

# UFZ - Serveis Web

Comunicacions segures

# Comunicacions segures

HTTP té el mateix problema que als inicis d'internet. El mateix que FTP, TFTP, SMTP...

La informació viatja sense protecció.

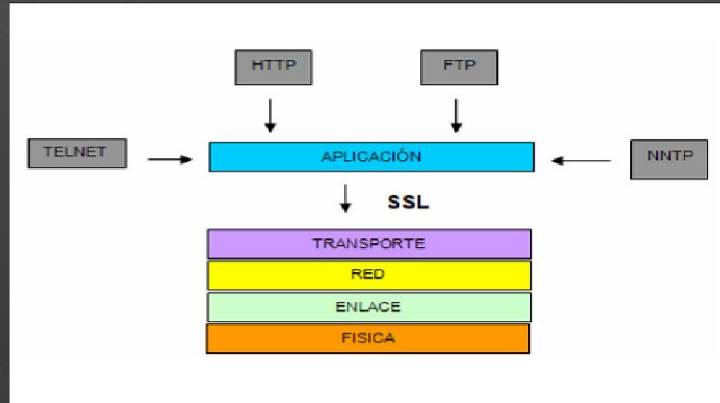
El primer mecanisme de seguretat implementat va ser SSL (Netscape).



# SSL

SSL proporciona una capa de seguretat entre la capa de transport TCP i la capa d'aplicació HTTP.


HTTPS ens indica que estem utilitzant HTML amb algun mecanisme de transport xifrat ( SSL o TLS). I utilitza el port 443.



# Comunicacions segures

HTTPS permet la confidencialitat entre tots dos extrems de la comunicació, encara que només un dels extrems s'hagi autenticat.

Els passos necessaris per implementar webs segures són:

- **Certificats digitals:** el servidor necessita un certificat digital.
  - **Mòdul mod\_ssl:** tenir instal·lat i activat el mòdul que proporciona SSL al servidor.
  - **Configurar la seu web segura:** cal establir les directives SSL apropiades per fer el nostre web accessible via SSL.
- 

# Certificats digitals

Un **Certificat digital** és un document electrònic expedit per una **Autoritat de Certificació** i que identifica una persona amb un **parell de claus**. La clau pública la deixem a disposició de tothom i la clau privada no la lliurem a ningú.

Els certificats digitals utilitzen **xifrat asimètric**, el que codifica una clau només ho pot descodificar l'altre.

També se'n pot dir Certificat públic i privat.



# Certificats del servidor

Cal generar un certificat!

Aquest pot ser generat per nosaltres o per una autoritat de certificació.

## **Generar un certificat autosignat**

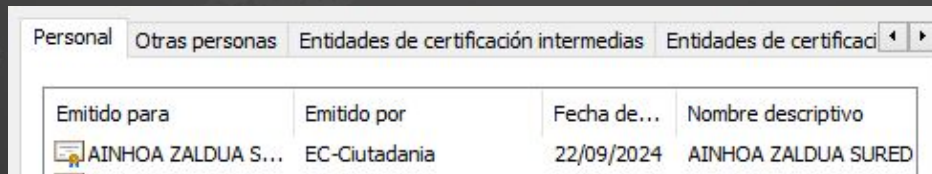
A mode de recordatori ràpid, es pot generar una clau privada i un certificat autosignat fent:

```
# openssl req -new -x509 -nodes -out server.crt -keyout server.key
```

# Certificats del servidor

Al subdirectori de certificats (`httpd/certs/`) hi haurà:

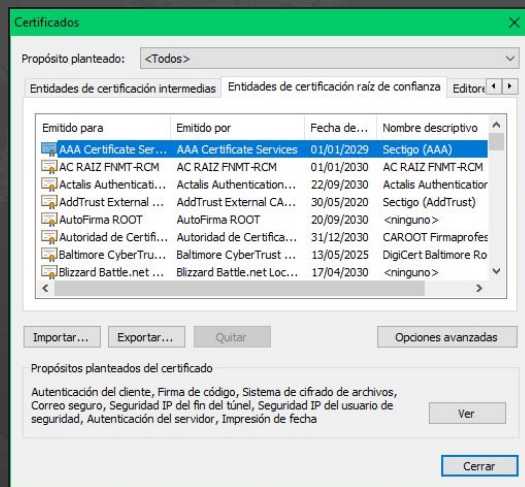
- **server.crt**: fitxer corresponent al certificat o clau pública del servidor.
- **server.key**: fitxer corresponent a la clau privada del servidor. S'ha de codificar amb una *passphrase*. Cada vegada que inicialitzem el servidor cal entrar aquesta frase.



# Certificats del servidor

Els navegadors validaran la confiança d'un certificat contrastant el seu emissor amb la llista d'entitats certificadores que tenen carregada.

Què passa si l'emissor del certificat no es troba a la llista?

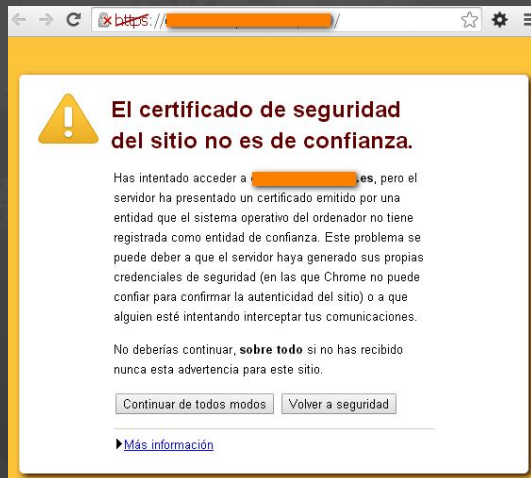




# Certificats del servidor

Si l'emissor no es troba a la llista caldrà:

- Admetre el certificat com a vàlid.
- Obtener el certificat de l'entitat que l'ha generat i incorporar l'entitat al llistat de confiança.



# Configuració d'Apache per SSL

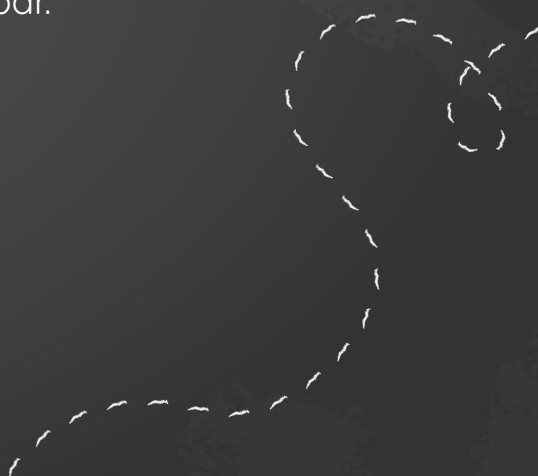
Habitualment tant el paquet com el mòdul SSL s'anomenen `mod_ssl`.

Un cop instal·lat caldrà habilitar-lo amb la comanda **`a2enmod`**

...i reiniciar el servidor!

Si accedim a la carpeta `/etc/apache2/mods-enabled` l'hauriem de trobar.

Si el volem desactivar ho farem amb la comanda **`a2dismod`**



# Configuració de la web amb SSL

Cal aplicar les directives apropiades per fer possible l'accés per HTTPS.

Recordem: el port canvia per HTTPS!  
per això esdevé un altre seu virtual.

...i reiniciar el servidor un cop hem acabat!

```
<VirtualHost www.ioc.cat:443>  
  ServerAdmin webmaster@ioc.cat  
  DocumentRoot /var/www/www.ioc.cat  
  SSLEngine On  
  SSLProtocol all -SSLv3  
  SSLCertificateKeyFile /var/www/certs/server.key  
  SSLCertificateFile /var/www/certs/server.crt  
</VirtualHost>
```

# Configuració de la web amb SSL

- **Port 443:** port usual per connexions segures HTTP.
- **SSL Engine On:** indica que cal activar el trànsit SSL per la web.
- **SSL Protocol all -SSLv3:** s'indica quins protocols es poden usar per generar el trànsit xifrat.
- **SSLCertificateKeyFile:** fitxer que conté la clau privada del servidor.
- **SSLCertificateFile:** fitxer que conté el certificat del servidor.
- **SSLCACertificateFile:** directiva opcional. Permet indicar quin és el fitxer que conté el certificat públic que ha emès la entitat de certificació.

# Verificació de les connexions SSL

Ens podem trobar amb problemes al connectar amb webs amb certificat:

- Amb un certificat autosignat no cal definir CA (certificate authority)
  - El navegador mostra la pantalla d'excepció.
- Amb un certificat emès per una CA cal incorporar manualment el certificat al navegador.
  - El navegador serà capaç de validar el certificat del servidor amb la CA que l'ha emès.

# Verificació de les connexions SSL

Eines per verificar la nostra connexió:

- Navegador (accedint al web per HTTPS)
  - OpenSSL
  - Curl
- 