CERTIFICADOS DIGITALES

Certificado Digital

Un **certificado digital** o **certificado electrónico** es un documento firmado electrónicamente por un prestador de servicios de certificación que vincula unos datos de verificación de firma a un firmante y confirma su identidad.

Es un documento que permite al firmante identificarse en Internet. Es necesario para realizar trámites, tanto con las administraciones públicas como con numerosas entidades privadas

Según la Sede Electrónica del Instituto Nacional de Estadística, un certificado electrónico sirve para:

- Autentificar la identidad del usuario, de forma electrónica, ante terceros.
- Firmar electrónicamente de forma que se garantice la integridad de los datos trasmitidos y su procedencia. Un documento firmado no puede ser manipulado, ya que la firma está asociada matemáticamente tanto al documento como al firmante
- Cifrar datos para que sólo el destinatario del documento pueda acceder a su contenido.

En España, actualmente los certificados electrónicos emitidos por entidades públicas son el **DNIe** o DNI electrónico y el de la Fábrica Nacional de Moneda y Timbre (**FNMT**).

Autoridad de Certificación

Autoridad de certificación, **certificadora** o **certificante** (**AC** o **CA** ***Certification Authority***) es una entidad de confianza, responsable de emitir y revocar los certificados digitales, utilizados en la firma electrónica, para lo cual se emplea la criptografía de clave pública. Jurídicamente es un caso particular de Prestador de Servicios de Certificación.

La **Autoridad de Certificación**, por sí misma o mediante la intervención de una Autoridad de Registro, verifica la identidad del solicitante de un certificado antes de su expedición o, en caso de certificados expedidos con la condición de revocados, elimina la revocación de los certificados al comprobar dicha identidad. Los certificados son documentos que recogen ciertos datos de su titular y su clave pública y están firmados electrónicamente por la **Autoridad de Certificación** utilizando su clave privada. La **Autoridad de Certificación** es un tipo particular de Prestador de Servicios de Certificación que legitima ante los terceros que confían en sus certificados la relación entre la identidad de un usuario y su clave pública.

Un **certificado revocado** es un certificado que no es válido aunque se emplee dentro de su período de vigencia. Un certificado revocado tiene la condición de suspendido si su vigencia puede restablecerse en determinadas condiciones.

Modo de funcionamiento

Solicitud de un certificado

El mecanismo habitual de solicitud de un certificado de servidor web a una CA consiste en que la entidad solicitante, utilizando ciertas funciones del software de servidor web, completa ciertos datos identificativos (entre los que se incluye el localizador URL del servidor) y genera

una pareja de claves pública/privada. Con esa información el software de servidor compone un fichero que contiene una petición **CSR** (Certificate Signing Request) en formato PKCS#10 que contiene la clave pública y que se hace llegar a la **CA** elegida. Esta, tras verificar por sí o mediante los servicios de una **RA** (Registration Authority, Autoridad de Registro) la información de identificación aportada y la realización del pago, envía el certificado firmado al solicitante, que lo instala en el servidor web con la misma herramienta con la que generó la petición CSR.

En este contexto, **PKCS** corresponde a un conjunto de especificaciones que son estándares de facto denominadas Public-Key Cryptography Standards.

La Jerarquía de Certificación

Las CA disponen de sus propios certificados públicos, cuyas claves privadas asociadas son empleadas por las CA para firmar los certificados que emiten. Un certificado de **CA** puede estar auto-firmado cuando no hay ninguna CA de rango superior que lo firme. Este es el caso de los certificados de CA raíz, el elemento inicial de cualquier jerarquía de certificación. Una jerarquía de certificación consiste en una estructura jerárquica de **CA**s en la que se parte de una CA auto-firmada, y en cada nivel, existe una o más **CA**s que pueden firmar certificados de **entidad final** (titular de certificado: servidor web, persona, aplicación de software) o bien certificados de otras CA subordinadas plenamente identificadas y cuya Política de Certificación sea compatible con las **CA**s de rango superior.

Confianza en la CA

Una de las formas por las que se establece la confianza en una CA para un usuario consiste en la "instalación" en el ordenador del usuario (tercero que confía) del certificado autofirmado de la CA raíz de la jerarquía en la que se desea confiar. El proceso de instalación puede hacerse, en sistemas operativos de tipo Windows, haciendo doble click en el fichero que contiene el certificado (con la extensión "crt") e iniciando así el "asistente para la importación de certificados". Por regla general el proceso hay que repetirlo por cada uno de los navegadores que existan en el sistema, tales como Opera (navegador), Firefox o Internet Explorer, y en cada caso con sus funciones específicas de importación de certificados.

Si está instalada una CA en el repositorio de CAs de confianza de cada navegador, cualquier certificado firmado por dicha CA se podrá validar, ya que se dispone de la clave pública con la que verificar la firma que lleva el certificado. Cuando el modelo de CA incluye una jerarquía, es preciso establecer explícitamente la confianza en los certificados de todas las cadenas de certificación en las que se confíe. Para ello, se puede localizar sus certificados mediante distintos medios de publicación en internet, pero también es posible que un certificado contenga toda la cadena de certificación necesaria para ser instalado con confianza.

Normativa Europea

La **Directiva 93/1999** ha establecido un marco común aplicable a todos los países de la Unión Europea por el que el nivel de exigencia que supone la normativa firma electrónica implica que los Prestadores de Servicios de Certificación que emiten certificados cualificados son merecedores de confianza por cualquier tercero que confía y sus certificados otorgan a la firma electrónica avanzada a la que acompañan el mismo valor que tiene la "firma manuscrita" o "firma ológrafa".

Las CA también se encargan de la gestión de los certificados firmados. Esto incluye las tareas de revocación de certificados que puede instar el titular del certificado o cualquier tercero con interés legítimo ante la CA por correo electrónico, teléfono o intervención presencial. La lista denominada CRL (Certificate Revocation List) contiene los certificados que entran en esta categoría, por lo que es responsabilidad de la CA publicarla y actualizarla debidamente. Por otra parte, otra tarea que debe realizar una CA es la gestión asociada a la renovación de certificados por caducidad o revocación.

CA de personas y de servidores

Los certificados de "entidad final" a veces designan personas (y entonces se habla de "certificados cualificados") y a veces identifican servidores web (y entonces los certificados se emplean dentro del protocolo SSL para que las comunicaciones con el servidor se protejan con un cifrado robusto de 128 bits)

CAs públicas y privadas

Una CA puede ser o bien pública o bien privada. Las CAs públicas emiten los certificados para la población en general (aunque a veces están focalizadas hacia algún colectivo en concreto) y además firman CAs de otras organizaciones.

OCSP

Online Certificate Status Protocol (OCSP) es un método para determinar el estado de revocación de un certificado digital X.509 usando otros medios que no sean el uso de CRL (Listas de Revocación de Certificados). Este protocolo se describe en el RFC 2560 y está en el registro de estándares de Internet.

Firma Digital

Una **firma digital** es una firma electrónica con la adición de un certificado digital de autoridad expedido por un tercero que valida la identidad del firmante y la firma. La aplicación de una

firma digital incluye PKI (*Public Key Infrastructure*, infraestructura de clave pública) como tecnología de encriptación.

En el caso de las firmas digitales, el secreto del firmante es el **conocimiento exclusivo de una clave (secreta)** utilizada para generar la firma. Para garantizar la seguridad de las firmas digitales es necesario a su vez que estas sean:

- Únicas: Las firmas deben poder ser generadas solamente por el firmante y por lo tanto infalsificable. Por tanto la firma debe depender del firmante
- Infalsificables: Para falsificar una firma digital el atacante tiene que resolver problemas matemáticos de una complejidad muy elevada, es decir, las firmas han de ser computacionalmente seguras. Por tanto la firma debe depender del mensaje en sí.
- Verificables: Las firmas deben ser fácilmente verificables por los receptores de las mismas y, si ello es necesario, también por los jueces o autoridades competentes.
- Innegables: El firmante no debe ser capaz de negar su propia firma.
- Viables: Las firmas han de ser fáciles de generar por parte del firmante.

Firma Electrónica

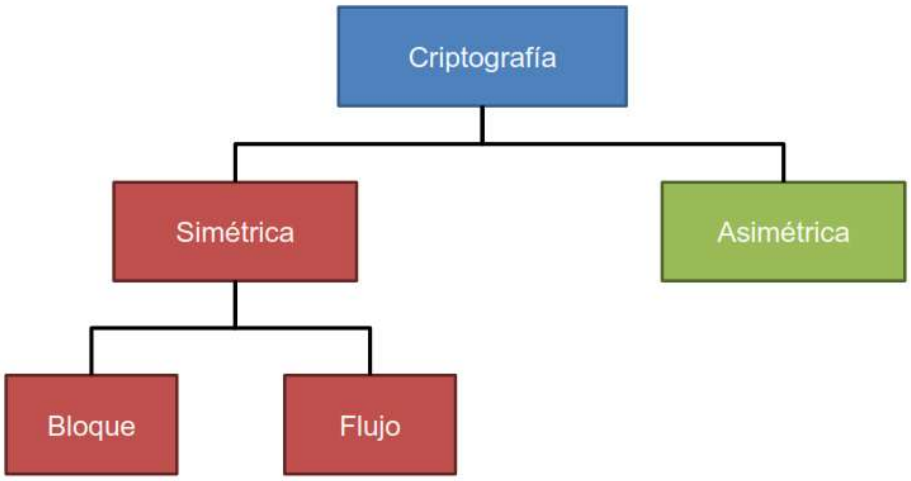
La **firma electrónica** es un concepto jurídico, equivalente electrónico al de la firma manuscrita, donde una persona acepta el contenido de un mensaje electrónico a través de cualquier medio electrónico válido. Ejemplos:

- Firma con un lápiz electrónico al usar una tarjeta de crédito o débito en una tienda.
- Marcando una casilla en un ordenador, a máquina o aplicada con el ratón o con el dedo en una pantalla táctil.
- Usando una firma digital.
- Usando usuario y contraseña.
- Usando una tarjeta de coordenadas.

Una firma electrónica crea un historial de auditoría que incluye la verificación de quién envía el documento firmado y un sello con la fecha y hora.

CRIPTOGRAFÍA

Los tipos de criptografía

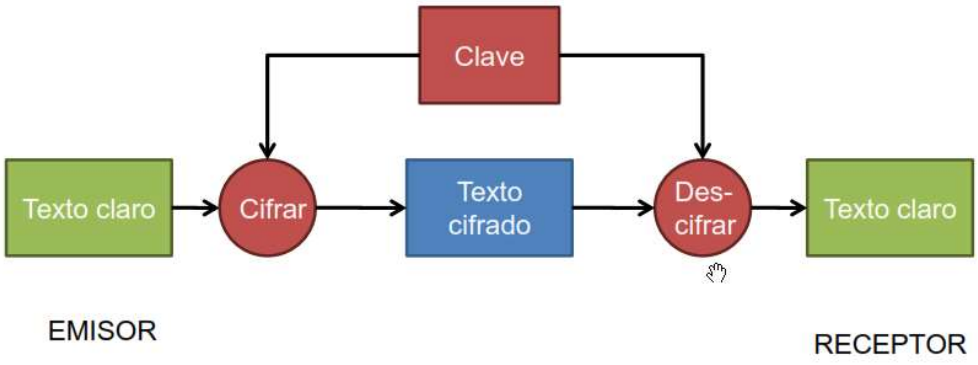


La **criptografía simétrica** (SKC *symmetric key cryptography*), también llamada **criptografía de clave secreta** (*secret key cryptography*) o criptografía de una clave (en inglés *single-key cryptography*), es un método criptográfico en el cual se usa una misma clave para cifrar y descifrar mensajes. Las dos partes que se comunican han de ponerse de acuerdo de antemano sobre la clave a usar. Una vez que ambas partes tienen acceso a esta clave, el remitente cifra un mensaje usando la clave, lo envía al destinatario, y éste lo descifra con la misma clave.

Un buen sistema de **cifrado** pone toda la seguridad en la clave y ninguna en el algoritmo.

Funcionamiento del cifrado simétrico

- Se utiliza la misma clave para cifrar y descifrar



Ataque de fuerza bruta (o búsqueda exhaustiva de claves)

- Un algoritmo está bien diseñado si la forma más simple de ataque es la búsqueda exhaustiva de claves.
- Los ataques de fuerza bruta o de búsqueda exhaustiva de claves consisten en probar una a una todas las posibles combinaciones de la clave.
- Para una clave de *n* bits, el número total de claves posibles (o el tamaño del espacio de claves) es igual a 2^n.
- En promedio, habrá que probar la mitad de claves hasta dar con la correcta.
- Hoy para que el ataque sea computacionalmente irrealizable se recomienda una longitud mínima de 128 bits de clave.

Algunos ejemplos de algoritmos simétricos son DES, 3DES, RC5, AES (**A**dvanced **E**ncryption **S**tandard), Blowfish e IDEA.

El algoritmo de cifrado **DES (D**ata **E**ncryption **S**tandard) usa una clave de 56 bits, lo que significa que hay 2 elevado a 56 claves posibles. Esto representa un número muy alto de claves, pero un ordenador genérico puede comprobar el conjunto posible de claves en cuestión de días. Una máquina especializada puede hacerlo en horas. Algoritmos de cifrado de diseño más reciente como **3DES**, **Blowfish** e **IDEA(I**nternational **D**ata **E**ncryption **A**lgorithm) usan claves de 128 bits, lo que significa que existen 2 elevado a 128 claves posibles. Esto equivale a muchísimas más claves.

Inconvenientes

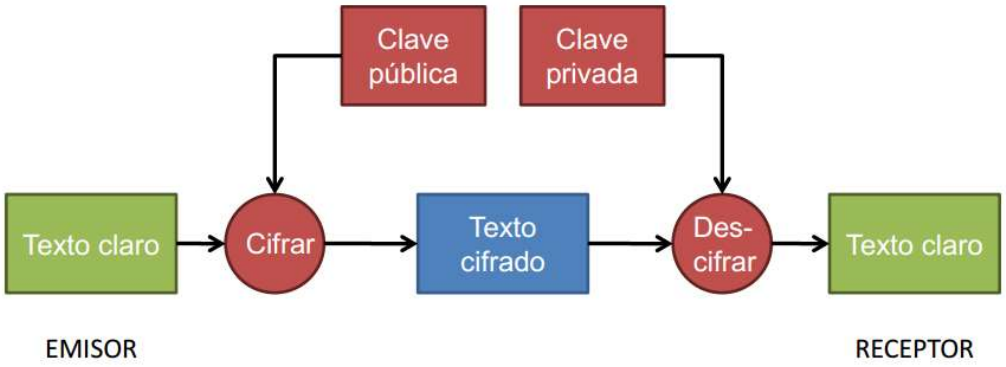
El principal problema con los sistemas de cifrado simétrico no está ligado a su seguridad, sino al intercambio de claves. Una vez que el remitente y el destinatario hayan intercambiado las claves pueden usarlas para comunicarse con seguridad, pero ¿qué canal de comunicación que sea seguro han usado para transmitirse las claves? Sería mucho más fácil para un atacante intentar interceptar una clave que probar las posibles combinaciones del espacio de claves.

Otro problema es el número de claves que se necesitan. Si tenemos un número **n** de personas que necesitan comunicarse entre sí, se necesitan **n/2** claves para cada pareja de personas que tengan que comunicarse de modo privado. Esto puede funcionar con un grupo reducido de personas, pero sería imposible llevarlo a cabo con grupos más grandes.

Para solucionar este problema existen la criptografía asimétrica y la criptografía híbrida.

Funcionamiento del cifrado asimétrico

- Se utilizan dos claves diferentes: una para cifrar y otra para descifrar



La **criptografía asimétrica** (A*symmetric Key Cryptography*), también llamada **criptografía de clave pública** (P*ublic Key Cryptography*) o **criptografía de dos claves** (T*wo-Key Cryptography*), es el método criptográfico que usa un par de claves para el envío de mensajes. Las dos claves pertenecen a la misma persona que ha enviado el mensaje. Una clave es *pública* y se puede entregar a cualquier persona, la otra clave es *privada* y el propietario debe guardarla de modo que nadie tenga acceso a ella. Además, los métodos criptográficos garantizan que esa pareja de claves sólo se puede generar una vez, de modo que se puede asumir que no es posible que dos personas hayan obtenido casualmente la misma pareja de claves.

Si el remitente usa la clave pública del destinatario para cifrar el mensaje, una vez cifrado, sólo la clave privada del destinatario podrá descifrar este mensaje, ya que es el único que la conoce. Por tanto se logra la *confidencialidad* del envío del mensaje, nadie salvo el destinatario puede descifrarlo.

Si el propietario del par de claves usa su clave privada para cifrar el mensaje, cualquiera puede descifrarlo utilizando su clave pública. En este caso se consigue por tanto la *identificación* y *autentificación* del remitente, ya que se sabe que sólo pudo haber sido él quien empleó su clave privada (salvo que alguien se la hubiese podido robar). Esta idea es el fundamento de la firma electrónica.

Los **sistemas de cifrado de clave pública** o **sistemas de cifrado asimétricos** se inventaron con el fin de evitar por completo el problema del intercambio de claves de los sistemas de cifrado simétricos. Con las claves públicas no es necesario que el remitente y el destinatario se pongan de acuerdo en la clave a emplear. Todo lo que se requiere es que, antes de iniciar la comunicación secreta, el remitente consiga una copia de la clave pública del destinatario. Es más, esa misma clave pública puede ser usada por cualquiera que desee comunicarse con su propietario. Por tanto, se necesitarán sólo **n** pares de claves por cada **n** personas que deseen comunicarse entre sí.

Características del cifrado asimétrico I

- La clave pública debe ser conocida por todo el mundo, pero la clave privada sólo debe conocerla su propietario
- A partir del conocimiento de la clave pública o del texto cifrado no se puede obtener la clave privada
- Lo que se cifra con una clave, sólo puede descifrarse con la otra

- Cualquiera puede cifrar un mensaje con la clave pública, pero sólo el propietario de la clave privada puede descifrarlo
  - Proporciona confidencialidad
- Si el propietario de la clave privada cifra con ella un mensaje, cualquiera puede descifrarlo con la correspondiente clave pública
  - Proporciona integridad, autenticación y no repudio

La mayor ventaja de la criptografía asimétrica es que la distribución de claves es más fácil y segura ya que la clave que se distribuye es la pública manteniéndose la privada para el uso exclusivo del propietario, pero este sistema tiene bastantes desventajas:

- Para una misma longitud de clave y mensaje se necesita **mayor tiempo de proceso**.
- Las claves deben ser de mayor tamaño que las simétricas.
- El mensaje cifrado ocupa más espacio que el original.

Herramientas como SSH (*) o la capa de seguridad SSL para la jerarquía de protocolos TCP/IP utilizan un híbrido formado por la criptografía asimétrica para intercambiar claves de criptografía simétrica, y la criptografía simétrica para la transmisión de la información.

SSH (**S**ecure **SH**ell, intérprete de órdenes segura) es el nombre de un protocolo y del programa que lo implementa, sirve para acceder a máquinas remotas a través de una red. Además de la conexión a otros dispositivos, SSH nos permite copiar datos de forma segura (tanto ficheros sueltos como simular sesiones FTP cifradas), gestionar claves RSA para no escribir claves al conectar a los dispositivos y pasar los datos de cualquier otra aplicación por un canal seguro tunelizado mediante SSH.

Secure Sockets Layer (***SSL***; en español «capa de conexión segura») y su sucesor ***Transport Layer Security*** (***TLS***; en español «seguridad de la capa de transporte») son protocolos criptográficos que proporcionan comunicaciones seguras por una red, comúnmente Internet.

Fundamento del cifrado asimétrico

- Usa funciones unidireccionales:
  - Su cálculo directo es viable, pero el cálculo de la función inversa tiene tal complejidad que resulta imposible
- Problemas matemáticos difíciles de resolver:
  - Factorización: descomponer un número grande en sus factores primos
  - Logaritmo discreto: obtener el exponente al que ha sido elevado una base para dar un resultado
  - Mochila tramposa: obtener los sumandos que han dado origen a una suma

Ejemplo RSA

- Clave pública:
  - $n = p \times q$, donde p y q son primos
  - e, primo con $(p-1)\times(q-1)$
- Clave privada:
  - d, tal que $d \times e \bmod (p-1)\times(q-1) = 1$
- Cifrar: $c = m^e \bmod n$
- Descifrar: $m = c^d \bmod n$

Algunos algoritmos y tecnologías de clave asimétrica son:

- Diffie-Hellman
- RSA *(Rivest, Shamir y Adleman)* es un sistema criptográfico de clave pública desarrollado en 1977. Es el primer y más utilizado algoritmo de este tipo y es válido tanto para cifrar como para firmar digitalmente.
- DSA
- ElGamal
- Criptografía de curva elíptica
- Merkle-Hellman

- Goldwasser-Micali
- Goldwasser-Micali-Rivest

Protocolos

Algunos protocolos que usan los algoritmos antes citados son:

- DSS ("Digital Signature Standard") con el algoritmo DSA ("Digital Signature Algorithm")
- PGP
- GPG, una implementación de OpenPGP
- SSH
- SSL, ahora un estándar del IETF
- TLS

Comparación entre criptografía simétrica y asimétrica

Atributo	Clave simétrica	Clave asimétrica
Años en uso	Miles	Menos de 50
Uso principal	Cifrado de grandes volúmenes de datos	Intercambio de claves; firma digital
Estándar actual	DES, Triple DES, AES	RSA, Diffie-Hellman, DSA
Velocidad	Rápida	Lenta
Claves	Compartidas entre emisor y receptor	Privada: sólo conocida por una persona Pública: conocida por todos
Intercambio de claves	Difícil de intercambiar por un canal inseguro	La clave pública se comparte por cualquier canal La privada nunca se comparte
Longitud de claves	56 bits (vulnerable) 256 bits (seguro)	1024 – 2048 (RSA) 172 (curvas elípticas)
Servicios de seguridad	Confidencialidad Integridad Autenticación	Confidencialidad Integridad Autenticación, No repudio

SSL/TLS

SSL (Secure Sockets Layer)

- La empresa Netscape Communication crea en la década de los 90 el protocolo estándar SSL, un procedimiento para proporcionar comunicaciones seguras en una red.

- Es un protocolo criptográfico que proporciona confidencialidad, autenticidad e integridad en una comunicación cliente/servidor.

¿Cómo establecer una comunicación segura con SSL?

- SSL Handshake protocol

  Facilita la negociación de parámetros de seguridad para facilitar la confidencialidad, integridad y autenticidad en una comunicación entre cliente y servidor.

- SSL Record protocol

  Especifica la forma de encapsular los datos transmitidos y recibidos, incluidos los de negociación.

Ejemplo negociación básica autenticación servidor. SSL handshake protocol (I)

1. El cliente envía un mensaje "ClientHello" especificando la versión más alta del protocolo TLS soportada, un número aleatorio y una lista de algoritmos de autenticación, cifrado y MAC (Message Authentication Code), así como algoritmos de compresión.

2. El servidor responde con un mensaje "ServerHello", indicando la versión del protocolo seleccionado (la más alta que soporten cliente y servidor), un número aleatorio, los algoritmos que selecciona de los enviados por el cliente y su certificado digital (mediante un mensaje Certificate) para autenticarle.

SSL handshake protocol (II)

3. El cliente verifica el certificado del servidor, típicamente mediante una autoridad de confianza o PKI. A continuación el cliente responde con un mensaje ***ClientKeyExchange***, el cual contiene una *PreMasterSecret (un número secreto)*, con información para generar la clave de sesión. Si se utiliza el algoritmo RSA este mensaje irá cifrado con la clave pública del servidor y este número aleatorio generado por el cliente será de 48 bytes.

4. El cliente y el servidor usan los números aleatorios intercambiados y la PreMasterSecret (el servidor necesita utilizar su clave privada para recuperarla). Con estos datos calculan un secreto común, denominado "master secret". Todas las subclaves de la conexión serán derivadas de ésta mediante la función pseudoaleatoria establecida.

5. El cliente ahora envía un registro **ChangeCipherSpec** e indica al servidor que a partir de ese momento toda la información intercambiada será autenticada y, si así lo estableció el servidor, cifrada.

6. Finalmente el cliente envía un mensaje **Finished** firmado y cifrado, conteniendo un hash y MAC de los mensajes negociados anteriormente.

7. El servidor intentará descifrar el mensaje Finished enviado por el cliente y verifica el hash y el MAC. Si el descifrado o la verificación falla, la conexión no tiene lugar.

8. Si todo va bien, el servidor envía un ChangeCipherSpec indicando al cliente que a partir de ese momento todo lo que le envíe estará firmado y, si fue negociado, también cifrado. El servidor envía su mensaje Finished firmado y cifrado, validándolo el cliente, conteniendo un hash y MAC de los mensajes negociados anteriormente.

9. Finaliza la fase de negociación, pudiendo intercambiar mensajes cliente y servidor autenticados y cifrados (si así fue establecido).

Aplicaciones del protocolo TLS/SSL

TLS: Mejora SSL en la protección frente a nuevos ataques (nuevos algoritmos criptográficos, evita downgrade, etc.).

USOS:

- Comercio electrónico y banca online
- Securizar redes privadas virtuales (OpenVPN)
- Autenticación y cifrado de datos VoIP

Seguridad del protocolo TLS/SSL

- La versión más moderna del protocolo TLS con las extensiones recomendadas, puede considerarse segura frente a los ataques conocidos.
- Los ataques que vulneran su seguridad se centran especialmente en engañar al usuario con la dirección a la que se conecta o con el certificado digital que autentifica al servidor.