1.2.Seguridad.

1.2.1.Seguridad en las transacciones vía Internet

1.2.1.1.Protocolo SSL.

El protocolo SSL (*Secure Sockets Layer*) fue creado e implementado por la compañía *Nescape* para su navegador de Internet. Es así un sistema que funciona sobre *http* permitiendo que la conexión que se efectúa no sea captada de forma comprensible por terceros.

Sus páginas seguras aparece según la denominación *https* y la conexión se realizará a través del puerto 443.

El SSL realiza las funciones:

- Fragmentación. Se fragmentan los bloques mayores de 2^{14} en la emisión del mensaje, para luego volver a ser ensamblados en la recepción.

- Compresión. Se aplica un algoritmo a los mensajes que consigue su compactación

- Autenticación. Ésta se realiza mediante certificados electrónicos

durante la transmisión. Se crea un resumen del mensaje, que incluye una clave, que se denomina MAC.

- Integridad. Se asegura la no manipulación del contenido del mismo.

- Confidencialidad. Todos los mensajes se envían encriptados. Se utilizan certificados *X.509v3* para la transmisión de claves públicas.

El protocolo SSL se basa en dos capas complementarias llamados Protocolo *Handshake* y *Protocolo de Regis*tro.

- Protocolo *Handshake*. Realiza:

  - Autenticación de usuario y servidor.
  - Selección de los parámetros de la sesión y de la conexión.
  - Establecer la conexión segura.

- *Protocolo de Registro* (*Record Protocol*). Encripta los protocolos de las capas más altas *Handshake* y aplicaciones.

SSL funciona como una máquina de estados. Para cambiar el estado actual activo al pendiente (lectura y escritura v.g.) usa un subprotocolo del *Handshake* llamado *Change Cipher Spec*. Así un estado de la sesión incluye los elementos:

- Identificación de la sesión mediante un número elegido por el servidor.

- Certificado.

- Algoritmo de compresión.

- Algoritmo de encriptación. Especifica el algoritmo simétrico de encriptación para la confidencialidad y la función *Hash* de resumen para la integridad.

- Clave maestra. Un número secreto entre el servidor y el cliente.

- *Flag* de nuevas conexiones. Indica si desde esta sesión se pueden iniciar nuevas conexiones.

Un estado de conexión incluye los elementos:

- Números de inicio de la secuencia elegidos por el cliente y el servidor.

- Número secreto del cliente para el MAC.

- Número secreto del servidor para el MAC. Número secreto utilizado por el servidor para calcular los MACs de sus mensajes.

- Clave secreta del cliente. Clave utilizada por el cliente para encriptar sus mensajes.

- Clave secreta del servidor. Clave utilizada por el servidor para encriptar sus mensajes.

- Vectores iniciales (IV). Si se utiliza encriptación con modo CBC (*Cipher Block Chainning*) se necesita un vector inicial para cada clave.

- Número de secuencia. En cada mensaje, los números de secuencia son cambiados.

1.2.1.1.1.Protocolos de registro en SSL.

Utiliza los parámetros de la conexión negociados previamente en la capa *Handshake*.

- La fragmentación divide los mensajes mayores de 2^{14} bytes en bloques más pequeños.

- La compresión se realiza con el algoritmo negociado previamente en la fase inicial, puede ser el algoritmo *Null* si no se establece compresión.

- La autenticación e integridad se realiza calculando un resumen del mensaje concatenando con un número secreto y el resumen de la secuencia. El resultado de este resumen es el MAC y se añade al mensaje. La autenticación se puede comprobar con el número secreto, que sólo comparten el cliente y el servidor y mediante el número de secuencia. La integridad se realiza mediante la función *Hash.*

- La confidencialidad se consigue al encriptar mediante un algoritmo simétrico negociado en el *Hadshake.*

Las encriptaciones pueden ser de:

- Bloque. Se encriptan en bloques de 128 bits. Los algoritmos utilizados son RC2 y DES en forma CBC, para la forma CBC se utiliza un vector inicial(IV) previamente pactado.

- *Stream*. Se encripta realizando la OR-Exclusiva entre los bytes y un generador pseudoaleatorio, este generador es el algoritmo RC4.

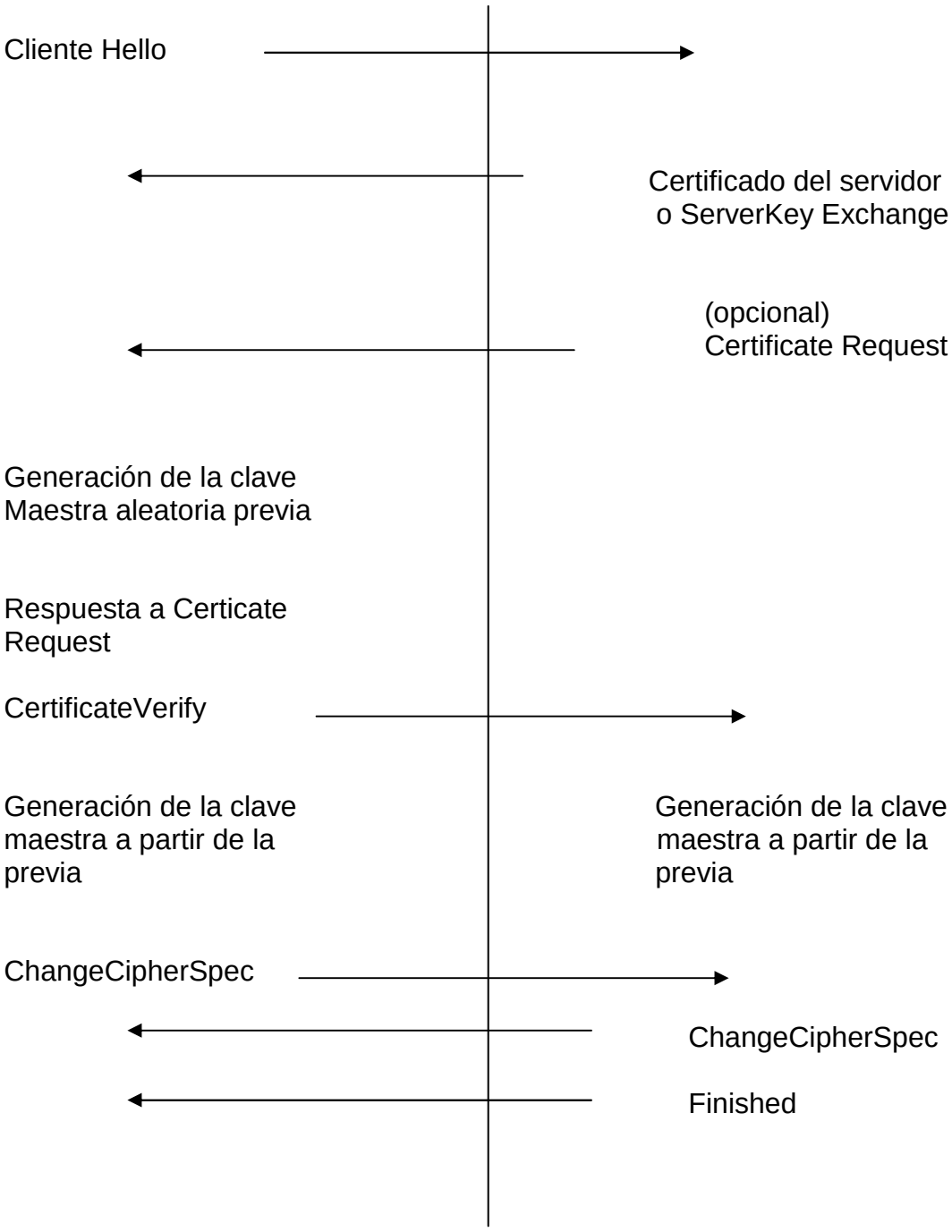
1.2.1.1.2.Protocolo Handshake en SSL.

Se encarga de establecer, mantener y finalizar la conexión SSL. Durante el *Handshake* se negocian los parámetros generales de la sesión y los particulares de la conexión. Hay dos protocolos:

- *Change Cipher Spec*. Es el que sirve para cambiar el estado activo en ese momento, al pendiente.

- Alerta. Son mensajes que avisan de problemas ocurridos durante la conexión.

Gráficamente, el proceso de comunicación inicial de SSL es:



Una breve explicación del proceso de comunicación anterior se muestra en el siguiente cuadro:

ClienteHello	Describe los parámetros hora y fecha, identificador de la sesión y los algoritmos de encriptación y de compresión.
ServerHello	Responde con el algoritmo elegido de que se han propuesto.
Certificado o *ServerKey Exchange*	Envía el certificado en el caso de que se posea o si no, la clave pública sin certificado.
CertificateVerify	Con este mensaje, el cliente manda su certificado.
ClienteKey Exchange	Se envía un número aleatorio que la utiliza para la clave maestra. Se envía encriptada con la clave pública del servidor.
ChangeCipherSpec	Inicia la sesión.
Finished	Termina la fase de *Handshake*. Sirve para comprobar que la negociación de parámetros y claves se realiza correctamente.