Smart Lock with AWS IoT

Quick Start Guide of Smart Lock with AWS IoT

Rev.2.00
Jul, 2023

Introduction

This quick start guide describes the setup process of CN058-1 smart lock with AWS IoT. The device connects to AWS IoT Cloud Server by low power WIFI module DA16200, mobile phone connects to the AWS IoT by the designed “smart lock” App to monitor and control door lock situation. Provisioning DA16200, managing fingerprint, opening the door lock by NFC card or fingerprint, controlling the door lock and monitoring the status of the door lock can all be realized by this system. Highlighted parts in this demo include low power WIFI module DA16200, RA2E1 MCU with the optimized processing and Renesas’s low power process technology, Zhongyin fingerprint module with Renesas high performance low pin count MCU RX651, and NFC reader IC for contactless communication.

Target Device

DA16200 module

RA2E1 MCU

ZYCM01-AS168 fingerprint module with Renesas RX651

PTX105R Pmod

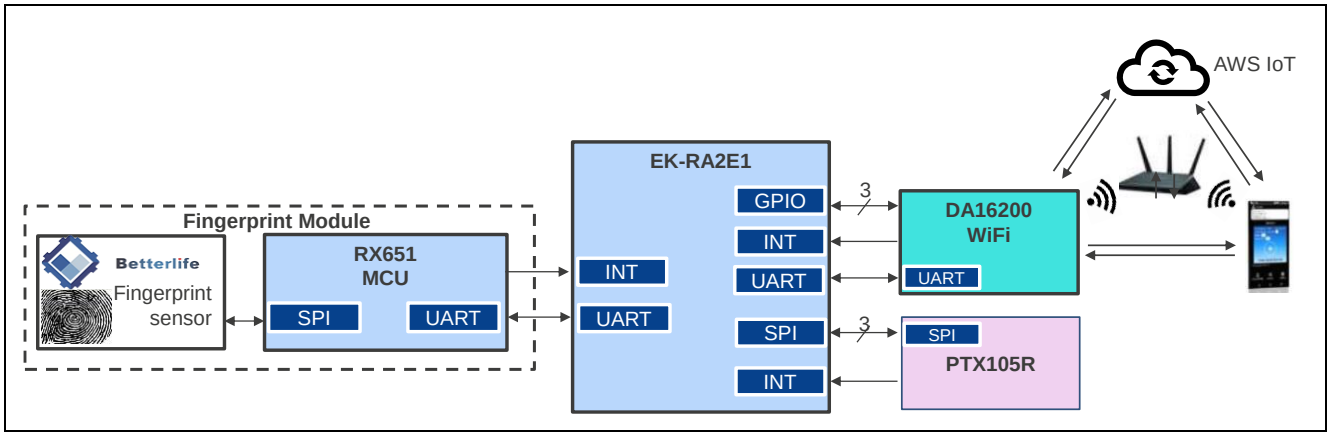
Contents

1) Kit Contents

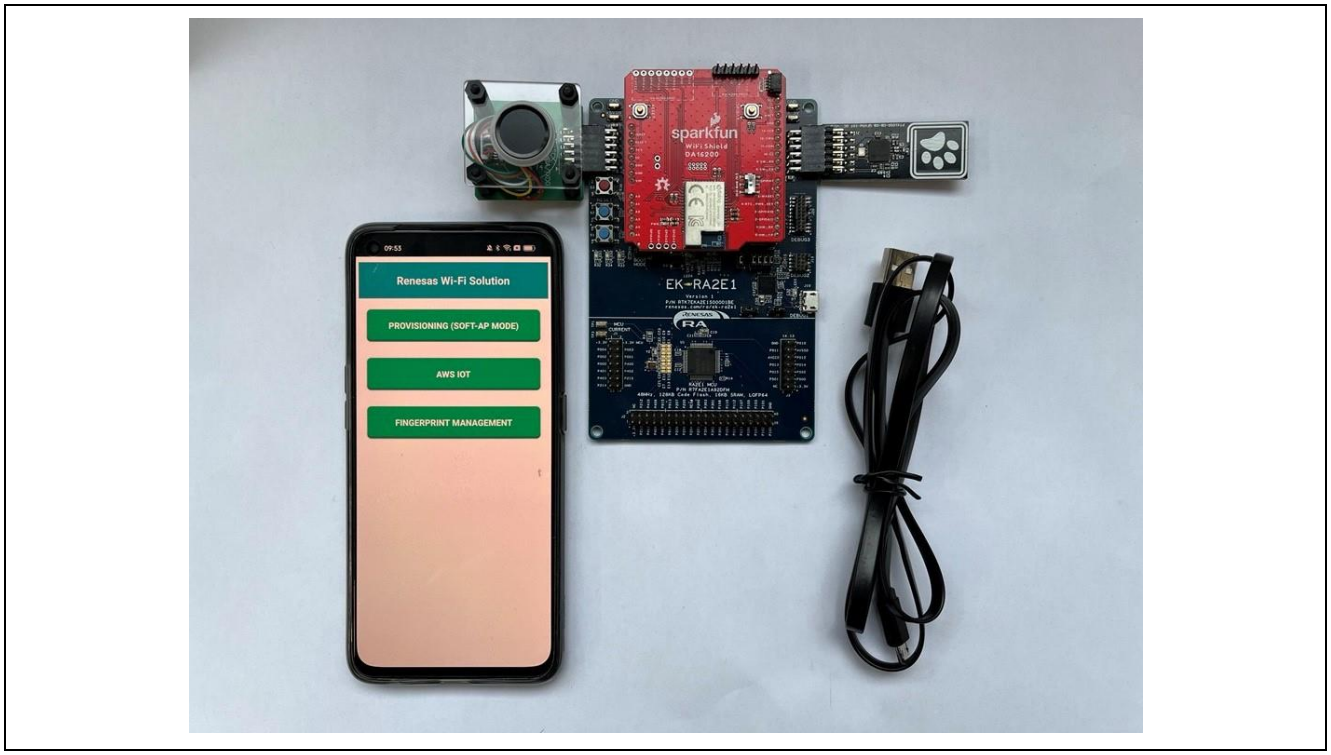
To set up this demo, the following components are needed:

1.1 Hardware Components

- EK-RA2E1
- SparkFun Qwiic WiFi Shield - DA16200, with Arduino interface
- ZYCM01-AS168 fingerprint module PMOD board
- PTX105R Pmod™ Board
- Mobile phone (Android Application)
- USB cable



System Block Diagram



System Image

1.2 Software Components

The following software components are needed:

Category		Item	Remark
MCU	Firmware	CN058_1_Smart_Lock_RA2E1_EUthing_0628.mot	Needs to be downloaded to RA2E1 MCU
	Software	SEGGER J-Link V7.22	A tool to program the firmware to MCU
DA16200 module	Image	DA16200_BOOT-GEN01-01-11003-000000_W25Q32JW.img DA16200_RTOS-GEN01-01-12627-000000.img DA16200_SLIB-GEN01-01-12283-000000.img	Either three img files or one ttl file need to be downloaded to DA16200
		Download_W25Q32JW_4MB.ttl	
	Software	Tera Term	A tool to program the firmware to DA16200
Mobile App	Android Application	Smart Lock.apk	An app for controlling and monitoring the system

2) Features

- Configure DPM (Dynamic Power Management) to DA16200 low power Wi-Fi module, supporting three types of sleep mode.
- Enroll new user's names and their fingerprints, or delete existed fingerprints from App through fingerprint management page on mobile phone's App.
- Open the door by enrolled fingerprint, NFC card, button on board or key on mobile phone's App. Close the door by button on board or key on mobile phone's App.
- Monitor the door's status and the like.
- All communication relies on AWS-IoT server with MQTT.

2.1 Fingerprint module

This fingerprint module integrates semiconductor sensor and fingerprint algorithm chip. It has the characteristics of small volume, low power consumption, simple interface, high reliability, good adaptability of dry and wet fingers, and fast fingerprint search speed, and also with self-learning function.

2.1 EK-RA2E1

Evaluation Kit for RA2E1 MCU Group, enables users to seamlessly evaluate the features of the RA2E1 MCU group and develop embedded systems applications using Flexible Software Package (FSP) and e2 studio IDE. R7FA2E1 MCU, a RA family's entry line single-chip microcontroller based on the 48-MHz Arm® Cortex®-M23 core, has the industry's most energy-efficient Ultra-Low power character. The on-board debug functionality makes it more convenient to use.

2.2 SparkFun Qwiic WiFi Shield - DA16200

The DA16200MOD is a fully integrated Wi-Fi® module with ultra-low power consumption, best RF performance and easy development environment. It is built from the ground up for the Internet of Things (IoT) and is ideal for door locks and other IoT devices.

2.3 NFC module

The PTX105R Pmod board is fully integrated into the Quick-Connect IoT ecosystem and provides a full-featured high-end NFC reader solution for easy integration.

2.4 AWS-IoT server

Any control and detection information from or send to mobile phone must be forwarded through the network. Here AWS-IoT server acts as a medium to connect the device and the mobile phone.

3) Image

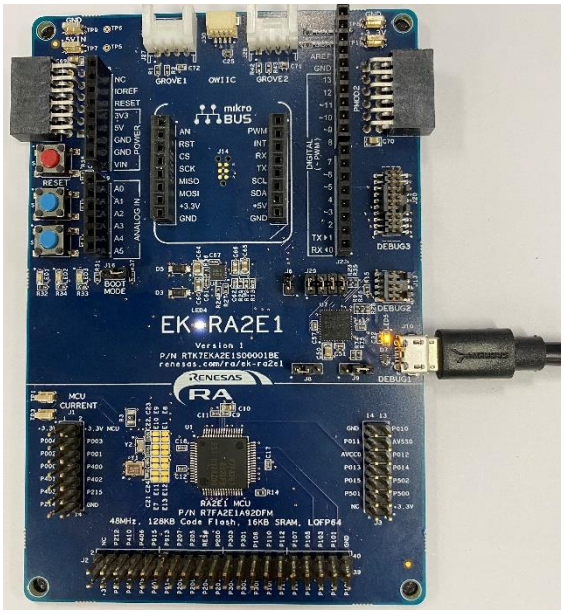
This demo realizes DA16200 DPM setting, fingerprint management, door lock opening by a few different ways, and door lock closing by button and App key. The mobile phone, as a remote controller and monitor, enrolling/deleting user's name information, open/close the door and observe the status of the system in real time.
For Android mobile phone, "smart lock" App designed by China SST is available.

Operation Image

4) Set Up the Demo

4.1 Download Code to EK-RA2E1 Board

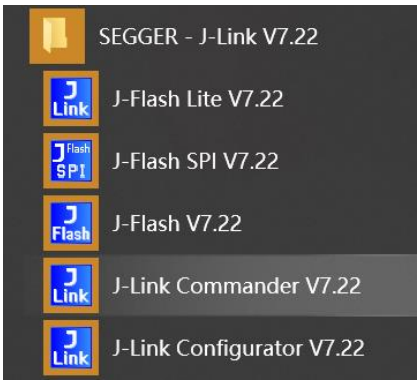
Step 1. Power EK-RA2E1 board by Micro USB cable.



Plug In Micro USB Cable

Step 2. Open J-Link Commander from Start menu in All Programs, SEGGER folder.

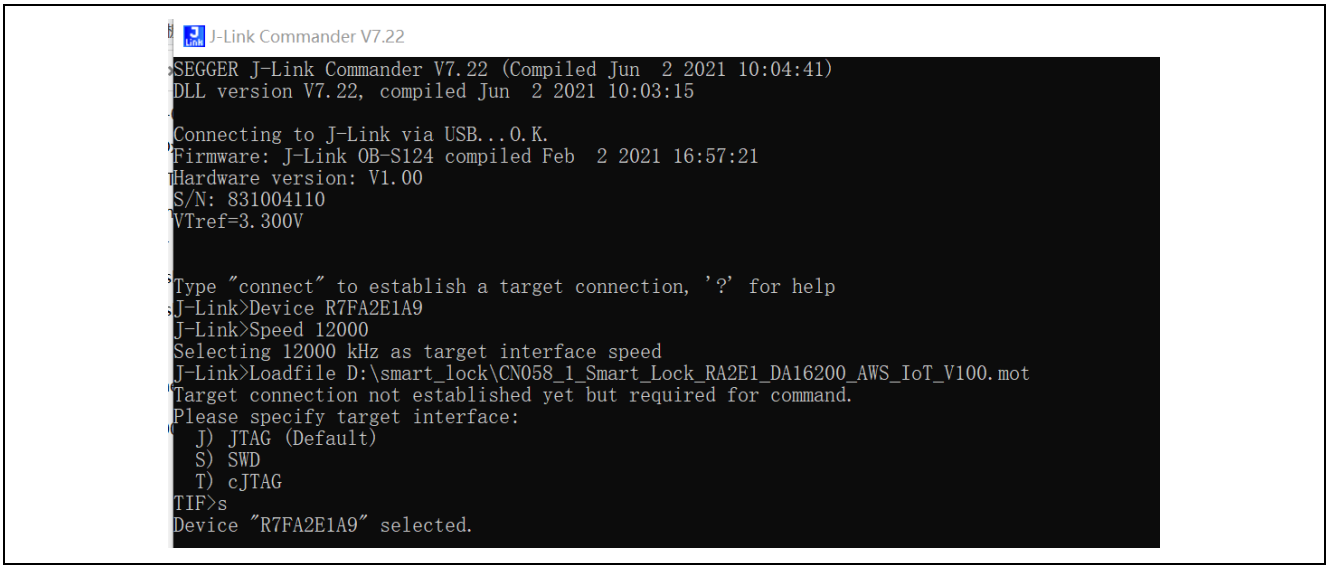
(Note: SEGGER J-Link download link: https://www.segger.com/downloads/jlink)



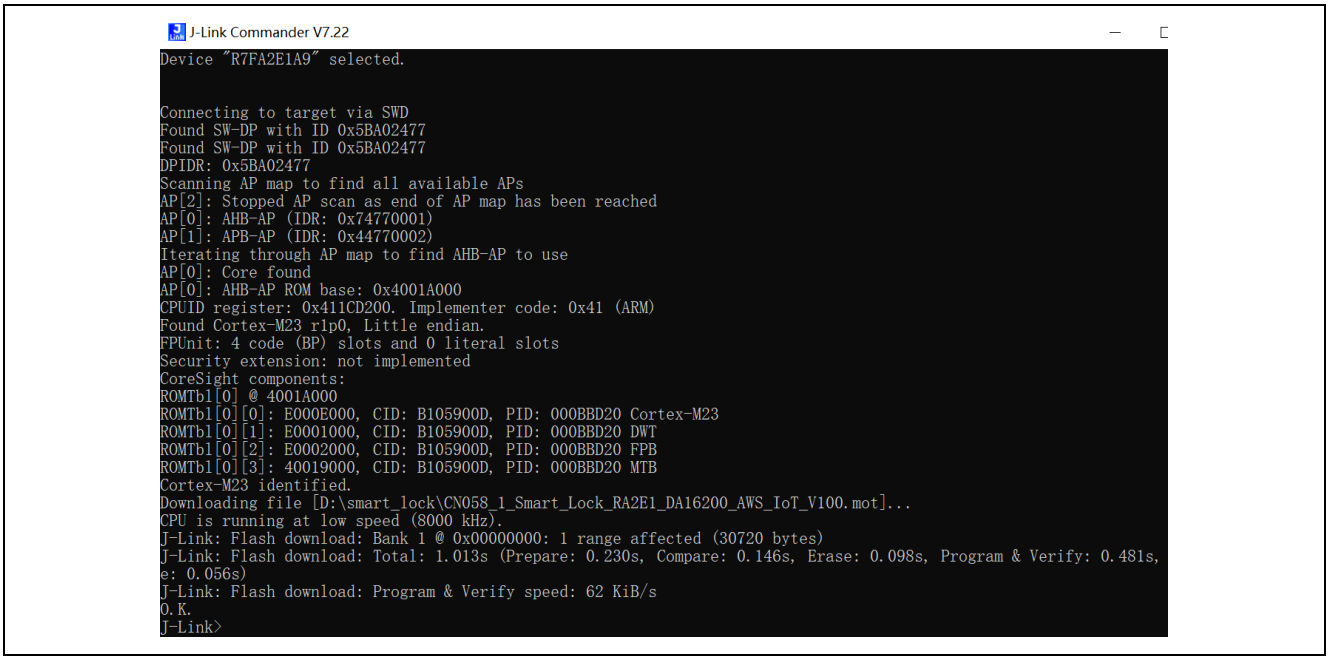
Select J-Link Commander

Step 3. Enter the below commands to program target device.

1. Device R7FA2E1A9
2. Speed 12000
3. Loadfile D:\smart_lock\CN058_1_Smart_Lock_RA2E1_EUthing_0628.mot
4. Type “s” command to select “SWD” interface and start to program



Step 4. After programming, disconnect the board from the PC.

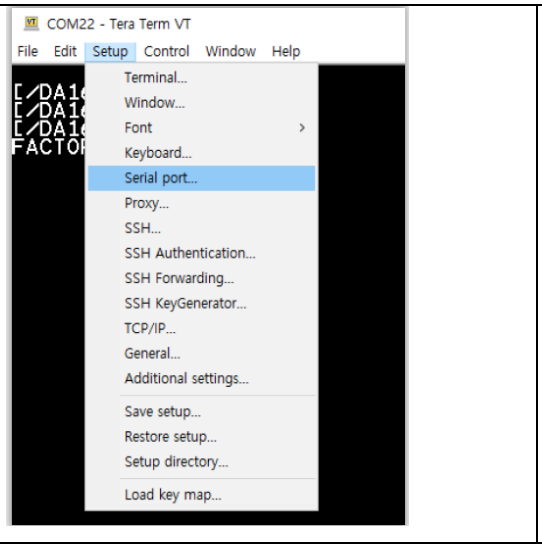


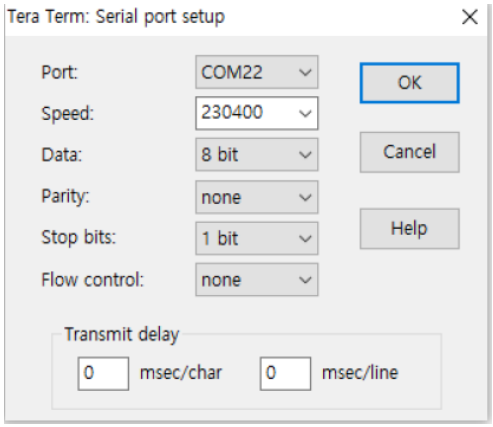
4.2 Download image to DA16200

Use a serial communication tool like "Tera Term" to download the firmware to DA16200MOD and debug it through output log information.

Tera Term link is https://ttssh2.osdn.jp/index.html.en

Step 1. Find the serial number connecting with DA16200MOD on PC, set the baud rate speed to 230400.





Check prompt window as below:

Step 2. Clear from exist firmware by “factory reset” command.

Step 3. There are 3 types of DA16200 images in the DA16200\img\folder: BOOT, Slib, RTOS, and one ttl file.
You can burn images by select Control > Marco > Download_W25Q32JW_4MB.ttl, which is a total file of BOOT, Slib and RTOS.

4.3 AWS IoT Configuration

In this demo, an account called “Thing name” for testing with AWS-IoT of Renesas’s account server, without your own AWS-IoT account server. Currently, “Doorlock_SST_for_Europe” has been assigned to this thing name, and this demo can be tested with SST IAM account. Please contact China SST for the account name and the password.

About creating and setting up your own AWS IoT account, please refer to “UM-WI-017 DA16200 AWS IoT Server Setup” User Manual, which introduces how to sign into the AWS IoT console. Meanwhile, the thing name can be modified accordingly.

4.4 Install Mobile Phone App

Customized “Smart Lock” App is available on Android mobile phone. Note that it is only used for demo, not for commercial purposes. Follow the steps below to setup this App:

(1) Install the “Smart Lock.apk”.

(2) Open the app, allow location and storage, and enable WIFI function.

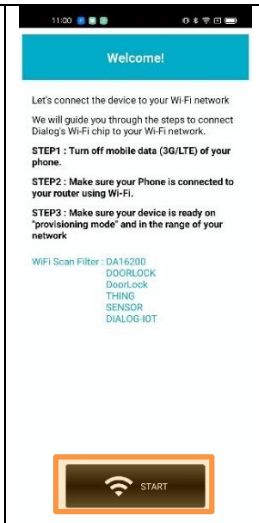
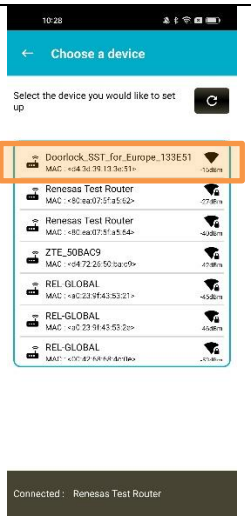
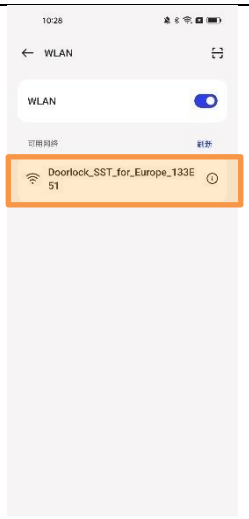
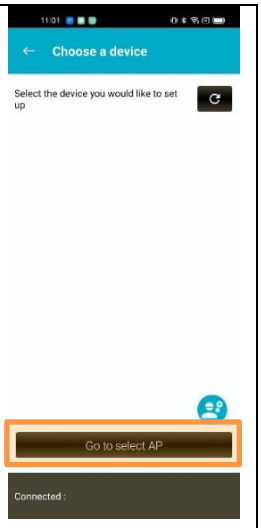
5) Run the Demo

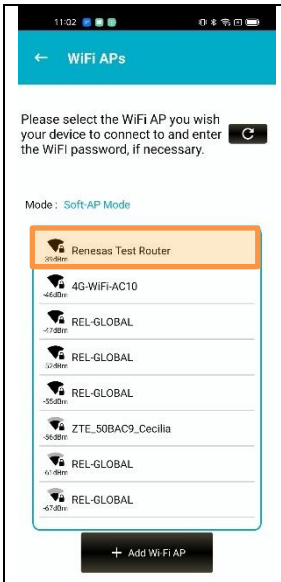
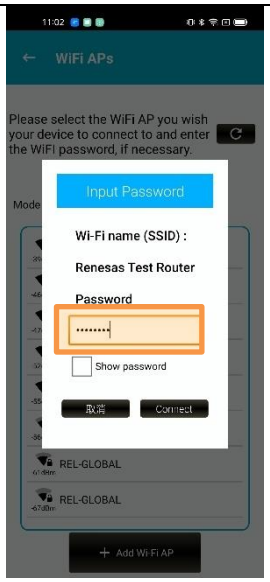
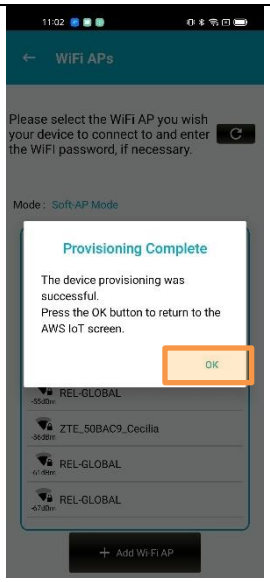
5.1 Provisioning

DA16200 supports a provisioning feature called Soft AP mode for an easy network configuration. Do this provisioning with the mobile network data off on your mobile phone and Wi-Fi turned on. Once provisioning is completed, turn on your mobile network data again.

Press the RESET button (S3) on EK-RA2E1 board to reset the MCU system, closely followed by pressing the Factory Reset button on Sparkfun Qwiic WiFi Shield board (button labeled GPIOA7) for above 5 seconds. Waiting for about 20 seconds, then start the Android Application and touch the START button in order to find the AP you wish to connect to.

Do the following steps on your Android device:

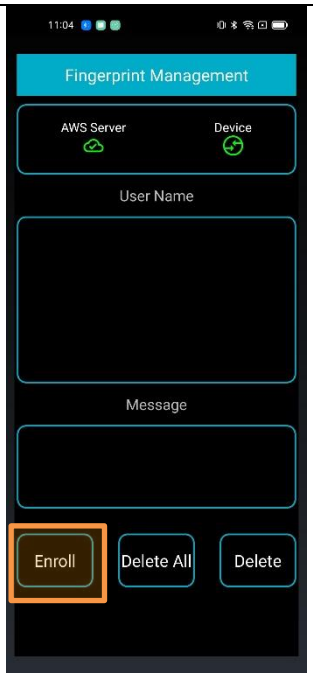
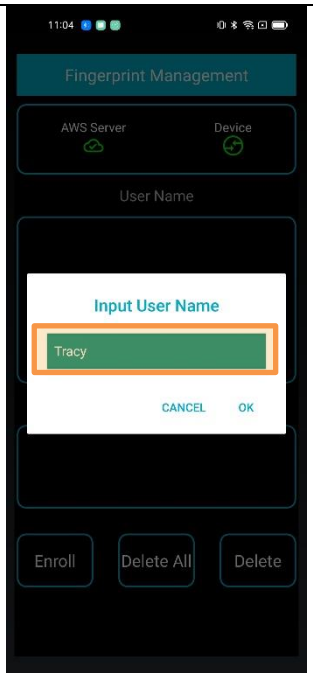
				
Click **Provisioning (Soft-AP mode)** button	Click **START** button	Click thing name as AP (start from **Doorlock_SST_for_ Europe**)	Confirm the thing name	Click **Go to Select AP** button

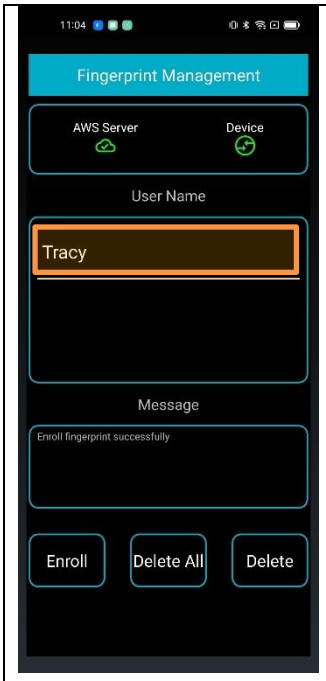
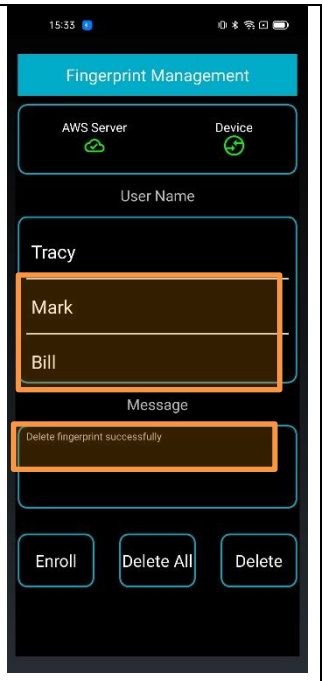
			
Click the AP name	Enter password	Success message, click **OK**	Show **AWS IoT** screen

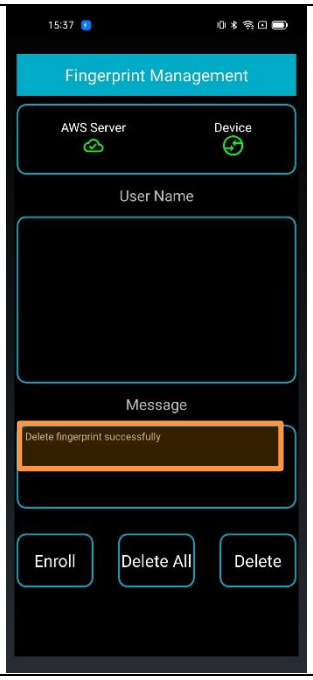
5.2 Fingerprint Management

Fingerprint management page on Android Application is used to manage user's fingerprint information, including enrollment and deletion. Even though the maximum of 100 fingerprint can be enrolled actually, in this demo only 12 of fingerprint is made as an example.

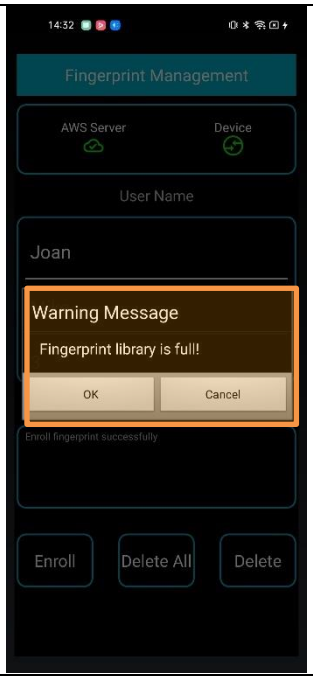
Do the following steps on your Android device:

			
Click "FINGERPRINT MANAGEMENT" button	Click "Enroll" button to enroll fingerprint	Input user's name, and click "OK"	Waiting for the finger put on the FP module to enroll successfully, or timeout

			
User's name displays in the message box after enrolling successfully	Delete one fingerprint by selecting corresponding user's name and clicking the "Delete" button	Wait for deleting the fingerprint successfully or timeout	User's name and Message box are updated after fingerprint deleting successfully

		
Click “Delete All” to delete all fingerprints	Wait for deleting all fingerprints successfully	User’s name is empty after deleting all fingerprints successfully

Some error messages are shown below:

		
Communication error between fingerprint module and MCU board	“userX” appears in user’s name box when the location enrolled by new fingerprint has been occupied.	Warning message indicates all 12 fingerprints has been enrolled. (The actual maximal number for fingerprint module is 100)

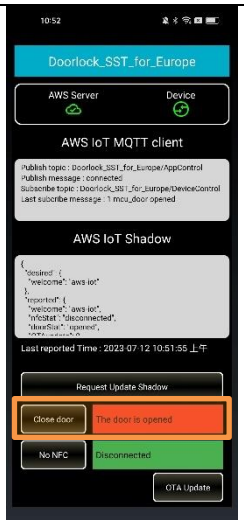
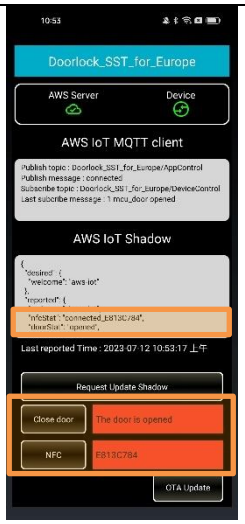
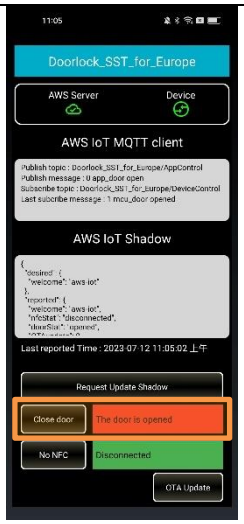
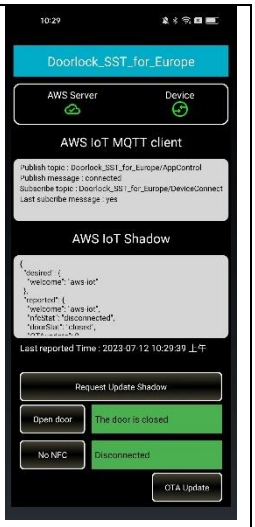
Notice:

1. When Enrollment period is waiting over 10s while your finger already put on the module, you can move your finger away and put it again to try.
2. If your fingerprint is too unclear or finger is too small to enroll easily, you can press a little bit harder to try.

5.3 AWS IoT monitoring

AWS IoT page is used to make the door opened or closed and monitor the door's status.

For this demo, there are four methods to open the door, fingerprint verification, button on the board pressed, approach of NFC card and open-door key on the mobile phone's App clicked. Only button on the board and key on the mobile phone's app can be used to close the door. While opening or closing the door, the red LED on the board is lit first, which means DA16200's wake-up. When the door is opened by button on the board, key on the mobile phone's App or fingerprint verification, the green LED is lit after the red LED is off. If the door is opened by approaching of NFC card, the blue LED blinks for a second then green LED is lit for door's opening.

				
Click "AWS IoT" button	Open the door by enrolled fingerprint	Open the door by approaching of NFC card	Open the door by the key on the mobile phone's App or button on the board	Click "Close door" on mobile phone's App to close the door

6) Reference Documents

UM-WI-038 User Manual DA16200 Getting Started with AT-Command for AWS-IoT 1v0

UM-WI-017 User Manual DA16200 AWS-IoT Server Setup_1v4

UM-WI-016 User Manual DA16200 Doorlock Application Using AWS IoT_1v6

SparkFun's New Qwiic Wi-Fi Shield Uses Renesas' DA16200 Module | Renesas

Evaluation Kit for RA2E1 MCU Group (EK-RA2E1)

YCM01-AN18 User Manual V1.3.1.pdf

Technical Updates/Technical News

(The latest information can be downloaded from the Renesas Electronics Website.)

Website and Support

Renesas Electronics Website

http://www.renesas.com/

Inquiries

http://www.renesas.com/contact/

Revision History

		Description	
Rev.	**Date**	**Page**	**Summary**
1.00	Jan., 2022	—	First edition issued
2.00	July., 2023		Add opening door with NFC card

General Precautions in the Handling of Micro processing Unit and Microcontroller Unit Products

The following usage notes are applicable to all Micro processing 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 near 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 micro processing 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 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.
5. 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.
6. 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.
7. 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.
8. 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.
9. 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.
10. 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.
11. This document shall not be reprinted, reproduced or duplicated in any form, in whole or in part, without prior written consent of Renesas Electronics.
12. 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.4.0-1 November 2017)

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/.