

## Práctico: Autoridad Certificadora con openssl

WALC 2004 – Track 2  
Cuzco, Perú  
Diego Di Pascua  
dipascua@seciu.edu.uy

Con usuario root:

1. Configurar openssl:

```
cd /usr/share/ssl  
cp -p openssl.cnf openssl.cnf.ori
```

Editar openssl.cnf, y modificar registros en sección [ CA\_default ]:

```
dir                = /home/taller2/ca  
certs              = $dir/certs  
crl_dir            = $dir/crl  
database           = $dir/index.txt  
new_certs_dir      = $dir/nuevoscerts  
  
certificate        = $dir/certs/certca.pem  
serial             = $dir/serial  
crl                = $dir/crl.pem  
private_key        = $dir/privado/clavesca.pem  
RANDFILE           = $dir/privado/.rand
```

(dejar el resto de archivo sin modificar)

Con usuario taller2:

2. Crear estructura a usar:

```
cd /home/taller2  
mkdir ca  
mkdir ca/certs  
mkdir ca/crl  
mkdir ca/nuevoscerts  
mkdir ca/privado  
mkdir ca/csr  
echo "01" > ca/serial  
touch ca/index.txt
```

3. Generar par de claves RSA de 2048 bits para la CA; archivo cifrado con 3DES:  
openssl genrsa -des3 -out ca/privado/clavesca.pem 2048

4. Generar certificado de la CA, de 3 años de validez:  
openssl req -new -x509 -out ca/certs/certca.pem -days 1095 -key  
ca/privado/clavesca.pem

5. Generar par de claves RSA de 1024 bits de un usuario:  
openssl genrsa -des3 -out ca/privado/clavesusr.pem 1024

6. Generar requerimiento de certificado de dicho usuario:  
openssl req -new -out ca/csr/csrusr.pem -key ca/privado/clavesusr.pem

7. Generar certificado del usuario:  
openssl ca -in ca/csr/csrusr.pem

Nota: Los puntos 5 y 6 deberían ser realizados por el usuario en su propia estación.