Fiche Technique TS2log

Installation du certificat SSL

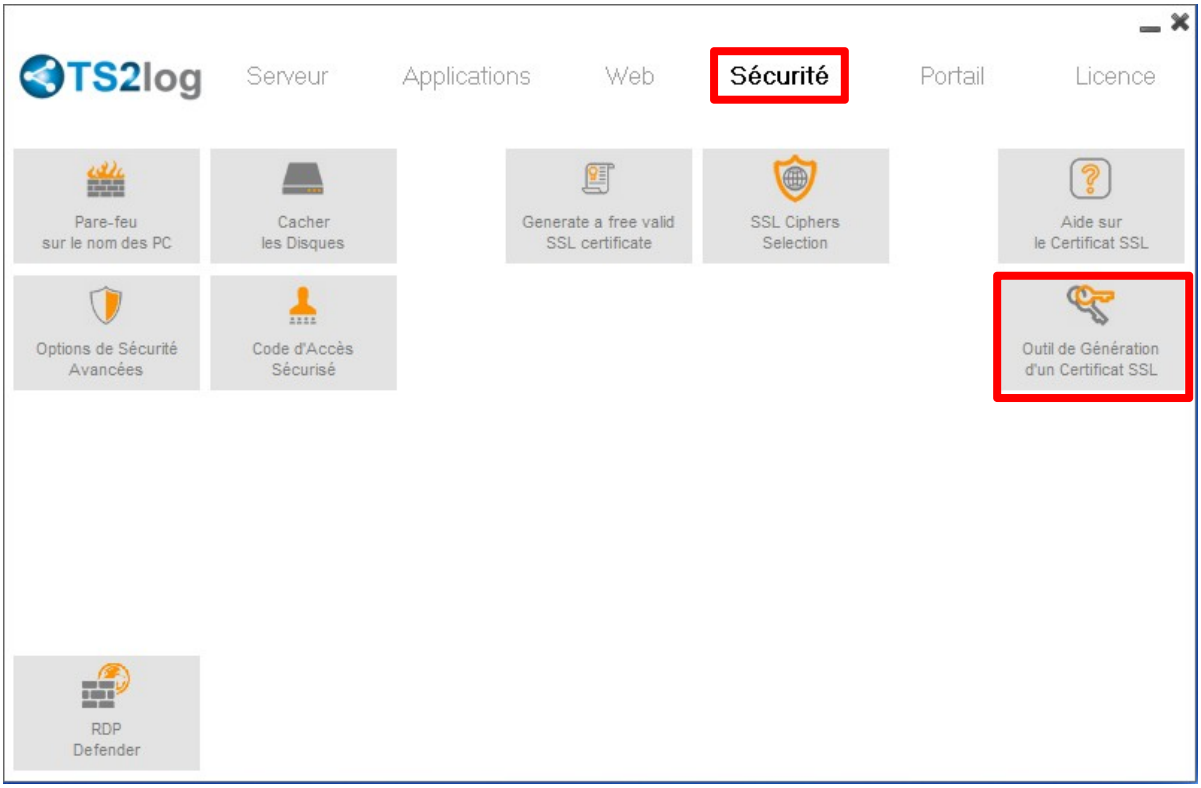
PREAMBULE

TS2log est livré avec un certificat SSL auto-signé ce qui déclenche une alerte du navigateur au moment de la connexion en mode HTTPS. Pour continuer la connexion, l'utilisateur doit faire confiance au serveur auquel il accède en validant l'alerte. La connexion est alors cryptée mais l'utilisateur ne peut être certain de l'identité du serveur.
Si ce scénario est concevable sur un réseau local d'entreprise, il ne serait pas de bonne pratique dans le cas d'une connexion via Internet. L'administrateur de TS2log peut alors facilement installer un certificat délivré par une autorité de certification officielle pour complètement sécuriser les accès via Internet des utilisateurs.

PROCEDURE d'INSTALLATION

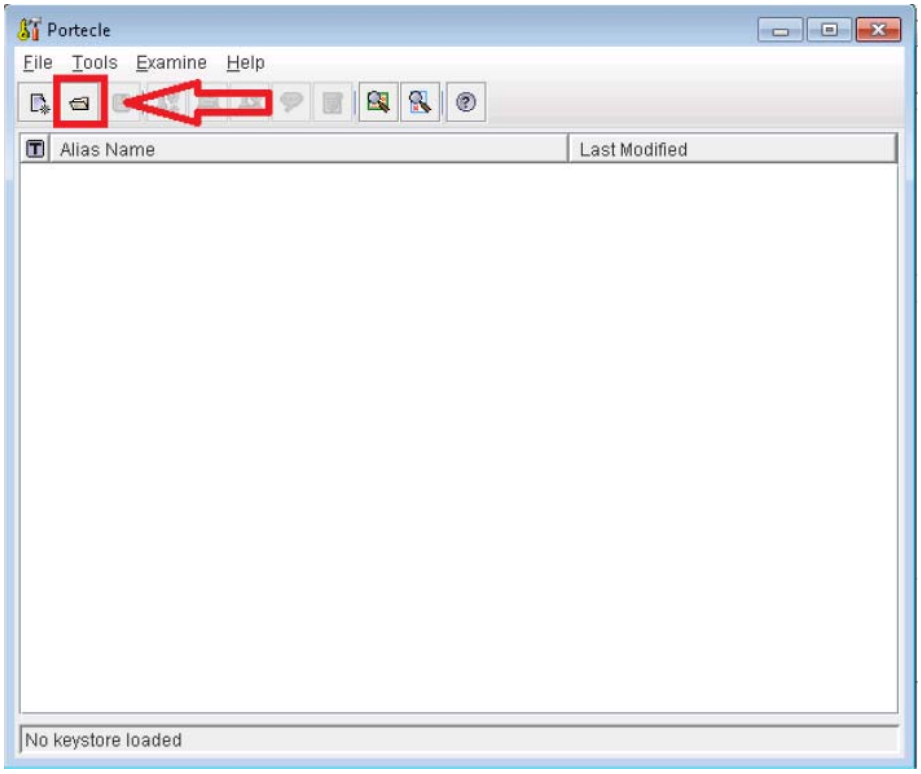
Vous devez d'abord acheter le certificat SSL avant de procéder à l'installation du certificat ssl sur le serveur Web TS2log.

1. Lancer AdminTools > Sécurité > Bouton « Outil de Génération d'un certificat SSL »

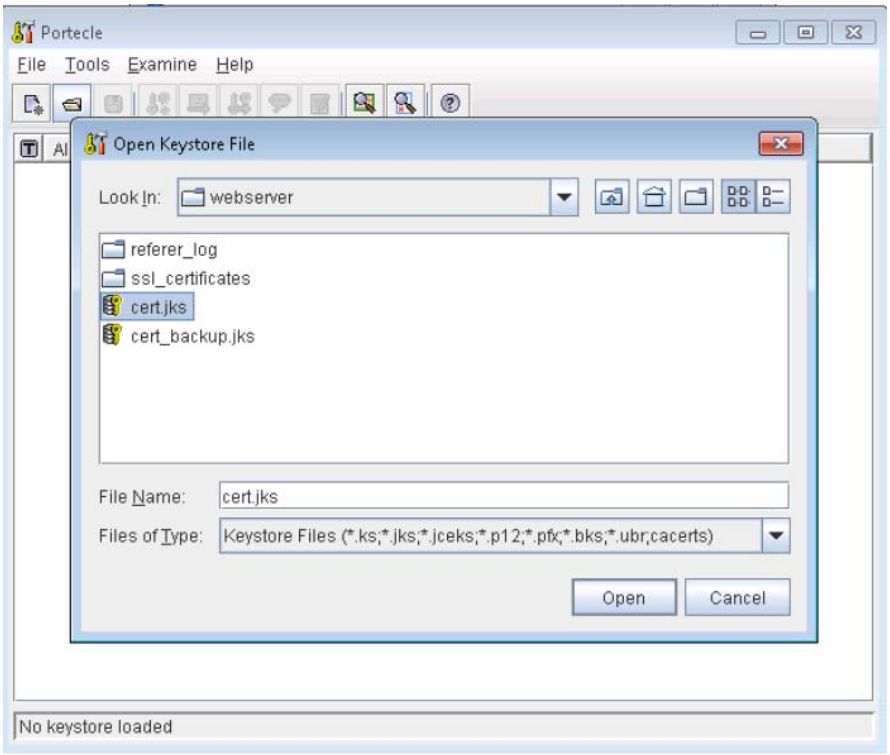


1, place Paul Verlaine 92100 BOULOGNE BILLANCOURT
Tél. : 09 50 26 82 18 – Fax : 09 55 26 82 18
Sarl au capital de 7500€ - RCS Nanterre – 487 612 947

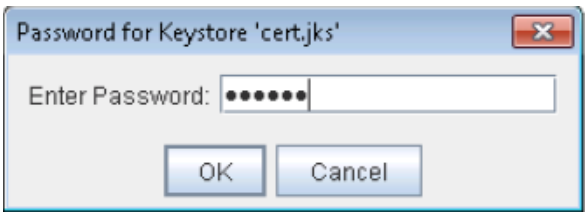
2. Cliquez dans le menu sur File > Open Keystore File



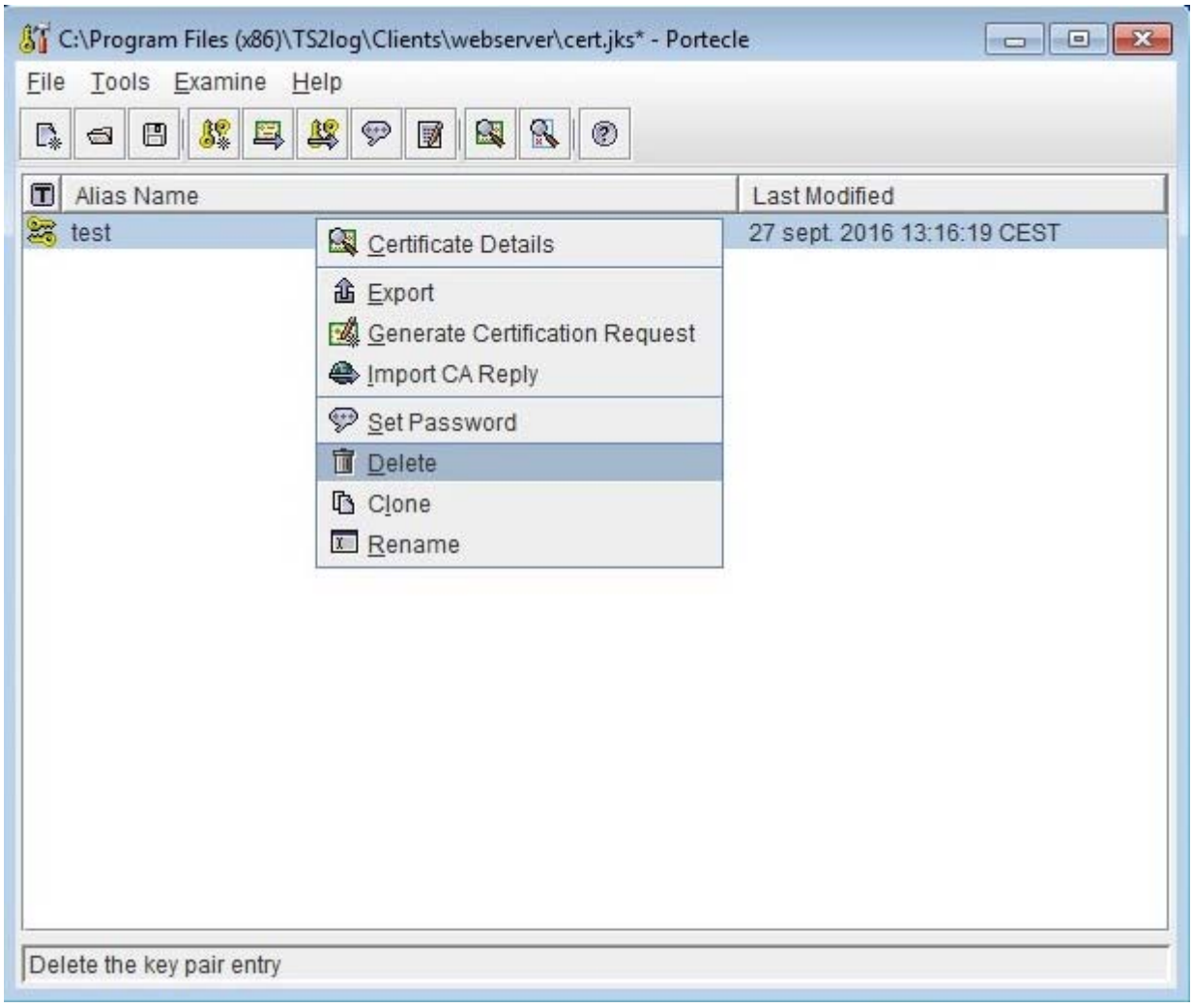
3. Dans la fenêtre “Open Keystore File” sélectionnez cert.jks (le dépôt par défaut des clés) et cliquez sur « Open ».



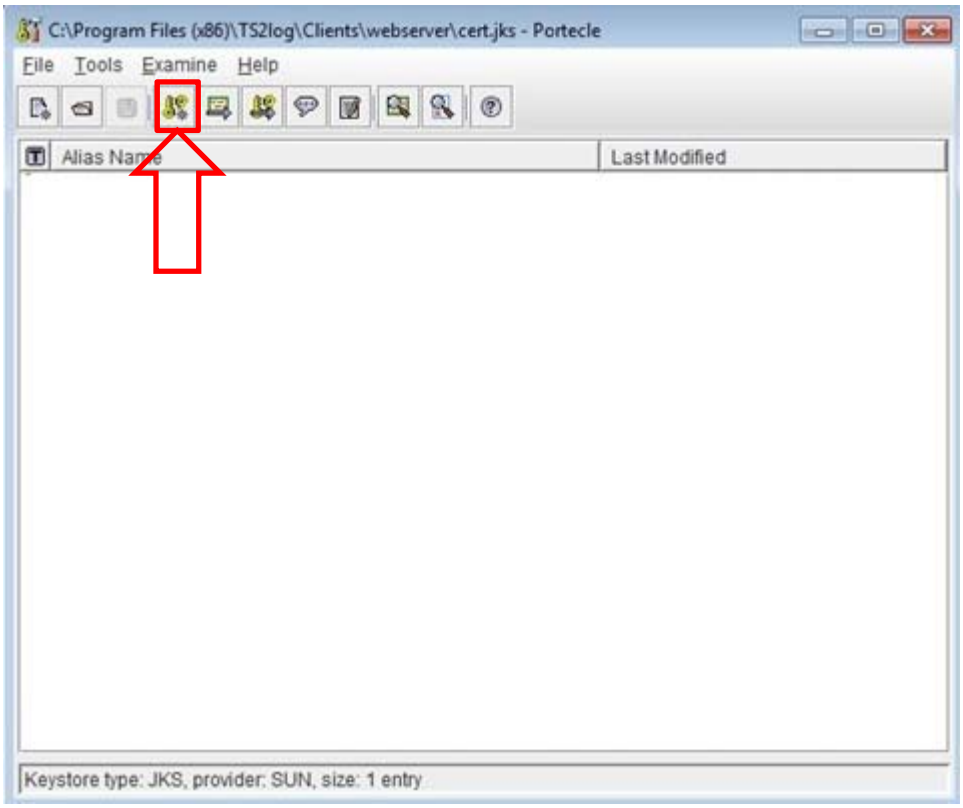
4. Au prompt de la fenêtre “Password for Keystore” vous devez saisir “**secret**”.



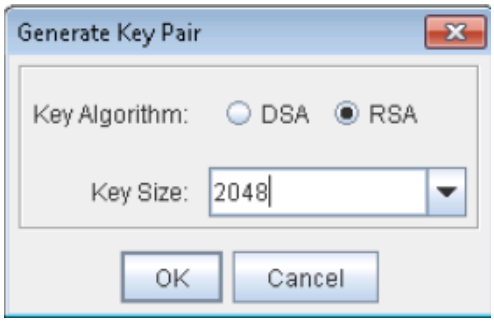
5. Effacez les clés existantes dans le dossier



6. Générez une nouvelle paire de clé auto signée en cliquant sur l'icône de génération.

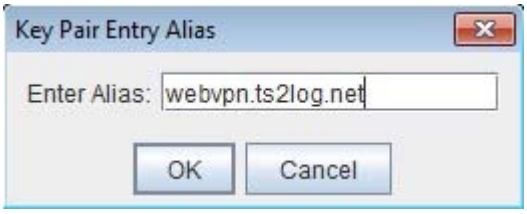


7. Configurez l'algorithme comme suit: RSA et taille de la clé: 2048 puis validez par OK.



8. Configurez l'algorithme de signature pour SHA512 avec RSA et complétez les champs vides :
   - Validity (days): Durée de validité de votre certificat.
   - Common Name (CN): Doit être configuré avec le nom de la machine permettant l'accès à celle-ci. Par exemple : webvpn.myriad.net
   - Organization Unit (OU): Nom du département de l'entreprise
   - Organization Name (O): Nom de l'entreprise
   - Locality Name (L): Nom de la ville
   - State (ST): Nom du département géographique
   - Country (C): Code d'abréviation du pays (par défaut US)
   - Email (E): Email adresse que vous souhaiteriez mentionner

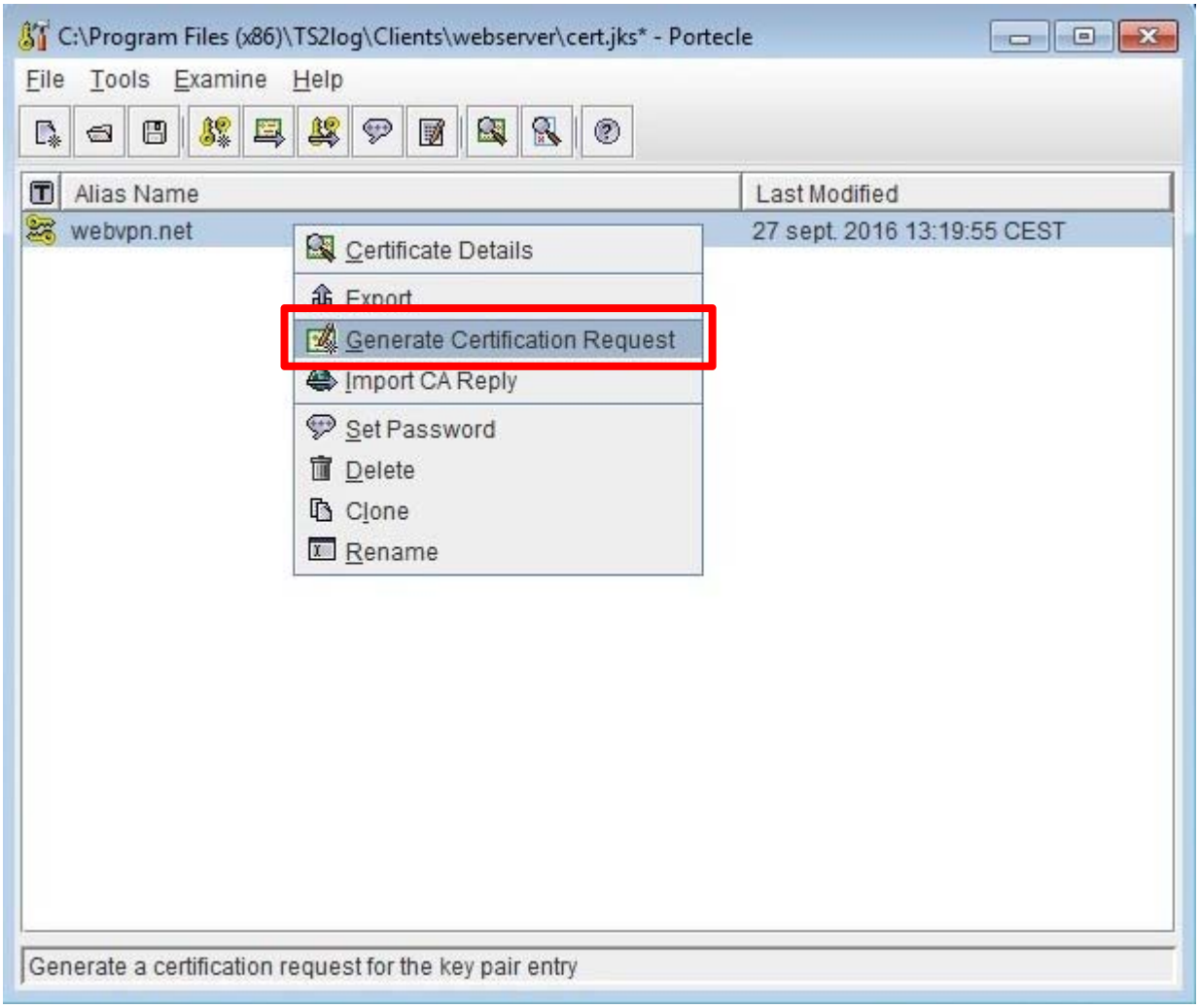
9. Par défaut, votre alias doit être identique au Common Name (CN) que vous avez déclaré précédemment.



10. Entrez le nouveau mot de passe de la paire de clé : "**secret**".

11. Vous verrez alors le message "**Key Pair Generation Successful**."

12. Vous devez maintenant générer un "CSR" (requête de certification) à transmettre à votre fournisseur de certificat par un clic droit sur la nouvelle paire de clés que vous venez de créer et en sélectionnant « **Generate Certification Request** ».



13. Sauvez le CSR dans le dossier de votre choix.

14. Ouvrez le CSR avec bloc-notes ou un éditeur de texte.

15. Sélectionnez tout le texte contenu dans le CSR à partir de « ------BEGIN CERTIFICATE REQUEST----- et jusqu'à -----END CERTIFICATE REQUEST-----». Vous aurez besoin ultérieurement de copier et coller ce texte dans le générateur SSL de votre fournisseur.

16. Avant de lancer la demande de certificat auprès de votre fournisseur, vous devez vous assurer que les informations relatives à votre nom de domaine sont à jour et correctes.

    PS : les illustrations suivantes ont été réalisées avec le service SSL du fournisseur **GoDaddy**

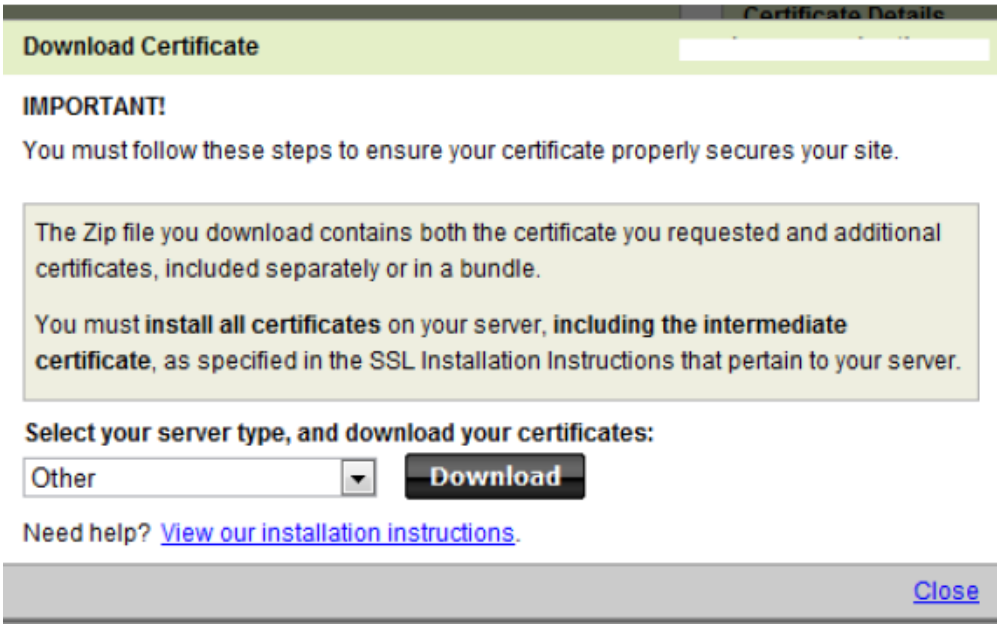
17. Loggez-vous dans votre compte chez le fournisseur. (GoDaddy dans cet exemple)
18. Dans l'onglet **Product**, sélectionnez **SSL Certificates**.
19. Choisissez SSL credit et montant désiré puis cliquez **Set Up**.
20. Cliquez "**Launch**" pour le certificat SSL que vous venez d'activer.
21. Si c'est votre premier certificat, vous devez valider votre agrément aux **conditions de souscription**.
22. Cliquez sur le dossier "**Credits**" sur la gauche.
23. NOTE: le nouveau montant de crédit s'affichera comme « **New Certificate** ». si vous ne le voyez pas, attendez un peu puis rafraichissez le navigateur.

24. Cliquez "**Request Certificate**" à coté du crédit du certificate que vous désirez activer.
25. Sélectionnez le type d'hébergement approprié pour votre certificat:
26. Sélectionnez "**Third Party**" ou "**Dedicated Server**" ou "**Virtual Private Server (VPS) without Simple Control Panel**", puis saisissez le "certificate signing request" (CSR) dans le champ prévu à cet effet. Vous devrez copier/coller le "Certification Request" (CSR) à partir du bloc-notes comme mentionné à l'étape précédente.
27. Faites votre choix de l'organisation de délivrance du certificat. Pour plus d'information, voir le chapitre « **Using the Right Issuing Organization for Your SSL**".
28. Cliquez sur "**Next**".
29. Choisissez votre préférence pour valider le domain pour lequel vous demandez ce certificat, puis cliquez sur **Next**.
30. Vérifiez l'exactitude de la requête puis cliquez sur "**Next**".

Après envoi de la requête vous pouvez suivre sa progression dans le dossier «Pending Requests ».Surveillez également les instructions qui pourraient vous être envoyées par mail.
Si votre domaine et votre hébergement sont dans des comptes différents, vous devrez mettre à jour le « A record » pour votre domaine avec la nouvelle adresse IP.
Voir le paragraphe « Finding Your Hosting Account's IP Address" pour plus d'information.
Pour savoir comment mettre à jour le champ "A record" de votre domaine, voir les infos dans "Managing DNS for Your Domain Names".

NOTE: Votre site peut être inaccessible jusqu'à ce que vous mettiez à jour le « A record ».

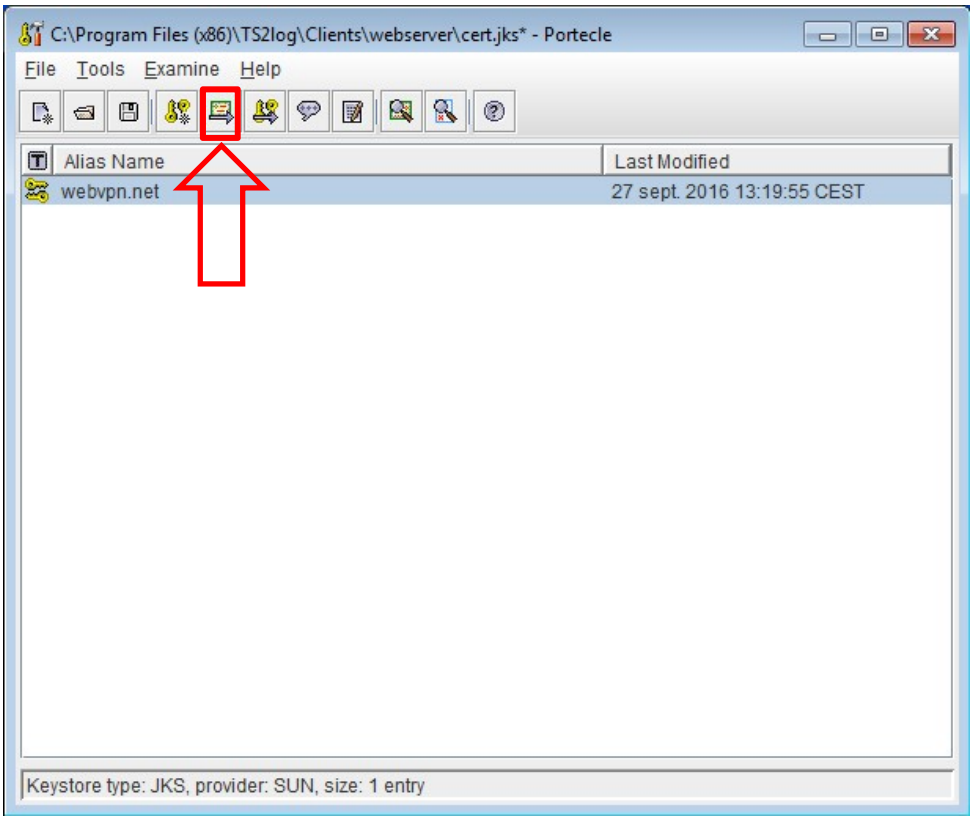
31. Sélectionnez Après la demande de certificat chez GoDaddy et la configuration de votre DNS, vous devrez importer le certificat SSL dans TS2log.
32. Sélectionnez le certificat commandé dans le Manager SSL et cliquez sur le bouton **Download**.
33. Sélectionnez le type de serveur "**Other**" et cliquez de nouveau sur **Download**.



34. Sélectionner un dossier pour fichier .ZIP et extrayez son contenu
35. Il contient votre certificat SSL xxxx.com.crt et un package de certificats intermédiaires.
36. Portecle ne permet pas l'importation des certificats packagés donc vous pouvez ignorer et supprimer ce package. Avant l'import de votre certificat, vous devez importer les certificats intermédiaires.
37. Ouvrez l'url https://certs.godaddy.com/anonymous/repository.seam pour télécharger les certificats racines qui sont requis pour votre importation de la réponse du CA.
    - Télécharger les deux composants suivants :
        - Go Daddy Class 2 Certification Authority Root Certificate: *gd-class2-root.crt*
        - Go Daddy Secure Server Certificate (Intermediate Certificate): *gd_intermediate.crt*

➢

38. Dans le Portecle cliquez sur le bouton **Import Trusted Certificate**.



39. Recherchez les 2 certificats intermédiaires et importés les.
40. Une fois importés cliquez droit sur la paire de clés et sélectionnez **Import CA Reply** en naviguant vers le certificat SSL téléchargé comme indiqué précédemment et importez le fichier.
41. Cliquez sur **File**: puis sur **Save** pour sauvegarder les changements dans le fichier keystore et relancez les services web de TS2log.
42. Testez en vous rendant sur l'adresse web HTTPS:\\ et vous ne devriez plus avoir d'alerte concernant le certificat SSL. La connexion est désormais sécurisée par un certificat signé par une autorité de confiance officielle.