Client Certificate PKI Configuration

The idea is simple, the implementation is complex and the execution simple.

The idea is that the client sends a certificate (and key) to the server. The server checks the certificate against a CA and, if it matches, approves the authentication.

The implemention means creating a CA (NOT using a commercial one - this is completely insecure) and a client certificate from the CA. This PKI could be really complicated (Root, Intermediates, signing etc.) or it could be a single Root CA and one certificate per device or user.

The complications are that the certs must contain certain attributes and have certain attribute values formatted in certain ways. Different OSes have different requirements.

The execution is easy. The client sends the cert to the server, which compares it to the stored CA. Again, this could be made more complex by having the CA stored elsewhere and the RADIUS server having to make a call to it.

The approach here is going to be simple. A Root CA with a single certificate and using eapol_test to test.

The Root CA