CHULETA PRÁCTICA 2 – CRIPTOGRAFÍA Y HTTPS (Rocky y Ubuntu)

---

1) Instalación Apache + SSL

```
# Rocky
sudo dnf install httpd mod_ssl openssl -y
sudo systemctl start httpd
sudo systemctl enable httpd
# Ubuntu
sudo apt update
sudo apt install apache2 openssl -y
sudo a2enmod ssl
sudo a2ensite default-ssl
sudo systemctl restart apache2
```

---

2) Crear CA (Autoridad Certificadora)

```
sudo find /etc -name openssl.cnf
sudo nano /etc/pki/tls/openssl.cnf
# Cambiar dir=/etc/pki/CA -> /etc/pki/tls
cd /etc/pki/tls
sudo openssl genrsa -aes256 -out private/cakey.pem 2048
sudo openssl req -new -key private/cakey.pem -out ca-csr.pem
sudo openssl req -x509 -extensions v3_ca -key private/cakey.pem -in ca-csr.pem -out cacert.pem -days 365
openssl rsa -noout -text -in private/cakey.pem
openssl x509 -noout -text -in cacert.pem
```

---

3) Crear lista de revocación (CRL)

```
openssl ca -gencrl -out crl.pem
openssl crl -noout -text -in crl.pem
```

---

4) Certificado servidor web

```
openssl genrsa -aes256 -out private/www.miservidor.es.pem 2048
openssl req -new -key private/www.miservidor.es.pem -out www.miservidor.es.csr.pem
openssl ca -extensions server_SAN -in www.miservidor.es.csr.pem -out certs/www.miservidor.es.crt.pem -days 365
```

---

5) Configurar Apache HTTPS

```
sudo mkdir -p /projects/miservidor
echo "Servidor HTTPS www.miservidor.es" | sudo tee /projects/miservidor/index.html
sudo vi /etc/httpd/conf.d/miservidor.conf
sudo systemctl restart httpd
```

---

6) Importar CA en navegador

```
scp root@192.168.32.128:/etc/pki/tls/cacert.pem C:\Users\\Desktop\
# mmc → certificados → equipo local → importar
```

---

7) Certificados de cliente (Carmen Cabrera)

```
openssl genrsa -out private/carmen.key.pem 2048
openssl req -new -key private/carmen.key.pem -out carmen.csr.pem
openssl ca -extensions user -in carmen.csr.pem -out certs/carmen.crt.pem -days 365
openssl pkcs12 -export -in certs/carmen.crt.pem -inkey private/carmen.key.pem -out carmen.p12
# Apache solicita certificados
sudo vi /etc/httpd/conf.d/miservidor.conf
sudo systemctl restart httpd
```

---

8) Certificado cliente (Mario Martínez)

```
openssl genrsa -out private/mario.key.pem 2048
openssl req -new -key private/mario.key.pem -out mario.csr.pem
```

```
openssl ca -extensions user -in mario.csr.pem -out certs/mario.crt.pem -days 365
openssl pkcs12 -export -in certs/mario.crt.pem -inkey private/mario.key.pem -out mario.p12
mkdir -p /projects/miservidor/Ventas /projects/miservidor/Personal
sudo vi /etc/httpd/conf.d/miservidor.conf
sudo systemctl restart httpd
```

---

9) Revocar certificado

```
openssl ca -revoke certs/mario.crt.pem -keyfile private/cakey.pem -cert cacert.pem
openssl ca -gencrl -out crl.pem -keyfile private/cakey.pem -cert cacert.pem
openssl crl -noout -text -in crl.pem
# En Apache -> SSLVerifyDepth 2
```

---

10) Servidor HTTPS Ubuntu (www.pruebas.com / .net)

```
sudo apt install apache2 openssl -y
sudo a2enmod ssl
sudo a2ensite default-ssl
sudo systemctl restart apache2
mkdir -p /projects/pruebas
vi /projects/pruebas/index.html
mkdir -p /etc/pki/tls/{certs,crl,newcerts,private}
touch /etc/pki/tls/index.txt
echo 01 > /etc/pki/tls/serial
echo 01 > /etc/pki/tls/crlnumber
ln -s /etc/ssl/openssl.cnf /etc/pki/tls/openssl.cnf
scp root@192.168.32.128:/etc/pki/tls/cacert.pem /etc/pki/tls/
openssl genrsa -out private/pruebas.key.pem 2048
openssl req -new -key private/pruebas.key.pem -out pruebas.csr.pem
# Firmar desde Rocky si da error
openssl ca -in pruebas.csr.pem -out certs/pruebas.crt.pem -extfile san_pruebas.ext -extensions server_SAN -days 365
```

---

11) Certificado wildcard (*.miempresa.es)

```
openssl genrsa -out private/miempresa.key.pem 2048
openssl req -new -key private/miempresa.key.pem -out miempresa.csr.pem
vi san_miempresa.ext
openssl ca -in miempresa.csr.pem -out certs/miempresa.crt.pem -extfile san_miempresa.ext -extensions server_SAN -days 365
scp /etc/pki/tls/certs/miempresa.crt.pem root@192.168.32.129:/etc/pki/tls/certs/
scp /etc/pki/tls/private/miempresa.key.pem root@192.168.32.129:/etc/pki/tls/private/
mkdir -p /projects/proyecto1 /projects/www
vi /etc/apache2/sites-available/miempresa.conf
sudo a2ensite miempresa.conf
sudo systemctl restart apache2
```