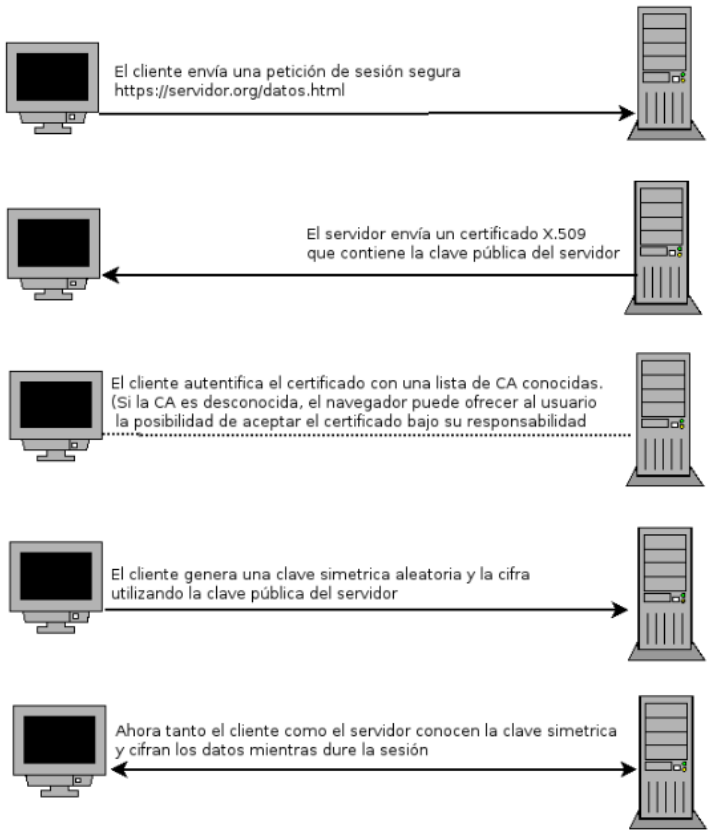
ACTIVITAT AVALUABLE AC7
Mòdul: MP08- Desplegament d'aplicacions web **UF:** UF1 – Servidors web i de transferència de fitxers **Professor:** Albert Guardiola **Data límit d'entrega:** 11/11/2024 **Mètode d'entrega:** Per mitjà del Clickedu de l'assignatura. Les activitats entregades més enllà de la data límit només podran obtenir una nota de 5. **Instruccions:** S'ha d'entregar un únic document amb el nom: ***MP08-UF1-AC7-Nom_Alumne.doc (o pdf)*** Es valorará la presentació.

Resultats de l'aprenentatge:
RA1. Implanta arquitectures web analitzant i aplicant criteris de funcionalitat. RA2. Gestiona servidors web avaluant i aplicant criteris de configuració per a l'accés segur als serveis.

En aquesta pràctica, muntarem un servidor virtual i el configurarem com un servidor segur, al que només es podrà accedir mitjançant el protocol HTTPS. El protocol HTTPS, sobre el nivell s'intercanvi de missatges HTTP, monta una capa de seguretat que es pot esquematitzar de la manera següent:



Tasca 1. Mira aquest vídeo i explica els seguents punts:

https://www.youtube.com/watch?v=THxIyHz191A&ab_channel=High-PerformanceProgramming

a)Quin és el protocol de xifrat que fa servir HTTPS?

b)Quina és la diferència entre SSL i TLS?

c)De quines dues fases consta el protocol TLS?

d)A la fase de *hadshake*, quin extrem HTTP proporciona el certificat SSL/TLS?

e)Com s'aconsegueix un certificat SSL/TLS?

f)Com es pot garantir que la clau de sessió generada pel client a la fase de *handshake* només podrà ser desencriptada pel servidor que ha presentat el certificat?

g)Quina clau es fa servir per encriptar els missatges HTTP: la clau pública o la privada (clau de sessió)?

h)El procés d'encriptació és simètric o asimètric?

i)Què vol dir que el protocol TLS proporciona també integritat de dades?

Tasca 2. Crea un servidor virtual pel domini www.securesite.org. Comprova que pots accedir-hi des del navegador i que aquest la considera una web no segura.

Tasca 3. A continuació, aconseguirem un certificat (més una clau pública) per a que el nou servidor virtual en faci ús.

a)Crea una carpeta *certs* al directori principal de configuració d'Apache.

b)Utilitza l'eina *openssl* per a crear un parell certificat + clau pública pel teu servidor:

sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout dawac6.key -out dawac6.crt

Openssl et demanarà una serie de dades per a incloure en el certificat:

```
albert@m8albert:/etc/apache2/certs$ sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout dawac6.key -out dawac6.crt
Generating a RSA private key
.....................................+++++
.....................+++++
writing new private key to 'dawac6.key'
-----
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]:Barcelona
Locality Name (eg, city) []:Barcelona
Organization Name (eg, company) [Internet Widgits Pty Ltd]:ETPX
Organizational Unit Name (eg, section) []:DAW
Common Name (e.g. server FQDN or YOUR name) []:www.securesite.org
Email Address []:
albert@m8albert:/etc/apache2/certs$ ls
```

c)Comprova que s'han generat els fitxers *dawac6.crt* i *dawac6.key*.

d)Abans de continuar, analitzem la comanda que hem fet servir: per què hem fet servir l'opció *-x509*?

Tasca 4. En aquest cas, hem generat un certificat autosignat: és a dir, un certificat signat, no per una autoritat certificadora, sinò pel propi administrador del servidor. Tot i que hi ha CAs (*certification authorities*) que proveeixen certificats de manera gratuïta (per exemple, cacert.org), és necessari tenir un domini propi (i públic) per a poder demanar-ne un.

a)Investiga quina és la limitació, de cara als clients, de l'ús de certificats autosignats.

b)Investiga quines són les principals autoritzats certificadores actuals.

Tasca 5. (Continuem amb tasca 3). Per a poder fer servir el xifrat SSL en el nostre servidor, hem de fer algunes configuracions:

a)Activa el mòdul *ssl*.

b)Canvia la configuració del servidor virtual que volem securitzar (www.securesite.org), de la següent manera:

```
<VirtualHost *:443>
        (...)

        SSLEngine on
        SSLCertificateFile /etc/apache2/certs/server.crt
        SSLCertificateKeyFile /etc/apache2/certs/server.key
</VirtualHost>
```

c)Reinicia el servidor per vere aplicats els canvis, i comprova què ocorre quan el navegador demana la web https://www.securesite.org.

d)Per què el navegador continua considerant el lloc insegur?

e)No obstant, comprova, amb les Eines del Programador del navegador, a la pestanya de Seguretat, que la connexió està xifrada.

f)Compara l'anterior amb el contingut de la pestanya Seguretat quan el servidor demana una pàgina HTTP convencional (per exemple, qualsevol dels servidors virtuals configurats en pràctiques anteriors).

Tasca 6. Amb les directives de configuració d'Apache treballades fins ara, com faries per a que el servidor servís, a una petició de http://www.securesite.org, el recurs segur https://www.securesite.org?

Tasca 7. Finalment, senyalarem algunes bones pràctiques de de seguretat en l'ús de servidors Apache. Investiga, per cada una d'aquestes bones pràctiques, 1) per què creus que es aconsellable, i 2) com la posaries en pràctica.

a)Ocultar la versió d'Apache instal·lada, la nostra IP i port, a les pàgines d'error proporcionades pel servidor.

b)Desactivar l'opció de llistat del contingut dels directoris sense index.

c)Deshabilitar els mòduls que no fem servir.

d)Deshabilitar els enllaços simbòlics.

e)Limitar el tamany de les peticions.

f)Mantenir el servidor actualitzat.

g)Fer servir algún firewall d'aplicacions web per Apache.