Intel® RSP SW Toolkit - Sensor NFC App

Installation & User's Guide

Document Number: 338454-001
Document Revision: 2018.12.17

Revision History

Revision	Description
2018.11.11	Initial draft.
2018.12.04	Updated screenshots.
2018.12.13	Branding updates.
2018.12.17	Updated screen shots and flow to match application.

Table of Contents

1 Introduction

This document is a guide to the installation, setup and use of the Sensor NFC Application Reference Design, which is one component of the Intel® RSP SW Toolkit. This application is used to program security credentials into the Intel® RFID Sensor Platform (Intel® RSP). The features included in this reference design are intended to provide the minimum functionality required to program the Intel® RSP. THIS SOFTWARE IS NOT INTENDED TO BE A MARKET READY SOLUTION.

1.1 Terminology

Term	Description
RSP	RFID Sensor Platform
RSP GW	IOT Gateway for Intel RFID Sensors

1.2 Reference Documents

Document	Document No./Location
RRS-Hx000_User_Guide	338088-001
RRS-Hx000_Message_API	338178-001
Intel® RSP SW Toolkit - Gateway User Guide	338443-001

2 Dependencies

2.1 Intel® RFID Sensor Platform (Intel® RSP)

The RSP-H1000, RSP-H3000 and RSP-H4000 are members of the Intel® RFID Sensor Platform (Intel® RSP) family of devices. These devices have capabilities for several on-board sensors including an EPC Gen 2 UHF RFID Interrogator (reader) and embedded NFC tag for configuring security credentials.

RSP-H4000 RSP-H3000 RSP-H1000

Figure 1: RFID Sensor Platform (RSP) Family

2.2 Gateway Reference Design

The Gateway Reference Design (another component of the Intel® RSP SW Toolkit) is an application that demonstrates the use of the API to collect and process RFID tag data and acts as the IOT Gateway between one or more RSP's and an Inventory Management or Asset Tracking application. The Gateway Reference Design creates the credentials used by the Sensor NFC Application.

2.3 Gateway Security Credentials

Securely provisioning a sensor allows for mutual authentication between a sensor and gateway. This is accomplished by providing a root CA certificate and a unique provisioning token. A hash of the ca cert is generated and given to the sensor and the sensor checks this hash against the root CA certificate that is downloaded as part of the gateway connection sequence. This allows the sensor to establish trust in the gateway to which it will connect. The provisioning token is sent by the sensor, to the gateway during connection and allows the gateway to confirm that the sensor should be allowed to connect.

```
{
  "username" : "gw_generated",
  "token" : "DBAF1C3F7C25EDC8C272FC2DA1A4CEFE562570A1E5F5460B8DAC4A98D1226149",
  "generatedTimestamp" : 1541966418186,
  "expirationTimestamp" : 1542052818186
}
```

Generating these credentials is covered in detail in the RSP Software Toolkit Gateway User's Guide.

2.4 Android Device

Any device running Android 6 (Marshmallow) or greater and has NFC write capabilities (i.e. Google Nexus 5) will support this reference application.

3 Intel® RSP SW Toolkit - Sensor NFC App

The source code and more information regarding the Sensor NFC Application can be downloaded from the Intel® Open Source Portal https://01.org. The project is located in the “Developer Toolkits” section under “Intel® RSP SW Toolkit”. Follow the “GIT REPO” link to obtain the software. Cloning the repo will download both the Gateway and Sensor NFC App.

3.1 Android Studio Project

Download Android Studio Integrated Development Environment (IDE) and follow the basic installation instructions. The Sensor NFC App currently targets Android version 26, so be sure to include that version when configuring / installing the accompanying Android SDK. This step will require several downloads to occur and will likely take a while to complete.

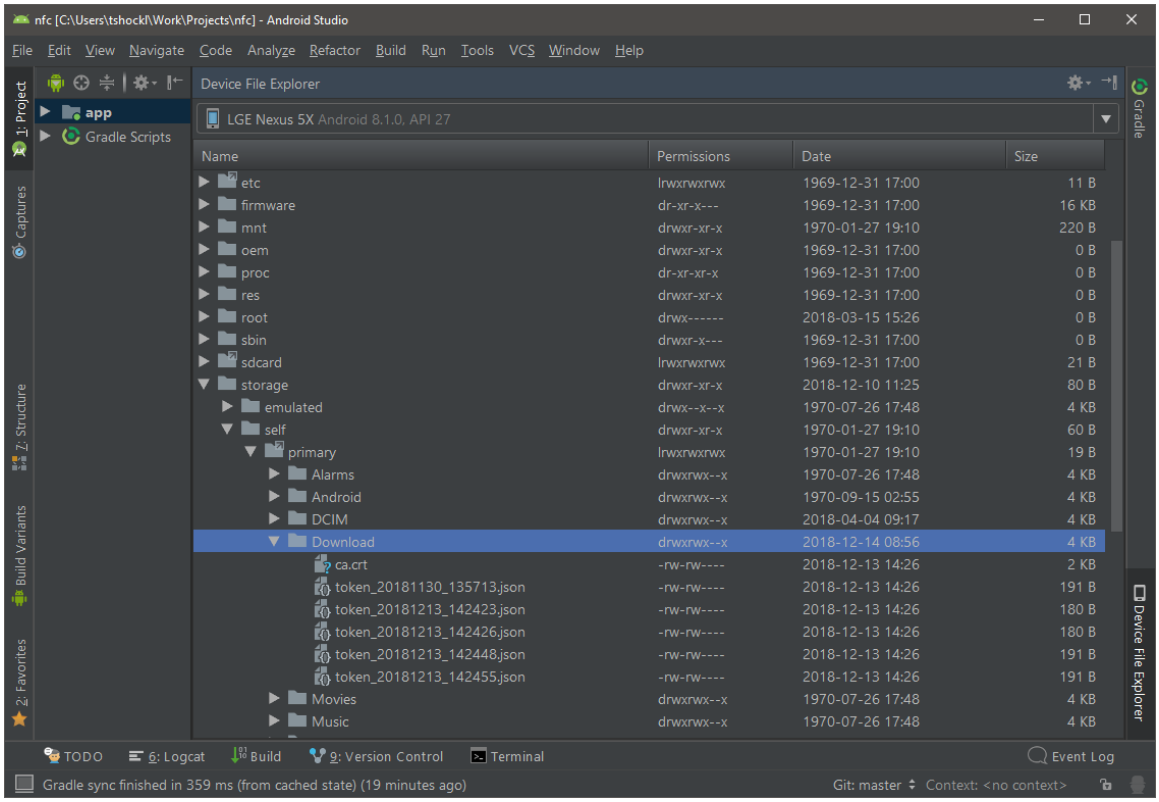
Once Android Studio has been installed, start the IDS and a welcome screen will appear. Select "Import project" and navigate to the sensor-nfc-app directory where the toolkit repository was cloned. This will setup the code and project files.

3.2 Connect Device

On the target Android device, enable developer options and USB debugging and then connect to the computer running the IDE using a USB cable. This will enable easy file transfer as well as run / debug capability with Android Studio. The device permission and options setting location will vary by device and version. Check that USB file transfer is also enabled on the target device.

3.3 Install Security Credentials

This step makes the security credentials described in section 2.3 available to the Sensor NFC App. Any method to get this files into the device's system Download folder is acceptable. In Android Studio, use the Device File Explorer to copy the credentials to the device's Download folder. Find this tool in the lower right of the IDE.



3.4 Build and Run

Android Studio uses gradle for building the application. With a device connected, it is a single click to trigger build / install / execute on the device. Navigate to

- Menu -> Run -> Run 'app'

This initial build will likely require gradle to download additional libraries, so a solid internet connection is highly recommended. After compilation, a popup screen to select the deployment device will be presented. The android device connected via USB should be available in this window.

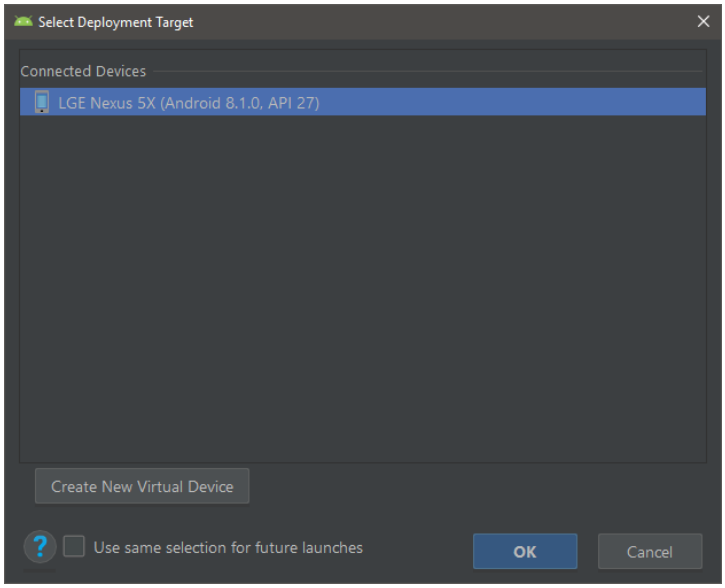


Figure 2 Select Deployment Target

This will install the app.apk onto the target device and start the app. The log of the running app can be monitored in the Run view of Android Studio.

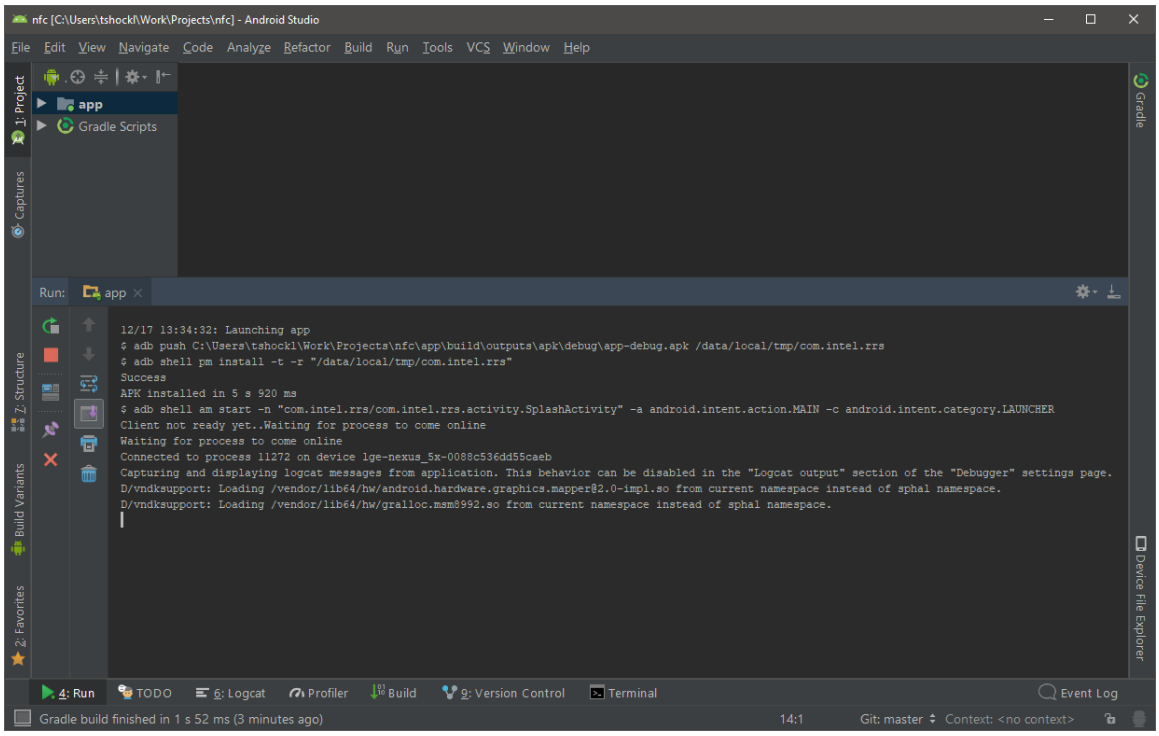


Figure 3 Run View

3.4.1 Splash

The initial splash screen provides general information regarding the security credentials required and where to copy them. You already know all of this because you have followed the instructions in this document.

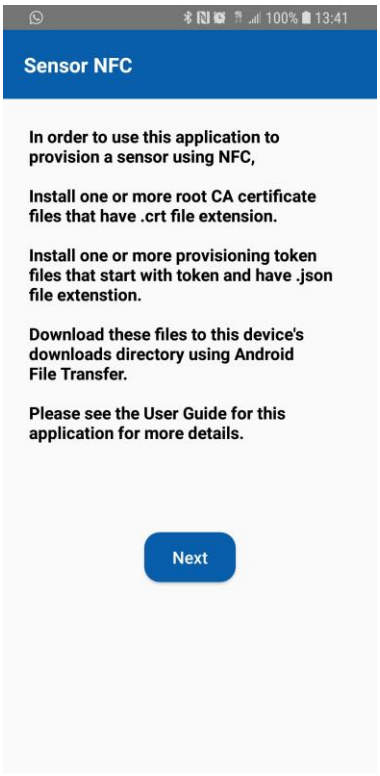


Figure 4 Splash Screen

3.4.2 Select Root CA Certificate

The app then presents the user with every file in the system Download folder that has a .crt extension. User selects one item from this screen by single tap.

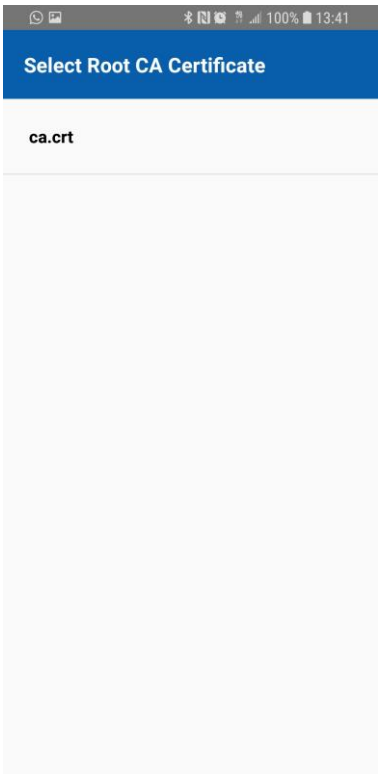


Figure 5 Select Root CA Screen

3.4.3 Select Token

As with the root CA cert, this screen will present a list of all files in the system Download folder that have "token" as part of the filename and with a .json extension. User selects one item from this screen by single tap.

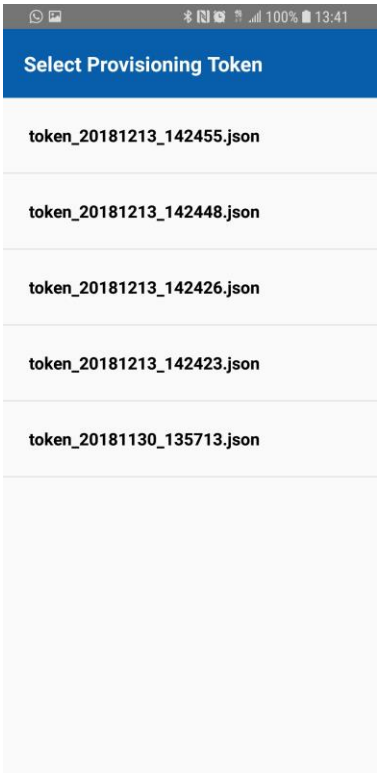


Figure 6 Select Token Screen

3.4.4 Program Provisioning Token

This screen presents details of what has been selected and will be written to the sensor's NFC tag. It includes the actual hash of the root CA certificate and the token. Additional information regarding the token validity is also shown.

The token expiration is conveyed in the .json file as a string representing the time in milliseconds since the epoch (midnight 01 JAN 1970). Tokens that have expired will show 'expired' in red. Tokens that never expire have a timestamp of negative one (-01).

As soon as this screen is activated, the app listens for the sensor's NFC tag to come into range and will write the credential information to the NFC tag when it is discovered.

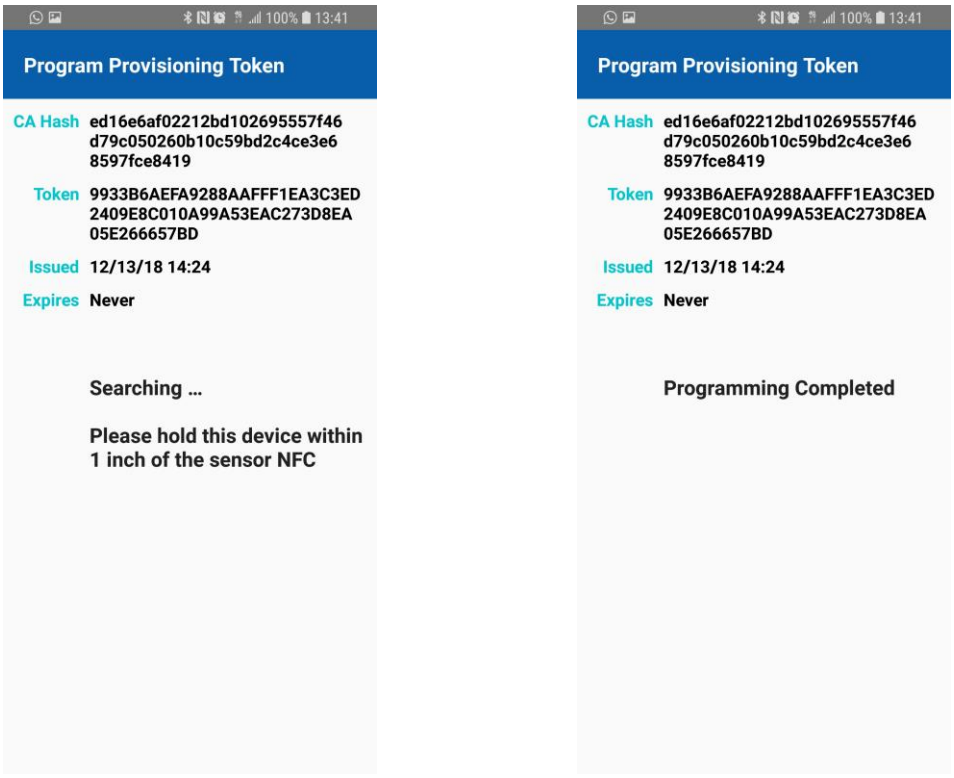


Figure 7 Program Token Screen

3.4.5 NFC Tag Locations

The Android device must be tapped within 1 – 2 inches of the NFC tag to successfully program. The Figure below shows the location of the NFC tag on each RSP.

Figure 8 NFC Tag Locations Identified