Preguntas frecuentes Certificados SSL

1. ¿Qué es un certificado digital de servidor o SSL?

Es el principal protocolo de seguridad en Internet. Se trata de una credencial electrónica que permite identificar a una entidad (persona, dispositivo...)

SSL son las siglas de " Secure Sockets Layer ", un protocolo desarrollado por Netscape en 1996 para transmitir información confidencial vía Internet.

2. ¿Qué características de seguridad nos proporciona un SSL?

Mediante la instalación de un certificado SSL en un servidor WEB se activan las siguientes características de seguridad:

- Cifrado de datos: los datos que se intercambien entre el navegador del usuario y el servidor serán cifrados. En caso de que estos datos fueran interceptados en su tránsito por la red serían directamente inteligibles.

- Autenticación del servidor: se busca verificar la identidad de las partes. El visitante de una página web podrá saber que el propietario de una web ha seguido un proceso de identificación ante una autoridad de certificación competente.

- Integridad: la información intercambiada está protegida de ser vista o alterada por terceros.

- No repudio: se evita la negación de una transacción válida.

3. ¿Por qué es tan importante hoy en día disponer de un certificado digital?

Es de sobra conocido que la mayor traba a la expansión del comercio electrónico a través de Internet es la sensación de inseguridad que experimentan los consumidores y usuarios a la hora de transmitir datos confidenciales, en especial los números de sus cuentas bancarias o tarjetas de crédito.

Los exigentes procedimientos de verificación y autenticación a la hora de emitir certificados digitales le garantizan la identidad real de la persona con la que mantenga una relación comercial en la Web. De este modo, se fomenta la confianza entre empresas y clientes de Internet.

4. ¿Quién puede solicitar un certificado digital de servidor?

Cualquier particular o empresa que posea una web y quiera garantizar la confidencialidad e integridad de todas las comunicaciones que a través de ella se realicen.

5. ¿Cómo sabrán los visitantes de mi web que están conectando a un servidor web con certificado digital?

Por convención las URLs que requieren de una conexión SSL comienzan por https en vez de http.

Además, en la esquina inferior derecha de la URL aparecerá el símbolo de un candado cerrado (Secured Seal), y pulsando sobre él se muestran los datos del certificado digital de servidor.

El sello VeriSign Secured Seal, disponible en 13 idiomas, es la marca de seguridad más conocida de Internet y puede aumentar la confianza que los visitantes tienen en su página Web.

6. ¿Qué certificados digitales ofrece Interdomain?

Interdomain le ofrece certificados digitales de 40 bits o de 128 bits . Estos certificados son emitidos por Verisign y gestionados a través de la Agencia Española de Certificación (ACE), afiliado de Verisign en España.

Verising es la autoridad de certificación líder a nivel mundial en la emisión de certificados digitales.

7. ¿Qué diferencia hay entre un certificado de 40 bits o de 128 bits?

Cuando hablamos de cifrado nos estamos refiriendo a la clave utilizada para el cifrado simétrico utilizado para la protección de datos mediante SSL.

El cifrado de alto nivel, a 128 bits, puede calcular 288 más combinaciones que un cifrado de 40 bits. Por lo tanto, es más de un billón de billones de veces más potente.

8. ¿Qué tipo de clientes trabajan con los certificados digitales?

Los certificados SSL de VeriSign son compatibles con prácticamente todos los navegadores actuales.

9. ¿Qué es un CSR?

Se trata de una cadena de texto generada por el software de su servidor cuyo objeto es identificar al servidor y a la organización solicitante del SSL.

El CSR se genera en el servidor que aloja el WEB y constituye el primer paso necesario para que pueda asegurar su servidor con Certificados SSL.

Para crear un CSR debe conocer el tipo de software de servidor que se está ejecutando en su servidor web para poder seleccionar las instrucciones adecuadas.

Siga estas indicaciones en el momento de generar el CSR:

- No utilice caracteres especiales (! @ # $ % ^ * ( ) ~ ? > < & / \) en ninguno de los campos de la solicitud del CSR.
- En el campo Nombre común (Common name) deberá ingresar el nombre de dominio (FQDN - Fully Qualified Domain Name) con o sin el www (tudominio.com o www.tudominio.com).

10. ¿Puedo utilizar un certificado digital para un servidor múltiple?

En el caso de que posea varios servidores (o servidores virtuales) que alberguen dominios diferentes necesitará adquirir un certificado digital para cada uno de los dominios.

Si hay múltiples servidores alojando un solo dominio, puede asegurar hasta un máximo de 5 servidores con un solo certificado.

En el caso de que utilice distintos tipos de software servidor, también necesitará solicitar certificados diferentes para cada paquete de software.

11. Si mi organización tiene varias compañías, ¿cuántos certificados necesito?

Cada servidor físico que usted quiera certificar necesitará al menos un certificado. Si es usted un Proveedor de Internet (ISP) o tiene albergados en su servidor sitios web de varias empresas u entidades, necesitará un certificado por cada organización.

Cada certificado requerirá una autenticación propia y el abono de su precio.

12. ¿Cuales son los pasos que debo seguir para solicitar mi certificado digital?

Los pasos a seguir son:

- Paso 1: *Generación del CSR.*
- Paso 2: *Inscripción*. Debe rellenar el formulario de inscripción que puede descargarse en nuestra web www.interdomain.es
- Paso 3: Debe remitirnos el CSR junto con el formulario de inscripción para iniciar el proceso de solicitud.

- Paso 4: Autenticación. La autoridad certificadora realizará la validación correspondiente. VeriSign debe comprobar la existencia de su empresa, la propiedad del nombre de dominio y la situación de empleo de la persona solicitante del certificado.
- Paso 5: Emisión e Instalación. En un par de días dispondrá de su certificado digital y podrá proceder a su instalación.
  Podrá instalarlo en su servidor web, en su servidor de correo, sitios de comercio electrónico y sitios FTP; es decir, en cualquier lugar en el que los clientes, empleados u otros usuarios proporcionen información confidencial o inicien sesión en una cuenta.

13. ¿Cuándo debo renovar mi certificado?

Los certificados pueden renovarse dentro de un plazo de 90 días antes de su caducidad. Para garantizar un servicio ininterrumpido le aconsejamos que realice la renovación al menos 30 días antes de la fecha de caducidad. No perderá el periodo de validez restante del certificado existente realizando la renovación antes de plazo.

14. ¿Dispongo de garantía?

Dispone de un período de 30 días para la revocación y sustitución gratuita de su certificado.