FSI LEI 2025/2026

Practical Exercises #5 Resolution examples

Goals

Create a private CA with OpenSSL

Create X.509 certificates

Server and client authentication using certificates with Apache

Create a private Certification Authority (CA)

1. Create a private CA using OpenSSL in Linux

```
cd /etc/pki/CA

openssl genrsa –out ca.key –des3

openssl req -new -key ca.key -out ca.csr

(CN = Name of CA)

openssl x509 -req -days 365 -in ca.csr -out ca.crt -signkey ca.key

openssl x509 –in ca.crt –text | more
```

2. Create a X.509 certificate for the Apache server using the new CA

```
openssl genrsa -out apache.key -des3

openssl req -new -key apache.key -out apache.csr

(CN = FQDN of server)

touch index.txt

echo 01>serial

openssl ca -in apache.csr -cert ca.crt -keyfile ca.key -out apache.crt

openssl x509 –in apache.crt -text
```

Configure Apache with server authentication

Installing Apache and mod_ssl:

```
yum install httpd mod_ssl
```

3. Configure Apache to use the previously created X.509 certificate

```
Edit /etc/httpd/conf.d/ssl.conf

SSLCertificateFile /etc/pki/CA/apache.crt

SSLCertificateKeyFile /etc/pki/CA/apache.key

SSLCACertificateFile /etc/pki/CA/ca.crt
```

Materials

- Apache SSL/TLS Encryption
- Segurança prática em Sistemas e Redes com Linux, Jorge Granjal, FCA 2017, "Capítulo 3. Autoridades de Certificação Digital"
- Segurança prática em Sistemas e Redes com Linux, Jorge Granjal, FCA 2017, "Capítulo 5. Servidores WWW seguros"

4. Connect to the server (the new CA isn't recognized yet)
5. Install the CA on the browser and repeat the previous test

Configure Apache with client authentication

6. Create a personal X.509 certificate using the new CA

```
openssl genrsa -out user.key -des3
openssl req -new -key user.key -out user.csr
(CN = Your name)
openssl ca -in user.csr -cert ca.crt -keyfile ca.key -out user.crt
openssl pkcs12 -export -clcerts -in user.crt -inkey user.key -out user.p12
```

7. Configure Apache to require client authentication using X.509 certificates

```
In ssl.conf:
SSLVerifyClient require
SSLVerifyDepth  10
```

8. Connect to the Apache server without using your personal certificate (the connection should be refused, check the server's logs)

```
Server logs (ssl) in:
tail –f /var/log/httpd/ssl_error_log
If necessary, increase log levels in ssl.conf:
ErrorLog logs/ssl_error_log
TransferLog logs/ssl_access_log
LogLevel debug
```

9. Install the personal certificate on the browser and repeat the previous test