Sociedad Andaluza para el Desarrollo de las Telecomunicaciones
CONSEJERÍA DE EMPLEO, EMPRESA Y COMERCIO

seguridad+ Y CONFIANZA DIGITAL | AndalucíaCERT CENTRO DE SEGURIDAD TIC

Informe de divulgación
Seguridad básica de SSL

Tipo de documento:	*Informe*
Autor del documento:	*AndalucíaCERT*
Código del Documento:	*CERT-IF-8802-150914*
Edición:	*0*
Categoría	*Público*
Fecha de elaboración:	*14/09/2015*
N° de Páginas	*1 de 14*

1 TABLA DE CONTENIDOS

TABLA DE CONTENIDOS 2
OBJETIVO Y ALCANCE 3
ALCANCE 3
SSL 3
VERSIONES 4
AUTORIDAD DE CERTIFICACIÓN 4
PROCESO "*HANDSHAKE*" 5
DIFERENTES TIPOS DE CERTIFICADOS SSL 8
ATAQUES CONTRA EL PROTOCOLO SSL/TLS 9
VULNERABILIDADES 11
APLICACIONES QUE UTILIZAN SSL/TLS 11
CERTIFICADOS DE LA FNMT 12
  Administración pública 12
  Persona física 13
CONCLUSIONES 14
REFERENCIAS 14

2 OBJETIVO Y ALCANCE

Éste documento tiene el objetivo de ofrecer una presentación de la seguridad y funcionamiento del protocolo SSL. También se verán varias aplicaciones de los certificados SSL y su correcto uso, junto con los detalles de cómo puede probar los certificados SSL en su servidor Web.

3 ALCANCE

Este documento va dirigido tanto al personal de la Junta de Andalucía, como al público en general. Pretende aportar las nociones necesarias para entender y tener conocimiento sobre el funcionamiento del protocolo, la seguridad de certificados SSL, lugar y forma de obtenerlos y sus distintas aplicaciones.

4 SSL

Secure Socket Layer (SSL) es un protocolo diseñado para permitir que las aplicaciones puedan transmitir información de forma segura a través de internet. Fue desarrollado por Netscape a principios de los 90 y pronto se convirtió en el método más utilizado para dichos traspasos de información.

SSL es una parte integral de la mayoría de los navegadores y servidores web y hace uso del sistema de codificación con dos claves: una pública y una privada, desarrollado por RSA. Para establecer una conexión SSL, se requiere que el servidor tenga instalado un *Certificado Digital*. Un certificado digital es un archivo electrónico que identifica de modo único a individuos o servidores, funcionando como una credencial digital que autentica al servidor antes de establecer la sesión SSL. Por lo general, los certificados digitales están firmados por un tercero independiente y fiable que garantiza su validez. Este tercero que firma un certificado se denomina Autoridad de Certificación (CA) que se verá con más profundidad en el punto 6 de este informe.

SSL proporciona comunicaciones seguras mediante la combinación de dos elementos:

- Autenticación

  El certificado digital va unido a un dominio específico y una CA realiza una cantidad de verificaciones para confirmar la identidad de la organización que solicita el certificado antes de emitirlo. De este modo, el certificado solo puede instalarse en el dominio contra el cual ha sido autenticado, ofreciendo a los usuarios la seguridad que necesitan.

- Cifrado

  El cifrado es el proceso de transformar la información para hacerla incomprensible para todos salvo para el receptor al que va dirigida. Esto constituye la base de la *Integridad* y privacidad de los datos, necesarias para la transmisión de información en internet.

5 VERSIONES

La primera versión del protocolo SSL ampliamente difundida fue la 2.0. Poco después Netscape publicó la versión 3.0, con muchos cambios respecto a la anterior.

La especificación TLS (*Transport Layer Security*) fue elaborada por la IETF. La versión 1.0 del protocolo TLS está publicada en el documento RFC 2246. Es prácticamente equivalente a SSL 3.0 con algunas diferencias, por lo que se podría considerar el TLS 1.0 como el protocolo SSL 3.1. Tanto esta versión TLS como las SSL comentadas anteriormente están desaconsejadas ya que son vulnerables a distintos ataques o tienen reconocidas algunas vulnerabilidades.

Tras TLS 1.0 han surgido otras dos versiones más TLS 1.1 y TLS 1.2 las cuales se están utilizando en la actualidad. Ya existe también un borrador de TLS 1.3, se puede encontrar más información acerca de esta versión del protocolo en el siguiente enlace: https://tlswg.github.io/tls13-spec/

6 AUTORIDAD DE CERTIFICACIÓN

La Autoridad de Certificación (AC o CA, por sus siglas en inglés, Certification Authority) es una entidad de confianza cuyo objeto es garantizar la identidad de los titulares de certificados y su correcta asociación a las claves de firma electrónica, para lo cual administra una Infraestructura de Clave Pública (PKI). En la actualidad, las Autoridades de Certificación se someten a leyes y reglamentos que plantean serios retos operativos, además de normas y estándares que les hacen asumir importantes responsabilidades.

En España existen distintas Autoridades de Certificación, la primera fue ANF y quedó oficialmente acreditada en 2000, pero tras ésta otras aparecieron. En el siguiente enlace puede verse una lista de las principales Autoridades de Certificación españolas que emiten certificados electrónicos de empresa:

- *http://firmaelectronica.gob.es/Home/Empresas/Autoridades-Certificacion.html*

Entre las funciones y responsabilidades de estas autoridades destacan las siguientes:

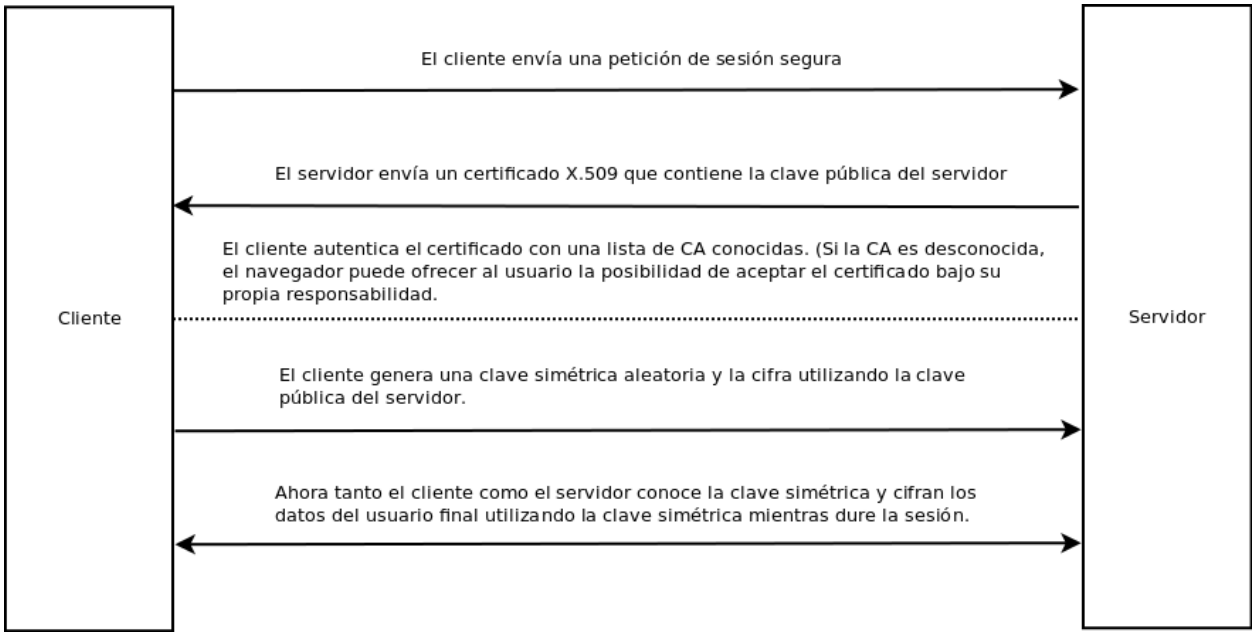
- Emitir y revocar certificados digitales.

- Mantener copia de todos los certificados emitidos, consignando su fecha de emisión, y de las correspondientes solicitudes de emisión.
- Mantener un listado actualizado de los certificados que se han emitido y la lista de certificados revocados.
- Administrar y mantener los servicios de firmas y certificados digitales.

7 PROCESO "*HANDSHAKE*"

Como ya se ha dicho anteriormente tanto SSL como TLS son protocolos usados para cifrar la información entre dos puntos, normalmente entre cliente y servidor. Para que esta negociación sea posible, el administrador del sistema debe preparar un mínimo de dos ficheros: la '*clave privada* ' y el '*Certificado* '.

Una vez que dichos ficheros están preparado y correctamente instalados, comienza la negociación SSL/TLS que se detalla a continuación.



1. El cliente envía el mensaje "*hello* " listando las posibilidades criptográficas que puede usar (ordenadas por orden de preferencia), como la versión SSL, grupos de programas de cifrado soportados y métodos de compresión de datos soportados por el cliente. Además viaja un número aleatorio.

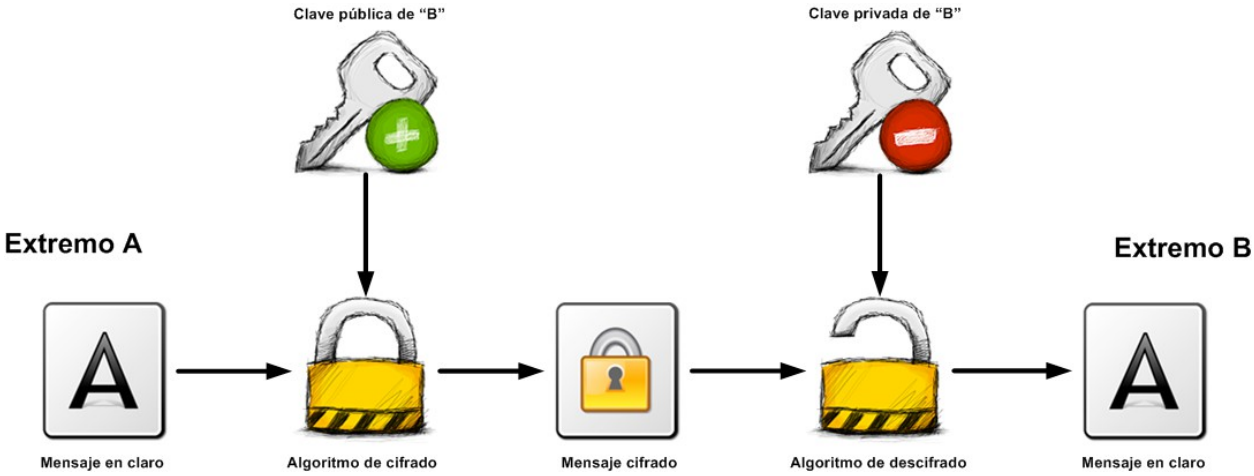
2. El servidor responde con el mensaje "*hello* " que contiene el método criptográfico y método de compresión seleccionados por el servidor, el ID de la sesión y otro número aleatorio. Es importante que el cliente y el servidor den soporte como mínimo a un conjunto de protocolos de cifrado comunes; de lo contrario, el protocolo de enlace dará un error. Generalmente, el servidor elige del conjunto de programas de cifrado comunes, el más potente (para más seguridad).
3. El servidor envía su Certificado Digital. Si el servidor utiliza SSLv3 y si la aplicación del servidor requiere un certificado digital para la autenticación de cliente, el servidor también le enviará el mensaje "*digital certificate request* ". En este mensaje, el servidor envía una lista de los tipos de certificados digitales soportados y los nombres distinguidos de autoridades de certificación aceptables.
4. El servidor envía el mensaje "*hello done* " de servidor y aguarda una respuesta del cliente.
5. Al recibir el mensaje "*hello done* " del servidor, el navegador web del cliente verifica la validez del certificado digital del servidor y comprueba si los parámetros del mensaje "*hello"* son aceptables. En el caso de que el servidor haya solicitado un certificado digital del cliente, éste le envía su certificado digital en el caso de que lo tenga o la alerta "*no digital certificate*" en caso contrario.
6. El cliente envía el mensaje "*client key exchange* ". Este mensaje contiene un secreto "pre-maestro", que consiste en un número aleatorio de 46 bytes utilizado en la generación de las claves de cifrado simétrico y las claves de *código de autenticación de mensajes* (MAC), cifradas con la clave pública del servidor.

   En el caso de que el cliente haya enviado un certificado digital al servidor, el cliente envía un mensaje "*digital certificate verify"* firmado con la clave privada del cliente. Al verificar la firma de este mensaje, el servidor puede verificar explícitamente la propiedad del certificado digital del cliente.

   No sería necesario este mismo procedimiento por parte del servidor, ya que si el servidor no tiene la clave privada que pertenece al certificado digital, no podrá descifrar el secreto pre-maestro y crear las claves correctas para el algoritmo de cifrado simétrico, y por tanto el protocolo dará error.
7. El cliente utiliza una serie de operaciones criptográficas para convertir el secreto *pre-maestro* en un secreto *maestro*, del que se deriva todo el material de clave necesario para el cifrado y la autenticación de mensajes. A continuación el cliente envía el mensaje "*change cipher spec* " para que el servidor conmute al conjunto de protocolos de cifrado que se habían negociado. El siguiente mensaje enviado por parte del cliente ("*finished* ") ya va cifrado con el protocolo pactado y esas claves de cifrado.
8. El servidor responde con mensajes propios "*change cipher spec* " y "*finished* ".

9. El protocolo de enlace SSL finaliza y ya se puede mantener una comunicación cifrada entre cliente y servidor.

En los anteriores pasos se ha nombrado los conceptos de *clave pública* y *clave privada*. A continuación se muestra el funcionamiento de las mismas y qué puede hacer cada una de ellas. Este concepto es lo que se conoce como *Criptografía asimétrica* o *Criptografía de clave pública*, donde las claves son distintas. En este escenario cada persona dispone de sus dos claves, una pública que puede distribuir libremente y una privada que deberá guardarla y evitar que otra persona tenga acceso a ella. Su característica fundamental y en la que se basa su funcionamiento es que cada una puede descifrar lo que ha cifrado la otra.



Por tanto, si utilizamos la imagen superior como referencia, si el Extremo A necesita enviar información que solo B pueda leer, deberá cifrarla con la clave pública de B. Dicha información viajará cifrada y como solo B dispone de su clave privada, nadie más podrá acceder a dicha información. De esta forma se garantiza la *Confidencialidad* de esta información.

También pueden utilizarse para conseguir la *Integridad* de la información. Si el usuario B necesita responder a A, y además de cifrar la información para que solo A la pueda leer, quiere garantizarle a A que dicha información no ha sido modificada por nadie más debería de hacer los siguientes dos pasos:

1. Cifrar el mensaje con la clave pública de A, de la misma forma que antes se hizo al revés. Así solo A podrá descifrar el mensaje con su clave privada.
2. Cifrar el mensaje con la clave privada de B (lo que se conoce como Firmar un mensaje). De esta forma cualquier persona puede descifrar este paso, pero este no es el objetivo ya que aun descifrándolo la información seguirá cifrada gracias al paso anterior. Entonces, ¿Para que sirve este último paso?, si B cifra con su clave privada, *solo* y *únicamente* su clave pública podrá descifrarlo, por lo que cuando el mensaje le llegue a A, si utilizando la clave pública de B para descifrarlo da algún error, significará que el mensaje ha sido alterado en el camino. En caso de

que se descifre bien tiene garantía de que ese mensaje fue el que envió el otro usuario y nadie lo ha modificado (Integridad). Una vez hecho este paso, ya podrá descifrarlo con su clave privada para acceder a la información que B le ha enviado.

Aplicando estos conceptos al Handshake explicado anteriormente, se utiliza este procedimiento para el paso de una clave que sí será *Simétrica*, pero haciéndolo de esta forma nadie ajeno al cliente y servidor conocerá esta clave con la que ambos cifrarán toda la información intercambiada.

El ENS (Esquema Nacional de Seguridad) determina los requisitos criptográficos exigidos a las administraciones públicas. En la guía "807 Criptografía de empleo en el Esquema Nacional de Seguridad" se identifican los algoritmos criptológicos acreditados, determinando la fortaleza criptológica mínima necesaria para cada dimensión de la seguridad y acorde con el nivel de criticidad del activo que interviene.

8 DIFERENTES TIPOS DE CERTIFICADOS SSL

En la actualidad, existe en el mercado una cantidad de certificados SSL diferentes:

- El primer tipo de certificado SSL es un certificado autofirmado. Como su propio nombre indica se trata de un certificado generado con fines internos y no es emitido por una autoridad de certificación. Dado que el propietario del sitio web genera su propio certificado, este no tiene el mismo peso que un certificado SSL completamente autenticado y verificado, emitido por una autoridad de certificación.
- Un certificado de dominio validado se considera un certificado SSL básico y se puede emitir rápidamente. La única comprobación de verificación que se realiza es para garantizar que el solicitante es dueño del dominio (dirección del sitio web) donde se piensa usar el certificado. No se realizan comprobaciones adicionales para garantizar que el propietario del dominio es una entidad comercial válida.
- Un certificado SSL totalmente autenticado es el primer paso para generar confianza y seguridad online verdaderas. Estos certificados tardan ligeramente más en emitirse y solo se otorgan una vez que la organización aprueba una determinada cantidad de procedimientos de validación y comprobaciones a fin de confirmar la existencia de la empresa, la propiedad del dominio y la autoridad del usuario para solicitar el certificado.

Otras consideraciones que se tiene con respecto a los certificados son las siguientes.

- Si bien un certificado SSL puede admitir cifrado de 128 bits o 256 bits, ciertos navegadores y sistemas operativos anteriores todavía no se pueden conectar en este nivel de seguridad. Los certificados SSL con una tecnología denominada "criptografía canalizada en el servidor" (SGC)

posibilitan el cifrado de 128 bits o 256 bits a más del 99,9% de visitantes de sitios web. Sin un certificado SGC en el servidor web, los navegadores y los sistemas operativos que no admitan el sólido cifrado de 128 bits solamente recibirán cifrado de 40 bits o de 56 bits. Los usuarios con ciertos navegadores y sistemas operativos anteriores se actualizarán temporalmente a un cifrado SSL de 128 bits si visitan un sitio web con un certificado SSL habilitado para SGC.

- Con frecuencia, se usa un nombre de dominio con una cantidad de sufijos de host diferentes. Por esta razón, puede emplear un certificado comodín que le permita proporcionar seguridad SSL completa a cualquier host de su dominio, por ejemplo, host.su_dominio.com (donde "host" varía, pero el nombre de dominio se mantiene igual).
- Similar al certificado comodín, pero un poco más versátil, el certificado SSL de SAN (nombre alternativo de sujeto) permite que se agregue más de un dominio a un solo certificado SSL.
- Los certificados de firma de código están especialmente diseñados para garantizar que el software descargado no fue manipulado mientras se transmitía. Hay muchos cibercriminales que manipulan el software disponible en Internet. Pueden adjuntar un virus u otro software malicioso a un paquete inocuo mientras este se descarga. Estos certificados aseguran que esto no suceda.
- Con frecuencia, los certificados SSL Extended Validation (EV) ofrecen el estándar de autenticación más alto del sector y proporcionan el mejor nivel de confianza disponible para el cliente. Cuando se visita un sitio web protegido con un certificado SSL EV, la barra de direcciones aparece de color verde (en los navegadores de alta seguridad) y se muestra un campo especial con el nombre del propietario legítimo del sitio web junto con el nombre del proveedor de seguridad que emitió el certificado SSL EV. En la barra de direcciones, también se muestra el nombre del titular del certificado y de la autoridad de certificación que lo emite. Esta prueba visual de certeza ha ayudado a incrementar la confianza del consumidor en el comercio electrónico.

9 ATAQUES CONTRA EL PROTOCOLO SSL/TLS

Tanto los protocolos SSL como TLS están diseñados para resistir los siguientes ataques:

- **Lectura de los paquetes enviados por el cliente y servidor.**

  Cuando los datos se envían cifrados, un atacante que tuviera acceso a los paquetes, por ejemplo utilizando técnicas de *sniffing* (escuchando el tráfico de red), se enfrenta al problema de romper el cifrado si quiere acceder a la información contenida en esos paquetes.

  Las claves que se utilizan para el cifrado se intercambian con métodos de clave pública y privada explicados en el Punto 7 de este informe, por lo que el atacante tendría que romper este procedimiento para conocer que clave se ha acordado para cifrar la comunicación.

  Si la comunicación es totalmente anónima, es decir, sin autenticación de servidor ni cliente, sí que existe la posibilidad de capturar las claves secretas con un ataque conocido como "*man in the*

middle ". En este caso, el atacante genera sus propias claves públicas y privadas, y cuando una parte envía a la otra información sobre su clave pública, tanto en un sentido como en el otro, el atacante la intercepta y la sustituye por la equivalente clave fraudulenta. Dado que el intercambio es anónimo, y no existe ninguna autoridad certificadora que valide que tanto servidor como cliente son quienes dicen ser, ambos no tienen manera de saber si la clave pública que recibe es la del emisor auténtico o no.

- **Suplantación de servidor o cliente.**

  Cuando se realiza la autenticación de servidor o cliente, el certificado digital debidamente firmado por la CA sirve para verificar la identidad del propietario. Un atacante que quiera hacerse pasar por el servidor (o cliente) auténtico debería obtener su clave privada, o bien la de la autoridad de certificación que ha emitido el certificado para poder generar otro con una clave pública diferente y que aparezca auténtico.

- **Alteración de los paquetes.**

  Un atacante puede modificar los paquetes para que no lleguen al destinatario con un contenido distinto del original (si están cifrados no podrá controlar cual será el contenido final descifrado, solamente se sabrá que será distinto al original). Si pasa esto, el receptor detectará que el paquete ha sido alterado porque el código de autenticación (MAC) será incorrecto.

  Si la alteración se realiza en los mensajes de negociación cuando aun no se aplica ningún código MAC, con la finalidad de forzar la adopción de algoritmos criptográficos más débiles y vulnerables, esta manipulación será detectada en la verificación de los mensajes *Finished*.

- **Repetición, eliminación o reordenación de paquetes.**

  Si el atacante vuelve a enviar un paquete correcto que ya había sido enviado antes, o suprime algún paquete haciendo que no llegue a su destino, o los cambia de orden, el receptor lo detectará porque los códigos MAC no coincidirán con el valor esperado. Esto es así porque en el cálculo del MAC se utiliza un número de secuencia que se va incrementando con cada paquete.

  Tampoco se pueden copiar los mensajes enviados en un sentido (de cliente a servidor o viceversa) al sentido contrario, porque en los dos flujos de la comunicación se utilizan claves de cifrado y MAC diferentes.

  Como consideración final, cabe destacar que la fortaleza de los protocolos seguros recae no solamente en su diseño si no en el de las implementaciones. Si una implementación solamente soporta algoritmos criptográficos débiles (con pocos bits de clave), o genera números pseudoaleatorios fácilmente predecibles, o guarda los valores secretos en almacenamiento (memoria o disco) accesibles por atacantes, etc. no estará garantizado la seguridad del protocolo.

10 VULNERABILIDADES

A continuación se listan las principales vulnerabilidades detectadas para SSL. La puntuación CVSS de estas vulnerabilidades es:

Vulnerabilidad	CVE	Impacto	Explotación	Base
Early CCS	CVE-2014-0224	6,4	8,6	**6,8**
OprahSSL	CVE-2015-1793	4,9	10	**6,4**
Heartbleed	CVE-2014-0160	2,9	10	**5**
LOGJAM	CVE-2015-4000	2,9	8,6	**4,3**
POODLE	CVE-2014-3566	2,9	8,6	**4,3**
FREAK	CVE-2015-0204	2,9	8,6	**4,3**
BEAST	CVE-2011-3389	2,9	8,6	**4,3**
BREACH	CVE-2013-3587	2,6	2,3	**3,2**
TLS-POODLE	CVE-2014-8730	2,9	8,6	**2,9**
Lucky13	CVE-2013-0169	2,9	4,9	**2,6**
CRIME	CVE-2012-4929	2,9	4,9	**2,6**

11 APLICACIONES QUE UTILIZAN SSL/TLS

Los protocolos SSL/TLS han sido diseñados para permitir la protección de cualquier aplicación basada en un protocolo de transporte como TCP. Algunas aplicaciones que utilizan esta característica son:

- **HTTPS** (HTTP sobre SSL/TLS): el protocolo más utilizado actualmente para la navegación web segura.
- **NNTPS** (NNTP sobre SSL): para el acceso seguro a la lectura y publicación de artículos de noticias en *Usenet* .

El funcionamiento de estas aplicaciones con SSL/TLS es el mismo que las originales, la única diferencia reside en el uso de la capa de transporte seguro que proporciona SSL/TLS y la asignación de puertos TCP propios: 443 para HTTPS y 563 para NNTPS.

Existen otros muchos casos, pero se aprovechan de extensiones previstas en el propio protocolo de la aplicación para negociar el uso de SSL/TLS, a fin de evitar la utilización innecesaria de nuevos puertos TCP. Entre estas aplicaciones se incluyen algunas como:

- **TELNET**, usando la opción de autenticación (RFC 1416).
- **FTP**, usando las extensiones de seguridad (RFC 2228).
- **SMTP**, usando sus extensiones para SSL/TLS (RFC 2487).
- **POP3 y IMAP**, también usando comandos específicos para SSL/TLS (RFC 2595).

También existe un mecanismo para negociar el uso de SSL/TLS en HTTP (RFC 2817) como alternativa a HTTPS.

12 CERTIFICADOS DE LA FNMT

A modo de ejemplo, se va a explicar qué tipos de certificados suministra la Fábrica Nacional de Moneda y Timbre (FNMT), enlaces con información de cada uno de ellos, pasos para la obtención de uno y algunas recomendaciones con respecto a la seguridad que necesitan.

La FNMT presta servicio como Autoridad Certificadora y pone a disposición de los usuarios diferentes tipo de certificados electrónicos mediante los cuales, un organismo, persona, etc podrá identificarse y realizar trámites de forma segura a través de internet.

En función del destinatario del certificado, la FNMT emite los siguientes tipos de certificados que se podrán solicitar a través de la SEDE electrónica:

- Persona física. https://www.sede.fnmt.gob.es/certificados/persona-fisica
- Persona Jurídica. https://www.sede.fnmt.gob.es/certificados/persona-juridica
- Entidad sin Personalidad Jurídica. https://www.sede.fnmt.gob.es/certificados/entidad-sin-personalidad-juridica
- Administración Pública. https://www.sede.fnmt.gob.es/certificados/administracion-publica
- Certificados de Componente. https://www.sede.fnmt.gob.es/certificados/certificado-componentes

12.1 ADMINISTRACIÓN PÚBLICA

La FNMT-RCM presta servicios de certificación electrónica para la Junta de Andalucía, también disponibles para las entidades de la Administración Local, las Diputaciones Provinciales, Universidades Públicas, la Cámara de Cuentas de Andalucía....

Los principales servicios son los siguientes:

- Acceso a la infraestructura de validación de certificados electrónicos emitidos por la FNMT-RCM.

- Constitución y gestión de oficinas de registro para certificados electrónicos de persona física.
- Emisión de certificados electrónicos de componente. La cobertura del número de estos certificados para un municipio es igual a la suma del número de certificados de sede electrónica y de sello electrónico que le corresponda.
- Emisión de certificados electrónicos para las Administraciones Públicas derivados de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.
- Sellado de tiempo.

Para más información acerca de este servicio se puede consultar el siguiente enlace:
https://ws024.juntadeandalucia.es/ae/adminelec/areatecnica/fnmt

12.2 PERSONA FÍSICA

En cambio, para la obtención de certificados de persona física es necesario seguir estos tres pasos:

- **Paso 1. Solicitar el certificado.** Tras completar la solicitud indicando el NIF se recibirá un código que deberá guardarse.
- **Paso 2. Acreditar tu identidad en una Oficina de Registro.** Con el código obtenido tras el proceso de solicitud y una forma de identificación adecuada (por ejemplo el DNI), deberá personarse en una de las Oficinas de Registro aprobadas.
- **Paso 3. Descargar tu certificado de usuario.** Disponible en línea tras acreditarse en la Oficina de Registro elegida. Se necesitará el código obtenido en el primer paso.

Es recomendable hacer una copia en un soporte extraíble (CD, memoria USB, DVD de datos) de la clave privada que se obtendrá tras descargar el certificado. Este archivo quedará protegido por una contraseña. También se debe recordar que el certificado digital y el DNI electrónico son diferentes. Sin embargo con el DNI electrónico y un lector de tarjetas se puede obtener el certificado sin necesidad de acudir a una Oficina de Registro.

Uno de los primeros pasos que se debe tomar es importar el Certificado Raíz de la FNMT. Este certificado será necesario para comprobar la autenticidad de cualquier Certificado emitido por dicha Autoridad de Certificación, y en particular en este caso los Certificados Raíz de la FNMT.

Servirán al usuario que los incorpore a su navegador para asegurarse que su Certificado de usuario está expedido por la FNMT, y también servirán a los servidores web que lo incorporen para comprobar que el Certificado que le presenta un usuario está firmado por la FNMT y así poder confiar en él.

13 CONCLUSIONES

En este documento se ha realizado una visión global del uso de SSL y TLS. Ambos aprovechan el uso de clave simétrica y el algoritmo de clave pública y privada para conseguir crear una sesión cifrada entre cliente y servidor. De esta forma se asegura la integridad de la información y autenticidad de la misma, apoyándose en autoridades certificadoras que afianzan que cada uno es quien dice ser.

El mayor ataque que se le puede realizar a este método es la colocación de un atacante en medio de la comunicación antes del intercambio de claves, encargándose él de repartir claves y cifrar hacia ambos sentidos, estando al tanto de toda la conversación y por tato de la información que en ella se transmite. Para evitar este tipo de ataques, con que exista una autoridad certificadora en la que tanto cliente y servidor confíen, y se siga bien el procedimiento de intercambio de claves no debería existir peligro alguno.

Para la obtención de dichos certificados SSL existen distintas autoridades certificadoras. En este documento se ha tratado la FNMT que con una serie de documentos que autentiquen de forma inequívoca a una persona física o jurídica, organismo público, empresa... generan un certificado que asegura que dicho ente es quien dice ser y, por tanto, aporta esa confianza en ambas partes.

14 REFERENCIAS

- *https://tools.ietf.org/html/rfc6101*
- *https://tools.ietf.org/html/rfc5246*
- *https://www.openssl.org/docs/*
- *http://www.tldp.org/HOWTO/SSL-Certificates-HOWTO/x64.html*
- *https://documentation.cpanel.net/pages/viewpage.action?pageId=1507527*
- *http://www.anf.es/es/certificacion/pki-anf-ac/autoridad-de-certificacion.html*
- *https://es.wikipedia.org/wiki/Autoridad_de_certificaci%C3%B3n*
- *http://www.symantec.com/connect/blogs/how-does-ssl-work-what-ssl-handshake*
- *http://www.criptored.upm.es/intypedia/docs/es/video9/DiapositivasIntypedia009.pdf*
- *http://www.fnmt.es/home*
- *https://community.qualys.com/blogs/securitylabs/2014/10/15/ssl-3-is-dead-killed-by-the-poodle-attack*
- *https://freakattack.com/*
- *https://web.nvd.nist.gov/view/vuln/search*