Cómo asegurar un

Servidor Web de Apache

con un **certificado digital thawte**

UNA GUÍA PASO A PASO *para probar, instalar y utilizar un certificado digital thawte en el servidor Web de Apache...*

La imagen "Pluma" que aparece en este documento es el logotipo de Apache Software Foundation: http://www.apache.org

thawte
it's a trust thing

1. Aspectos generales

En esta guía, podrá obtener información sobre cómo probar, adquirir, instalar y utilizar un certificado digital ***thawte*** en el servidor Web de Apache. En ella, se resaltan las mejores prácticas de la instalación a fin de asegurar una gestión eficaz y constante de las claves de cifrado y de los certificados digitales.

Asimismo, se indica el papel que juega ***thawte*** como tercera parte fiable y las ventajas de la utilización de un certificado digital de ***thawte*** para su negocio ya que permiten desarrollar la confianza de sus clientes gracias a la solución de los problemas de seguridad online.

2. Requisitos del sistema

Antes de instalar un certificado SSL en el servidor Web de Apache, tiene que instalar los componentes SSL necesarios. Tendrá que instalar OpenSSL, así como ModSSL o Apache-SSL. OpenSSL y sus bibliotecas criptográficas proporcionan el "back-end" de SSL, mientras ModSSL o Apache-SSL constituyen el interfaz entre Apache y OpenSSL. ModSSL es diferente a Apache-SSL. ModSSL es el paquete de SSL completo y es mejor documentado comparado con la alternativa de Apache-SSL que también tiene su sede en OpenSSL. El usuario decide cuál desea usar: ***thawte*** no tiene preferencia por ninguno de los dos.

En esta guía, se asume que va a utilizar Apache y que tiene instalado ModSSL.

SITIOS WEB ÚTILES:

www.apache.org

www.modssl.org

www.apache-ssl.org

www.openssl.org

3. Generación de la clave privada

Utilice el OpenSSL binario para generar la clave privada. Esta clave se mantendrá en el servidor Web por lo que se recomienda que siga las mejores prácticas de seguridad mediante protección criptográfica con el comando siguiente:

"openssl genrsa –des3 1024 –out www.mydomain.com.key 1024"

De este modo, se comunicará a OpenSSL que genere una clave RSA privada de 1024 bits y que encripte este archivo mediante la cifra "Triple DES" que envíe el resultado a un archivo denominado www.mydomain.com.key.

> Se le pedirá que introduzca una frase PEM (Privacy Enhanced Message) cuando genere el archivo de clave privada y que lo introduzca una segunda vez para verificarla.

Una clave privada encriptada se asegura con una frase y se recomienda que se especifique esta opción. Cuando se reinicia la máquina que utiliza esta clave o se reinicia Apache, se le pedirá que introduzca esta frase.

¡Importante!

¡HAGA UNA COPIA DE SEGURIDAD DE ESTE ARCHIVO CON LA CLAVE Y DE LA FRASE CORRESPONDIENTE!

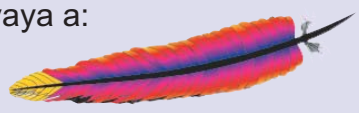
Generalmente, la mayoría de los problemas que tienen los usuarios al realizar este proceso está relacionado con las claves privadas. Si pierde la clave, no puede acceder a ella o no puede recordar la frase PEM definida en el archivo con la clave privada, no podrá utilizar el certificado que le emitamos.

Para copiar el archivo a otra ubicación (en este caso, la a:\drive) use el comando siguiente:

"cp www.mydomain.com.key path-to-removable-disk"

Si no sabe cómo continuar o necesita ayuda adiccional, vaya a:

"openssl genrsa --help"



4. Generación del CSR (Certificate Signing Request)

El paso siguiente es la creación de una CSR que tendrá que proporcionar a ***thawte*** para que pueda emitir el certificado. Para generar el CSR, use OpenSSL y su clave privada creada en el paso anterior, como sigue:

"openssl req –new –key www.mydomain.com.key –out www.mydomain.com.csr"

Este paso crea una CSR que tiene los mismos "módulos" que la clave privada. Se le pedirá que introduzca la información siguiente al generar la CSR:

Nombre del país (código de 2 letras) [ES]: AR
Nombre del estado o la provincia (nombre completo) [Granada]: Santa Fe
Nombre de la localidad (o ciudad) [Motril]: Rosario
Nombre de la organización (empresa) [Mi empresa SA]: Widgets Inc.
Nombre de las unidades organizativas (secciones) []: Widgets
Nombre común (su nombre o el del host) []: www.mydomain.com
Dirección de correo electrónico [Opcional] :

Estos son los detalles que ***thawte*** verificará, por lo que debe asegurarse de que los detalles de su CSR coincidan EXACTAMENTE con los de su empresa.

Nota: Se le pedirá que introduzca una frase PEM (Privacy Enhanced Message). (Se trata de la frase que define en el archivo con la clave privada generada en el paso anterior.)

Nota importante

El término "nombre común" es la terminología X.509 para el nombre que distingue mejor el certificado y lo vincula a la organización. En el caso de certificados SSL, introduzca su host exacto (Ej. www) y el nombre de dominio (Ej. Midominio.com) que desea asegurar.
Uno de los errores más frecuentes es la inserción de un nombre de dominio incorrecto en el campo de "nombre común" del archivo CSR. Un certificado se vincula al host y el nombre de dominio correspondiente, por lo que debe asegurarse que este campo se rellene con el host y nombre del dominio exacto y totalmente cualificado, que utilizará para acceder a las páginas aseguradas de su sitio Web. **NO DEBE** incluir la porción 'http://' de la dirección URL ni ningún directorio que se encuentre por debajo de este dominio. Por ejemplo, si para desconectarse se accede mediante https://secure.mydomain.com/checkout, sólo incluirá secure.mydomain.com en el campo de "nombre común".

El archivo CSR creado anteriormente se vuelca a un archivo denominado www.mydomain.csr y el archivo debe tener un aspecto similar al siguiente:

-----BEGIN CERTIFICATE REQUEST-----
MIIB2TCCAUICAQAwgZgxCzAJBgNVBAYTAlVTMRAwDgYDVQQIEwdHZW9yZ2lhMREwDwYDVQQ
HEwhDb2x1bWJ1czEbMBkGB1UEChMSQUZMQUMgSW5jb3Jwb3JhdGVkMQswCQYDVQQLEwJJV
DEYMBYGA1UEAxMPd3d3LmFmbGFjbnkuY29tMSAwHgYJKoZIhvcNAQkBFhFKR2FybW9uQGFmb
GFjLmNvbTCBnzANBgkqhkiG9w0BAQEFAAOBjqAWgYkCgYEAsRqHZCLIrlxqqh8qs6hCC0KR9qEPX
2buwmA6GxegICKpOi/IYY5+Fx3KZWXmta794nTPShh2lmRdn3iwxwQRKyqYKmP7wHCwtNm2taCRV
oboCQOuyZjS+DG9mj+bOrMK9rLME+9wz1f8l0FuArWhedDBnI2smOKQID45mWwB0hkCAwEAAaAA
MA0GCSqGSIb3DQEBBAUAA4GBAJNlxhOiv9P8cDjMsqyM0WXxXWgagdRaGoa8tv8R/UOuBOS8/H
qu73umaB9vj6VHY7d9RKqDElFc/xlXeDwoXNiF8quTm43pmY0WcqnL1JZDGHMQkzzGtg502CLTHM
ElUGTdKpAK6rJCkucP0DKKEJKcmTySSnvgUu7m
-----END CERTIFICATE REQUEST-----

Para ver el archivo CSR, use alguno de los siguientes comandos:
cat www.mydomain.csr
vi www.mydomain.csr

Ya ha realizado los tres pasos básicos que le permiten solicitar un certificado SSL de ***thawte***.

5. Utilización de un certificado de prueba

Para familiarizarse con el proceso de un certificado de ***thawte*** en un servidor de Apache, puede configurar un certificado en el servidor con un certificado de prueba de ***thawte***.

En este paso, se asume que ha configurado un SSL en Apache. De lo contrario, consulte la sección 7 para establecer la configuración antes de proceder.

Aunque estos certificados sólo son para evaluación y prueba, proporcionan encriptación, pero cuando se establece una sesión SSL con un servidor que tiene instalado un certificado de prueba, aparece un mensaje de advertencia. Este mensaje informa al usuario que se conecta, que el certificado no está garantizado, por lo que la integridad del sitio no está garantizada.

Estos certificados se han diseñado para probar la configuración del servidor antes de que adquiera un certificado garantizado de una autoridad certificadora (CA = Certification Authority).

Generarán errores en los exploradores que no hayan insertado manualmente el certificado raíz requerido.

Si lo inserta manualmente, el explorador confiará en ese certificado de prueba. Siga las instrucciones proporcionadas en el asistente para la instalación del certificado raíz de prueba de CA de ***thawte*** haciendo clic en : https://www.thawte.com/roots/index.html

Los certificados de prueba tienen una validez de 21 días y este servicio no tiene NINGUNA GARANTÍA !

Puede solicitar un certificado de prueba de ***thawte*** online en : http://www.thawte.com/ucgi/gothawte.cgi?a=w46840165337049000

Hasta ahora, ha creado tres archivos:

www.mydomain.key
- Una clave privada de RSA

www.mydomain.csr
- Una RSA

www.mydomain.crt
- Un archivo de certificado de prueba de ***thawte***

Se le pedirá que copie y pegue la CSR en el área de texto proporcionado en la página Test Certificate System.

Nota: tendrá que copiar y pegar la CSR, incluidas las barras y las sentencias de línea completas BEGIN y END.

El certificado de prueba se generará inmediatamente en función de la CSR proporcionada y podrá verlo en la página siguiente. Guarde el certificado de prueba en un archivo denominado www.mydomain.com.crt.

6. Solicitud de un certificado garantizado

Puede solicitar certificados SSL ***thawte*** :
https://www.thawte.com/buy/

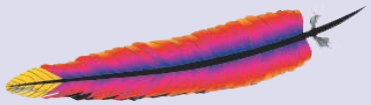
Durante el proceso de solicitud del certificado, se le pedirá que copie y pegue la CSR en una área de texto dentro del formulario online.

Nota: tendrá que copiar y pegar la CSR, incluidas las barras y las sentencias de línea completas BEGIN y END.

Importante

Asegúrese de enviar la CSR correcta, si ha generado más de una. Puede comprobar la CSR con el comando siguiente:

"openssl req –text –noout –in csrfilename.csr"



Tendrá que proporcionar la información siguiente durante el proceso de solicitud y enviarnos documentación que acredite su identidad o la de su empresa (por ejemplo, un certificado de registro de la empresa). Puede ver instrucciones detalladas sobre cómo obtener un certificado SSL de ***thawte*** en :
http://www.thawte.com/support/docs.html

Una vez completado el proceso de solicitud online, ***thawte*** iniciará un proceso exhaustivo de verificación de la identidad y de los detalles proporcionados en la CSR. ***thawte*** realiza una gran cantidad de comprobaciones exhaustivas antes de emitir un certificado. En consecuencia, la verificación de la identidad y los detalles de la empresa y la correspondiente emisión del certificado pueden llevar varios días.

Durante este período de verificación, puede comprobar el estado de la solicitud en la página de estado en (status page):
http://www.thawte.com/cgi/server/status.exe

Si tiene alguna consulta durante este período, puede ponerse en contacto con el representante del servicio al cliente asignado a su solicitud. Los detalles del representante se pueden encontrar en la página de estado de la dirección URL anterior en "Persona de contacto de ***thawte***".

7. Configuración de SSL en Apache

Antes de instalar los certificados de prueba o los “garantizados”, tendrá que configurar el servidor Web de Apache.

Las ‘directivas’ (directives) permiten comunicar a Apache el modo exacto en que debe comportarse en determinadas condiciones, desde cómo se gestionan ciertos contenidos hasta cómo comunicar a Apache el nombre del servidor.

Mod_ssl proporciona las directivas utilizadas para configurar la compatibilidad con SSL en Apache. A continuación se enumeran las directivas más frecuentes :

SSLCACertificateFile - Especifica la ruta de acceso a un archivo que contiene certificados raíz del CA.

SSLCertificateFile - Especifica la ubicación del certificado SSL que se va a utilizar en una máquina concreta.

SSLCertificateKeyFile - Ruta de acceso a la clave privada que corresponde al archivo mencionado en la directiva anterior.

SSLEngine - Esta directiva controla si SSL "está activa" o no para un servidor o host virtual determinado.

Mod_ssl proporciona un conjunto completo de directivas que le permiten configurar el servidor según sus necesidades. Para obtener una lista completa de las directivas SSL que proporciona Mod_ssl, consulte la documentación de Mod_ssl : http://www.modssl.org/docs/2.2/ssl_reference.html

Para configurar Apache para SSL, tendrá que actualizar el archivo “httpd.conf” para que busque un nuevo certificado. Abra el archivo de configuración “httpd.conf” y asegúrese de que las directivas ”SSLCertificateFile” y “SSLCertificateKeyFile” están asociadas a las rutas de acceso a los archivos correctos.

Por ejemplo, si tiene un certificado en el directorio “/usr/local/ssl/certs/” y la clave privada en el directorio “/usr/local/ssl/private/”, aparecerán los datos siguientes en el archivo “httpd.conf” :

SSLCertificateFile: /usr/local/certs/www.mydomain.com.crt
SSLCertificateKeyFile: /usr/local/ssl/private/www.mydomain.com.key

También tendrá que asegurarse de que el servidor Apache así como el cortafuegos y los encaminadores instalados escuchan al puerto 443 y “activan” SSL con las directivas “SSLEngine on” o SSLEnable en ModSSL o Apache-SSL respectivamente.

8. Instalar el certificado

Una vez emitido el certificado, tendrá que descargarlo de la página de estado haciendo clic en el botón “Fetch Certificate” (que sólo aparece cuando el certificado se ha emitido). El certificado puede ser copiado al directorio que usted prefiere. Para manejo fácil, recomendamos que lo guarden a un directorio apropiado en el archivo “httpd.conf”. De este modo, la clave y el certificado serán más fáciles de gestionar.

Para mentener la estabilidad del certificado, se recomienda guardarlo en un archivo denominado “www.mydomain.com.crt”. El certificado se almacena en la base de datos de ***thawte*** de forma indefinida y puede descargarse de nuevo en cualquier momento.

Si ha configurado el servidor Web, no tendrá que realizar ningún cambio al archivo de configuración. Tan sólo tiene que copiar el archivo de certificado real (garantizado) sobre el certificado de prueba.

Una vez emitido el certificado, puede abrir el archivo de configuración de Apache e instalar el certificado, así como configurar el entorno SSL.

El certificado tendrá un aspecto similar al siguiente :

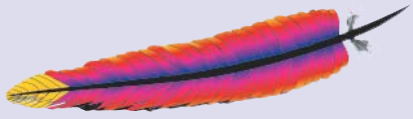
-----BEGIN CERTIFICATE-----
MIIDBTCCAm6gAwIBAgIDcxV2MA0GCSqGSIb3DQEBBAUAMIGHMQswCQYDVQQGEwJaQTEi
MCAGA1UECBMZRk9SIFRFU1RJTkcgUFVSUE9TRVMgT05MWTEdMBsGA1UEChMUVGhhd3RII
ENIcnRpZmljYXRpb24xFzAVBgNVBAsTDIRFU1QgVEVTVCBURVNUMRwwGgYDVQQDExNUaG
F3dGUgVGVzdCBDQSBSb290MB4XDTAyMTEwNTemJhDUzMloXDTAyMTEyNjE0MDUzMlowgd8
xFDASBgNVBAMTC3d3dy5jcmRiLmJlMRswGQYDVQQLHhlAQwBPAEwAVABAAarfJsdQBTAFQx
czBxBgNVBAoeagBDAGEAcAAgAEcAZQBtAGkAbgBpACAAVABlAGwAZQBjAG8AbQAgAE0BZq
BkAGkAYQAgACYAIABOAGUAdAB3AG8AcgBrAHMAIABCAGUAbABnAGkAdQB
BkRpZWdlbTeCxMBUGA1UECBMOVmxhYW1zIEJyYWJhbnQxCzAJBgNVBAYTAkJFMIGfMA0GC
SqGsIb3DQEBAQUAA4GNADCBiQKBgQDaNm3HPzG6Rbk5Am0HI6JFHoDQku2/YmVMGbZk5A
HeR13QxIP7UVa08/k8qR3B7B0mfbxaNlxdwV9c7c1z4mZYQRfAeryoW4sU2jh1OHc4Cin+i9UarkH
m8WnUnlcVZEnJrySdfLZNuxtbknXBNkca8rk6tnlbXodD3gEQJBMJtQIDAQABoyUwIzAT
-----END CERTIFICATE-----

Cuando se vea con OpenSSL, con el comando siguiente :

“openssl req –text –noout –in www.mydomain.com.crt”

el archivo de certificado contendrá los detalles siguientes:

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 645099 (0x9d7eb)
        Signature Algorithm: md5WithRSAEncryption
       Issuer: C=ZA, ST=Western Cape, L=Cape Town, O=thawte Consulting
cc, OU=Certification Services Division, CN=thawte Server CA/Email=server-
certs@thawte.com
        Validity
            Not Before: Dec 11 12:34:19 2002 GMT
            Not After : Dec 11 12:34:19 2003 GMT
        Subject: C=US, ST=Texas, L=Dallas, O=Widgets Inc., OU=Widgets,
CN=www.widgets.com
       Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:b5:89:6c:cb:bb:9c:56:32:5f:77:5d:3d:9c:9c:
                    81:41:3d:8a:37:bc:4d:10:26:03:8c:f4:27:07:74:
                    88:a5:3a:d5:32:82:ab:1b:42:12:2a:bf:65:ad:b8:
                    b3:c7:f1:b0:ea:66:94:5e:82:ca:55:6e:26:c4:7f:
                    b0:5b:e5:22:b1:39:12:fd:a0:0d:cd:ef:59:56:95:
                    d3:33:14:da:f6:b8:c1:f8:d7:c1:05:32:d7:2d:90:
                    83:e6:91:f0:70:b1:d9:88:29:06:6a:45:02:17:aa:
                    df:1d:4b:56:d8:8d:ff:02:fc:22:20:e2:be:63:e5:
                    4e:09:e1:9c:97:24:91:ef:b1
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Extended Key Usage:
                TLS Web Server Authentication
            X509v3 Basic Constraints: critical
                CA:FALSE
    Signature Algorithm: md5WithRSAEncryption
        97:48:b9:78:ca:66:f5:33:b9:3b:62:c2:52:26:04:8d:3f:e9:
        32:ec:c9:e4:a2:fa:a5:b0:f8:df:10:5b:11:8b:36:97:62:e3:
        82:63:20:93:7b:84:08:03:de:9e:a1:37:e3:12:e5:03:87:33:
        f5:74:7e:84:9e:bb:52:bb:e3:8a:c1:a8:68:87:ad:8a:a4:95:
        0d:61:98:4e:cd:da:13:fe:8c:0c:87:d4:7f:e6:18:3e:36:a4:
        d1:ad:23:13:07:fc:bf:8c:bd:8a:42:32:e3:22:af:1b:7c:fb:
        5e:d3:1a:94:f9:24:3c:4b:bd:3e:e9:f2:c6:9c:56:e4:b6:e2:
        1e:6d
```



Este certificado está vinculado a la clave privada que ha creado anteriormente (www.mydomain.com.key) y sólo se puede "adjuntar' a esa clave. Si pierde la clave privada a la que está vinculado un certificado, éste queda inutilizable.

Lo que tiene que hacer ahora es apuntar la directiva SSLCertificateFile a la ubicación que ha elegido guardar este archivo, que suele ser el mismo directorio en el que se encuentra el archivo "httpd.conf", /etc/apache o algo diferente.

SSLCertificateFile: /etc/apache/www.mydomain.com.crt

También puede indicar a Apache el archivo de clave que va a utilizar para este certificado. Por lo tanto, recuerde hacer que la directiva SSLCertificateKeyFile muestre la clave privada de este certificado :

SSLCertificateKeyFile: /etc/apache/www.mydomain.com.key

Las autoridades de certificación (CA) firman los certificados con una raíz de nivel superior y las aplicaciones que deseen verificar un certificado de usuarios finales tendrán que compaginar los certificados de los usuarios con el certificado raíz usado por la CA. ModSSL usa SSLCACertificateFile para ello y eso se incluye con ModSSL.

No debería tener que personalizar el contenido de este archivo. Este directivo se usa cuando se instala un certificado SSL123 o un SGC SuperCert y hace una referencia a "Intermediate Certificate" (certificado intermedio) que firma el Certificado emitido.

SSLCACertificateFile: /etc/apache/cacertificate.crt

Por lo tanto, ya que ha configurado todas estas directivas SSL, debería funcionar. ¿Verdad? No, no lo es. Hay más directivas pendientes: SSLEngine. Esta directiva tiene 2 argumentos: "on" o "off". Obviamente, SSL debería estar "on" (activado) :

SSLEngine on
La directiva anterior se puede utilizar en un contexto de servidor global o con el contenedor <VirtualHost>.

Si está utilizando el certificado en un host virtual correctamente configurado, la configuración tendría que ser similar a la siguiente:

```
<VirtualHost 192.168.1.22:443>
DocumentRoot /var/www/widgets
ServerName www.mydomain.com
ServerAdmin root@mydomain.com
ErrorLog /etc/httpd/logs/error_log
TransferLog /etc/httpd/logs/access_log
SSLEngine on
SSLCertificateFile /etc/httpd/conf/ssl.crt/www.mydomain.com.crt
SSLCertificateKeyFile /etc/apache/www.mydomain.com.key
SSLCACertificateFile /etc/apache/cacertificate.crt
SetEnvIf User-Agent ".*MSIE.*" nokeepalive ssl-unclean-shutdown
</VirtualHost>
```

Advertirá que en el contenedor <VirtualHost> se menciona un puerto específico, puerto 443. Se trata del puerto SSL predeterminado y se configura con la directiva global "Listen". De forma predeterminada, "Listen 80" se configura en el archivo "httpd.conf". Todo lo que tiene que hacer es añadir "Listen 443" a una nueva línea. Es aconsejable agrupar todas las directivas

9. Cómo asegurar hosts virtuales

Si tiene hosts virtuales seguros, cada uno necesitará su propia IP, puesto que SSL no suporta hosts virtuales que son “Name-based“.

SSL no puede configurarse en hosts virtuales que son “Name-based“ salvo que utilicen puertos SSL distintos.

Tenga en cuenta que la configuración mostrada anteriormente es muy básica y puede incluir muchas otras directivas SSL que le permitan personalizar el entorno SSL.

Una vez que se haya instalado el certificado y se haya configurado SSL correctamente, tendrá que reiniciar todo el servidor y no sólo el daemon. De este modo, se asegura de que la instalación tome efecto. La ubicación de los archivos de comandos que iniciarán Apache varía entre las distintas distribuciones de Linux. Por tanto, se asume que hay un archivo de comandos denominado "apache" en /etc/init.d/ que llama a un archivo de comandos en /usr/sbin/ denominado "apachectl".

widget@mydomain-pc/etc/init.d/apachectl startssl

Ya tendría que ser capaz de acceder a su máquina seguramente y ver los detalles del certificado. Sabrá si se ha establecido la sesión SSL si aparece un candado dorado en la barra de herramientas inferior del navegador. Haga doble clic en este icono para ver los detalles del certificado.

10. Direcciones URL útiles

Los problemas comunes que se experimentan con Apache-SSL y Apache ModSSL se indican en nuestro apartado de preguntas más frecuentes, FAQ:
http://www.thawte.com/support/keygen/index.html

La guía de generación de la clave para Apache-SSL se encuentra disponible en la dirección:
http://www.thawte.com/support/keygen/index.html

La guía de generación de la clave para Apache ModSSL se encuentra disponible en la dirección: http://www.thawte.com/support/keygen/index.html

El proceso de solicitud de certificado para Web Server Certificates y SuperCerts de 128 bits comienza en: https://www.thawte.com/buy/

Instrucciones para solicitar un certificado de prueba:
http://www.thawte.com/ucgi/gothawte.cgi?a=w46840168627049000

Dónde descargar el certificado raíz de prueba de CA de ***thawte***:
https://www.thawte.com/roots/index.html

11. ¿Qué papel juega *thawte*?

thawte Technologies es una autoridad Certificadora (CA) que emite certificados de servidor Web SSL para empresas e individuos a nivel mundial. thawte verifica que la empresa que solicita el certificado es una organización registrada y que la persona de la empresa que lo solicita está autorizada para ello.

thawte también comprueba que la empresa en cuestión posee el dominio relevante. Los certificados digitales de ***thawte*** interoperan con Apache y el último software de Microsoft y Netscape, de modo que pueda estar seguro de que la adquisición de un certificado digital de thawte proporcionará a sus clientes confianza e integridad en el sistema. Se sentirán seguros con en sus transacciones online.

12. El valor de la autenticación

La información es un valor clave para su negocio. Para asegurar la integridad y la seguridad de la información, es importante identificar con quién está comunicandose y si los datos que recibe son fiables. La autenticación puede contribuir al desarrollo de confianza entre las partes involucradas en todos los tipos de transacciones tras abordar conjuntos únicos de medidas de seguridad que incluye :

Simulación de falsificación de datos : El bajo costo del diseño de sitios Web y la facilidad con las que se pueden copiar páginas existentes facilita en su conjunto la creación ilegítima de sitios Web que aparecen como si hubieran sido publicados por organizaciones establecidas. De hecho, timadores profesionales han obtenido de forma ilegal números de tarjetas de crédito mediante la configuración de tiendas de comercio electrónico con aspecto profesional y camufladas en negocios legítimos.

Acción no autorizada : Una persona de la competencia o un cliente descontento puede alterar el sitio Web de modo que no funcione bien o que rechace a clientes potenciales.

Revelación no autorizada : Cuando se transmite información "abiertamente", los hackers pueden interceptar las transmisiones para obtener información sensible de los clientes.

Alteración de los datos : El contenido de una transacción se puede interceptar y alterar durante su trayectoria, bien de forma malintencionada o bien de forma accidental. Los nombres del usuario, los números de la tarjeta de crédito y las cantidades en divisas enviadas “abiertamente” son siempre vulnerables de alteración.

13. Como ponerse en contacto con *thawte*

Si tiene alguna pregunta sobre el contenido de esta guía o sobre los productos y servicios de ***thawte***, póngase en contacto con un asesor de ventas :

Correo electrónico : sales@thawte.com
Teléfono : +27 21 937 8902
Fax: +27 21 937 8967

14. Glosario de términos

Apache
Apache, como se conoce comunmente, es un proyecto de Apache Software foundation cuyo objetivo es producir un servidor Web seguro, eficaz y ampliable que proporcione servicios HTTP en sincronía con los estándares HTTP actuales.

jakarta.apache.org

Criptografía asimétrica
Método criptográfico en el que se utiliza un par combinado de clave pública y privada para la encriptación y el descifrado de mensajes. Para enviar un mensaje encriptado, un usuario encripta un mensaje con la clave pública del receptor. Al recibirlo, se descifra con la clave privada del receptor.

La utilización de diferentes claves para las funciones de encriptación y descifrado se conoce como la función de trampilla unidireccional, es decir, la clave pública se utiliza para encriptar un mensaje pero no se puede utilizar para descifrarlo. Sin saber la clave privada, es prácticamente imposible invertir esta función gracias a las potentes funciones de encriptación modernas

Autoridad Certificadora
Una autoridad certificadora (CA) es una organización (como ***thawte***) que emite y gestiona credenciales de seguridad y claves públicas para la encriptación de mensajes.

CSR (Certificate Signing Request)
Una CSR es una clave pública que se genera en su servidor y que valida la información específica del ordenador sobre el servidor Web y una organización cuando se solicita un certificado a ***thawte***.

Mod_ssl
Como Apache es una aplicación modular, una de sus funciones más potentes es su gran capacidad de personalización mediante con módulos de tercera parte que amplían sus prestaciones. Uno de los módulos más conocidos (y esencial en el mundo del comercio electrónico) creado para Apache es Mod_ssl. Mod_ssl es un módulo que proporciona compatibilidad SSL para Apache; sin Mod_ssl, Apache no sirve las solicitudes de SSL, pues actúa como si no supiera qué hacer con ellas.

OpenSSL
OpenSSL es un kit de herramientas criptográficas que implementa los protocolos de red Secure Sockets Layer (SSL v2/v3) y Transport Layer Security (TLS v1) y estándares criptográficos requeridos por éstos.

www.openssl.org

OpenSSL proporciona básicamente la plataforma sobre la que se ejecuta Mod_ssl y tiene que estar instalado en una máquina en la que se utilicen Apache + Mod_ssl. Sin OpenSSL, Mod_ssl no será de mucha utilidad. Cualquier utilidad o aplicación que requiera capacidades de encriptación usará las bibliotecas criptográficas de OpenSSL

Clave privada
Una clave privada es un código numérico utilizado para descifrar mensajes encriptados con una clave pública única correspondiente. La integridad de la encriptación depende de que la clave privada sea mantenida en secreto.

Clave pública
Una clave pública es un código numérico que habilita la encriptación de mensajes enviados al propietario de la única clave privada correspondiente. La clave pública puede circular libremente sin comprometer la encriptación mientras aumenta la eficacia y la conveniencia de habilitar la comunicación encriptada.

Criptografía simétrica
Método criptográfico en el que se utiliza la misma clave para encriptación y descifrado. Este enfoque se ve afectado por el riesgo de seguridad involucrado en la distribución segura de la clave dado que se debe comunicar tanto al receptor como al emisor sin ser revelada a partes terceras.