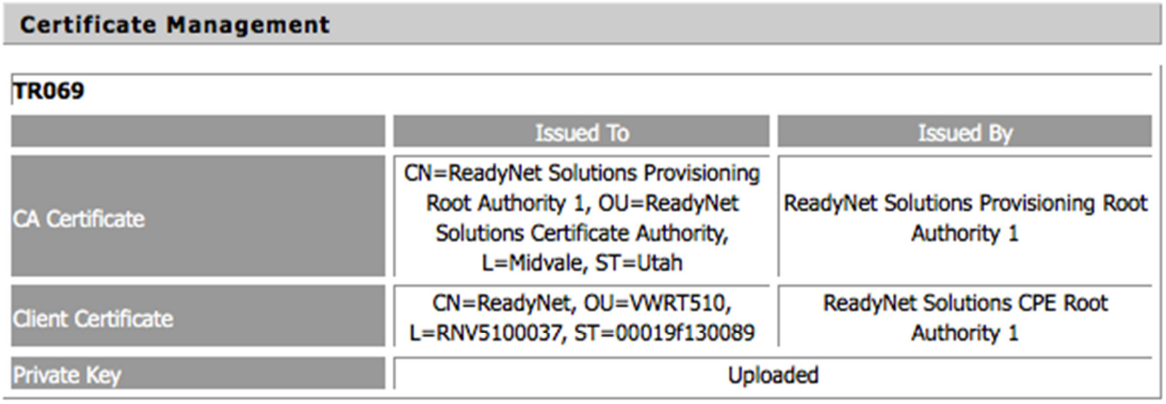
HTTPS Provisioning

For secure provisioning, ReadyNet devices ship with unique SSL Client Certificates and a ReadyNet CA root certificate. The client certificate allows the provisioning sever to identify the individual devices while the CA root certificate allows the device to recognize authentic provisioning servers.

Client certificates and the CA root certificate for a device may be viewed under Administration > Certification.



Certificate Management

TR069

	Issued To	Issued By
CA Certificate	CN=ReadyNet Solutions Provisioning Root Authority 1, OU=ReadyNet Solutions Certificate Authority, L=Midvale, ST=Utah	ReadyNet Solutions Provisioning Root Authority 1
Client Certificate	CN=ReadyNet, OU=VWRT510, L=RNV5100037, ST=00019f130089	ReadyNet Solutions CPE Root Authority 1
Private Key	Uploaded	

Figure 1.

The client certificates and ReadyNet CA root certificate are used both for provisioning via TR-069 and configuration profile synchronization. The client certificate and the ReadyNet CA root certificate are not overwritten by firmware upgrades.

For secure end-to-end HTTPS provisioning, the service provider will need to install a server certificate on each provisioning server by which ReadyNet devices will be configured. This server certificate must be signed by ReadyNet.

Obtaining a Provisioning Server Certificate

For each provisioning server, the service provider will need to submit to ReadyNet a Certificate Signing Request (CSR). There is no charge for obtaining or renewing provisioning server certificates. The steps show below use the openssl command.

1) First create a server key with;

```
openssl genrsa –out ServerKey.pem 1024
```

2) Then create a CSR with;

```
openssl req –new –key ServerKey.pem –out CSR.pem
```

Ensure that the ‘Common Name’ field contains the FQDN (Fully Qualified Domain Name) of the provisioning server and that the other fields are appropriate.

3) Email the CSR.pem file to SSLCA@readynetsolutions.com

We will return two files. The server certificate (server.crt) and the ReadyNet CPE Certificate Authority file (CPE_CA.pem). Below is an example Apache web server configuration snippet showing the deployment of the various files.

```
SSLCertificateKeyFile /etc/pki/ServerKey.key  # private key from step 1
SSLCertificateFile /etc/pki/server.crt  # returned server certificate
SSLCACertificateFile /etc/pki/CPE_CA.pem  # returned CPE_CA.pem file
SSLVerifyClient require
```

The provisioning server will verify the client certificate presented by the device using the CPE_CA.pem file. The device will use the ReadyNet CA root certificate to verify the authenticity of the server. On successful mutual SSL authentication, the contents of the client certificate will be available as CGI environment variables in the provisioning server.

SSL environment variables table:

Variable Name	Description
SSL_CLIENT_S_DN_CN	Company Name
SSL_CLIENT_S_DN_OU	Device Model
SSL_CLIENT_S_DN_L	Device Serial Number
SSL_CLIENT_S_DN_ST	Device WAN MAC Address

For the device in Figure 1, the SSL environment variables would have the following values:

Variable Name	Value
SSL_CLIENT_S_DN_CN	ReadyNet
SSL_CLIENT_S_DN_OU	VWRT510
SSL_CLIENT_S_DN_L	RNV5100037
SSL_CLIENT_S_DN_ST	00019f130089

Provisioning server certificates from ReadyNet are valid for 2 years and need to be renewed when they expire. There is no charge for renewal of provisioning server certificates. Perform steps 2 and 3 to renew a provisioning server certificate.