Sécurisez votre

serveur Web Internet Information Services de Microsoft (MS IIS)

avec un certificat numérique de thawte

UN GUIDE ÉTAPE PAR ÉTAPE , pour tester, acheter et utiliser un certificat numérique de thawte sur votre serveur web Microsoft IIS.

Microsoft Internet Information Server

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 web Internet Information Services de Microsoft (MS IIS). Les meilleures pratiques de mises 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.

Les informations dans ce guide s'appliquent à:

Microsoft Internet Information Services version 4.0
Microsoft Internet Information Services version 5.0
Microsoft Internet Information Services version 5.1
Microsoft Internet Information Services version 6.0

2. Configuration du système

Vous devez avoir installé le Service Pack le plus récent pour la version de MS IIS que vous utilisez.

Conseil pour le Service Pack:
Si vous utilisez MS IIS 4.0, vous devriez avoir installé le Service Pack 6a.
Si vous utilisez MS IIS 5.0 ou MS IIS 5.1, vous devriez avoir installé le Service Pack 3.

Pour plus d'informations sur les derniers Services Packs de MS IIS, veuillez consulter le site web de support de Microsoft du url suivante:
http://support.microsoft.com/default.aspx?scid=FH;[LN];sp&

SITES WEBS UTILES:

http://support.microsoft.com/default.aspx?scid=fh;en-us;iis
http://support.microsoft.com/default.aspx?scid=fh;EN-US;iis50
http://support.microsoft.com/default.aspx?scid=fh;EN-US;iis60

3. Générez votre paire clé privée et demande de certificat (CSR - Certificate Signing Request)

Avant de commencer le processus d'obtention d'un certificat, vous devez générer une paire clé privée et CSR à partir du serveur web. Ceci est réalisé via la console d'administration d'IIS (IIS doit être préalablement installé pour pouvoir générer une paire clé privée et CSR à partir du serveur web).

Une CSR est en fait une clé publique que vous générez sur votre serveur et qui valide les informations spécifiques à l'ordinateur à propos de votre serveur web et de votre organisation lorsque vous demandez un certificat vérifié (trusted) de *thawte*.

Les ID numériques utilisent une technologie appelée cryptographie à clé publique. Avant de pouvoir vous inscrire pour un certificat, une clé privée et une demande de certificat (CSR) doivent être générées depuis le serveur. La clé publique, également connue comme requête de signature de certificat (CSR - Certificate Signing Request), est la clé qui doit être envoyée à *thawte*.

La clé privée doit rester sur le serveur et ne devrait jamais être diffusée dans le domaine public. *thawte* n'a pas accès à votre clé privée. Elle est générée localement sur votre serveur et n'est jamais transmise à *thawte*. L'intégrité de votre ID numérique dépend du fait que votre clé privée soit exclusivement contrôlée et connue par vous.

Une CSR ne peut pas être générée sans générer un fichier de clé privée de même qu'une clé privée ne peut pas être générée sans générer un fichier CSR. Les deux sont générés simultanément via l'assistant d'installation sur le serveur web.

Normalement, il vous sera demandé de saisir les informations suivantes sur votre organisation de manière à générer la paire clé privée et CSR depuis le serveur web :

- Nom de l'organisation
- Unité de l'organisation
- Code du pays
- Département ou région
- Ville/Localité
- Nom usuel*

*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 de serveur web SSL et des certificats SuperCerts 128 bits, entrez les noms exacts d'hôte et de domaine que vous voulez sécuriser. Cela peut également être le serveur racine ou le nom intranet de votre organisation.

Exemple: Si vous souhaitez sécuriser www.mydomain.com, vous devrez alors entrer les noms exacts d'hôte (www) et de domaine dans ce champ. Si vous entrez mydomain.com, le certificat alors délivré ne fonctionnera sans erreur que pour ce nom de domaine exact. Une erreur se produira lorsque vous ou vos utilisateurs accéderont au domaine en tant que www.mydomain.com

- Pour générer une paire clé privée et CSR avec MS IIS 4.0, veuillez suivre les étapes indiquées à l'URL suivante : http://www.thawte.com/support/keygen/index.html
- Pour générer une paire clé privée et CSR avec MS IIS 5.0 ou MS IIS 5.1,veuillez suivre les étapes indiquées à l'URL suivante : http://www.thawte.com/support/keygen/index.html
- Pour générer une paire clé privée et CSR avec MS IIS 6.0, veuillez suivre les étapes indiquées à l'URL suivante : http://www.thawte.com/support/keygen/index.html

Le fichier CSR créé ci-dessus est enregistré en format texte et si vous l'éditez il doit être semblable 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-----

4. Sauvegardez le fichier de votre clé privée

Remarque importante :

De loin le problème le plus souvent rencontré par les utilisateurs au cours de cette procédure est associé aux clés privées du fait que les instructions d'exportation de la clé privée ne font pas partie de l'application d'installation au moment de générer la CSR. Le principal problème est que beaucoup d'utilisateurs ne savent pas que la clé privée est générée en même temps que la clé publique (c'est seulement que la clé privée n'est pas visible pour l'utilisateur).

Si vous perdez la clé privée ou n'y avez plus accès ou perdez le mot de passe utilisé pour protéger l'exportation du fichier de la clé privée, vous ne pourrez plus utiliser le certificat que nous vous avons délivré. Pour vous assurez que cela n'arrive jamais, nous vous conseillons de réaliser une sauvegarde du fichier de clé privée sur disquette, et de noter le mot de passe utilisé pour protéger l'exportation de la clé privée.

Pour sauvegarder votre clé privée avec MS IIS 4.0, veuillez suivre les étapes indiquées dans la solution suivante de la base de connaissances :
http://kb.thawte.com/thawte/thawte/esupport.asp?id=vs5500

Pour sauvegarder votre clé privée avec MS IIS 5.0 ou MS IIS 5.1, veuillez suivre les étapes indiquées dans la solution suivante de la base de connaissances :
http://kb.thawte.com/thawte/thawte/esupport.asp?id=vs2065

Pour sauvegarder votre clé privée avec MS IIS 6.0, veuillez suivre les étapes indiquées dans la solution suivante de la base de connaissances :
http://kb.thawte.com/thawte/thawte/esupport.asp?id=vs22515

5. Demandez un certificat de test

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

Nos certificats de test gratuits sont valides pendant 21 jours et ce service est fourni AVEC ABSOLUMENT AUCUNE GARANTIE !

Vous pouvez demander un certificat de test de *thawte* en ligne depuis : http://www.thawte.com/ucgi/gothawte.cgi?a=w46840168637049000

Il vous sera demandé de copier et coller votre CSR 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 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.

Copiez et collez le certificat, y compris les tirets et les déclarations complètes des lignes BEGIN et END, dans le bloc-notes, comme dans l'exemple ci-dessous.

Sauvegardez le certificat de test dans un fichier nommé :
testcert_mydomain.crt
Le fichier de certificat créé ci-dessus doit être semblable à ce qui suit :


```
-----BEGIN CERTIFICATE-----
MIIDDDCCAnWgAwIBAgIDAMpQMA0GCSqGSIb3DQEBBAUAMIGHMQswCQYDVQQGEwJa
QTEiMCAGA1UECBMZRk9SIFRFU1RJTkcgUFVSUE9TRVMgT05MWTEdMBsGA1UEChMU
VGhhd3RlIENlcnRpZmljYXRpb24xFzAVBgNVBAsTDlRFU1QgVEVTVCBURVNUMRww
GgYDVQQDExNUaGF3dGUgVGVzdCBDQSBSb290MB4XDTA0MDEyOTEzMTkyMVoXDTA0
MDIxOTEzMTkyMVowgZAxGTAXBgNVBAMTEHd3dy50ZXN0Y2VydC5jb20xCzAJBgNV
BAYTAlVTMRcwFQYDVQQIEw5Ob3J0aCBDYXJvbGluYTEQMA4GA1UEBxMHUmFsZWln
aDEeMBwGA1UEChMVTXkgVGVzdCBDb25zdWx0aW5nIGNjMRswGQYDVQQLExJUZXN0
aW5nIERlcGFydG1lbnQwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAJWPKgts
znqA6BoMkpryFKNRdJHwPisa7KrdpaQiqdnkCJIZZ/SQBVhMZAyLtjeKXeZsoHvt
/aUcXRIEGZ0TvHvpCzblCtog4WO+Ten9eEwgjLGXdTN07WNZIVQKAQuQdEVGZzio
tBLDwsol2TAwIkrQ9XyzpLeN8Hes3Vza9qUnAgMBAAGjezB5MAwGA1UdEwEB/wQC
MAAwMwYDVR0fBCwwKjAooCagJIYiaHR0cDovL3d3dy50aGF3dGUuY29tL3Rlc3Rj
ZXJ0LmNybDA0BgNVHSUELTArBggrBgEFBQcDAQYIKwYBBQUHAwIGCWCGSAGG+EIE
AQYKKwYBBAGCNwoDAzANBgkqhkiG9w0BAQQFAAOBgQAVqvhkJAAhPA7XPbDcxTz4
Vtr4Qi/wBFmnvDotv4jSF3CXQrHT6wrlxUVlvwptncG3j2emtdu5yfR68jqwwLEP
l7Z44limQBjwMT/4/tkPqMy3cqas0+mYIehQBqF25DPypz7UIoQXFeXF9B/vffD2
9l/pXxEEus1Skv8XxJZkqA==
-----END CERTIFICATE-----
```

6. Installez un certificat de test *thawte*

Pour installer un certificat avec MS IIS 4.0, veuillez suivre les étapes indiquées dans la solution suivante de la base de connaissances : http://kb.thawte.com/thawte/thawte/esupport.asp?id=vs8385

Pour installer un certificat avec MS IIS 5.0 ou MS IIS 5.1, veuillez suivre les étapes indiquées dans la solution suivante de la base de connaissances : http://kb.thawte.com/thawte/thawte/esupport.asp?id=vs7547

Pour installer un certificat avec MS IIS 6.0, veuillez suivre les étapes indiquées dans la solution suivante de la base de connaissances : http://kb.thawte.com/thawte/thawte/esupport.asp?id=vs22518

Une fois installé, veuillez procéder à l'étape 9, Configurez le certificat pour son utilisation avec MS IIS.

Remarques pour les certificats de test *thawte* :

Le certificat de test fournira un cryptage, mais si une session SSL est établie sur votre serveur avec un certificat de test installé, un message d'avertissement sera affiché. Ce message informe l'utilisateur en train de se connecter que le certificat n'est pas vérifié (not trusted), et que dans ce cas l'intégrité du site ne peut pas être garantie.

Vous pouvez faire en sorte que votre navigateur vérifie ce certificat de test en cliquant sur http://www.thawte.com/roots/index.html puis en suivant les instructions fournies par l'assistant d'installation du certificat CA Racine de Test *thawte*.

7. Demandez un certificat *thawte* vérifié (trusted)

Remarque importante :

Vous devrez suivre les étapes indiquées dans les étapes 3 et 4 afin de pouvoir demander un certificat vérifié (trusted) de *thawte*.

Vous ne devez PAS obtenir un certificat de test puis demander un certificat vérifié à *thawte* en utilisant LA MÊME PAIRE CSR ET CLÉ PRIVÉE. La procédure de remplacement d'un certificat de test par un certificat vérifié qui utilise les mêmes Clé privée/CSR n'est pas une procédure facile et n'est donc pas recommandée.

Les méthodes de certification de *thawte* sont du plus haut niveau. Nous croyons que des procédures d'authentification et de vérification excellentes sont absolument essentielles afin d'assurer la confiance sur l'Internet.

Les certificats de serveur web SSL et SuperCerts 128 bits de *thawte* peuvent être demandés en ligne depuis la page https://www.thawte.com/buy/

Pendant le processus de demande de certificat, il vous sera demandé de copier et coller votre CSR (Certificate Signing Request) 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.

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). Des informations supplémentaires sur l'obtention des certificats de serveur web SSL et SuperCerts 128 bits de *thawte* sont disponibles à la page : http://www.thawte.com/support/docs.html

Une fois que vous avez terminé le processus de demande en ligne, *thawte* démarrera un certain nombre d'étapes pour vérifier votre identité et les renseignements que vous avez fournis dans la CSR. *thawte* réalise une quantité considérable de vérifications des données avant de délivrer un certificat. Par conséquent, cela peut prendre quelques jours pour vérifier l'identité et les renseignements de votre société, et 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 :
https://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 trouvés sur votre page d'état à l'URL ci-dessus sous " *thawte* Contact Person" (Personne de contact chez *thawte*).

Une fois votre identité et les renseignements de la CSR vérifiés, le certificat sera délivré. Le contact technique indiqué pour la demande recevra un courrier électronique avec un lien depuis lequel le certificat peut être téléchargé, une fois qu'il a été délivré. Copiez et collez le certificat, y compris les tirets et les déclarations complètes des lignes BEGIN et END, dans le bloc-notes, comme dans l'exemple ci-dessous.

Sauvegardez le certificat délivré vers un fichier nommé :
realcert_mydomain.crt

Remarque : Il est préférable que vous assigniez au certificat un nom qui le distinguera du certificat de test demandé auparavant.

Le fichier du certificat créé ci-dessus doit être semblable à ce qui suit :

-----BEGIN CERTIFICATE-----
MIIDDDCCAnWgAwIBAgIDAMpQMA0GCSqGSIb3DQEBBAUAMIGHMQswCQYDVQQGEwJa
QTEiMCAGA1UECBMZRk9SIFRFU1RJTkcgUFVSUE9TRVMgT05MWTEdMBsGA1UEChMU
VGhhd3RlIENlcnRpZmljYXRpb24xFzAVBgNVBAsTDlRFU1QgVEVTVCBURVNUMRww
GgYDVQQDExNUaGF3dGUgVGVzdCBDQSBSb290MB4XDTA0MDEyOTEzMTkyMVoXDTA0
MDIxOTEzMTkyMVowgZAxGTAXBgNVBAMTEHd3dy50ZXN0Y2VydC5jb20xCzAJBgNV
BAYTAlVTMRcwFQYDVQQIEw5Ob3J0aCBDYXJvbGluYTEQMA4GA1UEBxMHUmFsZWln
aDEeMBwGA1UEChMVTXkgVGVzdCBDb25zdWx0aW5nIGNjMRswGQYDVQQLExJUZXN0
aW5nIERlcGFydG1lbnQwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAJWPKgts
znqA6BoMkpryFKNRdJHwPisa7KrdpaQiqdnkCJIZZ/SQBVhMZAyLtjeKXeZsoHvt
/aUcXRIEGZ0TvHvpCzblCtog4WO+Ten9eEwgjLGXdTN07WNZIVQKAQuQdEVGZzio
tBLDwsol2TAwIkrQ9XyzpLeN8Hes3Vza9qUnAgMBAAGjezB5MAwGA1UdEwEB/wQC
MAAwMwYDVR0fBCwwKjAooCagJIYiaHR0cDovL3d3dy50aGF3dGUuY29tL3Rlc3Rj
ZXJ0LmNybDA0BgNVHSUELTArBggrBgEFBQcDAQYIKwYBBQUHAwIGCWCGSAGG+EIE
AQYKKwYBBAGCNwoDAzANBgkqhkiG9w0BAQQFAAOBgQAVqvhkJAAhPA7XPbDcxTz4
Vtr4Qi/wBFmnvDotv4jSF3CXQrHT6wrlxUVlvwptncG3j2emtdu5yfR68jqwwLEP
l7Z44IimQBjwMT/4/tkPqMy3cqas0+mYIehQBqF25DPypz7UloQXFeXF9B/vffD2
9l/pXxEEus1Skv8XxJZkqA==
-----END CERTIFICATE-----

8. Installez un certificat *thawte* vérifié (trusted)

Une fois que le certificat vérifié a été délivré, 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 délivré.

Pour obtenir des instructions détaillées sur comment télécharger votre certificat de confiance, veuillez vous reporter aux instructions décrites dans la solution suivante de la base de connaissances de thawte :
http://kb.thawte.com/thawte/thawte/esupport.asp?id=vs7791

Remarque importante :

Ce certificat est lié à la clé privée que vous avez créée plus tôt dans l'étape 3, et ne peut être au joint qu'à cette clé privée.

Si vous perdez la clé privée à laquelle un certificat est lié ou le mot de passe utilisé pour protéger l'exportation du fichier de clé privée, le certificat qui vous a été délivré sera alors inutilisable.

Pour installer le certificat sur MS IIS 4.0, veuillez suivre les étapes indiquées dans la solution suivante de la base de connaissances :
http://kb.thawte.com/thawte/thawte/esupport.asp?id=vs8385

Pour installer le certificat sur MS IIS 5.0 ou MS IIS 5.1, veuillez suivre les étapes indiquées dans la solution suivante de la base de connaissances :
http://kb.thawte.com/thawte/thawte/esupport.asp?id=vs7547

Pour installer le certificat sur MS IIS 6.0, veuillez suivre les étapes indiquées dans la solution suivante de la base de connaissances :
http://kb.thawte.com/thawte/thawte/esupport.asp?id=vs22518

9. Configurez le certificat pour son utilisation avec MS IIS

Maintenant que le certificat a été installé, vous devrez activer le serveur ainsi que les firewalls ou les routeurs qui sont installés pour communiquer en toute sécurité.

Pour ce faire, activez le port SSL, qui est par défaut le port 443, puis attribuez une adresse IP unique pour votre certificat sur votre site web.

Le certificat n'est délivré et lié qu'au nom de domaine pleinement qualifié (nom usuel FQDN - Fully Qualified Domain Name), pour lequel le certificat a été délivré. Même s'il n'est pas lié à l'adresse IP assignée au site web, une adresse IP unique est requise pour chaque site web activé avec SSL, étant donné que SSL fonctionne avec des hôtes virtuels basés sur IP.

L'adresse IP attribuée au site web peut être modifiée et cela n'affectera pas du tout le certificat, pourvu qu'elle reste unique.

Remarque importante :

SSL ne fonctionne pas si vous utilisez des en-têtes hôtes, car ils sont inclus dans la demande cryptée. Ce n'est pas une limitation d'IIS, ce comportement est dû à sa conception.

Pour plus d'informations sur cette question, veuillez vous reporter à l'article de la base de connaissances de Microsoft :
http://support.microsoft.com/default.aspx?scid=kb;[LN];Q187504

Pour activer SSL sur MS IIS 4.0, suivre les instructions suivantes :

1. Depuis le groupe de programme « Serveur internet», ouvrir « Gestionnaire de clés/Key Manager».
2. Dans la fenêtre « Gestionnaire de clés/Key Manager», sélectionnez la clé sur laquelle votre certificat est installé.
3. Effectuez un clic droit sur la clé puis sélectionnez « Propriétés/Properties».
4. Dans la fenêtre « Pièces jointes au serveur/Server bindings», cliquez sur « Ajouter/Add».
5. Le champ « Adresse IP/IP Address » doit contenir l'adresse IP (saisi au clavier) du site web en question. Si vous n'avez qu'un seul site web, l'option par défaut « Tous les non assignés/Any unassigned port » pour votre adresse IP sera suffisante.
6. Sous « Numéro de port/Port number », cliquez sur le bouton radio à côté de « Numéro de port/Port number » puis ajoutez 443. Cliquez sur « OK » quand c'est terminé.
7. Depuis le menu « Ordinateurs/Computers », sélectionnez « Appliquer les modifications maintenant/Commit changes now » et quand il est demandé « Appliquer toutes les modifications maintenant/Commit changes now », sélectionnez « Oui/Yes ».

Pour activer SSL sur MS IIS 5.0, MS IIS 5.1 et MS IIS 6.0, suivez les instructions suivantes :

1. Dans l'onglet « Site Web/Website », le champ de l'adresse IP doit contenir l'adresse IP (saisie au clavier) du site web en question. Si vous n'avez qu'un seul site web, l'option par défaut « Tous les non assignés/Any unassigned port » pour votre adresse IP sera suffisante.

2. Cliquez sur le bouton « Avancés/Advanced » à côté du champ de l'adresse IP, assurez-vous que le numéro de port SSL est listé dans la section « Identités SSL multiples pour ce site web/Multiple identities for this Website ».

Vous pourrez maintenant accéder à votre machine en sécurité via : https://www.mydomain.com et afficher les renseignements de votre certificat.

Un cadenas doré apparaîtra sur la barre d'outil inférieure de votre navigateur lorsque la session SSL aura été établie.

10. Exportez le certificat *thawte* vérifié (trusted) avec la clé privée jointe après l'installation

Remarque importante :

Il est recommandé que vous fassiez une sauvegarde sur disquette du certificat installé avec le fichier de la clé privée en notant le mot de passe utilisé pour protéger l'exportation du fichier.

Ceci est fait comme mesure préventive pour vous assurer que si votre serveur se plante à cause de circonstances imprévues, vous ayez une sauvegarde de votre certificat ainsi que du fichier de la clé privée.

Pour sauvegarder le certificat avec la clé privée jointe sur MS IIS 4.0, veuillez vous reporter au URL suivante :
http://kb.thawte.com/thawte/thawte/esupport.asp?id=vs5500

Pour sauvegarder le certificat avec la clé privée jointe sur MS IIS 5.0 ou MS IIS 5.1, veuillez vous reporter au URL suivante :
http://kb.thawte.com/thawte/thawte/esupport.asp?id=vs1689

Pour sauvegarder le certificat avec la clé privée jointe sur MS IIS 6.0, veuillez vous reporter au URL suivante :
http://kb.thawte.com/thawte/thawte/esupport.asp?id=vs22520

11. URL utiles

Les problèmes habituels rencontrés avec MS IIS sont traités dans nos FAQ (questions fréquentes):

http://www.thawte.com/support/software/index.html

Guide de dépannage pour MS IIS 4:

http://kb.thawte.com/thawte/thawte/esupport.asp?id=vs6349

Guide de dépannage pour MS IIS 5:

http://kb.thawte.com/thawte/thawte/esupport.asp?id=vs12399

Les problèmes habituels rencontrés avec MS IIS utilisant des certificats de serveur web SSL thawte sont traités dans les FAQ (questions fréquentes) suivantes :

http://www.thawte.com/support/ssl/index.html

Les problèmes habituels rencontrés avec MS IIS utilisant des certificats SuperCerts 128-bits thawte sont traités dans les FAQ (questions fréquentes) suivantes :

http://www.thawte.com/support/sgc/index.html

12. Quel rôle joue *thawte* ?

thawte est une autorité de certification (CA - Certification Authority) qui délivre des certificats de serveur web SSL et SuperCerts 128-bits à des organisations ou à des personnes dans le monde entier. *thawte* vérifie que la société qui commandant le certificat est une organisation enregistrée et que la personne de la société qui a commande 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.

13. 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 tous 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 web 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.

14. Contacter *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

15. Glossaire

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.

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.

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.

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.

Infrastructure à clé publique (PKI - Public Key Infrastructure)
C'est une méthode pour échanger des informations en toute sécurité entre des organisations, des industries, des pays ou même dans le monde entier. Une PKI utilise la méthode de cryptage asymétrique pour crypter des ID et des documents ou des messages. (elle est également connue comme la méthode « clé privée/publique »). Une PKI démarre avec une autorité de certification (CA) telle que thawte, qui délivre et retire des certificats numériques (ID numériques) en authentifiant l'identité de personnes et d'organisations à travers un système public tel qu'internet.

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.