STI MEI/MIEBIOM 2022/2023

Practical Exercises #2

Create a private Certification Authority (CA)

1. Create a private CA using OpenSSL in Linux
2. Create a X.509 certificate for the Apache server using the new CA

Configure Apache with server authentication

3. Configure Apache to use the previously created X.509 certificate
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
7. Configure Apache to require client authentication using X.509 certificates
8. Connect to the Apache server without using your personal certificate (the connection should be refused, check the server's logs)
9. Install the personal certificate on the browser and repeat the previous test

Goals

Create a private CA with OpenSSL

Create X.509 certificates

Server and client authentication using certificates with Apache

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"