



GUÍA CORPORATIVA

CÓMO AUMENTAR LA CONFIANZA
PARA PROTEGER E IMPULSAR
SU NEGOCIO EN INTERNET
Autenticación y cifrado
Las bases de la seguridad en línea





CONTENIDO

+ Resumen principal	4
+ Descripción general	4
+ ¿Porqué es necesario contar con certificados SSL autenticados?	5
Cifrado	5
Autenticación	5
Certificados digitales	5
+ Funcionamiento de los certificados SSL autenticados	6
+ Riesgo de los certificados SSL sin autenticar	7
Situación 1: La autoridad de certificación no ha autenticado la empresa	8
Situación 2: La autoridad de certificación no ha comprobado la existencia de la empresa	8
+ Cómo saber si un sitio web es auténtico	9
+ Proceso de autenticación de VeriSign	10
Paso 1	10
Paso 2	10
Paso 3	10
Paso 4	10

(Continúa)





GUÍA CORPORATIVA



CONTENIDO

+ Razones por las que el método de autenticación de VeriSign es más seguro	10
+ Beneficios para su empresa	11
Atracción de clientes	11
Autenticación	11
Privacidad de los mensajes	11
Integridad de los mensajes	11
+ Conclusión	12
+ Información adicional	12



Where it all comes together.™

Resumen principal

A la luz de los riesgos asociados al comercio electrónico y la comunicación en línea, es importante no sólo utilizar tecnología de cifrado seguro cuando se realizan negocios en Internet, sino también probar la propia identidad y desarrollar relaciones de confianza con socios y clientes.

Para poder establecer estas relaciones en línea, es necesaria la autenticación de una tercera parte de confianza, así como recibir un certificado SSL (Secure Sockets Layer) firmado por esa tercera parte. El cifrado es el proceso de transformación de la información que la hace ininteligible para todos excepto para el destinatario original y sienta la base para la integridad de datos y la privacidad imprescindibles para el comercio electrónico. Sin embargo, sin la autenticación, la tecnología de cifrado no es suficiente para proteger a los usuarios de estos servicios electrónicos. Es necesario utilizar la autenticación junto con el cifrado para proporcionar:

- Confirmación de que la empresa nombrada en el certificado tiene derecho a utilizar el nombre de dominio que se incluye en el certificado.
- Confirmación de que la empresa nombrada en el certificado es una entidad legal.
- Confirmación de que la persona que solicitó el certificado SSL en nombre de la organización había sido autorizada a hacerlo.

Algunas autoridades de certificación (Certificate Authorities, CA) creen que el cifrado basta por sí mismo para garantizar la seguridad de un sitio web y promover la confianza de los clientes en dicho sitio. Pero de hecho, hay una diferencia entre certificados autenticados (“alta seguridad”), que nos dan confianza y seguridad, y los certificados no autenticados (“baja seguridad”), que socavan la confianza del cliente y vulneran la seguridad en la red. Además de utilizar la tecnología de cifrado, es de vital importancia que el sitio web esté autenticado, lo que aumentará la confianza de los internautas que visiten su sitio web y su negocio.

Si protege su sitio web con VeriSign®, podrá beneficiarse de una gran variedad de opciones para mejorar aún más sus operaciones de comercio electrónico. Con el sello Secured™ Seal de VeriSign, que se incluye con todos los servicios Secure Site, podrá utilizar la marca de seguridad número uno en Internet para dar a sus clientes la confianza necesaria para comunicarse y realizar transacciones comerciales en su sitio. Con el sello, los visitantes de su sitio podrán además comprobar la información de su certificado SSL y el estado del mismo en tiempo real, lo que contribuye a aumentar la confianza en su negocio en línea y por lo tanto a incrementar las ventas e ingresos.



Los servicios de seguridad Secure Site de VeriSign ofrecen los medios para asegurar y activar el comercio electrónico de su sitio web, lo que proporciona al cliente la tranquilidad de que sus operaciones en la Web son seguras. El aumento de la confianza en las transacciones realizadas en línea aporta muchos beneficios. Entre los más importantes están el aumento de los ingresos y la rentabilidad. El comercio electrónico nos presenta auténticos desafíos (e importantes oportunidades) para poder proporcionar el mismo nivel de confianza y personalización en Internet que los que ofrecen los comercios físicos.

Descripción general

Hasta muy recientemente, la mayoría de los certificados SSL podían clasificarse como certificados de seguridad media a alta que proporcionaban los siguientes tres servicios de seguridad: confidencialidad, autenticación e integridad. Los certificados digitales sólo identifican a sitios web e individuos y permiten comunicaciones seguras y confidenciales. Por desgracia, algunos proveedores de certificados SSL han preferido proporcionar certificados SSL de baja seguridad, para así poder disminuir los costes y acelerar el proceso de solicitud. Esto entra en conflicto con los métodos generalmente aceptados por el sector, socava la confianza del cliente y crea confusión entre los visitantes de los sitios web.

Los certificados SSL de “baja seguridad” proporcionan confidencialidad e integridad, pero no autenticación. En el pasado, el icono de candado que aparecía en el navegador del usuario se consideraba un signo fiable de autenticación. Ahora, los usuarios se ven obligados a examinar el propio certificado SSL para poder distinguir entre certificados autenticados de alta seguridad y certificados sin autenticar de baja seguridad.

Por ejemplo, si un usuario intenta comunicarse de forma segura con un sitio web que cuente con un certificado SSL con el nombre comercial de “ABC Inc.”, dicho usuario deberá comprobar si el certificado está autenticado por una tercera parte. El certificado SSL intenta transmitir la confianza de que el sitio web que se está visitando (como www.abc-incorporated.com) es definitivamente un sitio de “ABC Inc.” y no cualquier otra entidad que simula serlo para engañar a los visitantes del sitio web y obtener beneficios a su costa. Una autenticación rigurosa es la única prueba que una empresa puede presentar a clientes y socios para probar que el sitio web es auténtico y tiene derecho a utilizar el nombre de dominio que aparece en el certificado.

¿Por qué es necesario contar con certificados SSL autenticados?

Las nociones de identidad y autenticación son conceptos fundamentales en cualquier mercado. Los individuos y las instituciones deben conocerse mejor y tener confianza en el otro antes de poder realizar negocios. En el comercio tradicional, la gente se basaba en los documentos físicos (como una licencia comercial o una carta de crédito) para probar su identidad y asegurar a la otra parte su capacidad para realizar una transacción.

En la edad del comercio electrónico, los certificados SSL autenticados proporcionan la indispensable identidad y seguridad en línea que ayuda a establecer una relación de confianza entre las partes involucradas en transacciones electrónicas en redes digitales. Independientemente de si el negocio se realiza en el mundo digital o el físico, las partes involucradas deben poder responder a las siguientes preguntas:

- ¿Quién eres? (Requisito de identidad).
- ¿A qué comunidad perteneces? ¿Eres un miembro de confianza? (Respaldo de una asociación).
- ¿Cómo puedes probar tu identidad? (Validación de la identidad).

Los clientes deben tener la certeza de que el sitio web con el que se están comunicando es auténtico y de que la información que envíen mediante su navegador web seguirá siendo privada y confidencial.

+ Cifrado

Internet presenta una gama única de problemas relativos a la seguridad, problemas que los negocios deben superar desde el principio para minimizar riesgos. Los clientes envían información y adquieren productos o servicios a través de Internet sólo si se sienten seguros de que la información personal, como los números de sus tarjetas de crédito o sus datos financieros, está segura. La solución para los negocios que se toman el comercio electrónico en serio es implementar una infraestructura segura basada en tecnologías de cifrado. El cifrado es el proceso de transformación de la información que la hace ininteligible para todos excepto para el destinatario original y sienta la bases para la integridad de datos y la privacidad que son imprescindibles para el comercio electrónico.

+ Autenticación

Algunas autoridades de certificación creen que el cifrado basta por sí mismo para garantizar la seguridad de un sitio web y promover la confianza de los clientes en dicho sitio. Sin

embargo, el cifrado no es suficiente, siendo necesario que el sitio web también esté autenticado, lo que mejorará la confianza que los internautas tienen en el sitio web que visitan. Estar autenticado significa que una entidad de confianza puede probar que eres quien dices ser. Para probar que su negocio es auténtico, su sitio web debe estar asegurado por métodos de autenticación y una tecnología de cifrado de la mejor calidad.

+ Certificados digitales

Un certificado digital es un archivo electrónico que identifica de forma exclusiva a individuos y sitios web en Internet y permite establecer comunicaciones confidenciales y seguras. Los certificados digitales funcionan como una forma de credencial o pasaporte digital.

Por lo general el “signatario” de un certificado digital es una autoridad de certificación como, por ejemplo, VeriSign. Algunas autoridades de certificación de confianza autentican sus certificados digitales pero, por desgracia, también hay otras que proporcionan certificados SSL sin autenticar. Este hábito expone a los usuarios de Internet al riesgo de que haya negocios fraudulentos operando en la red. Como proveedor líder de servicios de confianza, VeriSign proporciona certificados SSL autenticados que aseguran una relación de confianza entre usted y sus clientes.

Los certificados SSL autenticados permiten al visitante del sitio web:

- Comunicarse de forma segura con el sitio web, de manera que la información suministrada por el visitante no pueda ser interceptada durante la transmisión (confidencialidad) ni alterada sin que nadie lo detecte (integridad).
- Comprobar que el sitio que el usuario está visitando realmente pertenece a la compañía, y que no ha sido suplantada (autenticación).

VeriSign garantiza esta confianza reforzando su servicio de autenticación con tecnologías de cifrado de vanguardia en sus soluciones de certificados digitales. Su empresa de comercio electrónico solo recibirá un certificado SSL de VeriSign autenticado una vez que:

- Se compruebe la identidad y se confirme que la organización es una entidad legal.
- Se confirme que tiene derecho a utilizar el nombre de dominio que se incluye en el certificado.
- Se compruebe que la persona que solicitó el certificado SSL en nombre de la organización había sido autorizada a hacerlo.

Funcionamiento de los certificados SSL autenticados

Los certificados SSL autenticados permiten al destinatario de un mensaje digital estar seguro tanto de la identidad del emisor como de la integridad del mensaje. Hay tres pasos básicos de autenticación y verificación que son fundamentales para que una empresa reciba certificados SSL de alta seguridad para su sitio web:

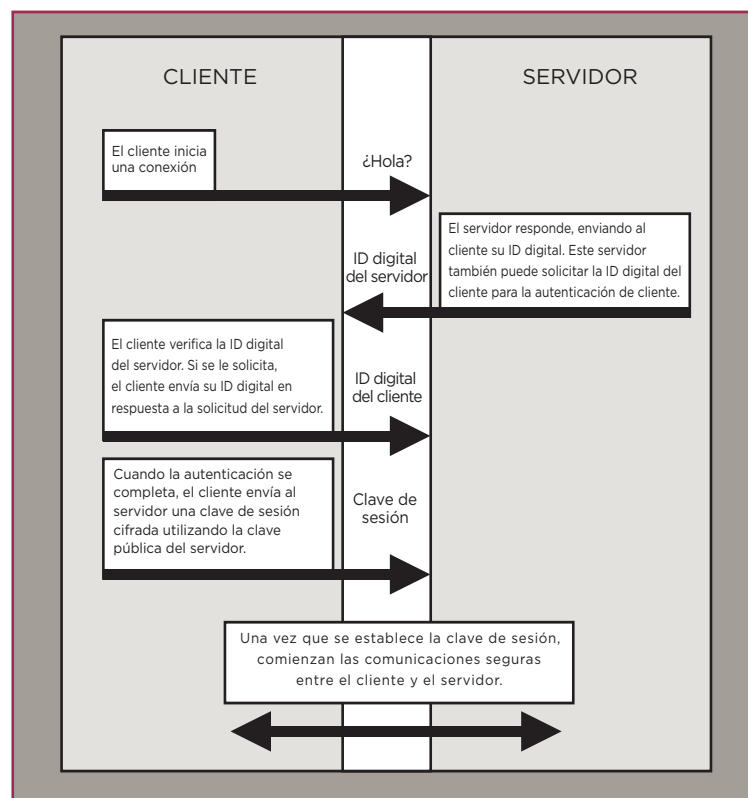
- Confirmación de que la empresa nombrada en el certificado tiene derecho a utilizar el nombre de dominio que se incluye en el certificado.
- Confirmación de que la empresa nombrada en el certificado es una entidad legal.
- Confirmación de que la persona que solicitó el certificado SSL en nombre de la organización había sido autorizada a hacerlo.

Cuando los visitantes se conecten a los sitios web, se encontrarán uno de los dos tipos de servidores. Si encuentran servidores seguros,

recibirán mensajes informándoles de ello. De igual forma, si encuentran servidores no seguros, recibirán advertencias a tal efecto. Un servidor web realmente seguro es aquél que cuenta con un certificado SSL seguro. El certificado autenticado asegura a los usuarios que una tercera parte independiente y de confianza ha comprobado que el servidor pertenece a la compañía a la que dice pertenecer. Un certificado autenticado válido asegura a los usuarios que la información confidencial que están enviando llega al lugar al que lo envían.

Un administrador web crea una solicitud de certificado, que a su vez crea dos claves cifradas: una privada y otra pública. El servidor web envía la clave pública a una autoridad de certificación, como VeriSign. Por ello, dichas autoridades de certificación deben entonces asegurarse de que están emitiendo los certificados a la compañía correcta. Las autoridades de certificación deben comprobar:

- Que la empresa que están certificando es la propietaria del nombre de dominio de Internet que han certificado.
- Que está registrada como empresa en uno o más países.
- Que el nombre registrado es igual al del certificado que la autoridad de certificación está firmando.
- Que la persona que solicita el certificado trabaja en dicha empresa.



Una vez que se han realizado las debidas comprobaciones y verificaciones, la autoridad de certificación firma la clave pública. La clave pública vuelve al servidor web, que la carga en el servidor. El SSL empezará a funcionar en cuanto la clave privada y la pública se emparejen perfectamente. El protocolo SSL asegura que la información que envía un servidor es idéntica a la que recibe un visitante web, sin que se haya producido ninguna modificación.

Riesgos de los certificados SSL sin autenticar

En la actualidad los navegadores no distinguen entre certificados SSL de alta seguridad (autenticados) y los de baja seguridad (sin autenticar). Generalmente, el usuario confía automáticamente en el certificado SSL cuando la autoridad de certificación lo emite y el nombre del dominio del certificado coincide con el dominio del sitio web visitado.

El icono de candado del navegador del usuario aparecerá indistintamente, tanto si el sitio en particular está utilizando un certificado SSL de alta seguridad autenticado como sin autenticar.



Hasta hace muy poco tiempo, este sencillo método había funcionado adecuadamente, y ha facilitado la expansión del comercio electrónico. Sin embargo, los últimos cambios en el mercado de los certificados SSL suponen una amenaza potencial para la confianza del cliente, y un riesgo para la seguridad de las transacciones en línea. Uno de los mayores riesgos de los certificados SSL sin autenticar es la técnica de las intrusiones ilícitas, también denominada "spoofing". El bajo coste del diseño de un sitio web y la sencillez con la que pueden copiarse las páginas existentes simplifican la creación de sitios falsos que parecen ser seguros y pertenecer a organizaciones establecidas. De hecho, hay casos de expertos del fraude que han conseguido números de tarjetas de crédito estableciendo tiendas de aspecto profesional que imitaban negocios legales, utilizando un nombre de dominio muy similar y presentando contenidos engañosos que hacían que la víctima tomara una decisión que ponía en peligro su seguridad.

Hay otras razones por las que la autenticación es importante. El fraude en Internet sigue constituyendo una gran barrera para el gasto de los consumidores, y un importante número de estafas se debe a que los clientes realizan transacciones con entidades de las que tienen muy poca o ninguna información.

A continuación se incluyen algunos datos relacionados con el fraude en Internet:

- Según GartnerG2, en 2001 se perdieron por fraude más de 700 millones de dólares en transacciones electrónicas, lo que representa el 1,14 por ciento de los 61.800 millones de ventas anuales en línea. En el año 2001, las pérdidas por fraude fueron 19 veces más altas en las transacciones electrónicas que en las ventas no electrónicas.
- Según Gartner Group, el fraude en Internet está causando pérdidas cuantiosas en el sector de los vendedores a través de Internet. Gartner estudió más de 160 empresas y descubrió que existe 12 veces más fraude en las transacciones a través de Internet que en la venta al por menor tradicional. Y lo que es más, los vendedores en línea deben asumir la responsabilidad y los costes en caso de fraude, mientras que en el caso de las transacciones tradicionales son las empresas de tarjetas de crédito las que se hacen cargo de dichos costes, siempre y cuando el vendedor siga los procedimientos y cuente con un recibo firmado.

- Las investigaciones llevadas a cabo por Jupiter Media Metrix han demostrado que es más habitual el miedo al fraude en línea que las situaciones de fraude real que se producen. "La prensa crea una mala imagen de las compras en línea, pero en la mayoría de los casos se trata de empresas que no han utilizado los medios de seguridad adecuados", asegura Harry Wolhanlder, vicepresidente de Market Research en ActivMedia. "Los negocios en Internet que aplican medios adecuados para comprobar la información de los clientes apenas se ven afectados por este problema y las pérdidas por fraude en este caso se limitan a un 1% aproximadamente. El control del fraude en línea es perfectamente posible, pero hay muchas empresas que no emplean rigurosas medidas de prevención y comprobación".

La siguiente sección describe algunos de los riesgos de una autenticación insuficiente del usuario e incluye dos posibles situaciones en las que la seguridad del comercio electrónico estaría en riesgo.

	Opción 1	Opción 2	Opción 3	Opción 4
Organización (O) =	Banco Mundial ABC	abcbancoelectronico.com	abcbancoelectronico.com	
Nombre común (CN) =	abcbancoelectronico.com	abcbancoelectronico.com	abcbancoelectronico.com	abcbancoelectronico.com
Exención de responsabilidad	Organización no autenticada	Organización no autenticada		

+ Situación 1: La autoridad de certificación no ha autenticado la empresa

Pepe el Pirata se registra en www.abcbancoelectronico.com, piratea el sitio del Banco Mundial ABC, atrae a los clientes desprevenidos al sitio falso que ha creado y consigue un certificado SSL sin autenticar. Este certificado incluye uno de los siguientes elementos en el nombre distintivo (consulte el gráfico anterior).

Cuando un cliente visita el sitio falso de Pepe el Pirata, no puede determinar con facilidad si el sitio es o no legítimo. Si el cliente ve el icono de candado, puede tener una sensación falsa de seguridad. Pensará que está conectado al sitio web del Banco Mundial ABC, aunque en realidad se esté conectando al sitio fraudulento de Pepe el Pirata. Cuando el icono de candado aparece en una página de envío de información, es muy probable que el cliente utilice su contraseña e ID de usuario. Pepe el Pirata puede intentar capturar la contraseña e ID de usuario y reenviar al usuario al sitio auténtico.

Pero si el cliente mira el certificado SSL y ve una exención de responsabilidad de “organización no autenticada” o se percató de que el Banco Mundial ABC no se nombra en el certificado, se podrá frustrar el plan de Pepe el Pirata. Pero sólo ocurriría en el caso de que el usuario tomara unas medidas adicionales antes de introducir su contraseña e ID de usuario o información personal o confidencial.

Supongamos que el Banco Mundial ABC se hubiera registrado el dominio www.bancoabc.com y hubiera implantado un sitio web bancario legítimo en línea mediante un certificado SSL. Este certificado incluye lo siguiente en el nombre distintivo:

Organización (O) =	Banco Mundial ABC
Nombre común (CN) =	bancoabc.com

Al requerir la autenticación de la organización se evita que una persona o entidad fraudulenta pueda obtener un certificado que contenga el nombre de otra organización. Al incluir un nombre de organización autenticado en el certificado SSL, los usuarios tendrán la seguridad de que la organización que presenta dicho certificado en su sitio web es legítima.

+ Situación 2: La autoridad de certificación no ha comprobado la existencia de la empresa

Pepe el Pirata registra un dominio como Banco Corporativo de Internet (que no existe) utilizando una tarjeta de crédito robada como medio de pago. Pepe el Pirata crea un sitio web y obtiene un certificado SSL sin autenticar que da a su sitio cierto aspecto de legal. Un cliente ve el icono de candado en el navegador y piensa que su información está segura. Si Pepe ofrece una tasa de interés superior a la normal o una financiación atractiva, puede inducir a los usuarios a introducir información personal.

Al exigir que se compruebe la existencia de una organización se evita que una persona finja ser una organización legítima.

Cómo saber si un sitio web es auténtico

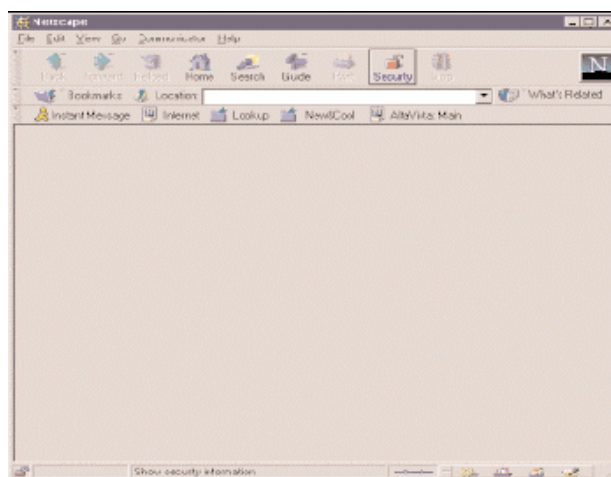
Antes de enviar información o adquirir productos de un vendedor en línea, debe saber que la empresa con la que está realizando la transacción es quien dice ser. Aunque los sitios web pueden comprar certificados de servidor de muchas autoridades de certificación, los navegadores de Internet están configurados para que sólo confíen en los certificados de servidor que provengan de empresas de buena reputación. Cuando visita un negocio en línea que está asegurado por VeriSign, por ejemplo, puede estar seguro de que el sitio es auténtico.

Aunque muchos consumidores y empresarios no comprenden totalmente el exhaustivo método de los servicios de autenticación de VeriSign, saben que pueden tomar el sello Secured Seal de VeriSign como prueba de que una empresa es real y que constituye un lugar seguro en el que comprar. Todas las empresas web autenticadas obtienen un sello con su solución de certificado para aumentar la confianza de los clientes en su sitio.

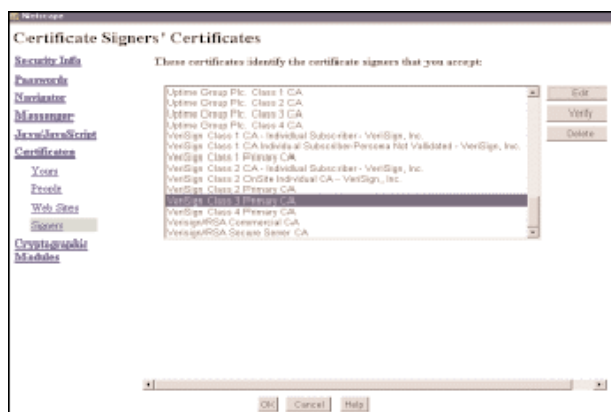


Los navegadores Netscape Navigator y Microsoft Internet Explorer incorporan mecanismos de seguridad que impiden que los usuarios envíen involuntariamente información confidencial a través de canales poco seguros. Si un usuario intenta enviar información a un sitio no seguro (un sitio sin un certificado SSL autenticado), el navegador mostrará de forma predeterminada un mensaje de advertencia, indicando que el proceso de compra puede suponer un riesgo.

Los certificados de VeriSign demuestran su identidad en el momento de realizar las transacciones electrónicas, de la misma forma que los permisos de conducir y el pasaporte lo hacen en situaciones de contacto directo. Gracias al certificado SSL de VeriSign podrá asegurar a sus clientes que la información electrónica que reciben de usted es auténtica.



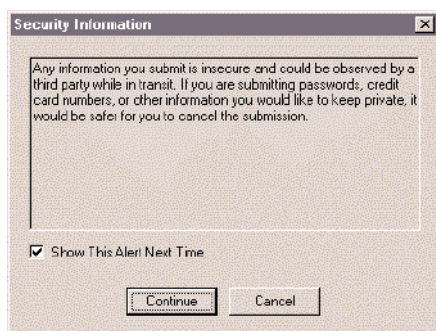
Arriba se muestra un ejemplo de un certificado SSL concreto, visto en la versión 4.0 de Netscape Communicator.



Para empezar, haga clic en el icono de seguridad de la barra de herramientas.



Seleccione los firmantes del certificado y visualice la lista de certificados.



Proceso de autenticación de VeriSign

Los procedimientos de autenticación y verificación fijados por VeriSign ayudan a que los comerciantes experimenten un crecimiento de sus negocios en línea, ya que inspiran confianza en los consumidores mediante la comprobación de la identidad de los negocios en línea y la reducción del riesgo de fraude. Estos procedimientos son el resultado de años utilizando una infraestructura fiable para Internet y autenticando más de medio millón de empresas. A continuación se incluye un resumen del proceso de autenticación de VeriSign que le ayudará a apreciar la seguridad y fiabilidad de este proceso y los beneficios que conlleva para el desarrollo de su negocio en línea:

+ Paso 1

Para iniciar el proceso de autenticación, las empresas y particulares proporcionan información a VeriSign, lo que forma parte del rápido y sencillo proceso de adquisición de soluciones de certificados digitales en línea.

+ Paso 2

Entonces VeriSign verifica que:

- La empresa y el personal de contacto empresarial no están incluidos en ninguna de las tres listas de entidades no autorizadas del gobierno de EE.UU.: Denied Persons List (lista de personas no autorizadas), Denied Entities List (lista de entidades no autorizadas), US Treasury Department List (lista del Ministerio de Hacienda de EE.UU.)
- La empresa cuenta con documentos oficiales, como estatutos de constitución o una licencia comercial que le permita realizar negocios.
- La empresa posee el nombre de dominio para el que se emite el certificado o ha obtenido un permiso legal del propietario del mismo para utilizar dicho nombre.
- Es posible utilizar números de terceros para comprobar que el personal de contacto empresarial trabaja en la empresa que solicita el certificado.

+ Paso 3

En ese momento VeriSign emite el certificado según la política de operaciones de VeriSign, que dispone:

- La separación de obligaciones: dos empleados de VeriSign diferentes deben completar el proceso de autenticación de la empresa que solicita el certificado y verificar que las personas de contacto trabajan para dicha empresa.
- Todos los empleados de VeriSign que procesan certificados digitales deben someterse a exhaustivos controles de sus antecedentes penales y financieros.

- Todas las instalaciones en las que se procesan los certificados digitales cuentan con sistemas de alta seguridad y biometría.
- Todos los datos de los clientes son estrictamente confidenciales y los centros de datos que almacenan dicha información están ubicados en lugares de alta seguridad con biometría.

+ Paso 4

Una vez se ha emitido el certificado SSL de VeriSign y que la empresa web autenticada lo coloca en su servidor web, los visitantes pueden acceder instantáneamente a los datos de autenticación. Estos datos aseguran a los visitantes del sitio web que dicho sitio es lo que aparenta ser y pertenece a una empresa real, y para visualizarlos basta con hacer clic en el icono de candado o en el sello Secured Seal de VeriSign que se suministra a todos los sitios web equipados con un certificado SSL.



Razones por las que el método de autenticación de VeriSign es más seguro

El proceso de autenticación de VeriSign es eficaz y seguro, a la vez que ofrecemos el plazo más breve posible de respuesta a las solicitudes de certificado SIN comprometer la fiabilidad del proceso.

Antes de emitir un certificado SSL, VeriSign comprueba sus documentos oficiales y completa el proceso de comprobación de veracidad para asegurar que su empresa es quien dice ser y que no está mostrando una identidad falsa. Después, VeriSign emite para su empresa un certificado SSL, que es una prueba electrónica que su negocio puede presentar para demostrar su identidad o su derecho a acceder a la información.

Beneficios para su empresa

Tras instalar su certificado de VeriSign, su servidor activa automáticamente la tecnología SSL, que sirve para crear un canal de comunicación seguro y autenticado entre su servidor y el navegador del cliente. Su sitio podrá comunicarse de forma segura con cualquier cliente que utilice Netscape Navigator, Microsoft Internet Explorer y los programas de correo electrónico más conocidos. Una vez haya activado su certificado de servidor, el SSL comenzará inmediatamente a proporcionarle los siguientes beneficios de una transacción electrónica segura:

+ Atracción de clientes

Cuando establezca su sitio web seguro, podrá beneficiarse de una gran variedad de opciones de VeriSign para mejorar aún más sus operaciones de comercio electrónico. Con el sello Secure Seal de VeriSign, que se incluye con todos los servicios de Secure Site, podrá utilizar la marca de seguridad número uno en Internet para dar a sus clientes la confianza necesaria para comunicarse y realizar transacciones comerciales en su sitio. Este sello permite a los visitantes de su sitio web comprobar la información y el estado de su certificado SSL en tiempo real, y proporciona protección adicional contra el uso indebido de certificados anulados o que han caducado.

VeriSign asegura más sitios web que ninguna otra empresa del mundo: más de 500.000. Este variado universo de clientes incluye la mayoría de las empresas de la famosa lista Fortune 500 y de los sitios de comercio electrónico más importantes, aunque también pequeñas y medianas empresas que dan sus primeros pasos en la Web.

El número de sitios asegurados por VeriSign es tan grande y la confianza en el sello Secured Seal de VeriSign tan enorme, que sólo en abril de 2002 se hizo clic en los sellos Secured Site Seal de VeriSign más de un millón de veces. El sello proporciona una prueba a los clientes de que el sitio web que están visitando está autenticado como negocio real, y que está asegurado con la tecnología de cifrado SSL.

Ventajas principales de contar con un certificado de servidor de VeriSign en su sitio: Garantizar transacciones electrónicas seguras que protejan a los clientes y a su negocio. Los clientes tendrán la seguridad de que envían su información personal a una empresa legal y no a un impostor. Por su parte, sabrá que su empresa recibe información precisa que el cliente no podrá denegar posteriormente.

Los servicios de seguridad Secure Site de VeriSign le proporcionan los medios para asegurar y activar el comercio electrónico de su sitio web, lo que proporciona al cliente la tranquilidad de que sus operaciones en la Web son seguras. El aumento de la confianza en las transacciones realizadas en línea aporta muchos beneficios. Entre los más importantes están el aumento de los ingresos y la rentabilidad.

+ Autenticación

Comprobando el certificado de VeriSign, sus clientes pueden asegurarse de que se trata es el propietario del sitio web y no un impostor. Este hecho les proporciona la confianza necesaria para enviar información confidencial.

+ Privacidad de los mensajes

El SSL cifra toda la información que se intercambia entre su servidor web y los clientes, como los números de tarjeta de crédito y otros datos personales, mediante una clave de sesión única. Para transmitir la clave de sesión al cliente de manera segura, el servidor la cifra con su clave pública. Cada clave de sesión se utiliza una sola vez, durante una única sesión (que puede incluir una o más transacciones) con un mismo cliente. Estos niveles de protección de la privacidad aseguran que la información no pueda visualizarse en caso de que terceras partes la intercepten.

+ Integridad de los mensajes

Cuando se envía un mensaje, los equipos que lo envían y lo reciben crean una clave que se basa en el contenido de dicho mensaje. Si un sólo carácter del contenido del mensaje se altera en el camino, el equipo receptor crea una clave diferente y advierte al receptor de que el mensaje no es legítimo. Gracias a la integridad de los mensajes, las dos partes involucradas en la transacción saben que lo que reciben es exactamente lo que ha enviado la otra parte.

Conclusión

Algunas autoridades de certificación creen que el cifrado sin autenticación basta para garantizar la seguridad de un sitio web y promover la confianza de los clientes en dicho sitio. Pero el cifrado por sí solo no es suficiente.

Los certificados SSL sin autenticar proporcionan confidencialidad e integridad, pero carecen de la autenticación de terceras partes tan necesaria para:

- Comprobar que el sitio que el usuario está visitando realmente pertenece a la compañía y no a un suplantador.
- Permitir al destinatario de un mensaje digital estar seguro tanto de la identidad del emisor como de la integridad del mensaje.
- Garantizar transacciones electrónicas seguras que protejan a los clientes y a su negocio.

Por estas razones, es de vital importancia que su sitio web esté autenticado, lo que aumentará la confianza que los visitantes de la Web depositan en su sitio y en su negocio. Por otra parte, si hay partes sin autorizar que emiten certificados, la veracidad de éstos suele verse mermada. Al requerir que se compruebe el derecho que tiene un solicitante de certificado para realizar dicha solicitud (por ejemplo, si está empleado en la empresa nombrada en el certificado) se evita el riesgo de emitir un certificado para un individuo con intenciones fraudulentas que no esté empleado en la empresa.

Los certificados SSL de VeriSign proporcionan una alta credibilidad a las empresas en línea. Nuestros exhaustivos métodos de autenticación fijan un estándar que asegura que:

- Los suscriptores están debidamente identificados y autenticados.
- Las solicitudes de certificados de los interesados son precisas y completas y han recibido la pertinente autorización.

Gracias al sello Secured Seal de VeriSign, puede dar a sus clientes la confianza necesaria para comunicarse y realizar transacciones en su sitio web. Este sello permite a los visitantes de su sitio comprobar la información y el estado de su certificado SSL en tiempo real y proporciona protección adicional contra el uso indebido de certificados anulados o que han caducado.

Los rigurosos métodos de autenticación, las técnicas de cifrado de última generación y las instalaciones de gran seguridad de VeriSign están orientados a potenciar su confianza y la de sus clientes. Estos métodos, tecnología e infraestructura son las bases de los certificados de servidor para asegurar las transacciones en colaboración con su servidor web.

Información adicional

Si desea ponerse en contacto con un experto en seguridad de VeriSign, llame al número gratuito 900 93 1298 o póngase en contacto con un representante de VeriSign por correo electrónico escribiendo a: ventas@verisign.es

Si desea más información, visítenos en www.verisign.es