

Base de connaissance K.SSL

Générez votre CSR

Pour effectuer votre demande de certificat serveur, vous devez générer une CSR (Certificate Signing Request, ou Requête de Signature de Certificat en français) depuis le serveur sur lequel vous installez le certificat. Si votre serveur ne figure pas dans la liste, consultez la documentation de votre serveur ou contactez votre support technique.

Votre fichier CSR doit contenir les éléments suivants :

- nom du site à sécuriser
- Organisation
- Unité d'organisation
- Localité/ville
- Etat/Province/Département
- Pays

Vous ne pouvez utiliser l'adresse IP de votre site comme nom courant

Générer une CSR sous :

Editeur	Plateforme serveur
Apache	ApacheSSL
Microsoft	Microsoft IIS 6.0 Microsoft IIS 5.0 Microsoft IIS 4.0
Red Hat	Red Hat Linux Apache/SSL Server
Sun	Java Web Server 6.x Sun ONE

Base de connaissance K.SSL

Générez votre CSR

Apache – ApacheSSL

Pour générer une CSR sur votre serveur, vous devez générer une bi-clé.

L'utilitaire OpenSSL que vous utilisez pour créer la clé privée et la CSR est livré avec le toolkit OpenSSL et est habituellement installé sous /user/bin. Si vous l'avez installé ailleurs, vous devrez modifier ces instructions.

Etape 1 : Générer la clé privée :

Tapez la commande suivante :

```
openssl genrsa -des3 -out keynectis.key 1024
```

Cette commande va générer une clé privée RSA de 1024 bits et la stocker dans un fichier `keynectis.key`. Un mot de passe vous sera demandé, choisissez-en un sécurisé et mémorisez le, votre certificat sera inutilisable sans sa clé privée associée.

Etape 2 : Générer la CSR

Tapez la commande suivante :

```
openssl req -new -key keynectis.key -out keynectis.key.csr
```

Cette commande vous demandera les attributs x.509 de votre certificat. Entrez votre pays, état ou province, localité ou ville. Nous vous recommandons de renseigner votre nom de société comme il apparaît sur votre KBIS. L'unité d'organisation est facultative. Pour laisser ce champ en blanc, pressez la touche « Entrée » sur votre clavier

Entrez votre nom de domaine exact ainsi que le host que vous souhaitez sécuriser.

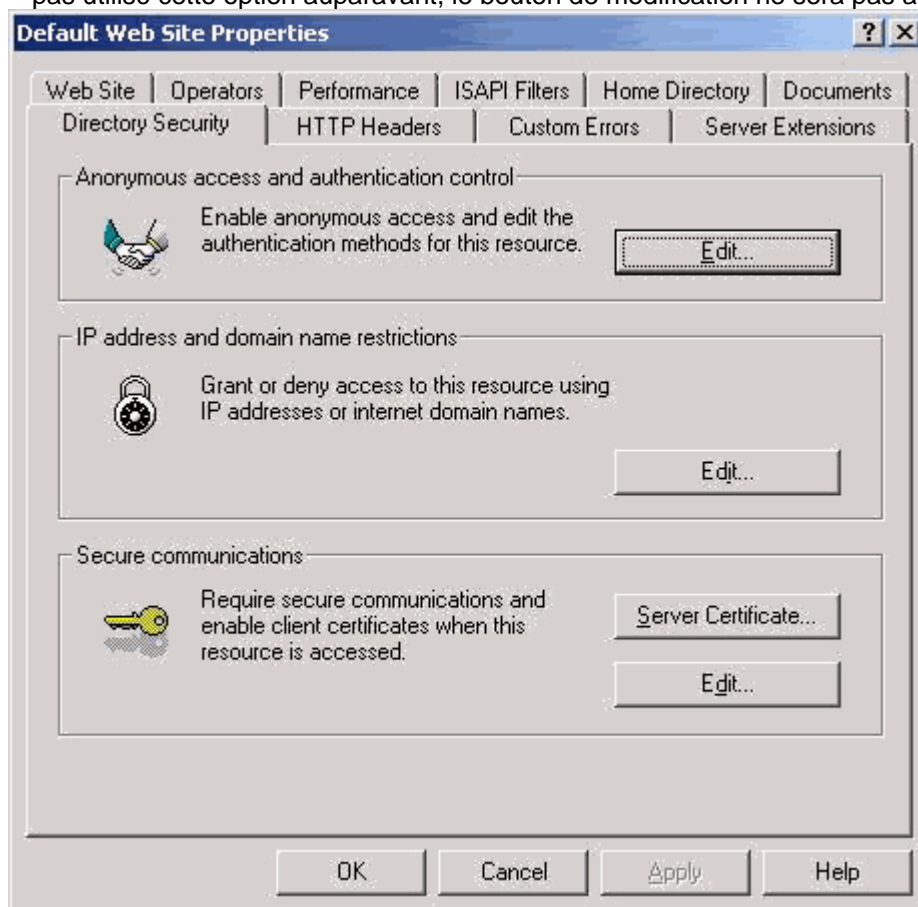
Etape 3 : Soumettez votre CSR

Base de connaissance K.SSL

Générez votre CSR

Microsoft - Microsoft IIS 6.0

1. Dans Outils d'administration, ouvrez le Gestionnaire des services Internet.
2. Ouvrez la fenêtre de propriétés en cliquant avec le bouton droit de la souris sur le nom du site Web à sécuriser.
3. Cliquez sur l'onglet Sécurité du répertoire.
4. Cliquez sur Certificat de serveur dans la section des communications sécurisées. Si vous n'avez pas utilisé cette option auparavant, le bouton de modification ne sera pas actif.



5. Sélectionnez Créer un nouveau certificat.



Base de connaissance K.SSL

Générez votre CSR

6. Sélectionnez Préparer la requête pour l'envoyer ultérieurement. Keynectis accepte uniquement les CSR par l'intermédiaire des formulaires d'inscription. Nous n'acceptons pas de CSR soumise par courrier électronique.



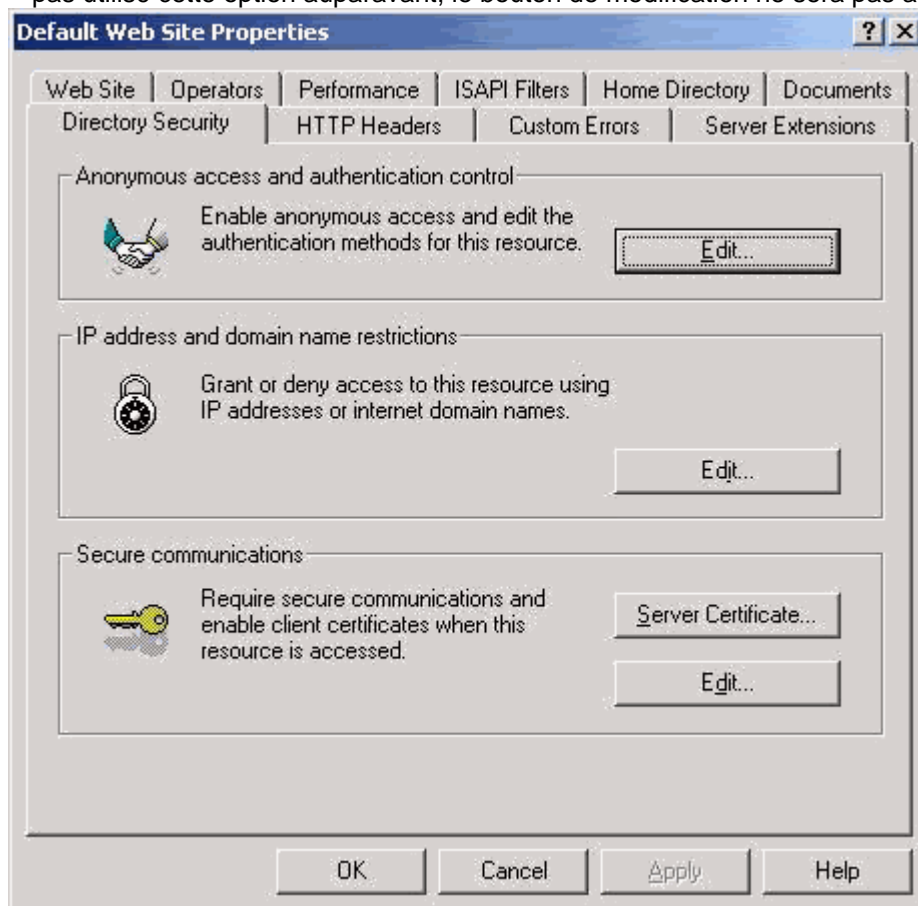
7. Complétez les informations demandées par l'assistant de certificat IIS pour créer une clé privée qui est stockée localement sur votre serveur et une clé publique (la requête de signature de certificat) que vous utiliserez pendant la procédure d'inscription. Vous venez de créer une paire de clés publique/ privée.
8. Cliquez sur Terminer pour quitter l'assistant de certificat IIS. Un fichier de CSR a été généré.
9. Accédez à la page Inscription
10. Pour copier et coller les informations dans le formulaire d'inscription, ouvrez le fichier dans un éditeur de texte qui n'ajoute pas de caractères supplémentaires (Notepad ou Vi sont recommandés)

Base de connaissance K.SSL

Générez votre CSR

Microsoft IIS 5.0

1. Dans Outils d'administration, ouvrez le Gestionnaire des services Internet.
2. Ouvrez la fenêtre de propriétés en cliquant avec le bouton droit de la souris sur le nom du site Web à sécuriser.
3. Cliquez sur l'onglet Sécurité du répertoire.
4. Cliquez sur Certificat de serveur dans la section des communications sécurisées. Si vous n'avez pas utilisé cette option auparavant, le bouton de modification ne sera pas actif.



5. Sélectionnez Créer un nouveau certificat.

Base de connaissance K.SSL Générez votre CSR



IIS Certificate Wizard
Server Certificate
There are three methods for assigning a certificate to a Web site.

Select the method you want to use for this web site:

- Create a new certificate.
- Assign an existing certificate
- Import a certificate from a Key Manager backup file.

6. Sélectionnez Préparer la requête pour l'envoyer ultérieurement. Keynectis accepte uniquement les CSR par l'intermédiaire des formulaires d'inscription. Nous n'acceptons pas de CSR soumise par courrier électronique.



IIS Certificate Wizard
Delayed or Immediate Request
You can prepare a request to be sent later, or you can send one immediately.

Do you want to prepare a certificate request to be sent later, or do you want to send it immediately to an online certification authority?

- Prepare the request now, but send it later.
- Send the request immediately to an online certification authority.

7. Complétez les informations demandées par l'assistant de certificat IIS pour créer une clé privée qui est stockée localement sur votre serveur et une clé publique (la requête de signature de certificat) que vous utiliserez pendant la procédure d'inscription. Vous venez de créer une paire de clés publique/ privée. Consultez le glossaire si vous avez des questions sur les informations demandées.
8. Cliquez sur Terminer pour quitter l'assistant de certificat IIS. Un fichier de CSR a été généré.
9. Soumettez votre CSR.

Base de connaissance K.SSL

Générez votre CSR

Microsoft IIS 4.0

1. Ouvrez la console de gestion Microsoft (MMC) pour IIS. Pour cela, il vous suffit normalement de sélectionner Démarrer -> Programmes -> Windows NT 4.0 Option Pack -> Microsoft Internet Information Server -> Gestionnaire des services Internet (ISS).
2. Développez le répertoire Internet Information Server en cliquant sur le signe + se trouvant à côté du nom de l'ordinateur.
3. Localisez le site Web qui utilisera le Certificat SSL. Il s'agit en général du site Web par défaut. Cliquez avec le bouton droit sur le site Web et choisissez Propriétés.
4. Dans la fenêtre Propriétés, cliquez sur l'onglet Sécurité du répertoire.
5. Vous devriez voir apparaître Sécurisation des communications et, à côté, le bouton Modifier. Cliquez sur ce bouton, puis sur le bouton Gestionnaire de clés.
6. Dans le Gestionnaire de clés, cliquez avec le bouton droit sur l'icône WWW et sélectionnez Créer une nouvelle clé.
7. Choisissez Placer la demande dans un fichier que vous enverrez à une autorité. Choisissez un nom de fichier approprié (ou acceptez le nom par défaut).
8. Remplissez la boîte de dialogue suivante. Les longueurs de clé disponibles varient selon la version et les Service Pack installés. Souvenez-vous du mot de passe que vous entrez. Sans lui, vous ne pourrez ni installer ni réaliser une copie de sauvegarde du certificat.
9. Vous devez aussi préciser une longueur en bits pour la CSR. Choisissez 1024.
10. Entrez les coordonnées appropriées et terminez. Vous pouvez entrer ici les informations que vous voulez puisqu'elles n'apparaîtront pas dans le certificat.
11. Le Gestionnaire de clés affichera sous l'icône WWW une clé barrée en rouge, indiquant qu'elle n'est pas complète.
12. Sélectionnez le menu Ordinateurs et cliquez sur Quitter. Cliquez ensuite sur OUI pour effectuer les modifications.
13. Vous venez de créer une paire de clés et une CSR. Pour copier et coller les informations dans le formulaire d'inscription, ouvrez le fichier dans un éditeur de texte qui n'ajoute pas de caractères supplémentaires (Notepad ou VI sont conseillés).
14. Soumettez votre CSR.

Base de connaissance K.SSL

Générez votre CSR

Red Hat - Linux Apache/SSL Server

Etape 1: Générer la clé privée

1. Utilisez la commande `cd` pour accéder au répertoire `/etc/httpd/conf`.
2. Entrez l'une des trois commandes suivantes en tant que racine pour générer votre clé :
3. Si vous utilisez Official Red Hat Linux Professional et souhaitez utiliser la fonction mot de passe incluse, entrez la commande suivante : `make genkey`
4. Votre clé sera générée et vous devrez entrer et confirmer un mot de passe. Notez que vous devrez retenir et entrer ce mot de passe à chaque fois que vous lancez votre serveur Web sécurisé. Alors, retenez-le !
5. Si vous utilisez Official Red Hat Linux Professional et ne souhaitez pas entrer un mot de passe à chaque démarrage de votre serveur Web sécurisé, utilisez la commande suivante au lieu de « `make genkey` » afin de créer votre clé (cette commande doit être entrée sur une seule ligne) :

```
/usr/sbin/sslgenrsa -rand /dev/urandom -out ssl.key/server.key 1024
```

6. Utilisez ensuite la commande suivante pour définir les autorisations sur votre clé :

```
chmod go-rwx ssl.key/server.key
```

7. Si vous utilisez les commandes ci-dessus pour créer votre clé, vous n'aurez pas besoin d'utiliser un mot de passe pour démarrer votre serveur Web sécurisé. Cependant, nous ne vous recommandons pas de désactiver la fonction mot de passe pour votre serveur Web sécurisé, car cela réduit le niveau de sécurité de votre serveur.
8. Votre clé est créée puis enregistrée dans le fichier `server.key`. Si vous utilisez Official Red Hat Linux Professional, ce fichier se trouve dans le répertoire `/etc/httpd/conf/ssl.key`. Si vous utilisez Official Red Hat Linux Professional, International Edition, le fichier `server.key` sera situé dans `/etc/httpd/conf`.

Etape 2 : Générer la CSR

1. Dans le répertoire `/etc/httpd/conf`, prenez le statut d'utilisateur root (racine) et saisissez l'une des deux commandes suivantes :
2. Si vous utilisez Official Red Hat Linux Professional, saisissez la commande suivante :

```
make certreq
```

3. Si vous utilisez Official Red Hat Linux Professional, International Edition, saisissez la commande suivante seule (sur une seule ligne) :

```
/usr/bin/openssl req -new -key /etc/httpd/conf/server.key -out /etc/httpd/conf/server.csr
```

4. Votre mot de passe vous sera demandé (si vous avez utilisé un mot de passe lorsque vous avez généré votre clé). Entrez le mot de passe, si nécessaire.
5. Vous verrez des instructions et des réponses vous seront demandées. Vos entrées sont alors incorporées dans la CSR.
6. Lorsque vous avez fini d'entrer vos informations, un fichier nommé `server.csr` sera créé. Si vous utilisez Official Red Hat Linux Professional, ce fichier se trouve dans le répertoire `/etc/httpd/conf/ssl.csr`.
7. Vous venez de créer une paire de clés et une CSR.
8. Le fichier `server.csr` contient votre demande de certificat. Pour copier et coller les informations dans le formulaire d'inscription, ouvrez le fichier dans un éditeur de texte qui n'ajoute pas de caractères supplémentaires (Notepad ou Vi sont conseillés).
9. Soumettez votre CSR.

Base de connaissance K.SSL

Générez votre CSR

Sun - Java System WebServer 6.x, Sun ONE

Etape 1 : Créer une base de données de clés

1. Sélectionnez l'instance serveur et cliquez sur Manage.
2. Cliquez sur Sécurité.
3. Cliquez sur Créer une Base de Données.
4. Entrez et confirmer un mot de passe pour protéger cette base de données.

Etape 2 : Générez une CSR

1. Cliquez sur Demander un certificat.
2. Entrez votre propre adresse mail pour l'adresse mail de l'AC. Même si votre Serveur Sun supporte l'email pour l'envoi de vos demandes de certificats, Keynectis vous demande de coller votre demande de certificat dans le formulaire d'enregistrement en ligne.
3. Attribuez un mot de passe à votre fichier bi-clé pour protéger vos clés. Ce peut être le même que celui de la base de données de clés.

Complétez toutes les informations de la CSR et cliquez sur OK

Le serveur va générer la CSR et vous l'afficher sur la page.

5. Pour copier les informations de la CSR dans votre formulaire d'enregistrement, ouvrez un éditeur de texte tel que bloc-notes ou Vi qui n'ajoute pas de caractères supplémentaires.
6. Cliquez sur appliquer pour sauvegarder ces modifications. Vous venez de créer une bi-clé et une CSR