Ajith

Ajithmn3@yahoo.com

Abstract

Device provisioning feature of Telit Wi-fi module

DEVICE PROVISIONING PROTOCOL

**|TELIT**

**Table of Contents**

[Device Provisioning Protocol 2](#_Toc48936089)

[Test procedure 2](#_Toc48936090)

[Test results 4](#_Toc48936091)

[Index 6](#_Toc48936092)

Table of Figures

[Figure 1- SSID and passphrase 2](#_Toc49692914)

[Figure 2- Public Key 3](#_Toc49692915)

[Figure 3- Copy public key 3](#_Toc49692916)

[Figure 4- Test result 5](#_Toc49692917)

[Figure 5 Sniffer log 5](#_Toc49692918)

## Device Provisioning Protocol

This document demonstrates the DPP feature of GS2K Telit Wi-Fi module. DUT acts as enrollee (responder) and receives configuration from configurator (initiator). If the protocol is successful;

1. DUT will print the received credentials.
2. Saves the received credentials in profile.
3. Configures DUT to starts NCM and resets the device.
4. After device reset is complete, DUT will connect to the provisioned AP.

No responses will be sent to the host, if the protocol fails.

**Note:** See ‘Test result’ section for complete test with AT commands and its responses.

## Test procedure

1. Download source code from the link [https://github.com/HewlettPackard/dpp](https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Fgithub.com%2FHewlettPackard%2Fdpp&data=02%7C01%7CSharath.Jose%40telit.com%7C97fcbf5548104de403f508d6cf17848e%7C15d9cfdc338445c582dc3426a208a45c%7C1%7C0%7C636924097268496312&sdata=ei3DG2zgjWoGo02CAKNxwSBd%2Faf167Dseh5BKJA1gD0%3D&reserved=0) on a Linux machine OR from the attached content, which is already tested.
2. Extract the source code and follow the instructions in read me file to build the project. Change the SSID and passphrase in configuration object in file dpp.c, and make the project. Sample configuration object for using “psk” is below.

"{\"wi-fi\_tech\":\"infra\",\"discovery\":{\"ssid\":\"DLINK\_TELIT\",\"op\_cl\":81,"

"\"ch\_list\":[{\"ch\":1}]},\"cred\":{\"akm\":\"psk\",\"pass\":\"gsdemo123\"}}"

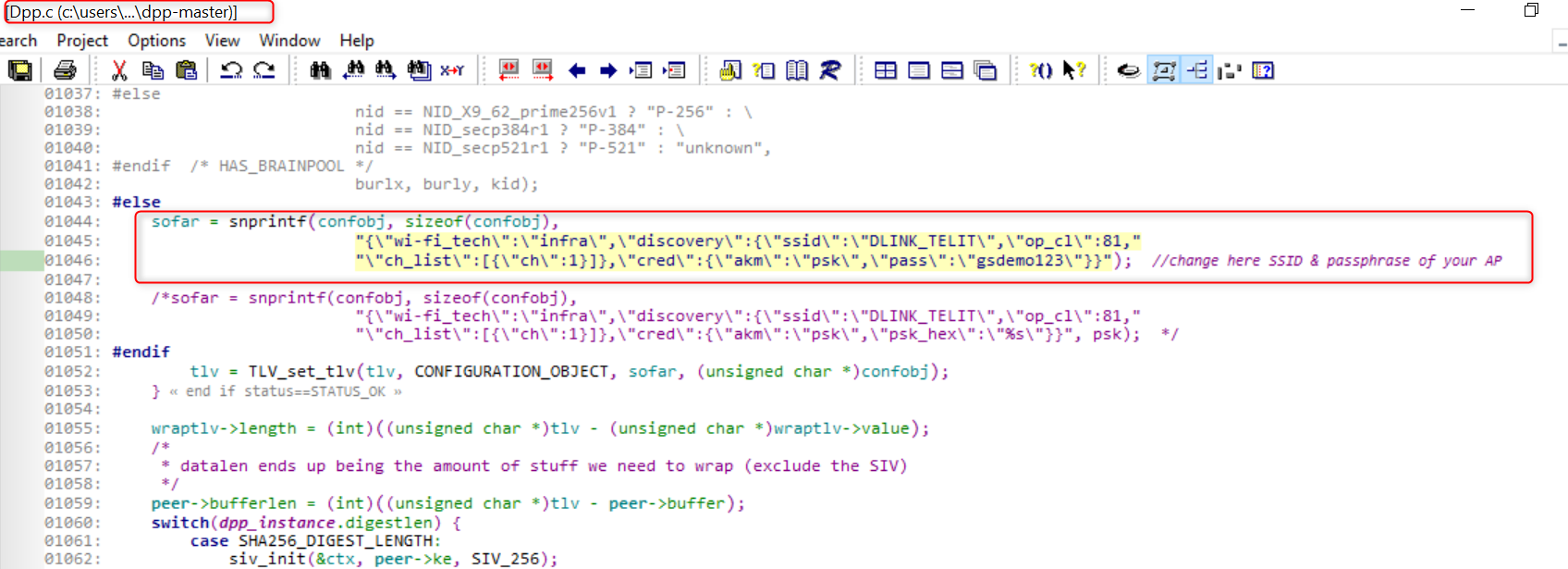


Figure 1- SSID and passphrase

1. Generate EC private key.

openssl ecparam -name secp256r1 -genkey -noout -out alice\_priv\_key.pem

1. Generate public key from above private key.

openssl ec -in alice\_priv\_key.pem -pubout -out alice\_pub\_key.pem

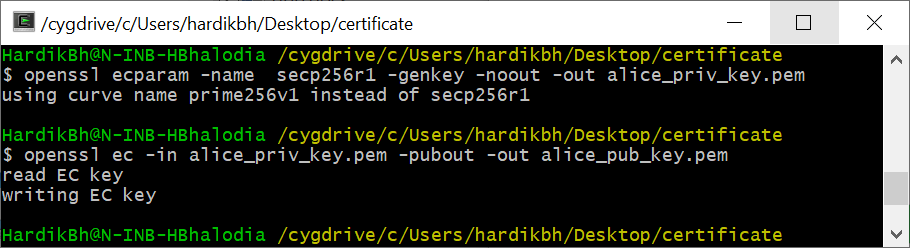


Figure 2- Public Key

1. Upload private key using tcert command on DUT.

at+tcertadd=cert1,0,227,0

**Note:** 227 bytes is size of this cert and cert1 is random name of the cert.

1. Copy the public key and add it in the file “dpp-master\linux\initbkeys.txt” file as shown below.



Figure 3- Copy public key

As shown in figure 3, change following fields;

* Public key
* MAC address of DUT
* Chanel on which DUT is listening

1. Disable network manager on the Linux machine.
2. Issue the following at command to start DPP on DUT.
   1. Add certificate –

AT+TCERTADD=cert1,0,227,0

* 1. Enable DPP protocol on DUT –

AT+DPPEN=<enable/disable>,<CHANNEL>,<CERT\_NAME>

1. Start the configurator on Linux machine using following command.

sudo ./sss -I wlp3s0 -i -c signp256.pem -k initp256.pem -B initbkeys.txt -d 63 -x 1 -a

**Note:** wlp3s0 in this command is the name of Linux machine’s Wi-Fi interface.

AT Command Params details:

AT+DPPEN=<enable/disable>,<CHANNEL>,<CERT\_NAME>

<enable/disable> value 1 will start the protocol. Value 0 will stop the protocol.

<channel> DUT will listen on this channel.

<CERT\_NAME> EC Private key.

**Note:** After completing step 9 on Linux machine, as shown in ‘Test results’ section, DUT will print the received credentials, saves it in profile, configures DUT to starts NCM and reset the device. When device reset is complete, DUT will connect to the provisioned AP.

**Important:** The configurator must wait for 3O seconds before retrying.

## Test results

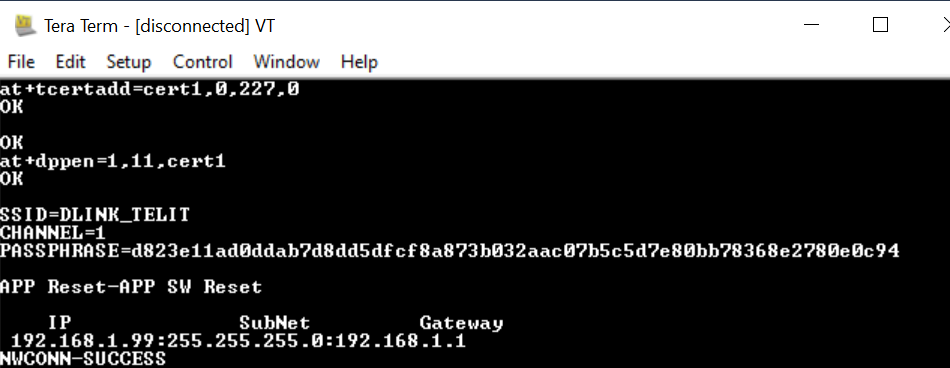


Figure 4- Test result

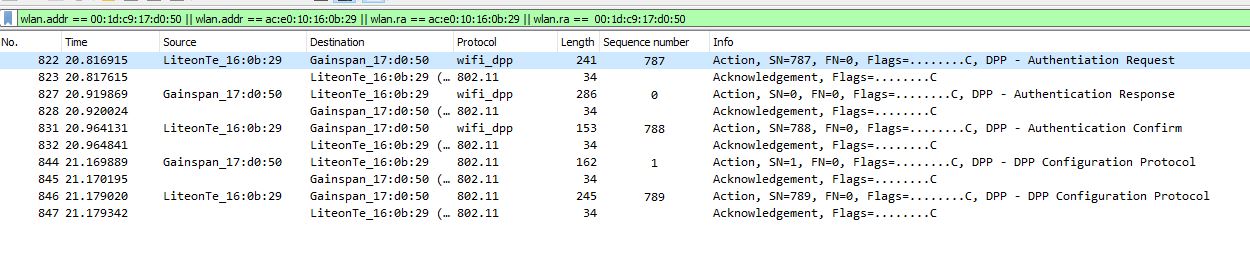


Figure 5 Sniffer log

Index

configurator 4

DPP 2

network manager 4

private key 3

provisioned AP 2

public key 3

Sniffer log 5

source code 2

Test results 5