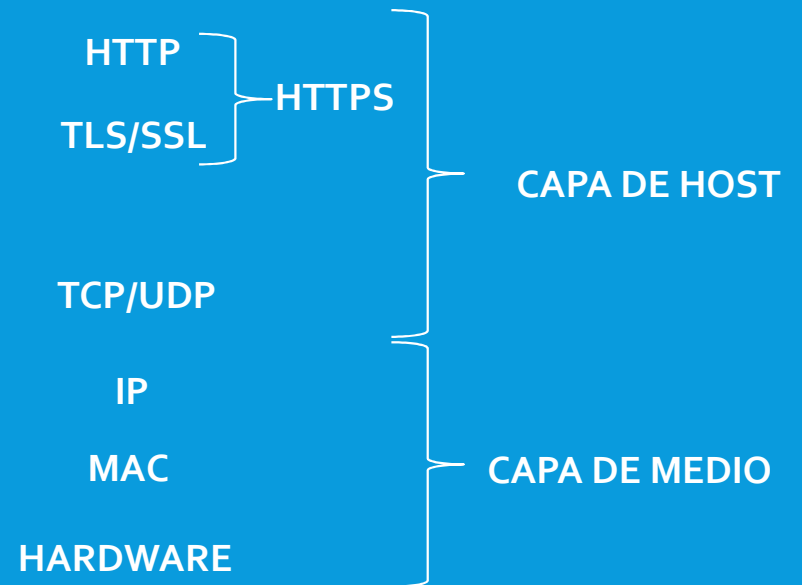


# HTTPS & SSL

Basics to understand connection

# HTTP VS HTTPS

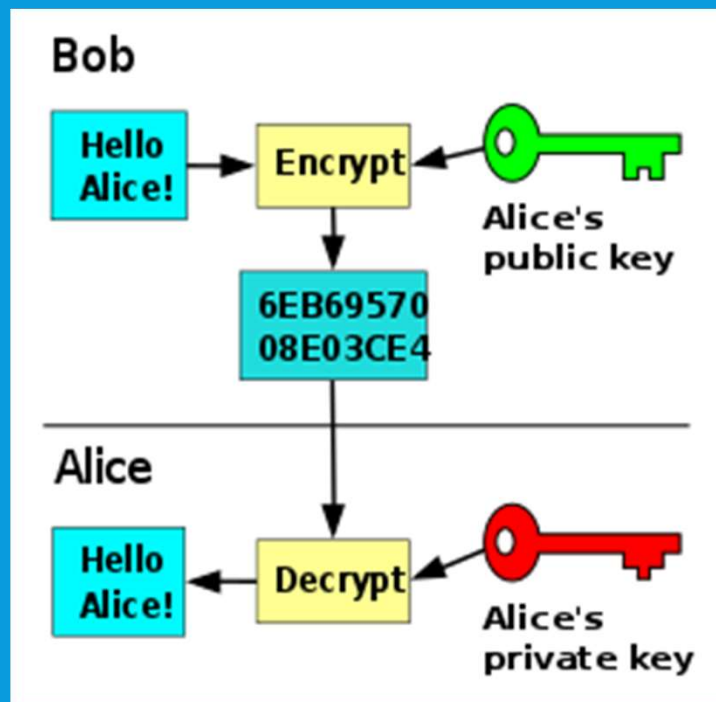
## EL MODELO OSI



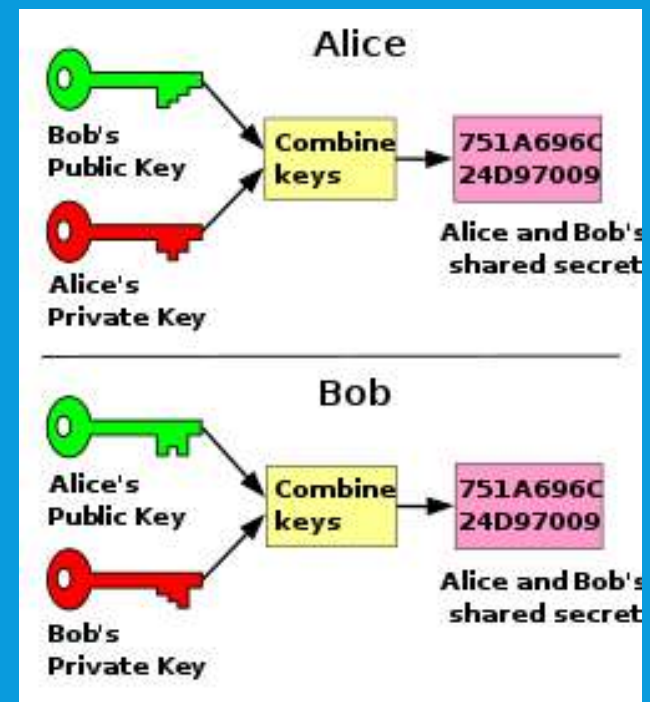
# HTTPS

- 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

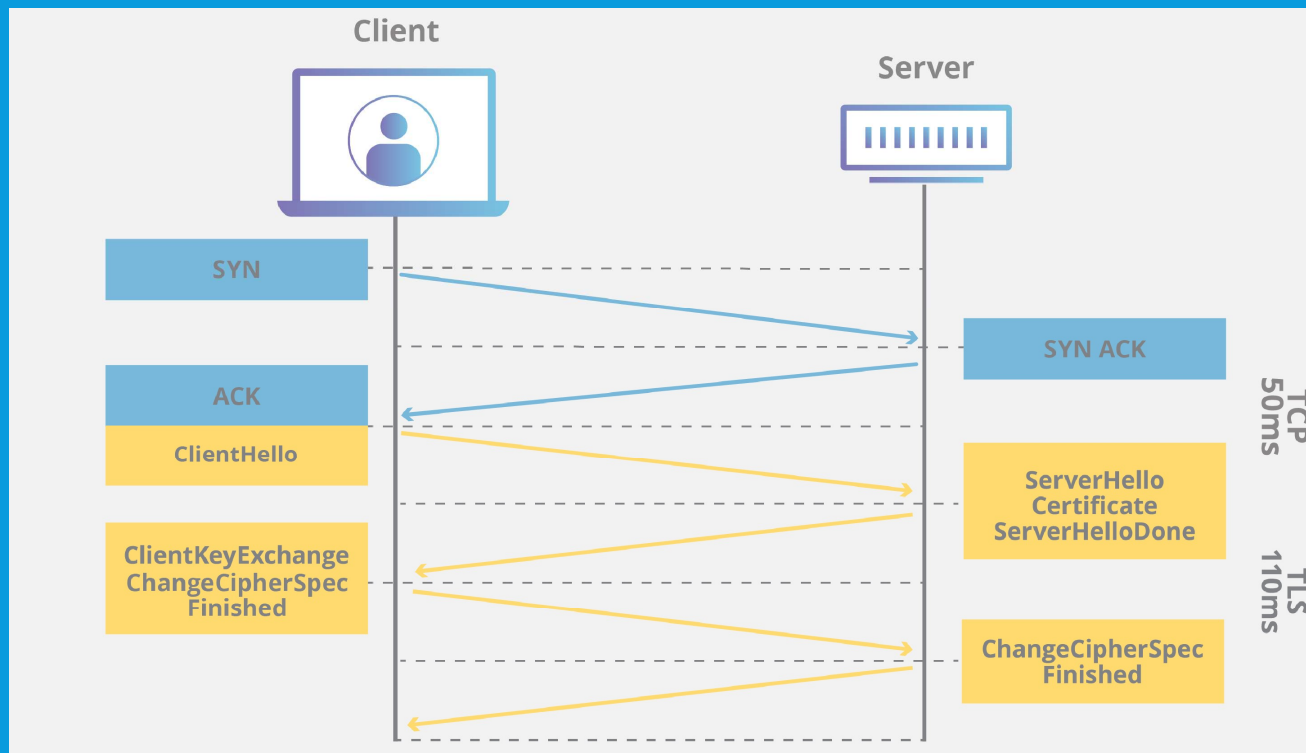


Modelo de Encriptación Simétrica

# 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 posible 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 TLS, 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)

**User Management**

- Roles
- Users
- Organizations
- Login Options

**Real-time Monitoring**

- System Monitor
- Active Calls
- Port Distribution

**System Maintenance**

- Audit Log Viewer
- Trace Viewer
- Log Viewer
- Alarm Manager

**System Management**

- EPM Manager
- MPP Manager
- Software Upgrade
- System Backup

**System Configuration**

- Applications
- MPP Servers**
- Speech Servers
- VoIP Connections
- Zones

**Security**

- Certificates
- Licensing

**Reports**

- Standard
- Custom
- Scheduled

**Multi-Media Configuration**

**VoiceXML Browser Properties**

Maximum Branches: 100000

**Cache**

Total Size: 40 MB

Low Water: 10 MB

Maximum Entry Size: 4 MB

Entry Expiration Time: 5 seconds

**Interpreter**

Maximum Documents: 500

Maximum Execution Context Stack Depth: 10

Maximum Loop Iterations: 1000

**INET**

Proxy Server:

Proxy Port: 8000

SSL Verify: ☐ Yes ☒ No

Connection Persistent: ☒ Yes ☐ No

**CCXML Browser Properties**

Fetch Timeout: 15 seconds

# AEP – SI EL SERVIDOR USA HTTPS

**User Management**

- Roles
- Users
- Organizations
- Login Options

**Real-time Monitoring**

- System Monitor
- Active Calls
- Port Distribution

**System Maintenance**

- Audit Log Viewer
- Trace Viewer
- Log Viewer
- Alarm Manager

**System Management**

- EPM Manager
- MPP Manager
- Software Upgrade
- System Backup

**System Configuration**

- Applications
- EPM Servers
- MPP Servers**
- SNMP
- Speech Servers
- VoIP Connections

### MPP Servers

This page displays the list of Media Processing Platform (MPP) servers in the Experience Portal system. When an MPP application server and communicates with ASR and TTS servers as necessary to process the call.

| Name                                 | Host Address | Network Address (VoIP) | Network Address (MRCP) | Network Address (AppSvr) | Maximum Simultaneous Calls |
|--------------------------------------|--------------|------------------------|------------------------|--------------------------|----------------------------|
| <input type="checkbox"/> alatompp001 | 10.26.1.227  | <Default>              | <Default>              | <Default>                | 10                         |

**Add** **Delete**

**MPP Settings** **Browser Settings** **Video Settings** **VoIP Settings** **Help**

### MPP Manager (May 19, 2020 12:08:56 PM PDT)

This page displays the current state of each MPP in the Experience Portal system. To enable the state selected MPPs must also be stopped.

Last Poll: May 19, 2020 12:08:39 PM PDT

| Server Name                          | Mode   | State   | Config | Auto Restart | Restart Schedule |           | Active Calls |     |
|--------------------------------------|--------|---------|--------|--------------|------------------|-----------|--------------|-----|
|                                      |        |         |        |              | Today            | Recurring | In           | Out |
| <input type="checkbox"/> alatompp001 | Online | Running | OK     | Yes          | No               | None      | 0            | 0   |

**State Commands**

**Start** **Stop** **Restart** **Reboot** **Halt** **Cancel**

**Mode Commands**

**Restart/Reboot Options**

- ☒ One server at a time
- ☐ All servers

**GRACIAS**