



Configuration Adobe XI sous Windows pour signer avec un Produit LuxTrust

V 1.0

24/03/2015
Français

Disclaimer

Ce document ne peut être reproduit en totalité ou en partie sans le consentement écrit préalable et explicite de LuxTrust SA. Des droits d'auteur de tiers peuvent exister pour les parties de cette documentation. LuxTrust SA décline toute responsabilité pour les dommages directs, indirects, spéciaux, indirects ou consécutifs à des dommages matériels ou autres en quelque sorte liée à ou découlant de l'exécution de tous les conseils donnés dans le présent document. Ce document est fourni "tel quel" et rien n'est prévu en termes d'adéquation à un usage particulier ou de l'applicabilité. En faisant usage de ce document, l'utilisateur accepte de l'utiliser à ses propres risques et comprend que ce document ne peut être fourni sans ces limitations.

Contents

I	Etape préliminaire	3
II	Ajout Module PKCS#11	4
III	Ajout des certificats racine dans Adobe.....	7
III.1	Pour les clients d'une Smartcard ou Signing Stick :.....	12

I Etape préliminaire

Veuillez ouvrir votre Adobe, ici veuillez ouvrir le Menu Edit et puis sélectionnez Préférences. (voir flèche rouge dans Figure 1)

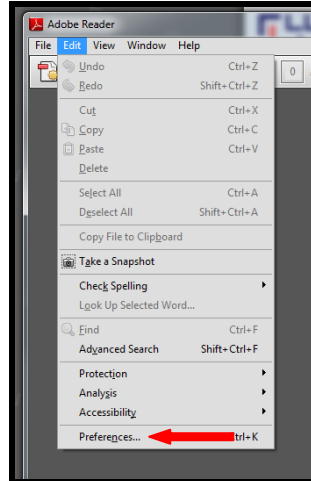


Figure 1

Dans le menu veuillez sélectionner « Security (Enhanced » et puis décochez « Enable Protected Mode » (voir flèche rouge dans figure 2)

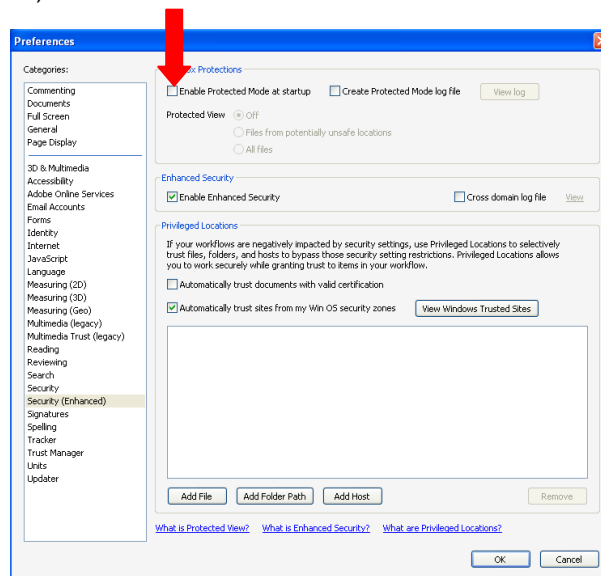


Figure 2

II Ajout Module PKCS#11

Voici les étapes pour ajouter le module PKCS#11 dans l'Adobe Reader XI:

Pour les clients utilisant un Signing Stick ou une Smartcard, veuillez vérifier si votre Gemalto est correctement installé et opérationnel.

Appuyez sur le bouton « Edit » et naviguez jusqu'au menu « Preferences... ».(figure 3)

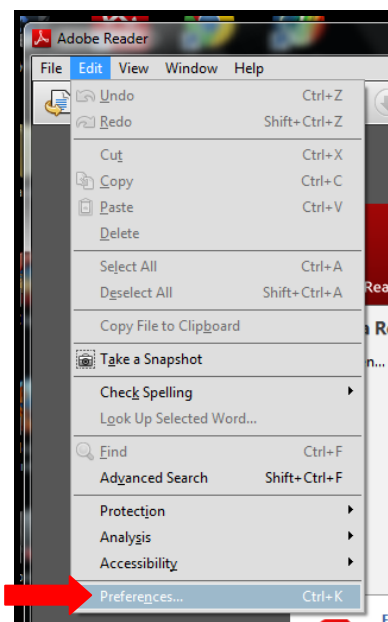


Figure 3

La fenêtre Préférences va s'ouvrir, veuillez sélectionner ici, le menu « Signatures » (voir figure 4)

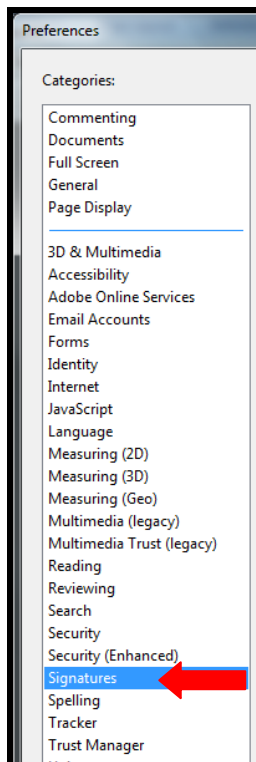


Figure 4

Puis sur le côté droit de votre fenêtre vous trouvez le bloc “Identities & Trusted Certificates, cliquez ici sur “More...”; (voir figure 5)

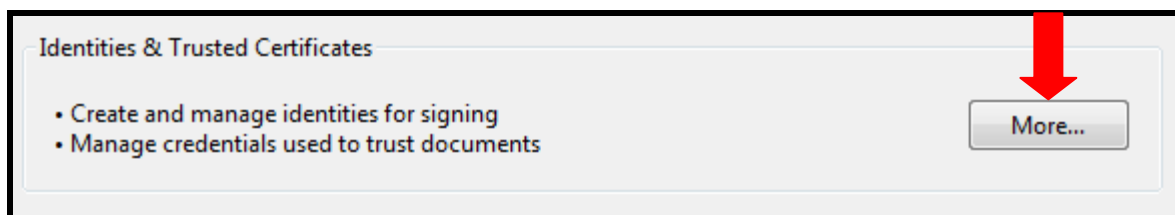


Figure 5

Dans la prochaine fenêtre s'affiche, le menu « PKCS#11 Modules and Tokens », veuillez le sélectionner (voir Figure 6) Puis appuyez sur le bouton « **Attach Module** » pour pouvoir charger le module PKCS#11 (voir cercle rouge Figure 6). Si vous ne pouvez pas sélectionner « **Attach Module** », et votre version Adobe vous affiche qu'il démarre en mode « protection », alors il faut changer cette configuration et réessayer encore une fois.

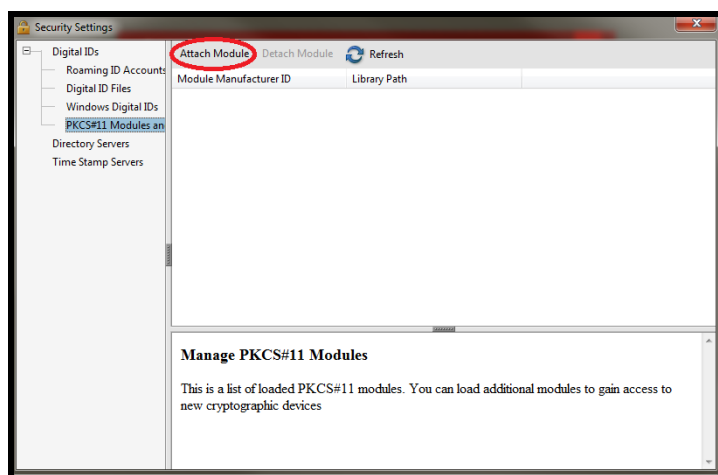


Figure 6

La fenêtre suivante va s'ouvrir, veuillez choisir ici le répertoire où vous avez sauvegardé le programme Gemalto. Pour les clients d'une Smartcard ou d'un Signing Stick, veuillez sélectionner le fichier « gclib.dll », dans le répertoire C:\Program Files\Gemalto\Classic Client\BIN valider votre choix avec « ouvrir » (Figure 7)

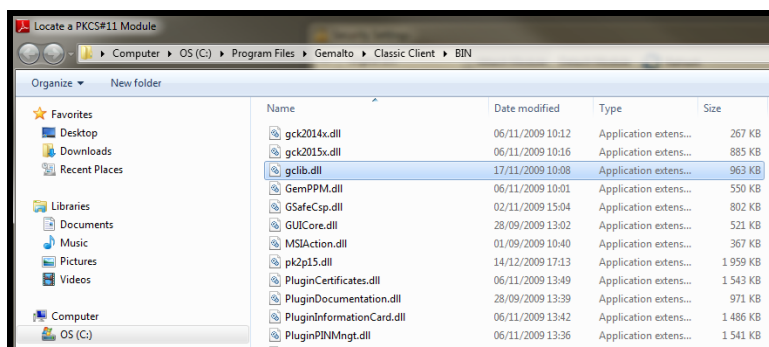


Figure 7

Attention pour les clients utilisant une version Windows de 64bit veuillez prendre C:/Program Files

86...

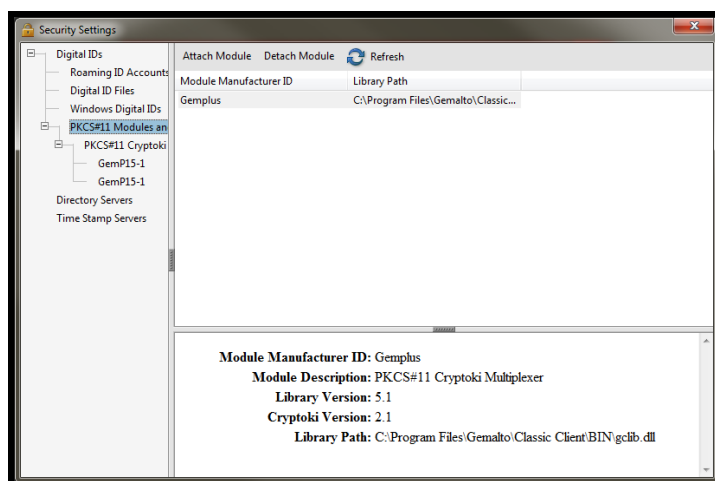


Figure 8

Lorsque vous avez terminé l'ajout du module PKCS#11 la fenêtre suivante va s'afficher et vous pouvez la fermer et commencer à signer vos documents. (Figure 8)

III Ajout des certificats racine dans Adobe

Appuyez sur le bouton « Edit » et naviguez jusqu'au menu « Preferences... » et ouvrez-le.

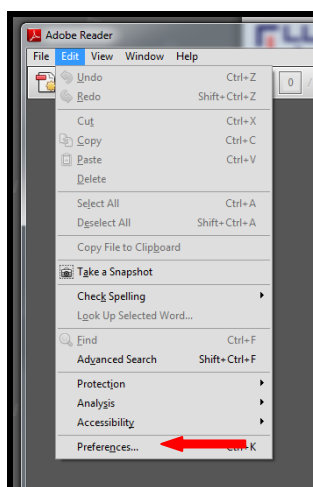


Figure 9

La fenêtre « Preferences » va s'ouvrir, veuillez sélectionner ici, le menu « Signatures » (voir figure 10)

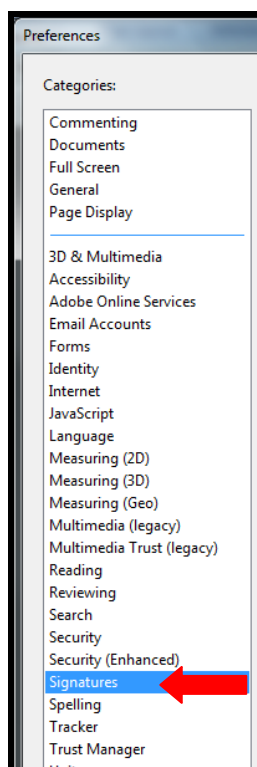


Figure 10

Puis sur le côté droit de votre fenêtre vous trouvez le bloc "Identities & Trusted Certificates, cliquez ici sur "More..."; (voir figure 10)

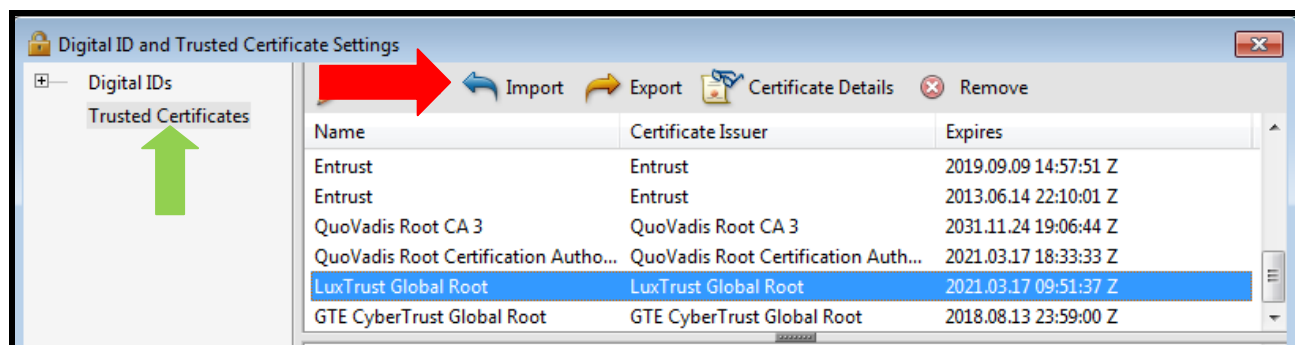


Figure 10a

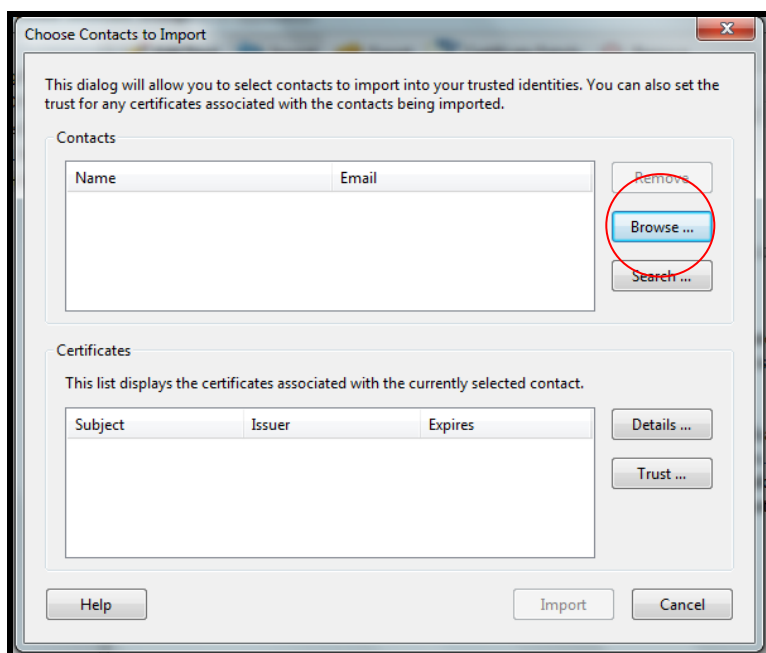


Figure 11

Vérifiez si le LuxTrust Global Root CA (DER) est installé dans les certificats d'Adobe, (voir flèche rouge, dans Figure 10a).

Si le certificat n'est repris dans la liste, veuillez le sauvegarder sur votre desktop à partir de notre site internet : <https://www.luxtrust.lu/fr/simple/191> . Puis cliquez sur « Import » (flèche rouge, dans la figure 10a) et sélectionnez ici « Browse » (cercle rouge, voir dans la figure 11).

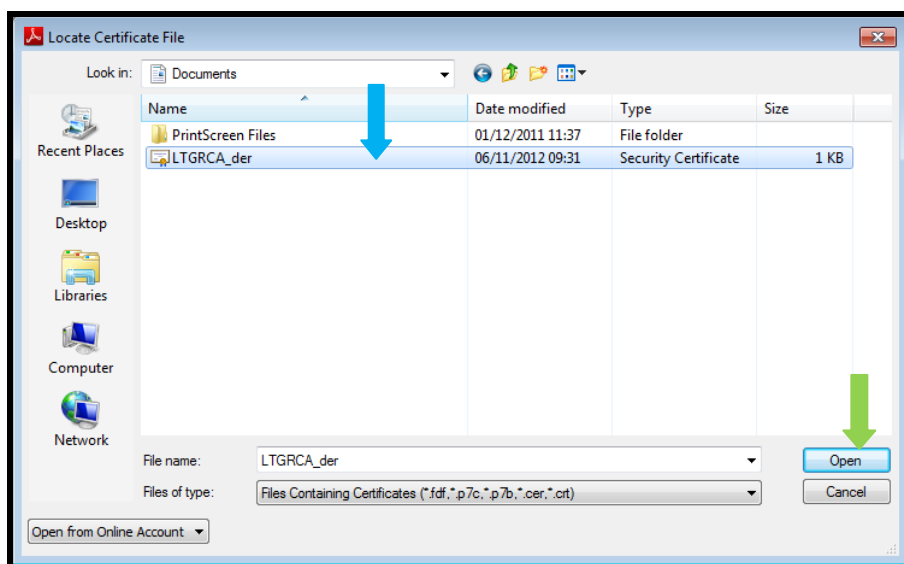


Figure 12

Sur la prochaine fenêtre le certificat que vous venez de télécharger va s'afficher, voir figure 13

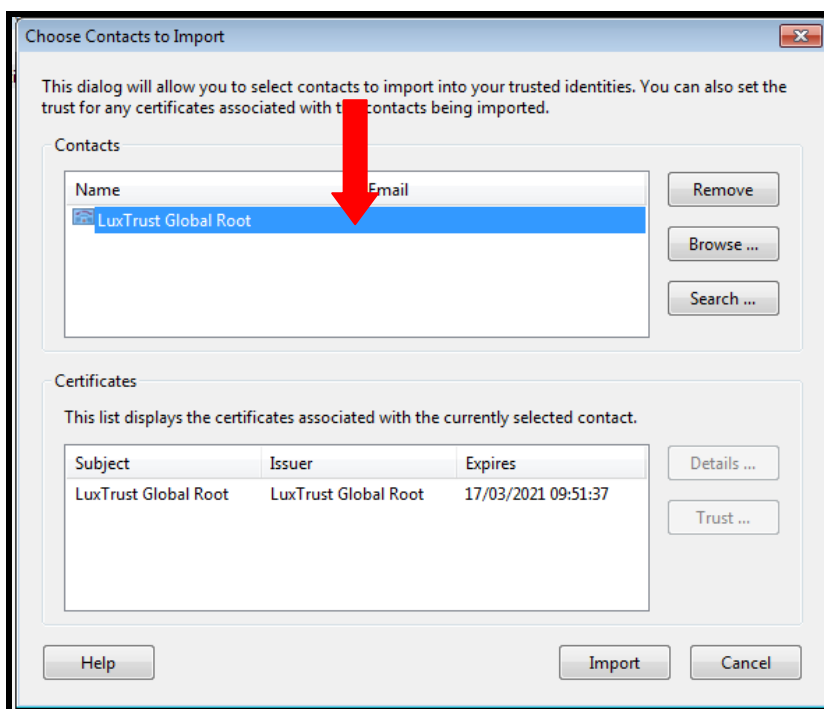


Figure 13

Sélectionnez maintenant le certificat dans la partie en bas, « Certificates ».

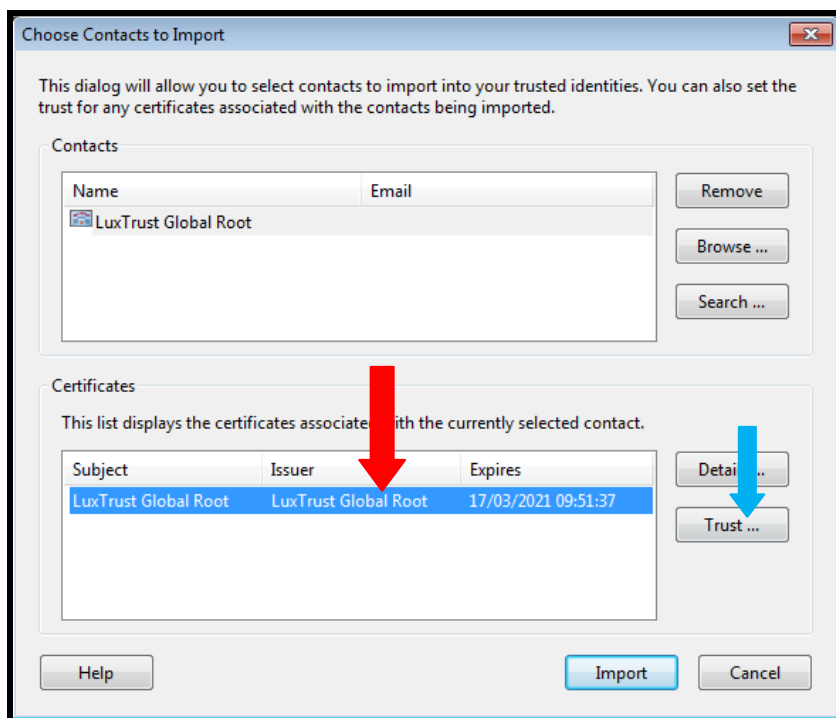


Figure 14

Puis cliquez sur « Trust... », voir dans la figure 14, la fenêtre suivante va s'afficher (voir figure 15). Cochez ici « Use this certificate as a trusted root » et validez votre modification en cliquant sur « OK ».

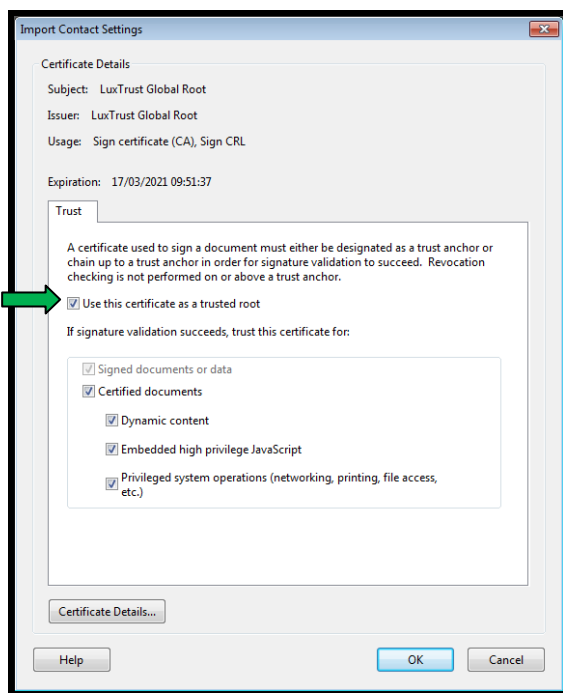


Figure 15

Cliquez sur « Import » (voir figure 16) pour installer le certificat dans l'Adobe Reader, puis fermer le programme et redémarrer-le.

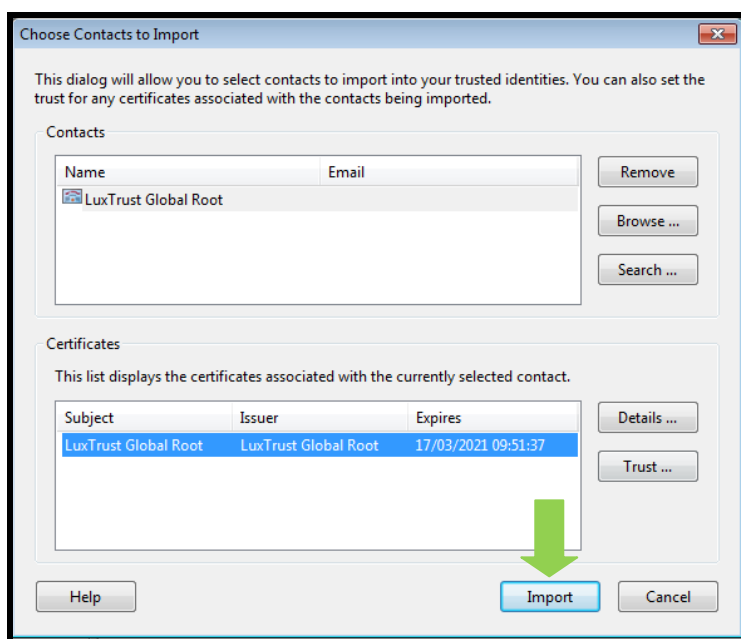


Figure 16

III.1 Pour les clients d'une Smartcard ou Signing Stick :

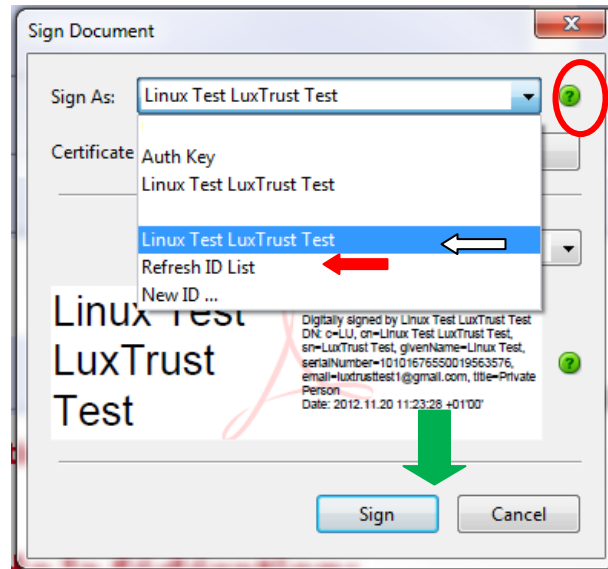


Figure 17

Sélectionnez la petite flèche noir (voir cercle rouge dans la figure 17), afin de pouvoir ouvrir le menu déroulant, dans ce menu veuillez sélectionner la deuxième ligne avec votre nom, dans notre exemple il s'agit du Linux Test LuxTrust Test (voir flèche blanche dans la figure 17). Sélectionnez cette ligne et cliquez sur « sign », (voir flèche verte dans la figure 17). Afin de confirmer votre Signature vous devez encore saisir votre code Pin de votre Smartcard ou Signing Stick.

Si « votre nom ne s'affiche pas, veuillez cliquer sur « Refresh ID List », (voir flèche rouge dans la figure 17).

Si vous ne voyez toujours pas « votre nom », veuillez revoir les étapes de ce guide.

Si après vérification vous ne voyez toujours pas l' « votre nom », alors désinstaller complètement l'Adobe Reader XI et recommencer la configuration.