerShell windows to use the Azure CLI.
4. After the Azure CLI installation is successful, open and launch the Windows PowerShell to use the Azure CLI. A screenshot of the launch of Windows PowerShell is shown below.

Figure 9. Windows Power Shell

5. If you already have Azure CLI installed locally, go to the directory of the installed AzureCLI and run `az --version` to check the version. This application note requires Azure CLI 2.44.0 or later.

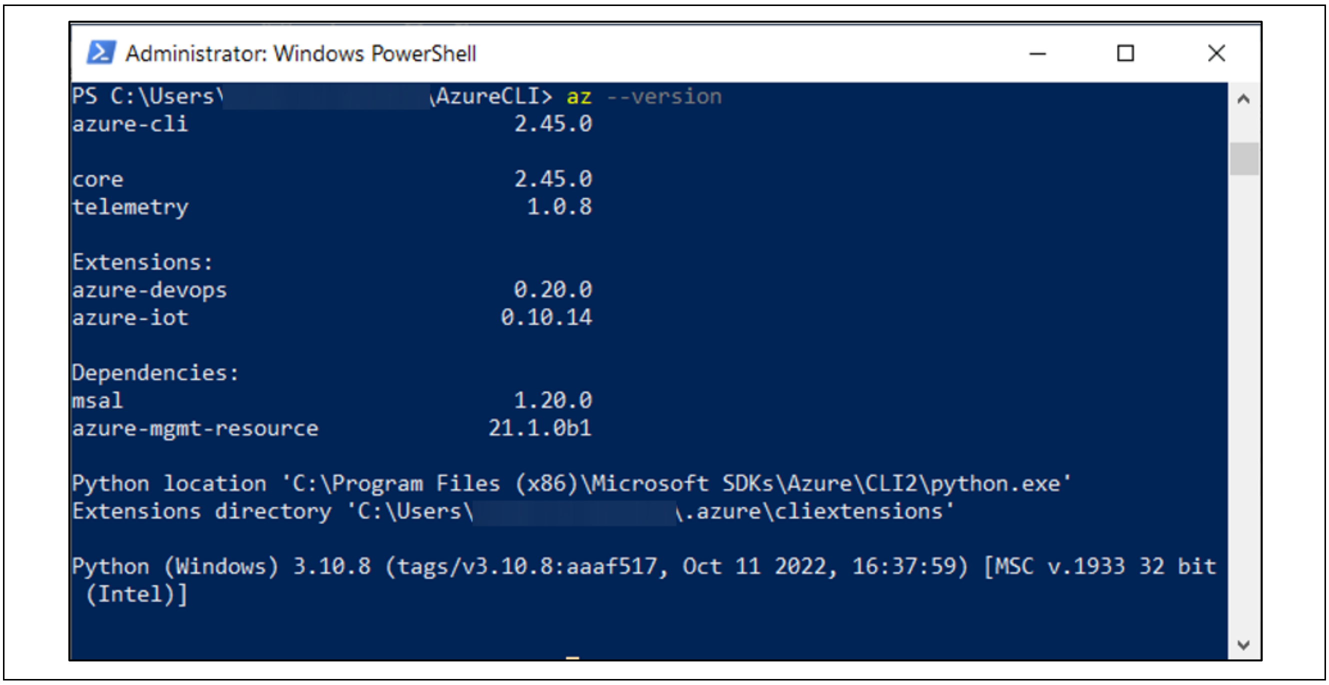

Figure 10. Azure CLI Version

3.4 Create an IoT Hub

You can use Azure CLI to create an IoT Hub that handles events and messaging for your device.

Note 1: Before you start creating the IoT Hub you are required to have a login to your Azure Portal via web browser. If not logged in, then you may notice an error that you are not logged in, while creating the IoT Hub:
https://portal.azure.com/

Note 2: If you do not have the Azure account, you can create one which is valid for 12 months with limited features from the following link:
https://azure.microsoft.com/en-us/free/

To create an IoT Hub:

Note 3: Some of the user parameters while creating the IoT Hub needs to be unique. Users are required to take care of this while creating the IoT Hub credentials.

1. In your CLI console, run the `az extension add` command to add the Microsoft Azure IoT Extension for Azure CLI to your CLI shell. The IoT Extension adds IoT Hub, IoT Edge, and IoT Device Provisioning Service (DPS) specific commands to Azure CLI.
   — `az extension add --name azure-iot`

Note 4: When you run the command for the first time you may not notice output on the console as shown below. It just accepts the command.

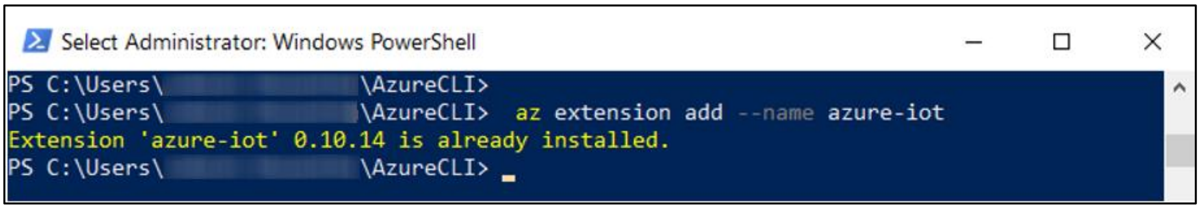

Figure 11. Add Extension for Azure CLI

2. Run the `az login` command to login to the Azure account. Running the `az login` command opens the browser for login. You can enter the login credentials to login to the Azure account. You will notice a similar message on the browser on successful login.

   Note: You can find more info on the Azure CLI at Overview of the Azure CLI | Microsoft Docs

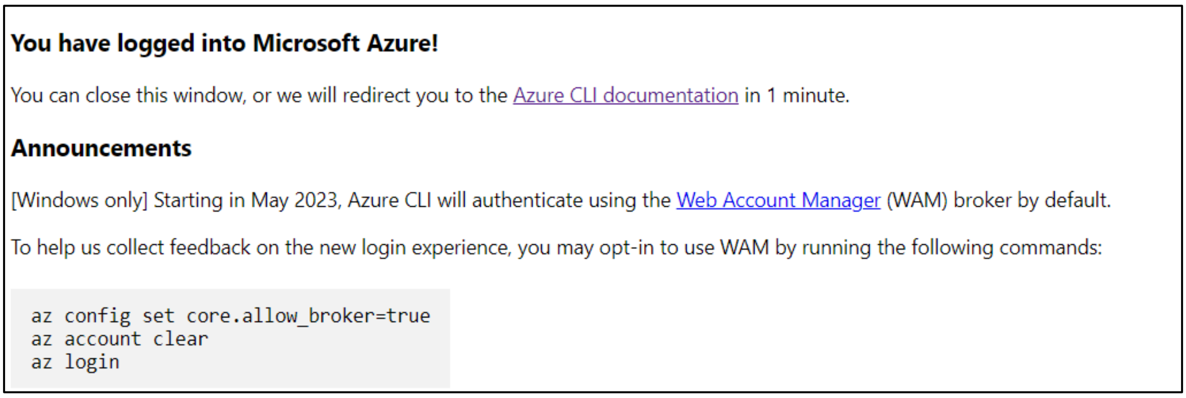

Figure 12. Successful Login to the Azure Account

3. Run the `az group create` command to create a resource group. The following command creates a resource group named `MyRAResourceGroup` in the `westus` region.
4. Note: Optionally, to set an alternate `location`, run `az account list-locations` to see available locations. Then specify the alternate location in the following command in place of `westus`.
   — *`az group create --name MyRAResourceGroup --location westus`*

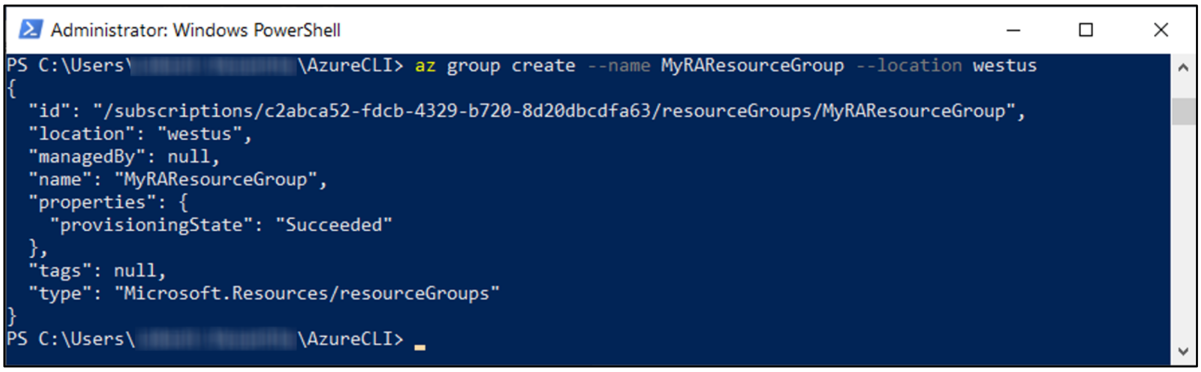

Figure 13. Create Resource Group

5. Run the `az iot hub create` command to create an IoT Hub. It might take a few minutes to create an IoT Hub.
   Replace the *`YourIotHubName`* placeholder below with the name you chose for your IoT Hub. An IoT Hub name must be globally unique in Azure. This placeholder is used in the rest of this tutorial to represent your unique IoT Hub name. Use any command given below.
   — `az iot hub create --resource-group MyRAResourceGroup --name {YourIoTHubName}`

   `OR`

   — `az iot hub create --resource-group MyRAResourceGroup --name {YourIoTHubName} --location {YourLocation}`

Note: It may take few minutes to create the IoT Hub. In this case the IoT Hub name used is `RACLOUDHUB`.

Note: Microsoft recommends to create new IoT Hub. If the IoT Hub created previously (2-3 year old) it may not work as desired. So, we recommend to create new IoT Hub to run the application to yield the proper results

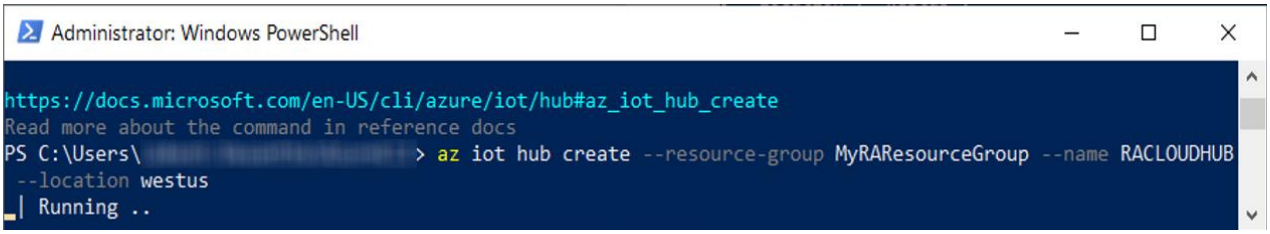

Figure 14. IoT Hub Creation in Progress

6. After the IoT Hub is created, view the JSON output in the console, and copy the `hostName` value to a safe place. You use this value in a later step. The `hostName` value looks like the following example:
   — `{Your IoT hub name}.azure-devices.net`

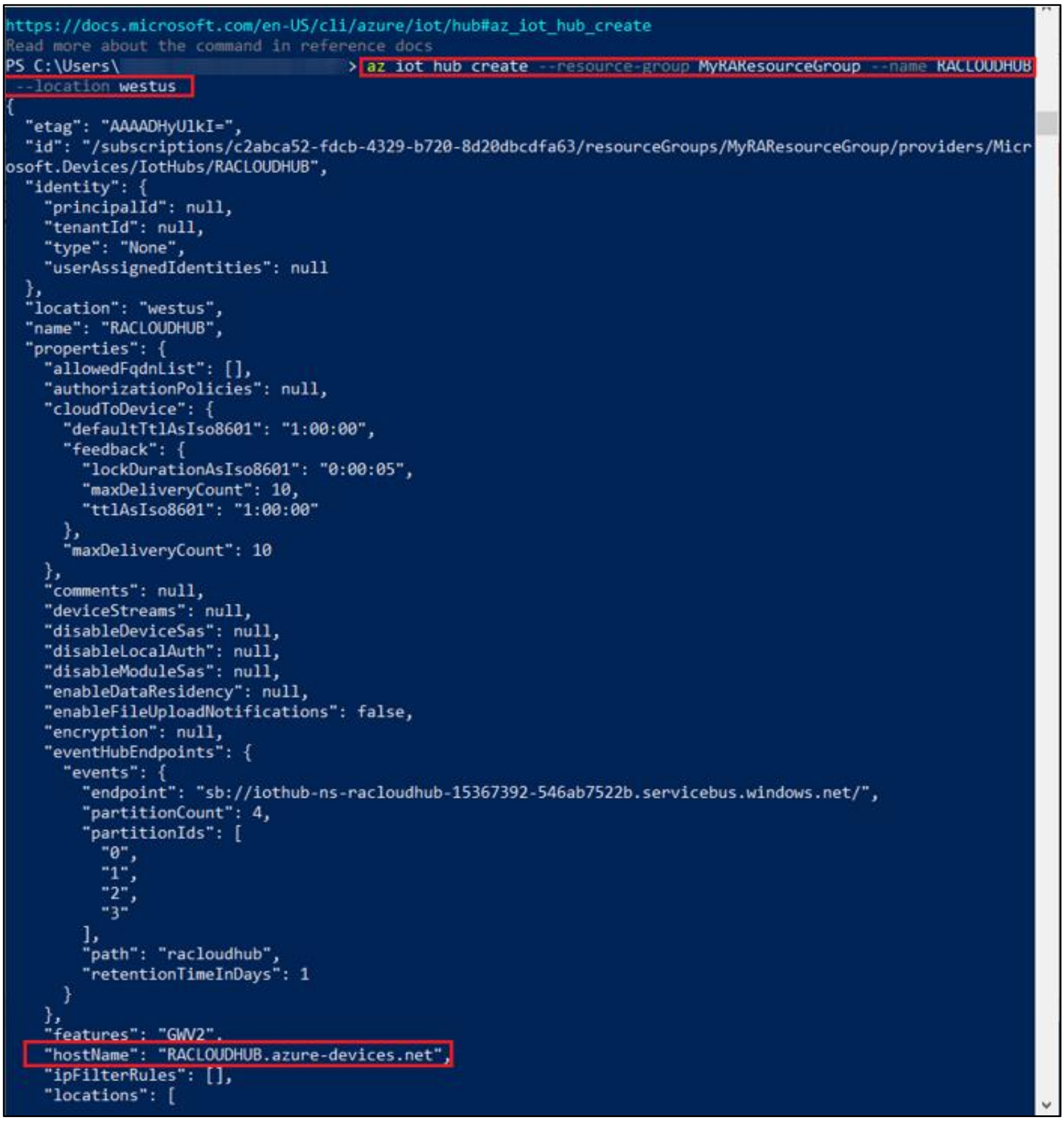

Figure 15. JSON Output After IoT Hub Creation

3.5 Certificate Creation Process

You can use GIT Bash utility for this process. If not installed on your computer, you can download and install it (Git for Windows or Git for Windows (github.com)).

1. Install Git for windows.
2. Launch the Git Bash
3. Create a directory of your choice (for example, `mkdir Azure`).
4. Go to the directory and create the configuration. This created directory is the place where your self-signed certificate is created and stored.

5. Copy paste the configuration listed below to create `x509_config.cfg` as show in the following figure.

```
cat > x509_config.cfg <<EOT
[req]
req_extensions = client_auth
distinguished_name = req_distinguished_name

[req_distinguished_name]

[ client_auth ]
basicConstraints = CA:FALSE
keyUsage = digitalSignature, keyEncipherment
extendedKeyUsage = clientAuthEOT
```

Note: All OpenSSL commands and self-signed certificate creation process is given at this link.

Steps are as follows:

1. Set x509 configuration file for common name in cert.

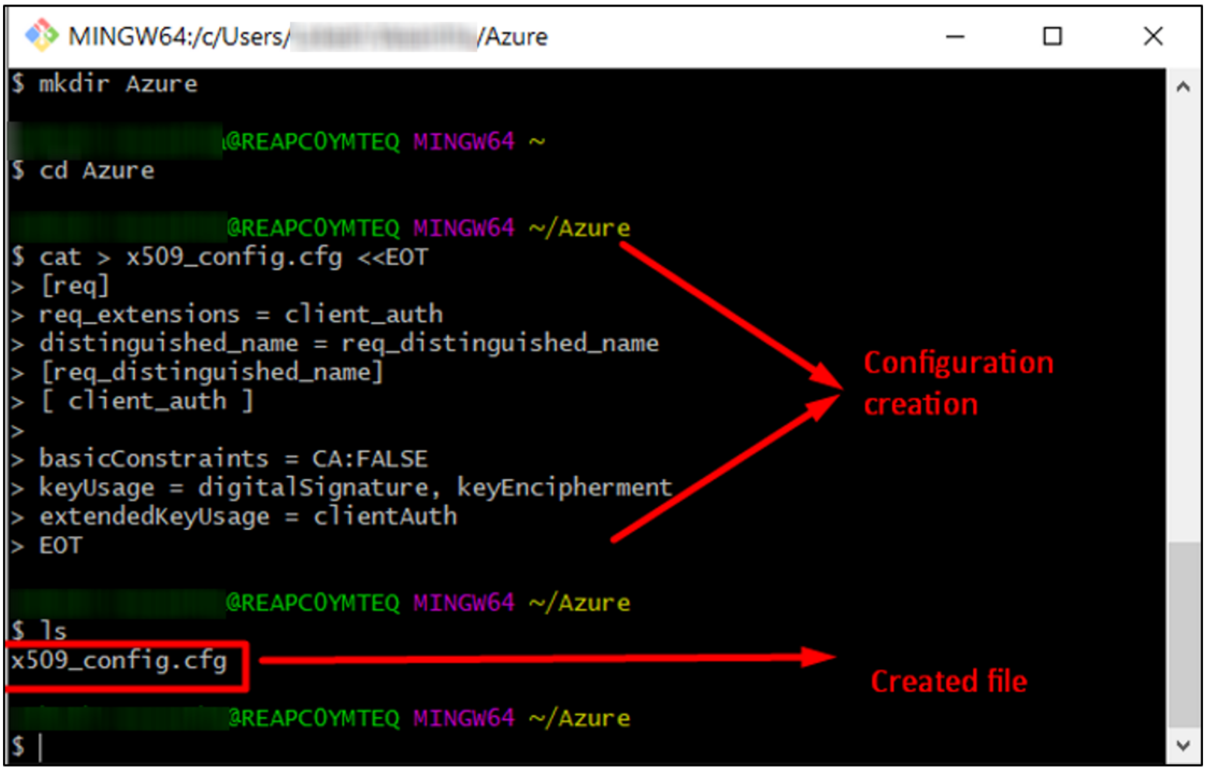

Figure 16. Set X509 Configuration File

2. Create RSA self-signed certificate.
   Generate private key and certificate (public key) using the command as shown in the snapshot
   “openssl genrsa -out privkey.pem 2048”

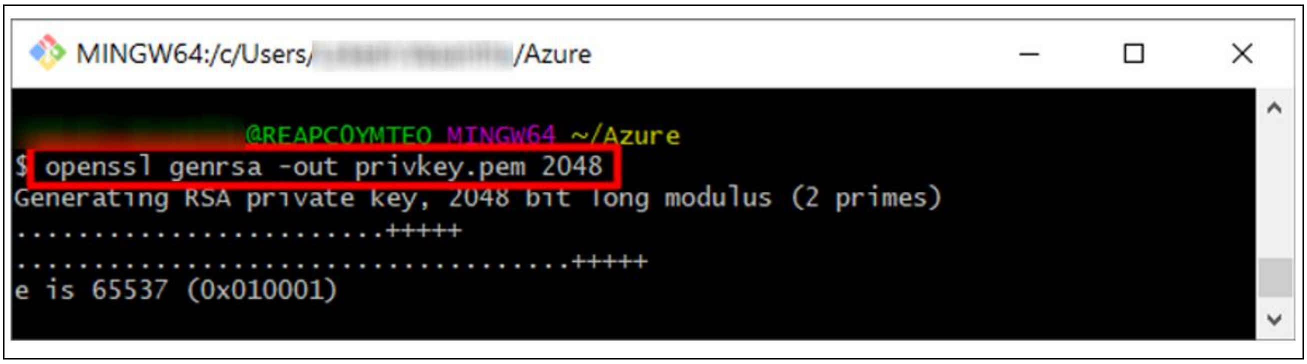

Figure 17. Generate Private Key and Certificate (public key)

3. Embed Device ID in certificate
   This command will not give you any response if successfully executed.
   `openssl req -new -days 365 -nodes -x509 -key privkey.pem -out cert.pem -config x509_config.cfg -subj "//CN=<Same as device Id>"`
   Note: In this example the device ID name “CK_RA6M5_X509” is used. Note down this Device ID. This will be used in the future steps. Use your own Device ID to make it unique across your system.

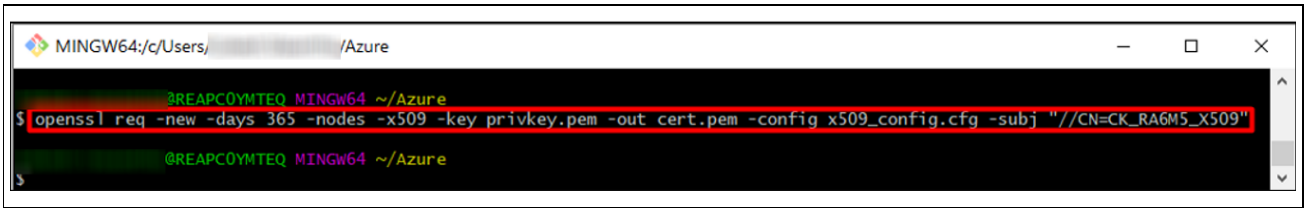

Figure 18. Embed Device ID in Certificate

4. Run command to convert format of key from pem to der
   `openssl rsa -outform der -in privkey.pem -out privkey.der`
   Here you get response “writing RSA key”

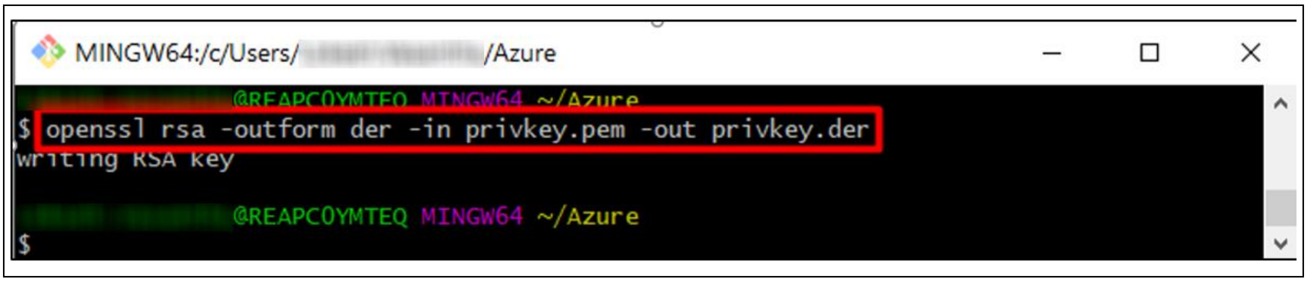

Figure 19. Convert Format from key to der

5. Run command to Convert format of cert from pem to der
   `openssl x509 -outform der -in cert.pem -out cert.der`
   This command will not give you any response if successfully executed.

Figure 20. Convert Format of cert from pem to der

6. Convert der to hex array and set them in `sample_device_identity.c` file in the project.
   For easier access the command text is given as follows. User can copy paste text in the command line to create `sample_device_identity.c`.

```
echo "#include \"nx_api.h\"
/**
device cert (`openssl x509 -in cert.pem -fingerprint -noout | sed 's/://g' `) :
`cat cert.pem`

device private key :
`cat privkey.pem`
*/
" > sample_device_identity.c
```

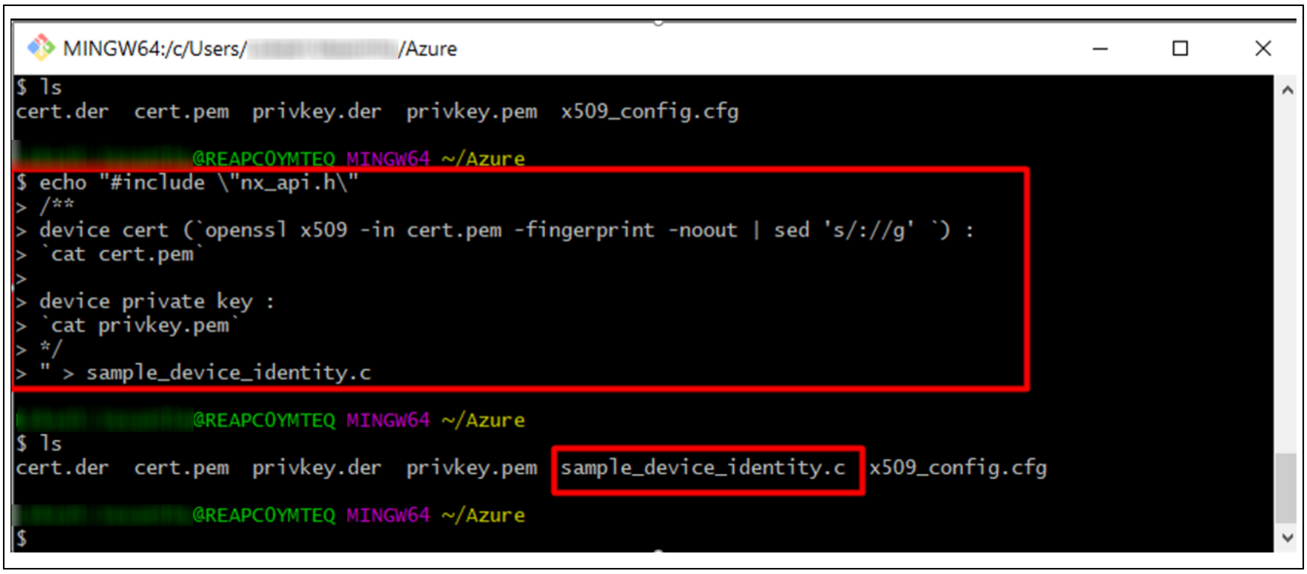

Figure 21. Convert der to Hex Array and Set them in sample_device_identity.c

7. Run “ls” command to check whether `sample_device_identity.c` is created.
8. Run the following commands to produce `sample_device_cert_ptr` and `sample_device_private_key_ptr` array containing device certificate and private key equivalent hex values along with length.

```
“xxd -i cert.der | sed -E "s/(unsigned char) (\w+)/\1
sample_device_cert_ptr/g; s/(unsigned int) (\w+)_len/\1
sample_device_cert_len/g" >> sample_device_identity.c”
```

```
“xxd -i privkey.der | sed -E "s/(unsigned char) (\w+)/\1
sample_device_private_key_ptr/g; s/(unsigned int) (\w+)_len/\1
sample_device_private_key_len/g" >> sample_device_identity.c”
```

These commands will not give you any response if successfully executed.

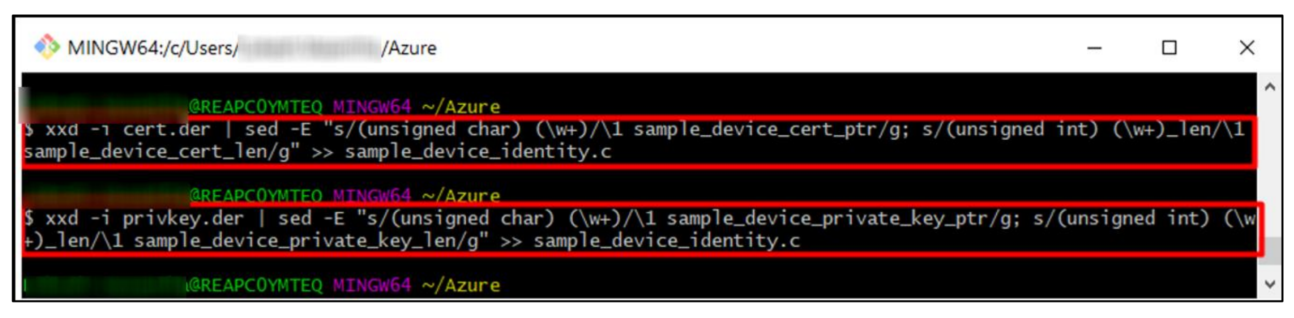

Figure 22. Producing arrays containing hex values

Check the content of `sample_device_identity.c` with cat command. In this file you will get Device certificate along with SHA1 fingerprint, Device Private Key, `sample_device_cert_ptr` and `sample_device_private_key_ptr` array along with their length. You will also notice the Fingerprint; you need to use this fingerprint as "thumbprint" in device creation process using the IoT Explorer in later sections. Please note down this Fingerprint.

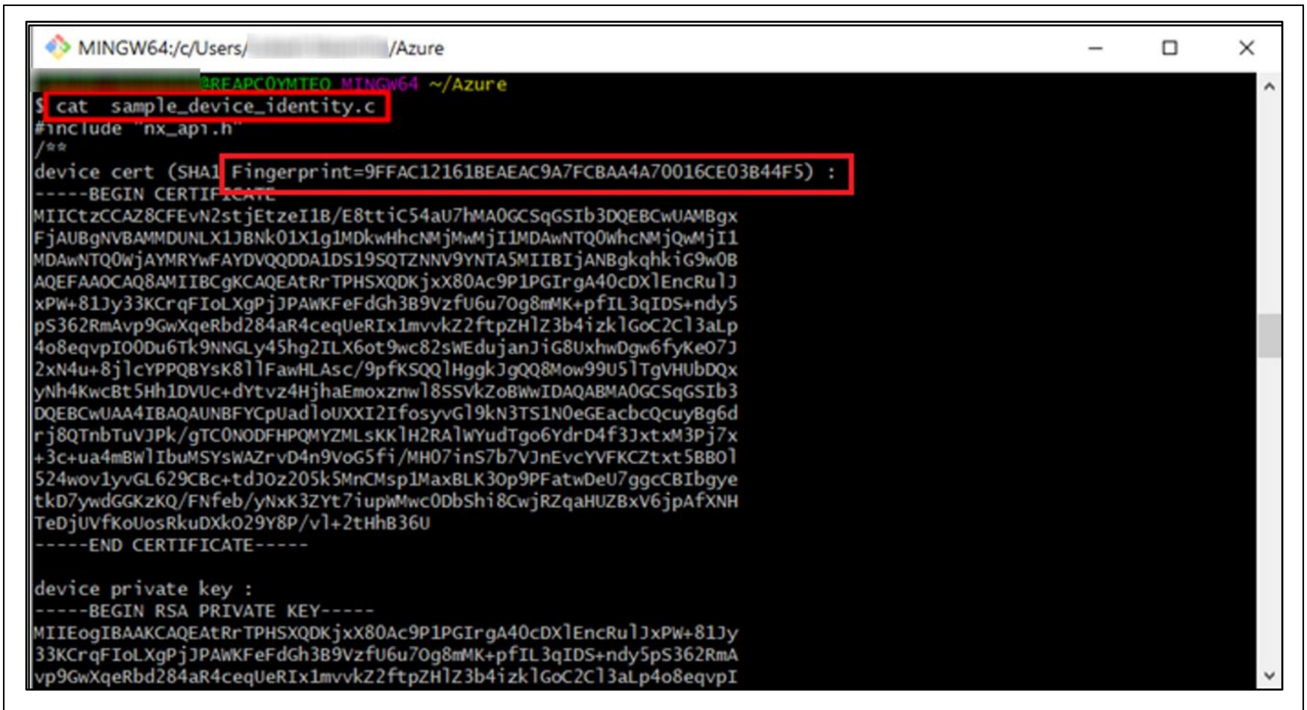

Figure 23. Check the Content of sample_device_identity.c

3.6 View Device Properties

You can use the Azure IoT Explorer (https://docs.microsoft.com/en-us/azure/iot-pnp/howto-use-iot-explorer) to view and manage the properties of your devices. In the following steps, you will add a connection to your IoT Hub in IoT Explorer. With the connection, you can view properties for devices associated with the IoT Hub.

Download and install latest (above v0.15.6.0) Azure IoT Explorer from: https://github.com/Azure/azure-iot-explorer/releases

Note: Click and install the downloaded msi file `Azure.IoT.Explorer.Preview.0.15.6.msi` or newer version of the downloaded file. The install shield guides you through the installation process.

3.7 Set IoT Hub

To add a connection to your IoT Hub:

1. In your Azure CLI console, run the `az iot hub connection-string show` command to get the connection string for your IoT Hub.
   — `az iot hub connection-string show -n {YourIoTHubName}`

Note: See section **Error! Reference source not found.**, Create an IoT Hub for the IoT Hub Name.

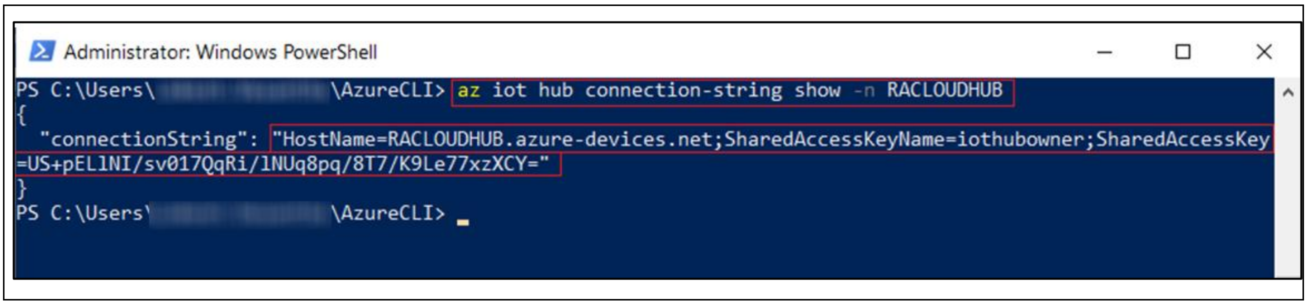

Figure 24. Connection String

2. Copy the connection string.
3. Open the Azure IoT Explorer and select **IoT hubs > Add connection**.
4. Paste the connection string into the **Connection string** box.
5. Select **Save**.

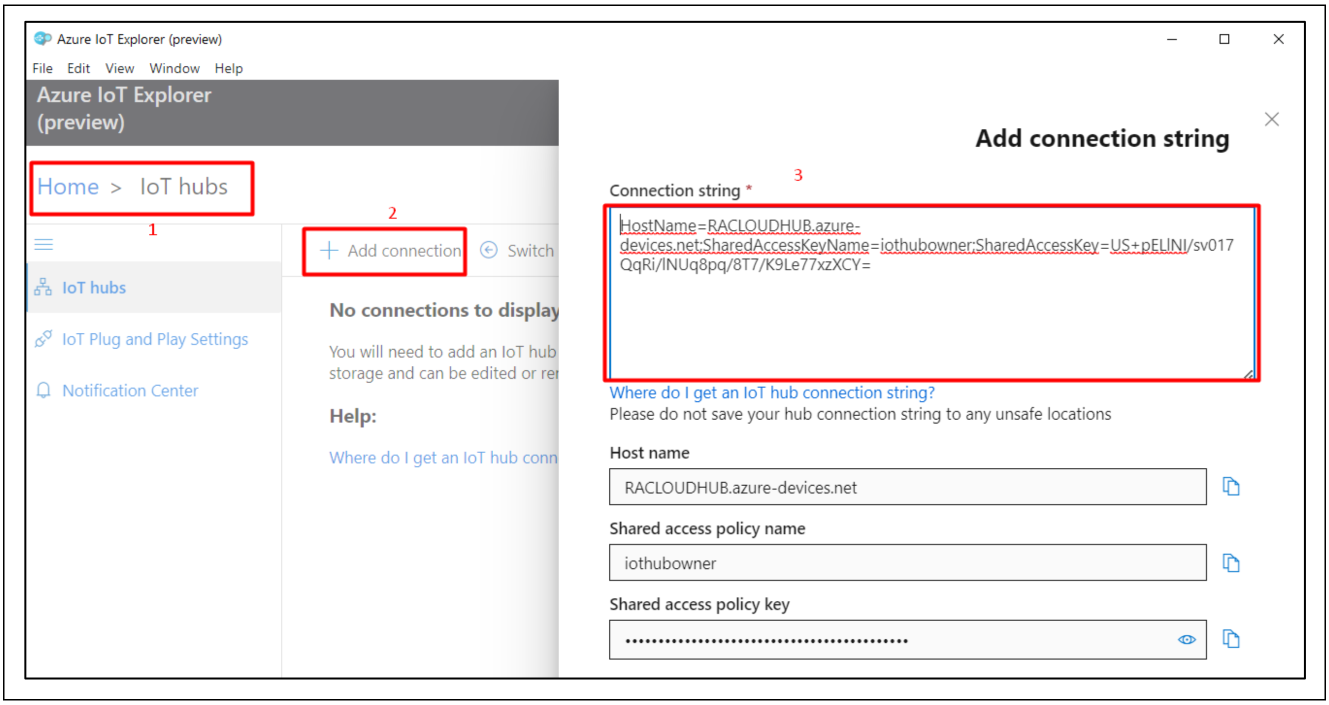

Figure 25. Adding Connection String

Note: In some cases, Azure IoT Explorer may report an error that the default port that IoT Explorer is trying to use is being used by another application. In order to overcome this error, you can add a different port number for the Azure IoT Explorer shown as follows.

On your PC, edit the system environmental variables as shown in the following screenshots.

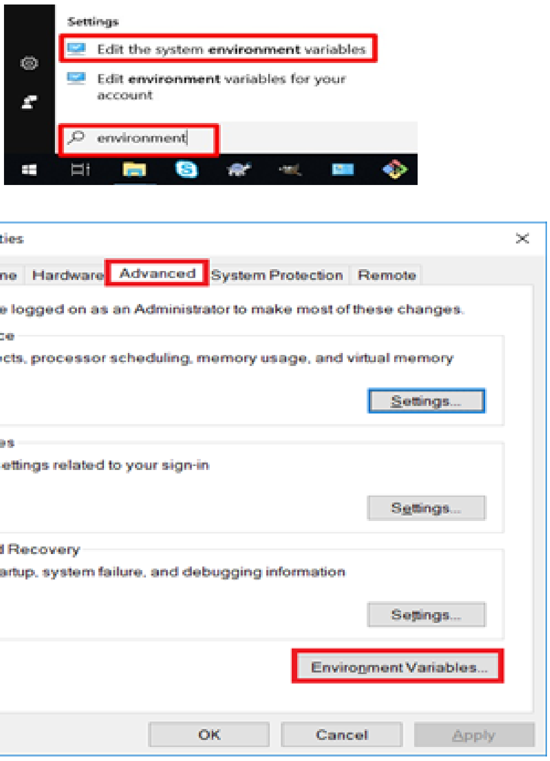

Figure 26. Editing System Environment Variable

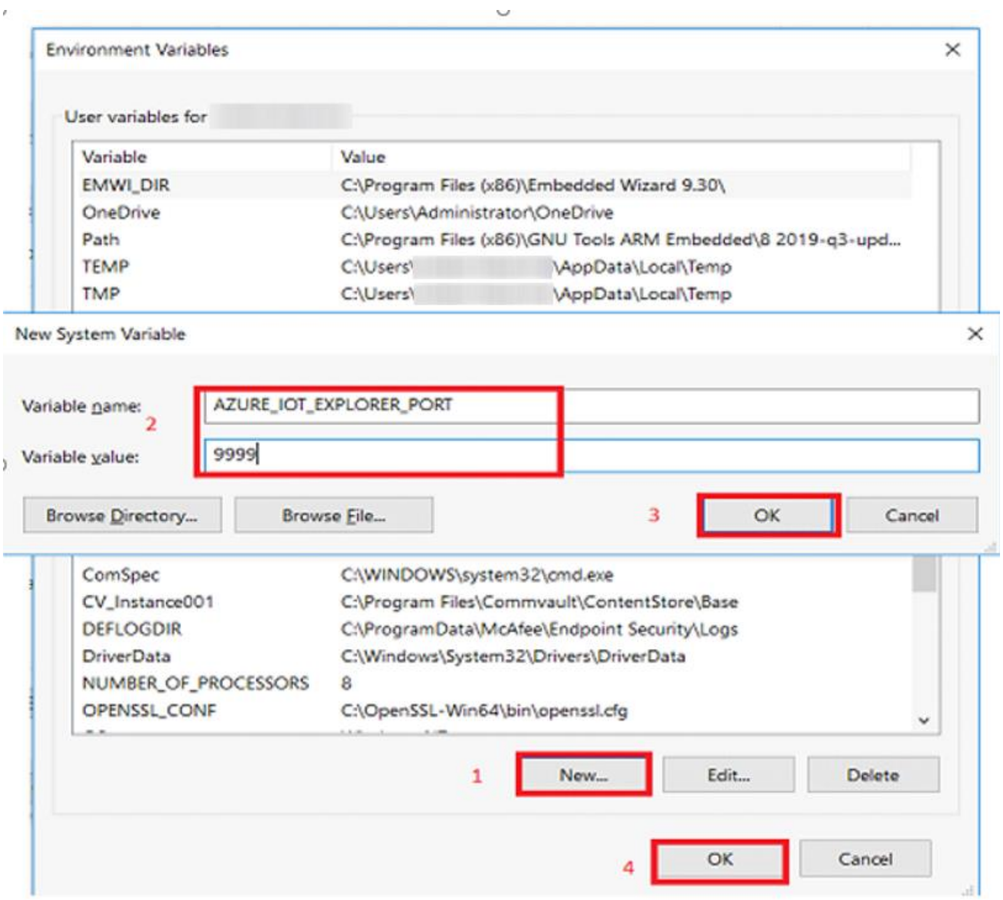

Figure 27. Adding System Environment Variable for Alternate Port - Azure IoT Explorer

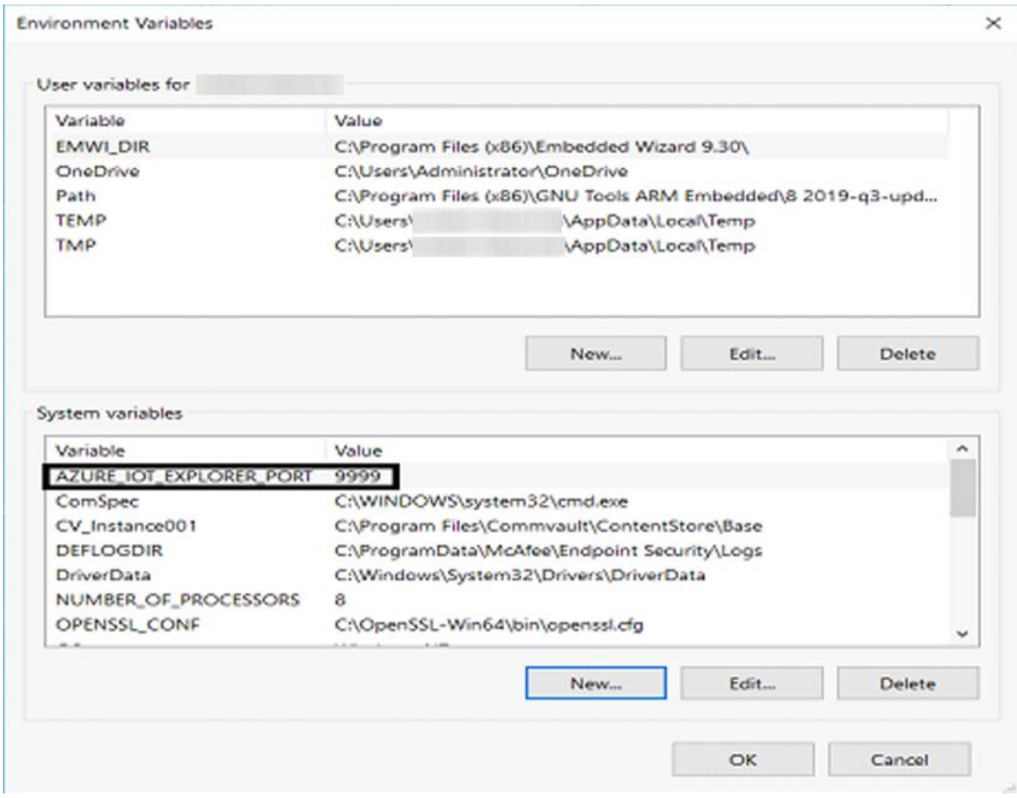

Figure 28. Added Alternate Port for Azure IoT Explorer

If the connection succeeds, the Azure IoT Explorer switches to a **Devices** view and lists your device.

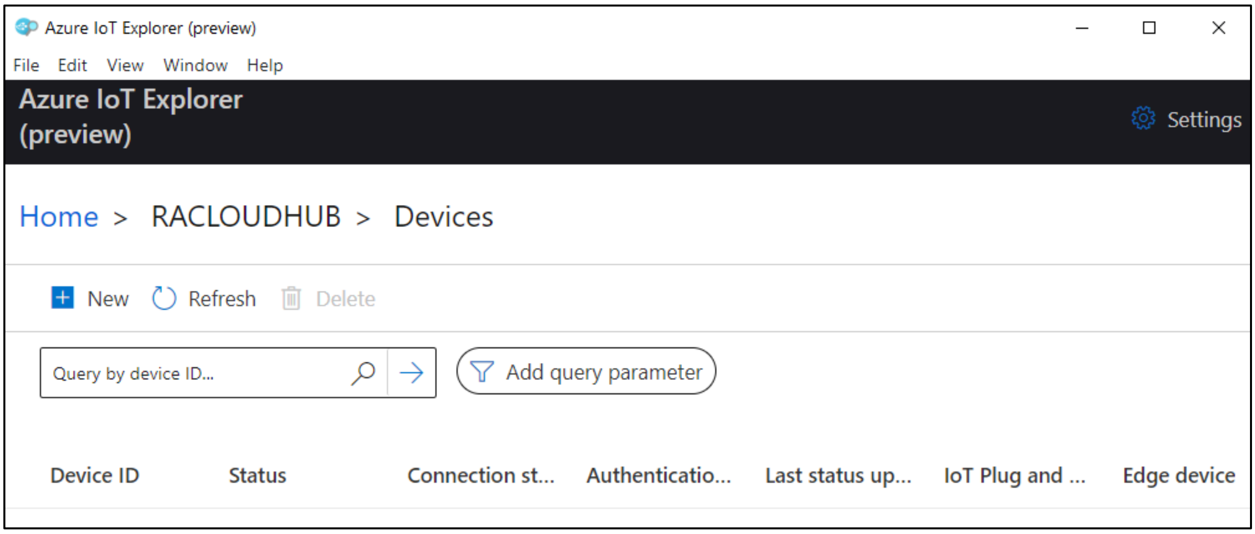

Figure 29. Listed Devices

3.8 Register an IoT Hub Device

In this section, you create a new device instance and register it with the IoT Hub you created. You will use the connection information for the newly registered device to securely connect your physical device in a later section.

To register a device:

1. You can Create Device with help of Azure IoT Explorer shown as follows:
   Click on **New**.

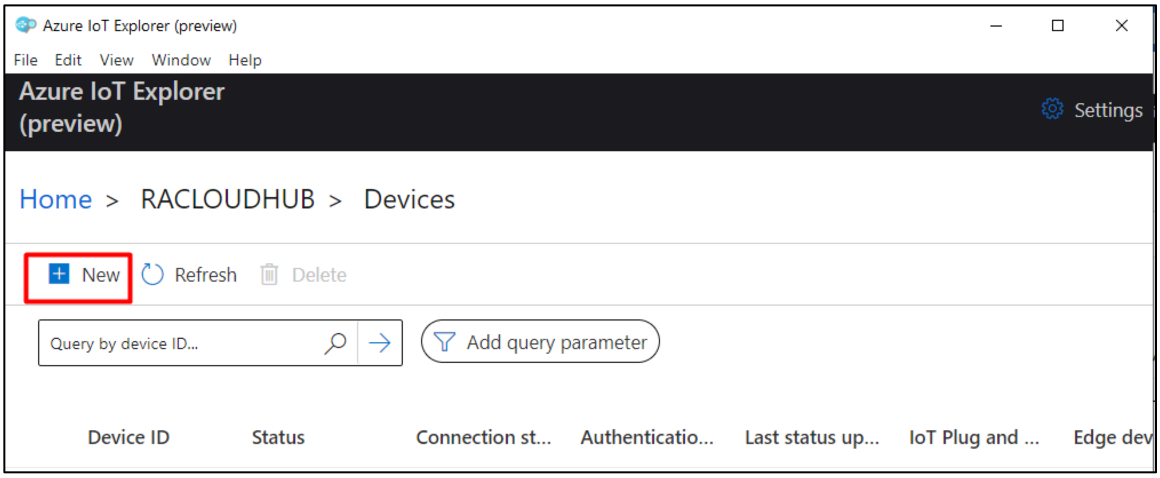

Figure 30. New Device Creation Process with Azure IoT Explorer

2. In this stage, you have to give Device ID, Authentication type, Primary thumbprint, Secondary thumbprint then click on **Create**. Use fingerprint generated in Figure 23 in section 3.5, Certificate Creation Process for the primary and secondary thumbprints. Follow steps 1-5 in Figure 31, to create the device.

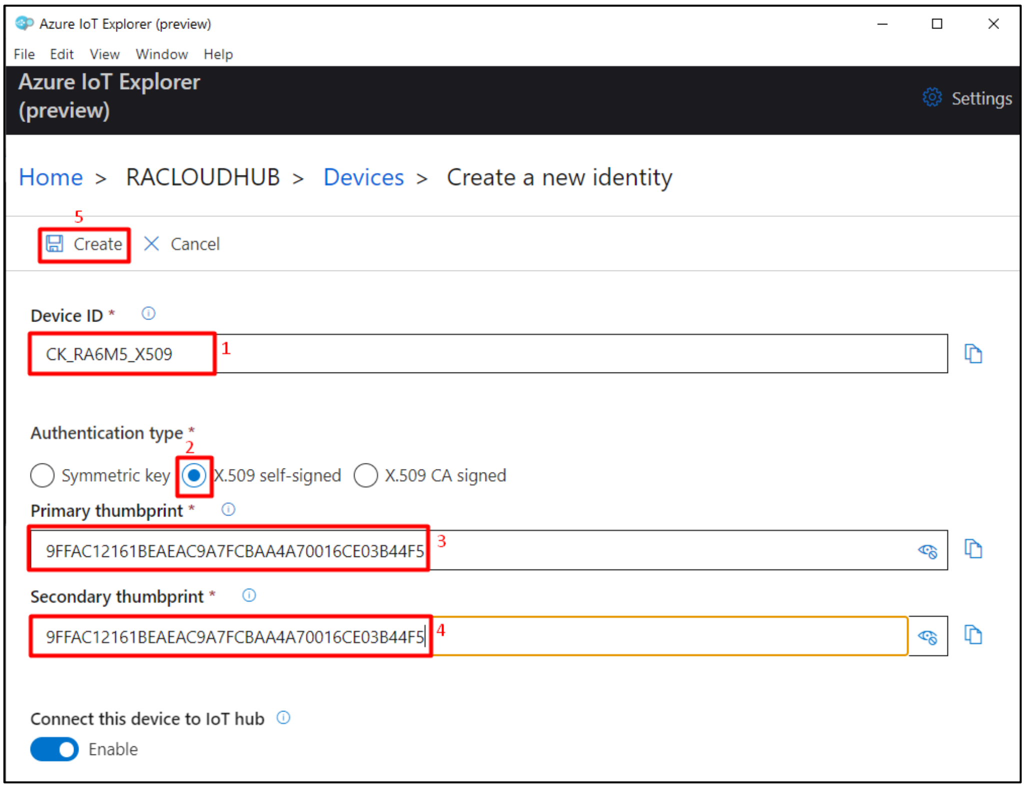

Figure 31. Naming, Authentication type and Thumbprints

3. You can see your created device in Devices section of Azure IoT Explorer

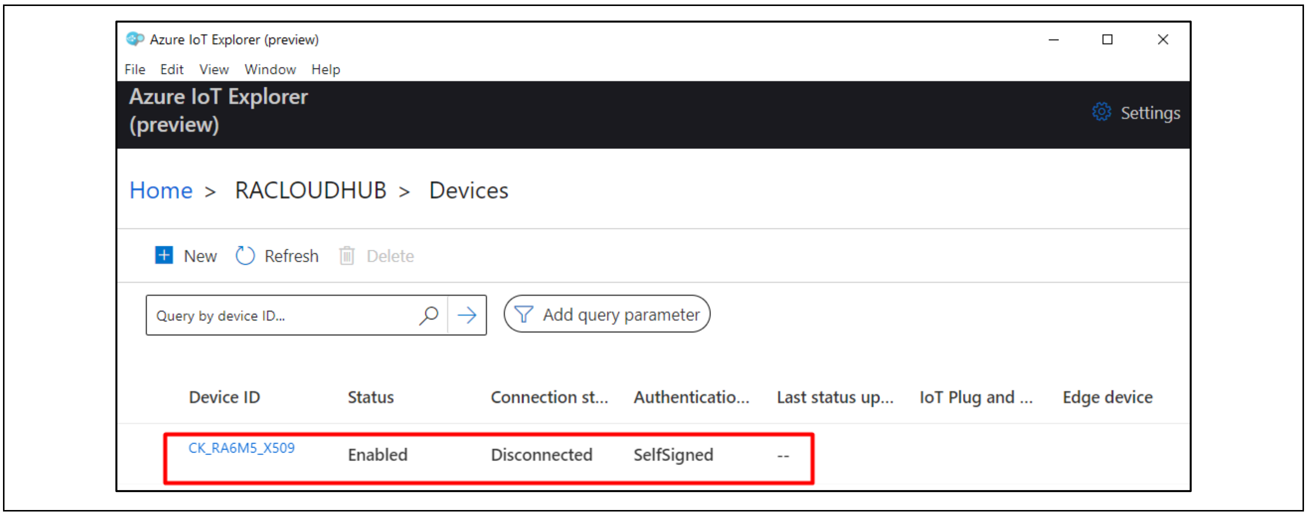

Figure 32. Newly Created Device

3.9 Prepare the Device

To connect the device to Azure, modify a configuration file for Azure IoT settings (of your Device ID and Hostname), build and flash the imageto the device.

Add configuration

1. Import the application project into an empty e[2] studio. Open `sample_config.h` and make the changes to the configuration as shown in the snapshot with your host name, device ID and USE_DEVICE_CERTIFICATE.

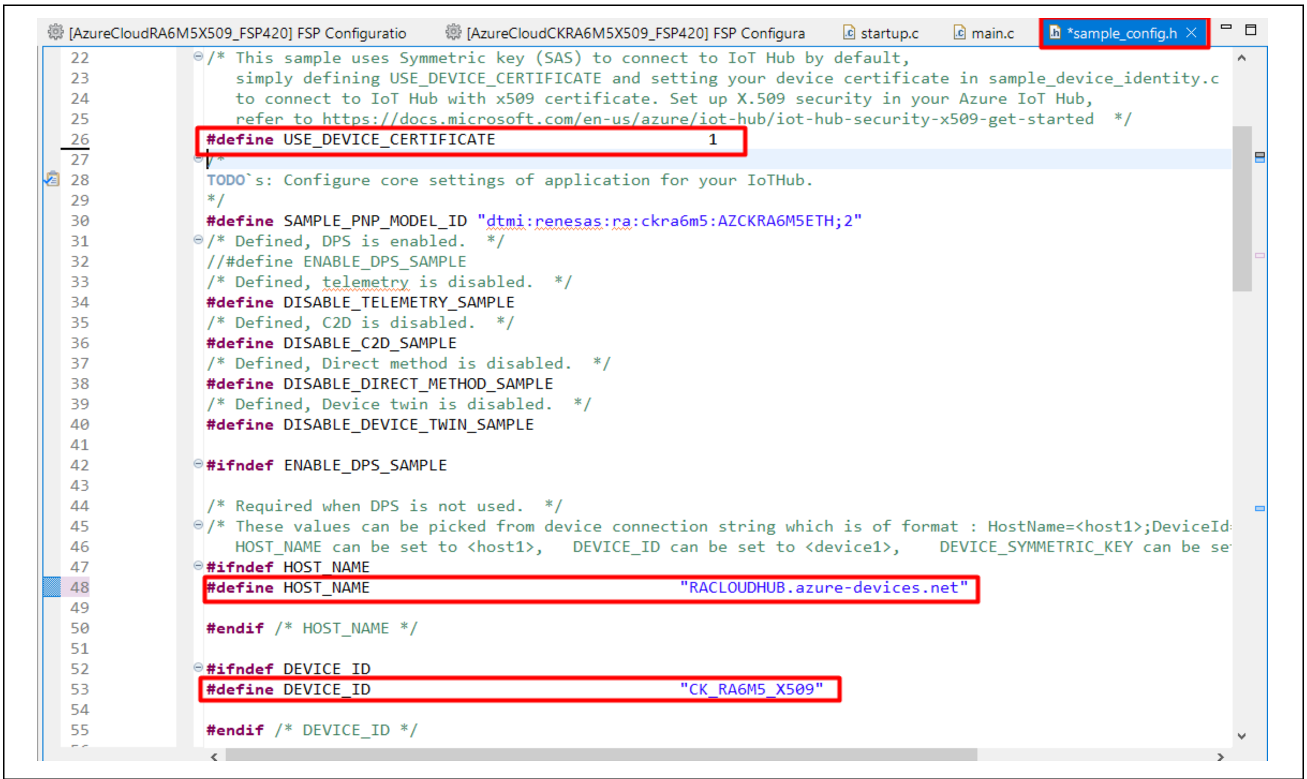

Figure 33. Configuration Changes to sample_config.h

Constant name	Value
`HOST_NAME`	{Your IoT hub hostName value}
`DEVICE_ID`	{Your deviceID value}
`USE_DEVICE_CERTIFICATE`	1

3.10 Building and Running the Application

The project is now ready to compile. Press the **Build** (hammer icon) to start building the project.

Figure 34. Starting to Build the Project

The toolchain will report compilation and build status to the console pane in the lower-right corner of e[2]studio. When the build has completed, confirm that there are zero errors and few warnings. Warnings, if any, may result from highly restrictive compilation warnings settings being applied by e[2] studio to third partycode.

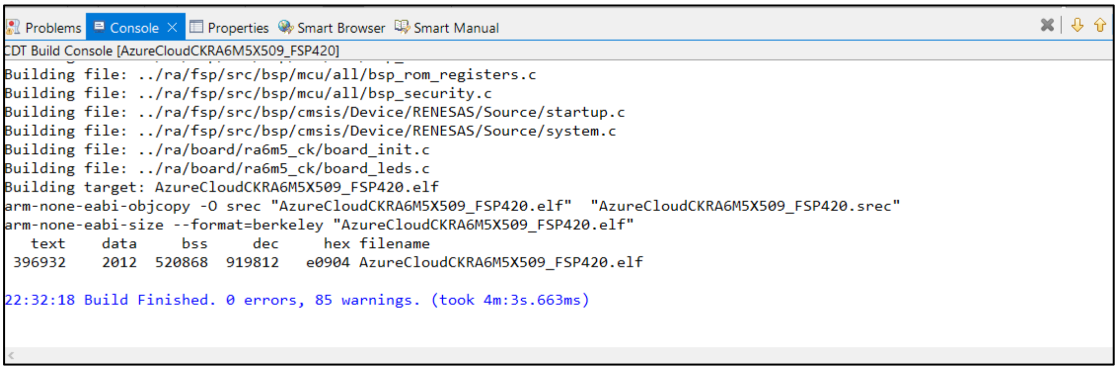

Figure 35. Compilation and Build Status Report

3.11 Download and Run the Project

1. Connect the micro-USB cable to the DEBUG1 port (J14) of the CK-RA6M5 Cloud Kit and other end to the host computer.
2. Connect the second USB Cable to J20 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.
3. Make sure the Cellular Module is connected to the PMOD2 of the board and other end to the supplied antenna.
4. In e[2] studio, open the **Debug Configurations** dialog and launch the **AzureCloudCKRA6M5X509_FSP440 Debug_Flat** debug configuration.

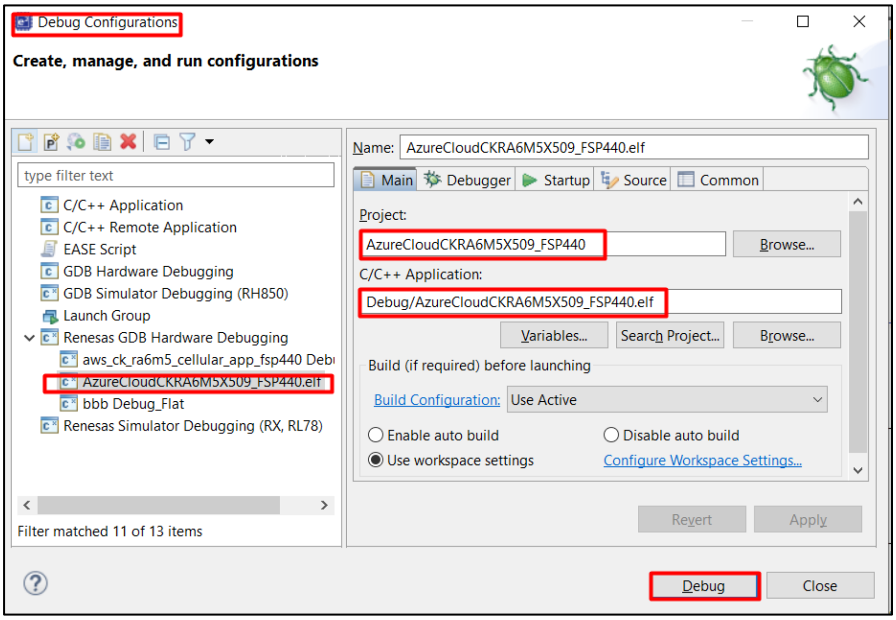

Figure 36. Start Debug

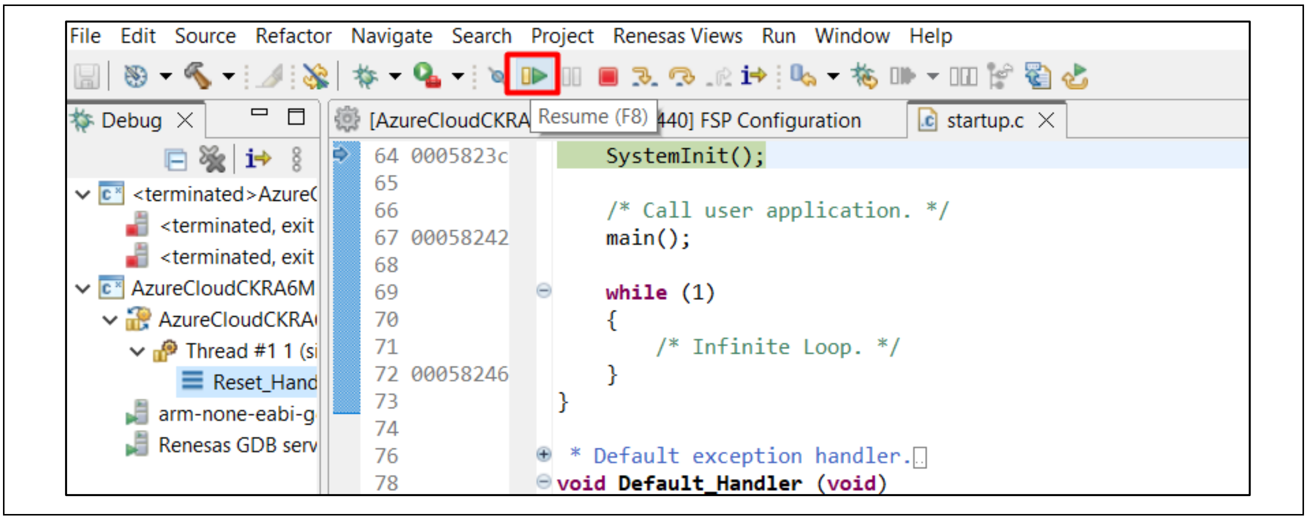

Figure 37. Resume the Debug

5. To view output, you have use serial terminal like tera term. To know your COM port, 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.

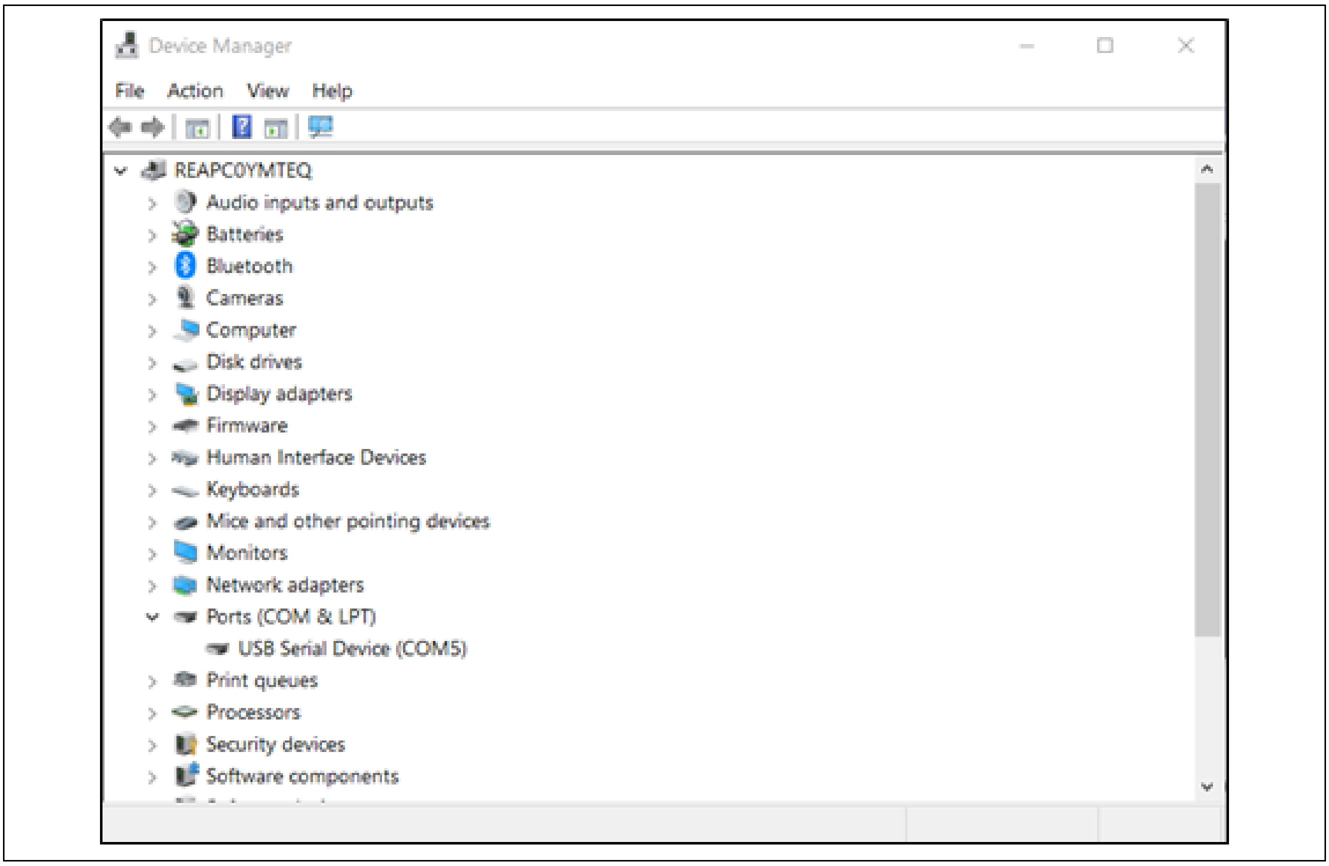

Figure 38. USB Serial Device in Windows Device Manager

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

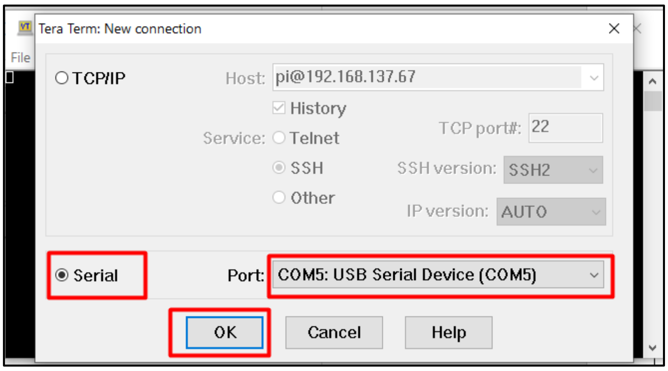

Figure 39. Selecting the Serial Port on Tera Term

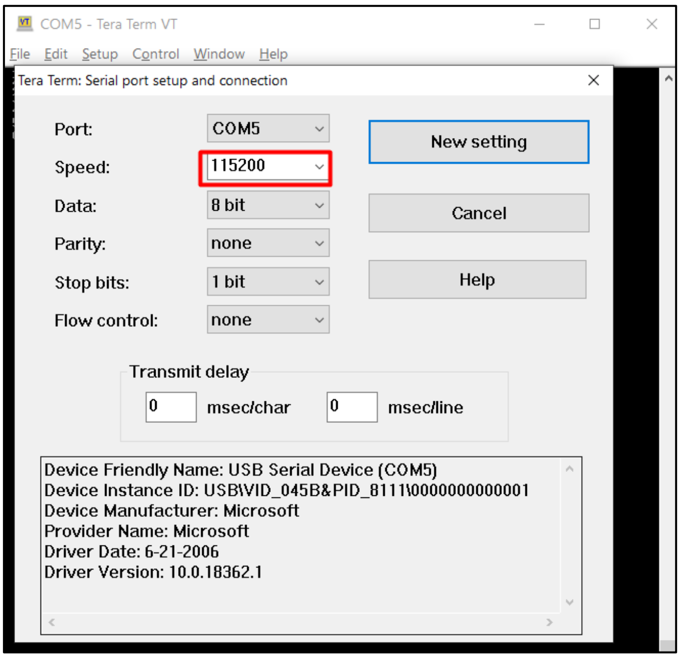

Figure 40. Select 115200 on the Speed Pulldown

7. Using the **Setup** menu pull-down, select **Serial port…** and ensure that the speed is set to **115200**, shown as follows.
8. Complete the connection. The Configuration CLI Menu will be displayed on the console shown as follows.
   Note: Please reset the board by pressing the S1 user switch if the menu is not displayed.

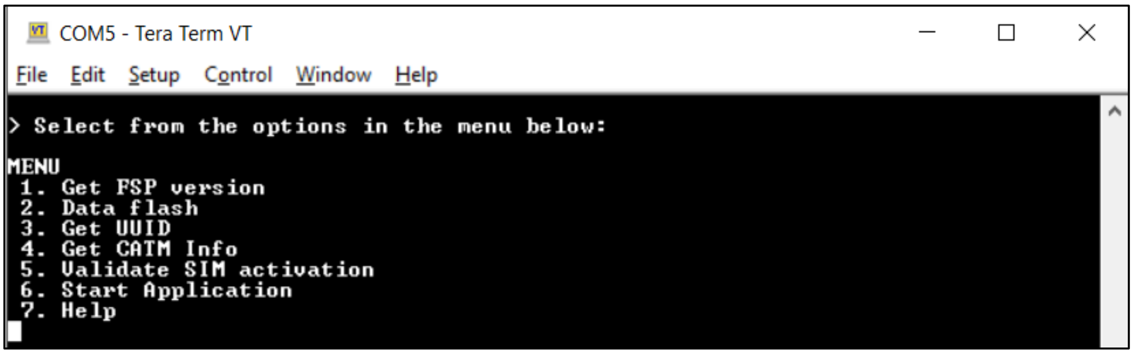

Figure 41. Main Menu

9. Here you can select options from the MENU by pressing key **1 to 7**. Press spacebar to go to previous menu.
10. User can get FSP Version by pressing key 1, and UUID by pressing key 3, as follows.

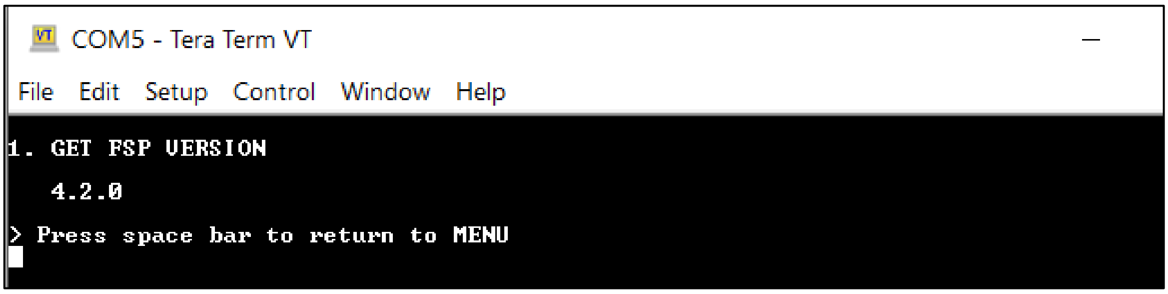

Figure 42. FSP Version Information

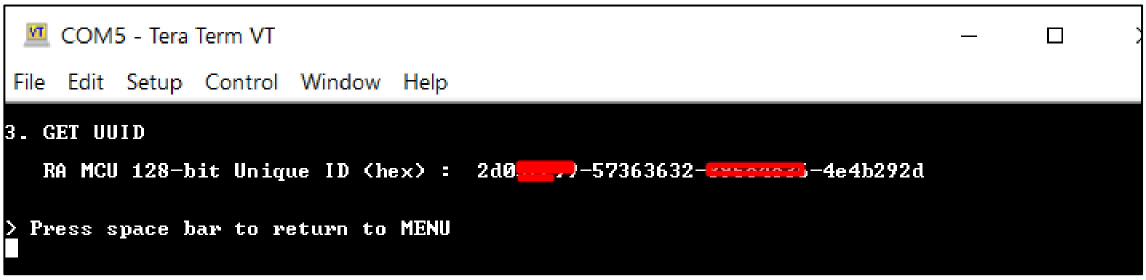

Figure 43. Getting Board UUID Information

11. 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 **3.12 Activating the SIM card).**

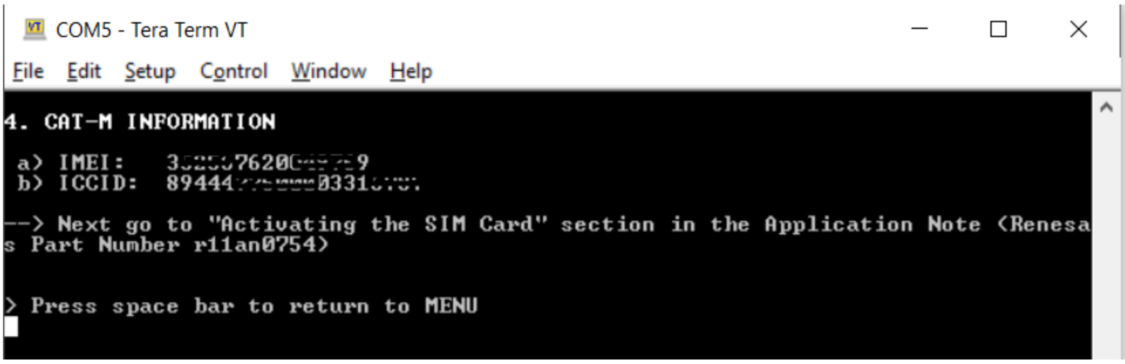

Figure 44. Getting CAT-M Information

3.12 Activating the 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.**

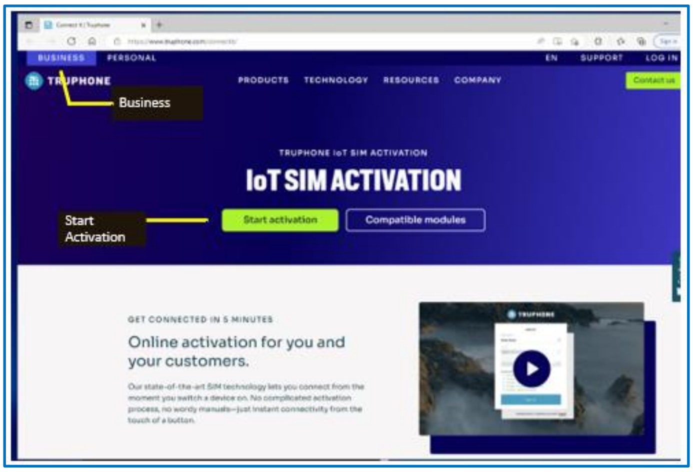

Figure 45. Activating the SIM card

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 Application project**. See the **ICCID** value in **Figure 44. Getting 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 */`

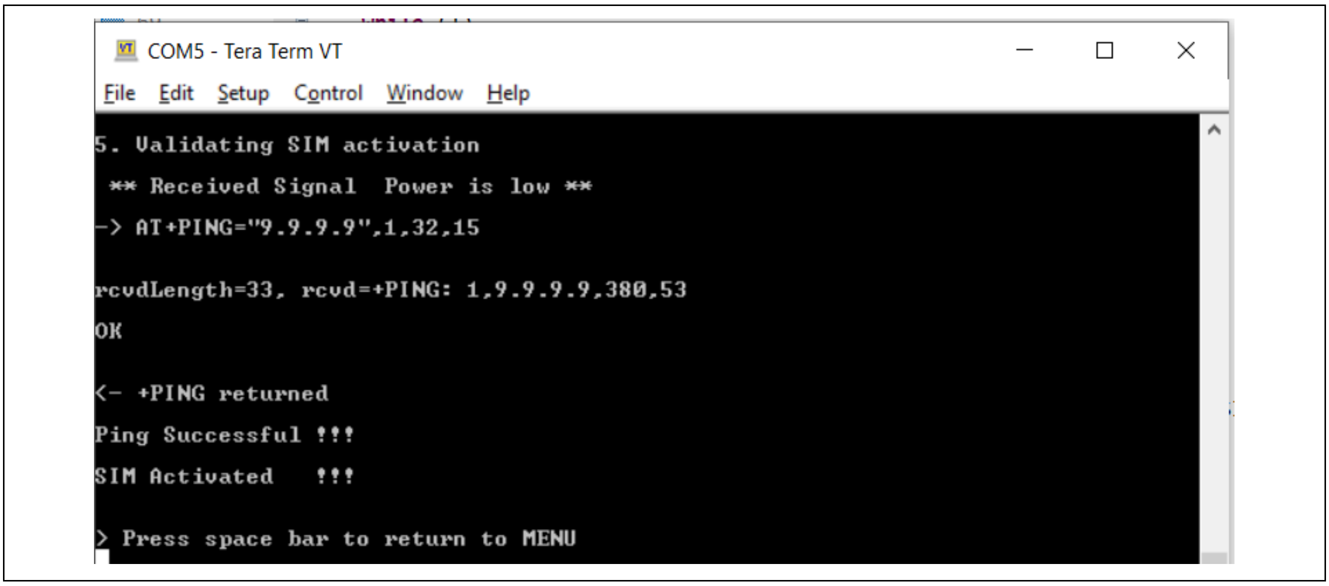

Figure 46. Validating SIM Activation – SIM Card Active

3.13 Storing Device Certificate, Host Name, Device ID

Reset the board by pressing the S1 user switch if the menu is not displayed.

Figure 47. Main Menu

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.

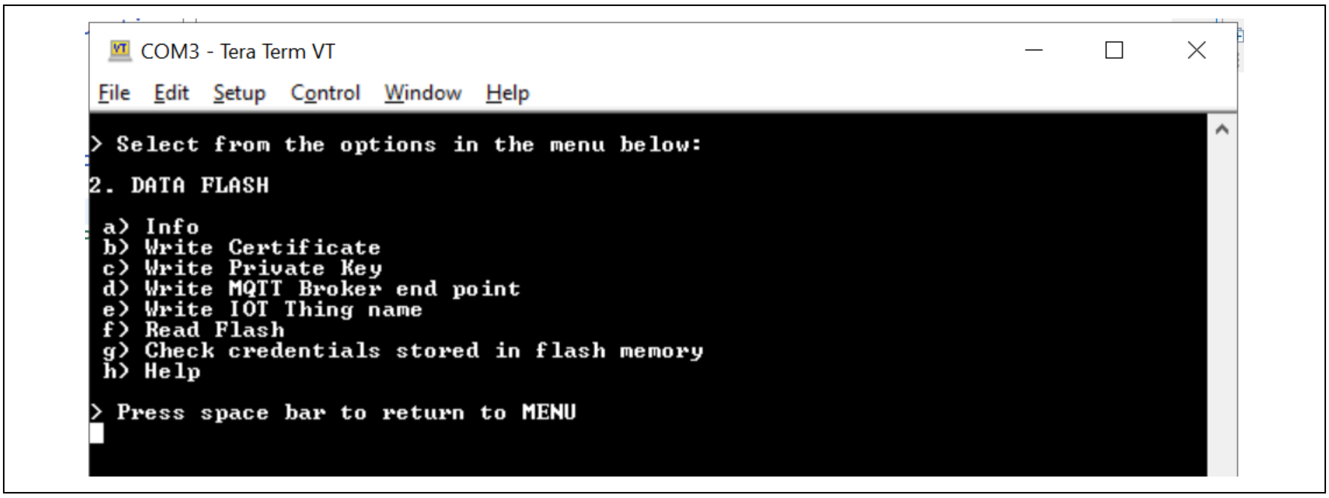

Figure 48. Data Flash Menu

2. Press **b** for Write Certificate**.**

Figure 49. Select File to Write Data in Data Flash.

3. Go to **Tera Term > File > Send file**

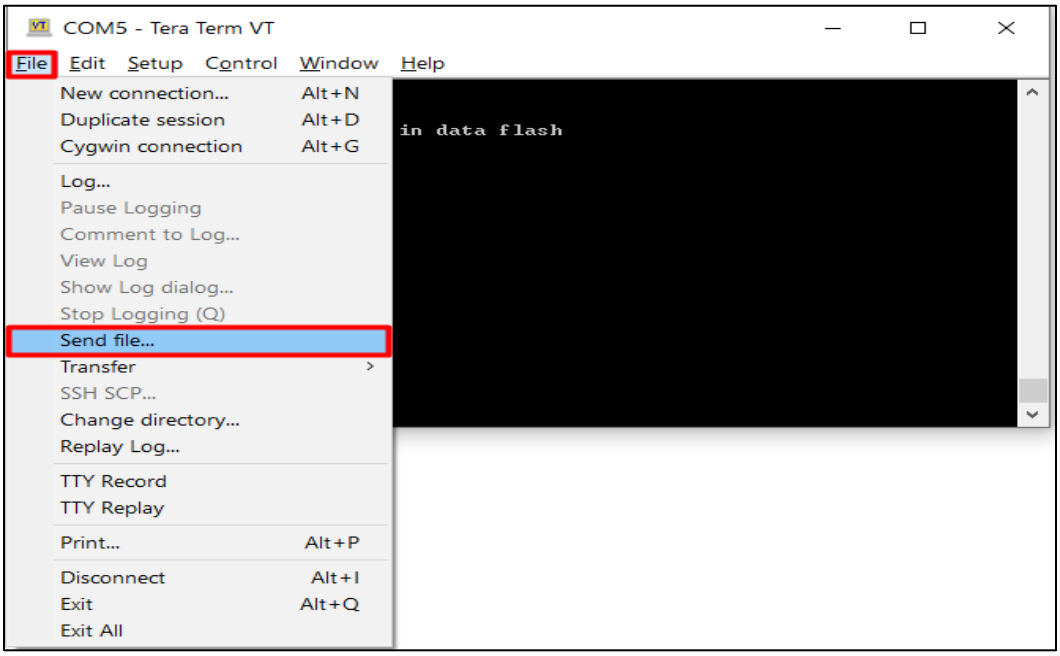

Figure 50. Send File Option in File Menu

4. Browse to the folder where X509 certificates are generated as part of the section 3.5, Certificate **Creation Process**. Select **cert.pem**. Press **Open**.

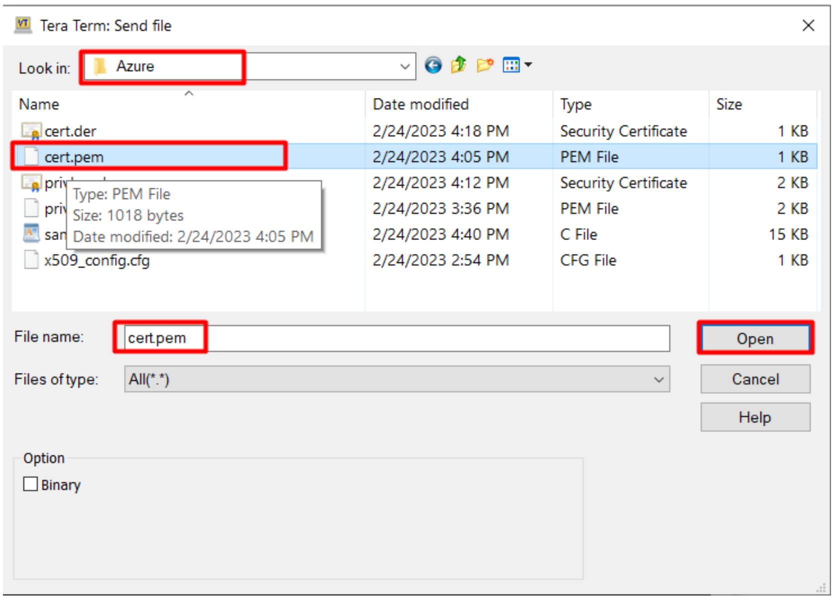

Figure 51. Browse, Select and Open the File to be Written

5. Status of Device Certificate Downloading is as follows:

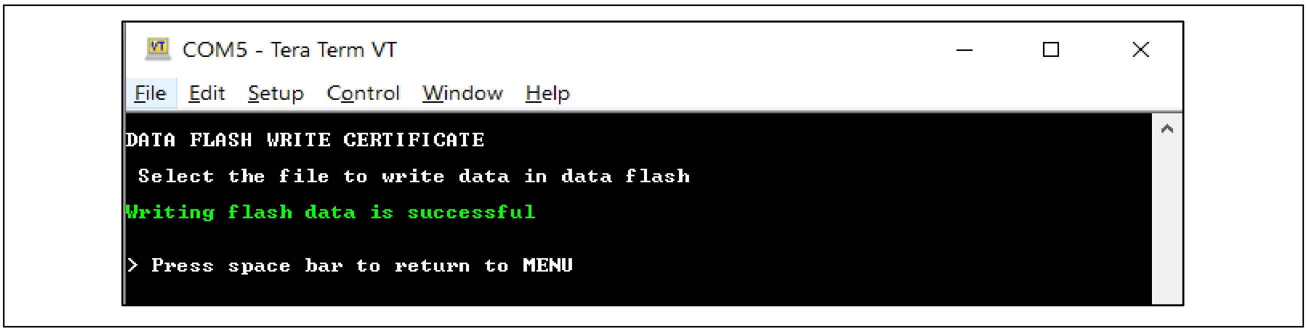

Figure 52. Status of File Writing Process

6. To store the device private key, go back to data flash menu by pressing the space bar key. **Press c** in **Data Flash menu**, go to **Tera Term > File > Send file** Select file **privkey.pem** from the folder where you have generated Certificates.
7. To store MQTT Broker End point aka **Host Name,** first copy Host Name without double quotes then **press d** in **Data Flash** menu, Go to **Tera Term > Edit > Paste<CR>,** you will get copied Host Name in the clipboard, please verify and confirm it and press **OK**

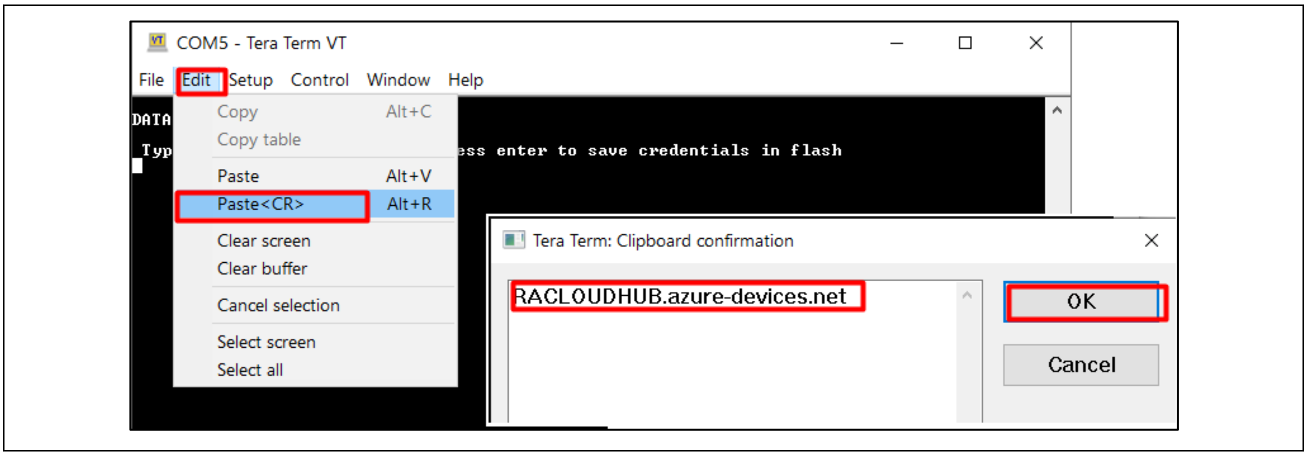

Figure 53. Input MQTT Broker End point aka Host Name

8. To store IoT Thing Name, that is, **DEVICE ID**, first copy DEVICE ID created without double quotes, **press e** in **Data Flash** Menu and follow the procedure in step 5.

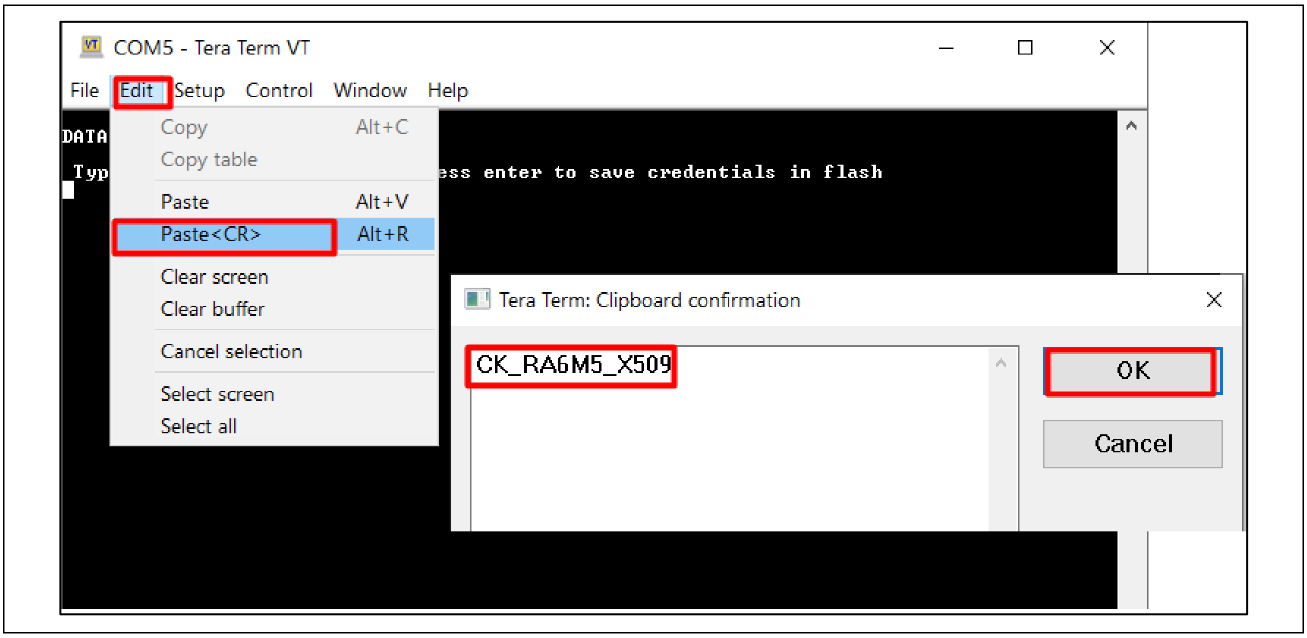

Figure 54. Input Device ID aka IoT Thing Name

9. To verify the data stored in Datas Flash, **press f** in Data Flash menu, scroll down to see data**.**

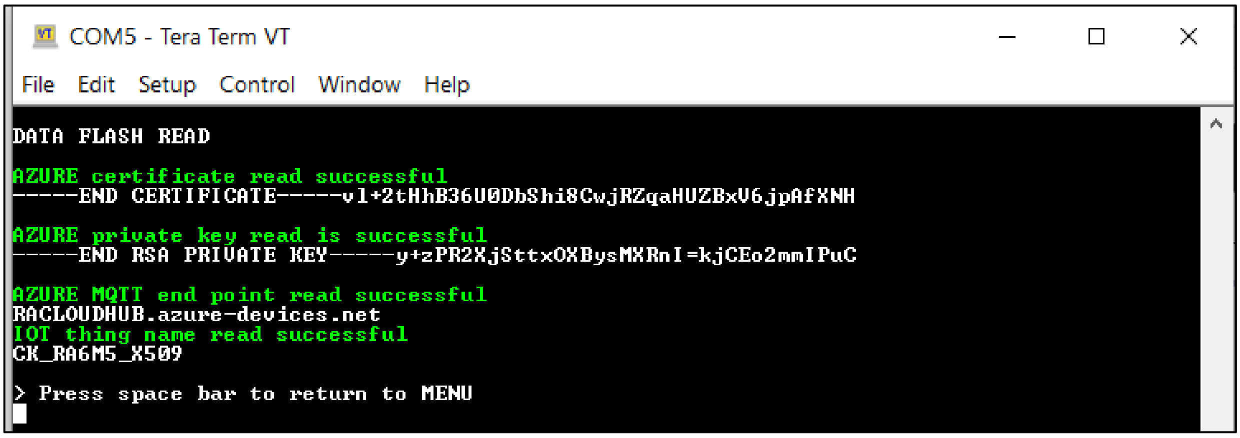

Figure 55. Scroll Down and Verify the Data Stored in Data Flash

10. To check credentials stored in Data Flash, **press g.**
11. Press spacebar to go to previous menu or main menu.
12. Press **6** to start the application from the main menu.
13. Serial terminal output on successful start of application

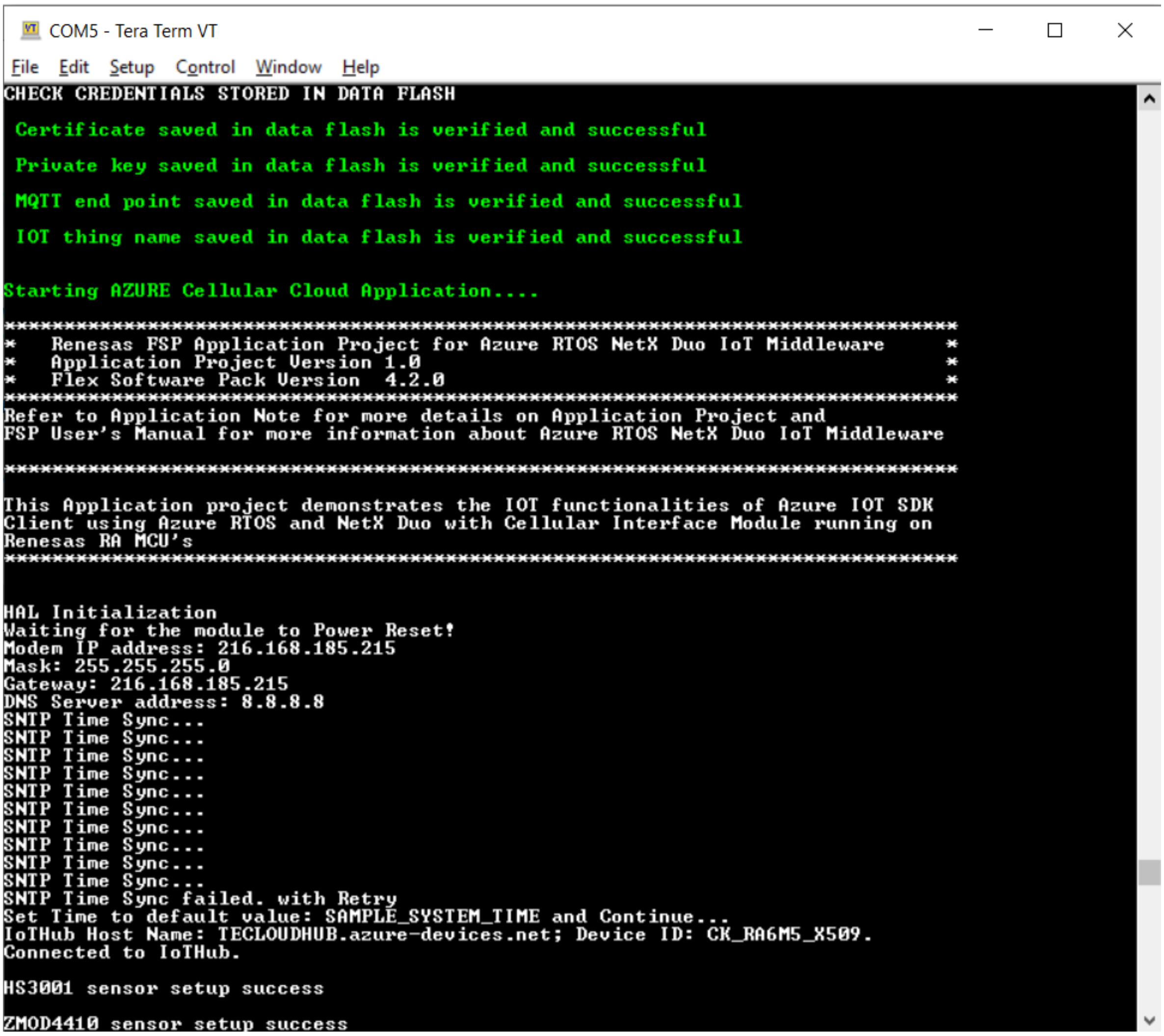

Figure 56. Device Connected to Azure IoT Hub

14. Sensor Data Output on Serial Terminal.

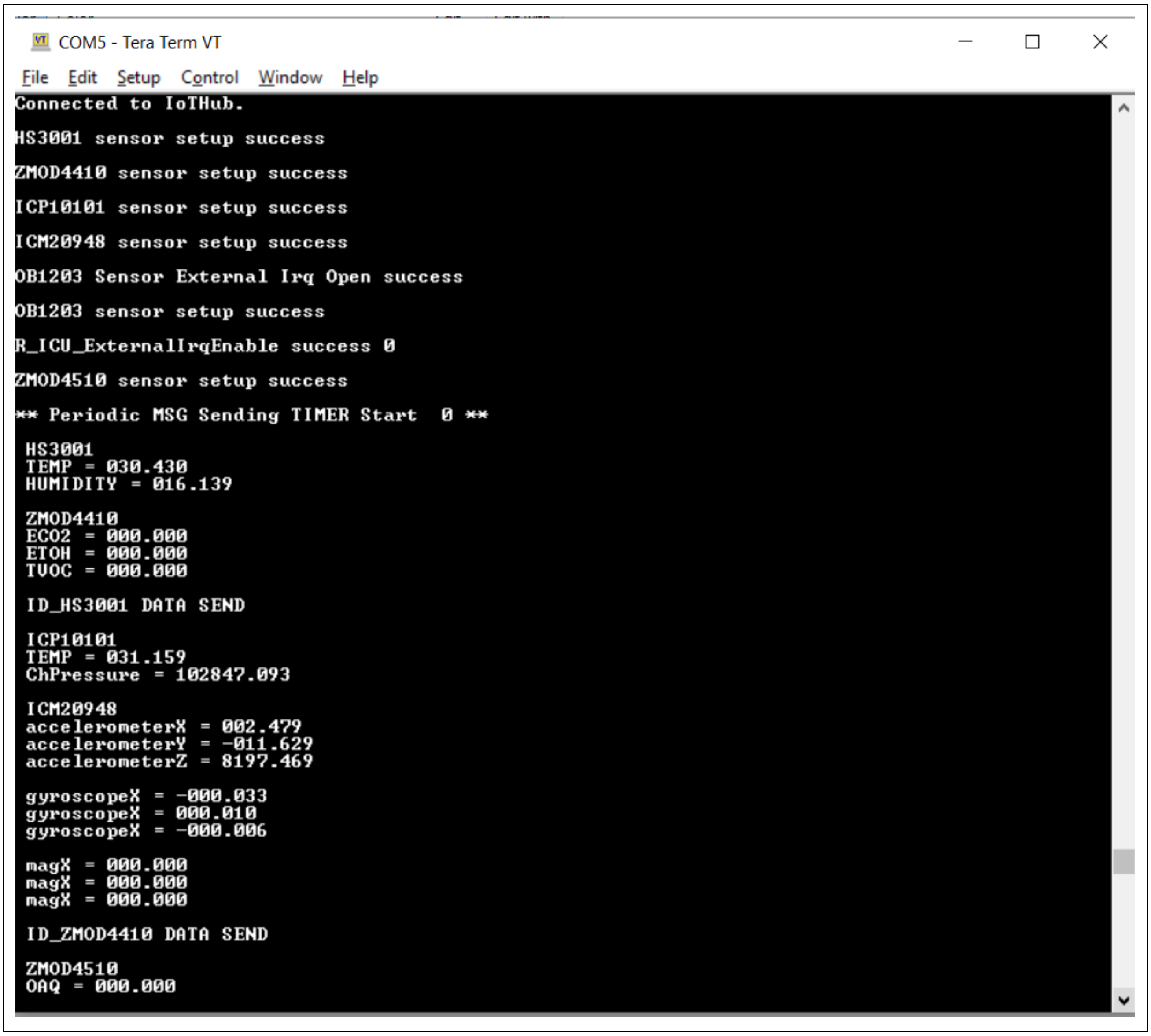

Figure 57. Sensor Data on Serial Terminal

3.14 Send Device to Cloud Message

With Azure IoT Explorer, you can view the flow of telemetry from your device to the Cloud. To view telemetry in Azure IoT Explorer:

1. In IoT Explorer select your created IoT Hub and click on **view devices in this hub**, click on the created device (Device ID). Finally select the **Telemetry (Home > TECLOUDHUB > Devices > CK_RA6M5_X509 >Telemetry)**. Confirm that **use built-in event hub** is set to **Yes**.
2. Select **Start**.
3. View the telemetry as the device sends messages to the Cloud.

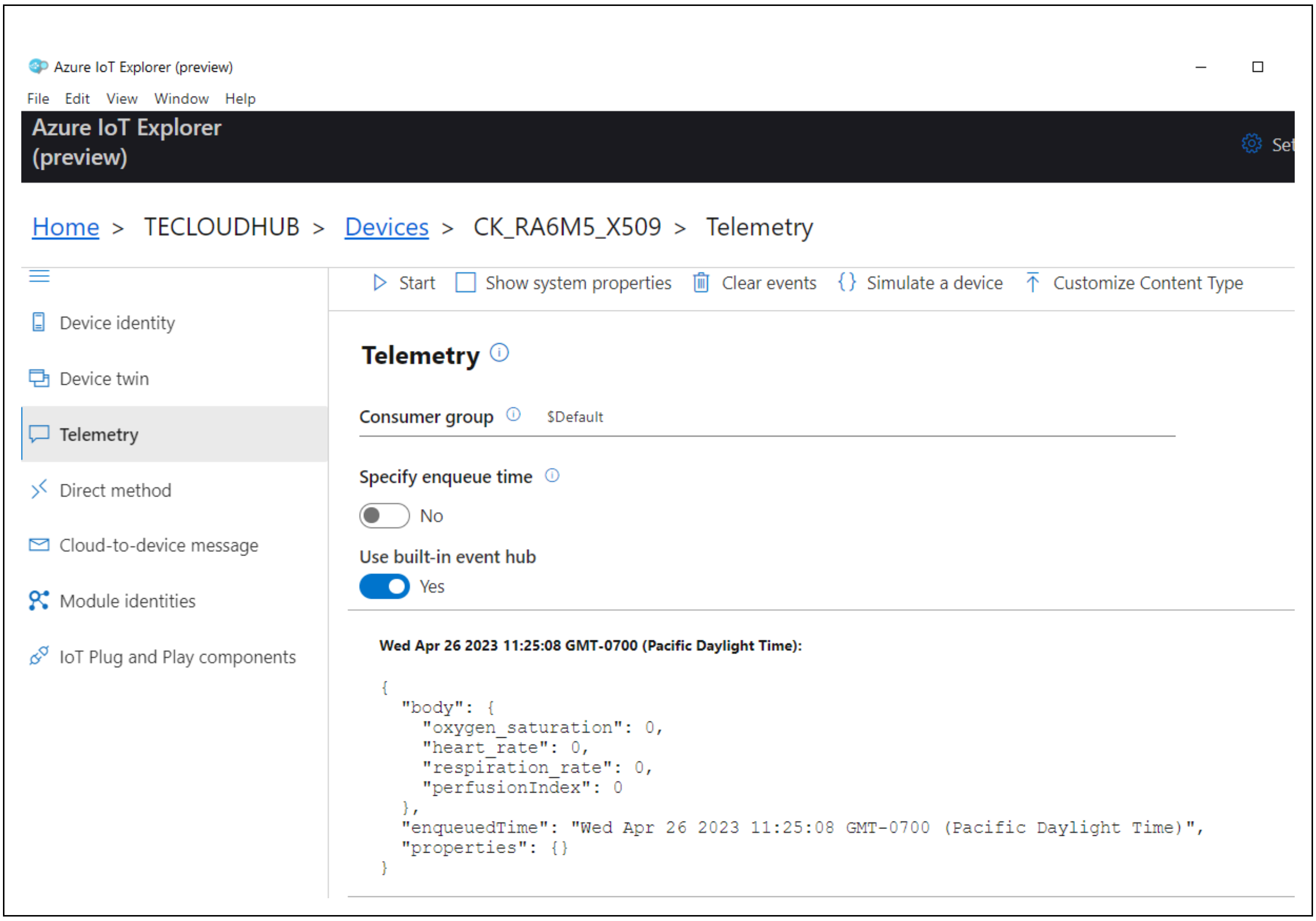

Figure 58. Device Telemetry Details

3.15 Send Cloud-to-Device Message

To send a Cloud-to-device message in Azure IoT Explorer:

1. In IoT Explorer select **Cloud-to-device message**.
2. Enter the message in the **Message body** = "**LED**", **Key** = **LED**, **Value** = **Given in Table**
3. **Check** Add timestamp to message body.
4. Select **Send message to device.**

LED On Board	Value
LED2 (Tri Color LED)	TC_GREEN_ON, TC_RED_ON, TC_BLUE_ON TC_GREEN_OFF, TC_RED_OFF, TC_BLUE_OFF
LED4 BLUE	BLUE_ON, BLUE_OFF

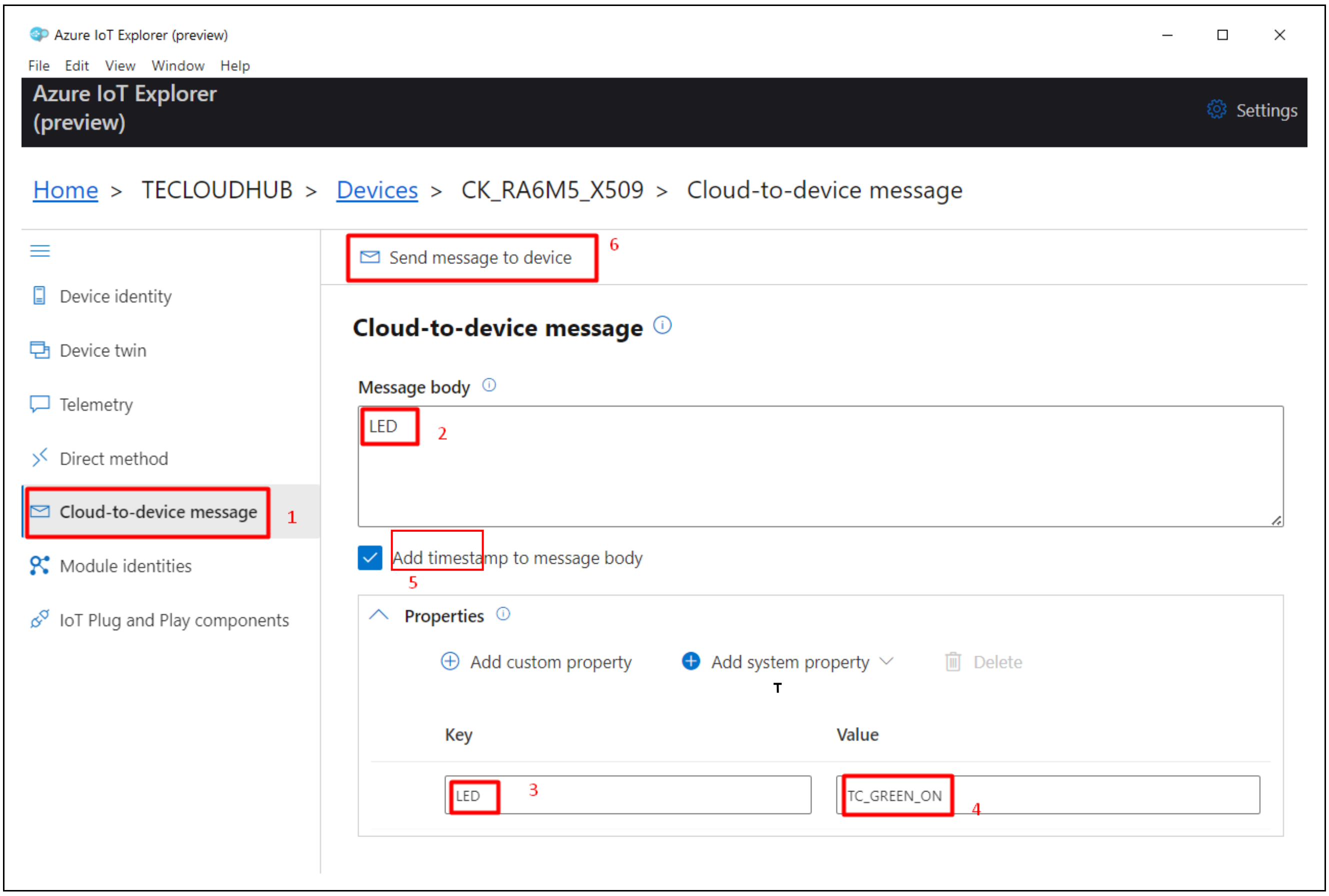

Figure 59. Device Telemetry Details

5. In the terminal window, you can see that the message is received by the IoT Device.

Figure 60. Serial Terminal Output

4. Importing, Building and Loading the Project

For a quick validation of this application project, import and build the project. The following steps show howto import, build, and download the project.

Note: To run the application project successfully and to communicate to the cloud, follow the instructions for setting up the cloud interface as described in the section **Error! Reference source not found.**, which d etails making changes to the credentials and creating your own cloud devices, running and validating the application.

4.1 Importing

The application project bundled as part of this app note can be imported into e^2 studio using instructions provided in the *RA FSP User's Manual*. See Section *Starting Development > e2 studio ISDE User Guide > Importing an Existing Project into e2 studio ISDE.*

4.2 Building the Latest Executable Binary

Upon successfully importing and/or modifying the project into e^2 studio IDE, follow 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.

4.3 Loading the Executable Binary into the Target MCU

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

4.3.1 Using a Debugging Interface with e^2 studio

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

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

4.3.2 Using J-Link Tools

SEGGER J-Link Tools such as J-Flash, J-Flash Lite, and J-Link Commander can be used to program the executable binary into the target MCU. Refer User Manuals UM08001, and UM08003 on www.segger.com.

4.3.3 Using Renesas Flash Programmer

The Renesas Flash Programmer (https://www.renesas.com/us/en/software-tool/renesas-flash-programmer-programming-gui) provides usable and functional support for programming the on-chip flash memory of Renesas microcontrollers in each phase of development and mass production. The software supports all RA MCUs and the software user's manual is available on renesas.com.

5. Next Steps and References

- Refer to the following GitHub repository for various FSP modules example projects and application projects (https://github.com/renesas/ra-fsp-examples/)
- Refer to *Establishing and Protecting Device Identity using SCE7 and Security MPU* (R11AN0449) on renesas.com
- Refer to *Securing Data at Rest Utilizing the RA Security MPU* (R11AN0416) on renesas.com.
- Refer to Azure GitHub link for more details on Azure SDK for Embedded C (https://github.com/Azure/azure-sdk-for-c)

6. MQTT/TLS References

- *FSP v4.4.0 User's Manual* (www.renesas.com/RA/FSP).
- Azure IoT documentation (https://docs.microsoft.com/en-us/azure/iot-hub/)

7. Known Issues and Limitations

1. Occasional outages in cloud connectivity may be noticed during the demonstration due to changes in the cloud server. Contact the Renesas support team for questions.
2. Currently, there is no support for direct device-to-device communications with Azure IoT Hub.
3. Device will reconnect after 65 minutes due to SAS token refresh. Currently it is under SDK control. Users need to know this when developing the application.

7.1 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.

8. Website and Support

Visit the following 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.31.23	—	Initial release
1.01	May.02.23		Added support for Truphone and updated to 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/.