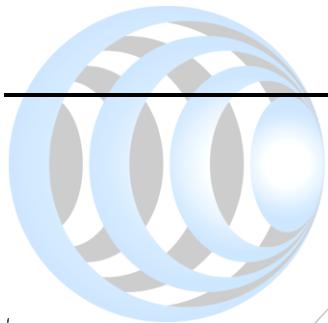


Procédure de configuration carte à puce pour ouverture de session Windows



INFINIGATE
.... Adding Value to Distribution

Infinigate France

Evolutions du document

Version	Date	Auteur	Nature des modifications
1.0	01/01/2022	Dorian DELORME	Version Initiale

Table des matières

INSTALLATION DU MINIDRIVER (DEJA EFFECTUE)	3
CREATION D'UN TEMPLATE SMARTCARD POUR L'AUTO-ENROLLMENT (ADCS).....	3
AJOUT DU MODELE DE CERTIFICAT A L'AUTORITE DE CERTIFICATION (ADCS).....	4
EDITION DES GPO POUR PERMETTRE L'AUTO ENRÔLEMENT (DC).....	4
AUTO-ENROLLEMENT DE L'UTILISATEUR (Windows 10)	4
REGLAGE DU CODE PIN (Windows 10, minidriver requis)	5
LOGIN WINDOWS ET RDP AVEC LA YUBIKEY (WINDOWS 10).....	5
GESTION DES CERTIFICATS PIV AVEC YKMAN	5
GESTION DES CERTIFICATS SUR ADCS	5
OPTIONNEL : EDITION DES GPO POUR FORCER LA SMARTCARD.....	6
OPTIONNEL : EDITION DES GPO POUR DEFINIR LE COMPORTEMENT QUAND ON RETIRE LA YUBIKEY DU PORT USB.....	7

INSTALLATION DU MINIDRIVER (DEJA EFFECTUE)

1. Téléchargement du Yubikey Minidriver, disponible ici :
<https://www.yubico.com/support/download/smart-card-drivers-tools/>.

The command line install is:

```
msiexec /i YubiKey-Minidriver-4.1.0.172-x64.msi INSTALL_LEGACY_NODE=1
```

For unattended mode - progress bar only:

```
msiexec /i YubiKey-Minidriver-4.1.0.172-x64.msi INSTALL_LEGACY_NODE=1 /passive
```

For quiet mode, no user interaction:

```
msiexec /i YubiKey-Minidriver-4.1.0.172-x64.msi INSTALL_LEGACY_NODE=1 /quiet
```

CREATION D'UN TEMPLATE SMARTCARD POUR L'AUTO-ENROLLMENT (ADCS)

Note : L'ADCS est déjà installé, mais aucune configuration n'a été apporté.

1. Win+R et tapez "certtmpl.msc"
2. Cliquez sur "Modèle de certificat", repérez et clic droit sur **Connexion par carte à puce** puis "Dupliquer le modèle".
3. Clic sur la section Général et effectuer les changements suivants :
 - a. Dans **Onglet General / Nom du modèle**, entrez un nom court sans espace comme "Yubikey" ou "YubicoSC".
 - b. Assurez-vous que l'option « **Publier le certificat dans Active Directory** » est sélectionnée.
4. Cliquez sur l'onglet **Compatibilité**, et effectuez les changements suivants:
 - a. Côté **Autorité de certification** l'OS sur lequel l'AC est hébergé. (Ici AC = Win 2016 et Destinataire = Win10/2016)
 - b. Côté **Destinataire du certificat** sélectionnez la plus ancienne version de Windows qui utilisera smartcard. (Windows 10 / Windows 2016)
5. Cliquez sur l'onglet "Traitement de la demande", et effectuez les changements suivants :
 - a. Pour **Objet**, sélectionnez **Signature et chiffrement**.
 - b. Assurez-vous que l'option "**Inclure des algorithmes symétriques autorisés par le sujet**" est sélectionnée.
 - c. Assurez-vous que l'option « **Renouveler avec le même clé** » est décochée.
 - d. Cochez l'option « **Pour le renouvellement automatique des certificats de carte à puce, utiliser la clé existante si la création d'une clé est impossible** »
 - e. Cocher l'option pour **Demandeur à l'utilisateur lors de l'inscription**.
6. Dans l'onglet "**Chiffrement**", effectuez les changements suivants:
 - a. Catégorie de Fournisseur: Sélectionnez **Fournisseur de stockage de clé** dans la liste.
 - b. Algorithme : Sélectionnez **RSA**
 - c. Taille minimum: Pour RSA, renseignez minimum **2048**.
 - d. Cochez l'option « **Les demandes doivent utiliser l'un des fournisseurs suivants** ».
 - e. Sous **Fournisseur**, sélectionnez **Microsoft Smart Card Key Storage Provider**.
 - f. Dans **Hachage de la demande** : Sélectionnez dans la liste **SHA256**.
7. Dans l'onglet Sécurité, effectuez les changements suivants :
 - a. Groupe et utilisateurs: Ajouter le groupe (PIV_USERS) dont fait partie alex_piv pour qu'il ait accès au modèle de certificat.

b. Permissions de PIV_USERS :

L'utilisateur sera auto-enrôlé en utilisant les fonctionnalités Windows native, assurez-vous que les options **Lecture, Incrire et Inscription automatique** sont autorisés.

8. Cliquez sur "Appliquer" et OK.

AJOUT DU MODELE DE CERTIFICAT A L'AUTORITE DE CERTIFICATION (ADCS)

1. Right-click the Windows Start button and select **Run**.
2. Win+R et **certsrv.msc** puis pressez entré.
3. Cliquez sur "Autorité de certification ", double-cliquer sur **l'ADCS/Modèle de certificat**, clic-droit au centre et sélectionner « **Nouveau** » et « **Modèle de certificat à délivrer** »
4. Localiser et sélectionner le modèle créé et OK.
5. Update de la CRL : Sur **Certificats révoqués** : Clic droit/**Toutes les tâches/Publier/Nouvelle liste de révocation des certificats**

EDITION DES GPO POUR PERMETTRE L'AUTO ENRÔLEMENT (DC)

1. Win+R et **gpmc.msc** puis entrée.
2. Naviguer dans "Clients/Utilisateurs PIV" dans la forêt infinilab.local.
3. Créer une GPO sur « Utilisateurs PIV » et éditez là (Nom : PIV_autoenroll)
4. Etendre **User Configuration > Policies > Windows Settings > Security Settings > Public Key Policies (Stratégie de clé publique)**
5. Clic droit sur **Client des services de certificats – Stratégie d'inscription des certificats** et sélectionner **Propriété**.
5. Dérouler la liste et sélectionner "Activer".
7. Cliquer **OK**.
8. Clic-droit sur **Client des services de certificat – Inscription automatique** et sélectionner **Propriété**.
9. Dérouler la liste et sélectionner "Activer".
10. Cocher « **Renouveler les certificats expirés, mettre à jour les certificats en attente et supprimer les certificats révoqués** »
11. Cocher « **Mettre à jour les certificats qui utilisent les modèles de certificats** »
12. Cliquer **OK**.
13. Dans la sécurité de la GPO (Onglet Délégation), ajoutez le groupe « **PIV_USERS** » en « **Modifier les paramètres, supprimer, modifier la sécurité** »
14. Clic droit « **Appliqué** » sur la GPO.

23. Ouvrez une MMC/Ajouter un composant enfichable/Certificats/Compte Ordinateur Local/
24. Publier manuellement le certificat dans Active Directory : Déployer le dossier « **Personnel/Certificats** », clic-droit « **Toutes les tâches/Demander un nouveau certificat/Stratégie d'inscription à l'Active Directory/Authentification du contrôleur de domaine** »

AUTO-ENROLLEMENT DE L'UTILISATEUR (Windows 10)

⚠ La partie PIV sur la Yubikey doit être vierge pour que l'auto-enrôlement aboutisse.(Reset PIV)

1. Redémarrez la machine Windows 10 et se reconnecter avec le compte **alex_piv**
Une notification apparaît dans la barre des tâches.
2. Branchez la Yubikey puis dans les paramètres VMWARE : Removable Devices/ Yubico.com
OTP+FIDO+CCID/ Connect
 - ⚠ Si aucun popup n'apparaît, redémarrez une seconde fois la VM.
3. Cliquer sur l'icône de la barre des tâches pour ouvrir le guide d'enrôlement utilisateur. Si le popup a disparu ou n'apparaît pas, cliquez sur la petite flèche pour étendre les icônes pour la barre des tâches.
4. Dans l'écran initial, cliquez **Suivant**.
5. Sélectionnez le certificat approprié et cliquez sur Inscription.
STATUT: Inscription requise devrait apparaître à côté du modèle de certificat.
6. Entrez le code PIN de la Yubikey. Si vous ne l'avez pas changé, entrez sa valeur par défaut : **123456**
7. Windows enrôle la Yubikey pour le login. Le process prend quelque secondes. Cliquez sur « Finir ».

REGLAGE DU CODE PIN (Windows 10, minidriver requis)

Une fois que la Yubikey est enregistrée, le code PIN utilisateur devrait être changé.

Une fois que l'utilisateur s'est logué, il peut changer le code PIN de la manière suivante :

1. Pressez **Ctrl+Alt+Del** pour ouvrir le gestionnaire.
2. Sélectionnez **Changer le mot de passe**.
3. Entrez le code PIN actuel puis le nouveau code PIN que vous souhaitez. The user is prompted to enter the current PIN, as well as the new PIN.
4. Pressez entrée pour valider le nouveau code PIN.

LOGIN WINDOWS ET RDP AVEC LA YUBIKEY (WINDOWS 10)

1. Se déconnecter de windows, et se reconnecter avec la Yubikey en mode PIV :
 - a. « Option de connexion » / « Carte à puce »
 - b. Entrer son code PIN, on se connecte ainsi en mode PIV sur le compte **alex_piv**
2. Une fois connecté sur Windows, ouvrez un invite de bureau à distance.
 - a. Entrer 192.168.1.4 (SRV-WEB)
 - b. « Autre choix » / « Identification par carte à puce »
 - c. Entrer son code PIN, on se connecte ainsi en tant qu'**alex_piv** sur **srv-web**

GESTION DES CERTIFICATS PIV AVEC YKMAN

#Lister les certificats sur la yubikey

```
Ykman piv info
```

#Changer le code PUK

```
Ykman piv change-puk
```

#Débloquer le code PIN avec le code PUK

```
ykman piv unblock-pin
```

#Reset la partie PIV (si les code PIN et PUK sont bloqués ou réattribution)

```
ykman piv reset
```

GESTION DES CERTIFICATS SUR ADCS

Pour révoquer un certificat (perte d'une clé, départ d'un salarié...) :

Certsrv.msc :

Révocation du certificat utilisateur

The screenshot shows the Windows Certificates snap-in (Certsrv.msc). In the left navigation pane, 'ADCS-CA' is selected under 'Autorité de certification (Local)'. In the main pane, a list of certificates is displayed, with the fourth item (ID 9) highlighted. A context menu is open over this certificate, with the 'Toutes les tâches' option expanded. The 'Révoquer un certificat' option is highlighted with a red box.

ID de la demande	Nom du demandeur	Certificat binaire	Modèle de certificat	Numéro de série	Date d'effet
2	INFINILAB\DC\$	-----BEGIN CERTI...	Contrôleur de doma...	16000000026d402...	22/07/2021
3	INFINILAB\DC\$	-----BEGIN CERTI...	Authentification du ...	16000000031b15e...	10/03/2021
7	INFINILAB\alex_piv	-----BEGIN CERTI...	YUBICOSC (1.3.6.1.4...	16000000073260a...	12/03/2021
9	INFINILAB\john	-----BEGIN CERTI...	YUBICOSC (1.3.6.1.4...	1600000009ba4fb...	12/03/2021

Publication des crl :

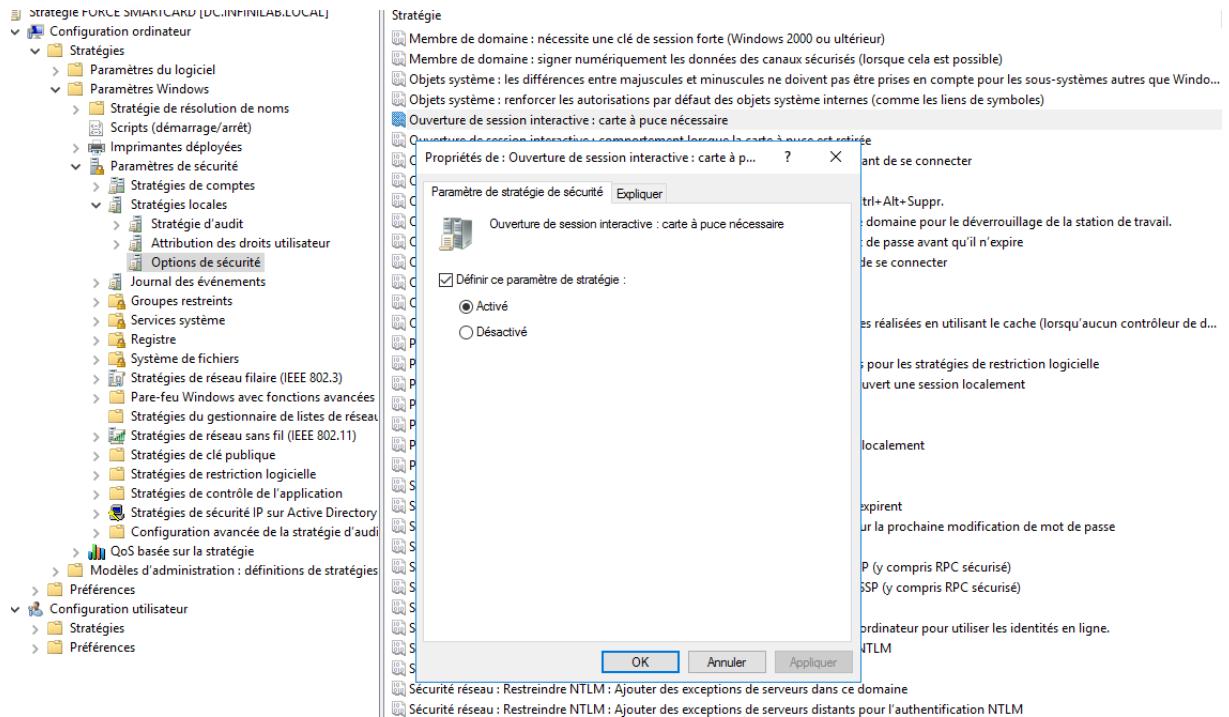
The screenshot shows the Windows Certificates snap-in (Certsrv.msc). In the left navigation pane, 'ADCS-CA' is selected under 'Autorité de certification (Local)'. In the main pane, a list of certificates is displayed, with the first item (ID 2) highlighted. A context menu is open over this certificate, with the 'Toutes les tâches' option expanded. The 'Publier' option is highlighted with a red box.

ID de la demande	Nom du demandeur	Certificat binaire	Modèle de certificat
2	INFINILAB\DC\$	-----BEGIN CERTI...	Contrôleur de doma...
	INFINILAB\alex_piv	-----BEGIN CERTI...	Authentif...
	INFINILAB\john	-----BEGIN CERTI...	YUBICOSC...

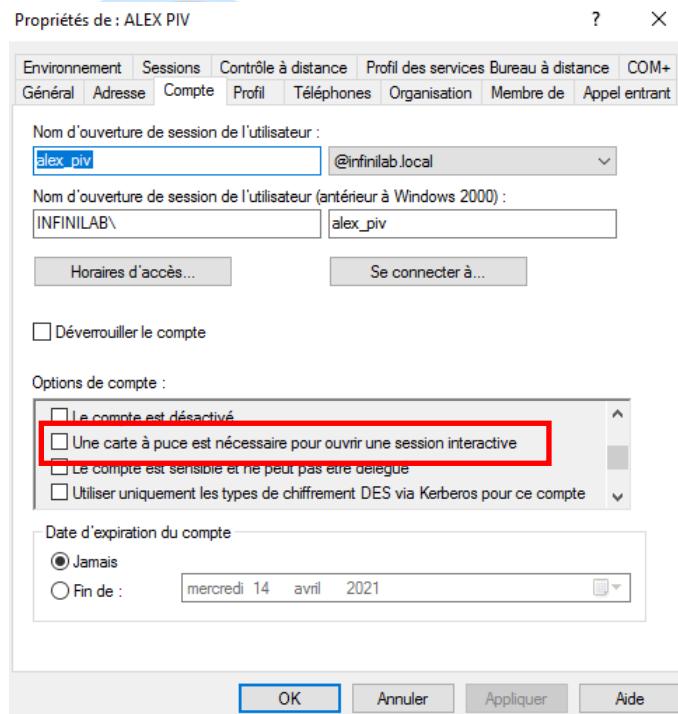
Note : Il est possible qu'à cause du cache windows, une session puisse toujours se connecter avec le certificat révoqué un certain temps sur une machine qui avait l'habitude de recevoir ce certificat.

OPTIONNEL : EDITION DES GPO POUR FORCER LA SMARTCARD

Configuration Ordinateur / Stratégies / Paramètres Windows / Paramètres de sécurité / Stratégies locales / Option de sécurité / Ouverture de session interactive : Carte à puce nécessaire :



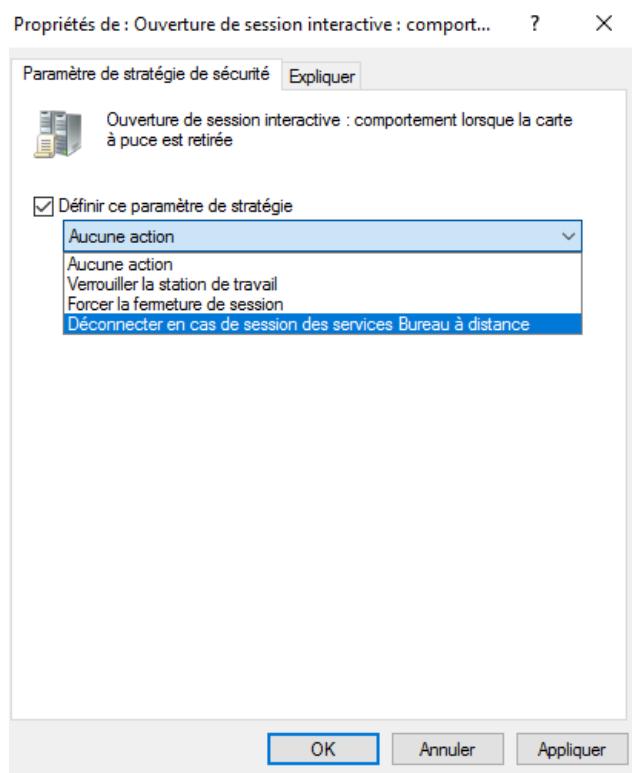
On peut aussi forcer individuellement la smartcard sur chacun des comptes :



NIGATE
Value to Distribution

OPTIONNEL : EDITION DES GPO POUR DEFINIR LE COMPORTEMENT QUAND ON RETIRE LA YUBIKEY DU PORT USB

Configuration Ordinateur / Stratégies / Paramètres Windows / Paramètres de Sécurité / Stratégies locales / Options de sécurité / Ouverture de session interactive : Comportement lorsque la carte à puce est retirée



Plusieurs comportements possibles :

- Déconnexion de l'utilisateur
- Verrouillage de la session
- Déconnexion des sessions RDP

Note : Depuis windows Vista, il faut activer le service scpollicysvc pour que ce comportement fonctionne : `sc config scpollicysvc start=auto`

Powershell : `Start-Service -Name "scpollicysvc"`