

# 0202 Instal·lació d'un certificat SSL autosignat.



Siscar Pascual, Lorena

Curs: 2024-2025

2ºDAW

## Índex

Enunciat.....	3
---------------	---

## Enunciat

1. Crea un certificat autosignat i configura'l en Apache de forma que en accedir a l'URL `https://###.aula218.lan` s'establisca una connexió segura. Guarda el certificat en la carpeta `/var/cert`.

El openssl es una biblioteca de software de codi obert que proporciona eines i funcions per a la implementació de protocols de seguretat. S'utilitza per xifrar i assegurar comunicacions en xarxa.

## Instal·lar opensall

```
# apt install openssl
```

**Crear un directori per a guardar el certificat.**

```
# mkdir /var/cert
```

## Genera un certificat SSL autosignat amb una clau.

```
# openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout/var/cert/aula218.key -out /var/cert/aula218.crt
```

[illegible]

You are about to be asked to enter information that will be incorporated into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.

There are quite a few fields but you can leave some blank

For some fields there will be a default value.

If you enter '.', the field will be left blank.

Country Name (2 letter code) [AU]:**ES**

State or Province Name (full name) [Some-State]: **Alacant**

Locality Name (eg, city)

Organization Name (eg, company) [Internet Widgits Pty Ltd]: IES Enric Valor

Organizational Unit Name (eg, section) []: **aula218**Common Name (e.g. server FQDN or YOUR name) []: **DAW**

Email Address []:

**Com poder vorer ens ha fet una sèrie de preguntes que com podem vorer les respostes estan de color roig.**

**Explicació del comandament:**

**openssl req:** Indica que estem utilitzant OpenSSL per gestionar una sol·licitud de certificat.

**-x509: Crea un certificat autofirmat.**

**-nodes:** Genera la clau privada sense xifrat.

**-day 365:** La validesa del certificat serà de 365 dies.

**-newkey rsa:2048** Crea una nova clau privada de 2048 bits amb l'algorisme RSA.

**-keyout /var/cert/aula218.key:** desa la clau privada en el fitxer /var/cert/aula218.lan.

**-out /var/cert/aula218.crt:** desa el certificat generat en /var/cert/aula218.crt.

## Editem el arxiu de configuració default-ssl.conf.

```
# nano /etc/apache2/sites-available/default-ssl.conf
```

Busquem SSLCertificateFile i SSLCertificateKeyFile modifiquem la ruta a on volem que estiga.

```
SSLCertificateFile    /var/cert/aula218.crt
SSLCertificateKeyFile /var/cert/aula218.key
```

Activem el mòdul SSL d'apache.

```
# a2enmod ssl
```

```
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Module socache_shmcb already enabled
Module ssl already enabled
```

També activem la configuració del lloc SSL.

```
# a2ensite default-ssl
```

```
Site default-ssl already enabled
```

Per últim reiniciem el servidor apache per aplicar els canvis.

```
# systemctl restart apache2
```

2. S'ha aconseguit establir una connexió segura? El navegador mostra algún avís?  
Justifica les respostes i documenta-les.

Si, s'ha establert la connexió segura, xifrada HTTPS, ha detectat i mostra un avís. Si el navegador mostra l'avís com a que no pots entrar però vaig de tot ix la url i pots accedir perfectament.



### La connexió no és privada

És possible que hi hagi atacants que estiguin provant de robar-vos informació de **02.aula218.lan** (per exemple, contrasenyes, missatges o targetes de crèdit). [Més informació sobre aquest advertiment](#)

NET::ERR\_CERT\_AUTHORITY\_INVALID



[Activa la protecció millorada](#) per obtenir el màxim nivell de seguretat de Chrome

[Amaga la configuració avançada](#)

[Torna a una pàgina segura](#)

Aquest servidor no ha pogut comprovar que sigui **02.aula218.lan** perquè el sistema operatiu del vostre ordinador considera que el seu certificat de seguretat no és de confiança. Això pot ser a causa d'una configuració incorrecta o d'un atacant que intercepta la vostra connexió.

[Continua per accedir a 02.aula218.lan \(no segur\)](#)