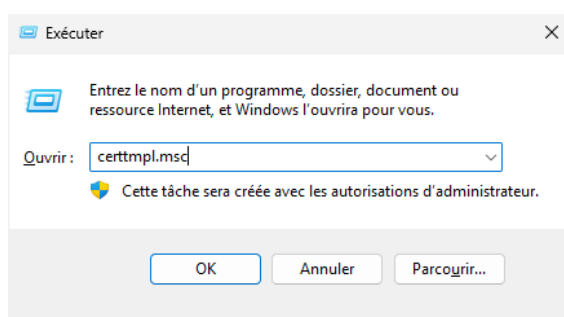


FICHE 3 – CONFIGURATION DE L'INSCRIPTION AUTOMATIQUE POUR L'AUTHENTIFICATION SMARTCARD / PIV

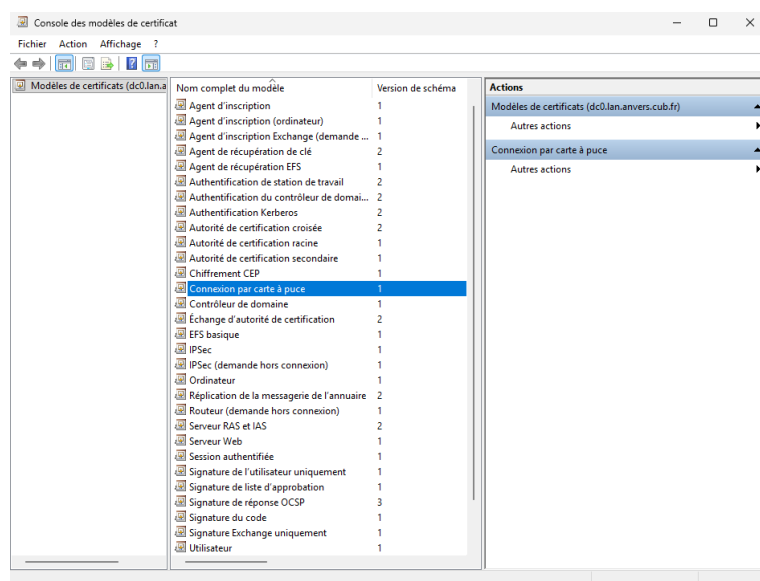
CRÉATION D'UN MODÈLE DE CERTIFICAT SMARTCARD POUR L'AUTORITÉ DE CERTIFICATION INTERNE

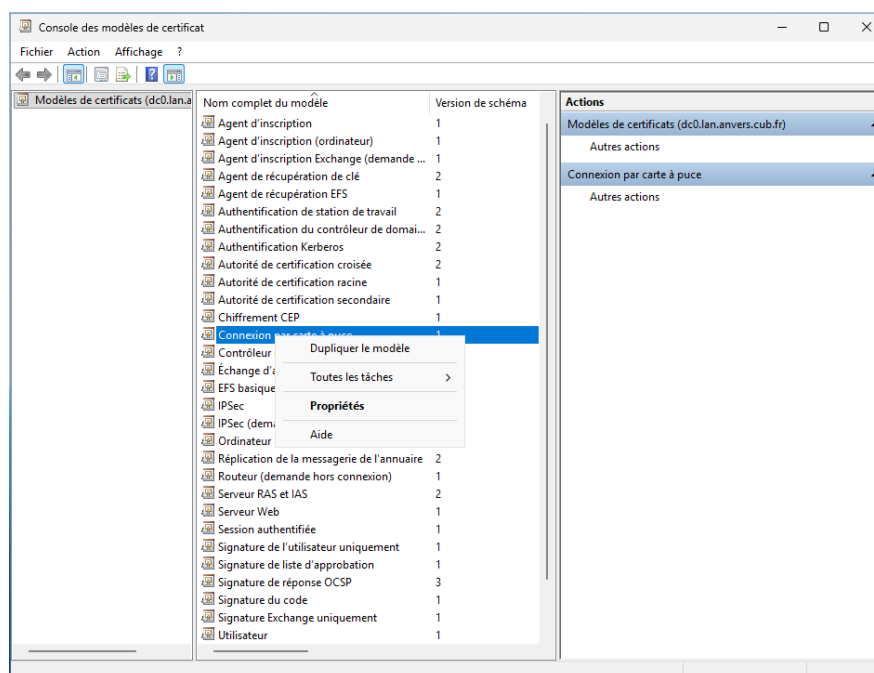
Il est essentiel de créer un modèle de certificat pour l'authentification SmartCard / PIV sur le serveur contrôleur de domaine et PKI avant de distribuer les clés de sécurité matérielles aux utilisateurs concernés pour qu'ils puissent eux-mêmes générer leur certificat, leur clé privée à intégrer sur leur Yubikey.

Sur le serveur Windows, taper sur les touches "Windows + r" ou faire un clic droit sur l'icône Windows Démarrer puis sélectionner "Exécuter". Enfin, saisir certtmpl.msc et appuyer sur la touche Entrée.



Cliquer sur Modèles de certificats puis sur Connexion par carte à puce, faire un clic droit et sélectionner Dupliquer le modèle.

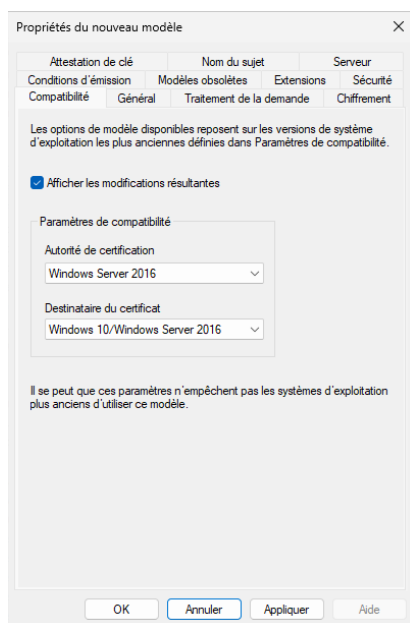




Sélectionner l'onglet Général et réaliser les modifications suivantes :

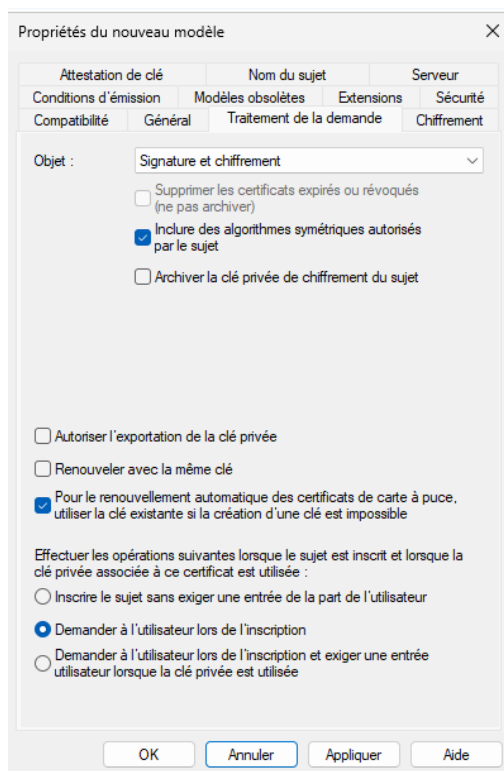
- Définir un nom pour la template (ex : Yuikey).
- Pour la période de validité, s'assurer de choisir un délai cohérent avec la valeur d'expiration fixée lors de la création de la PKI.

Dans l'onglet Compatibilité, sélectionner comme autorité de certification et destinataire du certificat les versions de Windows les plus récentes proposées.



Dans l'onglet Traitement de la demande :

- Vérifier que l'objet sélectionné est Signature et chiffrement, puis cocher la case Inclure des algorithmes symétriques autorisés par le sujet.
- **S'assurer que la case Renouveler avec la même clé est bien décochée.**
- Cocher la case Pour le renouvellement automatique des certificats de carte à puce, utiliser la clé existante si la création de clé est impossible.
- S'assurer que l'option Demander à l'utilisateur lors de l'inscription est validée.





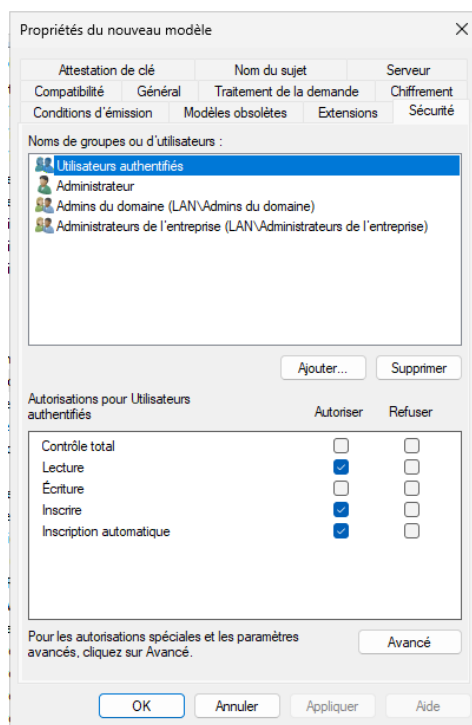
Attention ! Si la case Renouveler avec la même clé est cochée, le renouvellement automatique des certificats échouera.

Dans l'onglet Chiffrement :

- Choisir Fournisseur de stockage de clés comme Catégorie de fournisseur.
- Choisir le nom de l'algorithme de chiffrement le plus pertinent.
- L'option Les demandes doivent utiliser l'un des fournisseurs suivants doit être activée.
- Dans le menu Fournisseurs situé en dessous, cocher la case Microsoft Smart Card Key Storage Provider.
- Concernant le hachage de la demande, sélectionner la fonction SHA-256.

The screenshot shows the 'Propriétés du nouveau modèle' dialog box with the 'Chiffrement' tab selected. The 'Catégorie de fournisseur' is set to 'Fournisseur de stockage de clés', the 'Nom de l'algorithme' is 'ECDH_P256', and the 'Taille de clé minimale' is '256'. Under 'Choisissez les fournisseurs de chiffement pouvant être utilisés pour les demandes', the option 'Les demandes doivent utiliser l'un des fournisseurs suivants' is selected. In the 'Fournisseurs' list, 'Microsoft Smart Card Key Storage Provider' is checked. The 'Hachage de la demande' is set to 'SHA256'. The 'Utiliser un autre format de signature' checkbox is unchecked. The dialog has buttons for 'OK', 'Annuler', 'Appliquer', and 'Aide'.

Dans l'onglet Sécurité, veiller à ce que les utilisateurs du domaine disposent des droits "Lecture, Inscrire, et inscription automatique".

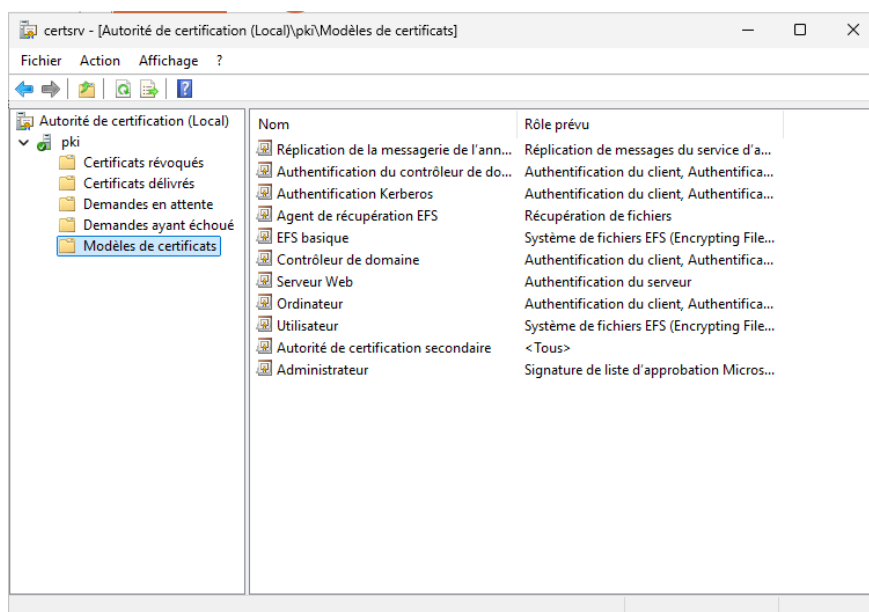


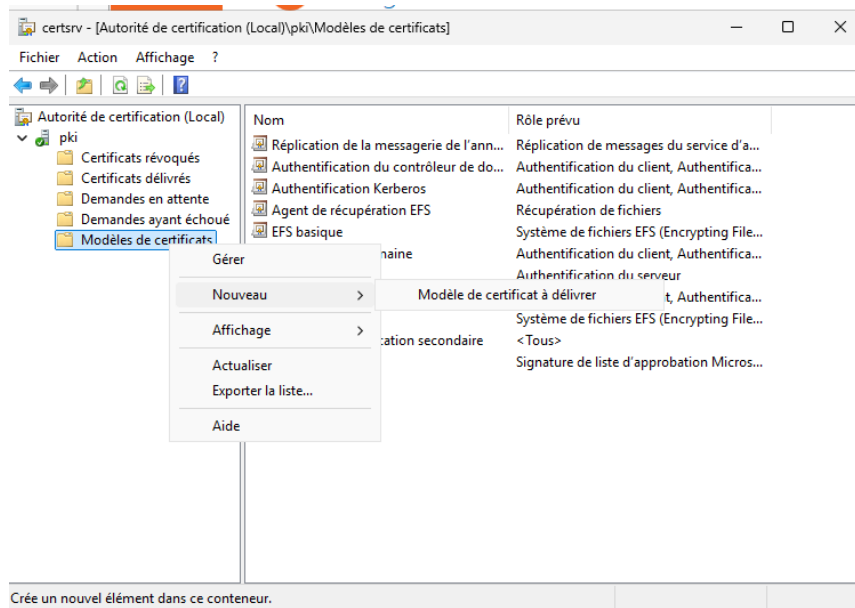
Cliquer sur Appliquer, OK puis fermer la fenêtre.

AJOUT DU MODÈLE CRÉÉ DANS LA CONFIGURATION DE L'AUTORITÉ DE CERTIFICATION INTERNE

Sur le serveur Windows, taper sur les touches "Windows + r" ou faire un clic droit sur l'icône Windows Démarrer puis sélectionner "Exécuter". Enfin, saisir `certsrv.msc` et appuyer sur la touche Entrée.

Cliquer sur Autorité de certification puis sur le nom de votre PKI et sur Modèles de certificats. Faire un clic droit sur Modèles de certificats puis Nouveau > Modèle de certificat à délivrer.





Sélectionner le modèle précédemment créé (YubikeyAuto dans l'exemple) et vérifier que ce dernier a été ajouté dans les modèles de certificats présents dans l'autorité de certification.

