

FICHE D'APPLICATION	CREATION DES AUTORITE , CERTIFICATS , CLES A PARTIR D'UN FICHER .XDB
P400XI – Autorité Certificats Clés	

REPertoire DES EVOLUTIONS

Version	Date	Auteur	Nature des modifications	Pages
E				
D				
C	17/07/20	Pascal Nguyen	Sauvegarde	8
B	19/05/20	Pascal Nguyen	Ajout Nota	1/2/3/5
A	25/02/20	Pascal Nguyen	Création du document	Toutes

1 DOCUMENTS ET LOGICIELS DE REFERENCE

- Logiciel XCA : setup_xca
- Document : DO_P400XI_NOTETECH_OPENVPN_XCA.pdf
- Document : DO_P400XI_NOTETECH_OPENVPN_PKI.pdf
- Fichier avec extension xdb modele_perax.xdb contient autorité, certificats et clés

2 LOGICIEL

Installation du logiciel setup_xca.

3 EXEMPLE DE PROJET

Considérons une configuration avec un PC (de supervision) et 3 P400Xi. Le PC (de supervision) sera le serveur VPN **et** un client ; les 3 P400Xi seront 3 clients.

Donc on va configurer :

- * 1 serveur (PC de supervision)
- * 4 clients (PC de supervision et P400Xi)

Considérons une configuration avec 3 PC et 12 P400Xi. Le premier PC sera mon serveur VPN ; un PC sera une console pour visualiser les 12 P400Xi, et le troisième sera mon poste de supervision.

Donc on va configurer :

- * 1 serveur (PC n°1)
- * 14 clients (PC de console + PC de supervision + 12 P400Xi)

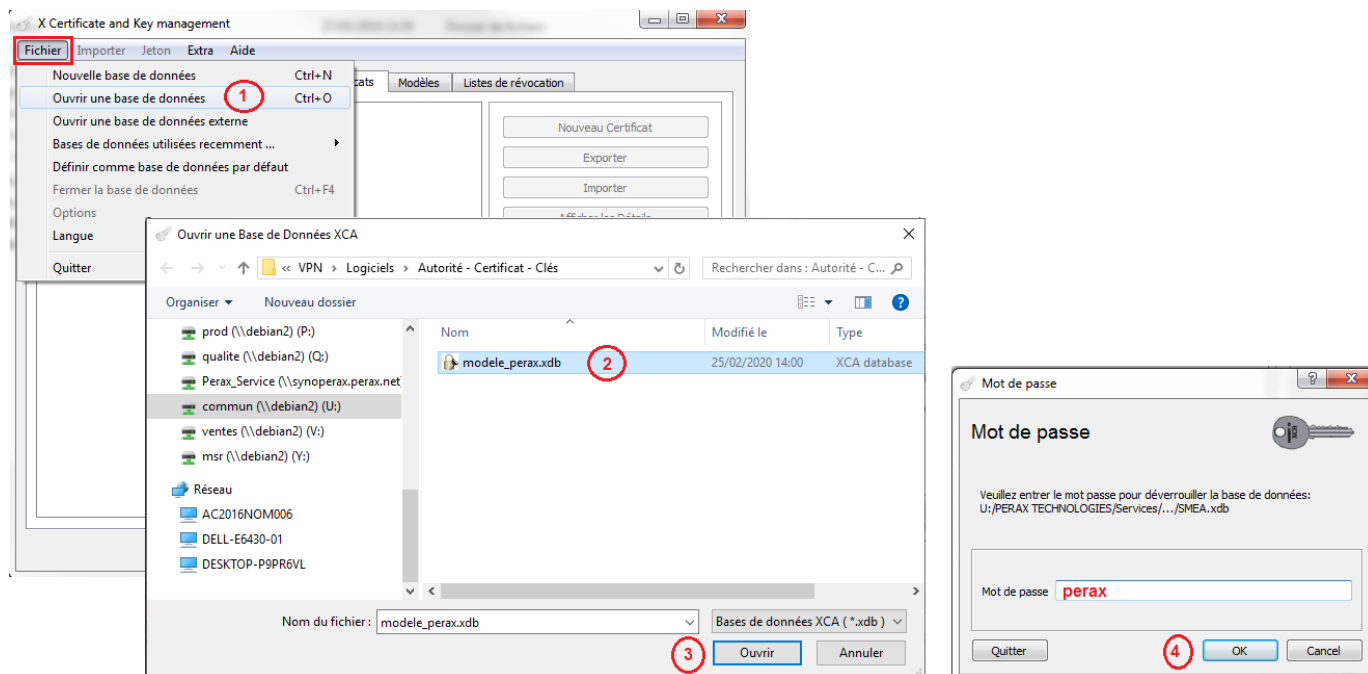
Nota : le serveur VPN peut être installé dans une machine virtuelle (VM) installée elle-même dans la même machine physique que le logiciel de supervision par exemple .

Dans cette situation on aura par exemple :

- Une machine virtuelle VM où sera installé le serveur VPN
- Pc de supervision machine physique client VPN du serveur VPN
- Un parc d'automates de télégestion clients du même serveur VPN

4 OUVERTURE BASE DE DONNEES

Lancer le logiciel XCA et ouvrir la base de données fournie : modele_perax.xdb . Le mot de passe est **perax** .

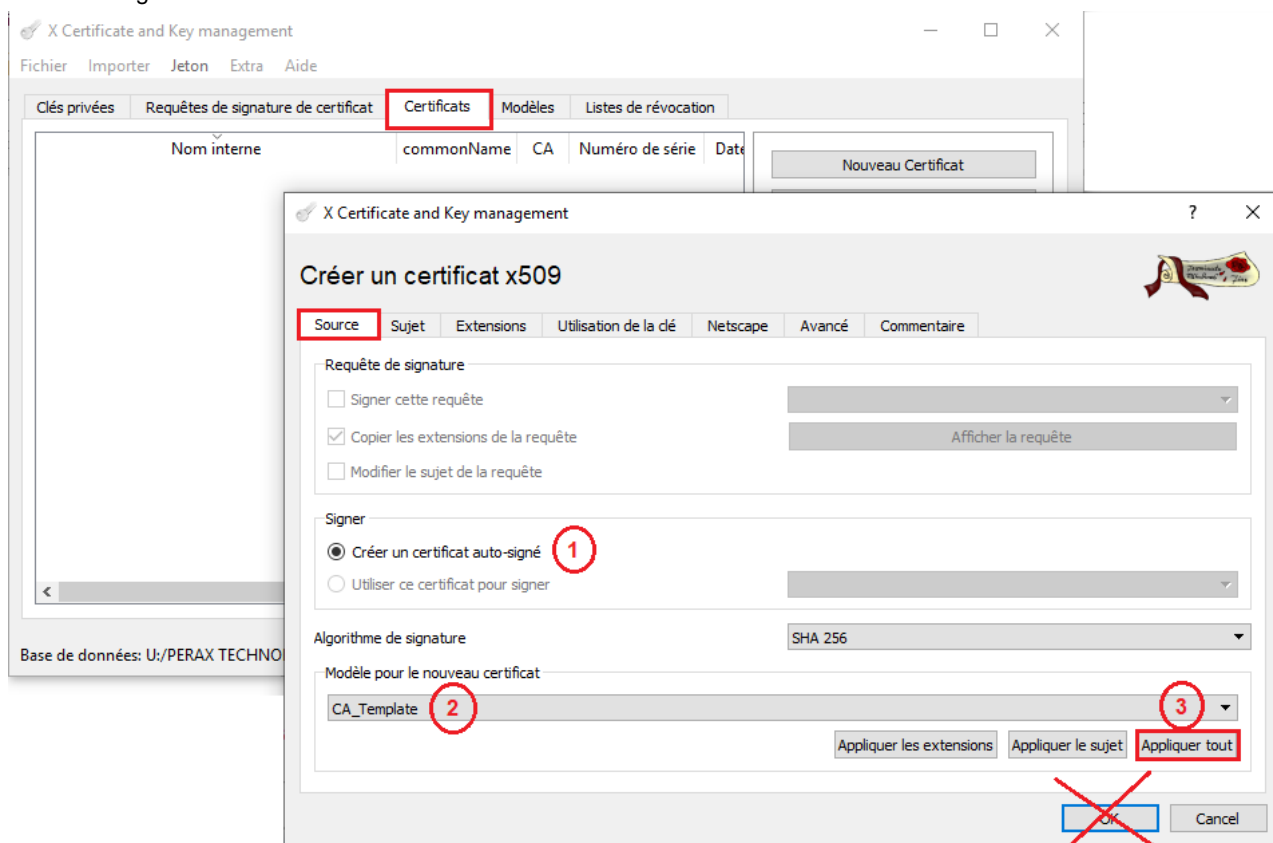


Nota : si à l'ouverture de la base de donnée, des certificats et des clés apparaissent, les détruire tous avant de commencer .

5 CREATION DU CERTIFICAT DE L'AUTORITE

L'autorité de certification signe les certificats et les équipements ayant été signés par cette autorité. On pourra utiliser openvpn et un réseau VPN dans notre projet.

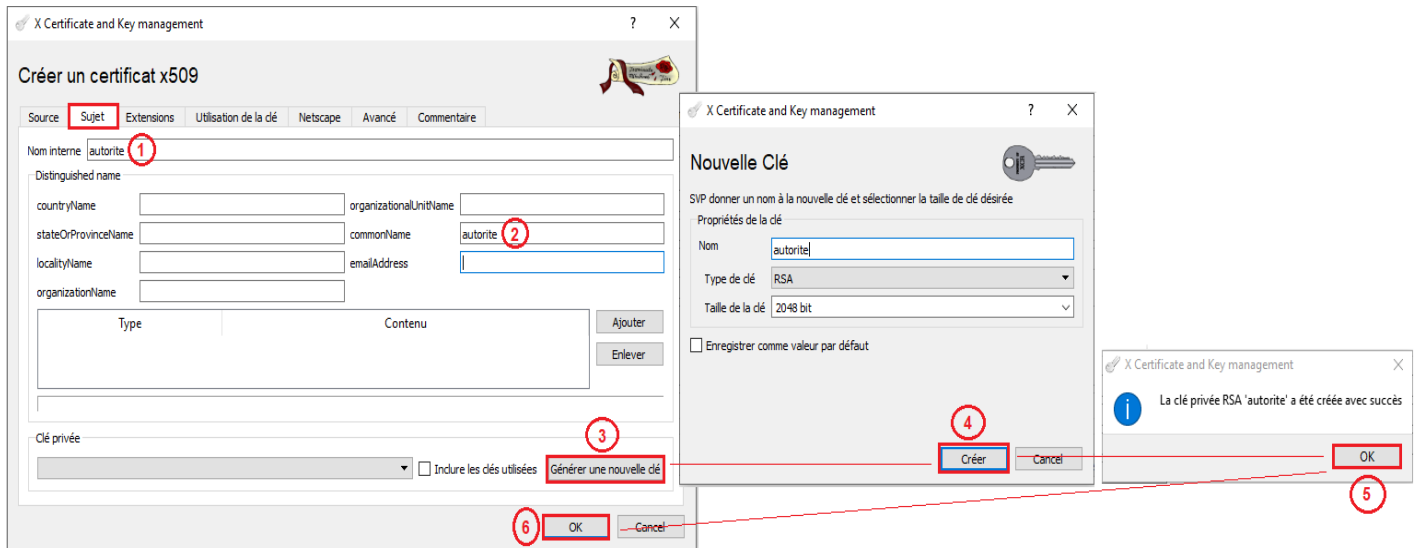
Dans les onglets Certificats – Source :



- Repère 1 : garder l'auto-signature
- Repère 2 : sélectionner le modèle CA_Template
- Repère 3 : cliquer sur le bouton «Appliquer tout»

Ne surtout pas cliquer sur le bouton OK

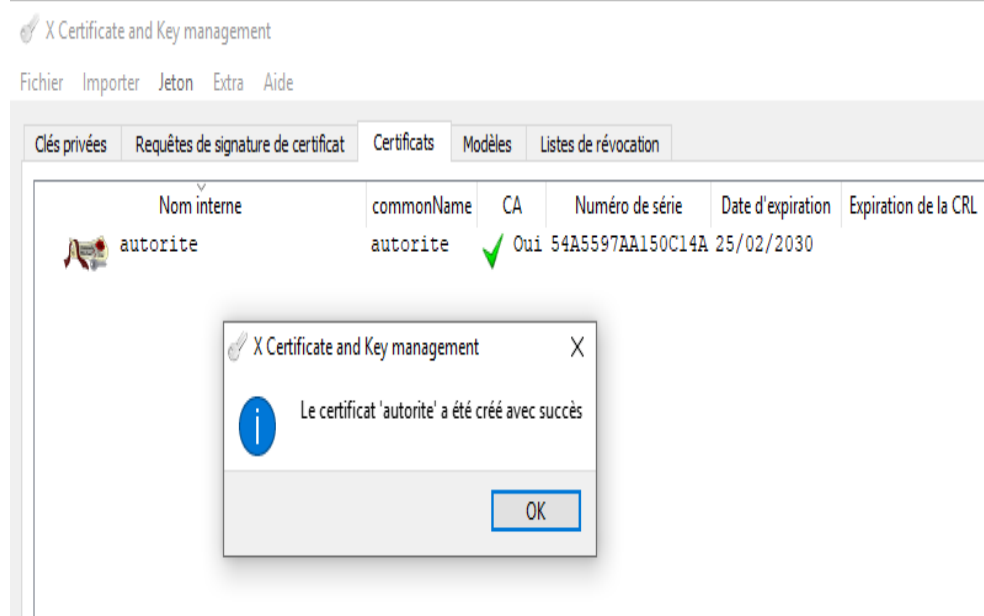
Dans les onglets Certificats – Sujet :



Nota 1 : ne pas mettre d'espace si le nom donné à l'autorité comprend plusieurs mots .

Nota 2 : en 2, indiquer la même chose qu'en 1 .

Le message suivant apparaît :

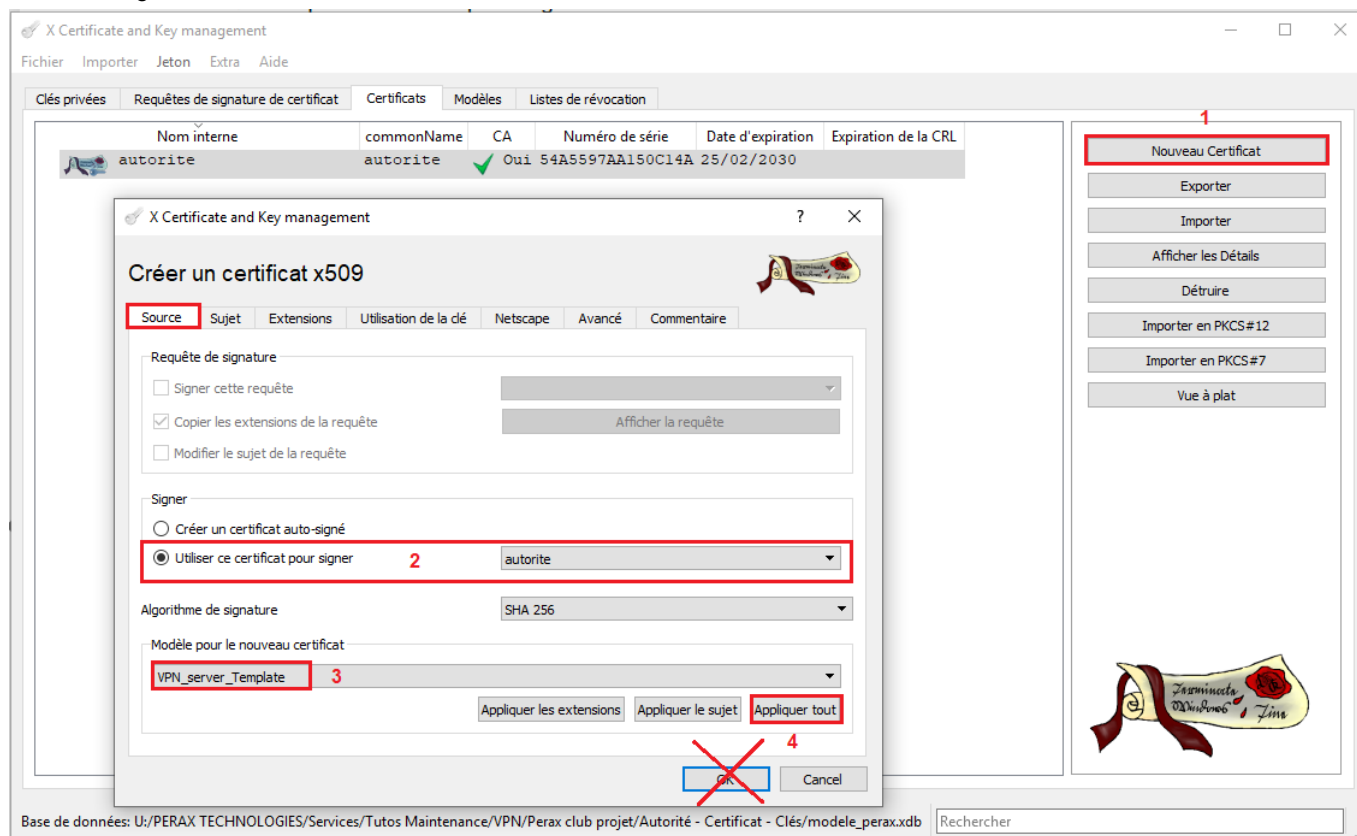


Suite à l'activation de «OK» du chapitre précédent , une fenêtre s'affiche pour signifier que le certificat autorisé a été créé et la liste des certificats est actualisé.

6 CREATION DU CERTIFICAT DU SERVEUR

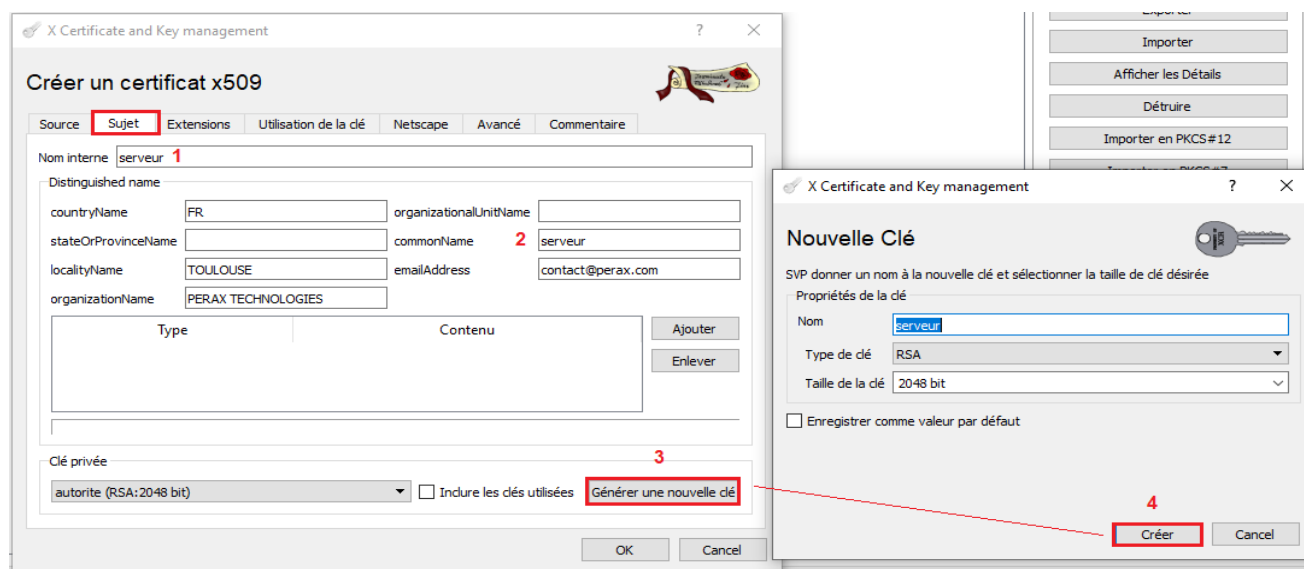
Nous allons créer le certificat du serveur .

Dans les onglets Certificats – Source :



- Repère 1 : l'activation de ce bouton a provoqué l'affichage de cette fenêtre
- Repère 2 : choisir l'option de signature du certificat - vérifier que le signataire est bien l'autorité de certification
- Repère 3 : choisir le modèle correspondant à un serveur VPN
- Repère 4 : activer le bouton «Appliquez tout» pour appliquer le modèle

Ne surtout pas cliquer sur le bouton OK



Dans les onglets Certificats – Sujet :

- Repère 1 : choisir le même nom du serveur
Nota : ne pas mettre d'espace si le nom donnée au serveur comprend plusieurs mots .
Nota 2 : en 2, indiquer la même chose qu'en 1 .
- Repère 2 : cliquer sur «Générer une nouvelle clé» pour générer la clé privée protégeant ce certificat

Dans les onglets Certificats – Extensions : définir la durée de validité du certificat . Exemple : 10 ans .

Créer un certificat x509

Source Sujet **Extensions** Utilisation de la clé Netscape Avancé Commentaire

X509v3 Basic Constraints
 Type: Entité Finale
 Distance aux entités finales: ☐ Critical

Key identifier
☒ Subject Key Identifier
☐ Authority Key Identifier

Validité
 Pas avant: 2020-02-25 15:06 GMT
 Pas après: 2030-02-25 15:06 GMT

Intervalle de temps: 10 Années Appliquer

Le certificat serait valide plus longtemps que son signataire. Ce n'est probablement pas ce qui est désiré.

Ajuster la date et continuer Modifier les limites de validité Interrompre le déploiement Continuer le déploiement

X509v3 Subject Alternative Name
 X509v3 Issuer Alternative Name
 X509v3 CRL Distribution Points
 Authority Information Access: OCSP

OK Cancel

Au final

X Certificate and Key management

Fichier Importer Jeton Extra Aide

Clés privées Requêtes de signature de certificat **Certificats** Modèles Listes de révocation

Nom interne	commonName	CA	Numéro de série	Date d'expiration	Expiration de la CRL
autorite	autorite	✓	54A5597AA150C14A	25/02/2030	
serveur	serveur	Non	6862CEF9AD4D9BB6	25/02/2030	

Le certificat 'serveur' a été créé avec succès

OK

7 CREATION DU CERTIFICAT DES CLIENTS

Il faut procéder exactement de la même manière que pour le serveur .

Les 2 seules différences :

- le choix de VPN_Client_Template dans la rubrique « Modèle de pour le nouveau certificat » .

X Certificate and Key management

Créer un certificat x509

Source | Sujet | Extensions | Utilisation de la clé | Netscape | Avancé | Commentaire

Requête de signature

- ☐ Signer cette requête
- ☒ Copier les extensions de la requête
- ☐ Modifier le sujet de la requête

Signer

- ☐ Créer un certificat auto-signé
- ☒ Utiliser ce certificat pour signer (autorite)

Algorithme de signature: SHA 256

Modèle pour le nouveau certificat: VPN_Client_Template

Appliquer les extensions | Appliquer le sujet | **Appliquer tout**

OK (crossed out) | Cancel

- le nom du premier client

X Certificate and Key management

Fichier | Importer | Jeton | Extra | Aide

Clés privées | Requêtes de signature de certificat | Certificats | Modèles | Listes de révocation

Créer un certificat x509

Source | **Sujet** | Extensions | Utilisation de la clé | Netscape | Avancé | Commentaire

Nom interne: **poste1**

Distinguished name

countryName	FR	organizationalUnitName	
stateOrProvinceName		commonName	poste1
localityName	TOULOUSE	emailAddress	contact@perax.com

Nouvelle Clé

SVP donner un nom à la nouvelle clé et sélectionner la taille de clé désirée

Propriétés de la clé

Nom: **poste1**

Type de clé: RSA

Taille de la clé: 2048 bit

☐ Enregistrer comme valeur par défaut

Créer | Cancel

Contenu

Ajouter | Enlever

☐ Inclure les clés utilisées | Générer une nouvelle clé

OK | Cancel

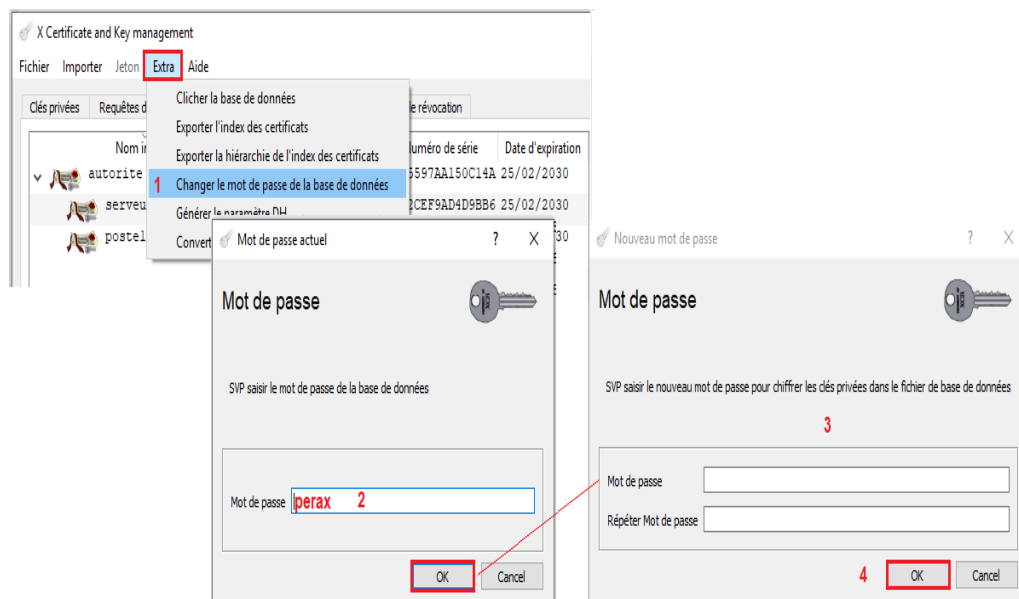
Remarques :

- il faut créer autant de clients qu'il y aura d'appareils connectés au VPN .
- dans les rubriques « Nom interne » et « commonName » vous devez indiquer le nom exact de l'appareil connecté .
- un pc de supervision, comme un pc de paramétrage sont des clients .

Nota : ne pas mettre d'espace si le nom donnée au client comprend plusieurs mots .

8 CHANGEMENT DU MOT DE PASSE

Il est possible de changer le mot de passe d'origine . Saisir d'abord celui d'origine perax et ensuite les nouveaux

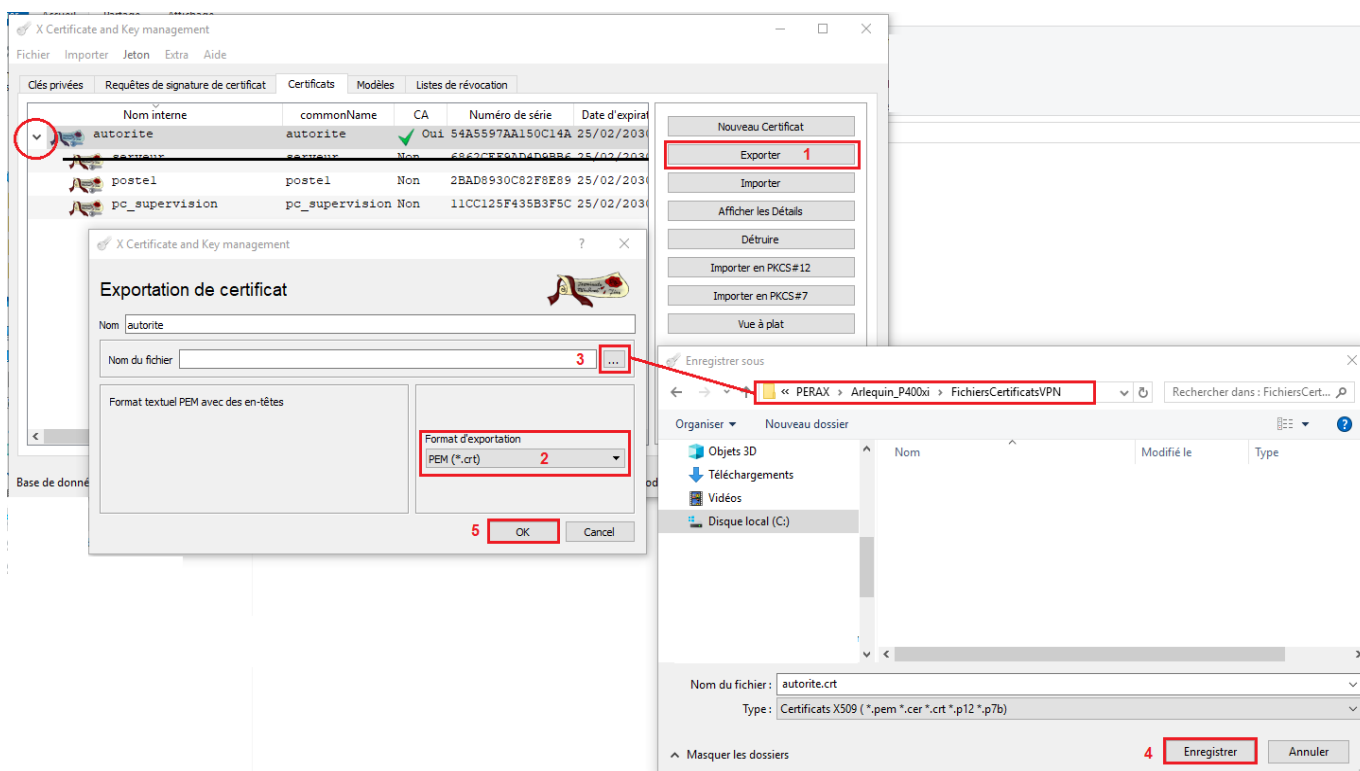


9 EXPORTATION DES CERTIFICATS AUTORITE ET CLIENTS

Cliquer sur l'onglet « Certificats », et effectuer l'exportation des certificats de l'autorité et de tous les clients au format pem (*.crt) .

Nota1 : ne surtout pas exporter le serveur . Dans notre exemple il faudra exporter autorité, poste1 et pc_supervision .

Nota2 : il est préférable d'exporter les fichiers dans le répertoire C:\PERAX\Arlequin_P400xi\FichiersCertificatsVPN . Les fichiers ne pourront être transférés qu'à partir de ce répertoire .

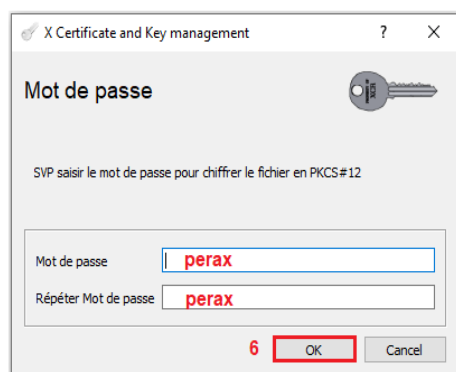
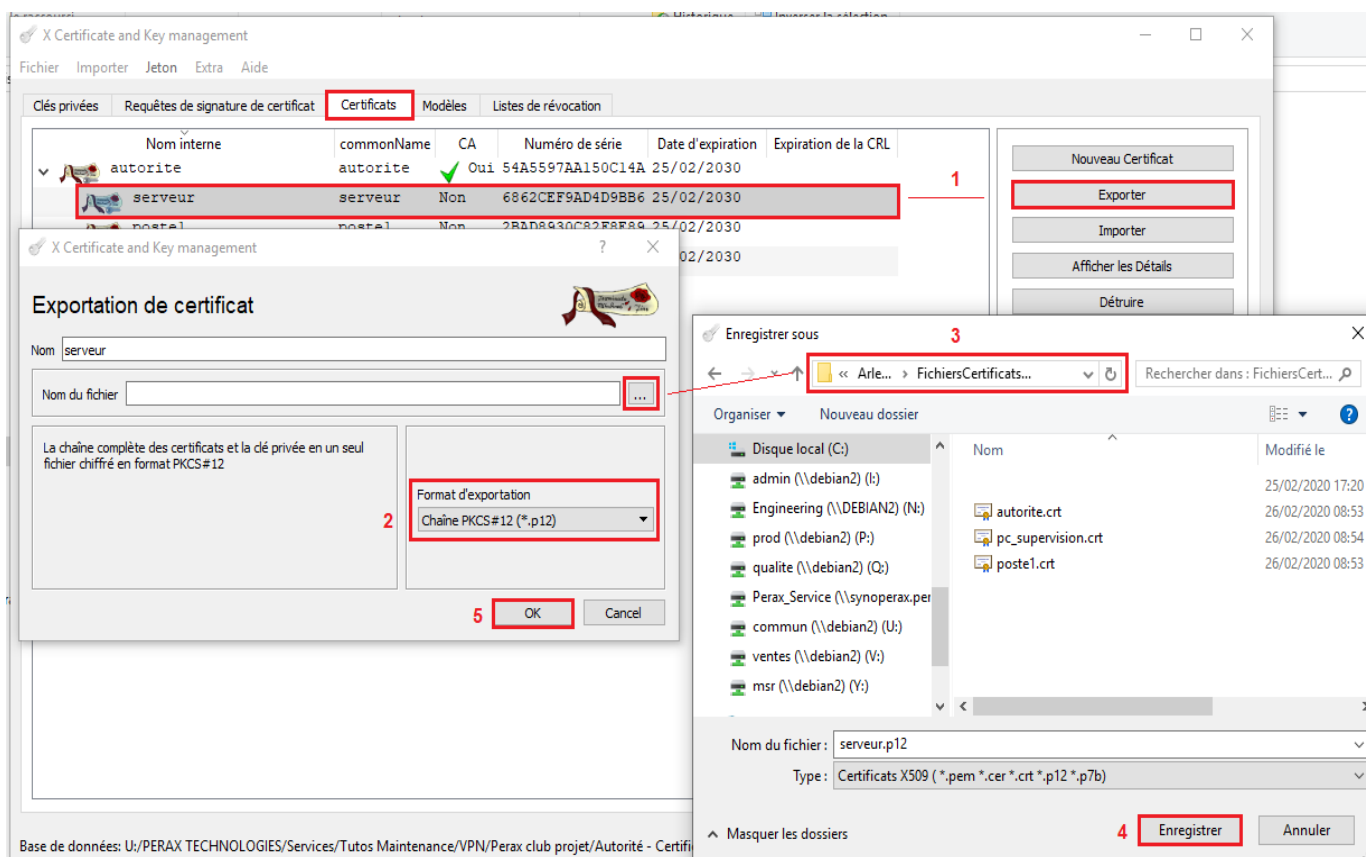


10 EXPORTATION DU CERTIFICAT DU SERVEUR

Cliquer sur l'onglet « Certificats », et effectuer l'exportation du serveur au format **chaîne PKCS#12 (*.p12)**.

Nota1 : ne surtout pas exporter les clients et l'autorité.

Nota2 : il est préférable d'exporter le fichier dans le répertoire C:\PERAX\Arlequin_P400xi\FichiersCertificatsVPN. Le fichier ne pourra être transféré dans le P400xi qu'à partir de ce répertoire.

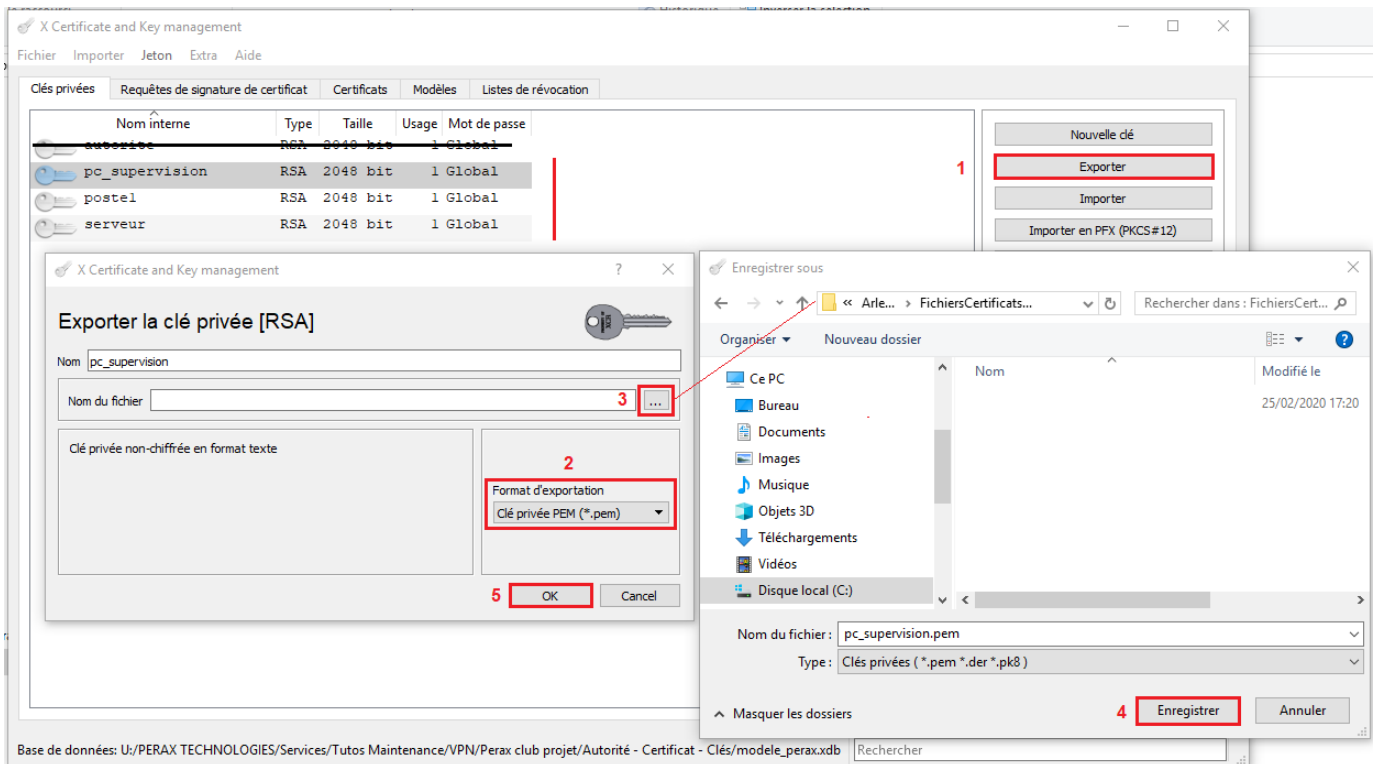


11 EXPORTATION DES CLES

Cliquer sur l'onglet « Clés privées », sélectionner un par un chaque client et serveur et exporter les au **format PEM (*.pem)**

Nota1 : ne surtout pas exporter l'autorité .

Nota2 : il est préférable d'exporter le fichier dans le répertoire C:\PERAX\Arlequin_P400xi\FichiersCertificatsVPN . Les fichiers ne pourront être transférés dans le P400xi qu'à partir de ce répertoire .



12 SAUVEGARDE

Pour une utilisation ultérieure, définir la base de données comme base de données par défaut . Le fichier .xdb prendra les nouveaux paramètres .

