HTTPS & SSL

Basics to understand connection

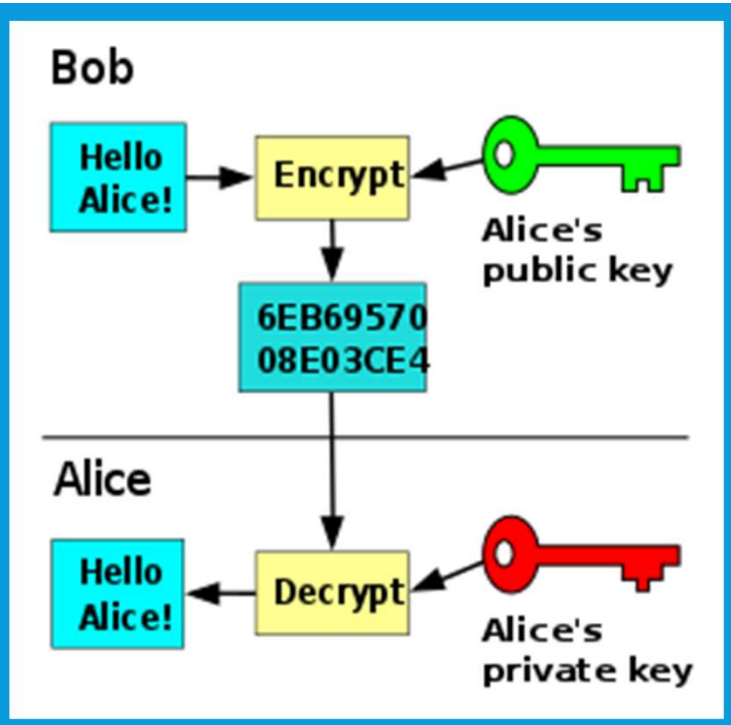
HTTP VS HTTPS

HTTP
TLS/SSL
HTTPS
TCP/UDP
CAPA DE HOST
IP
MAC
HARDWARE
CAPA DE MEDIO

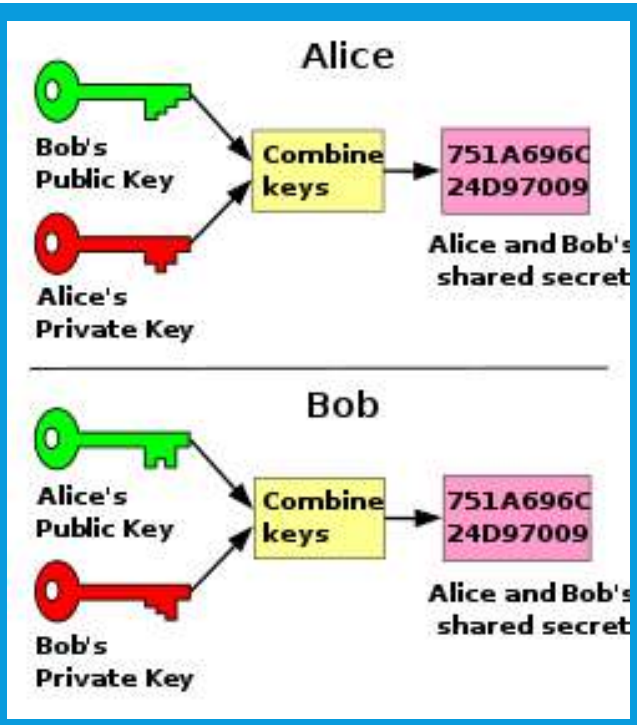
HTTPS

- La encriptación protege contra:
  - Intercepción de mensajes por terceros.
  - Alteración de los mensajes por terceros.
- Básicamente asegura el canal.
- Para garantizar la protección se usan certificados y encriptación de clave pública y privada.

CLAVE PUBLICA – CLAVE PRIVADA



Encriptación Asimétrica



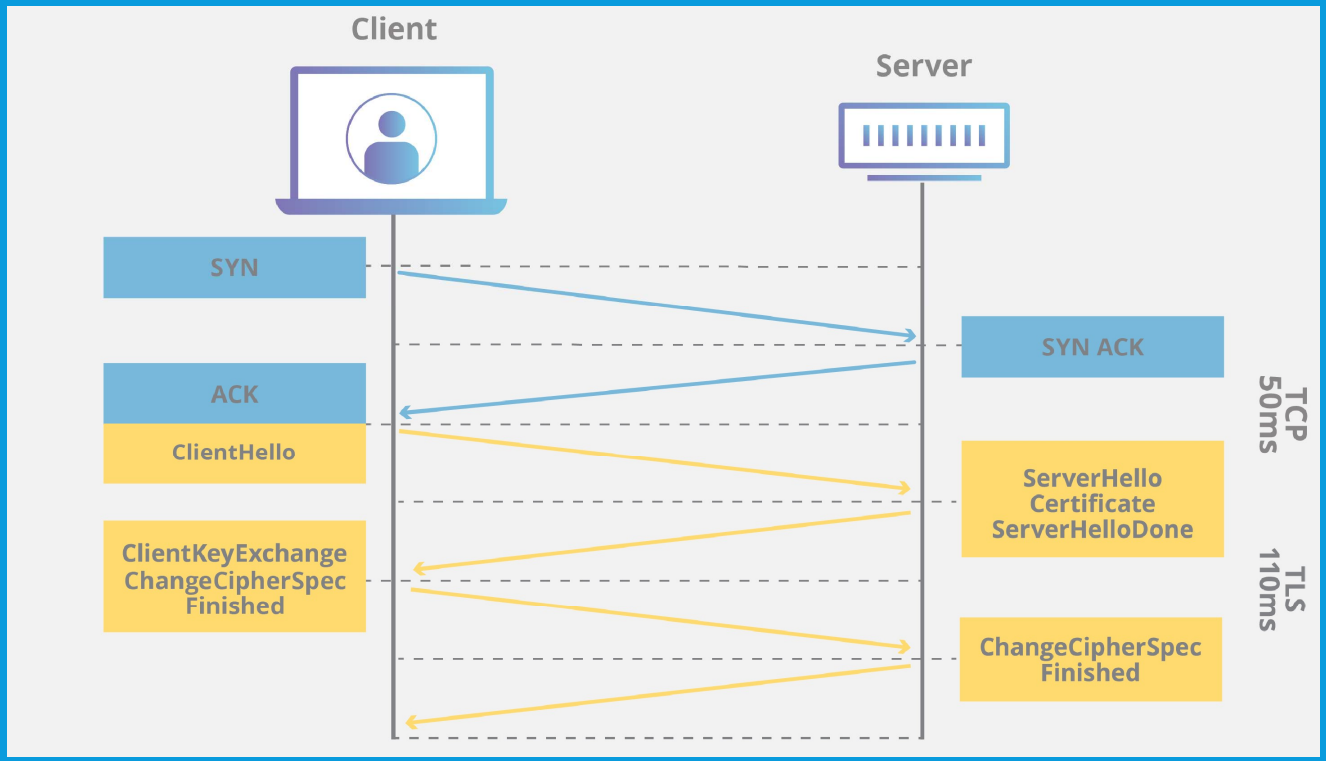
Modelo de Encriptación Simétrica

CERTIFICADOS

- Las claves son guardadas en certificados en formato X.509:
  - https://tools.ietf.org/html/rfc4158

- El servidor tiene su clave publica en un certificado, idealmente firmado. Este certificado es publicado para poder realizar la conexión. A su vez el servidor tiene su clave privada que no la publica.
- El certificado puede estar firmado, en este caso debería estarlo por una autoridad certificadora que verifica que esa clave corresponde a ese servidor.
- Estos certificados se suelen guardar en un keystore, un archivo encriptado que contiene certificados.

TLS HANDSHAKE



PROCESO – ALGORITMO RSA

1. El **cliente** envía el "hello", que incluye: version de TLS, ciphers suites (algoritmos que usa para generar la clave de session) que soporta y un random (un string aleatorio).
2. El **servidor** envía su hello, que incluye: el certificado con la clave pública, el cipher suite que eligió y un random.
3. El **cliente** verifica el certificado con la autoridad certificante. Identificando al servidor.
4. El **cliente** envía un secreto (otro string aleatorio) encriptado con la clave pública.
5. Tanto el **cliente** como el **servidor** generan un secreto compartido con el secreto del cliente y los random del cliente y el servidor.

VARIANTES

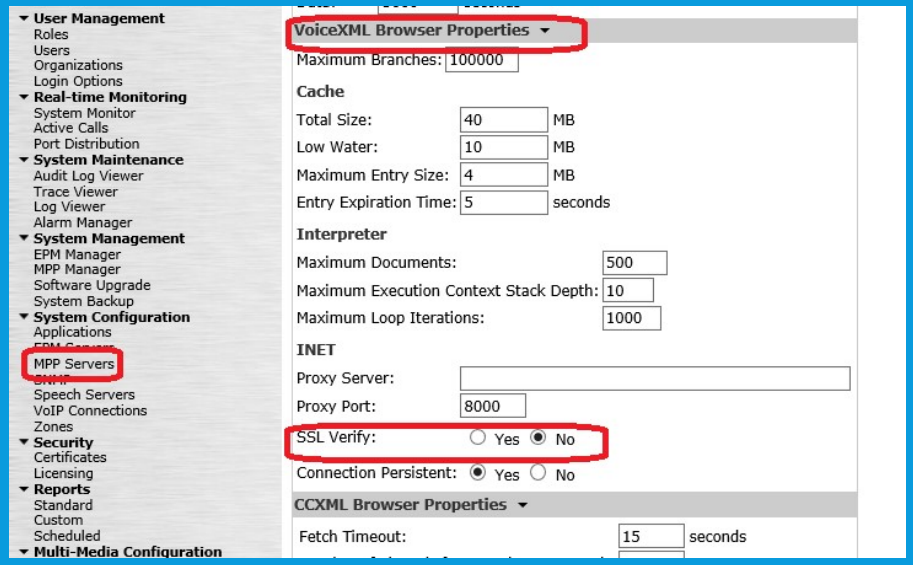
- Pueden existir casos que involucren certificados de clientes, cuando el servidor quiere limitar el acceso. No es el caso de las páginas web públicas.
- Los web browsers resuelven el proceso de intercambio y Pedido de certificados, sin embargo es possible que otras situaciones requieran obtener el certificado con la clave pública a mano.

AEP – SI EL SERVIDOR USA HTTPS

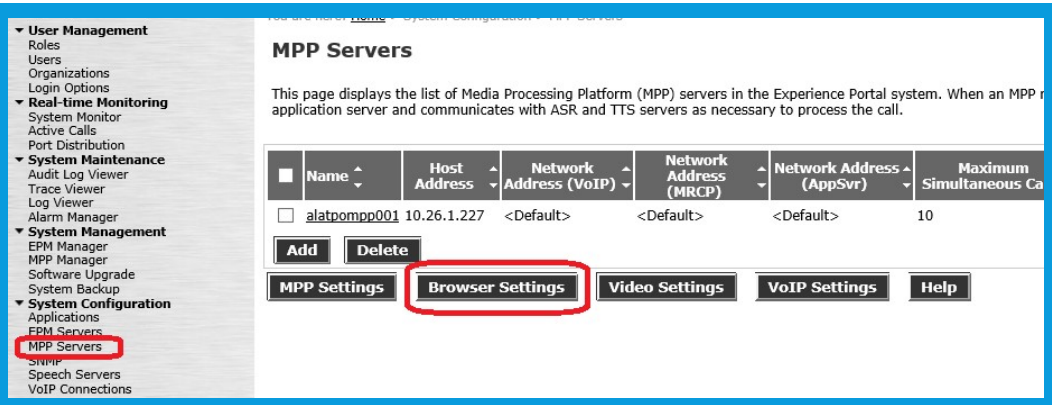
- Los MPPs estan capacitado paras hacer el handshake TSL, sin embargo es necesario habilitarlo.

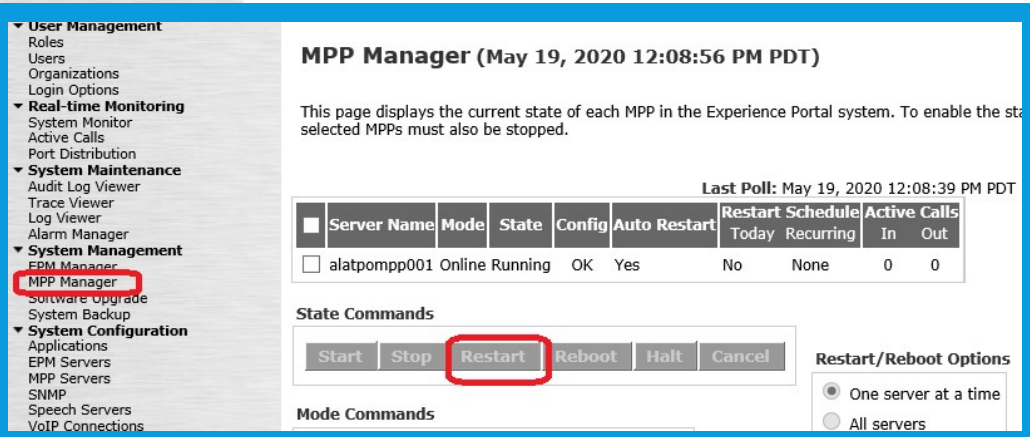
AEP – SI EL SERVIDOR USA HTTPS

- System Configuration -> MPP Servers -> Browser Settings -> SSL Verify (Yes)
- System Management -> MPP Manager -> Restart (Para c/u)



AEP – SI EL SERVIDOR USA HTTPS





GRACIAS