TLS / Certificates for Radmind

On the Server:

Create a Certificate Authority

1. Create the Certificate Authority directory structure:

   In terminal, enable root in terminal – (I usually type sudo su – at the prompt)

   ```
   root# cd /var/radmind
   root# mkdir CA
   root# mkdir CA/certs
   root# mkdir CA/crl
   root# mkdir CA/newcerts
   root# mkdir CA/private
   root# echo "01" > CA/serial
   root# touch CA/index.txt
   ```

2. Download the openssl config file from Umich

   ```
   root# cd /var/radmind/CA
   root# curl –O http://www.rsug.itd.umich.edu/software/radmind/files/openssl.cnf
   ```

   Watch file download

3. Create self-signed certificate authority (CA) certificate and encrypted private key

   ```
   root# cd /var/radmind/CA
   root# openssl req –new –x509 –days 360 –keyout private/CAkey.pem –out ca.pem –config \
   openssl.cnf
   ```

   (note: I've been unable to set my certificates to last longer than 360 days even if I enter a different number after the days field)

   when prompted, create PEM passphrase

   Data for fields:
   Country Name: US
   State/Province Name: Massachusetts
   Locality Name: City Name
   Org. Name: College
   Org Unit Name: Dept Name
   Common Name: servername.college.edu
   E-mail Address: acctname@college.edu

Create a Certificate for the Server

1. Create a certificate request and an unencrypted private key

   ```
   root# cd /var/radmind/CA
   root# openssl req –new –keyout key.pem –out req.pem –days 360 –config openssl.cnf –nodes
   ```

   Data for fields:
   Country Name: US

State/Province Name: Massachusetts
Locality Name: City Name
Org. Name: College
Org Unit Name: Dept Name
Common Name: servername.college.edu
E-mail Address: acctname@college.edu

2. Sign the certificate request with the CA’s certificate and private key

```
root# cat req.pem key.pem > new-req.pem
root# openssl ca –policy policy_match –out out.pem –config openssl.cnf –infiles new-req.pem
```

Confirm signing of certificate

3. Combine the certificate and key into one file

```
root# cat out.pem key.pem > cert.pem
```

4. Remove temporary files

```
root# rm req.pem new-req.pem out.pem
```

Extra Steps

1. Copy the server’s certificate into /var/radmind/cert on the server

```
root# cp /var/radmind/CA/cert.pem /var/radmind/cert
```

2. Copy the CA’s certificate into /var/radmind/cert on the server

```
root# cp /var/radmind/CA/ca.pem /var/radmind/cert
```

Create a Certificate for the Client

1. Create a certificate request and an unencrypted private key – this certificate will only be valid for 360 days, so you may want to make the time longer

```
root# cd /var/radmind/CA
root# openssl req –new –keyout key.pem –out req.pem –days 360 –config openssl.cnf –nodes
```

Data for fields:
Country Name: US
State/Province Name: Massachusetts
Locality Name: City Name
Org. Name: College
Org Unit Name: Dept Name
Common Name: **labname**
E-mail Address: fake@college.edu

2. Sign the certificate request with the CA’s certificate and private key

```
root# cat req.pem key.pem > new-req.pem
root# openssl ca –policy policy_match –out out.pem –config openssl.cnf –infiles new-req.pem
```

Confirm signing of certificate

3. Combine the certificate and key into one file

```
root# cat out.pem key.pem > labname.pem
```

4. Remove temporary files

```
root# rm req.pem new-req.pem out.pem
```

5. Move combined certificate & key into /var/radmind/CA/certs

```
root# mv labname.pem certs/labname.pem
```

On the Client:

Enable root in terminal (back door – see beginning of documentation)

1. Create the directory called cert in radmind

```
root# mkdir cert /var/radmind
```

2. Copy the client's certificate into /var/radmind/cert on the client

```
ftp servername.college.edu
Enter name: acctname
Enter password: xxxxxxxxxxx
get /var/radmind/CA/certs/knapp.pem /var/radmind/cert/cert.pem
```

3. Copy the CA's certificate into /var/radmind/cert on the client

```
If disconnected, reconnect via ftp to server
get /var/radmind/CA/ca.pem /var/radmind/cert/ca.pem
bye (disconnects)
```

4. Open Radmind Assistant. In Preferences, set SSL Authorization/Encryption to Verify Client & Server

5. Restart client just to be on the safe side

On Radmind Server Manager

1. Add client **labname** – choose command file
2. In Radmind Server Prefs, set SSL Authorization/Encryption to Verify Client & Server
3. In Terminal you will modify one line in a file called RadmindServer using a unix text editor called pico:
   a. Log in as root
   b. root# cd /Library/StartupItems/Radmind\ Server
   c. root# pico RadmindServer
      i. change /usr/local/sbin/radmind –u 077 to /usr/local/sbin/radmind –u 077 –w 2
      ii. Save (Ctrl + x then RETURN)
4. **Restart Server**