


## UTILISATION DU SYSTEME EFS

<b>PARCOURS</b>	<b>SISR</b> <input checked="" type="checkbox"/>	<b>SLAM</b> <input type="checkbox"/>
-----------------	---	--------------------------------------

<b>Lieu de réalisation</b>	Campus Montsouris	
<b>Période de réalisation</b>	Du : 19.01.2024	Au :
<b>Modalité de réalisation</b>	SEUL <input checked="" type="checkbox"/>	EN EQUIPE <input type="checkbox"/>

<b>Intitulé de la mission</b>	Utilisation du système EFS
<b>Description du contexte de la mission</b>	Chiffrer des données et gérer leur accès

<b>Contraintes &amp; Résultat</b>	Ressources fournies / contraintes techniques / Résultats attendu
	Windows Server 2022, Laptop, Hyper V
<b>Productions associées</b>	Liste des documents produits et description

<b>Modalités d'accès aux productions</b>	Identifiants, mots de passe, URL d'un espace de stockage et présentation de l'organisation du stockage

## Table des matières

<b>1. Introduction.....</b>	<b>3</b>
<b>1. Création des utilisateurs, création et chiffrement de dossiers et fichiers .....</b>	<b>4</b>
1.1. Création des utilisateurs .....	4
1.2. Création et chiffrement des dossiers et fichiers.....	6
<b>2. Gestion des accès aux fichiers et dossiers chiffrés .....</b>	<b>9</b>
2.1. Permettre l'accès à certains fichiers : les autorisations simples.....	9
2.2. Permettre l'accès à tous les fichiers : l'utilisation de clés.....	11
2.2.1. Exportation d'une clé .....	11
2.2.2. Importation d'une clé .....	13
2.3. Permettre l'accès à l'ensemble des fichiers à l'ensemble des utilisateurs .....	16
2.3.1. Création d'un certificat d'agent de récupération de données .....	16
2.3.2. Création d'un agent de récupération de données .....	18

### **1. Introduction**

Le système de fichiers EFS (Encrypting File System) est une fonctionnalité de Windows permettant de chiffrer des fichiers et des dossiers afin de sécuriser les données sensibles contre les accès non autorisés. Contrairement à BitLocker, qui chiffre l'ensemble d'un disque, EFS fonctionne au niveau des fichiers et des dossiers, offrant ainsi une flexibilité accrue pour la protection des informations.

Dans un environnement professionnel ou personnel, l'utilisation d'EFS garantit la confidentialité des données stockées sur un ordinateur, même en cas de vol ou d'accès physique au disque dur. Ce système repose sur un chiffrement basé sur des certificats, propres à chaque utilisateur, permettant ainsi un contrôle précis des autorisations d'accès aux fichiers protégés.

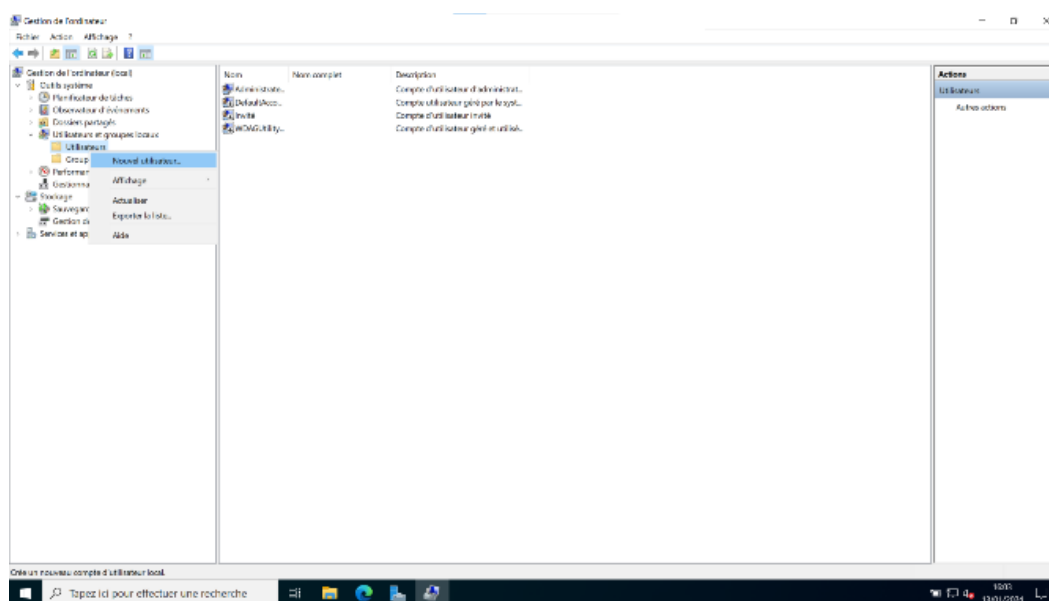
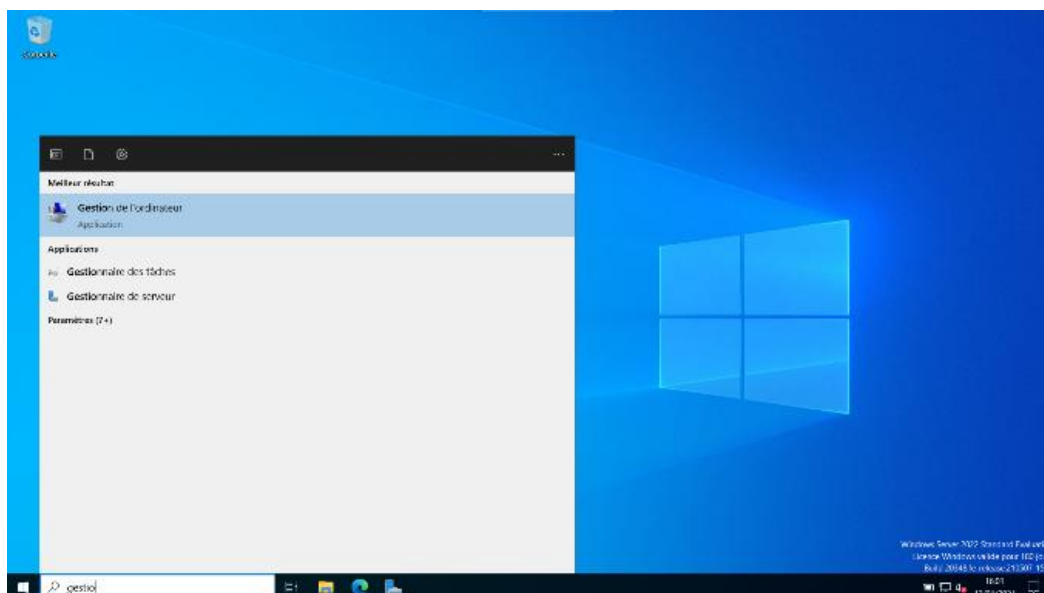
Ce guide détaille les étapes essentielles pour configurer et utiliser EFS sur Windows Server 2022. Il couvre la création d'utilisateurs, le chiffrement de fichiers et dossiers, ainsi que la gestion des accès à ces données. Il présente également des méthodes avancées, comme l'exportation et l'importation de clés de chiffrement, et la mise en place d'un agent de récupération pour assurer un accès de secours aux fichiers chiffrés.

En suivant ces procédures, les administrateurs et utilisateurs pourront sécuriser efficacement leurs données tout en maîtrisant les différentes options de gestion des accès et des clés de chiffrement offertes par Windows.

### 1. Création des utilisateurs, création et chiffrement de dossiers et fichiers

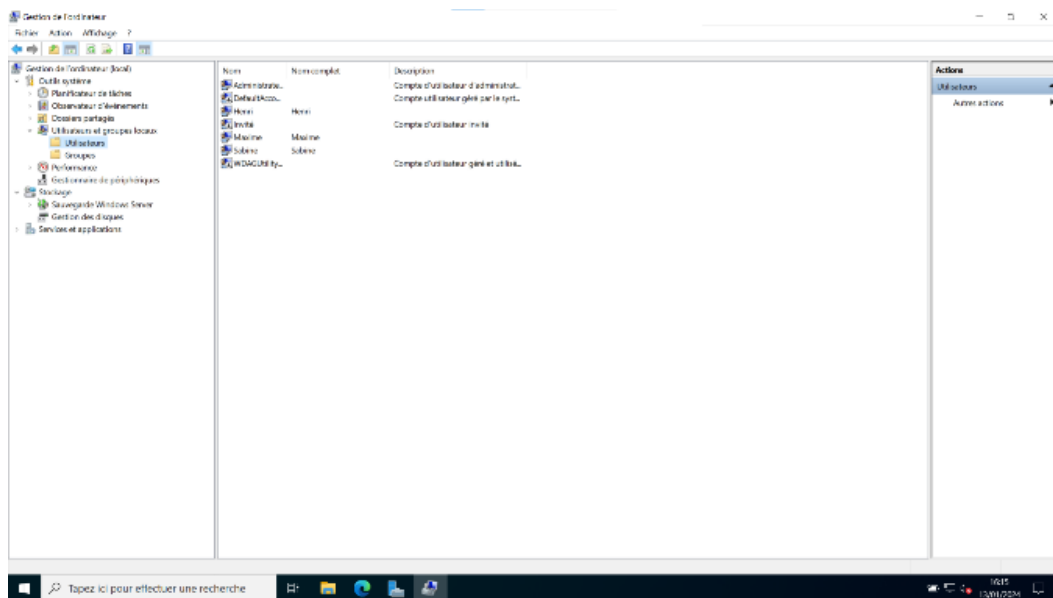
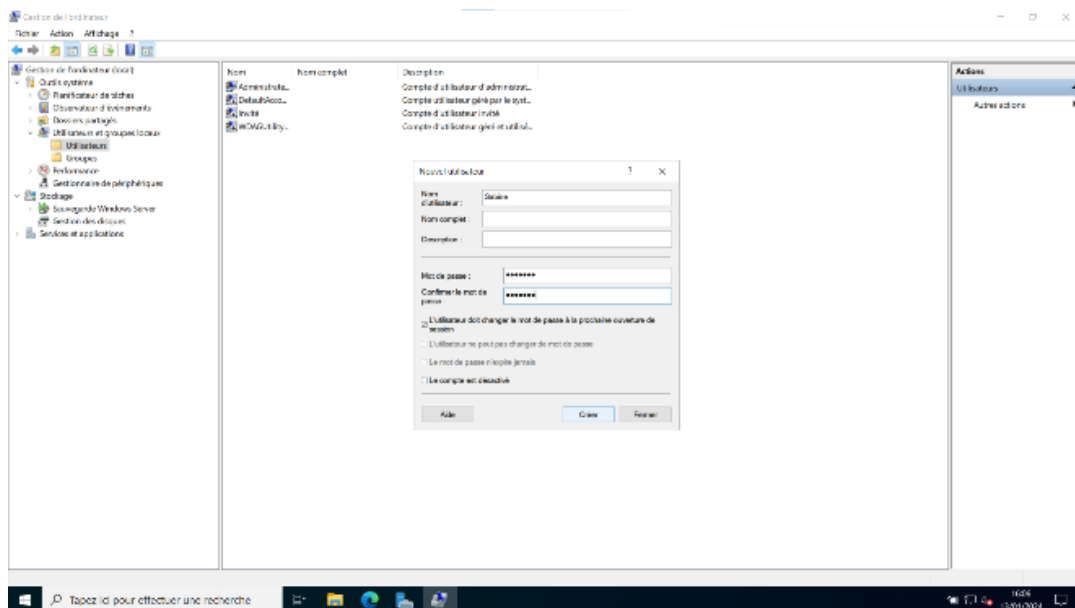
#### 1.1. Création des utilisateurs

La procédure débute avec la création des utilisateurs. Accéder au gestionnaire de l'ordinateur, à l'aide de la barre des tâches. Dérouler successivement Gestion de l'ordinateur > Outils système > Utilisateurs et groupes locaux > Utilisateurs. Faire un clic droit, puis sélectionner Nouvel utilisateur dans la fenêtre.



## Configuration et utilisation du système Windows EFS

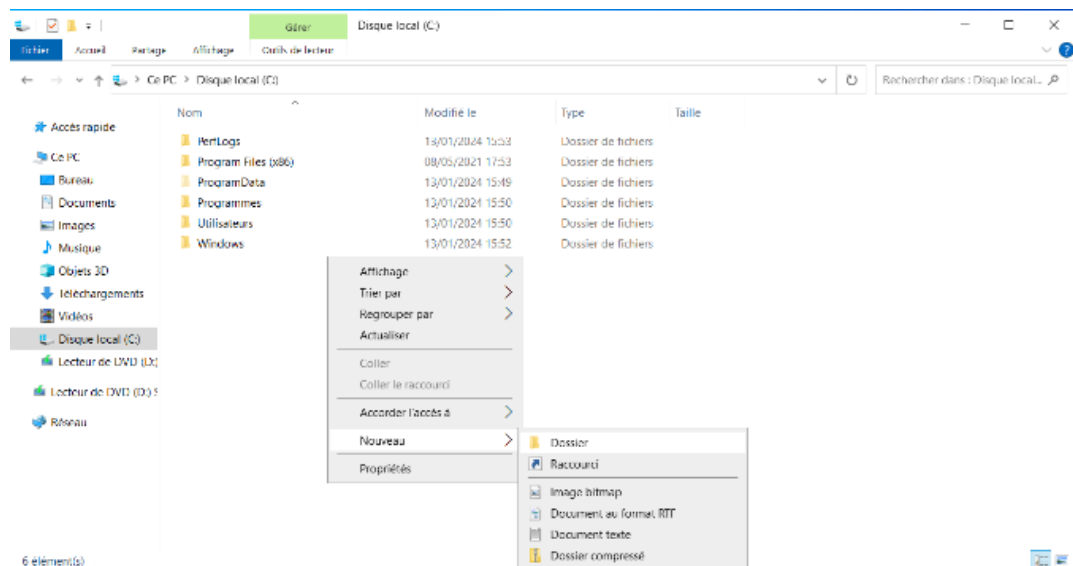
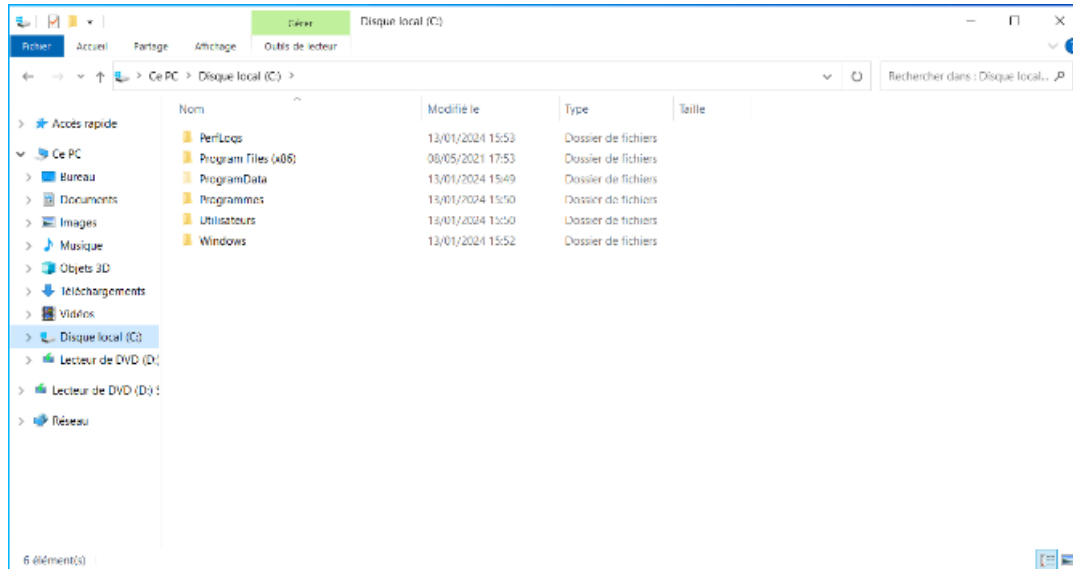
Une nouvelle fenêtre apparaît invitant l'administrateur à remplir les données du futur utilisateur.



Répéter cette procédure 3 fois, en créant Sabine, Maxime, et Henri.

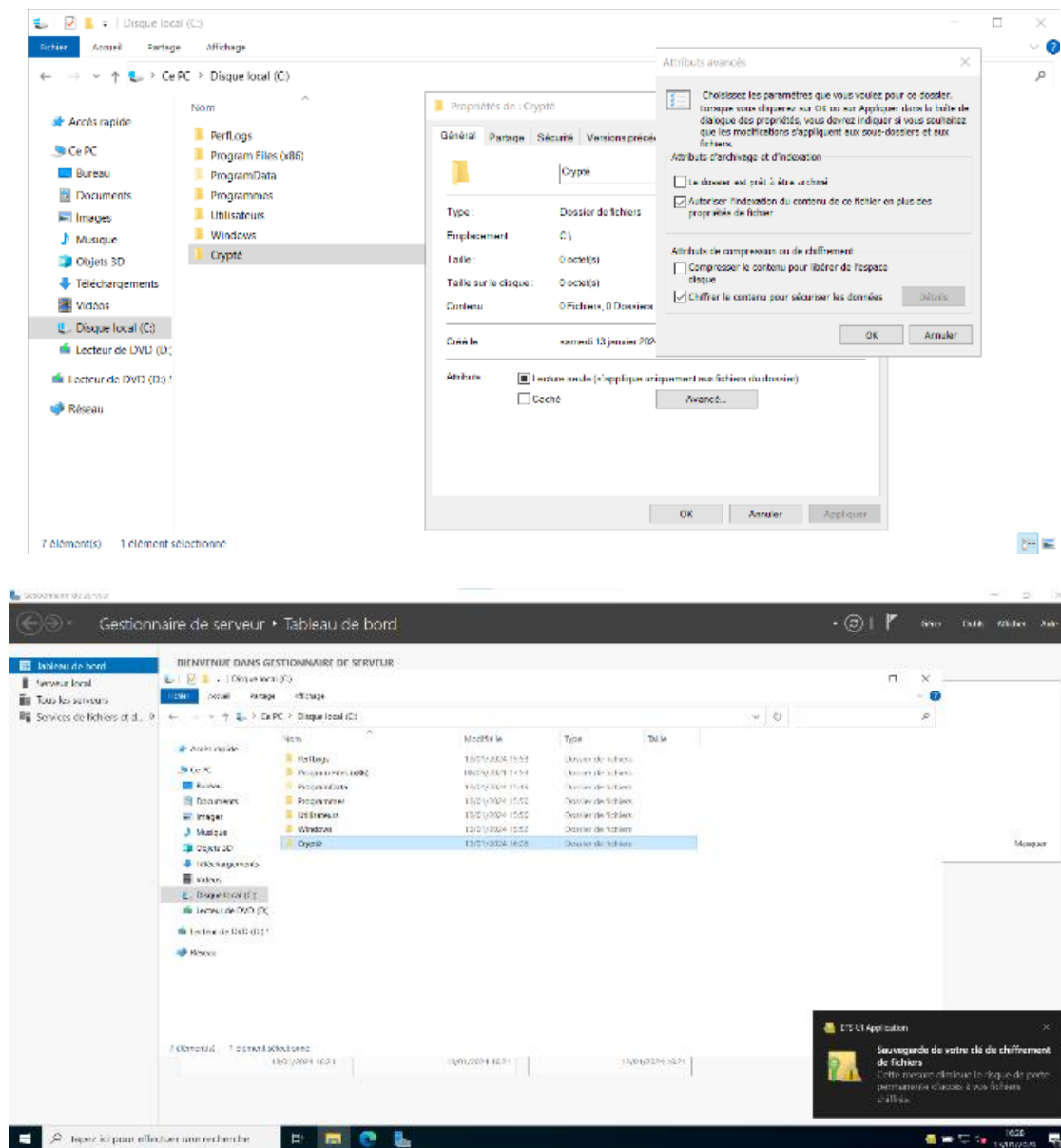
## 1.2. Création et chiffrement des dossiers et fichiers

Créer un dossier nommé “Chiffré” dans le volume C:\.



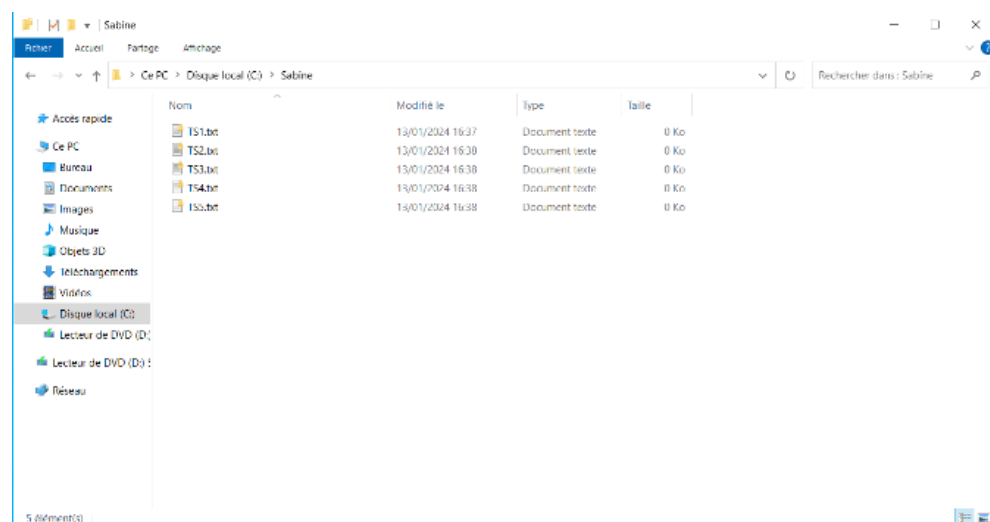
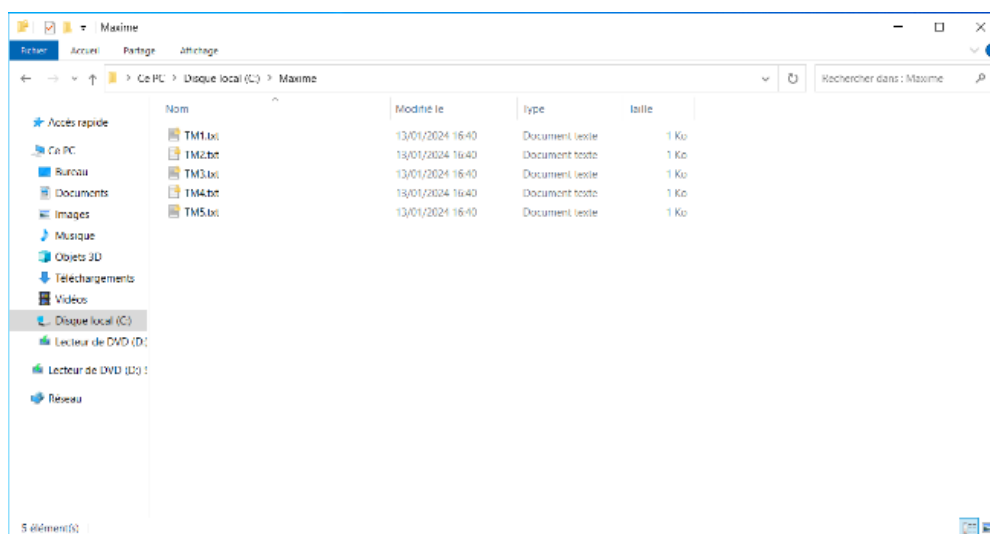
## Configuration et utilisation du système Windows EFS

Accéder à ces propriétés à l'aide du menu déroulant en cliquant droit dessus.



## Configuration et utilisation du système Windows EFS

Se connecter à l'utilisateur Sabine, accéder au dossier Chiffré, créer 5 fichiers textes, nommés successivement TS1, TS2, etc. Jusqu'à TS5. Ces fichiers sont intrinsèquement chiffrés. Ecrire à l'intérieur de chacun "Ce fichier est chiffré.". Répéter cette procédure avec l'utilisateur Maxime, en les nommant TM1, TM2, etc. Jusqu'à TM5.

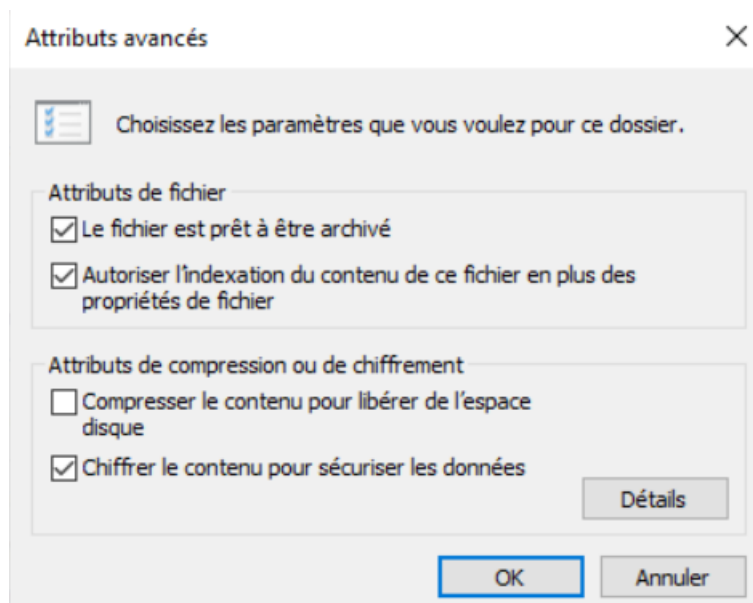
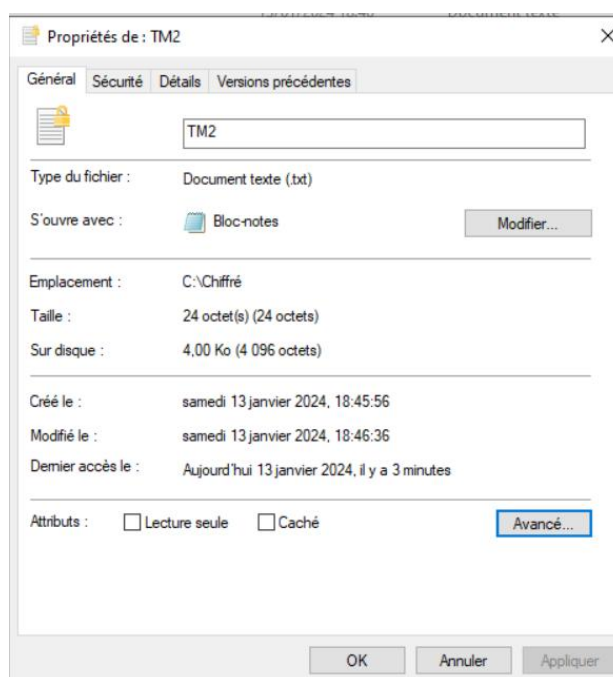




### 2. Gestion des accès aux fichiers et dossiers chiffrés

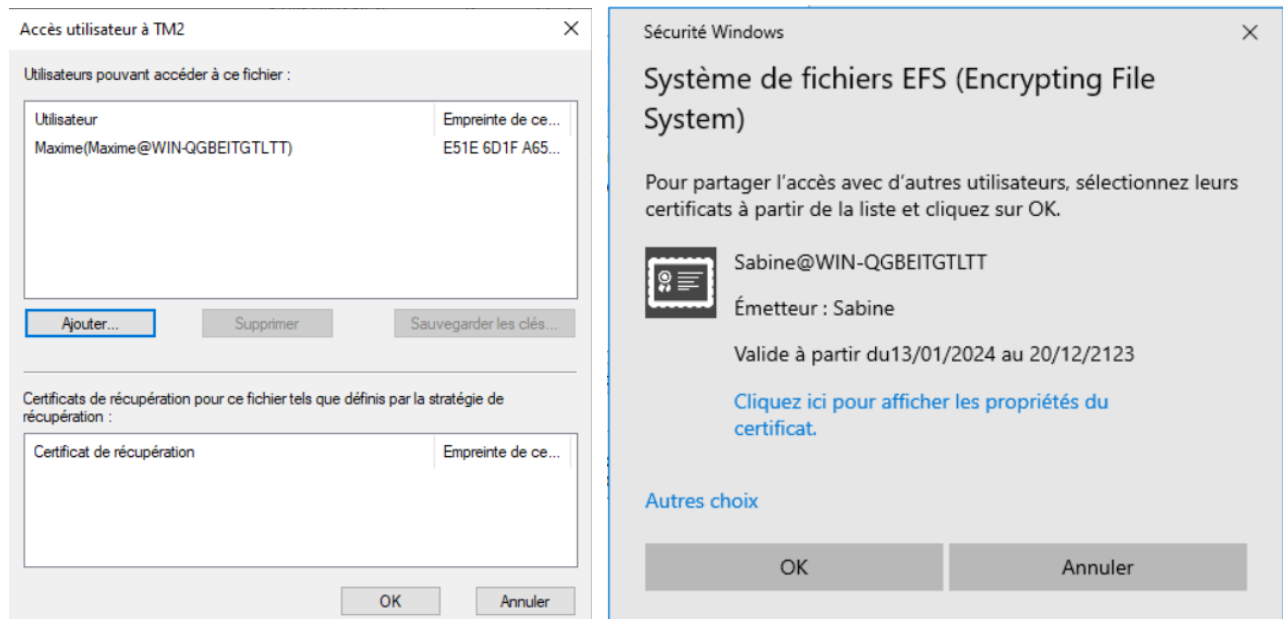
#### 2.1. Permettre l'accès à certains fichiers : les autorisations simples

Permettre l'accès de seulement certains fichiers d'un utilisateur à l'autre peut se faire à l'aide d'autorisations en allant dans les propriétés du fichier. Par la suite, aller dans "Avancé".

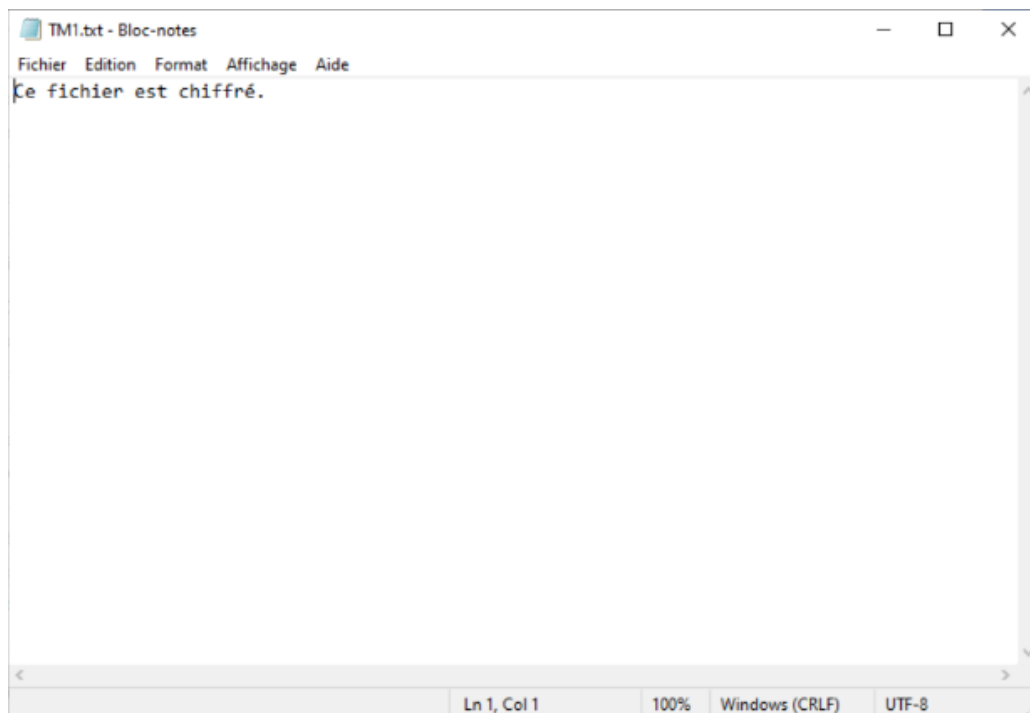


## Configuration et utilisation du système Windows EFS

Cliquer sur “Ajouter”. Ici, choisir l'utilisateur souhaité, Maxime, dans “Autres choix”. Répéter cette procédure avec le fichier TM1.



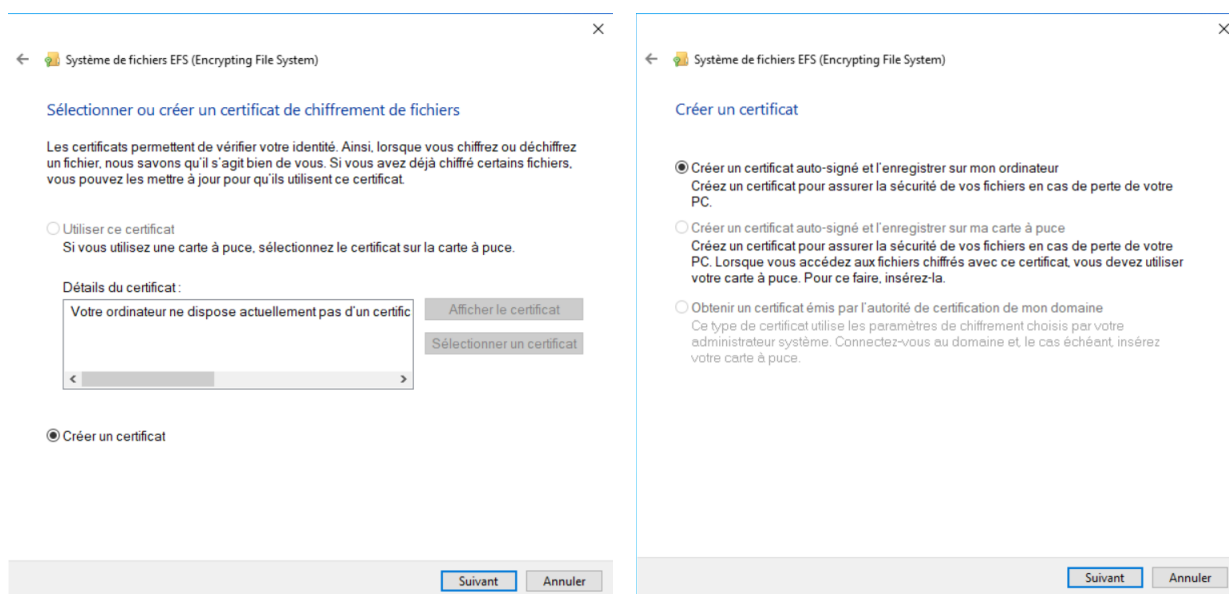
L'utilisateur Sabine peut désormais lire les fichiers TM1 et TM2 de Maxime.



### 2.2. Permettre l'accès à tous les fichiers : utilisation de clés

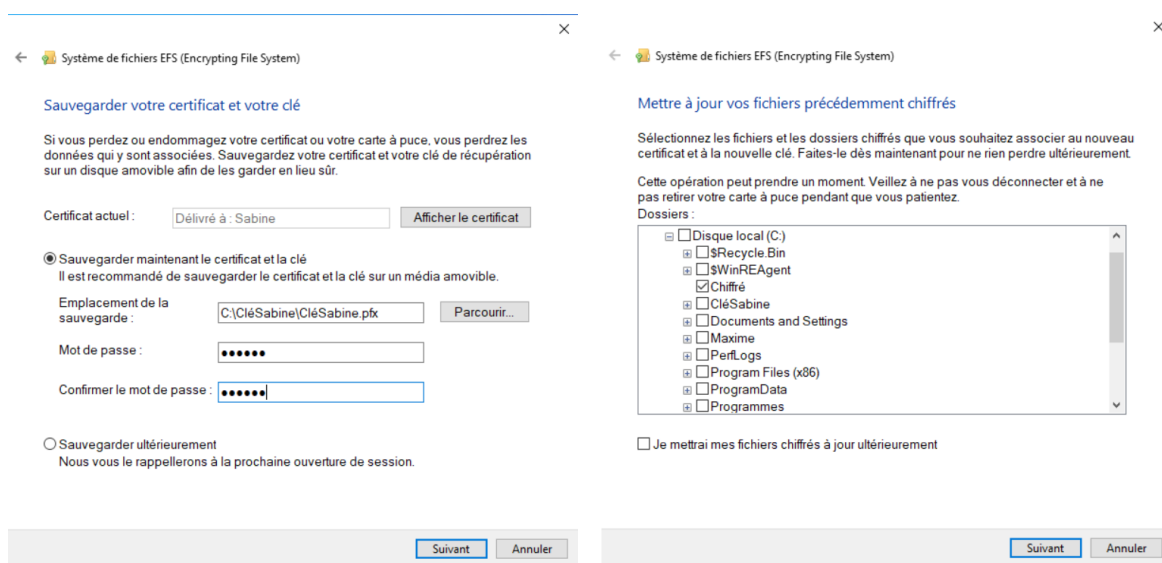
#### 2.2.1. Exportation d'une clé

Se connecter sur la session de Maxime et chercher “gérer les certificats de recherche” dans la barre Windows. Par la suite, le système nous propose la création d'un certificat.



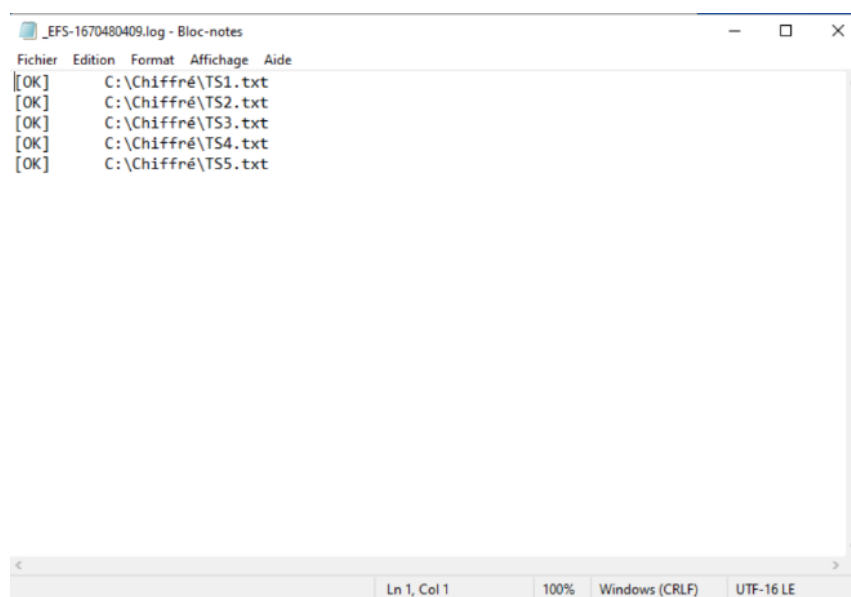
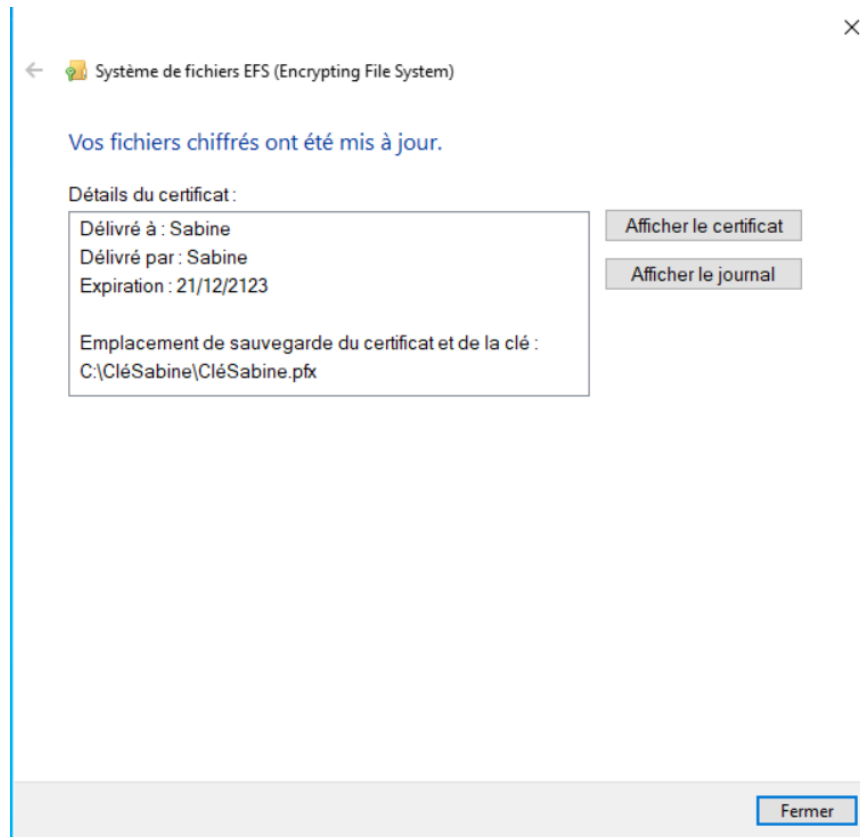
Il faut nommer et sauvegarder la future clé de format pfx dans un dossier. Nous allons la nommer “CléSabine”, et la rangerons dans le dossier “CléSabine” dans le volume C:\.

Enfin, choisir les fichiers et dossiers chiffrés que nous voulons associer à cette clé. Nous choisissons le dossier “Chiffré”, qui contient les fichiers auxquels nous voulons donner accès.



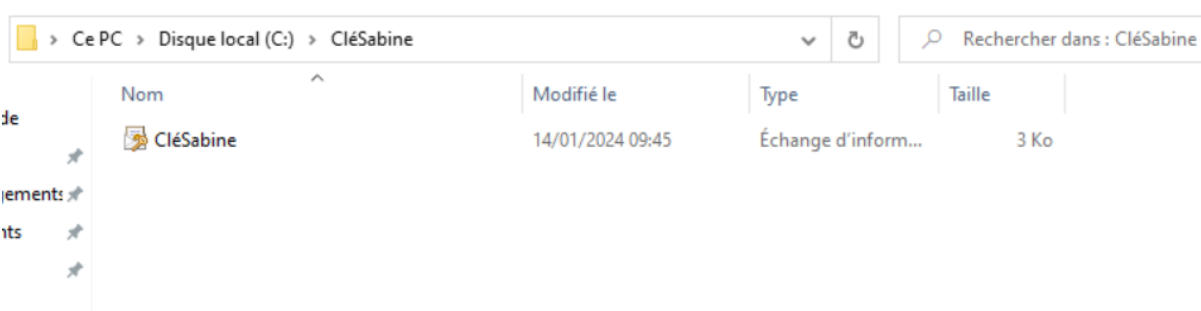
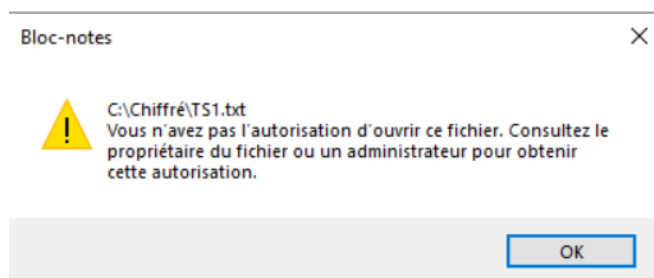
## Configuration et utilisation du système Windows EFS

Lorsque ceci est fait, le système nous informe de la réussite de la procédure, que nous pouvons vérifier en cliquant sur “afficher le journal”, qui ouvre un fichier texte renseignant la réussite ou non de la procédure fichier par fichier.

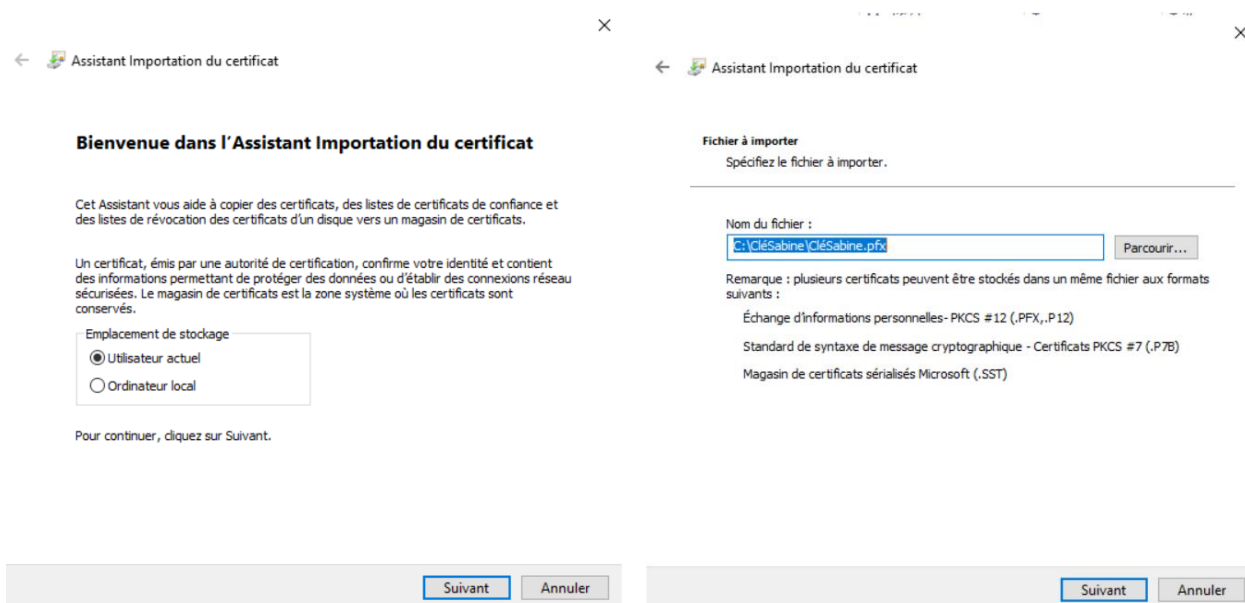


### 2.2.2. Importation d'une clé

La suite de la procédure consiste en l'importation de la clé. Nous nous connectons sur la session de Maxime, puis accédons au fichier de la clé. Double-cliquer dessus.



Cliquer sur “utilisateur actuel”. Cliquer sur suivant. Le fichier à importer est rentré par défaut. Cliquer sur suivant.



## Configuration et utilisation du système Windows EFS

Rentrer le mot de passe précédemment configuré. Cliquer sur suivant. La prochaine fenêtre indique le magasin de certificats concerné. Cliquer sur suivant.

The image shows two side-by-side screenshots of the 'Assistant Importation du certificat' window.

**Left Screenshot: Protection de clé privée**

- Text: "Pour maintenir la sécurité, la clé privée a été protégée avec un mot de passe."
- Text: "Tapez le mot de passe pour la clé privée."
- Form: A password input field with 6 dots and a checkbox labeled "Afficher le mot de passe".
- Section: "Options d'importation :"
- Options:
  - ☐ Activer la protection renforcée de clé privée. Une confirmation vous est demandée à chaque utilisation de la clé privée par une application, si vous activez cette option.
  - ☐ Marquer cette clé comme exportable. Cela vous permettra de sauvegarder et de transporter vos clés ultérieurement.
  - ☐ Protéger la clé privée à l'aide de la sécurité par virtualisation (non exportable)
  - ☒ Induire toutes les propriétés étendues.
- Buttons: "Suivant" and "Annuler".

**Right Screenshot: Magasin de certificats**

- Text: "Les magasins de certificats sont des zones système où les certificats sont conservés."
- Text: "Windows peut sélectionner automatiquement un magasin de certificats, ou vous pouvez spécifier un emplacement pour le certificat."
- Options:
  - ☒ Sélectionner automatiquement le magasin de certificats en fonction du type de certificat
  - ☐ Placer tous les certificats dans le magasin suivant
- Form: "Magasin de certificats : " followed by a text box and a "Parcourir..." button.
- Buttons: "Suivant" and "Annuler".

Le système nous informe de la réussite de la procédure.

The image shows two screenshots related to the completion of the certificate import process.

**Left Screenshot: Fin de l'Assistant Importation du certificat**

- Text: "Le certificat sera importé après avoir cliqué sur Terminer."
- Text: "Vous avez spécifié les paramètres suivants :"
- Table:

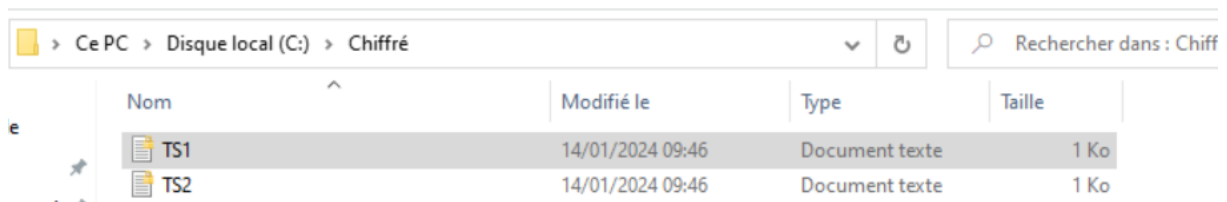
Magasin de certificats sélectionné	Déterminé automatiquement par l'Assistant
Contenu	PFX
Nom du fichier	C:\CléSabine\CléSabine.pfx
- Buttons: "Terminer" and "Annuler".

**Right Screenshot: Confirmation Dialog**

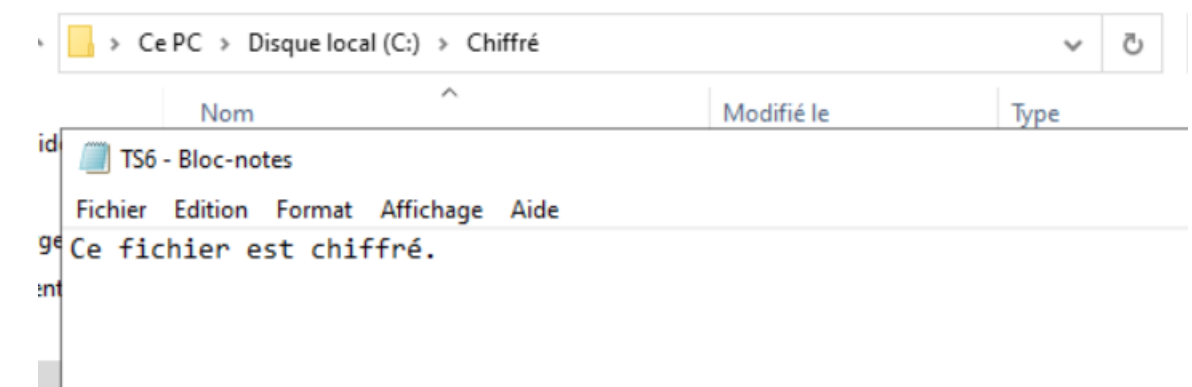
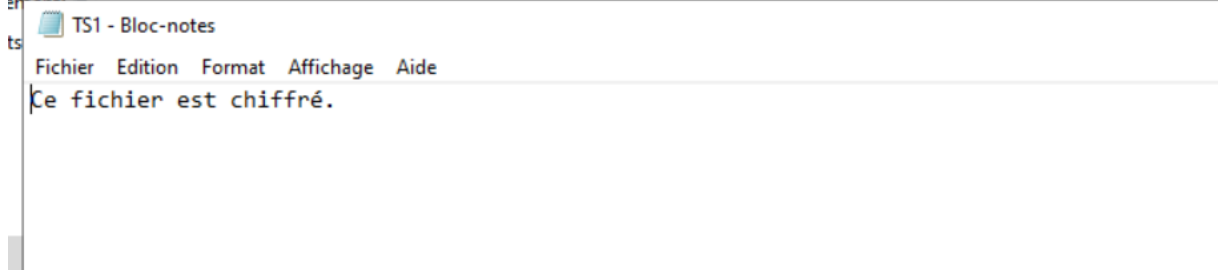
- Title: "Assistant Importation du certificat"
- Icon: Information icon (i)
- Text: "L'importation a réussi."
- Button: "OK"

## Configuration et utilisation du système Windows EFS

Tester la procédure en tentant d'accéder à un fichier chiffré. Celui-ci s'ouvre bien, dans le cas d'un fichier présent depuis avant la procédure (TS1), ou créé après celle-ci (TS6).



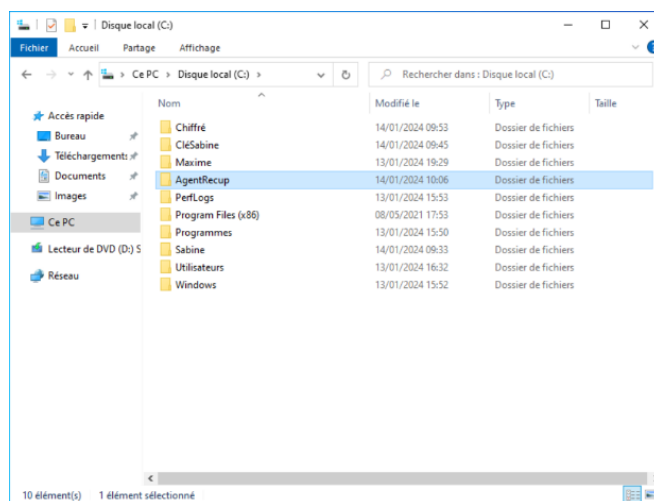
Nom	Modifié le	Type	Taille
TS1	14/01/2024 09:46	Document texte	1 Ko
TS2	14/01/2024 09:46	Document texte	1 Ko



### 2.3. Permettre l'accès à tous les fichiers à tous les utilisateurs : création d'un agent de récupération

#### 2.3.1. Création d'un certificat d'agent de récupération de données

Créer un dossier destiné à contenir la future clé. En l'espèce, ce sera "AgentRecup" dans le volume C:\.



Accéder à la console cmd. Taper la commande "cipher /r:C:\AgentRecup\certificat-agent", qui signifie que le système va créer une clé d'agent dans le dossier AgentRecup. Créer un mot de passe.

```
C:\Windows\system32\cmd.exe
Microsoft Windows [version 10.0.20348.587]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\Henri>cipher /r:C:\AgentRecup\certificat-agent
```

```
C:\Windows\system32\cmd.exe - cipher /r:C:\AgentRecup\certificat-agent
Microsoft Windows [version 10.0.20348.587]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\Henri>cipher /r:C:\AgentRecup\certificat-agent
Entrez le mot de passe protégeant votre fichier .PFX :
```



## Configuration et utilisation du système Windows EFS

Le système nous indique la réussite de la procédure.

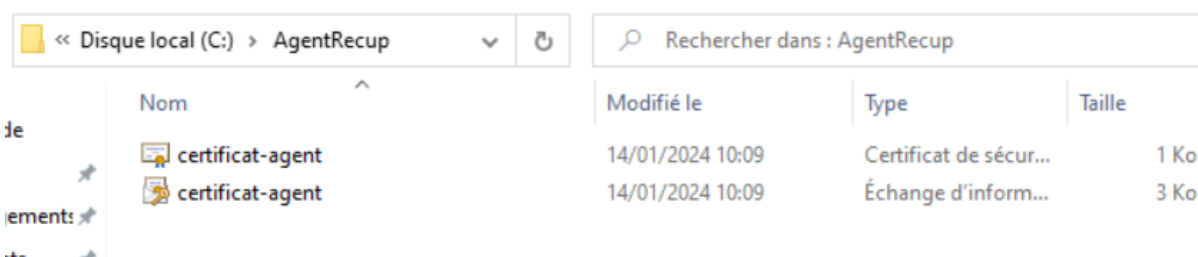
```
C:\Windows\system32\cmd.exe
Microsoft Windows [version 10.0.20348.587]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\Henri>cipher /r:C:\AgentRecup\certificat-agent
Entrez le mot de passe protégeant votre fichier .PFX :
Entrez à nouveau le mot de passe pour confirmation :

Votre fichier .CER a été créé.
Votre fichier .PFX a été créé.

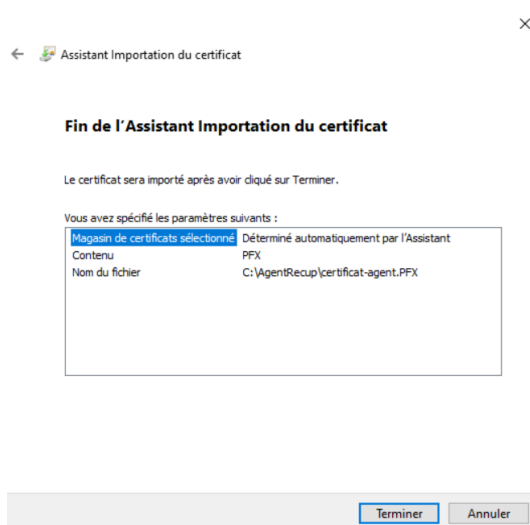
C:\Users\Henri>
```

Accéder au dossier AgentRecup. 2 clés ont été créées.



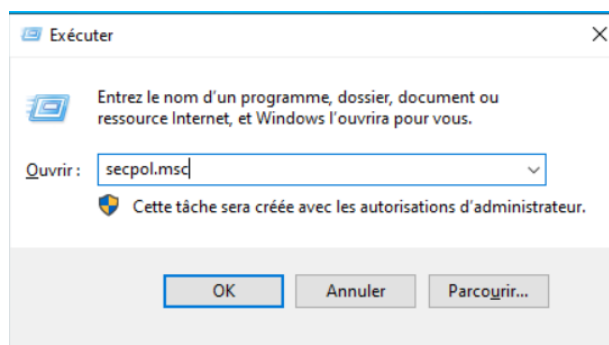
	Nom	Modifié le	Type	Taille
	certificat-agent	14/01/2024 10:09	Certificat de sécur...	1 Ko
	certificat-agent	14/01/2024 10:09	Échange d'inform...	3 Ko

Double-cliquer sur la clé d'échange d'information pour entamer la procédure d'importation. Celle-ci est identique à celles précédentes. La procédure est un succès.

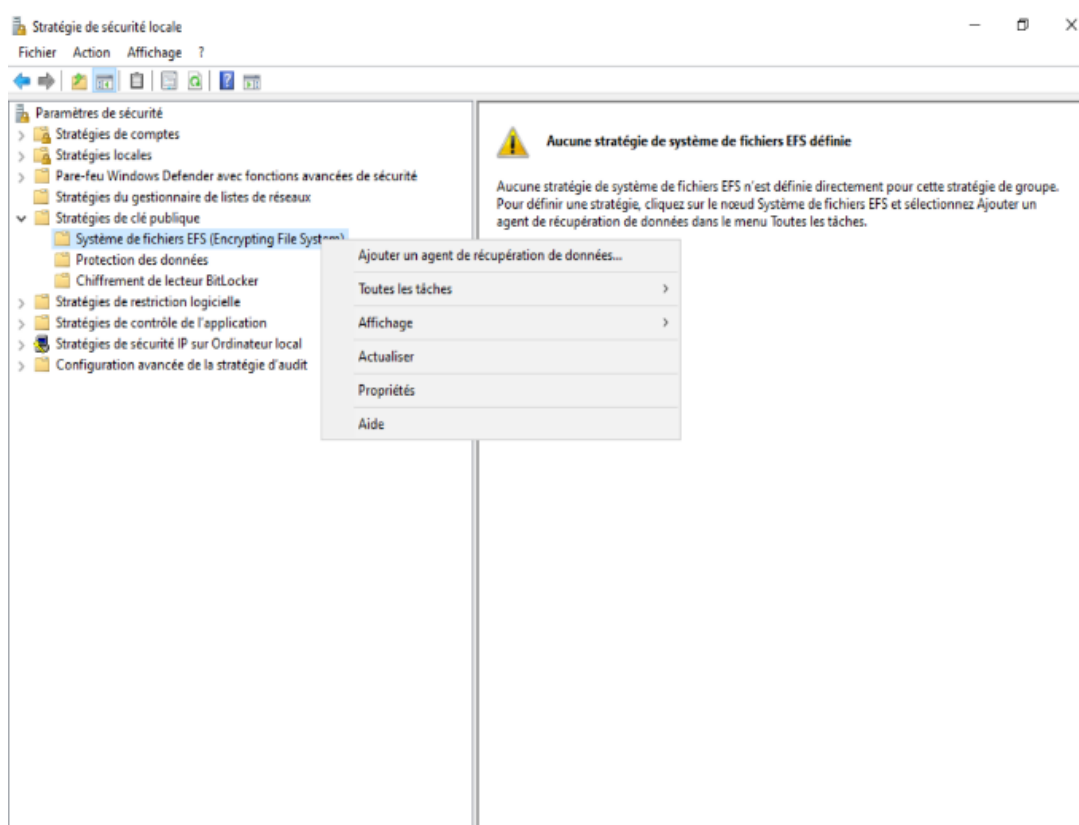


### 2.3.2. Création d'un agent de récupération de données

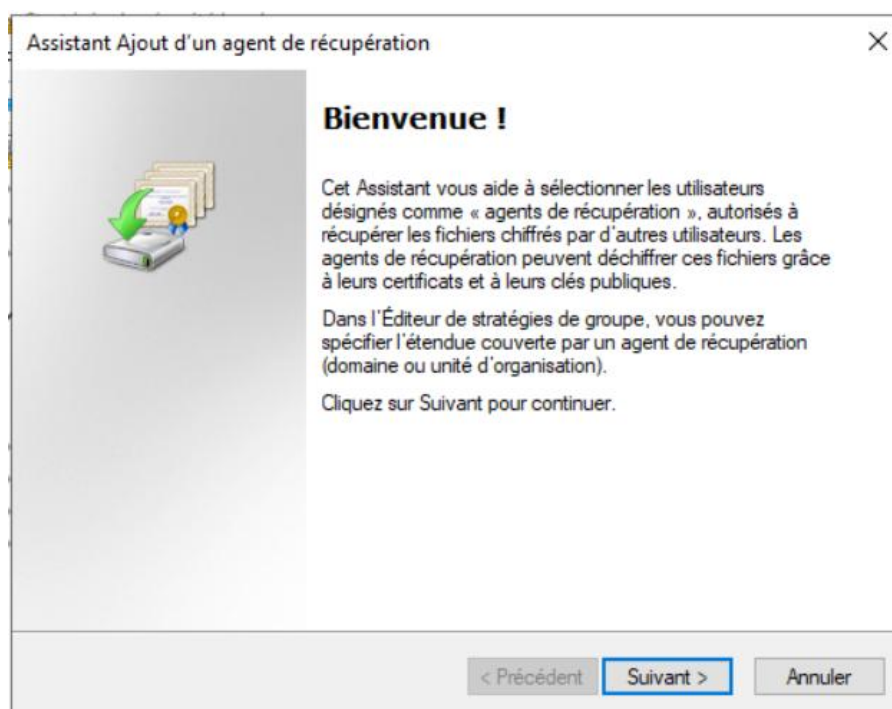
Ouvrir exécuter (windows+r), taper "secpol.msc", cliquer sur ok.



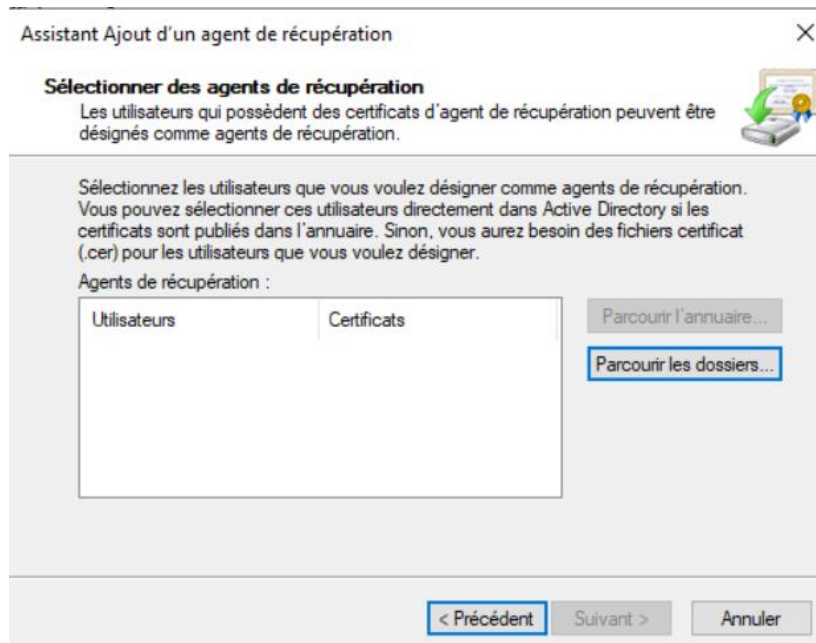
Dérouler successivement Paramètres de sécurité > Stratégies de clé publique > Système de fichiers EFS. Double-cliquer.



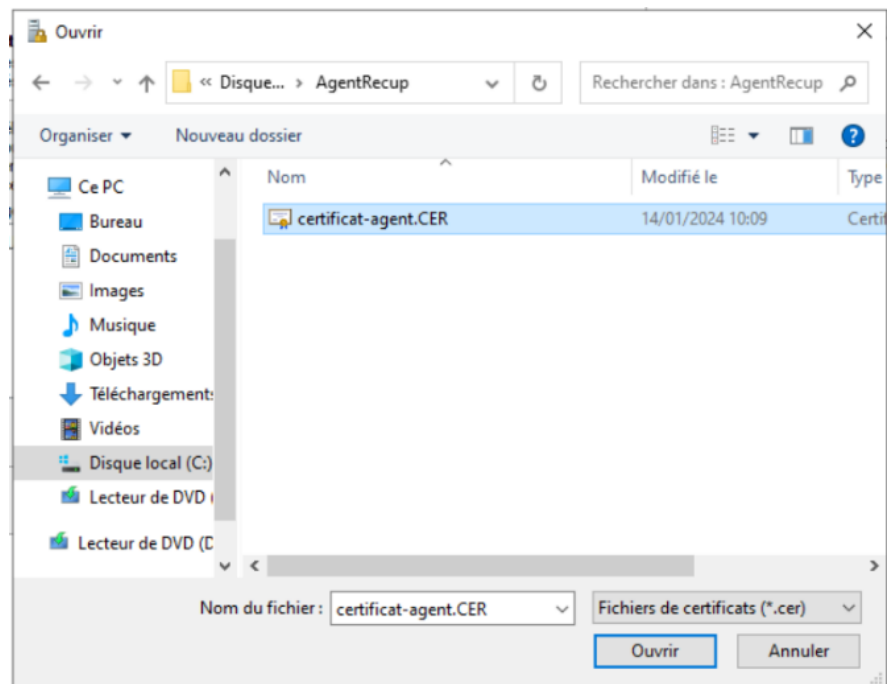
## Configuration et utilisation du système Windows EFS



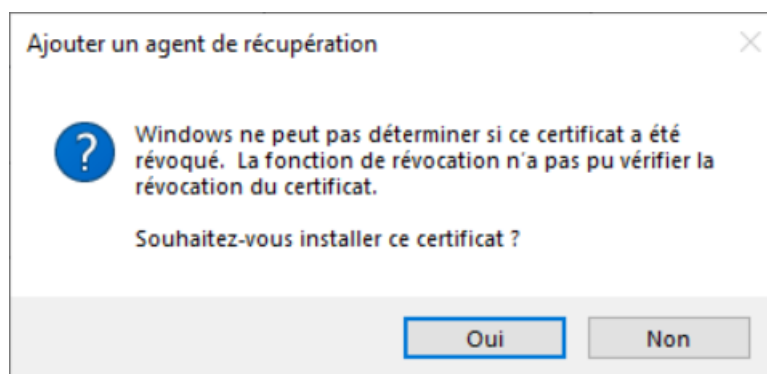
Parcourir les dossiers pour accéder à celui-ci qui contient les clés, AgentRecup. Sélectionner le fichier CER.



## Configuration et utilisation du système Windows EFS



Cliquer sur oui.



## Configuration et utilisation du système Windows EFS

L'utilisateur concerné a été rentré par défaut. Cliquer sur suivant. Cliquer sur Terminer.

Assistant Ajout d'un agent de récupération

**Sélectionner des agents de récupération**

Les utilisateurs qui possèdent des certificats d'agent de récupération peuvent être désignés comme agents de récupération.

Sélectionnez les utilisateurs que vous voulez désigner comme agents de récupération. Vous pouvez sélectionner ces utilisateurs directement dans Active Directory si les certificats sont publiés dans l'annuaire. Sinon, vous aurez besoin des fichiers certificat (.cer) pour les utilisateurs que vous voulez désigner.

Agents de récupération :

Utilisateurs	Certificats
USER_UNKNOWN	Henri

Parcourir l'annuaire...  
Parcourir les dossiers...

< Précédent   **Suivant >**   Annuler

Assistant Ajout d'un agent de récupération

**Dernière étape de l'Assistant Ajout d'un agent de récupération**

L'Assistant Ajout d'un agent de récupération est terminé.

Les utilisateurs suivants ont été désignés comme agents de récupération :

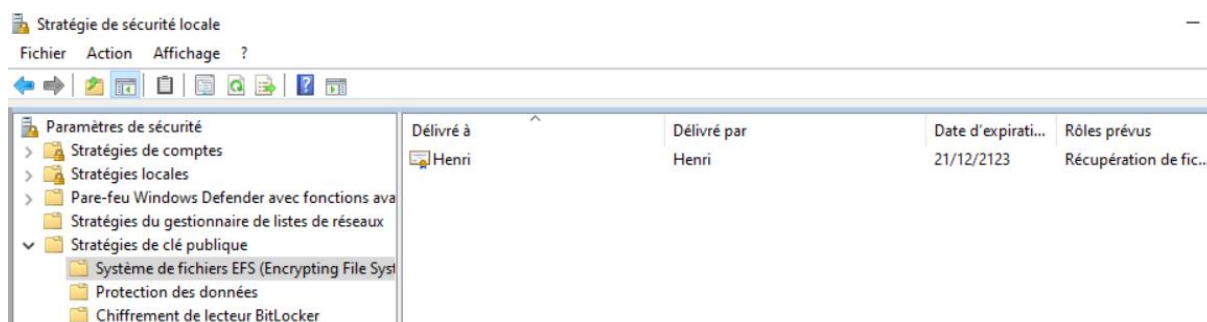
Utilisateurs	Certificats
USER_UNKNOWN	Henri

Pour fermer cet Assistant, cliquez sur Terminer.

< Précédent   **Terminer**   Annuler

## Configuration et utilisation du système Windows EFS

Le certificat de l'agent de récupération a été ajouté à la liste, et délivré à l'utilisateur Henri.



Tester la réussite de la procédure en créant 2 nouveaux fichiers dans le dossier chiffré "Chiffré" à l'aide des utilisateurs Sabine et Maxime. Par la suite, se connecter sur l'utilisateur Henri, et lire les fichiers.

