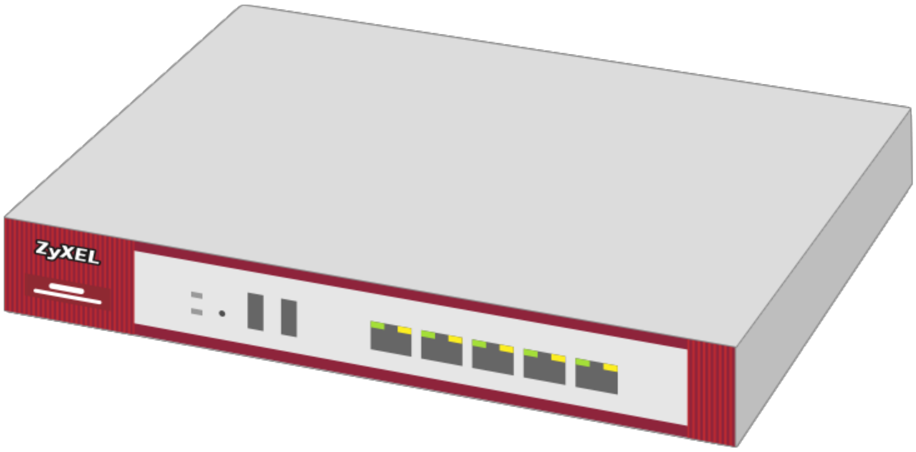


Importation d'un certificat personnel

Série firewall Zyxel
à partir du firmware version 4.33

Knowledge Base KB-3810
février 2019

IMPORTATION D'UN CERTIFICAT PERSONNEL

Ces instructions décrivent le remplacement d'un certificat auto-signé par un certificat signé publiquement, à l'exemple d'un certificat SSL wildcard de Let's Encrypt. Le certificat a été créé via https://www.sslforfree.com.

Nous utilisons OpenSSL pour préparer les certificats au importation sur un pare-feu. Win32 OpenSSL est disponible sur la page du fabricant : https://slproweb.com. Ces étapes sont nécessaires qu'une seule fois pour la préparation des certificats et ne sont plus pertinentes pour une utilisation ultérieure des certificats.

Préparation de OpenSSL :

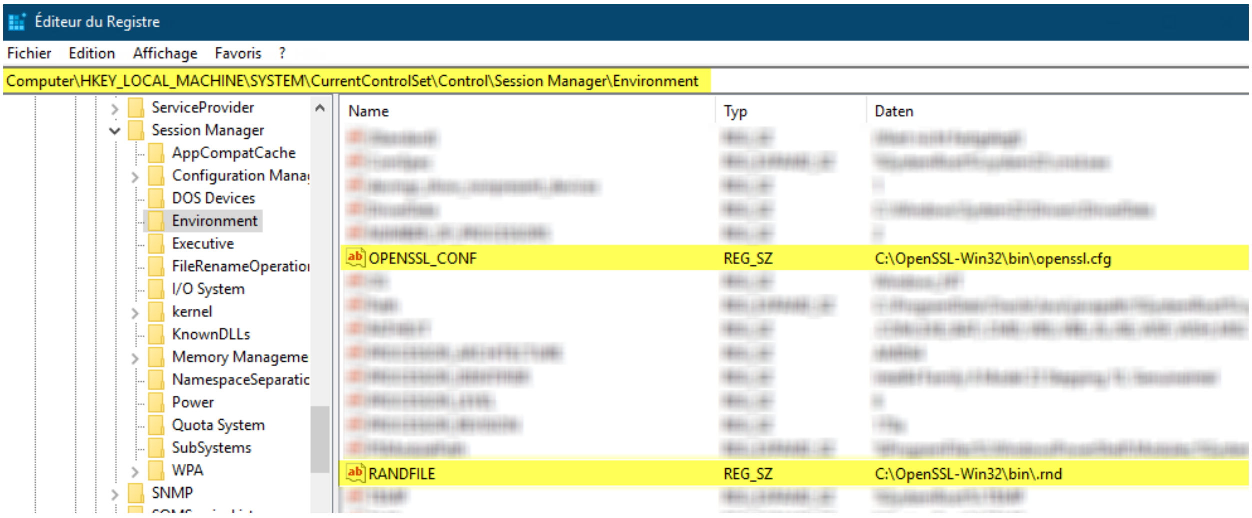
Dans cet exemple, OpenSSL est installé dans le répertoire C:\OpenSSL-win32\. Si un autre répertoire est utilisé, cela doit être adapté en conséquence. Le certificat et la clé privée se trouvent dans le répertoire C:\OpenSSL-win32\bin.

Pour que OpenSSL fonctionne correctement avec Windows, il faut définir deux variables d'environnement. Cela peut se faire avec l'éditeur du registre (regedit.exe) dans le répertoire suivant (regedit.exe) :

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Environment

1. type : chaîne de caractères, nom : RANDFILE, valeur : C:\OpenSSL-win32\.rnd
2. type : chaîne de caractères, nom : OPENSSL_CONF, valeur : C:\OpenSSL-win32\bin\openssl.cfg

Le PC doit être redémarré pour que les paramètres prennent effet.



Création du certificat privé (PKCS#12)

Pour créer le certificat, OpenSSL.exe est démarré depuis le répertoire C:\OpenSSL-win32\bin. La génération s'effectue avec les commandes suivantes :

OpenSSL> *pkcs12 -export -in* **certificate.crt** *-inkey* **private.key** *-out* **cert.pfx**
Enter Export Password
Verifying - Enter Export Password

Type du certificat à exporter : pkcs12
Certificat d'origine : -in (commande pour l'importation) + nom du certificat
Clé privée : -inkey (commande pour l'importation) + nom de la clé
Certificat exporté : -out (commande pour l'exportation) + nom du certificat privé avec l'extension .pfx

Si le certificat ou la clé privée se trouvent dans un autre répertoire ou si le certificat doit être exporté vers un dossier différent, il faut indiquer le chemin entier.

p. ex. C:\User\Nom d'utilisateur\Documents\certificate.crt

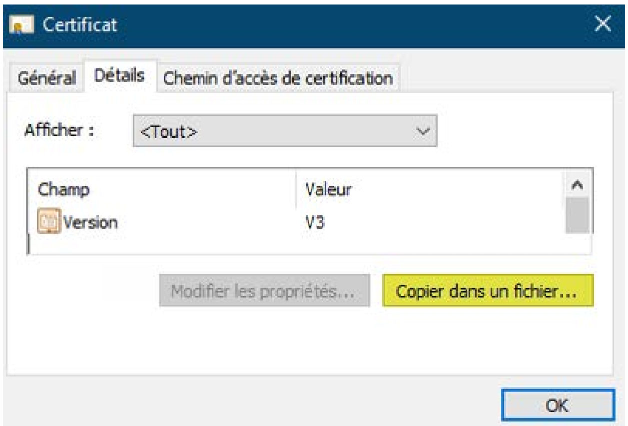
Export Password : ce mot de passe est nécessaire pour l'importation du certificat sur l'USG. Sans ce mot de passe, l'installation n'est pas possible.

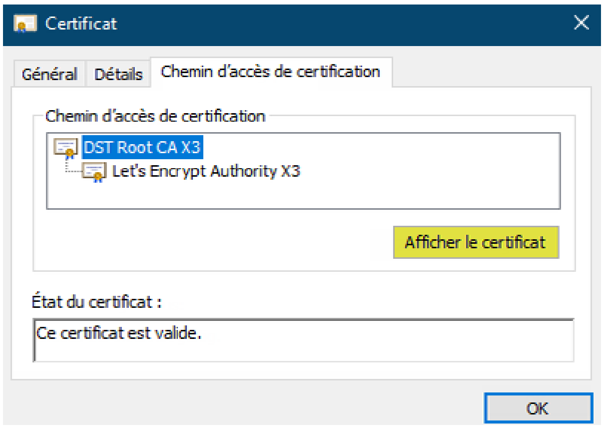
Certificat Root et Intermediate

Les certificats Root et Intermediate ne peuvent pas être importés en tant que bundle. Si un bundle est uniquement disponible, les différents certificats doivent être extrait du bundle.

Pour extraire le certificat Intermediate, il faut ouvrir le paquet de certificats et démarrer l'assistant d'exportation sous *Détails > Copier dans un fichier...* Pour l'exportation, les paramètres définis peuvent être utilisés.

Il est possible d'afficher le certificat Root sous *Chemin d'accès de certification > [certificat Root] > Afficher le certificat.* L'exportation s'effectue de la même manière.

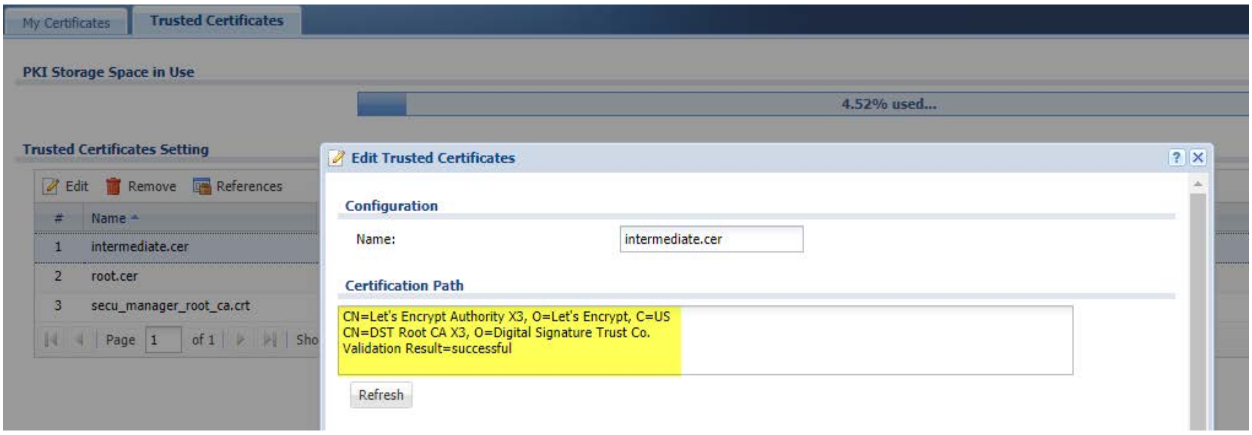




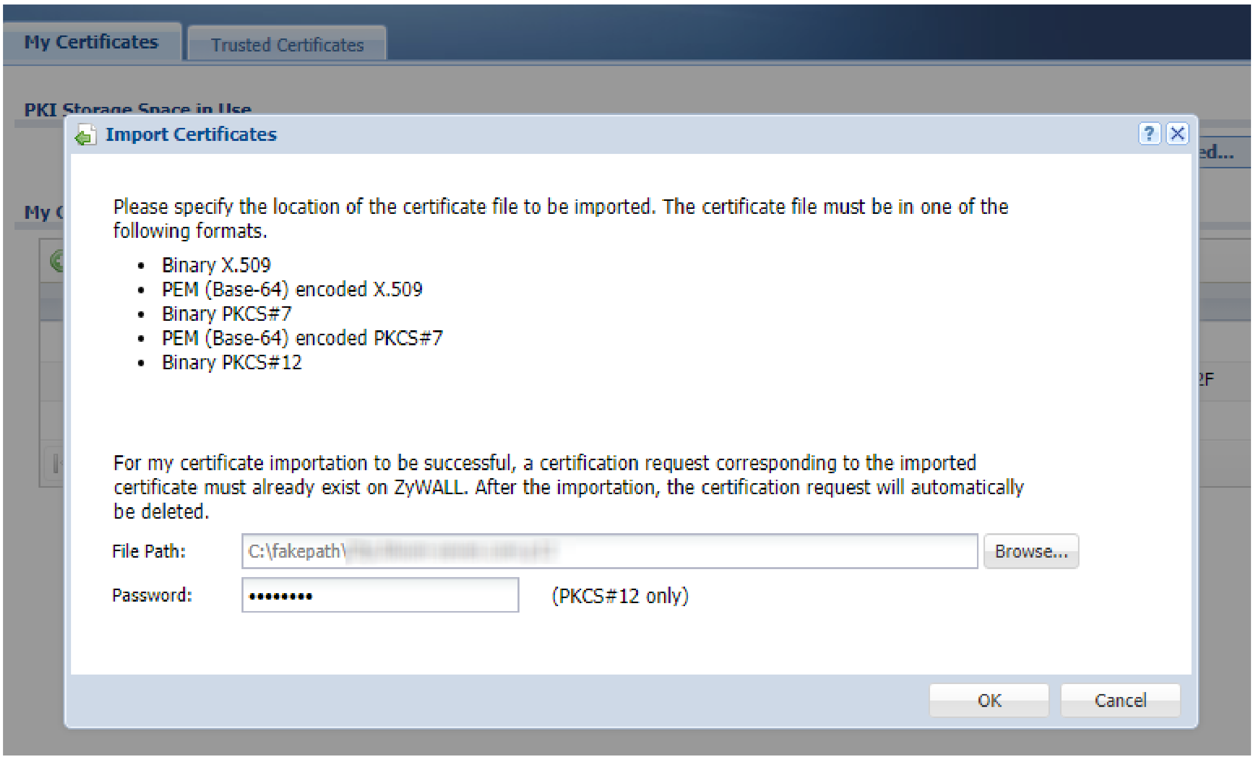
Importation sur l'USG

Sur l'USG, il faut d'abord importer le certificat Root et puis le certificat Intermediate sous Configuration > Object > Certificate > Trusted Certificates > Import.

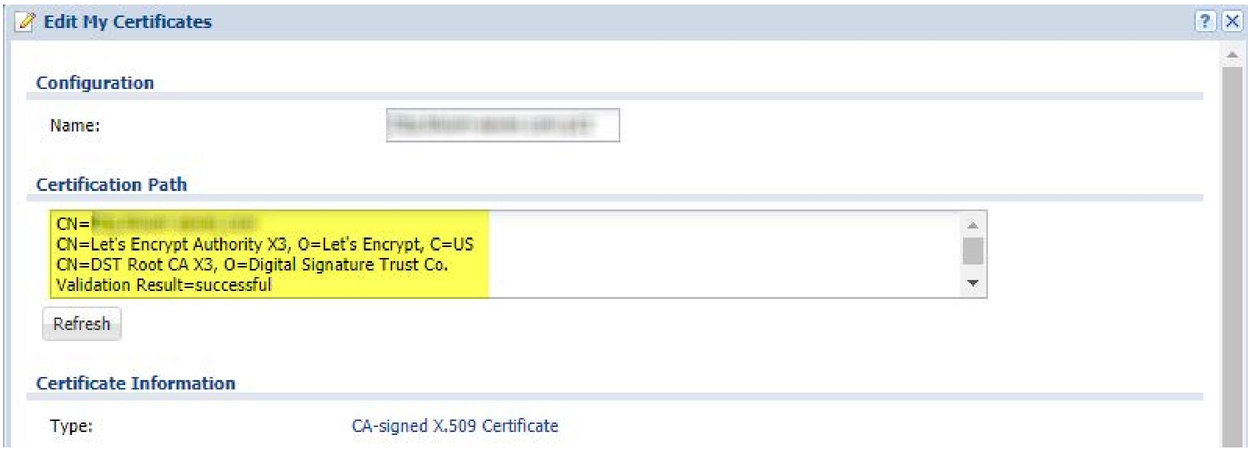
Validation Result=successful confirme la réussite de l'importation du certificat Intermediate.



Le certificat PKCS#12 est installé sous My Certificates. Le mot de passe du certificat doit être indiqué lors de l'importation.



Aussi ici le message Validation=successful est affiché en cas d'une importation correcte.



Sous Configuration > System > WWW > Service Control > HTTPS > Server Certificate, le certificat peut ensuite être utilisé pour l'accès à l'USG.

L'accès est maintenant possible sans message d'erreur du certificat :