AN12661

EdgeLock™ SE05x for Wi-Fi Credential Protection

Rev. 1.2 — 7 December 2020 Application note

582911

Document information

Information	Content
Keywords	EdgeLock SE05x, Wi-Fi credentials, WPA-EAP-TLS
Abstract	This application note describes how to leverage EdgeLock SE05x for Wi-Fi credential protection. It explains how to run a demo setup that showcases the use of EdgeLock SE05x ease of use configuration to authenticate devices to a Wi-Fi network based on WPA-EAP-TLS protocol.

Revision history

Revision history

Revision number	Date	Description
1.0	2020-05-14	First version.
1.1	2020-06-12	ssscli compilation instructions updated
1.2	2020-12-07	Updated to the latest template and fixed broken URLs

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2020. All rights reserved.

1 Abbreviations

Table 1. Abbreviations

Acronym	Description
WSN	Wireless Sensor Network
AP	Access Point
CA	Certificate Authority
RADIUS	Remote Authentication Dial-In User Service
PCR	Platform Configuration Registers
OEM	Original Equipment Manufacturer
ECC	Elliptic-Curve Cryptography
MCU	Micro Controller Unit
PMK	Pairwise Master Key
PTK	Pairwise Transient Key
PBKDF	Password-Based Key Derivation Function
PSK	Pre-Shared Key
EAP	Extensible Authentication Protocol
TLS	Transport Layer Security
SSL	Secure Sockets Layer

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2020. All rights reserved.

2 EdgeLock SE05x for Wi-Fi credential protection

Today's networks include a wide range of wireless devices, from computers and phones to IP cameras, smart TVs and connected appliances. As such, wireless networks must be secured to protect your devices and your sensitive data from being compromised.

Wi-Fi Protected Access (WPA), and its evolution WPA2, are security standards designed to create secure wireless networks. There are different WPA versions based on the target end-user, method of authentication key distribution and encryption protocol used.

Designed for home networks, WPA-PSK secures wireless networks using Pre-Shared Key (PSK) authentication. The device network traffic is encrypted deriving its key from this shared key, which may be entered as hexadecimal digits or as a passphrase. For instance, if a passphrase is used, the encryption key is calculated by applying the PB-KDF2 key derivation function to the passphrase.

Designed for enterprise use, WPA-Enterprise typically secures wireless networks using a Remote Authentication Dial-In User Service (RADIUS) server dedicated to authentication purposes. The device authentication to the network is achieved using variants of the Extensible Authentication Protocol (EAP) protocol. For instance, EAP-TLS (Transport Layer Security) provides certificate-based and mutual authentication of the client and the network. It relies on client-side and server-side certificates to perform authentication and can be used to dynamically generate user-based and session-based keys to secure subsequent communications between the Wi-Fi client and the access point.

The EdgeLock SE05x allows us to securely authenticate devices to a Wi-Fi network based on the WPA-EAP-TLS authentication protocol. In this respect, the EdgeLock SE05x offers a tamper resistant platform that allows you to safely store credentials such as the sensitive private key and certificate in the case of WPA-EAP-TLS authentication. If the security of an IoT device is breached, the whole network can be compromised as well. By incorporating the EdgeLock SE05x in your design, it provides a very strong level of security for the network credentials that a regular host could not offer.

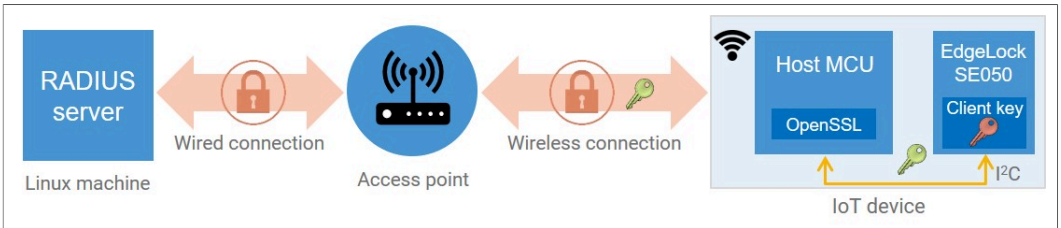

Figure 1. EdgeLock SE05x Wi-Fi credential protection

Note: *The RADIUS server can also be an integral part of the access point. This simplified setup is especially convenient for the home-gateway use case.*

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2020. All rights reserved.

3 EdgeLock SE05x demo setup for WPA-EAP-TLS authentication

To demonstrate the use of EdgeLock SE05x to authenticate devices to a Wi-Fi network based on WPA-EAP-TLS protocol, this section describes how to run the demo setup depicted in Figure 2:

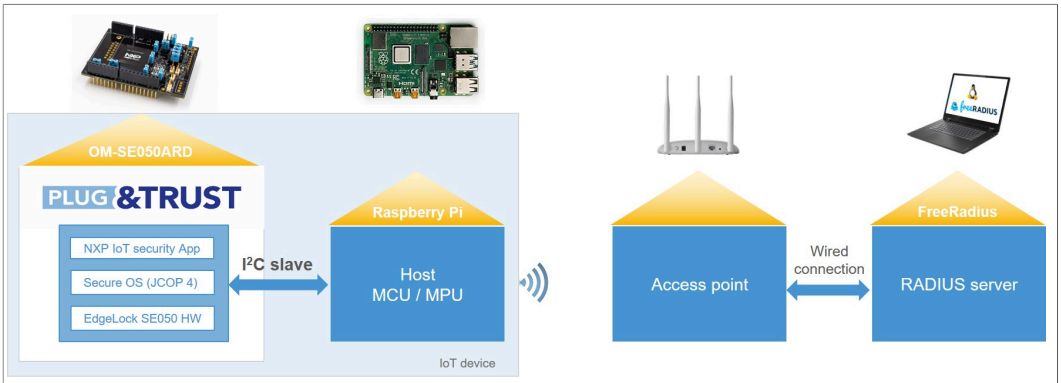

Figure 2. EdgeLock SE05x demo setup for Wi-Fi WPA-EAP-TLS connection

The demo architecture consists of three main elements: the *IoT device*, the *access point* and the *RADIUS server*. The *IoT device* is represented by a Raspberry Pi connected to the OM-SE050ARD board; the *access point* is represented by any commercial wireless router or access point with WPA/WPA2 Enterprise capabilities, and the *RADIUS* server is represented by a FreeRADIUS instance running on a Linux machine.

For authentication of the IoT device to the WiFi network the NXP-pre-provisioned keys and certificates inside EdgeLock SE05x will be used.

To set up the demo, you can follow these steps:

1. Check prerequisites
2. Configure the access point
3. Configure the FreeRADIUS server on a Linux machine
4. Configure the client (Raspberry Pi)
5. Run device network connection

Note: *The network settings shown in this example are provided only for demonstration purposes. Therefore, the subsequent procedure must be adapted as required for a production deployment.*

3.1 Prerequisites

Check the document AN12570-Quick Start Guide with Raspberry Pi for detailed instructions on how to bring up the hardware and software setup for the Raspberry Pi board.

3.2 Configure the access point

This section explains how to configure the access point to work in cooperation with the FreeRADIUS server. The following instructions are prepared using ASUS RT-AC58U access point as a reference. You might need to check the user manual of your access point vendor to replicate the same network configuration for your access point model.

To configure the access point, follow these instructions using any laptop:

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2020. All rights reserved.

1. Connect to the access point with an Ethernet cable.
2. Open a browser and log in to the access point (AP). The address of the AP is usually `192.168.1.1` or `192.168.0.1`, but this might be different for your access point. We will later refer to it as `access_point_ip`.
3. Go to the wireless settings menu and make the following adjustments:
   a. Give the wireless network name (SSID) an identifiable name. We will later refer to it as `ssid_name`.
   b. Set the wireless security/authentication method to `WPA/WPA2 Enterprise`.
   c. Provide the IP address of the linux machine behaving as the RADIUS server. We will later refer to it as `radius_server_ip`.
   d. Set the RADIUS server port to `1812`, which is the default for the RADIUS protocol.
   e. Choose a password in RADIUS server password field. We will refer to this password as `radius_server_password` later.

Note: *For your convenience, you can set up a static IP address to the Linux machine and the Raspberry Pi. Check the user manual of your AP for instructions.*

See Figure 3 as a reference on what the network configuration looks like on ASUS RT-AC58U access point.

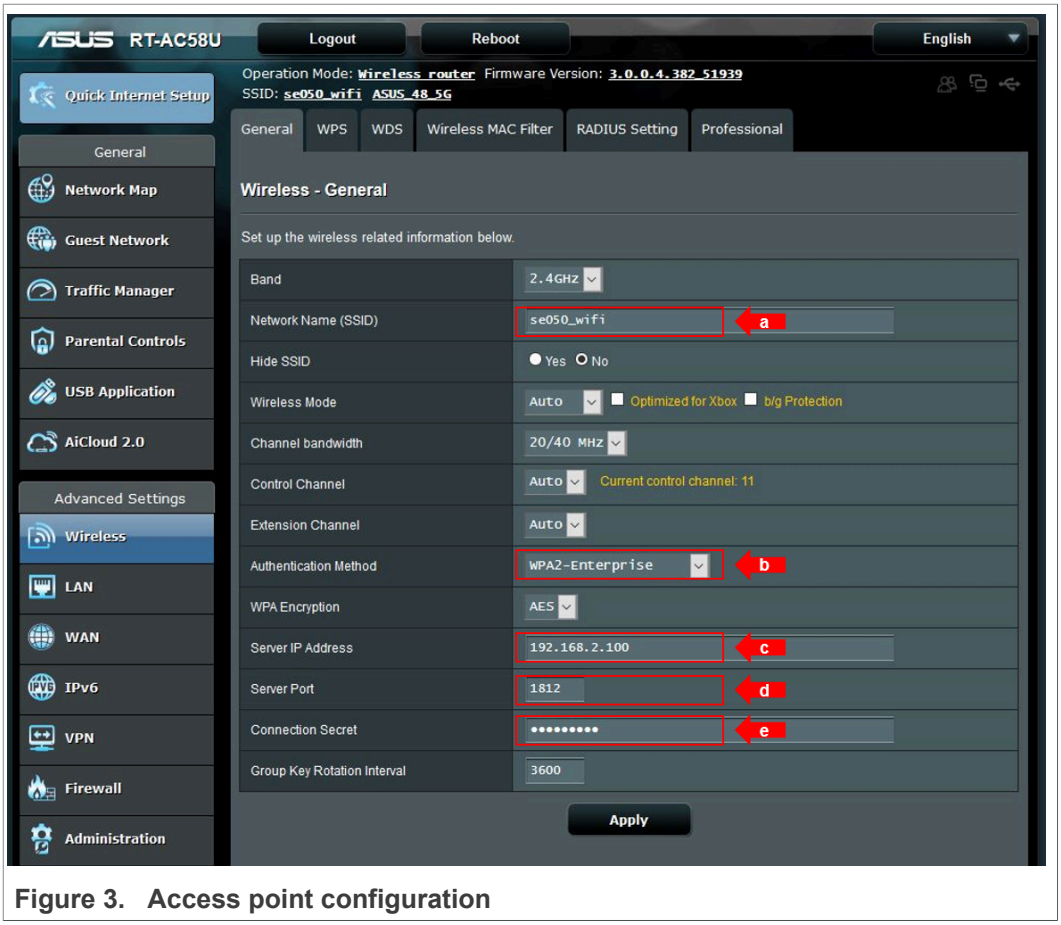

Figure 3. Access point configuration

3.3 Configure the FreeRADIUS server on a Linux machine

This section explains how to install and configure FreeRADIUS server on a Linux computer. The Linux distribution chosen for this demonstration is Ubuntu 16.04 LTS, but

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2020. All rights reserved.

it was tested on Debian Buster as well. You might need to adapt the instructions below if you use a different distribution.

3.3.1 Install FreeRADIUS

To install FreeRADIUS in Ubuntu 16.04 LTS, follow the steps below.

1. Send `$ sudo apt-get update` to update the list of available packages.
2. Send `$ sudo apt-get install freeradius` to install FreeRADIUS
3. Send `$ freeradius -v` to check that the FreeRADIUS has been installed correctly. Make sure the version is 3.0.x or newer.

3.3.2 Set the client configuration

Run `$ sudo nano /etc/freeradius/3.0/clients.conf` and add the following snippet outside any example clients in the file, detailing the IP address and the password we set in the previous section:

```
client router {
    ipaddr = <access_point_ip>
    secret = <radius_server_password>
}
```

This configuration allows the access point to forward any device network authentication request to the FreeRADIUS server to be handled.

3.3.3 Generate the FreeRADIUS server credentials

Now we will generate the server credentials used for RADIUS authentication. We will be using an ECC-based X.509 key to create a self-signed certificate. Run the following commands in order:

```
$ cd /etc/freeradius/3.0/certs

$ sudo openssl ecparam -out server.key -name prime256v1 -genkey

$ sudo openssl req -x509 -key server.key -out server.crt -days
365 -subj "/CN=radius server"

$ sudo chown freerad:freerad server.key
```

The `openssl ecparam` command is used to generate a NISP256 ECC key for a self-signed certificate. Then, the certificate itself is generated using the command `openssl req`, and finally we allow FreeRADIUS to access the key with the `chown` command.

Note: *Please keep in mind this is the minimum required credential management needed to get the demo up and running. In a real-world case, the client can use a different key and certificate, setting up specific requirements or using their own custom solution.*

3.3.4 Set the FreeRADIUS server configuration

The FreeRADIUS server configuration requires these credentials:

- *private_key_file*: The FreeRADIUS server private key, created in Section 3.3.3.
- *certificate_file*: The FreeRADIUS server certificate, created in Section 3.3.3.
- *ca_file*: The NXP CA certificate used to sign the client certificates (here using IoT connectivity key and certificate 0 from EdgeLock SE05x) attempting to connect to the

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2020. All rights reserved.

network. You can download it and convert it to the expected format using these two instructions:

```
$ sudo wget https://www.gp-ca.nxp.com/CA/getCA?
caid=63709315060011 -O NXP_CAvE206.crt
$ sudo openssl x509 -inform der -in NXP_CAvE206.crt -out
NXP_CAvE206.pem
```

Note: *Refer to AN12436 - SE050 configurations for more details about EdgeLock SE05x ease of use configuration, including the EdgeLock SE05x chain of trust certificates.*

Now configure the FreeRADIUS server to use the credentials above. This configuration is set in the file `eap`. Run

```
$ sudo nano /etc/freeradius/3.0/mods-available/eap
```

and replace the `eap` section with this snippet:

```
eap {
        default_eap_type = eap-tls
        timer_expire     = 60
        ignore_unknown_eap_types = no

        tls-config tls-common {
                private_key_file = /etc/freeradius/3.0/certs/server.key
                certificate_file = /etc/freeradius/3.0/certs/server.crt
                ca_file = /etc/freeradius/3.0/certs/NXP_CAvE206.pem

                cipher_list = "DEFAULT"
                cipher_server_preference = no
                ecdh_curve = "prime256v1"
        }
        tls {
                tls = tls-common
        }
}
```

Create a temporary directory called `radiusd` and give permissions for user `freerad`. Run the following commands:

```
$ mkdir /tmp/radiusd
```

```
$ sudo chown freerad:freerad /tmp/radiusd
```

Please keep in mind that this temporary directory is automatically removed on system reboot, so you will need to run the last two commands when the system boots back up.

3.4 Configure the client (Raspberry Pi)

This section explains the configuration of the Raspberry Pi as part of the IoT device of this demo. It includes:

- Configuration of the RADIUS client
- Installation of the EdgeLock SE05x Plug & Trust Middleware
- Extraction of client certificate from the EdgeLock SE05x
- Configuration of the Raspberry Pi network interface

To configure the Raspberry Pi, follow these instructions:

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2020. All rights reserved.

1. First, run the following commands one by one to make sure all needed packages are installed:
   ```
   $ sudo apt-get update
   $ sudo apt-get install cmake cmake-curses-gui cmake-gui libssl-dev python3-pip libffi-dev
   ```
2. Copy the EdgeLock SE05x Plug & Trust Middleware zip file into your home directory `~/` and unzip it using the command:
   ```
   $ unzip se050_mw_vxx.xx.xx.zip -d se050_middleware
   ```
   Please note that your EdgeLock SE05x Plug & Trust Middleware version can be different, so you will need to set the name of the zip file accordingly.
3. Set the `OPENSSL_ENGINE_EMBSE_ID` definition to `pkcs11` in the header file called `ax_embSeEngine.h`.
   Run
   ```
   $ nano ~/se050_middleware/simw-top/sss/plugin/openssl/engine/inc/ax_embSeEngine.h
   ```
   and modify lines 73 and 75 so that it looks like Figure 4.

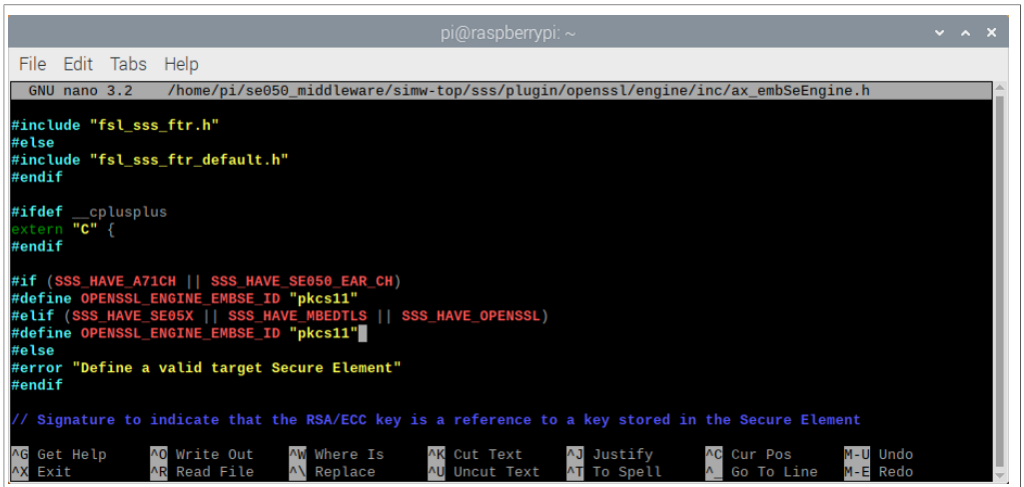

Figure 4. Set the engine id to `pkcs11` in the header file `ax_embSeEngine.h`

4. Build and install the `openssl` engine. Run these commands in order:
   ```
   $ cd ~/se050_middleware/simw-top
   $ python scripts/create_cmake_projects.py
   $ cd ~/se050_middleware/simw-top_build/raspbian_native_se050_t1oi2c
   $ cmake --build .
   $ sudo make install
   $ sudo ldconfig /usr/local/lib
   ```
5. Build and install the `ssscli` command line client. Run these commands in order:
   ```
   $ cd ~/se050_middleware/simw-top/pycli
   $ sudo pip3 install -r requirements.txt
   $ sudo pip3 install --editable src
   ```
   Please refer to AN12570-Quick start guide with Raspberry Pi for a detailed guide on building the EdgeLock SE05x Plug & Trust Middleware.

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2020. All rights reserved.

6. The device public key can be directly read from the EdgeLock SE05x ease of use configuration. Table 2 shows the ECC256 key pair we selected for this purpose:

Table 2. ECC256 public key selected from the EdgeLock SE05x ease of use configuration

Key name and type	Certificate	Usage policy	Erasable by customer	Identifier
IoT connectivity	Cloud Connectivity Certificate 0, ECC signed	Anybody, read	No	Key: 0xF0000000 Cert: 0xF0000001

***Note**: This ECC256 key pair has been selected as an example, for a complete detail of the EdgeLock SE05x ease of use configuration, refer to AN12436 - SE050 configurations.*

Now, use the `ssscli` tool to extract the client ECC certificate from the EdgeLock SE05x with the argument `get`. Then, the argument `refpem` is used to obtain a reference key which tells the OpenSSL engine to forward the cryptographic request to the EdgeLock SE05x.

Run the commands:

```
$ cd ~/wifiEAP
$ ssscli connect se050 t1oi2c none
$ ssscli get cert 0xF0000001 client.crt
$ ssscli refpem ecc pair 0xF0000000 client_ref.pem
```

If you are not able to connect to the EdgeLock SE05x with an error saying that there is a session already open, run `$ ssscli disconnect` first. See Figure 5 for reference.

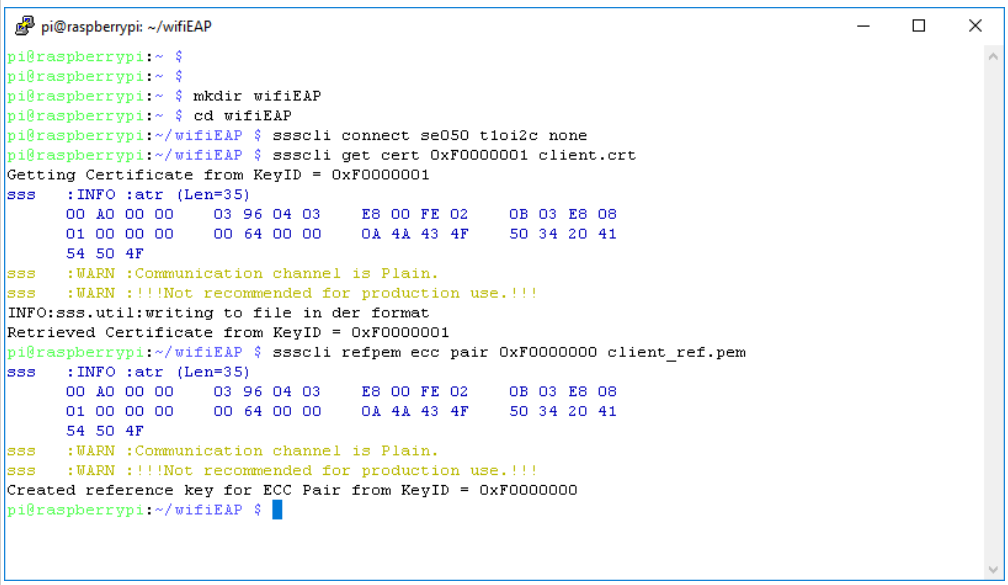

Figure 5. Raspberry Pi connecting to the EdgeLock SE05x, extracting the client key and creating a reference certificate

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2020. All rights reserved.

7. Set the `wpa_supplicant` configuration so that the Raspberry Pi connects to the wireless network and uses the appropriate credentials, as configured in Figure 3. Run the command
   `$ sudo nano /etc/wpa_supplicant/wpa_supplicant.conf`
   and replace all contents with the following snippet:

```
pkcs11_engine_path=/usr/local/lib/libsss_engine.so
pkcs11_module_path=/usr/local/lib/libsss_engine.so
network={
    ssid="ssid_name"
    priority=1
    engine=1
    key_mgmt=WPA-EAP
    pairwise=CCMP TKIP
    auth_alg=OPEN
    eap=TLS
    # identity string, will not be checked on server
    identity="user1"
    # disable server CA checking for demo purpose
    # ca_cert="/home/pi/wifiEAP/ca.pem"
    client_cert="/home/pi/wifiEAP/client.crt"
    private_key="/home/pi/wifiEAP/client_ref.pem"
}
```

3.5 Run device network connection

After the configuration of the access point, the FreeRADIUS server and the Raspberry Pi, we will proceed with the device network connection leveraging EdgeLock SE05x and WPA2 EAP-TLS authentication by following the steps below.

Note: *For clarity, command windows with a white background correspond to the client (Raspberry Pi), and the black background corresponds to the FreeRADIUS server.*

1. Start the FreeRADIUS server on the Linux machine. Launch the service in debugging mode to be able to watch the log. To do this, run the command:
   `$ sudo freeradius -X`
   When it's ready, it should say 'Ready to process requests', as shown in Figure 6.

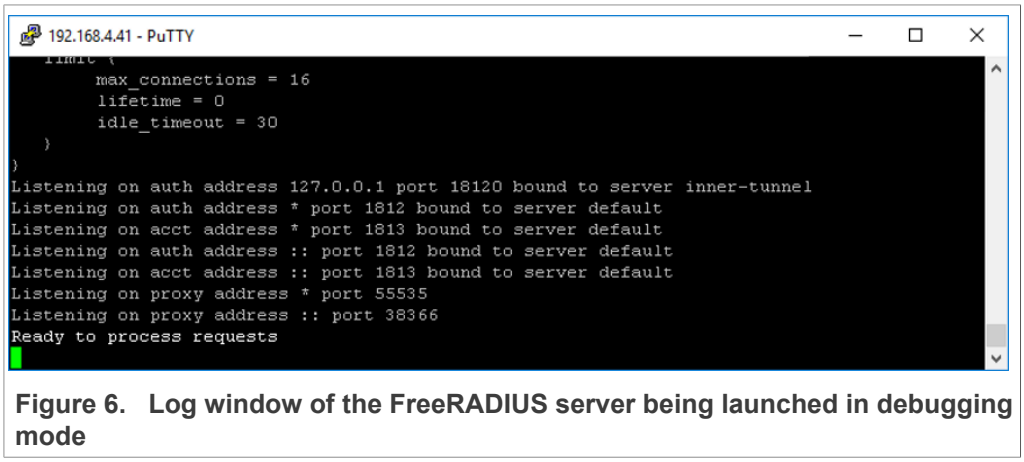

Figure 6. Log window of the FreeRADIUS server being launched in debugging mode

2. Back on the Raspberry Pi acting as a client, kill the current `wpa_supplicant` process with the command:
   `$ sudo pkill wpa_supplicant`

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2020. All rights reserved.

3. Restart the supplicant on the wireless network interface with the settings we configured in the last section using this command on one line:
   `$ sudo wpa_supplicant -c /etc/wpa_supplicant/wpa_supplicant.conf -i wlan0 -D wext`
   After a short time, you should see in the log that the authentication was successful, as shown in Figure 7

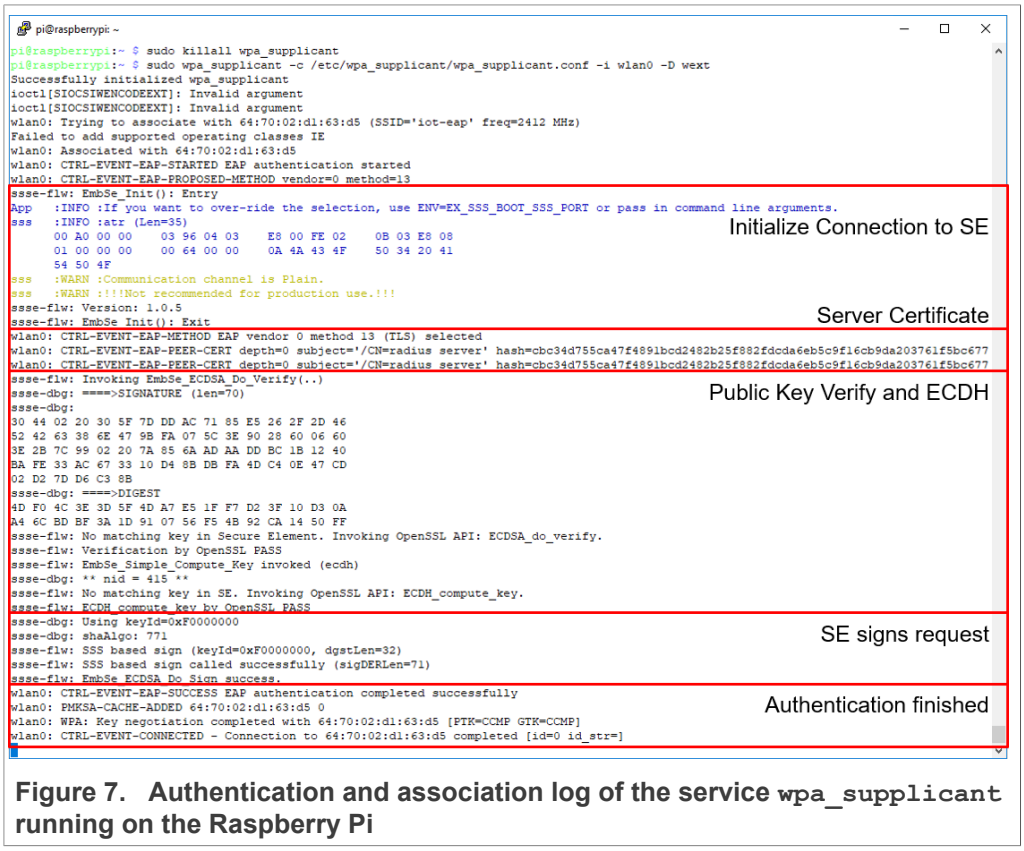

Figure 7. Authentication and association log of the service `wpa_supplicant` running on the Raspberry Pi

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2020. All rights reserved.

4. The Raspberry Pi will be assigned an IP address on the successful EAP-TLS handshake. In the FreeRADIUS server, you should now see a new connection request in the terminal window, as shown in Figure 8.

Figure 8. Log window of the FreeRADIUS server showing a successful authentication request

In this demo we have covered the complete setup process of a network using WPA2 Enterprise. We have set up the access point, the FreeRADIUS machine as the authentication server, and successfully connected a client to the network. We have used a Raspberry Pi as a wireless device with the EdgeLock SE05x as a companion security chip to safely store credentials.

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2020. All rights reserved.

4 Legal information

4.1 Definitions

Draft — A draft status on a document indicates that the content is still under internal review and subject to formal approval, which may result in modifications or additions. NXP Semiconductors does not give any representations or warranties as to the accuracy or completeness of information included in a draft version of a document and shall have no liability for the consequences of use of such information.

4.2 Disclaimers

Limited warranty and liability — Information in this document is believed to be accurate and reliable. However, NXP Semiconductors does not give any representations or warranties, expressed or implied, as to the accuracy or completeness of such information and shall have no liability for the consequences of use of such information. NXP Semiconductors takes no responsibility for the content in this document if provided by an information source outside of NXP Semiconductors. In no event shall NXP Semiconductors be liable for any indirect, incidental, punitive, special or consequential damages (including - without limitation - lost profits, lost savings, business interruption, costs related to the removal or replacement of any products or rework charges) whether or not such damages are based on tort (including negligence), warranty, breach of contract or any other legal theory. Notwithstanding any damages that customer might incur for any reason whatsoever, NXP Semiconductors' aggregate and cumulative liability towards customer for the products described herein shall be limited in accordance with the Terms and conditions of commercial sale of NXP Semiconductors.

Right to make changes — NXP Semiconductors reserves the right to make changes to information published in this document, including without limitation specifications and product descriptions, at any time and without notice. This document supersedes and replaces all information supplied prior to the publication hereof.

Suitability for use — NXP Semiconductors products are not designed, authorized or warranted to be suitable for use in life support, life-critical or safety-critical systems or equipment, nor in applications where failure or malfunction of an NXP Semiconductors product can reasonably be expected to result in personal injury, death or severe property or environmental damage. NXP Semiconductors and its suppliers accept no liability for inclusion and/or use of NXP Semiconductors products in such equipment or applications and therefore such inclusion and/or use is at the customer's own risk.

Applications — Applications that are described herein for any of these products are for illustrative purposes only. NXP Semiconductors makes no representation or warranty that such applications will be suitable for the specified use without further testing or modification. Customers are responsible for the design and operation of their applications and products using NXP Semiconductors products, and NXP Semiconductors accepts no liability for any assistance with applications or customer product design. It is customer's sole responsibility to determine whether the NXP Semiconductors product is suitable and fit for the customer's applications and products planned, as well as for the planned application and use of customer's third party customer(s). Customers should provide appropriate design and operating safeguards to minimize the risks associated with their applications and products. NXP Semiconductors does not accept any liability related to any default, damage, costs or problem which is based on any weakness or default in the customer's applications or products, or the application or use by customer's third party customer(s). Customer is responsible for doing all necessary testing for the customer's applications and products using NXP Semiconductors products in order to avoid a default of the applications and the products or of the application or use by customer's third party customer(s). NXP does not accept any liability in this respect.

Export control — This document as well as the item(s) described herein may be subject to export control regulations. Export might require a prior authorization from competent authorities.

Evaluation products — This product is provided on an "as is" and "with all faults" basis for evaluation purposes only. NXP Semiconductors, its affiliates and their suppliers expressly disclaim all warranties, whether express, implied or statutory, including but not limited to the implied warranties of non-infringement, merchantability and fitness for a particular purpose. The entire risk as to the quality, or arising out of the use or performance, of this product remains with customer. In no event shall NXP Semiconductors, its affiliates or their suppliers be liable to customer for any special, indirect, consequential, punitive or incidental damages (including without limitation damages for loss of business, business interruption, loss of use, loss of data or information, and the like) arising out the use of or inability to use the product, whether or not based on tort (including negligence), strict liability, breach of contract, breach of warranty or any other theory, even if advised of the possibility of such damages. Notwithstanding any damages that customer might incur for any reason whatsoever (including without limitation, all damages referenced above and all direct or general damages), the entire liability of NXP Semiconductors, its affiliates and their suppliers and customer's exclusive remedy for all of the foregoing shall be limited to actual damages incurred by customer based on reasonable reliance up to the greater of the amount actually paid by customer for the product or five dollars (US$5.00). The foregoing limitations, exclusions and disclaimers shall apply to the maximum extent permitted by applicable law, even if any remedy fails of its essential purpose.

Translations — A non-English (translated) version of a document is for reference only. The English version shall prevail in case of any discrepancy between the translated and English versions.

Security — Customer understands that all NXP products may be subject to unidentified or documented vulnerabilities. Customer is responsible for the design and operation of its applications and products throughout their lifecycles to reduce the effect of these vulnerabilities on customer's applications and products. Customer's responsibility also extends to other open and/or proprietary technologies supported by NXP products for use in customer's applications. NXP accepts no liability for any vulnerability. Customer should regularly check security updates from NXP and follow up appropriately. Customer shall select products with security features that best meet rules, regulations, and standards of the intended application and make the ultimate design decisions regarding its products and is solely responsible for compliance with all legal, regulatory, and security related requirements concerning its products, regardless of any information or support that may be provided by NXP. NXP has a Product Security Incident Response Team (PSIRT) (reachable at PSIRT@nxp.com) that manages the investigation, reporting, and solution release to security vulnerabilities of NXP products.

4.3 Trademarks

Notice: All referenced brands, product names, service names and trademarks are the property of their respective owners.

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2020. All rights reserved.

Tables

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2020. All rights reserved.

Figures

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2020. All rights reserved.

Contents

Please be aware that important notices concerning this document and the product(s) described herein, have been included in section 'Legal information'.

© NXP B.V. 2020. **All rights reserved.**

For more information, please visit: http://www.nxp.com
For sales office addresses, please send an email to: salesaddresses@nxp.com

Date of release: 7 December 2020
Document identifier: AN12661
Document number: 582911