

UTILISATION DU CHIFFREMENT BITLOCKER SOUS WINDOWS 10

Utilisation de bitlocker sous windows et apprentissage du concept de
chiffrement

Sofiane acheraïou

Table des matières

III. Chiffrer un disque	2
IV. BitLocker en ligne de commande	5
V. EFS	6
UTILISATION DE LA COMMANDE CIPHER.....	8
SAUVEGARDE CLE DE CHIFFREMENT ET CERTIFCAT.	12
Accès depuis un autre compte aux données chiffrées.....	14
DIFFERENCES AVEC BITLOCKER	22
Identifier les risques associés à l'utilisation d'EFS.....	22
VI. Autres outils.....	23

III. Chiffrer un disque

Question - Lire et résumer la ressource suivante :

[article malekal](#)

AES est un système de chiffrement symétrique et par bloc (utilisant la même clé de chiffrement pour le chiffrement et le déchiffrement. Chaque donnée est découpée en blocs dont la taille est fixe (128 pour AES-128, 512 pour AES-512 etc...) avec une taille de clé qui définira le nombre de fois que le chiffrement s'effectuera (tours) plus la taille de la clé est grande plus le nombre de combinaisons sera élevée et prendra du temps à attaquer.

Taille de la clé AES	Nombre combinaisons possibles
1 bit	2
2 bits	4
4 bits	16
8 bits	256
16 bits	65536
32 bits	4.2×10^9
56 bits (DES)	7.2×10^{16}
64 bits	1.8×10^{19}
128 bits (AES)	3.4×10^{38}
192 bits (AES)	6.2×10^{57}
256 bits (AES)	1.1×10^{77}

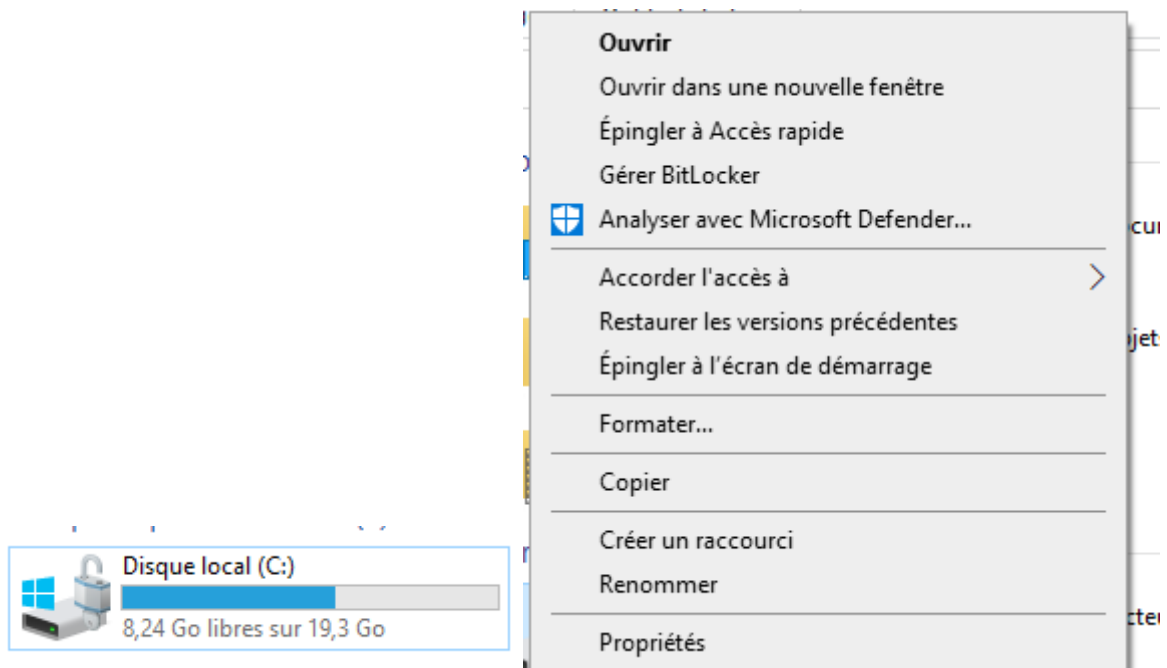
Tailles de clé et combinaisons possibles correspondantes à craquer par attaque par force brute.

Source: https://www.eetimes.com/document.asp?doc_id=1279619#

Question :

- Proposez 3 méthodes pour vérifier que le lecteur est bien chiffré


Première méthode explorateur Windows :



Aller dans l'explorateur faire clique droit sur le disque qu'on a chiffré, si « Gérer Bitlocker » apparait dans le menu contextuel, c'est bon signe, cliquer sur gérer bitlocker, et cette ecran devrait apparaitre. sinon le disque n'est pas chiffré par bitlocker.

Chiffrement de lecteur BitLocker

Protégez vos fichiers et dossiers contre l'accès non autorisé en protégeant vos lecteurs avec BitLocker.

 Par sécurité, certains paramètres sont gérés par l'administrateur système.

Lecteur du système d'exploitation

C: Chiffrement BitLocker en cours



Sauvegarder votre clé de récupération




Désactiver BitLocker

Lecteurs de données fixes

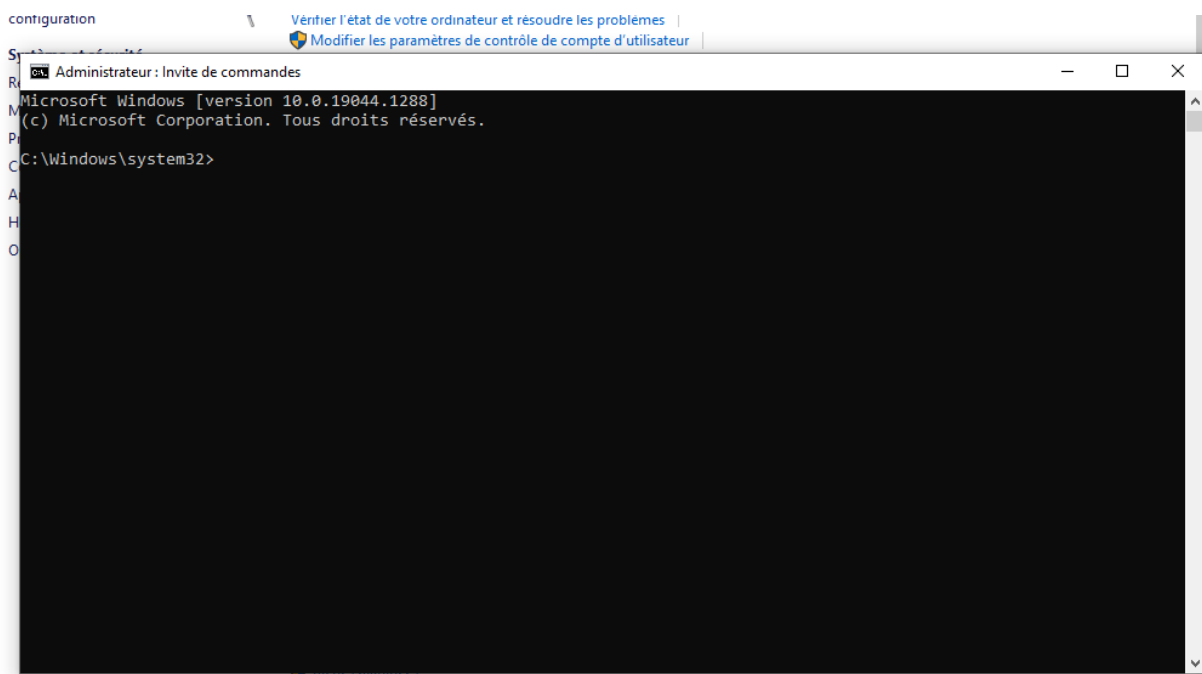
Lecteurs de données amovibles - BitLocker To Go

Insérez un lecteur flash USB amovible pour utiliser BitLocker To Go.

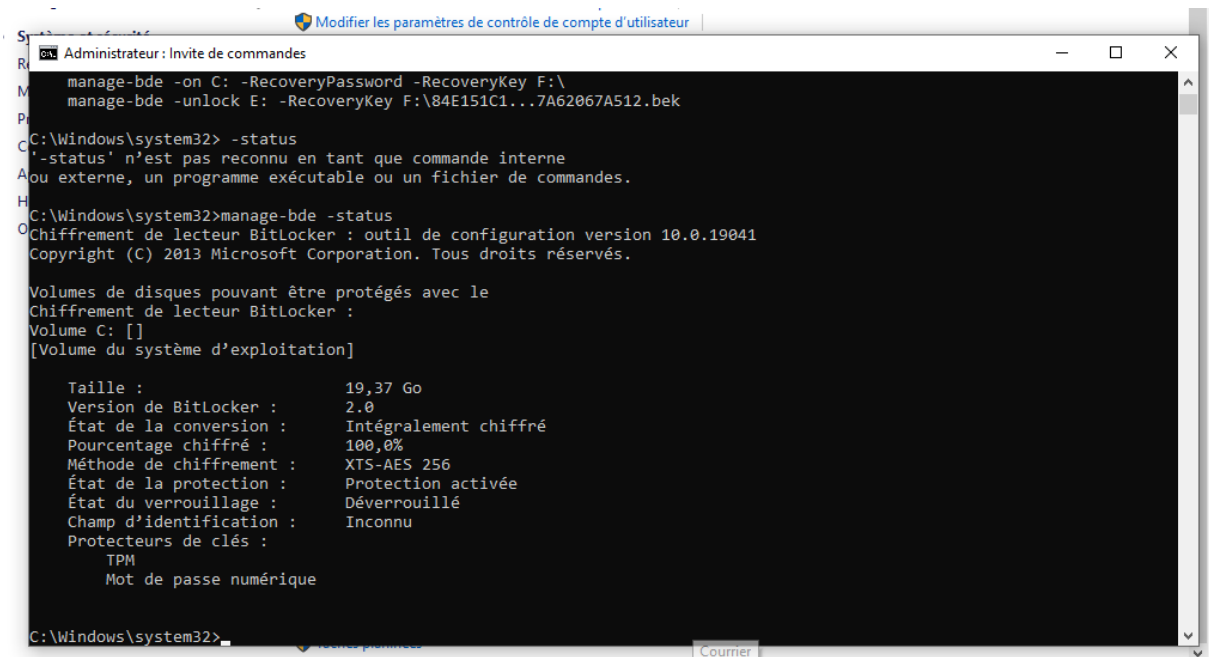
 Ce PC

2eme méthode : ligne de commande

Ouvrir l'invite de commande, ou PowerShell en mode administrateur.



Et taper la commande `manage-bde -status`, cela permet de vérifier les paramètres avancés de bitlocker et son état actuel.



```
Administrateur : Invite de commandes
manage-bde -on C: -RecoveryPassword -RecoveryKey F:\
manage-bde -unlock E: -RecoveryKey F:\84E151C1...7A62067A512.bek

C:\Windows\system32> -status
'-status' n'est pas reconnu en tant que commande interne
ou externe, un programme exécutable ou un fichier de commandes.

C:\Windows\system32>manage-bde -status
Chiffrement de lecteur BitLocker : outil de configuration version 10.0.19041
Copyright (C) 2013 Microsoft Corporation. Tous droits réservés.

Volumes de disques pouvant être protégés avec le
Chiffrement de lecteur BitLocker :
Volume C: []
[Volume du système d'exploitation]

Taille : 19,37 Go
Version de BitLocker : 2.0
État de la conversion : Intégralement chiffré
Pourcentage chiffré : 100,0%
Méthode de chiffrement : XTS-AES 256
État de la protection : Protection activée
État du verrouillage : Déverrouillé
Champ d'identification : Inconnu
Protecteurs de clés :
TPM
Mot de passe numérique

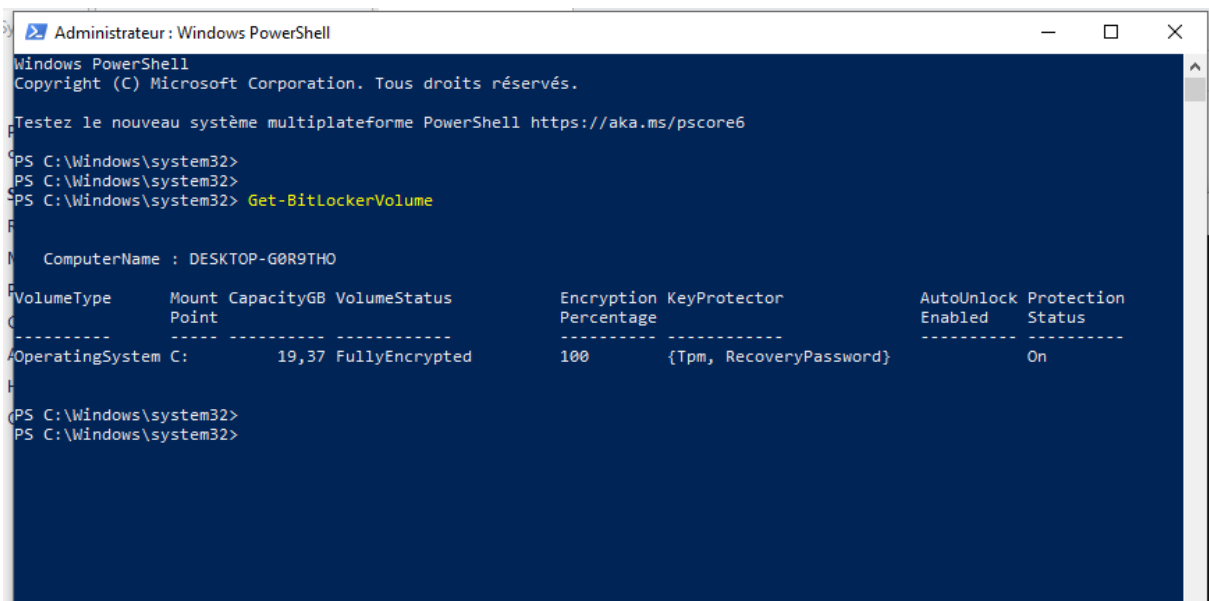
C:\Windows\system32>
```

Si Etat de protection affiche « protection activée » alors le chiffrement est en place.

3 eme methode, powershell exclusivement

Ouvrir powershell en mode administrateur et taper la commande Get-Bitlockervolume.

ProtectionStatus devrait afficher « on » si le lecteur est chiffré.



```
Administrateur : Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. Tous droits réservés.

Testez le nouveau système multiplateforme PowerShell https://aka.ms/pscore6

PS C:\Windows\system32>
PS C:\Windows\system32>
PS C:\Windows\system32> Get-BitLockerVolume

ComputerName : DESKTOP-G0R9TH0

VolumeType Mount CapacityGB VolumeStatus Encryption KeyProtector AutoUnlock Protection
----- Point -----
OperatingSystem C: 19,37 FullyEncrypted 100 {Tpm, RecoveryPassword} Enabled On

PS C:\Windows\system32>
PS C:\Windows\system32>
```

IV. BitLocker en ligne de commande

Afficher l'état bitlocker -> manage-bde -status

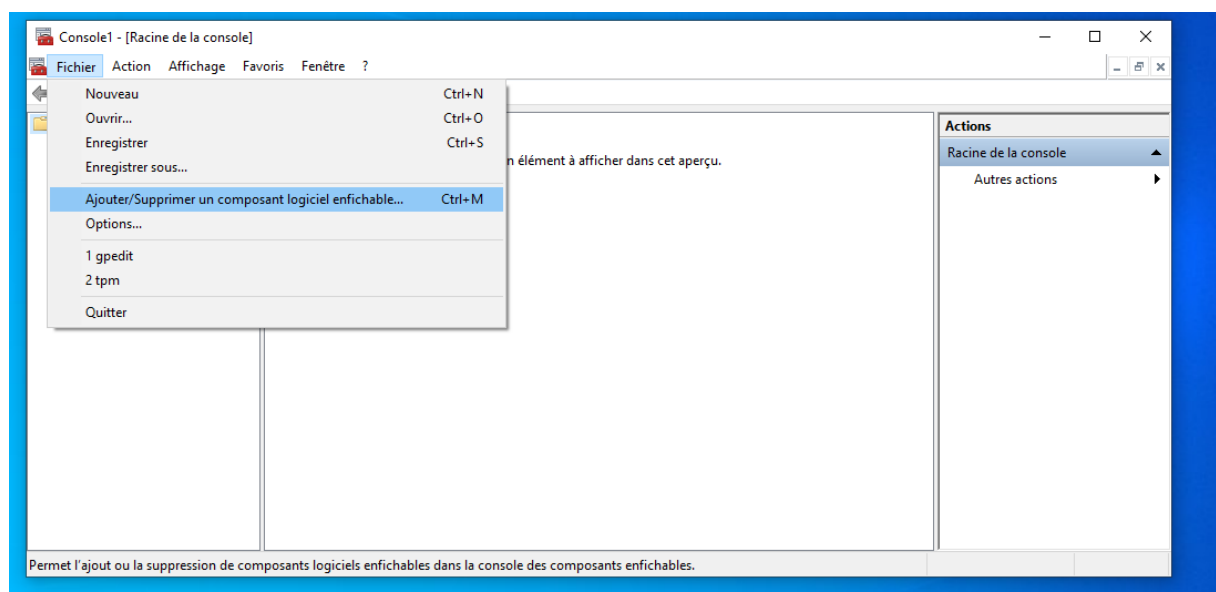
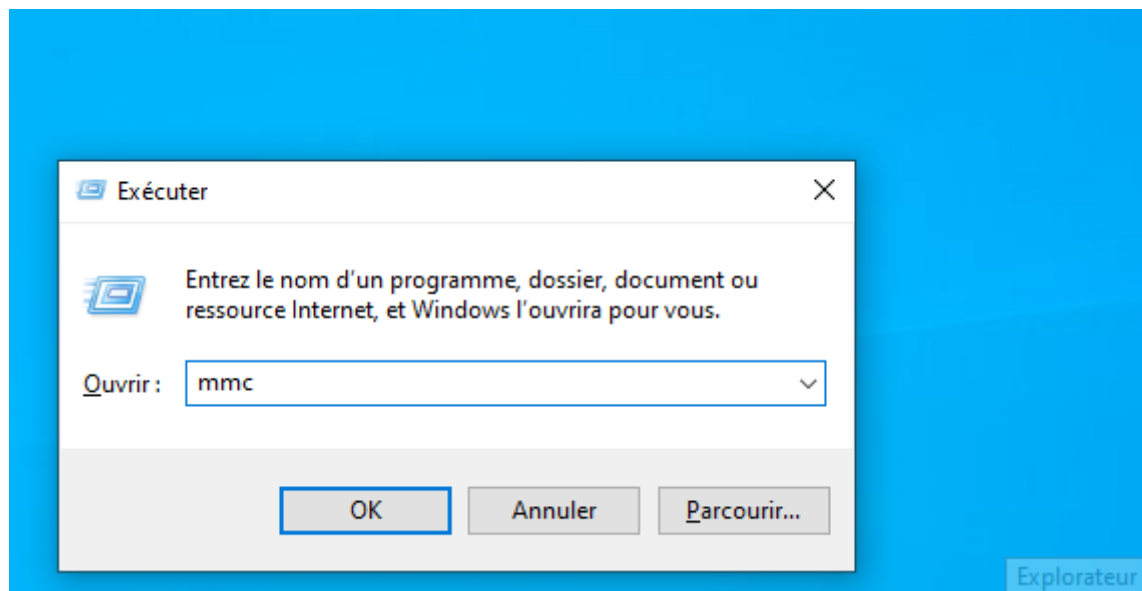
Modifier le code pin du volume manage-bde -changePIN [nom du volume](C: par exemple)

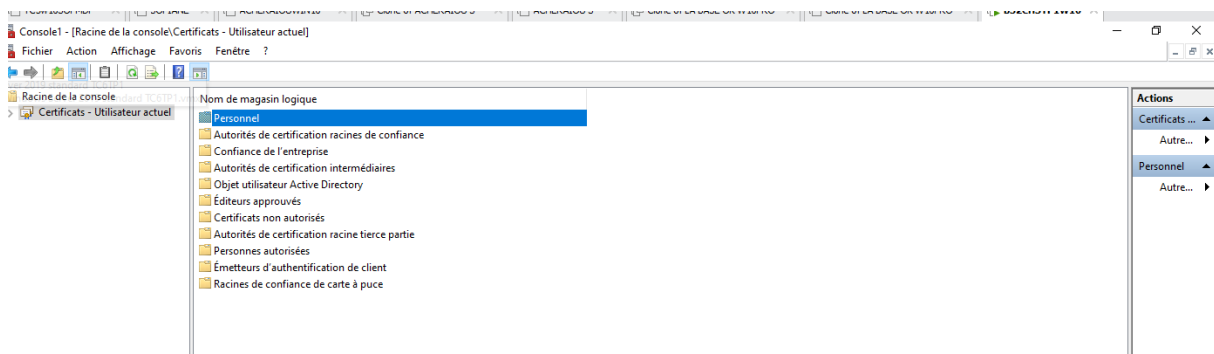
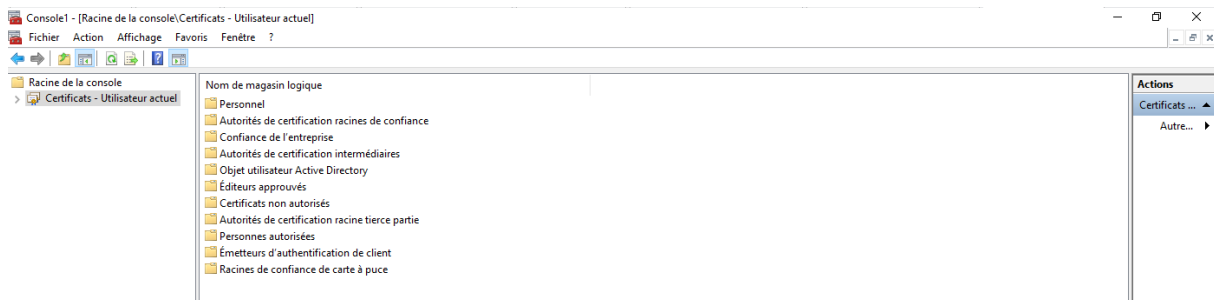
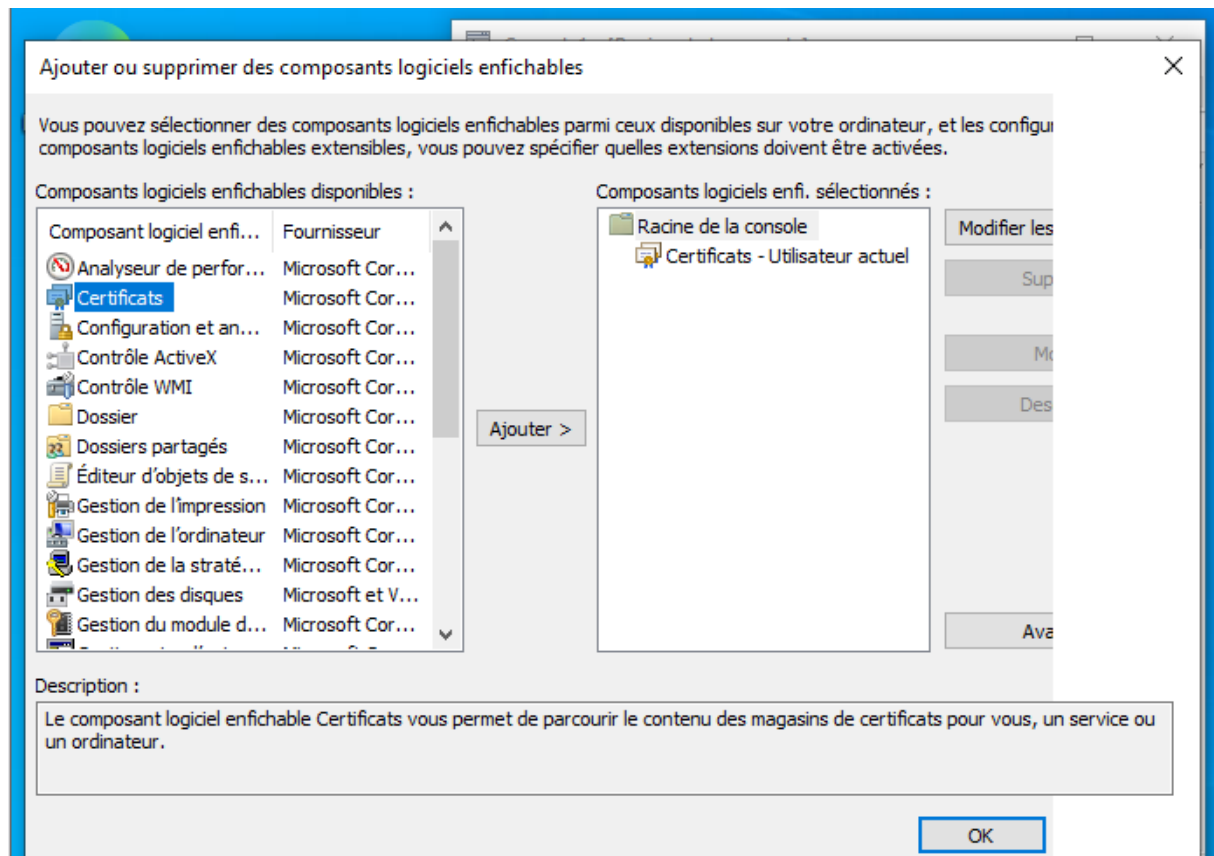
De déchiffrer et désactiver Bitlocker manage-bde -off [nom du volume]

De chiffrer et d'activer Bitlocker manage-bde -on [nom du volume](

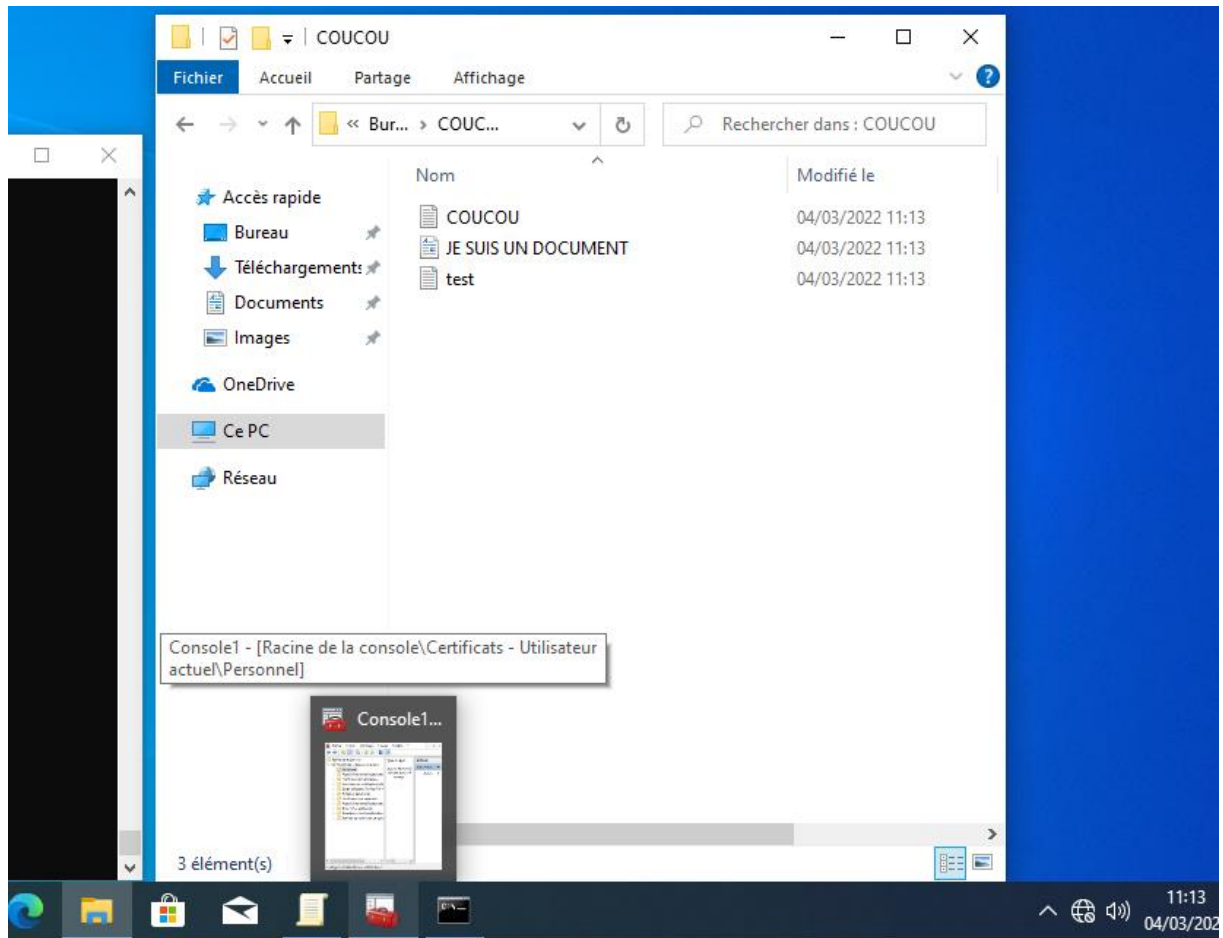
V. EFS

EFS est une méthode de chiffrement de disque sous Windows qui chiffre les fichiers avec une clé symétrique ou File Encryption Key (FEK), sur un disque NTFS, une clé symétrique (qui permet de chiffrer et déchiffrer avec la même clé, comme AES), permet un temps plus rapide de chiffrement et de déchiffrement. Cette clé est ensuite chiffrée avec une clé publique liée à l'utilisateur.





UTILISATION DE LA COMMANDE CIPHER



Exemple : dossier COUCOU créé et fichiers créés.

Cipher pour afficher sur un fichier/dossier est chiffré ou pas (U ou E)

```
Administrator : Invite de commandes
15 Rép(s) 8 793 341 952 octets libres

C:\Users\adminisio>cd Desktop

C:\Users\adminisio\Desktop>mkdir
La syntaxe de la commande n'est pas correcte.

C:\Users\adminisio\Desktop>mkdir COUCOU

C:\Users\adminisio\Desktop>cd COUCOU

C:\Users\adminisio\Desktop\COUCOU>touch
'touch' n'est pas reconnu en tant que commande interne
ou externe, un programme exécutable ou un fichier de commandes.

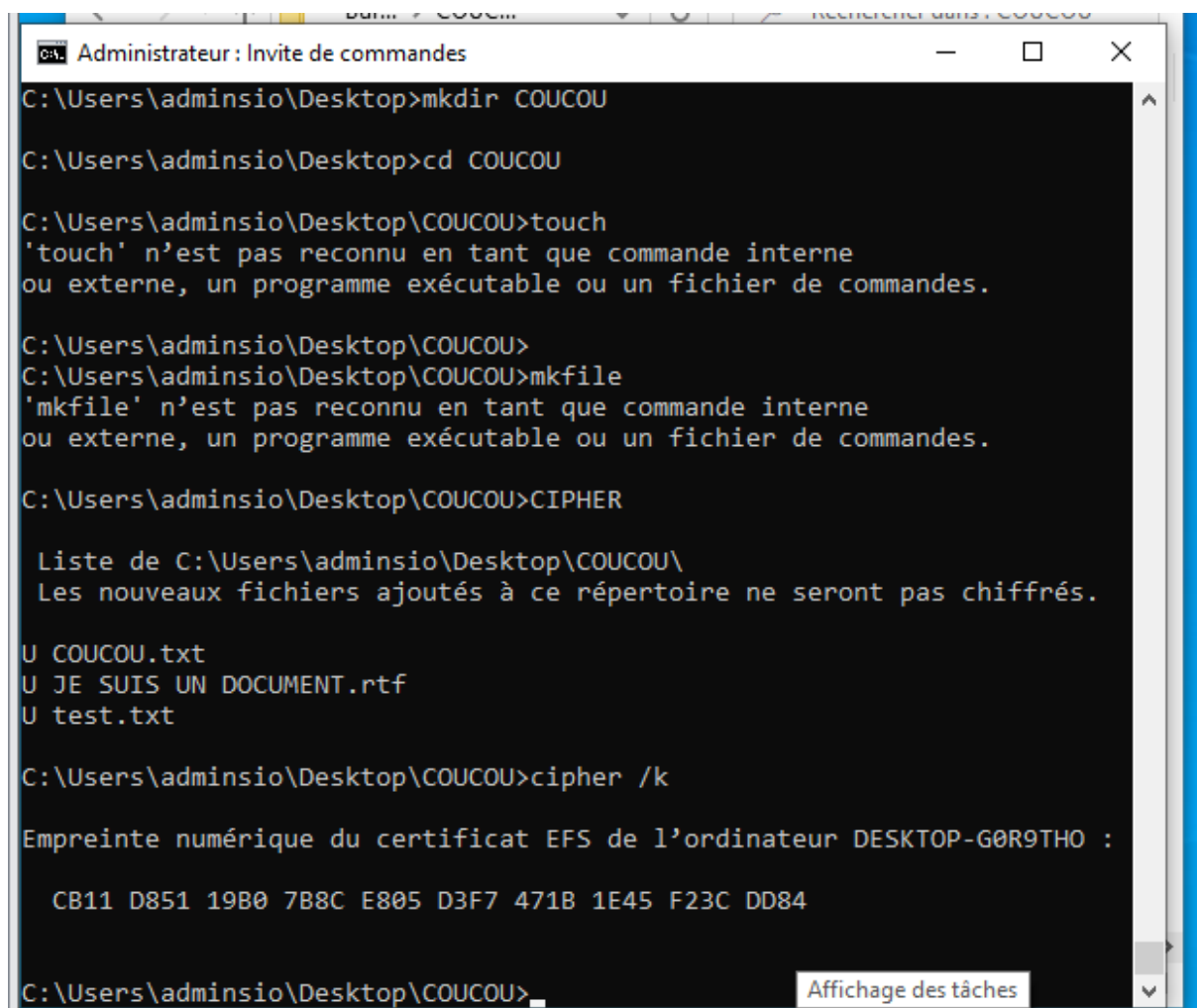
C:\Users\adminisio\Desktop\COUCOU>
C:\Users\adminisio\Desktop\COUCOU>mkfile
'mkfile' n'est pas reconnu en tant que commande interne
ou externe, un programme exécutable ou un fichier de commandes.

C:\Users\adminisio\Desktop\COUCOU>CIPHER

Liste de C:\Users\adminisio\Desktop\COUCOU\
Les nouveaux fichiers ajoutés à ce répertoire ne seront pas chiffrés.

U COUCOU.txt
U JE SUIS UN DOCUMENT.rtf
U test.txt

C:\Users\adminisio\Desktop\COUCOU>c
```



```
C:\Users\adminisio\Desktop>mkdir COUCOU

C:\Users\adminisio\Desktop>cd COUCOU

C:\Users\adminisio\Desktop\COUCOU>touch
'touch' n'est pas reconnu en tant que commande interne
ou externe, un programme exécutable ou un fichier de commandes.

C:\Users\adminisio\Desktop\COUCOU>
C:\Users\adminisio\Desktop\COUCOU>mkfile
'mkfile' n'est pas reconnu en tant que commande interne
ou externe, un programme exécutable ou un fichier de commandes.

C:\Users\adminisio\Desktop\COUCOU>CIPHER

Liste de C:\Users\adminisio\Desktop\COUCOU\
Les nouveaux fichiers ajoutés à ce répertoire ne seront pas chiffrés.

U COUCOU.txt
U JE SUIS UN DOCUMENT.rtf
U test.txt

C:\Users\adminisio\Desktop\COUCOU>cipher /k

Empreinte numérique du certificat EFS de l'ordinateur DESKTOP-GØR9TH0 :

CB11 D851 19BØ 7B8C E8Ø5 D3F7 471B 1E45 F23C DD84

C:\Users\adminisio\Desktop\COUCOU>
```

Cipher /k pour créer une clé sécurisée.

```
Administrateur : Invite de commandes

Liste de C:\Users\adminisio\Desktop\COUCOU\
Les nouveaux fichiers ajoutés à ce répertoire ne seront pas chiffrés.

U COUCOU.txt
U JE SUIS UN DOCUMENT.rtf
U test.txt

C:\Users\adminisio\Desktop\COUCOU>cipher /k

Empreinte numérique du certificat EFS de l'ordinateur DESKTOP-G0R9TH0 :

    CB11 D851 19B0 7B8C E805 D3F7 471B 1E45 F23C DD84

C:\Users\adminisio\Desktop\COUCOU>cipher /e

Chiffrement des fichiers dans C:\Users\adminisio\Desktop\COUCOU\

COUCOU.txt           [OK]
JE SUIS UN DOCUMENT.rtf [OK]
test.txt             [OK]

3 fichier(s) [ou répertoire(s)] dans 1 répertoire(s) ont été chiffrés.

La conversion de fichiers de texte en clair à texte chiffré peut laisser des
fichiers en texte en clair sur les volumes de disque. Il est recommandé
d'utiliser la commande CIPHER /W:directory pour nettoyer le disque après la
fin de la conversion.

C:\Users\adminisio\Desktop\COUCOU>
```

Cipher /e (suivi d'un paramètre optionnel /s pour préciser le dossier) pour chiffrer.

```
Administrateur : Invite de commandes

Empreinte numérique du certificat EFS de l'ordinateur DESKTOP-G0R9TH0 :

    CB11 D851 19B0 7B8C E805 D3F7 471B 1E45 F23C DD84

C:\Users\adminisio\Desktop\COUCOU>cipher /e

Chiffrement des fichiers dans C:\Users\adminisio\Desktop\COUCOU\

COUCOU.txt           [OK]
JE SUIS UN DOCUMENT.rtf [OK]
test.txt             [OK]

3 fichier(s) [ou répertoire(s)] dans 1 répertoire(s) ont été chiffrés.

La conversion de fichiers de texte en clair à texte chiffré peut laisser des
fichiers en texte en clair sur les volumes de disque. Il est recommandé
d'utiliser la commande CIPHER /W:directory pour nettoyer le disque après la
fin de la conversion.

C:\Users\adminisio\Desktop\COUCOU>cipher

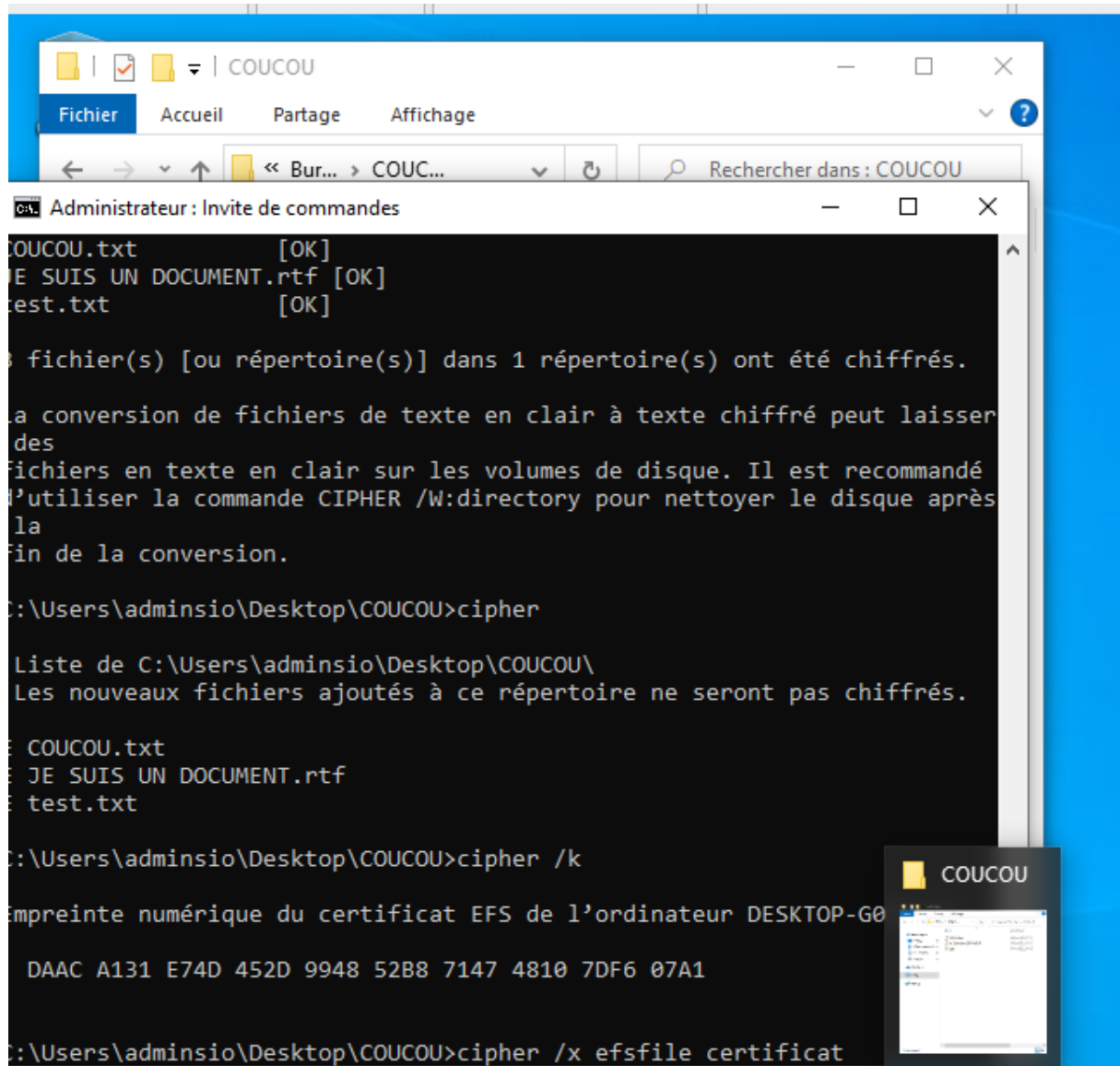
Liste de C:\Users\adminisio\Desktop\COUCOU\
Les nouveaux fichiers ajoutés à ce répertoire ne seront pas chiffrés.

E COUCOU.txt
E JE SUIS UN DOCUMENT.rtf
E test.txt

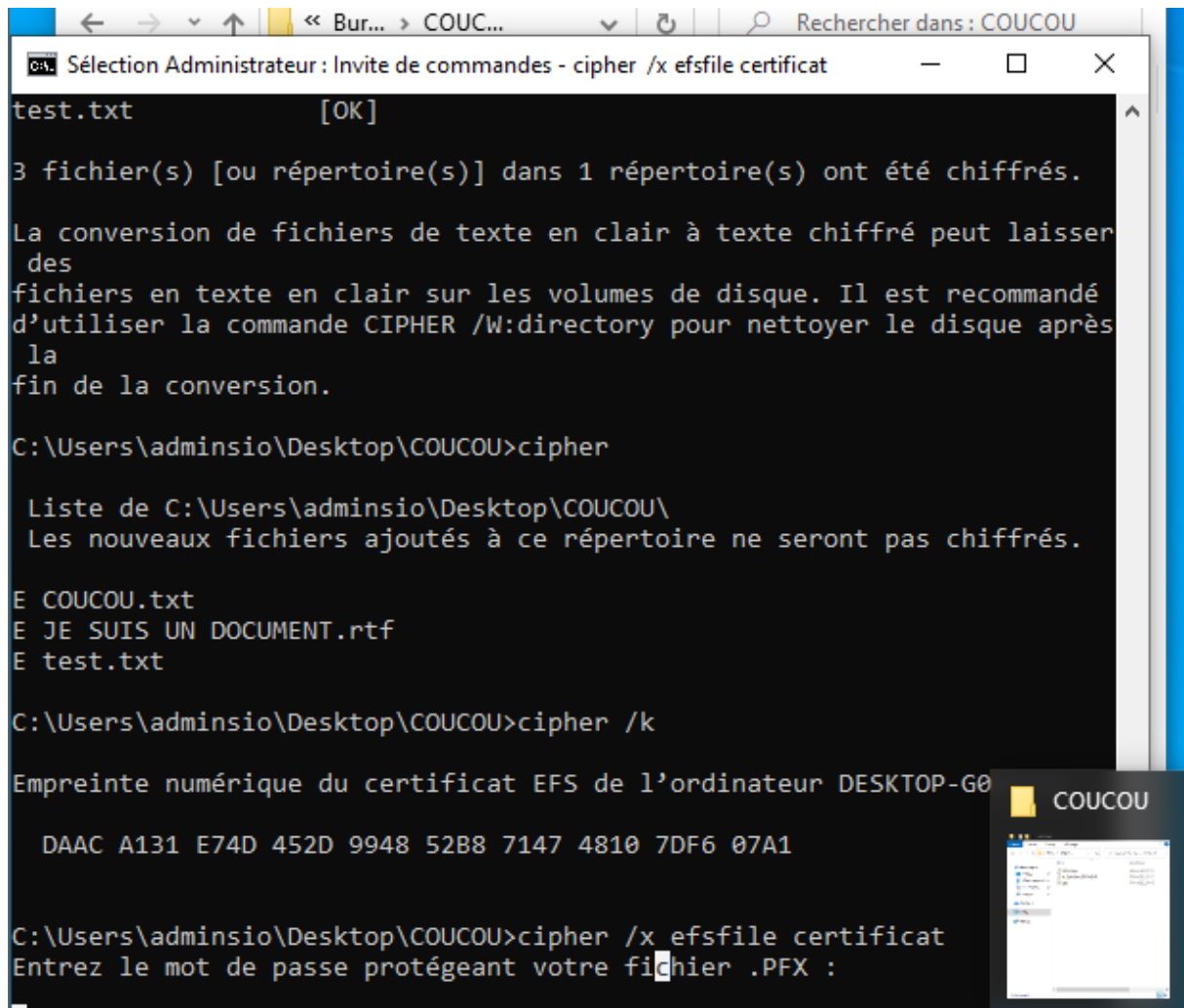
C:\Users\adminisio\Desktop\COUCOU>
```

Cipher /d pour déchiffrer.

SAUVEGARDE CLE DE CHIFFREMENT ET CERTIFICAT.



Cipher /x [nomFichier] pour sauvegarder le certificat contenant la clé. Efsfile permet de sauvegarder toutes les clés utilisées lors de la commande cipher /e



```
test.txt [OK]

3 fichier(s) [ou répertoire(s)] dans 1 répertoire(s) ont été chiffrés.

La conversion de fichiers de texte en clair à texte chiffré peut laisser
des
fichiers en texte en clair sur les volumes de disque. Il est recommandé
d'utiliser la commande CIPHER /W:directory pour nettoyer le disque après
la
fin de la conversion.

C:\Users\adminisio\Desktop\COUCOU>cipher

Liste de C:\Users\adminisio\Desktop\COUCOU\
Les nouveaux fichiers ajoutés à ce répertoire ne seront pas chiffrés.

E COUCOU.txt
E JE SUIS UN DOCUMENT.rtf
E test.txt

C:\Users\adminisio\Desktop\COUCOU>cipher /k

Empreinte numérique du certificat EFS de l'ordinateur DESKTOP-G0

DAAC A131 E74D 452D 9948 52B8 7147 4810 7DF6 07A1

C:\Users\adminisio\Desktop\COUCOU>cipher /x efsfile certificat
Entrez le mot de passe protégeant votre fichier .PFX :
```

Entrez mot de passe (memo : itsfile1001)

Le fichier est créé dans le dossier où se trouve le cmd (ici Dans le dossier COUCOU sur le Bureau). On peut le déplacer librement après

Accès depuis un autre compte aux données chiffrées

Nouvel utilisateur

Nom d'utilisateur : TEST

Nom complet : TEST

Description : TEST

Mot de passe : [masked]

Confirmer le mot de passe : [masked]

☒ L'utilisateur doit changer le mot de passe à la prochaine ouverture de session

☐ L'utilisateur ne peut pas changer de mot de passe

☐ Le mot de passe n'expire jamais

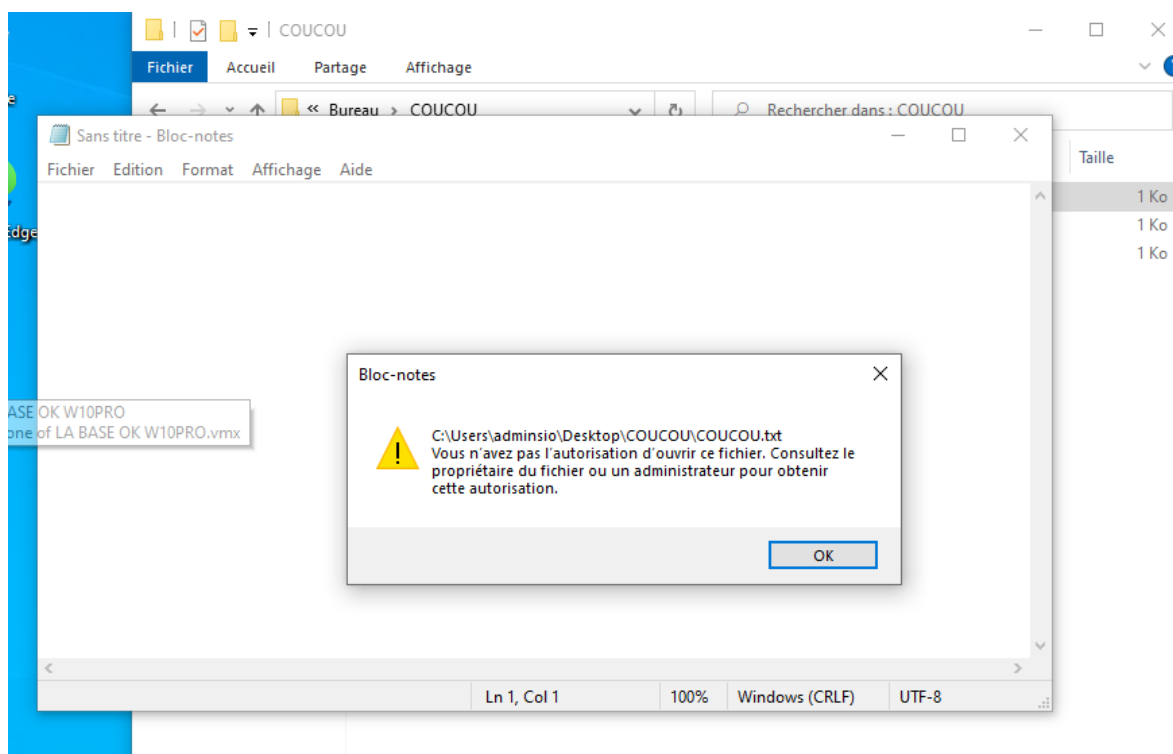
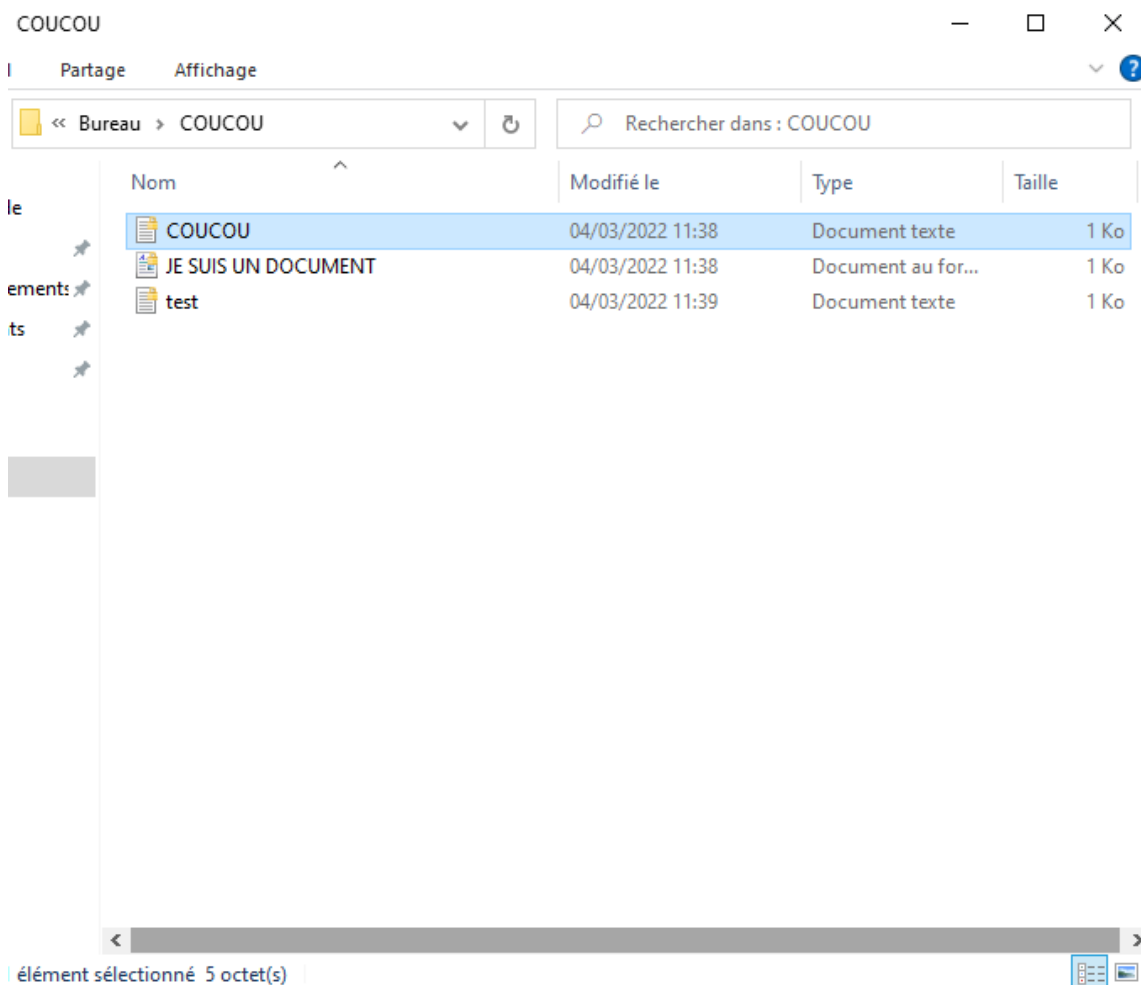
☐ Le compte est désactivé

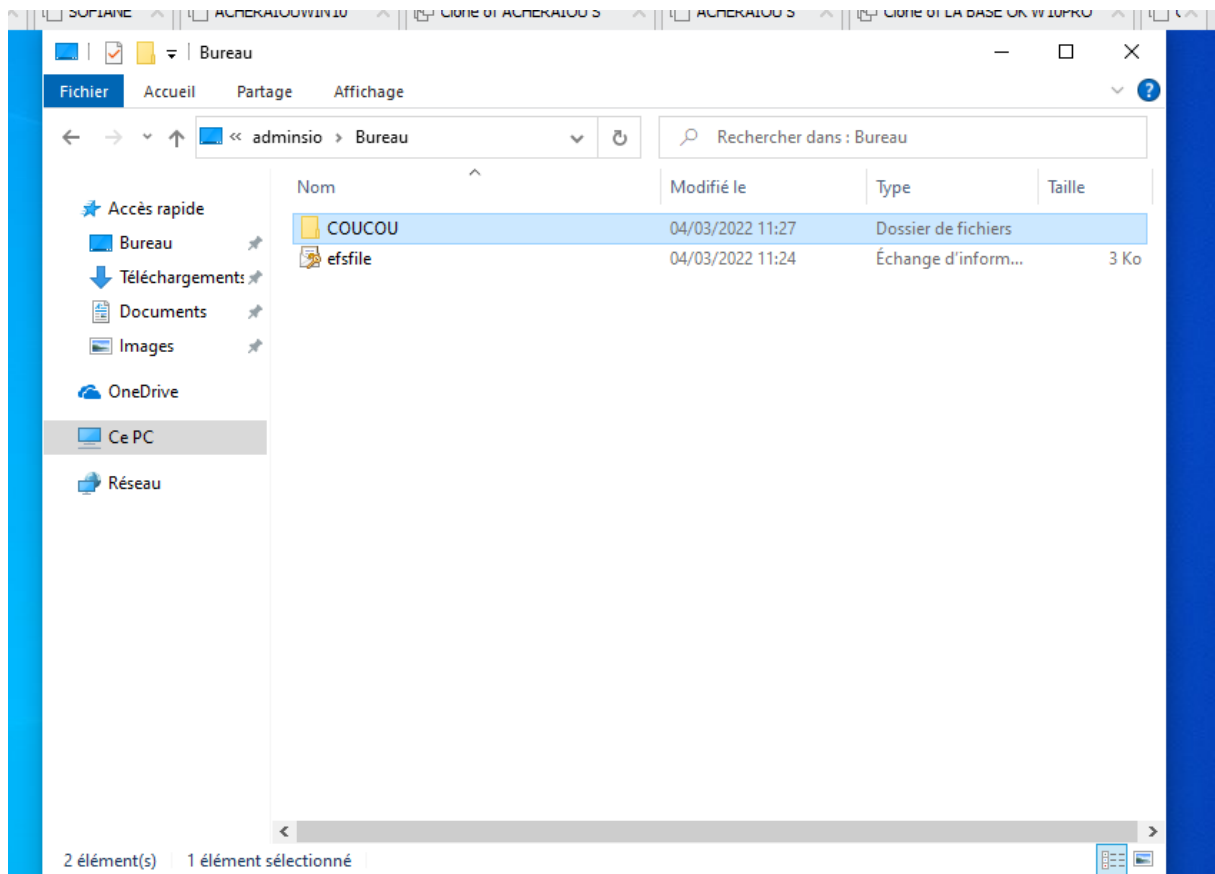
Aide Créer Fermer

Création d'un utilisateur test.

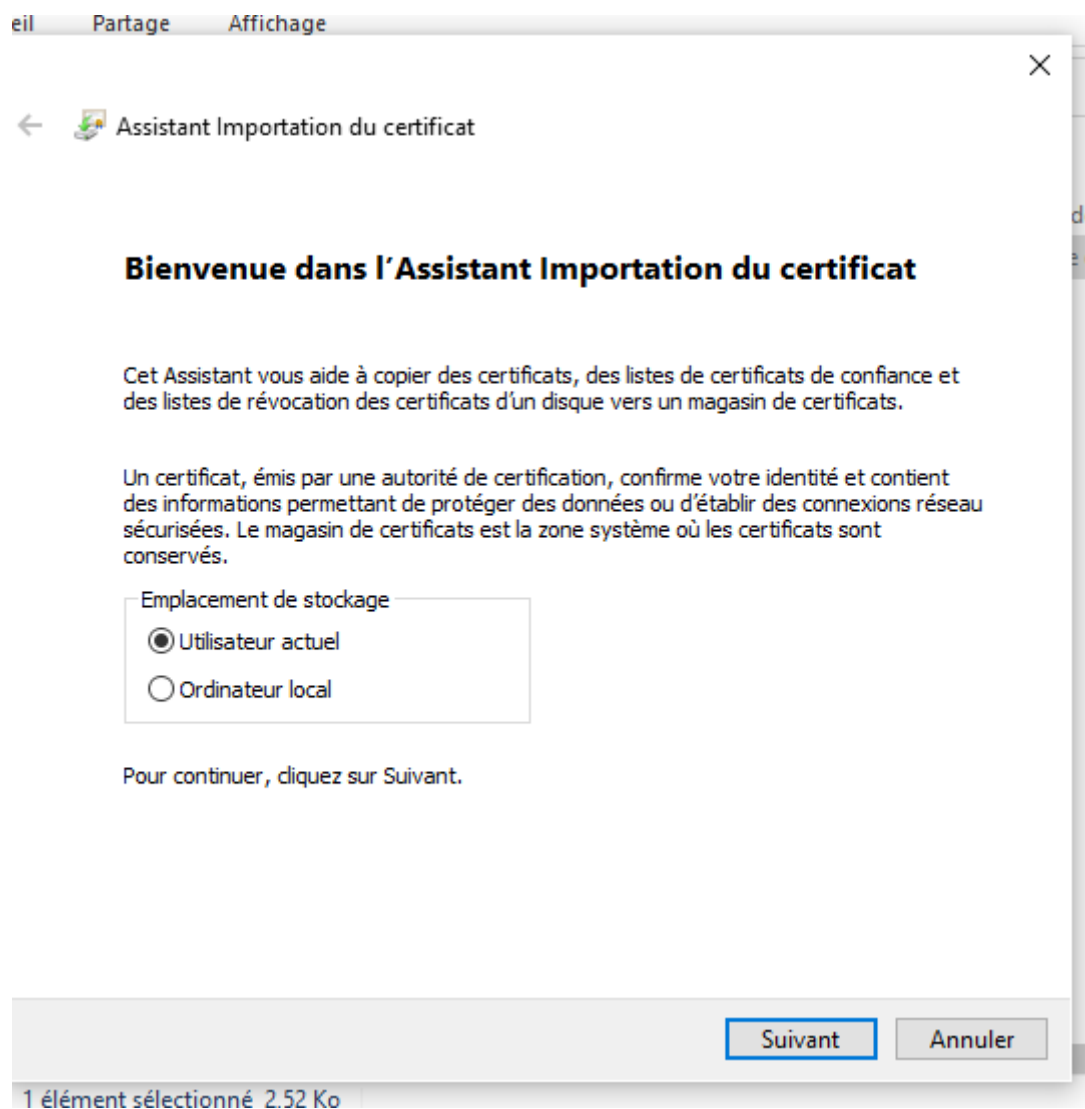
Une fois l'utilisateur crée on va sur son compte puis on cherche les fichiers chiffrés.

(C:/Users/adminsio).



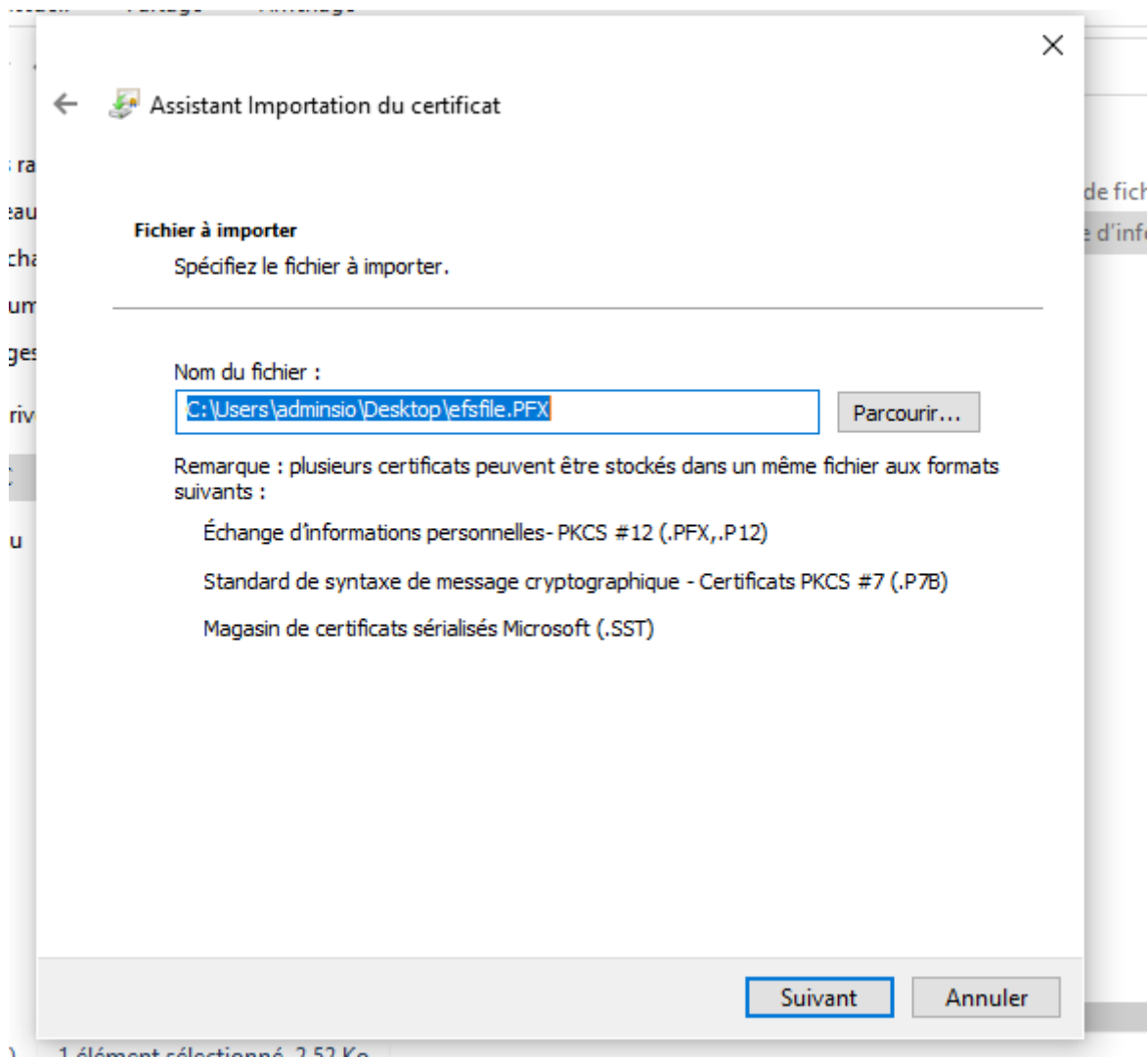


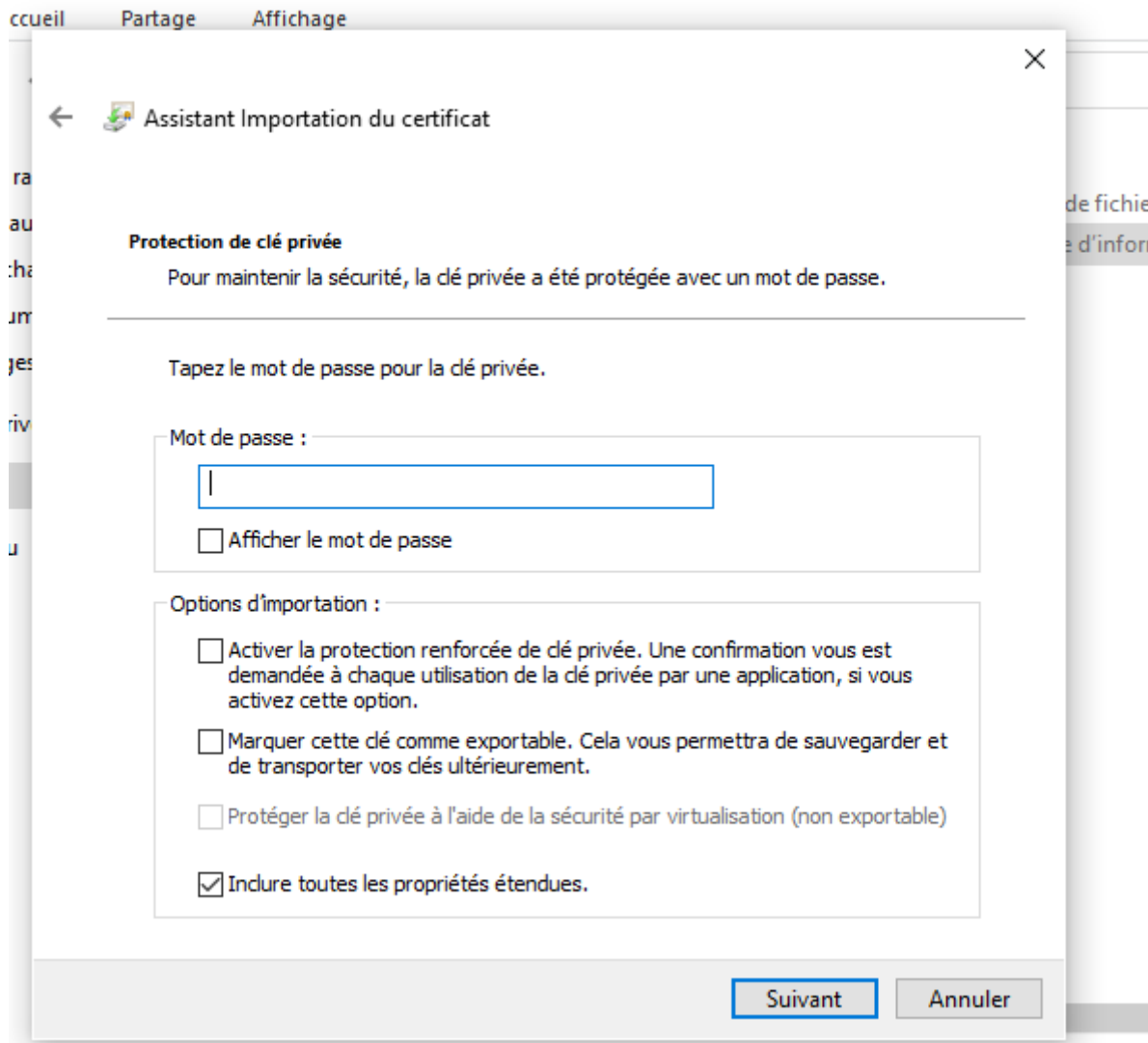
Double cliquer sur le certificat un écran comme ceci apparait.



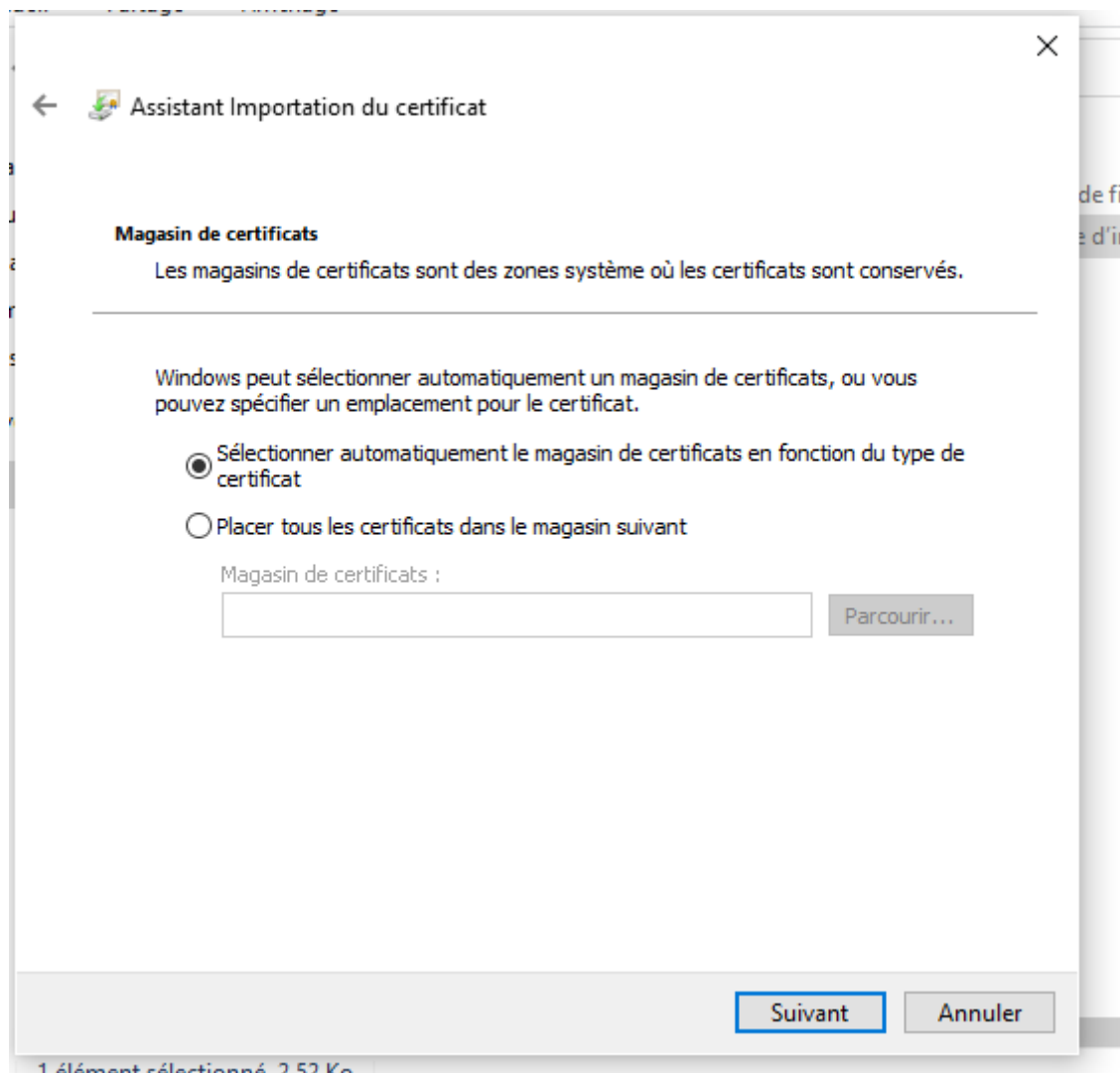
Ordinateur local peut-être utile dans le cas ou de nombreux utilisateurs sont sur un même PC.

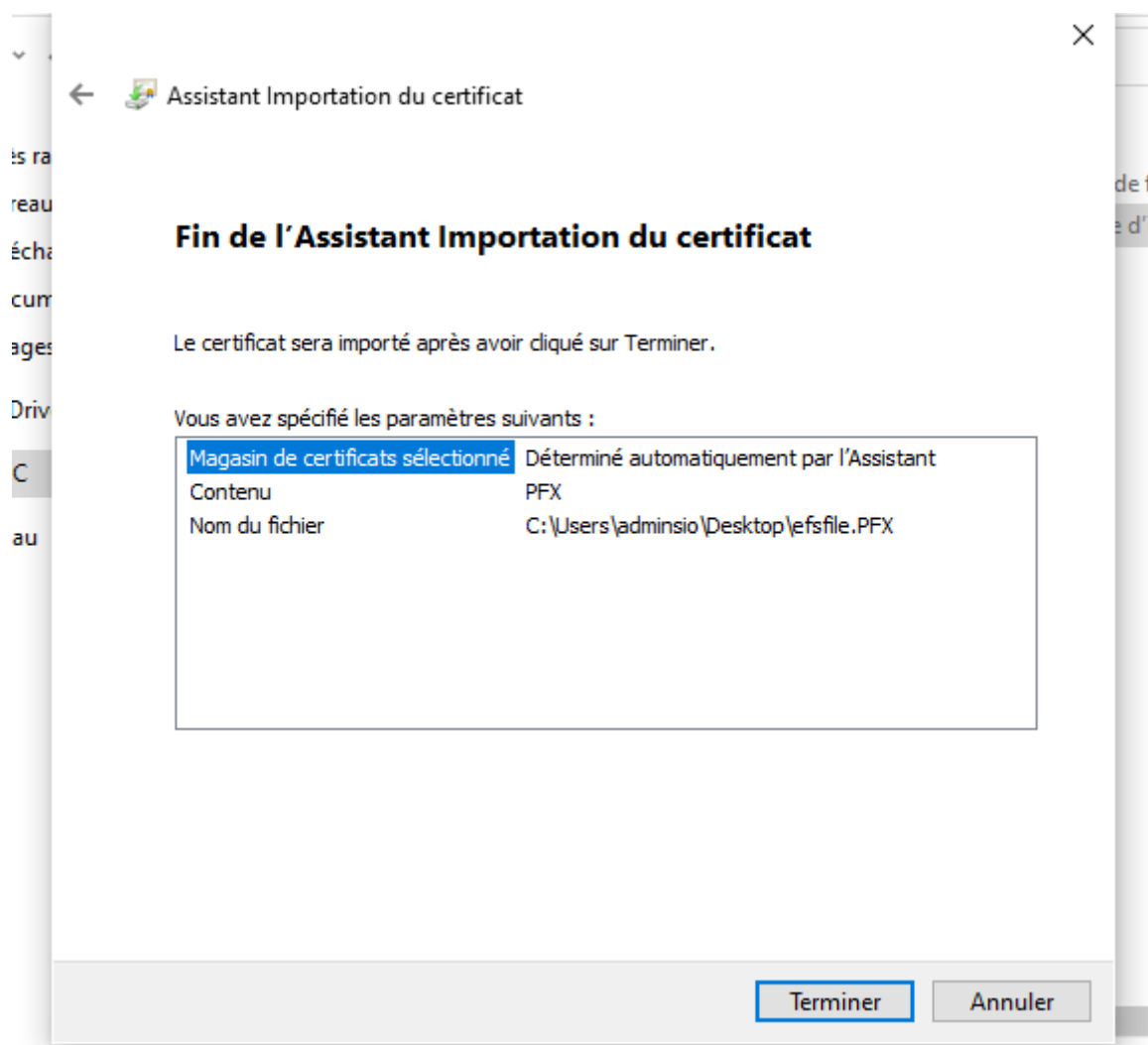
Choisir « utilisateur actuel »

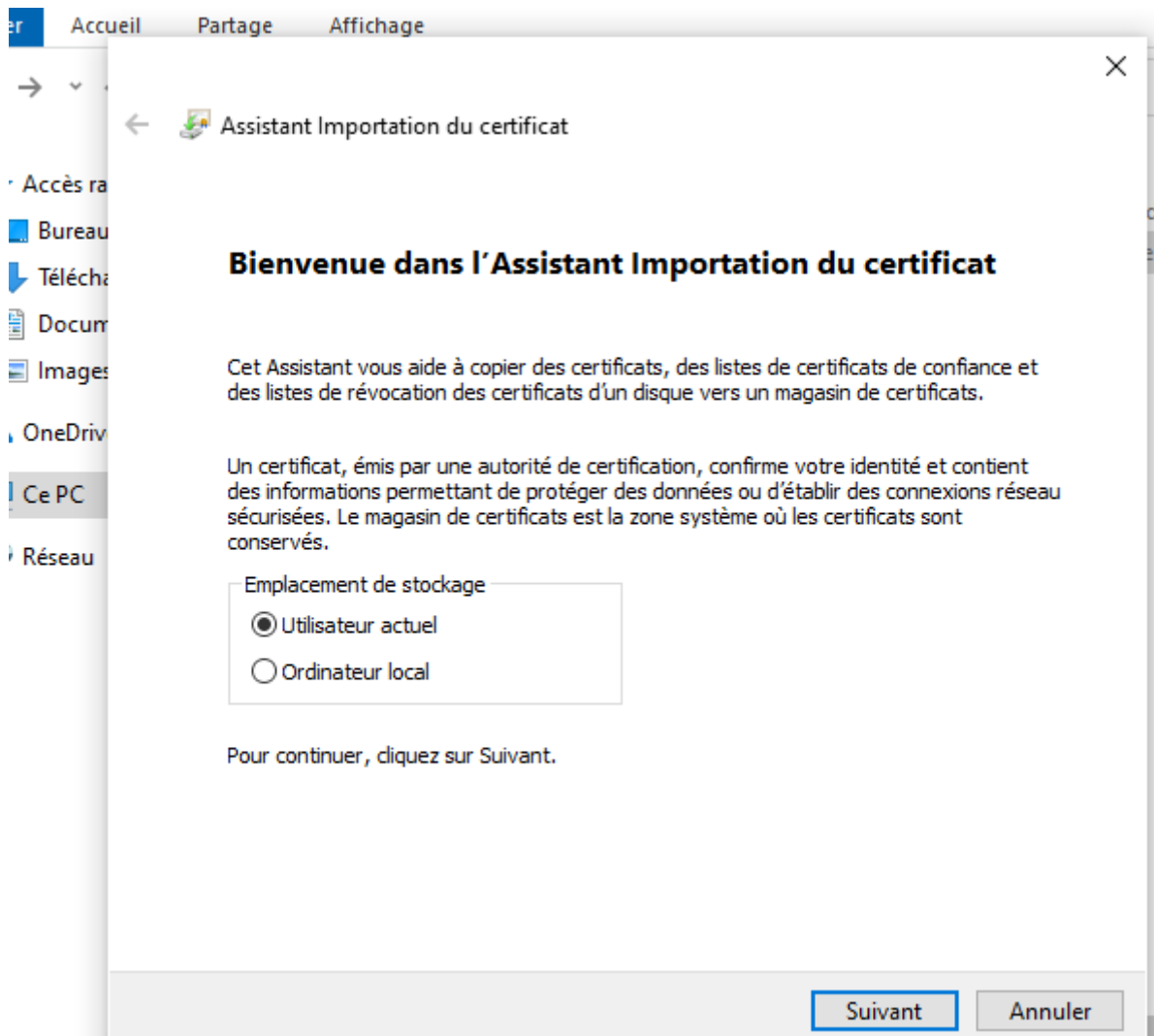




Taper le mot de passe qui va protégé le certificat(dans notre exemple :itsfile1001)







DIFFERENCES AVEC BITLOCKER

Contrairement à BitLocker, EFS permet de chiffrer un dossier ou fichier en particulier, alors que BitLocker doit chiffrer le disque en entier.

BitLocker sauvegarde la clé de chiffrement dans une puce matérielle (TPM) tandis que EFS utilise un certificat stocké et généré en local ce qui peut poser des problèmes si quelqu'un non-autorisé y accède

Identifier les risques associés à l'utilisation d'EFS

Si le certificat, est volé ou perdu, on perd complètement l'accès aux fichiers chiffré sans méthode de récupération, voir on laisse potentiellement l'accès a des personnes non autorisées aux fichiers. Il faut donc stocker le certificat dans un endroits sécurisé tel qu'un coffre fort.

VI. Autres outils

-VeraCrypt

-encryptonclick

-TrueCrypt