Protocolo de enlace de SSL estándar

A continuación, se muestra un protocolo de enlace de SSL estándar cuando se utiliza un algoritmo de intercambio de claves RSA:

**1. Hola cliente**

Información que el servidor necesita para comunicarse con el cliente mediante SSL. Incluye el número de versión de SSL, la configuración de cifrado y datos específicos de la sesión.

**2. Hola servidor**

Información que el servidor necesita para comunicarse con el cliente mediante SSL. Incluye el número de versión de SSL, la configuración de cifrado y datos específicos de la sesión.

**3. Autenticación y número secreto principal preliminar**

El cliente autentica el certificado de servidor, por ejemplo, nombre común / fecha / emisor. El cliente (según el cifrado) crea el número secreto principal preliminar de la sesión, cifra con la clave pública del servidor y envía el número secreto principal preliminar cifrado al servidor.

**4. Descifrado y número secreto principal**

El servidor utiliza su clave privada para descifrar el número secreto principal preliminar. El servidor y el cliente efectúan pasos para generar el número secreto principal con el cifrado acordado.

**5. Cifrado con clave de sesión**

El cliente y el servidor intercambian mensajes para informar de que se cifrarán futuros mensajes.

## Identidad de cliente o de usuario

Si hablamos de PKI o certificados de cliente, a muchas personas le vienen a la cabeza imágenes de empresas protegiendo y completando las transacciones online de sus clientes.

**Ejemplos:**

* Cuando iniciamos sesión en una VPN o cuando utilizamos una tarjeta bancaria en un cajero.
* Una tarjeta para acceder a un edificio.
* Una tarjeta inteligente para el transporte público.

“Estos *certificados digitales se encuentran en las gasolineras, los robots de cadenas de montaje de automóviles o, incluso, en los pasaportes.*

*Los gobiernos emiten documentos de identidad que tienen diferentes usos, por ejemplo, para pagar impuestos locales, facturas de electricidad y permisos de conducir.*

*Y la razón es fácil de entender: los certificados de cliente son muy importantes para la protección en Internet de las personas.*

*Como su nombre indica, se utilizan para identificar a un cliente o a un usuario autenticando el cliente en el servidor y estableciendo con exactitud su identidad.”*

**Los certificados de cliente y de servidor SSL desempeñan una función muy similar, pero los segundos se utilizan para identificar al cliente o al individuo, y los primeros autentican al propietario del sitio web.**