IoT Security and Privacy

Assignment 4 – ESP32 WPA2 (25 bonus points in the final grade)

We need to download certificate from ***https://library.ucf.edu/services/computers-technology/wireless-networking/***

We get a file downloaded named Incommon.cer which has the certificate key which needs to be properly formatted as below:

```
"-----BEGIN CERTIFICATE-----\n"\
"MIIF+TCCA+GgAwIBAgIQRyDQ+oVGGn4XoWQCkYRjdDANBgkqhkiG9w0BAQwFADCB\n"\
"iDELMAkGA1UEBhMCVVMxEzARBgNVBAgTCk5ldyBKZXJzZXkxFDASBgNVBAcTC0pl\n"\
"cnNleSBDaXR5MR4wHAYDVQQKExVUaGUgVVNFUlRSVVNUIE5ldHdvcmsxLjAsBgNV\n"\
"BAMTJVVTRVJUcnVzdCBSU0EgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkwHhcNMTQx\n"\
"MDA2MDAwMDAwWhcNMjQxMDA1MjM1OTU5WjB2MQswCQYDVQQGEwJVUzELMAkGA1UE\n"\
"CBMCTUkxEjAQBgNVBAcTCUFubiBBcmJvcjESMBAGA1UEChMJSW50ZXJuZXQyMREw\n"\
"DwYDVQQLEwhJbkNvbW1vbjEfMB0GA1UEAxMWSW5Db21tb24gUlNBIFNlcnZlciBD\n"\
"QTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJwb8bsvf2MYFVFRVA+e\n"\
"xU5NEFj6MJsXKZDmMwysE1N8VJG06thum4ltuzM+j9INpun5uukNDBqeso7JcC7v\n"\
"HgV9lestjaKpTbOc5\MZNrun8XzmCB5hJ0R6lvSoNNviQsil2zfVtefkQnI\tBPP\n"\
"iwckRR6MkYNGuQmm\BijBgLsNI0yZpUn6uGX6Ns1oytW61fo8BBZ321wDGZq0GTl\n"\
"qKOYMa0dYtX6kuOaQ80tNfvZnjNbRX3EhigsZhLI2w8ZMA0\6fDqSl5AB8f2IHpT\n"\
"eIFken5FahZv9JNYyWL7KSd9oX8hzudPR9aKVuDjZvjs3YncJowZaDuNi+L7RyML\n"\
"fzcCAwEAAaOCAW4wggFqMB8GA1UdIwQYMBaAFFN5v1qqK0rPVIDh2JvAnfKyA2bL\n"\
"MB0GA1UdDgQWBBQeBaN3j2yW4luHS6a0hqxxAAznODAOBgNVHQ8BAf8EBAMCAYYw\n"\
"EgYDVR0TAQH\BAgwBgEB\wIBADAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUH\n"\
"AwIwGwYDVR0gBBQwEjAGBgRVHSAAMAgGBmeBDAECAjBQBgNVHR8ESTBHMEWgQ6BB\n"\
"hj9odHRwOi8vY3JsLnVzZXJ0cnVzdC5jb20vVVNFUlRydXN0UlNBQ2VydGlmaWNh\n"\
"dGlvbkF1dGhvcml0eS5jcmwwdgYIKwYBBQUHAQEEajBoMD8GCCsGAQUFBzAChjNo\n"\
"dHRwOi8vY3J0LnVzZXJ0cnVzdC5jb20vVVNFUlRydXN0UlNBQWRkVHJ1c3RDQS5j\n"\
"cnQwJQYIKwYBBQUHMAGGGWh0dHA6Ly9vY3NwLnVzZXJ0cnVzdC5jb20wDQYJKoZI\n"\
"hvcNAQEMBQADggIBAC0RBjjW29dYaK+qOGcXjeIT16MUJNkGE+vrkS\fT2ctyNMU\n"\
"11ZlUp5uH5gIjppIG8GLWZqjV5vbhvhZQPwZsHURKsISNrqOcooGTie3jVgU0W+0\n"\
"+Wj8mN2knCVANt69F2YrA394gbGAdJ5fOrQmL2pIhDY0jqco74fzYefbZ\VS29fR\n"\
"5jBxu4uj1P+5ZImem4Gbj1e4ZEzVBhmO55GFfBjRidj26h1oFBHZ7heDH1Bjzw72\n"\
"hipu47Gkyfr2NEx3KoCGMLCj3Btx7ASn5Ji8FoU+hCazwOU1VX55mKPU1I2250Lo\n"\
"RCASN18JyfsD5PVldJbtyrmz9gn\TKbRXTr80U2q5JhyvjhLf4lOJo\UzL5WCXED\n"\
"Smyj4jWG3R7Z8TED9xNNCxGBMXnMete+3PvzdhssvbORDwBZByogQ9xL2LUZFI\i\n"\
"eoQp0UM\L8zfP527vWjEzuDN5xwxMnhi+vCToh7J159o5ah29mP+aJnvujbXEnGa\n"\
"nrNxHzu+AGOePV8hwrGGG7hOIcPDQwkuYwzN\xT29iLp\cqf9ZhEtkGcQcIImH3b\n"\
"oJ8ifsCnSbu0GB9L06Yqh7lcyvKDTEADsIIaeSEINxhO2Y1fmcYFX\Fqrrp1WnhH\n"\
"OjplXuXE0OPa0utaKC25Aplgom88L2Z8mEWcyfoB7zKOfD759AN7JKZWCYwk\n"\
"-----END CERTIFICATE-----\n"\
```

Now embedding this certificate to the code will help us to establish connection to WPA_2 network from esp32 kit. We will require one extra variable for this certificate which can be stated as:

esp_wifi_sta_wpa2_ent_set_ca_cert((uint8_t *)ssl_cert, strlen(ssl_cert));

So after adding the certificate and its variable we get the final code which looks like as given below:

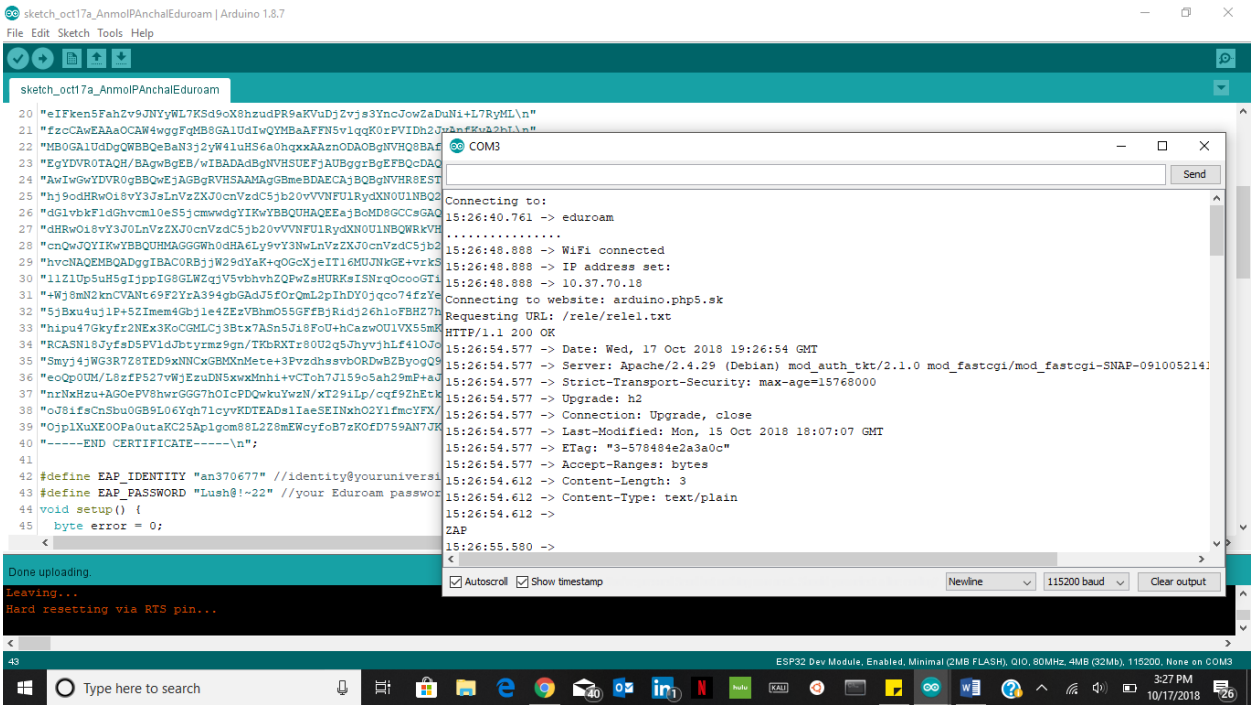
CODE:

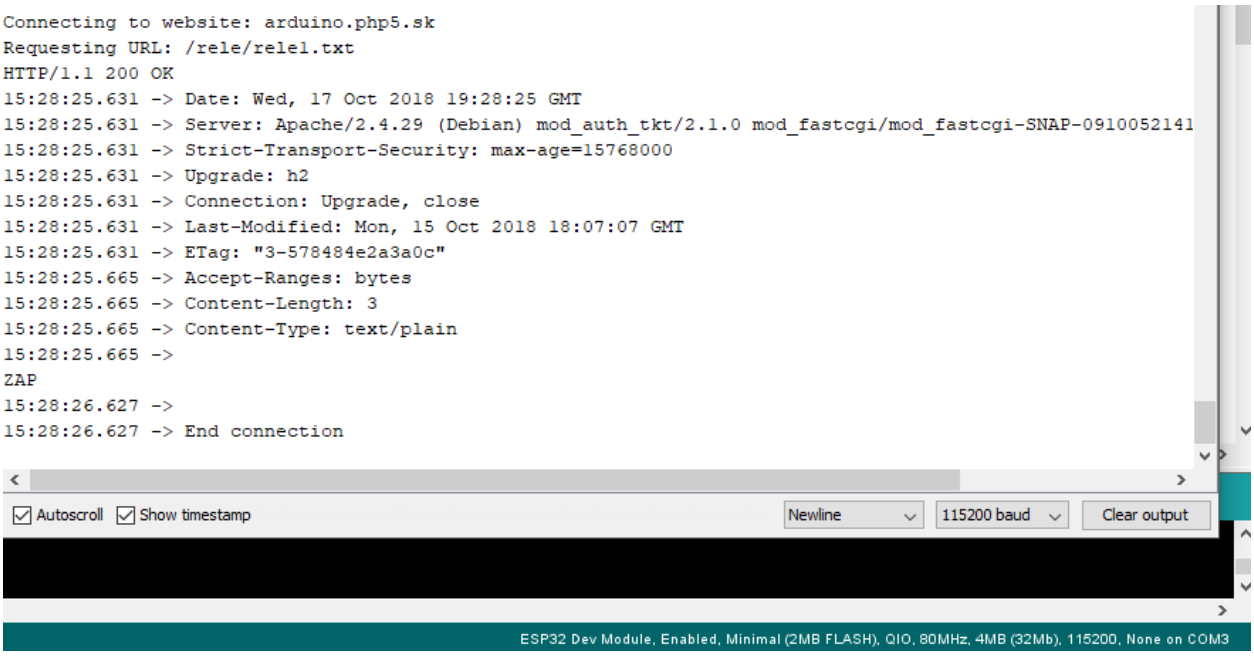
```
#include "esp_wpa2.h"
#include <WiFi.h>
String line; //variable for response
const char* ssid = "UCF_WPA2"; // Eduroam SSID
const char* host = "arduino.php5.sk"; //external server domain
// Getting ssl certificate from ucf libary wireless network

const char* ssl_cert = \
"-----BEGIN CERTIFICATE-----\n"\
"MIIF+TCCA+GgAwIBAgIQRyDQ+oVGGn4XoWQCkYRjdDANBgkqhkiG9w0BAQwFADCB\n"\
"iDELMAkGA1UEBhMCVVMxEzARBgNVBAgTCk5ldyBKZXJzZXkxFDASBgNVBAcTC0pl\n"\
"cnNleSBDaXR5MR4wHAYDVQQKExVUaGUgVVNFUlRSVVNUIE5ldHdvcmsxLjAsBgNV\n"\
"BAMTJVVTRVJUcnVzdCBSU0EgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkwHhcNMTQx\n"\
"MDA2MDAwMDAwWhcNMjQxMDA1MjM1OTU5WjB2MQswCQYDVQQGEwJVUzELMAkGA1UE\n"\
"CBMCTUkxEjAQBgNVBAcTCUFubiBBcmJvcjESMBAGA1UEChMJSW50ZXJuZXQyMREw\n"\
"DwYDVQQLEwhJbkNvbW1vbjEfMB0GA1UEAxMWSW5Db21tb24gUlNBIFNlcnZlciBD\n"\
"QTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJwb8bsvf2MYFVFRVA+e\n"\
"xU5NEFj6MJsXKZDmMwysE1N8VJG06thum4ltuzM+j9INpun5uukNDBqeso7JcC7v\n"\
"HgV9lestjaKpTbOc5\MZNrun8XzmCB5hJ0R6lvSoNNviQsil2zfVtefkQnI\tBPP\n"\
"iwckRR6MkYNGuQmm\BijBgLsNI0yZpUn6uGX6Ns1oytW61fo8BBZ321wDGZq0GTl\n"\
"qKOYMa0dYtX6kuOaQ80tNfvZnjNbRX3EhigsZhLI2w8ZMA0\6fDqSl5AB8f2IHpT\n"\
"eIFken5FahZv9JNYyWL7KSd9oX8hzudPR9aKVuDjZvjs3YncJowZaDuNi+L7RyML\n"\
"fzcCAwEAAaOCAW4wggFqMB8GA1UdIwQYMBaAFFN5v1qqK0rPVIDh2JvAnfKyA2bL\n"\
"MB0GA1UdDgQWBBQeBaN3j2yW4luHS6a0hqxxAAznODAOBgNVHQ8BAf8EBAMCAYYw\n"\
"EgYDVR0TAQH\BAgwBgEB\wIBADAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUH\n"\
"AwIwGwYDVR0gBBQwEjAGBgRVHSAAMAgGBmeBDAECAjBQBgNVHR8ESTBHMEWgQ6BB\n"\
"hj9odHRwOi8vY3JsLnVzZXJ0cnVzdC5jb20vVVNFUlRydXN0UlNBQ2VydGlmaWNh\n"\
"dGlvbkF1dGhvcml0eS5jcmwwdgYIKwYBBQUHAQEEajBoMD8GCCsGAQUFBzAChjNo\n"\
"dHRwOi8vY3J0LnVzZXJ0cnVzdC5jb20vVVNFUlRydXN0UlNBQWRkVHJ1c3RDQS5j\n"\
"cnQwJQYIKwYBBQUHMAGGGWh0dHA6Ly9vY3NwLnVzZXJ0cnVzdC5jb20wDQYJKoZI\n"\
"hvcNAQEMBQADggIBAC0RBjjW29dYaK+qOGcXjeIT16MUJNkGE+vrkS\fT2ctyNMU\n"\
"11ZlUp5uH5gIjppIG8GLWZqjV5vbhvhZQPwZsHURKsISNrqOcooGTie3jVgU0W+0\n"\
"+Wj8mN2knCVANt69F2YrA394gbGAdJ5fOrQmL2pIhDY0jqco74fzYefbZ\VS29fR\n"\
"5jBxu4uj1P+5ZImem4Gbj1e4ZEzVBhmO55GFfBjRidj26h1oFBHZ7heDH1Bjzw72\n"\
"hipu47Gkyfr2NEx3KoCGMLCj3Btx7ASn5Ji8FoU+hCazwOU1VX55mKPU1I2250Lo\n"\
"RCASN18JyfsD5PVldJbtyrmz9gn\TKbRXTr80U2q5JhyvjhLf4lOJo\UzL5WCXED\n"\
"Smyj4jWG3R7Z8TED9xNNCxGBMXnMete+3PvzdhssvbORDwBZByogQ9xL2LUZFI\i\n"\
"eoQp0UM\L8zfP527vWjEzuDN5xwxMnhi+vCToh7J159o5ah29mP+aJnvujbXEnGa\n"\
"nrNxHzu+AGOePV8hwrGGG7hOIcPDQwkuYwzN\xT29iLp\cqf9ZhEtkGcQcIImH3b\n"\
"oJ8ifsCnSbu0GB9L06Yqh7lcyvKDTEADsllaeSEINxhO2Y1fmcYFX\Fqrrp1WnhH\n"\
"OjplXuXE0OPa0utaKC25Aplgom88L2Z8mEWcyfoB7zKOfD759AN7JKZWCYwk\n"\
"-----END CERTIFICATE-----\n"\


#define EAP_IDENTITY "an370677" //identity@youruniversity.domain - my nid
#define EAP_PASSWORD "**********" //your Eduroam password
```

```
void setup() {
  byte error = 0;
  Serial.begin(115200);
  delay(10);
  Serial.println("Connecting to: ");
  Serial.println(ssid);
  WiFi.disconnect(true);  //disconnect from wifi to set new wifi connection
  WiFi.mode(WIFI_STA);
  esp_wifi_sta_wpa2_ent_set_ca_cert((uint8_t *)ssl_cert, strlen(ssl_cert));
  error += esp_wifi_sta_wpa2_ent_set_identity((uint8_t *)EAP_IDENTITY, strlen(EAP_IDENTITY));
  error += esp_wifi_sta_wpa2_ent_set_username((uint8_t *)EAP_IDENTITY, strlen(EAP_IDENTITY));
  //error  +=  esp_wifi_sta_wpa2_ent_set_new_password((uint8_t  *)EAP_PASSWORD,  strlen(EAP_PASSWORD));
//First time running, i think i needed to set this, although i received an error from the server, claiming the password
was not set?
  error += esp_wifi_sta_wpa2_ent_set_password((uint8_t *)EAP_PASSWORD, strlen(EAP_PASSWORD)); //Following
times, it ran fine with just this line (connects very fast).

  if (error != 0) {
    Serial.println("Error setting WPA properties.");
  }
  WiFi.enableSTA(true);

  esp_wpa2_config_t config = WPA2_CONFIG_INIT_DEFAULT();
  if (esp_wifi_sta_wpa2_ent_enable(&config) != ESP_OK) {
    Serial.println("WPA2 Settings Not OK");
  }

  WiFi.begin(ssid); //connect to Eduroam function
  WiFi.setHostname("RandomHostname"); //set Hostname for your device - not neccesary
  while (WiFi.status() != WL_CONNECTED) {
    delay(500);
    Serial.print(".");
  }
  Serial.println("");
  Serial.println("WiFi connected");
  Serial.println("IP address set: ");
  Serial.println(WiFi.localIP()); //print LAN IP
}
void loop() {
    delay(5000);
 if (WiFi.status() != WL_CONNECTED) { //if we lost connection, retry
       WiFi.begin(ssid);
       delay(500);
    }
    Serial.print("Connecting to website: ");
    Serial.println(host);
    WiFiClient client;
    if (!client.connect(host, 80)) { // HTTP connection on port 80
       Serial.println("Connection lost! - Failed response");
    }
    String url = "/rele/rele1.txt"; //read .txt file
    Serial.print("Requesting URL: ");
    Serial.println(url);
```

```
  // This will send the request to the server
  client.print(String("GET ") + url + " HTTP/1.1\r\n" +
               "Host: " + host + "\r\n" +
               "Connection: close\r\n\r\n");
  unsigned long timeout = millis();
  while (client.available() == 0) {
    if (millis() - timeout > 5000) {
      Serial.println("Client timed out! - retry");
      client.stop();
    }
  }
  while(client.available()) {
     line = client.readStringUntil('\n');
    Serial.println(line);
  }
  Serial.println();
  Serial.println("End connection");
}
```

Now after this we connect esp32 to my machine and start Arduino to compile and upload this code. After successful compilation and uploading the code on esp32 we get a successful established connection between esp32 and WPA_2 wifi network. This can be confirmed by the output given below:





References:

M. (2018, October 08). Martinius96/ESP32-Eduroam. Retrieved from https://github.com/martinius96/ESP32-Eduroam