FreeRADIUS Certificate (TLS) Configuration

From the RADIUS point of view, this is pretty easy, with only minor changes to the base configuration.

The hard bit is the certificates themselves. Not only do they have to work with RADIUS but they also have to cope with the idiosyncrasies of the operating systems they're installed on.

Instructions for generating client certificate PKI.

If you've got a RADIUS configuration that works for EAP-PEAP then the changes would be in the mods-available/eap file.

```
eap {
      ...
      tis-config {
                   ...
                   private_key_file = <Private key for the server cert
created above>
                   certificate_file = <Server certificate created above>
                   ca_file = <Root CA created for the client cert above>
                   ...
                  }
     }
```

The private_key_file and the certificate_file define the server identity. The client carries the Root CA so that it can authenticate that the server is derived from the PKI. IF these are already set as part of the EAP-PEAP config then there's no need to change them. The Client→Server auth and Server→Client auth should be separate operations and work with completely different PKIs.

The ca_file is actually used to authenticate the clients in the same way as above. When the client sends the certificate the server uses the Root CA to prove that the client is derived from the PKI.

eapol_test configuration

Using eapol_test is the easiest and most reliable way to test EAP-TLS

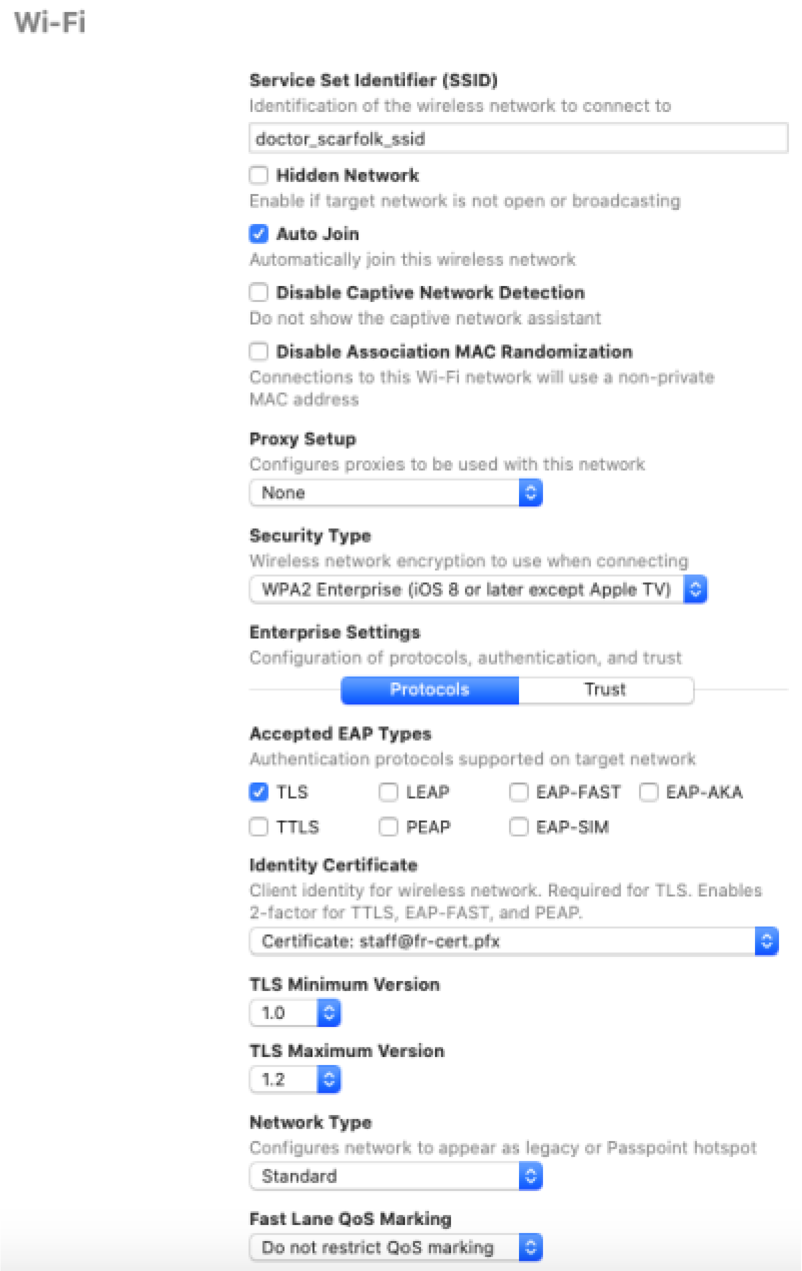
```
network={
    ssid="govroam"
    key_mgmt=WPA-EAP
    eap=TLS
    identity="<Outer ID>"
    ca_cert="<CA Certificate>"
    client_cert="<Client Certificate>"
    private_key="<Client Key>"
    eapol_flags=3
}
```

Apple MacOS configuration

ProfileCreator and the CAT aren't good enough to generate suitable mobileconfig files. ProfileCreator doesn't appear to include the right fields and the CAT can't deploy client certificates.

The only way appears to be to use Apple Configurator 2.

Create a profile that contains the client certificate, the root CA certificate and the wireless configuration for the SSID. The certificates must be in PKCS12 format with a password. The wireless configuration sets the SSID, the security type (WPA2 Enterprise), EAP Type of TLS and the identity certificate.



Wi-Fi

Service Set Identifier (SSID)
Identification of the wireless network to connect to
doctor_scarfolk_ssid

☐ **Hidden Network**
Enable if target network is not open or broadcasting

☑ **Auto Join**
Automatically join this wireless network

☐ **Disable Captive Network Detection**
Do not show the captive network assistant

☐ **Disable Association MAC Randomization**
Connections to this Wi-Fi network will use a non-private MAC address

Proxy Setup
Configures proxies to be used with this network
None

Security Type
Wireless network encryption to use when connecting
WPA2 Enterprise (iOS 8 or later except Apple TV)

Enterprise Settings
Configuration of protocols, authentication, and trust
Protocols | Trust

Accepted EAP Types
Authentication protocols supported on target network
☑ TLS ☐ LEAP ☐ EAP-FAST ☐ EAP-AKA
☐ TTLS ☐ PEAP ☐ EAP-SIM

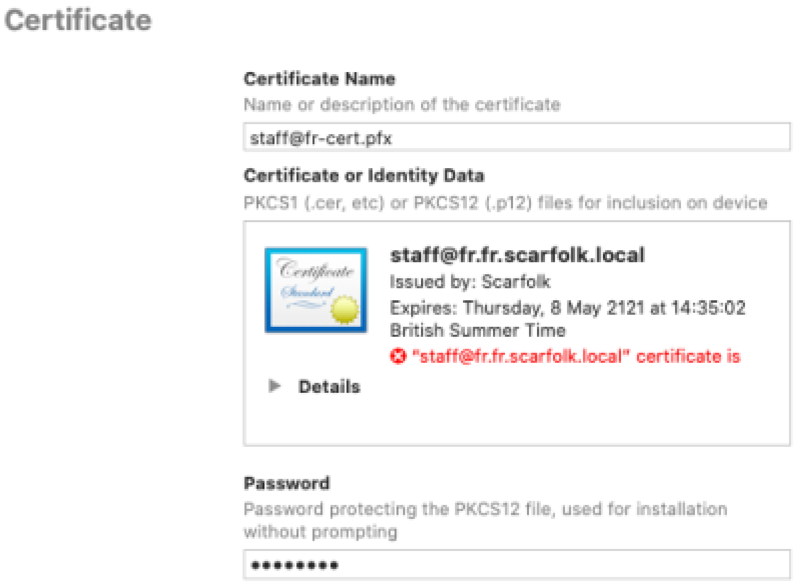
Identity Certificate
Client identity for wireless network. Required for TLS. Enables 2-factor for TTLS, EAP-FAST, and PEAP.
Certificate: staff@fr-cert.pfx

TLS Minimum Version
1.0

TLS Maximum Version
1.2

Network Type
Configures network to appear as legacy or Passpoint hotspot
Standard

Fast Lane QoS Marking
Do not restrict QoS marking



Certificate

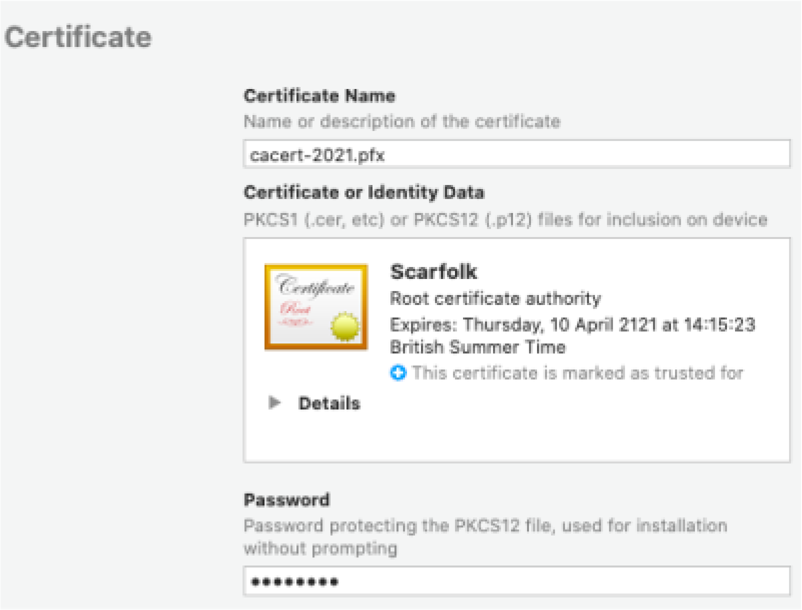
Certificate Name
Name or description of the certificate
staff@fr-cert.pfx

Certificate or Identity Data
PKCS1 (.cer, etc) or PKCS12 (.p12) files for inclusion on device

staff@fr.fr.scarfolk.local
Issued by: Scarfolk
Expires: Thursday, 8 May 2121 at 14:35:02 British Summer Time
⊗ "staff@fr.fr.scarfolk.local" certificate is

▶ **Details**

Password
Password protecting the PKCS12 file, used for installation without prompting
••••••••



Certificate

Certificate Name
Name or description of the certificate
cacert-2021.pfx

Certificate or Identity Data
PKCS1 (.cer, etc) or PKCS12 (.p12) files for inclusion on device

Scarfolk
Root certificate authority
Expires: Thursday, 10 April 2121 at 14:15:23 British Summer Time
⊕ This certificate is marked as trusted for

▶ **Details**

Password
Password protecting the PKCS12 file, used for installation without prompting
••••••••

From:
https://wiki.govroam.uk/ - **Govroam**

Permanent link:
https://wiki.govroam.uk/doku.php?id=siteadmin:freeradius_certificate_tls_authentication

Last update: **2021/05/07 08:11**