



DOCUMENTATION

Certificats HTTPS & SSL Tutorial

Table des matières

1 - Fonctionnalités Portail Web, HTTPS & SSL.....	3
2 - Processus de certification	3
3 - Les certificats	4
3.1 - Propriétés des certificats	4
3.2 - Au sujet des clés privées	5
4 - Importation des certificats.....	6
4.1 - Ce dont nous avons besoin pour l'importation.....	6
4.2 - Importation d'une clé privée	6
4.3 - Importation des certificats.....	7
4.4 - Résultat de l'importation du certificat.....	8
4.5 - Importation de la réponse CA.....	8
4.6 - Remise en marche le serveur web.....	9
5 - Dépannage	9
5.1 - J'ai reçu 1 seul fichier (.crt ou Cer).....	9
5.2 - Ma clé est au format .pem. Je ne peux pas l'importer dans Portecle.....	10
5.3 - Erreurs Https.....	10
5.4 - A propos de Microsoft IIS.....	10
5.5 - Clés à fort chiffrement (Ne peut pas importer le fichier .pkcs12).....	10
6 - Comment faire une demande de CA et obtenir un certificat.....	11
6.1 - Rappel - Processus de certification	11
6.2 - Créer la clé privée	11
6.3 - Générer la demande CA (Request)	14
6.4 - Le fichier CSR généré.....	14

1 - Fonctionnalités Portail Web, HTTPS & SSL

Le serveur HTML5 intégré à TS2log Remote Access prend en charge le protocole Https, le chiffrement SSL avec un certificat auto-signé ou un certificat fourni par une autorité de certification.

Le protocole https chiffre la communication entre le client et le serveur. Le certificat unique produit une clé 2048 bits RSA, inclut la clé de cryptage et la certification du serveur ou du Domain Name sur lesquels l'utilisateur est connecté. L'utilisateur a la garantie que la communication est chiffrée et le serveur ou le Domain Name certifié par une autorité de certification. Cette information apparaît dans la barre d'adresse du navigateur, sous forme d'un cadenas.



You are connected to
godaddy.com
which is run by
GoDaddy.com, LLC
Scottsdale
Arizona, US
Verified by: GoDaddy.com, Inc.



The connection to this website is secure.

Dans ce document, nous apprendrons comment installer un certificat SSL sur le serveur Web TS2log, fournissant ainsi la sécurité HTTPS, le chiffrement 2048 SSL et la certification de Domaine.

Référez-vous au dernier chapitre de ce document pour obtenir des informations sur la manière de réaliser une demande auprès d'une autorité de certification et obtenir un certificat.

2 - Processus de certification

Les certificats sont fournis par les autorités de certification (OCA). Le processus se déroule en 3 étapes.

a) La génération d'une clé privée au standard RSA 2048 bit. Cette clé sera employée pour produire une demande de CA basée sur elle.

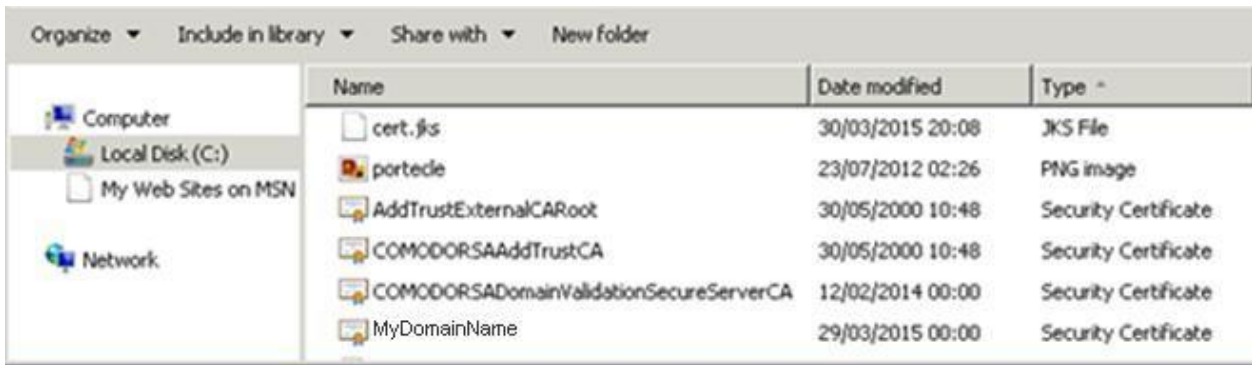
b) La demande de CA produite est transmise à l'OCA. Elle contient toutes les informations qui sont nécessaires pour fournir un certificat (le pays, le nom de l'Etat ou de la province, le nom de la compagnie, un e-mail valide et le nom commun (NC) par exemple MyDomainName.com).

c) L'OCA vérifie les informations que vous avez transmises et renvoie le certificat. Il contient votre certificat certifiant votre Domain Name, et les certificats intermédiaires qui sont requis pour accéder à votre certificat. Le certificat contient également la réponse CA (la clé privée validée). Le certificat, la réponse CA, (clé privée) et les certificats intermédiaires doivent ensuite être importés dans le magasin de certificats géré par le serveur web de TS2log. Pour simplifier le déploiement, les fichiers qui composent le certificat peuvent être compilés au sein d'un seul certificat, au format .pfx (PKCS#12).

3 - Les certificats

Le certificat contient habituellement plusieurs fichiers. Chaque fichier est un certificat. Comme dit précédemment, l'autorité fournit le certificat de votre Domain Name et les intermédiaires qui sont requis pour accéder à votre certificat.

Le fichier est au format .cer ou .crt. Ces extensions sont identifiées par l'OS qui associe l'icône de certificat.

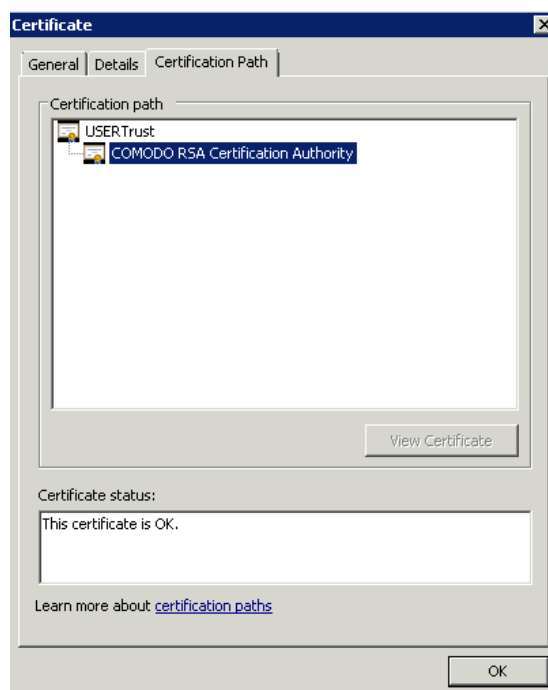
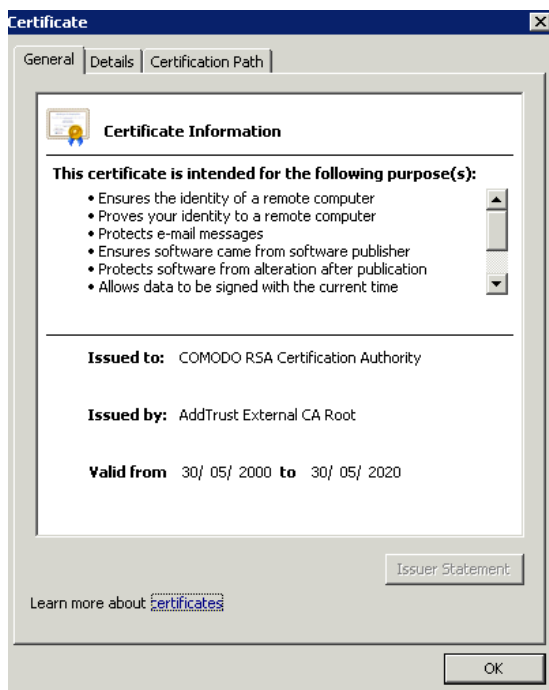


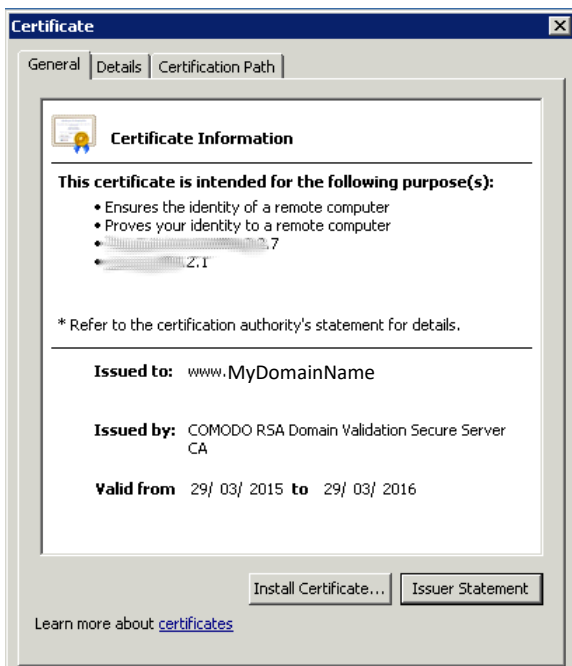
Dans notre exemple ci-dessus, nous avons reçu 4 certificats (.crt). Le premier, deuxième et troisième sont les certificats intermédiaires (CARoot, TrustCA, DomainValidation CA). Le quatrième est notre certificat qui certifie notre Domain Name MyDomainName.crt. Ils doivent tous être installés.

Pour une meilleure compréhension sur la façon de procéder, examinons les certificats.

3.1 - Propriétés des certificats

Les propriétés du certificat montrent son chemin. Chaque certificat a un chemin de la racine au certificat de votre Domain Name.



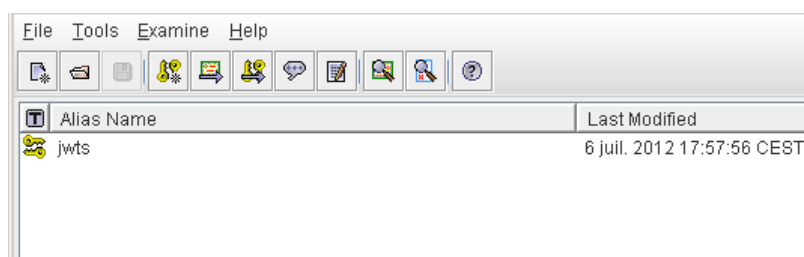
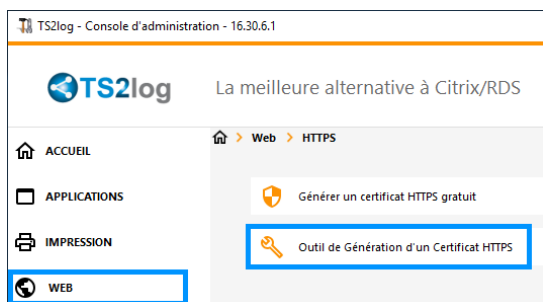


La fenêtre Propriétés de notre certificat affiche toutes les informations générales au sujet du certificat (Nature du certificat, adresses, Domain Name, validité... Il est important de noter le chemin de certification. Il inclut le chemin entier requis pour accéder à notre certificat. Il montre tous les certificats intermédiaires qui sont inclus à l'intérieur du nôtre.

Le jeu est simple. Nous devons importer ce chemin entier de certification, plus la réponse CA (clé privée) dans le magasin (keystore).

3.2 - Au sujet des clés privées

La clé privée RSA 2048 bit est produite pour la demande du certificat. Elle peut être produite via l'outil supplémentaire Portecle que nous fournissons, ou avec un autre générateur disponible comme Openssl, IIS, ou le site en ligne du fournisseur OCA. Vous devez avoir et garder cette clé privée. C'est un fichier plat au format .pem, ou .p12 ou .pfx. La clé privée produite est obligatoire pour pouvoir installer correctement les certificats.



Le fichier cert.jks, localisé dans le dossier 'C:\Program Files (x86)\ts2log\clients\webserver' est utilisé par le serveur web TS2log. Il s'agit du magasin de certificats (keystore) dans lequel les certificats et la réponse CA doivent être importés. Par défaut, ce magasin contient seulement une clé privée associée à un certificat auto-signé (jwts). Cert.jks est protégé par un mot de passe. Ce mot de passe doit être « secret ». La clé privée « jwts » est également protégée par un mot de passe. Ce doit également être « secret ».

En d'autres termes, le fichier keystore dans lequel vous importez les certificats doit être appelés cert.jks. Son mot de passe doit être « secret ». La clé privée contenue dans cert.jks doit être nommée « jwts » (alias). Son mot de passe doit être « secret ».

Une fois que nous avons recueilli tous ces éléments, nous devons les importer correctement dans le magasin cert.jks.

4 - Importation des certificats

4.1 - Ce dont nous avons besoin pour l'importation

- Les certificats intermédiaires inclus dans le chemin. Un fichier par certificat (.crt ou .cer)
- Le certificat de notre Domain Name. Il contient le chemin entier, le certificat et la réponse CA. Un fichier (.crt ou .cer)
- la clé privée employée pour faire la demande. (Voir la section comment faire une demande pour de plus amples informations)
- Le fichier Magasin (aussi appelé Keystore (cert.jks)
- Add On Portecle que nous fournissons pour gérer les fichiers keystore.

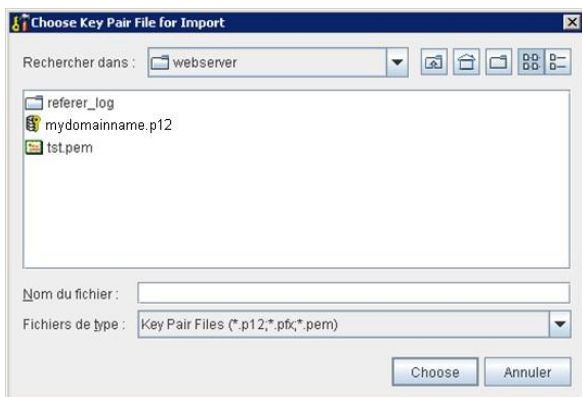
Dans notre exemple, nous supposons que nous avons produit une clé privée avec Portecle dans cert.jks (voir la section comment faire une demande). Ainsi nous présumons que la clé privée produite est déjà dans cert.jks. Si la clé était créée avec un autre outil, elle doit être importée dans cert.jks.

4.2 - Importation d'une clé privée

Seulement si créée avec un autre outil que Portecle, autrement, consulter directement le chapitre 4.3.

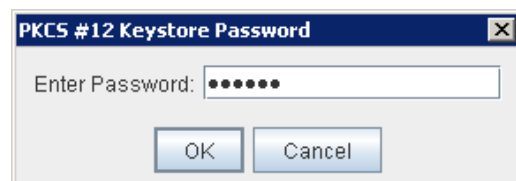
Nous faisons d'abord une copie du fichier cert.jks pour disposer d'une sauvegarde. Ouvrir le fichier original cert.jks (mot de passe «secret »). Puis clic droit sur la clé privée, choisissez Suppression et confirmez. Nous n'avons pas besoin d'elle car nous importerons la nôtre.

Une clé privée au format texte plat .pem ne peut pas être importée dans Portecle. Vous devez avoir un format .pfx ou .p12. Reportez-vous à la section Support et Dépannage de ce document pour plus d'informations sur la façon d'obtenir un format .pfx ou .p12.



Menu Tools / Import Key Pair.
Choisir la clé puis confirmer.

Saisir le mot de passe de la clé.

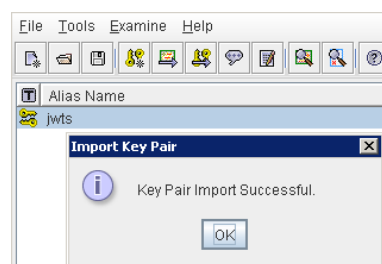
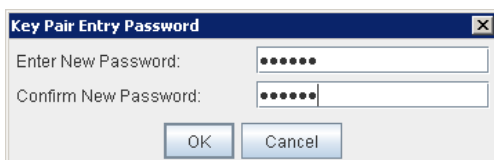


Confirmer l'importation.

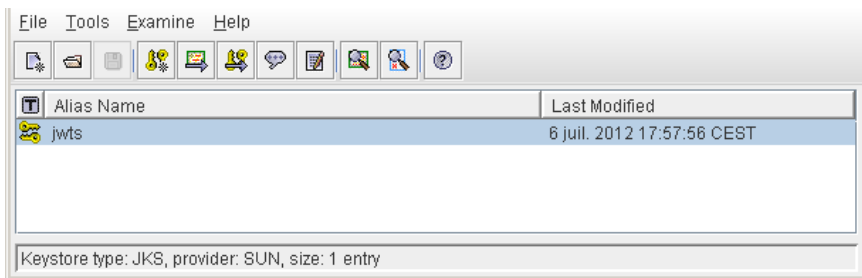
Nommez la clé (alias) « jwt ». L'alias est le nom de la clé, pas le nom du domaine (domain name mydomainname.com)



Entrez le nouveau mot de passe « secret » (Rappelez-vous, ce mot de passe est obligatoire)



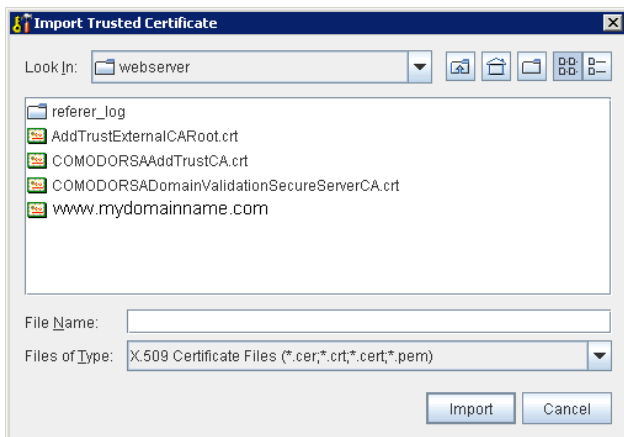
4.3 - Importation des certificats



On commence ici avec cert.jks qui contient la clé RSA 2048 bit utilisée pour la demande.

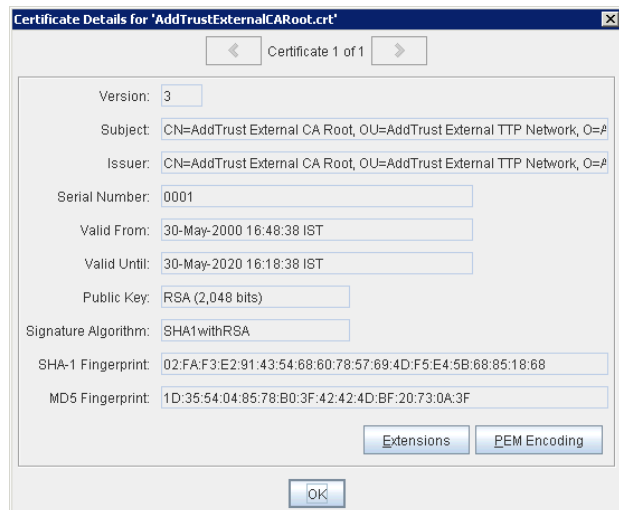
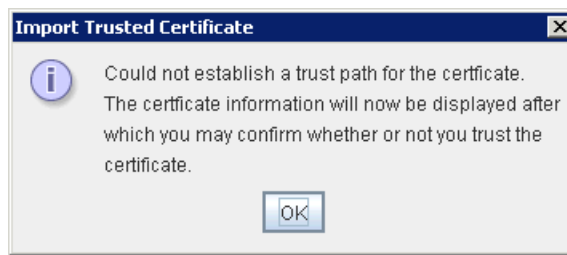
On importe chacun des certificats du chemin.

Tools / Import Trusted Certificate



Sélectionner le certificat.

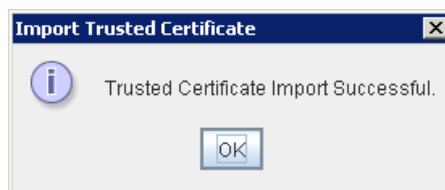
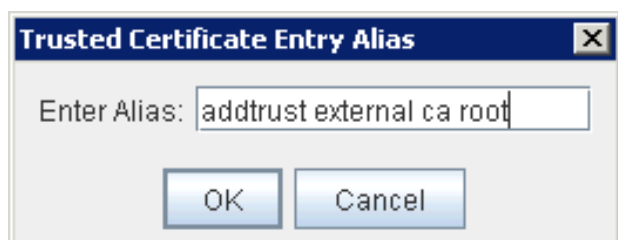
Confirmer.



Confirmez que vous acceptez le certificat comme conforme.

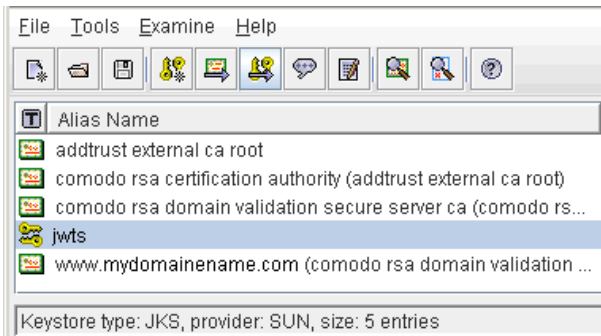


Confirmez le nom (Alias).
Le certificat est alors importé.



4.4 - Résultat de l'importation du certificat

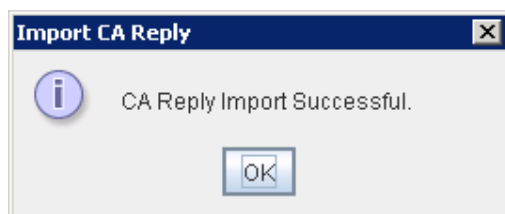
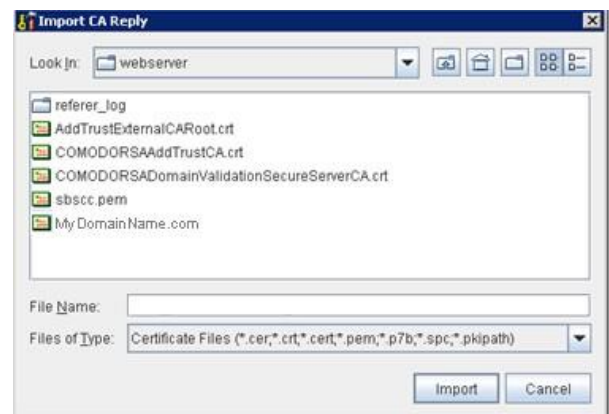
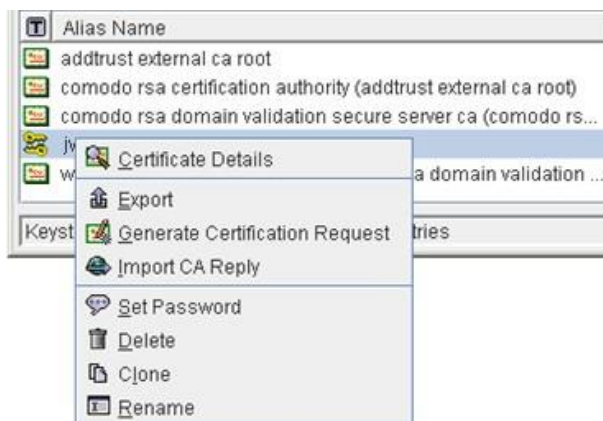
Une fois que nous avons importé tous les certificats que nous avons reçus et qui sont dans le chemin, Portecle montre les certificats importés. Nous notons que la liste respecte l'ordre du chemin attaché au certificat. En conséquence, nous avons le même affichage qui a été présenté dans les propriétés du certificat, excepté la clé privée qui apparaît dans Portecle au-dessus du certificat du Domain Name.



4.5 - Importation de la réponse CA

La réponse CA est la clé privée certifiée par l'OCA. Elle est contenue dans le certificat de Domaine (par exemple certificat MyDomainName.com). C'est la raison pour laquelle il est important, quand cela est possible, d'obtenir un certificat avec une clé exportable.

Pour importer la réponse CA, clic droit sur la clé privée (jwts) et choisir Import CA reply. Suivez les étapes et confirmez l'importation. Il est important de se rappeler que le mot de passe de la clé privée doit être « secret ». Si vous avez un doute, clic droit sur la clé privée, choisir Set Password.



Entrez le mot de passe de fichier Magasin (Keystore) si demandé. Le mot de passe du fichier cert.jks (choisi dans des outils /options). Ce devrait être cert.jks, avec « secret » comme mot de passe

Entrez le mot de passe de la clé privée. Le mot de passe pour la clé privée doit être « secret »

4.6 - Remise en marche le serveur web

Les certificats et la Réponse CA ont été importés. Notre serveur web html5 est maintenant prêt.

Sauvez le fichier cert.jks. Le mot de passe doit être « secret ». Redémarrer le serveur web TS2log depuis l'onglet 'Accueil' dans AdminTool.

Le certificat est maintenant installé et affiché dans la barre d'adresse du navigateur sous forme https://mydomainname.com.

Dans les sections suivantes, nous examinons quelques dépannages.

5 - Dépannage

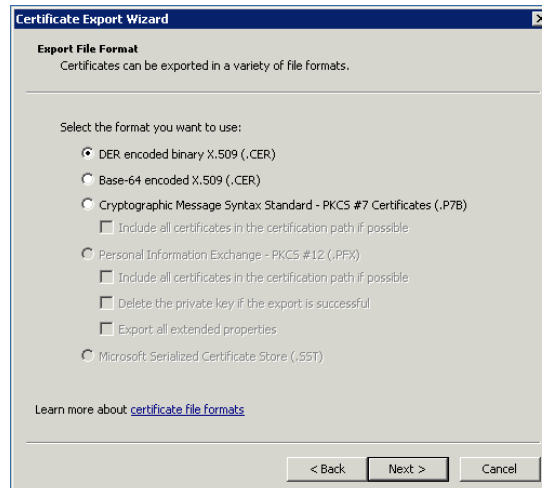
5.1 - J'ai reçu 1 seul fichier (.crt ou Cer)

Il contient le certificat de MydomainName.com. Regardez le chemin dans les propriétés du certificat. Si votre certificat est à la racine, alors vous n'avez aucun certificat intermédiaire. Vous devez seulement importer le fichier.cer que vous avez reçu.

Si le chemin contient d'autres certificats intermédiaires, alors ils seront nécessaires. Vous pouvez exporter les certificats inclus dans le vôtre et créer un fichier par certificat.



Double clic sur le certificat que l'on souhaite exporter. Ensuite Détails / Exporter.



Puis Suivant. Les valeurs par défaut sont correctes. Suivant puis nommer le fichier. Confirmer l'exportation. Le résultat est un fichier.cer qui contient uniquement le certificat exporté. Répétez ces étapes pour chaque niveau du chemin. Vous obtiendrez un fichier par certificat.

5.2 - Ma clé est au format .pem. Je ne peux pas l'importer dans Portecle

Vous pouvez convertir un format .pem au format pfx avec un outil tel que OpenSSL. Nous préconisons cette méthode plus sécurisante que l'utilisation d'un site web de conversion SSL.

Vous devez avoir votre clé privée et votre certificat (par exemple MyDomainName.com). Sélectionner le certificat à convertir et la clé privée qui lui est associé. Renseigner le type de certificat (.pem par exemple). Puis le format PFX pour le fichier converti. Renseigner également le mot de passe du certificat.

Le résultat est un format .pfx que vous pourrez importer dans Portecle. Comme nous avons vu dans la section d'installation, cette clé privée importée dans Portecle doit recevoir la réponse CA. Voir chapitre Importation de la réponse CA.

SSL Converter

Use this **SSL Converter to convert SSL certificates** to and from different formats such as **pem, der, p7b, and pfx**. Different platforms and devices require SSL certificates to be converted to different formats. For example, a Windows server exports and imports .pfx files while an Apache server uses individual PEM (.crt, .cer) files. To use the SSL Converter, just select your certificate file and its current type (it will try to detect the type from the file extension) and then select what type you want to convert the certificate to and click **Convert Certificate**. For more information about the different [SSL certificate](#) types and how you can convert certificates on your computer using OpenSSL, see below.

Certificate File to Convert: MyDomainName_com.crt

Private Key File: private key.pem

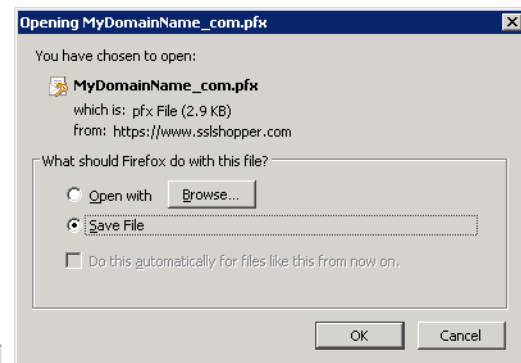
Chain Certificate File (optional): No file selected.


Chain Certificate File 2 (optional): No file selected.

Type of Current Certificate: Detected type from file extension

Type To Convert To:

PFX Password:



 Your private key is intended to remain on the server. While we try to make this process as secure as possible by using SSL to encrypt the key when it is sent to the server,

<https://www.sslshopper.com/ssl-converter.html>

5.3 - Erreurs Https

La clé privée n'a pas été importée dans cert.jks ou est invalide.

D'autres erreurs donnent le même type d'écran avec un autre code d'erreur. Examinez cette erreur. Elle concerne le certificat et une de ses données renseignées. Parfois, un des champs du certificat est invalide ou vide. Ouvrez les Propriétés du certificat. Vérifiez que tous les champs sont corrects.

5.4 - A propos de Microsoft IIS.

Voici quelques informations importantes sur IIS et les certificats.

Avec IIS, le certificat doit être installé dans le keystore cert.jks. Ceci doit être fait de la même manière que si nous employons le serveur web TS2log, comme décrit dans le chapitre précédent.

C'est le serveur web TS2log qui manipule le protocole https, le certificat et son chiffrement. Aucune Liaison(binding) sur le port 443 ne doit être créée dans IIS. Ainsi, IIS doit seulement avoir une liaison sur le port 81.

IIS peut aussi être utilisé pour créer la clé privée et la demande de CA. Il est simple d'exporter la clé privée de IIS (site/certificats IIS) au format .pfx et de l'importer dans cert.jks comme décrit dans le chapitre précédent.

5.5 – Clés à fort chiffrement (Ne peut pas importer le fichier .pkcs12)

Une erreur se produit lorsque vous tentez d'importer votre certificat au format Pkcs12. Le type de clé à fort chiffrement n'est pas pris en charge par PorteClé.

Pour ce cas de figure nous conseillons l'utilisation de l'application keyStore Explorer.

Il s'agit d'une application gratuite disponible depuis le site <https://keystore-explorer.org/index.html>

6 - Comment faire une demande de CA et obtenir un certificat

Voici le processus de certification expliqué. Il peut être fait dans Portecle que nous fournissons, ou avec un autre générateur disponible comme Openssl, IIS, ou les sites en ligne, les applications du fournisseur de certificats.

6.1 - Rappel - Processus de certification

Les certificats sont fournis par les autorités de certificats (CA). Le processus a 3 étapes.

a) La génération d'une clé privée au standard RSA 2048. Cette clé sera employée pour produire une demande de CA basée sur elle.

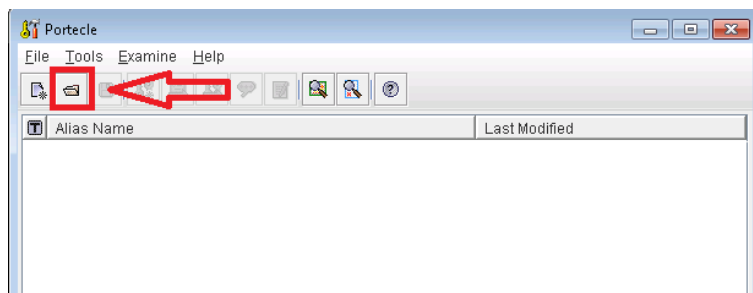
b) La demande de CA produite est transmise à l'organisme de certification. Elle contient toutes les informations qui sont nécessaires au fournisseur pour fournir un certificat (le nom, l'état, la province, le nom de la localité, et de la compagnie, l'adresse e-mail valide et le nom commun (NC) par exemple MyDomainName.com).

Le principal travail consiste à renseigner correctement toutes les informations énumérées ci-dessus.

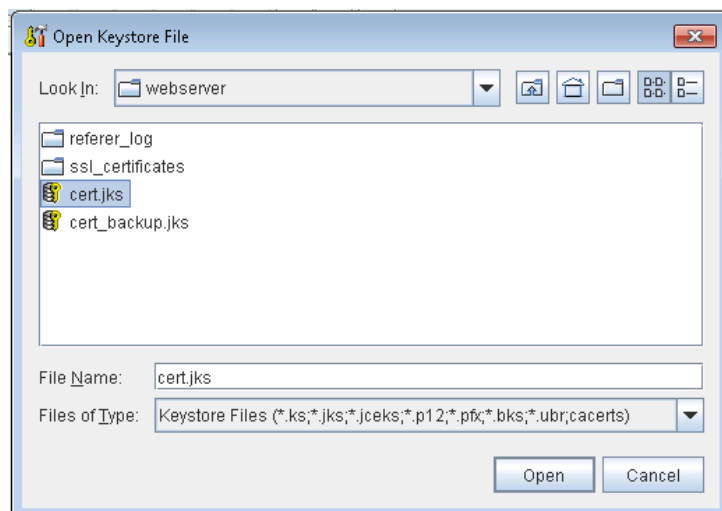
c) L'organisme de certification vérifie l'information que vous avez transmise et renvoie un fichier qui contient votre certificat certifié à votre Domain Name, éventuellement accompagné des certificats intermédiaires qui sont requis. Le certificat contient également la réponse CA (la clé privée validée). Une fois que vous avez le certificat, la réponse CA, (clé privée), et les certificats intermédiaires, ils doivent être importés dans le keystore manipulé par TS2log.

6.2 - Créer la clé privée

Nous suggérons de conserver une sauvegarde de cert.jks avant de le modifier. Nous devons d'abord ouvrir le keystore cert.jks situé dans le dossier .clients\webserver de TS2log. Cliquer sur le bouton Ouvrir

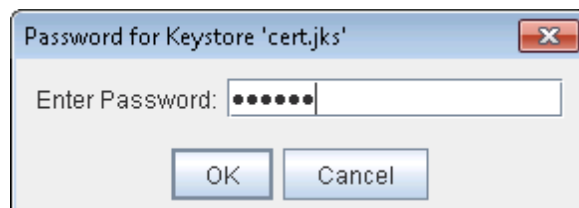


Sélectionner cert.jks (keystore utilisé par TS2log) dans lequel la clé privée et les futurs certificats doivent être importés.

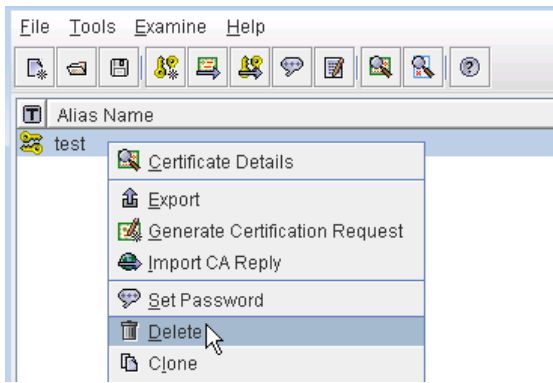


Le Mot de passé est "secret" Ce mot de passe est obligatoire et ne doit pas être modifié

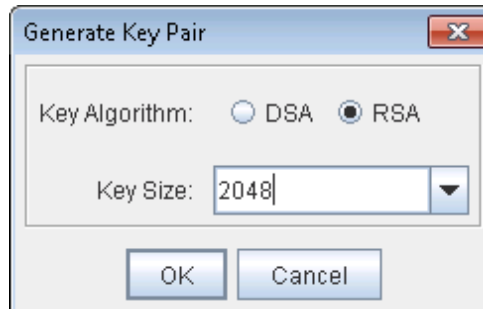
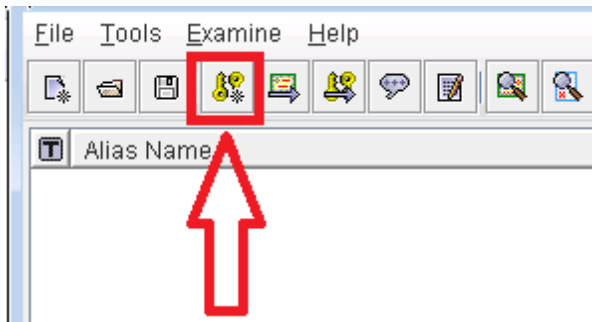
Ce mot de passé doit être laissé tel quel pour le keystore cert.jks.



Le fichier original cert.jks contient la clé privée utilisée par défaut. Elle peut être supprimée car elle n'est d'aucune utilité. Clic droit sur la clé privée puis Delete.

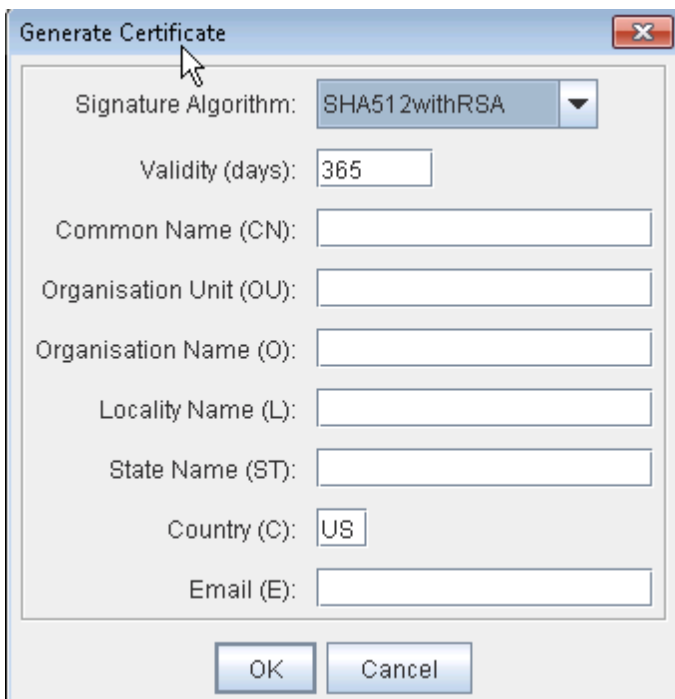


Maintenant on génère la clé privée.



Cliquez sur New key. Renseigner le type de clé RSA et Key Size 2048.

Régler la signature sur l'algorithme SHA512 with RSA. Tous les champs suivants doivent être correctement remplis.



Nom commun (NC) : Doit contenir le nom de Domaine pour accéder au serveur. C'est l'une des informations les plus importantes. Ce doit être avec précision le Domain Name employé pour atteindre le site Web. (par exemple webvpn.ts2log.net)

Unité d'organisation (OU) : Nom de l'unité d'organisation dans l'entreprise

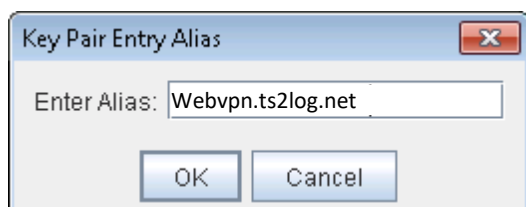
Nom d'organisation (o) : Nom de votre organisation (entreprise). Cette information est également très importante. Si non rempli, le certificat affichera une erreur.

Nom de localité (l) : Nom de la ville de l'organisation

État (St) : Etat (Département)

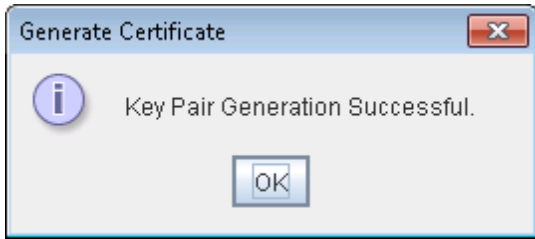
Pays (c) : Nom du pays de l'entreprise

Email (e) : Renseignez une adresse e-mail valide



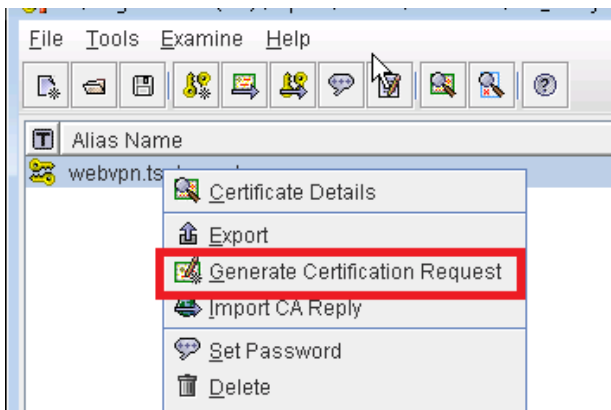
Par défaut, l'alias devrait être le Nom Commun (CN) entré

Entrez le mot de passe "secret". Ce mot de passe « secret » est obligatoire. Il peut être réinitialisé avec un clic droit sur la clé puis Set Password.



6.3 - Générer la demande CA (Request)

Il faut maintenant générer la demande de certification (CSR) qui doit être déposée auprès de l'organisme de certification. Clic-droit sur la clé, puis Generate Certification Request



Sauvegarder le fichier dans le dossier de votre choix. Conserver précieusement ce fichier.

6.4 - Le fichier CSR généré

Le fichier CSR généré est un fichier plat. Il contient la demande de certification (Certification Request - CSR)

```
-----BEGIN CERTIFICATE REQUEST -----  
Dmfspi4687976z1fefgkuo6p85sdfghyi6  
4ed54rgerty4jzQ8UY4IK8UYOGFL14rt4ez7z(e'95gjh65k8u7l6l46  
k564setezrg54ryh4gujuk564setezrg54ryh4gujukFL14rt4eFL14rt  
...  
...  
-----END CERTIFICATE REQUEST-----
```

Il peut être copié pour le soumettre à n'importe quel fournisseur de certificat et faire la demande d'un certificat.

Référez-vous au chapitre 4 de ce document pour obtenir des informations sur la façon d'importer le certificat dans le keystore cert.jks