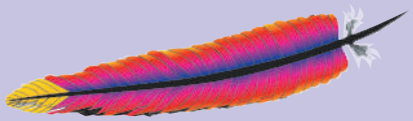

Sécuriser votre

Serveur Web Apache

avec un certificat numérique de thawte

UN GUIDE ÉTAPE PAR ÉTAPE pour tester, installer et utiliser un certificat numérique de thawte sur votre serveur web Apache...

L'image de la "plume" qui apparaît tout au long de ce document est le logo de la Fondation Apache Software : http://www.apache.org

thawte
it's a trust thing

1. Aperçu

Dans ce guide, vous découvrirez comment tester, acheter, installer et utiliser un certificat numérique de *thawte* sur votre serveur Apache. Les meilleures pratiques de mise en place sont mises en évidence tout au long de ce document pour vous aider à assurer une gestion suivie et efficace de vos clés de cryptage et de vos certificats numériques.

Nous parlerons également de *thawte* en tant que tierce partie de confiance et comment l'utilisation d'un certificat numérique de *thawte* peut être avantageuse pour vos affaires, en abordant de manière unique les problèmes de sécurité en ligne afin d'accroître la confiance auprès du consommateur.

2. Configuration Requise

Avant d'installer un certificat SSL sur votre serveur web Apache, vous devriez avoir installé les composants SSL requis. Vous aurez besoin d'installer OpenSSL, ainsi que ModSSL ou Apache-SSL. OpenSSL et ses bibliothèques cryptographiques fournissent le SSL arrière, alors que ModSSL ou Apache-SSL fournissent l'interface entre Apache et OpenSSL. ModSSL et Apache-SSL sont très similaires et c'est à vous de décider lequel des deux utiliser - *thawte* ne fait aucune recommandation entre les deux.

Dans ce guide, nous ferons la supposition que vous utilisez Apache avec ModSSL installé.

SITES WEB UTILES:

www.apache.org

www.modssl.org

www.apache-ssl.org

www.openssl.org

3. Générez votre clé privée

Utilisez l'OpenSSL binaire pour générer votre clé privée. Cette clé sera conservée sur votre serveur web. Nous vous recommandons de suivre la meilleure méthode qui consiste à la sécuriser avec une protection cryptée en utilisant la commande suivante:

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

Cette commande indiquera à OpenSSL de générer une clé privée RSA, d'une longueur de 1024 bits et de crypter ce fichier en utilisant le triple chiffrage DES et d'acheminer la sortie vers un fichier nommé www.mydomain.com.key.

> Il vous sera demandé de saisir une phrase de passe au format PEM (PEM – 'Privacy Enhanced Message') au moment de générer le fichier de clé privée ainsi que de la saisir une deuxième fois pour vérifier la phrase de passe définie.

Une clé privée cryptée est sécurisée avec une phrase de passe, et nous recommandons de spécifier cette option. Si la machine utilisant cette clé est rebootée, ou si Apache est redémarré, il vous sera demandé de saisir ce phrase de passe.

Important!

FAITES UNE COPIE DE SAUVEGARDE DE CE FICHIER DE CLÉ ET DE SA PHRASE DE PASSE !

De loin le problème le plus souvent rencontré par les utilisateurs au cours de cette procédure, est associé aux clés privées. Si vous perdez ou ne pouvez plus accéder à une clé privée ou si vous ne pouvez plus vous souvenir de la phrase de passe définie sur le fichier de clé privée, vous ne pourrez pas utiliser le certificat qu'on vous a délivré. Pour vous assurer que ceci ne se produit jamais, nous vous conseillons de faire une sauvegarde du fichier de clé privée, et que la phrase de passe PEM utilisée pour protéger le fichier de clé privée soit notée.

Pour copier le fichier à un autre emplacement (dans ce cas, votre lecteur a:\), utilisez la commande suivante :

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

Si vous êtes bloqué ou avez besoin d'une aide supplémentaire, veuillez vous rendre à :

"openssl genrsa --help"

4. Générez votre Requête de Signature de Certificat (CSR)

L'étape suivante consiste à créer une CSR (Requête de Signature de Certificat) que vous devrez fournir à *thawte* avant que votre certificat ne puisse vous être délivré. Pour générer la CSR, utilisez OpenSSL et votre clé privée créée à l'étape précédente, comme suit:

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

Cette étape crée la CSR qui a le même "module" que la clé privée. Il vous sera demandé de saisir les informations suivantes au moment de générer la CSR:

Nom du pays (code de 2 lettres) [GB] : FR
Nom du département ou de la région (nom complet) [Berkshire]: Finistère
Nom de la localité ou de la ville [Newbury] : Brest
Nom de l'organisation (p. ex. société) [My Company Ltd] : Widget SARL
Unité d'organisation (p. ex. division) [] : E-commerce widget
Nom usuel (p. ex. votre nom ou celui de votre serveur) [] : www.mydomain.csr
Adresse de courrier électronique [en option] :

Ce sont les renseignements que *thawte* va vérifier, veuillez donc vous assurer que ceux saisis dans votre CSR correspondent EXACTEMENT avec ceux de votre société.

Remarque : Il vous sera demandé de saisir la phrase de passe PEM (PEM – 'Privacy Enhanced Message'). (Il s'agit de celle que vous avez définie dans le fichier de clé privée généré au cours de l'étape précédente.)

Remarque importante

Le terme "nom usuel" appartient à la terminologie X.509 et est le nom qui distingue le mieux le certificat et qui le lie à votre organisation. Dans le cas des certificats SSL, entrer le nom exact de l'hôte et du domaine que vous voulez sécuriser.
Une des erreurs les plus fréquentes consiste à mettre un nom de domaine incorrect dans le champ Nom usuel du fichier CSR. Un certificat est lié au nom pour lequel il a été délivré, donc assurez-vous que ce champ est rempli avec le nom exact de domaine pleinement qualifié (FQDN – 'fully qualified domain name') que vous utiliserez pour accéder à la partie sécurisée de votre site. Vous NE DEVEZ PAS inclure la partie 'http://' dans l'URL, ni aucun répertoire situé sous ce domaine. Par exemple, si votre page de paiement est accédée via https://secure.mydomain.com/checkout, vous ne devrez inclure que secure.mydomain.com dans le champ Nom usuel.

Le fichier CSR créé ci-dessus est acheminé vers un fichier appelé www.mydomain.csr et si vous consultez le contenu du fichier, il devrait ressembler à ce qui suit:


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


Pour voir le fichier CSR, utilisez l'une des commandes suivantes:
cat www.mydomain.csr
vi www.mydomain.csr

Vous venez tout juste de terminer les trois étapes fondamentales qui vous permettront de demander un certificat SSL de *thawte*.

5. Utilisez un certificat de test

Pour vous familiariser avec le fonctionnement d'un certificat de *thawte* sur un serveur Apache, vous pouvez mettre en place un certificat de test sur votre serveur en utilisant un certificat de test de *thawte*.

Dans cette étape, nous ferons la supposition que SSL a été configuré sur Apache. Si ce n'est pas le cas, veuillez vous reporter à la section 7 pour régler la configuration avant de continuer.

Etant donné que ces certificats sont seulement prévus pour des tests et des évaluations, ils fourniront un cryptage, mais si une session SSL est établie avec votre serveur ayant un certificat de test installé, un message d'avertissement sera affiché. Ce message informe l'utilisateur se connectant que le certificat n'est pas vérifié (not trusted), et que dans ce cas l'intégrité du site ne peut être garantie.

Ces certificats sont prévus pour que vous puissiez tester la configuration de votre serveur avant d'acheter un certificat vérifié (trusted) auprès d'une autorité de certification (CA – 'Certification Authority').

Ils généreront des erreurs avec les navigateurs pour lesquels le certificat racine requis n'a pas été inséré manuellement.

Vous pouvez faire en sorte que votre navigateur "valide" (trust) ce certificat de test en insérant la racine requise dans votre navigateur. Suivez les instructions fournies par l'assistant d'installation (Wizard) pour installer le certificat racine du test CA *thawte* en cliquant sur : http://www.thawte.com/roots/index.html

Nos certificats de test sont valides pour une durée de 21 jours et ce service est fourni avec ABSOLUMENT AUCUNE GARANTIE !

Vous pouvez demander un certificat de test de *thawte* en ligne sur : http://www.thawte.com/ucgi/gothawte.cgi?a=w46840168607049000

Il vous sera demandé de copier et coller votre Requête de Signature de Certificat dans la zone de texte proposée sur la page du Système de Certificat de Test.

Remarque : vous devrez copier et coller la CSR, y compris tous les tirets et les déclarations complètes des lignes BEGIN et END.

Le certificat de test sera généré immédiatement, se basant sur la CSR fournie et vous pourrez le voir sur la page suivante. Sauvegardez le certificat de test dans un fichier nommé www.mydomain.com.crt.

Jusqu'à présent, vous avez créé trois fichiers:

www.mydomain.key
-la clé privée RSA

www.mydomain.csr
-la Requête de Signature de Certificat

www.mydomain.crt
- le fichier du certificat de test de *thawte*

6. Demandez un certificat vérifié (trusted)

Les certificats SSL de *thawte* sont demandés en ligne sur: https://www.thawte.com/buy/

Pendant le processus de demande de certificat, il vous sera demandé de copier et coller votre Requête de Signature de Certificat (CSR) dans une zone de texte sur le formulaire d'inscription en ligne.

Remarque: vous devrez copier et coller la CSR, y compris les tirets et les déclarations complètes des lignes BEGIN et END.

Important

Veuillez vous assurer que vous êtes en train de soumettre la CSR correcte, si vous en avez généré plus d'une. Vous pouvez vérifier votre CSR avec la commande suivante:

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

Vous devrez nous fournir toutes les informations demandées pendant le processus d'inscription et nous envoyer les documents justifiant votre identité ou celle de votre société (un certificat d'enregistrement de société par exemple). Vous pouvez voir les instructions détaillées pour l'obtention d'un certificat SSL de *thawte* à l'adresse: http://www.thawte.com/support/docs.html

Une fois que vous avez terminé le processus de demande en ligne, *thawte* entreprendra un certain nombre de démarches pour vérifier votre identité et les renseignements que vous avez fournis dans la CSR. *thawte* réalise un nombre considérable de vérifications de données avant de délivrer un certificat. Par conséquent, cela peut prendre quelques jours pour vérifier l'identité et les renseignements de votre société, et de délivrer le certificat.

Pendant la période de vérification, vous pouvez suivre la progression de votre demande sur votre page d'état (status page) personnelle à l'adresse: http://www.thawte.com/cgi/server/status.exe

Si vous avez des questions pendant cette période, vous pouvez contacter le représentant du service client affecté à votre demande. Les coordonnées de votre représentant peuvent être trouvées sur votre page d'état à l'URL ci-dessus sous le titre "*thawte* Contact Person" (Personne de contact chez *thawte*).

7. Configuration SSL sur Apache

Avant d'installer des certificats de test ou "vérifiés" (trusted), vous devrez configurer votre serveur web Apache.

Les 'Directives' sont utilisées pour dire à Apache exactement comment il doit se comporter dans certaines situations, et ce depuis comment certains contenus doivent être gérer jusqu'à spécifier le nom de votre serveur à Apache.

Mod_ssl fournit les directives utilisées pour configurer le support SSL sur Apache, et les directives les plus souvent utilisées sont celles listées ci-dessous :

SSLCACertificateFile - spécifie le chemin vers un fichier qui contient les certificats racines CA.

SSLCertificateFile - spécifie l'emplacement du certificat SSL qui doit être utilisé par une machine spécifique.

SSLCertificateKeyFile - chemin vers la clé privée qui correspond au fichier mentionné dans la directive précédente.

SSLEngine - cette directive détermine si le protocole SSL est "activé" (on) ou non pour un serveur/hôte virtuel spécifique.

Mod_ssl fournit toute une série de directives qui vous permettent de configurer votre serveur en fonction de vos besoins spécifiques. Pour obtenir une liste complète des directives SSL que fournit Mod_ssl, veuillez consulter la documentation Mod_ssl: http://www.modssl.org/docs/2.2/ssl_reference.html

Pour configurer Apache pour SSL, vous devrez mettre à jour votre fichier "httpd.conf" pour chercher un nouveau certificat. Ouvrez le fichier de configuration "httpd.conf" et assurez-vous que vous avez les directives "SSLCertificateFile" et "SSLCertificateKeyFile" associées avec les chemins de fichier corrects.

Par exemple, si votre certificat se trouve dans le répertoire "/usr/local/ssl/certs/" et votre clé privée dans le répertoire "/usr/local/ssl/private/", vous aurez ce qui suit dans votre fichier "httpd.conf" :

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

Vous devrez également vous assurer que votre serveur Apache ainsi que les éventuels pare-feu ou routeurs installés écoutent sur le port 443 et activer SSL avec les directives "SSLEngine on" ou SSLEnable dans ModSSL ou Apache-SSL respectivement.

8. Installez votre certificat

Une fois que le certificat a été émis, vous pourrez le télécharger depuis votre page d'état (Status page) en cliquant sur le bouton "Fetch Certificate" (Rapporter le certificat qui n'apparaît que lorsque le certificat a été émis). Sauvegardez-le dans le répertoire opportun dans votre fichier "httpd.conf", ceci rendra la gestion de la clé et du certificat plus facile.

Par souci d'uniformité, il est conseillé de sauvegarder le certificat dans un fichier appelé "www.mydomain.com.crt". Le certificat est stocké indéfiniment dans la base de données de *thawte*, et peut-être téléchargé à nouveau à tout moment.

Si nous supposons que vous avez configuré votre serveur web, vous n'aurez désormais pas besoin de modifier votre fichier de configuration. Il vous suffit de simplement copier le fichier de votre vrai certificat (vérifié- trusted) par-dessus le certificat de test en effaçant ce dernier.

Une fois que votre certificat a été émis, vous pouvez ouvrir le fichier de configuration d'Apache et installer votre certificat, ainsi que configurer votre environnement SSL.

Le certificat ressemblera à quelque chose comme ça:

-----BEGIN CERTIFICATE-----
MIIDBTCCAm6gAwIBAgIDcxV2MA0GCSqGSIb3DQEBBAUAMIGHMQswCQYDVQQGEwJaQTEi
MCAGA1UECBMZRk9SIFRFU1RJTkcgUFVSUE9TRVMgT05MWTEdMBsGA1UEChMUVGhhd3RI
ENlcnRpZmljYXRpb24xFzAVBgNVBAsTDlRFU1QgVEVTVCBURVNUMRwwGgYDVQQDExNUaG
F3dGUgVGVzdCBDQSBSb290MB4XDTAyMTEwNTemJhDUzMloXDTAyMTEyNjE0MDUzMlowgd8
xFDASBgNVBAMTC3d3dy5jcmRiLmJlMRswGQYDVQQLHhIAQwBPAEwAVABBAAarfJsdQBTAFQx
czBxBgNVBAoeagBDAGEAcAAgAEcAZQBtAGkAbgBpACAAVABlAGwAZQBjAG8AbQAgAE0BZq
BkAGkAYQAgACYAIABOAGUAdAB3AG8AcgBrAHMAIABCAGUAbABnAGkAdQB
BkRpZWdlbTeCxMBUGA1UECBMOVmxhYW1zIEJyYWJhbnQxCzAJBgNVBAYTAkJFMIGfMA0GC
SqGsIb3DQEBAQUAA4GNADCBiQKBgQDaNm3HPzG6Rbk5Am0HI6JFHoDQku2/YmVMGbZk5A
HeR13QxIP7UVa08/k8qR3B7B0mfbxaNIxdwV9c7c1z4mZYQRfAeryoW4sU2jh1OHc4Cin+i9UarkH
m8WnUnlcVZEnJrySdfLZNuxtbknXBNkca8rk6tnIbXodD3gEQJBMJtQIDAQABoyUwIzAT
-----END CERTIFICATE-----

Quand il est affiché avec OpenSSL en utilisant la commande suivante:

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

le fichier du certificat contient les renseignements suivants:

```
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
```

Ce certificat est lié à la clé privée que vous avez créée plus tôt (www.mydomain.com.key) et ne peut être “joint” qu’à cette clé. Si vous perdez la clé privée à laquelle un certificat est lié, votre certificat est inutilisable.

Vous devez maintenant pointer la directive SSLCertificateFile vers l’emplacement où vous avez choisi de sauvegarder ce fichier, habituellement dans le même répertoire que celui de votre fichier “httpd.conf”, /etc/apache ou similaire :

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

Vous devez également dire à Apache quel fichier de clé doit être utilisé pour ce certificat, donc n’oubliez pas de pointer la directive SSLCertificateKeyFile vers la clé privée pour ce certificat :

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

Les autorités de certification (CA - Certificate Authorities) signent leurs certificats avec une racine de premier niveau et toute application souhaitant vérifier le certificat d’un utilisateur final doit être capable de comparer le certificat de l’utilisateur avec le certificat racine utilisé par l’autorité de certification. ModSSL utilise SSLCACertificateFile pour faire ceci, et ceci est inclus avec ModSSL. Vous ne devriez pas avoir besoin d’adapter le contenu de ce fichier.

SSLCACertificateFile: /etc/apache/ca –bundle.crt

Donc, maintenant que vous avez configuré toutes ces directives SSL, cela devrait fonctionner, n’est-ce pas ? Et bien non. Il y a une directive supplémentaire qui nécessite notre attention - SSLEngine. Cette directive a deux arguments, “on” ou “off”. Evidemment, vous souhaiteriez que SSL soit sur “activé” (on):

SSLEngine on

La directive ci-dessus peut être utilisée dans un contexte de serveur global ou dans le cadre du conteneur <VirtualHost> (Hôte virtuel).

En supposant que vous utilisez le certificat sur un hôte virtuel configuré correctement, vous devriez avoir une configuration qui ressemble à ceci:

```
<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/ca_bundle.crt
SetEnvIf User-Agent ".*MSIE.*" nokeepalive ssl-unclean-shutdown
</VirtualHost>
```

Vous remarquerez que dans le conteneur <VirtualHost> un port spécifique, le port 443, est mentionné. Il s’agit du port SSL par défaut et il est configuré en utilisant la directive globale ‘Listen’ (Écoute). Par défaut, ‘Listen 80’ est configuré dans le fichier “httpd.conf”, et tout ce que vous avez à faire maintenant est d’ajouter ‘Listen 443’ sur une nouvelle ligne. Il est préférable de grouper toutes les directives semblables.

9. Sécurisation des hôtes virtuels

Si vous avez des hôtes virtuels sécurisés, chacun d'entre eux aura besoin de sa propre adresse IP, étant donné que SSL ne supporte pas les hôtes virtuels basés sur des noms.

SSL ne peut pas être configuré sur des hôtes virtuels à base de nom, sauf si ces hôtes virtuels utilisent des ports SSL différents.

Notez que la configuration démontrée ci-dessus est très élémentaire et que vous pouvez inclure beaucoup d'autres directives SSL qui vous permettent d'adapter votre environnement SSL.

Une fois que le certificat a été installé et que SSL a été configuré correctement, vous devrez redémarrer tout le serveur et pas seulement le démon. Ceci garantit que l'installation prend effet. L'emplacement des scripts qui démarreront Apache sera différent pour les diverses distributions de Linux, nous ferons donc la supposition qu'il y a un script nommé 'apache' dans /etc/init.d/ qui appelle un script dans /usr/sbin/ appelé 'apachectl.'

widget@mydomain-pc/etc/init.d/apache start

Vous devriez maintenant pouvoir accéder en sécurité à votre machine et afficher les renseignements du certificat. Vous saurez si la session SSL a été établie si un cadenas doré apparaît sur la barre d'outil inférieure de votre navigateur. En double-cliquant sur cette icône, les renseignements sur le certificat s'afficheront.

10. URL utiles

Les problèmes habituels qui surviennent avec Apache-SSL et Apache ModSSL sont traités dans nos FAQ (questions fréquentes): http://www.thawte.com/support/keygen/index.html

Le guide de génération de clé pour Apache-SSL est disponible à l'adresse URL suivante: http://www.thawte.com/support/keygen/index.html

Le guide de génération de clé pour Apache ModSSL est disponible à l'adresse URL suivante: http://www.thawte.com/support/keygen/index.html

Le processus d'inscription de certificat pour les certificats de serveur web et les certificats Supercerts 128 bits démarre à l'adresse URL: https://www.thawte.com/buy/

Instructions pour générer un certificat de test:
http://www.thawte.com/ucgi/gothawte.cgi?a=w46840168607049000

Où télécharger le certificat de test CA racine de $thawte$:
https://www.thawte.com/roots/index.html

11. Quel rôle joue *thawte*?

thawte est une autorité de certification (CA - Certification Authority) qui délivre des certificats de serveur web SSL à des organisations ou à des personnes dans le monde entier. *thawte* vérifie que la société commandant le certificat est une organisation enregistrée et que la personne de la société qui a commandé le certificat est autorisée à le faire.

thawte vérifie également que la société en question est propriétaire du domaine approprié. Les certificats numériques de *thawte* interagissent facilement avec Apache et avec les derniers logiciels de Microsoft et Netscape, de sorte que vous pouvez être tranquille et assuré que votre achat d'un certificat numérique de thawte permettra à vos clients d'être confiants en votre système et son intégrité – ils se sentiront en sécurité en commerçant en ligne.

12. La valeur de l'authentification

L'information constitue un atout primordial dans vos affaires. Pour assurer l'intégrité et la sécurité de vos informations, il est important d'identifier avec qui vous êtes en train de traiter, et d'être sûr que les données que vous recevez sont fiables. L'authentification peut aider à établir la confiance entre des parties impliquées dans toutes types de transactions en abordant un ensemble unique de risques de sécurité comprenant :

La mystification : Le faible coût de la conception d'un site web et la facilité avec laquelle des pages existantes peuvent être copiées font qu'il est trop facile de créer des sites webs illégitimes qui semblent avoir été publiés par des organisations reconnues. De fait, des escrocs ont illégalement obtenu des numéros de cartes bancaires en réalisant des devantures ayant un aspect professionnel qui simulaient des commerces légitimes.

Les actions non autorisées : Un concurrent ou un client mécontent peut endommager votre site web de telle sorte qu'il fonctionne mal ou refuse de servir des clients potentiels.

La communication d'informations non autorisée : Quand des informations de transaction sont transmises "au clair", des pirates informatiques peuvent intercepter les transmissions pour obtenir des informations sensibles de vos clients.

Altération de données : Le contenu d'une transaction peut être intercepté et altéré en route, de manière malicieuse ou accidentelle. Des noms d'utilisateurs, des numéros de cartes bancaires et des sommes d'argent transmises "au clair" sont vulnérables et peuvent être altérées.

13. Contactez *thawte*

Si vous avez des questions supplémentaires à propos du contenu de ce guide ou des produits et services de *thawte*, veuillez contacter un conseiller commercial :

Courrier électronique : sales@thawte.com
Téléphone : +27 21 937 8902
Fax: +27 21 937 8967

14. Glossaire

Apache
Apache, comme il est généralement su, est un projet de la fondation Apache Software qui a pour objectif de produire des serveurs web sûrs, efficaces et extensibles qui fournissent des services http en synchronisation avec les standards http habituels.

jakarta.apache.org

Autorité de certification
Une autorité de certification (CA – Certification authority) est une organisation (telle que *thawte*) qui délivre et gère des certificats de sécurité et des clés publiques pour le cryptage de messages.

Clé privée
Une clé privée est un code numérique utilisé pour décrypter des messages cryptés avec une unique clé publique correspondante. L'intégrité du cryptage dépend de ce que la clé privée reste secrète.

Clé publique
Une clé publique est un code numérique qui permet un cryptage de messages transmis au propriétaire de l'unique clé privée correspondante. La clé publique peut circuler librement sans pour autant compromettre le cryptage tout en augmentant l'efficacité et la commodité de permettre une communication cryptée.

Cryptographie asymétrique
C'est une méthode cryptographique utilisant une paire de clés publique et privée combinée, pour crypter et décrypter des messages. Pour envoyer un message crypté, un utilisateur crypte un message avec la clé publique du récipient. Après réception, le message est décrypté avec la clé privée du récipient.

L'utilisation de clés différentes pour réaliser les fonctions de cryptage et de décryptage est connue comme étant une fonction unidirectionnelle de trappe, c'est-à-dire que la clé publique est utilisée pour cryptée le message, mais ne peut pas être utilisée pour décrypter le même message. Sans connaître la clé privée, il est pratiquement impossible d'inverser cette fonction quand un cryptage puissant et moderne est utilisé.

Cryptographie symétrique
C'est une méthode de cryptage où la même clé est utilisée pour le cryptage et le décryptage. Cette méthode est handicapée par les risques de sécurité impliqués par la distribution sûre de la clé étant donnée qu'elle doit être communiquée à la fois au récepteur et à l'émetteur sans qu'elle soit divulguée à des tiers.

Mod_ssl
Etant donné qu'Apache est une application modulaire, une de ses caractéristiques les plus puissantes est qu'elle est hautement adaptable avec des modules tiers qui étendent ses fonctionnalités. L'un des modules les plus populaires créé pour Apache (et essentiel dans le monde de l'e-commerce) est Mod_ssl. Mod_ssl est un module qui fournit un support SSL pour Apache ; sans Mod_ssl, Apache ne peut pas répondre aux requêtes SSL car il ne saurait pas quoi en faire.

OpenSSL
OpenSSL est une valise cryptographique qui mets en œuvre les protocoles SSL Secure Sockets Layer (SSL v2/v3) et TLS Transport Layer Security (TLS v1) et les standards de cryptages correspondants qui sont requis par ces protocoles.

www.openssl.org

OpenSSL fournit essentiellement la plate-forme sur laquelle Mod_ssl s'exécute, et doit être installé sur une machine où Apache + Mod_ssl vont être utilisés. Sans OpenSSL, Mod_ssl ne sera pas d'une grande utilité. Toute application/utilitaire qui requière des aptitudes de cryptage utilisera les bibliothèques cryptographiques OpenSSL.

Requête de Signature de Certificat (CSR – 'Certificate signing request')
Une CSR est une clé publique que vous générez sur votre serveur et qui valide les informations spécifiques à l'ordinateur concernant votre serveur web et de votre organisation lorsque vous demandez un certificat de *thawte*.