APACHE 2.4

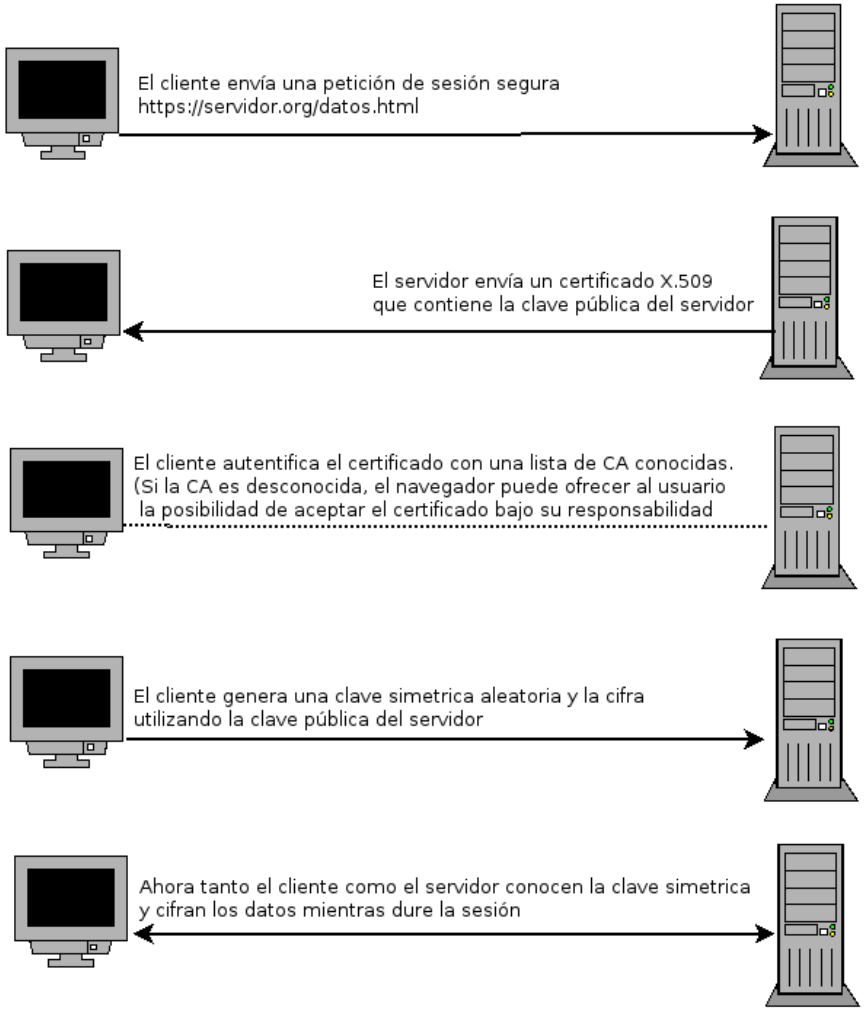
HTTPS

HTTPS

- Utiliza el protocolo SSL (actualmente TLS) para el cifrado de datos.
- El servidor utiliza por defecto el puerto 443/tcp.
- Utiliza mecanismos de cifrado de clave pública y las claves públicas se denominan certificados.
- El formato de los certificados está especificado por el estándar X.509 y normalmente son emitidos por una entidad denominada Autoridad Certificadora.

HTTPS

- En el caso de HTTPS, la función principal de la CA es demostrar la autenticidad del servidor y que pertenece legítimamente a la persona u organización que lo utiliza.
- El navegador contiene una lista de certificados de CA en las que confía y acepta inicialmente sólo los certificados de los servidores emitidos por alguna de estas CA.
- Una vez aceptado el certificado de un servidor web, el navegador utiliza éste para cifrar los datos que quiere enviar al servidor mediante el protocolo HTTPS y cuando llegan al servidor sólo éste podrá descifrarlos ya que es el único que posee la clave privada que los descifra.


El cliente envía una petición de sesión segura
https://servidor.org/datos.html
El servidor envía un certificado X.509
que contiene la clave pública del servidor
El cliente autentifica el certificado con una lista de CA conocidas.
(Si la CA es desconocida, el navegador puede ofrecer al usuario
la posibilidad de aceptar el certificado bajo su responsabilidad
El cliente genera una clave simetrica aleatoria y la cifra
utilizando la clave pública del servidor
Ahora tanto el cliente como el servidor conocen la clave simetrica
y cifran los datos mientras dure la sesión