



26/10/17 guía_creacion_certificados_radius_v1.odt

Guía para la generación de certificados para el Radius

Siguiendo estos pasos de la guía le permitirá generar los certificados en su servidor Radius para que sean firmados y contar así con los permisos necesarios.

Creamos estos 2 directorios:

```
# cd /usr/local/etc/raddb
# mkdir -p newcerts
# cd newcerts
# mkdir private
```

esta opción cifra la clave privada:

```
# openssl genrsa -aes256 -out private/radius.key 4096
Generating RSA private key, 4096 bit long modulus
.....++
.....++
e is 65537 (0x10001)
Enter pass phrase for private/radius.key:esta_es_la_clave_privada_del_radius_no_hay_que_perderla
Verifying - Enter pass phrase for

private/radius.key:esta_es_la_clave_privada_del_radius_no_hay_que_perderla

# openssl dhparam -out dh 1024
# dd if=/dev/urandom of=./random count=10
# touch index.txt
# echo '01' > serial
```

Ahora tenemos que bajar la clave publica de la CA en la que confiamos (de eduroam.uy), de la siguiente dirección:

```
# cd /usr/local/etc/raddb/newcerts
# wget http://eduroam.uy/docs/ca.crt
```

Hay que crear el certificado para el radius que vamos a configurar, lo primero es crear un archivo de configuración, donde esté definido los valores que va a tener el certificado, a este archivo le llamo radius.cnf:

```
# cd /usr/local/etc/raddb/newcerts
# wget http://eduroam.uy/docs/radius.cnf
```

luego en el archivo radius.cnf cambiaremos lo que corresponda dentro del [server] (en negrita):

```
[server]
countryName          = UY
stateOrProvinceName = Montevideo
localityName         = Montevideo
organizationName     = RAU
emailAddress       = eduroam@<Institución>.edu.uy
```



Universidad de la República
Red Académica Uruguay

```
commonName          = radius.<Institución>.edu.uy
```

y salvamos.

Nota:

eduroam@<Institución>.edu.uy: Es la cuenta de correo del responsable del servicio eduroam en su Institución.

radius.<Institución>.edu.uy: Este nombre coincide con el Hostname de su servidor <Institución>

Ahora ejecutamos Openssl para la creación de una solicitud de certificado digital para el RADIUS:

```
# openssl req -new -nodes -out radius.<Institución>.csr -key private/radius.key -config
./radius.cnf
Enter pass phrase for ./prueba.key:esta_es_la_clave_privada_del_radius_no_hay_que_perderla
```

El certificado radius.<Institución>.csr, lo tienen que mandar vía correo electrónico a eduroam@rau.edu.uy, para que lo devuelvan firmado (radius.<Institución>.crt), y deberá quedar guardado en el directorio:

```
# cd /usr/local/etc/raddb/newcerts
```
