Atelier : Chiffrement EFS

1. Objectif

Au-delà de l'implémentation du chiffrement EFS sur un ordinateur local, cet atelier vous permettra d'appréhender de façon concrète les fondements de la cryptographie et les concepts associés (chiffrements symétrique et asymétrique, utilisation de clé privées et publiques). Cet atelier met aussi en pratique la gestion des certificats et de leurs formats.

Les ordinateurs virtuels utilisés dans cet atelier sont les suivants :

W10 : ordinateur en groupe de travail (Workgroup).

2. Préparation de l'atelier

En préparation de notre atelier, nous allons restaurer l'ordinateur client en mode Groupe de travail, puis nous créerons les utilisateurs et le dossier de test.

a. Restauration de l'ordinateur w10 en Workgroup

Restaurer le point de contrôle **Base** afin de disposer d'un poste Windows 10 en Workgroup

Dans le gestionnaire Hyper-V, sélectionnez l'ordinateur virtuel **w10**.

Dans la zone centrale **Points de contrôle**, faites un clic droit sur le point de contrôle **Base** et sélectionnez le menu **Appliquer**.

Si une boîte de dialogue de confirmation s'affiche, cochez à nouveau sur le bouton **Appliquer**.

Suivez la progression de restauration de l'ordinateur virtuel (colonne **statut**).

Après restauration complète, redémarrez le client.

Ouvrir une session avec l'administrateur local adminw10

Appuyez simultanément sur les touches [Ctrl] [Alt] et [Fin], sélectionnez l'utilisateur **adminw10**, saisissez son mot de passe (**pw**) et validez.

Créer trois utilisateurs u1, u2 et u3 (pas de mots de passe)

Faites un clic droit sur l'icône Windows et sélectionnez le menu **Gestion de l'ordinateur**.

Développez Gestion de l'ordinateur (local)\Outils système\Utilisateurs\groupes locaux, faites un clic droit sur le dossier **Utilisateurs** et sélectionnez le menu **Nouvel utilisateur**.

Dans la fenêtre **Nouvel utilisateur**, dans la zone **Nom d'utilisateur** saisissez **u1**.

Dans les zones **Mot de passe** et **Confirmer le mot de passe** saisissez **pw**.

Décochez la case **l'utilisateur doit changer le mot de passe à la prochaine ouverture de session**.

Cliquez sur le bouton **Créer**.

Répétez cette opération pour créer deux utilisateurs supplémentaires, u2 et u3.

Cliquez sur le bouton **Fermer**.

Fermez la console de gestion Gestion de l'ordinateur.

Créer un nouveau dossier (c: \EfsTests)

Cliquez sur l'icône **Explorateurs de fichiers** de la barre de tâches.

Faites un clic droit sur **Disque local (C:)** et sélectionnez les menus **Nouveau\Dossier** puis modifiez le nom du nouveau dossier en **EfsTests**.

Modifier les autorisations NTFS du dossier EfsTests

Afin d'être certains que les refus d'accès aux fichiers seront liés à des protections de chiffrement EFS et non à des manques d'autorisations, nous allons accorder l'autorisation NTFS Contrôle Total à tous les utilisateurs de test sur le dossier de test.

Faites un clic droit sur le dossier EfsTests et sélectionnez le menu **Propriétés**.

Sélectionnez l'onglet **Sécurité**, cliquez sur le bouton **Modifier**, cliquez sur le bouton **Ajouter**, saisissez **Tout le monde** cliquez sur le bouton **Vérifier les noms** puis cliquez sur le bouton **OK**.

Cochez la case **Contrôle total** pour le groupe **Tout le monde**.

Cliquez sur le bouton **OK** sur le bouton **Fermer**.

Créer une console MMC (Microsoft Management Console) personnalisée pour visualiser les certificats de l'administrateur local AdminW10

Nous allons créer une console MMC personnalisée qui nous permettra de visualiser les certificats de l'utilisateur AdminW10.

Faites un clic droit sur l'icône Windows et sélectionnez le menu **Exécuter**, saisissez **mmc** puis cliquez sur le bouton **OK**.

Dans la console Contrôle de compte d'utilisateur, cliquez sur le bouton **Oui** pour autoriser l'exécution de la console.

Sélectionnez le menu **Fichier\Ajouter\Supprimer un composant logiciel enfichable**.

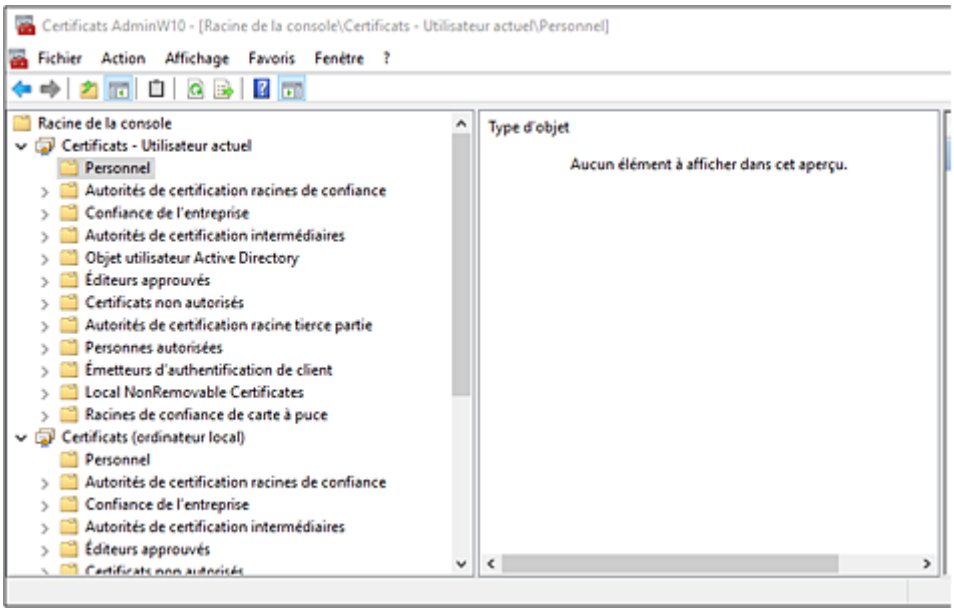
Dans la fenêtre Ajouter ou supprimer des composants logiciels enfichables, dans la zone **Composants logiciels enfichables disponibles** sélectionnez **Certificats**, cliquez sur le bouton **Ajouter**, sélectionnez **Mon compte d'utilisateur** et cliquez sur le bouton **Terminer**.

Sélectionnez à nouveau le composant enfichable **Certificats**, cliquez sur le bouton **Ajouter**, sélectionnez **Un compte d'ordinateur** puis cliquez sur les boutons **Suivant**, **Terminer** et **OK**.

Développez **Certificats\Utilisateur actuel\Personnel**.

Ce dossier contient les certificats personnels de l'utilisateur AdminW10. Il est actuellement vide.

Fermez et enregistrez cette console MMC personnalisée sur le bureau sous le nom Certificats AdminW10.



Les administrateurs locaux peuvent visualiser leurs certificats personnels mais également ceux de l'ordinateur local !

Fermer la session de l'utilisateur adminw10

Appuyez simultanément sur les touches [Ctrl][Alt] et [Fin] et sélectionnez le menu **Se déconnecter**.

Créez un fichier et une console MMC personnalisée pour l'utilisateur local u1.

Connectez-vous avec l'utilisateur local u1.

Créez un nouveau document texte nommé u1 dans le dossier C: \EfsTests.

Ouvrez le fichier u1, ajoutez-lui un contenu et enregistrez-le.

Créer une console MMC (Microsoft Management Console) personnalisée pour visualiser les certificats de l'administrateur local u1

Faites un clic droit sur l'icône Windows et sélectionnez le menu **Exécuter**, saisissez **mmc** puis cliquez sur le bouton **OK**.

Dans la console Contrôle de compte d'utilisateur, cliquez sur le bouton **Oui** pour autoriser l'exécution de la console.

Sélectionnez le menu **Fichier\Ajouter\Supprimer un composant logiciel enfichable**.

Dans la fenêtre Ajouter ou supprimer des composants logiciels enfichables, dans la zone Composants logiciels enfichables disponibles sélectionnez **Certificats**, cliquez sur le bouton **Ajouter** et cliquez sur le bouton **OK**.

> Un utilisateur non administrateur ne peut pas ajouter le composant enfichable Certificats pour le compte de l'ordinateur.

Développez **Certificats\Utilisateur actuel\Personnel**.

> Ce dossier contient les certificats personnels de l'utilisateur u1. Il est actuellement vide.

Fermez et enregistrez cette console MMC personnalisée sur le bureau sous le nom Certificats u1.

Fermez la session de l'utilisateur local u1.

Répétez les opérations ci-dessus pour créer un fichier personnel et une console MMC personnalisée pour les utilisateurs locaux u2 et u3.

Chiffrer le fichier de l'utilisateur u1

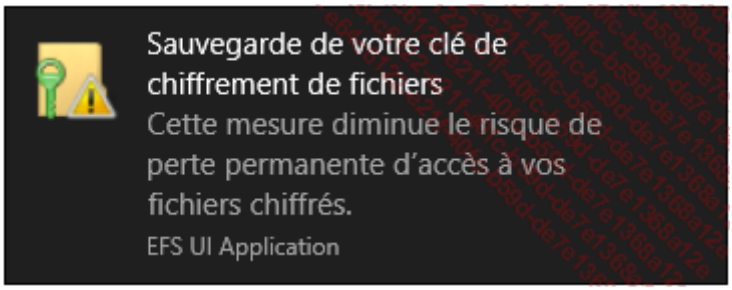
Nous allons maintenant procéder au chiffrement du fichier de l'utilisateur u1.

Faites un clic droit sur le fichier u1 et sélectionnez le menu **Propriétés** puis cliquez sur le bouton **Avancé**.

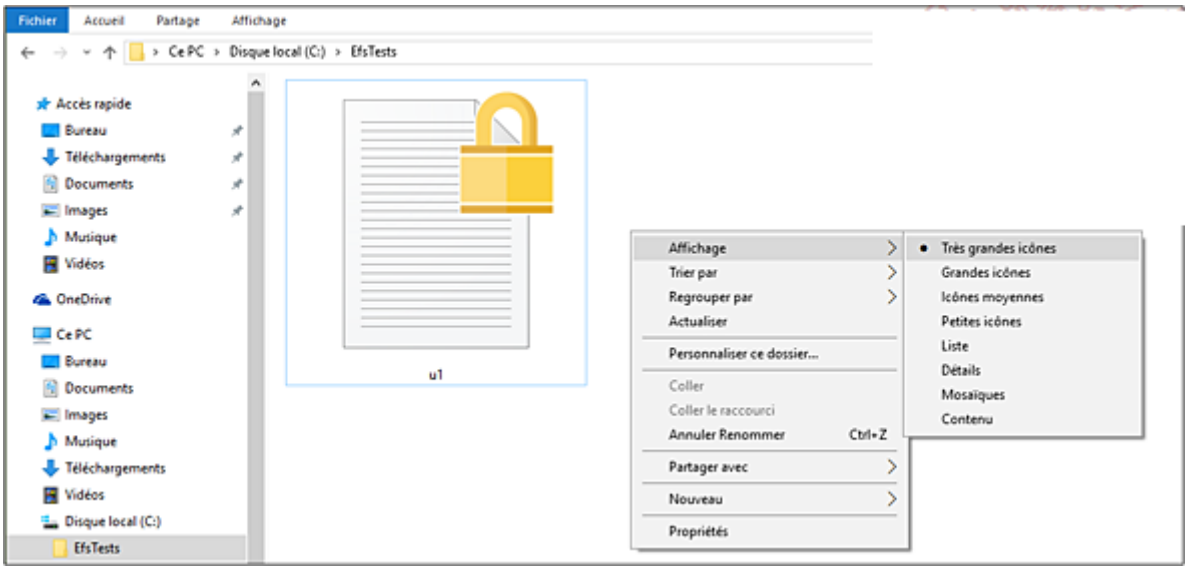
Cochez **Chiffrer le contenu pour sécuriser les données** puis cliquez sur le bouton **OK** et à nouveau sur le bouton **OK**.

Dans la boîte de dialogue Avertissement de chiffrement, cochez **Chiffrer le fichier uniquement** puis cochez **Toujours chiffrer les fichiers uniquement**.

Cliquez sur le bouton **OK** et à nouveau sur le bouton **OK**.



Un message apparaît vous invitant à sauvegarder votre certificat. Ignorez ce message pour le moment, nous reviendrons sur la sauvegarde des certificats plus tard dans cet atelier.



Le fichier de l'utilisateur est maintenant chiffré. L'activation du chiffrement est indiquée par l'ajout d'une icône représentant un cadenas fermé dans le coin supérieur droit du fichier (l'icône est plus visible en mode Affichage\Très grande icônes).

Dans les versions précédentes de Windows, les fichiers chiffrés sont affichés en couleur verte, le symbole cadenas est une nouveauté Windows 10.

Création d’un certificat autosigné

Nous allons vérifier qu’après chiffrement du fichier, le système EFS a généré automatiquement un certificat autosigné pour l’utilisateur.

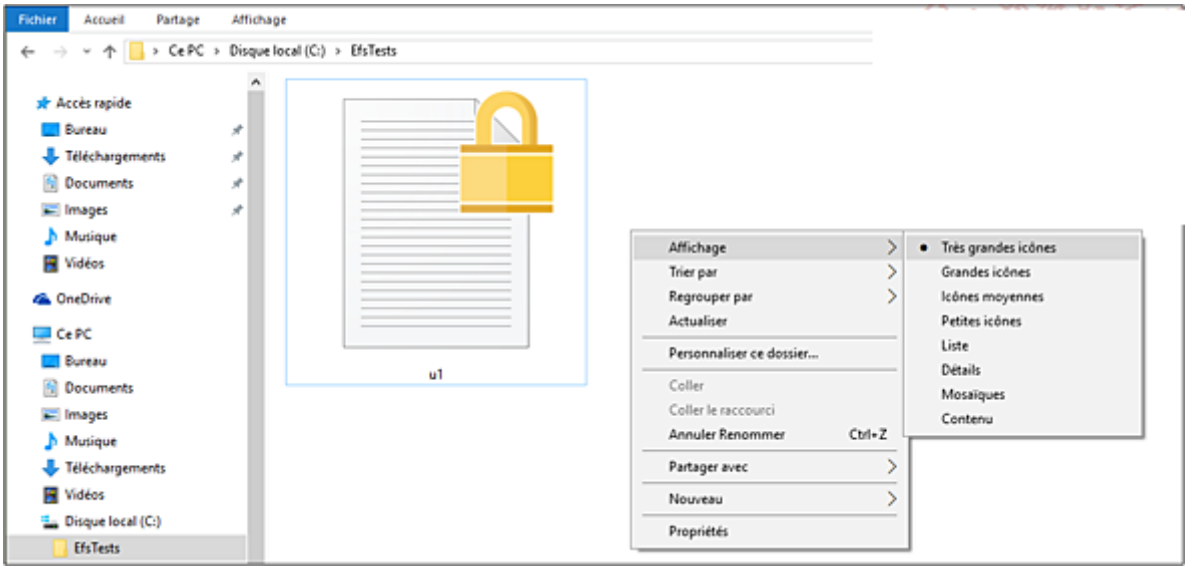
Ouvrez la console MMC personnalisée Certificats u1.

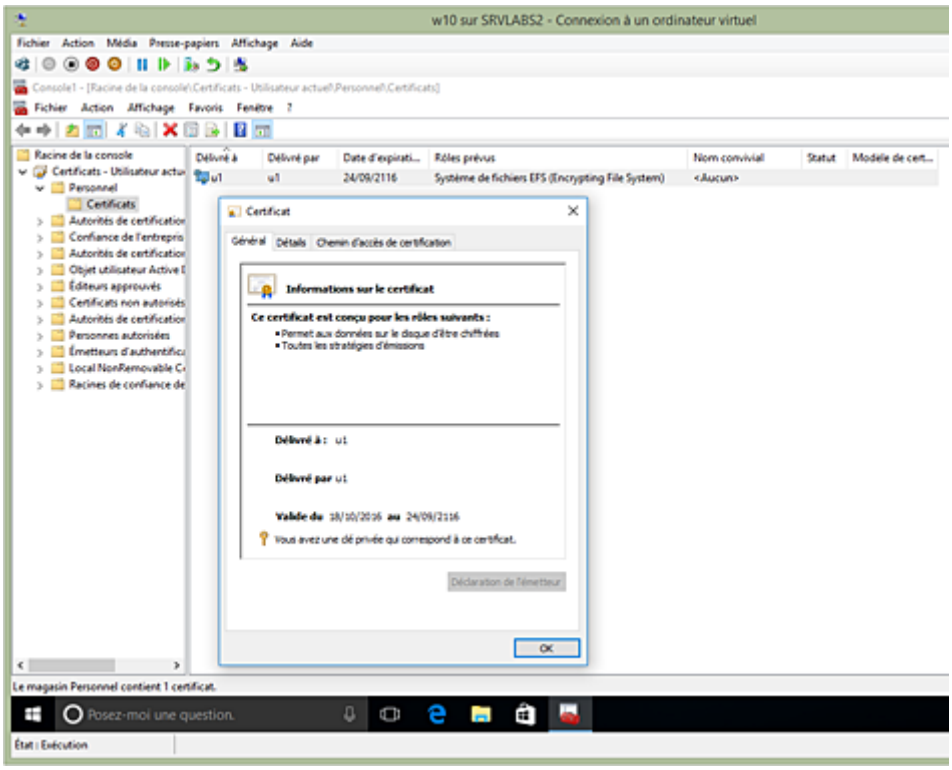
Développez **Certificats\Utilisateur actuel\Personnel**.

Un nouveau certificat apparaît maintenant dans le dossier personnel de l’utilisateur u1 !

Double cliquez sur le certificat pour afficher ses propriétés.

Sélectionnez l’onglet **Général** et validez la durée de vie du certificat, à qui et par qui il a été délivré, ainsi que le lien avec une clé privée.

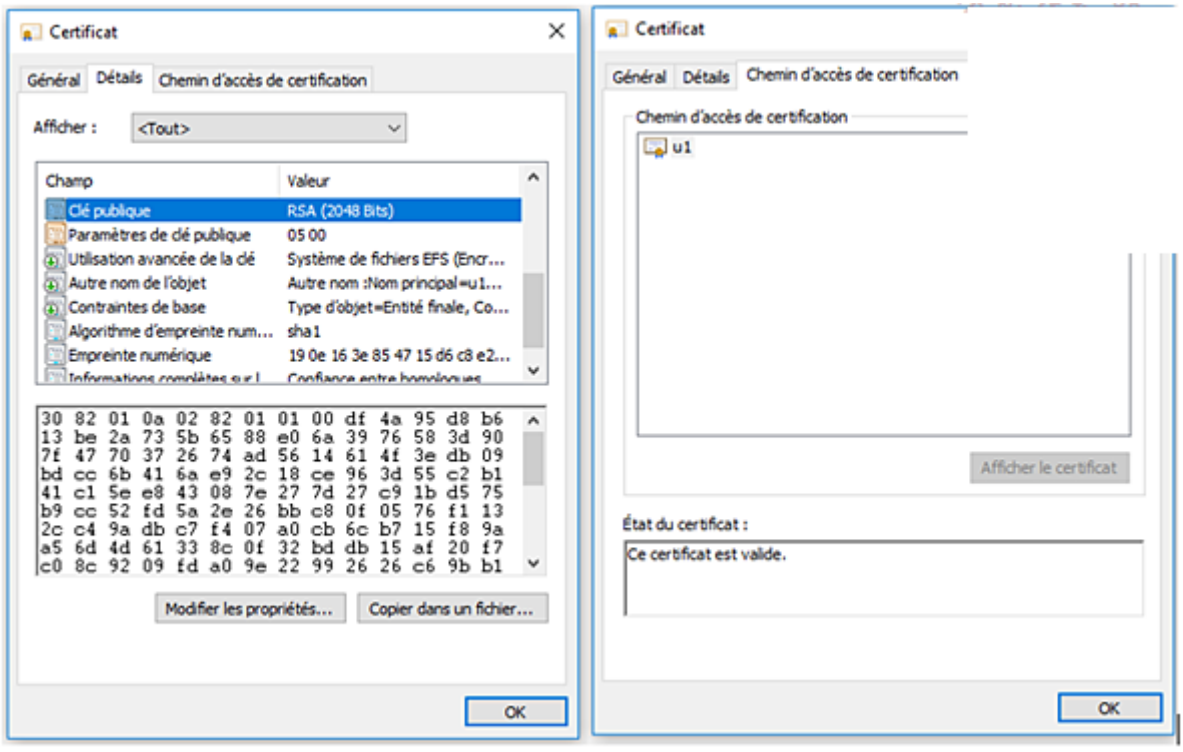




Les propriétés du certificat affichent des informations en clair. Ici, le délivrement du certificat à u1 par u1 (certificat autosigné), les dates de validité (100 ans) et la liaison de ce certificat avec une clé privée.

Sélectionnez l'onglet **Détails** puis le champ **Clé publique**, la clé publique associée au certificat est affichée.

Sélectionnez l'onglet **Chemin d'accès de certification**, il n'y a pas de mention d'autorité de certification. Seul apparaît le nom de l'utilisateur (c'est un certificat autosigné).



*Les onglets **Détails** et **Chemin d'accès de certification** affichent aussi d'autres informations pertinentes comme la clé publique associée au certificat de l'utilisateur.*

Validez la possibilité de lire et de modifier le fichier u1.

Fermez la session de l'utilisateur local u1 et connectez-vous avec l'utilisateur local u2.

Essayez de lire le fichier chiffré u1.txt de l'utilisateur u1.

L'application Bloc-notes s'ouvre mais un message d'erreur "Accès refusé" s'affiche. L'utilisateur u2 ne dispose pas de la clé privée de u1 et ne peut donc pas déchiffrer la clé de chiffrement symétrique qui est dans l'en-tête du fichier.

Fermez la session de l'utilisateur local u2 et connectez-vous avec l'utilisateur local Adminw10.

Essayez de lire le fichier chiffré u1.txt de l'utilisateur u1.

L'application Bloc-notes s'ouvre mais un message d'erreur "Accès refusé" s'affiche. L'administrateur adminw10 ne dispose pas de la clé privée de u1 et ne peut donc pas déchiffrer la clé de chiffrement symétrique qui est dans l'en-tête du fichier.

Disposer d'un compte administrateur ne donne pas accès aux fichiers chiffrés des utilisateurs !

b. Partage de fichiers chiffrés

Objectif : l'utilisateur local u1 souhaite partager son fichier chiffré avec les utilisateurs locaux u2 et u3.

Chiffrer le fichier de l'utilisateur u2

L'utilisateur de va procéder au chiffrement de son fichier.

Connectez-vous avec l'utilisateur local u2.

Faites un clic droit sur le fichier de u2 et sélectionnez le menu **Propriétés** puis cliquez sur le bouton **Avancé**.

Cochez **Chiffrer le contenu pour sécuriser les données** puis cliquez sur le bouton **OK** et à nouveau sur le bouton **OK**.

Dans la boîte de dialogue Avertissement de chiffrement, cochez **Chiffrer le fichier uniquement** puis cochez **Toujours chiffrer les fichiers uniquement**.

Cliquez sur le bouton **OK** et à nouveau sur le bouton **OK**.

Un message apparaît vous invitant à sauvegarder votre certificat. Ignorer ce message pour le moment, nous reviendrons sur la sauvegarde des certificats plus tard dans cet atelier.

Le fichier de l'utilisateur est maintenant chiffré. Une icône représentant un cadenas fermé apparaît dans le coin supérieur droit du fichier.

Création d'un certificat autosigné

Vérifions que le système EFS a bien délivré un certificat autosigné pour l'utilisateur u2.

Ouvrez la console **MMC personnalisée Certificats u2**.

Développez **Certificats\Utilisateur actuel\Personnel\Certificats**.

Un nouveau certificat apparaît maintenant dans le dossier personnel de l'utilisateur u2 !

Double cliquez sur le certificat pour afficher ses propriétés.

Sélectionnez l'onglet **Général** et validez la durée de vie du certificat, à qui et par qui il a été délivré, ainsi que le lien avec une clé privée.

Sélectionnez l'onglet **Détails** puis le champ **Clé publique**, la clé publique associée au certificat est affichée.

Sélectionnez l'onglet **Chemin d'accès de certification**, il n'y a pas de mention d'autorité de certification. Seul apparaît le nom de l'utilisateur (c'est un certificat autosigné).

Les propriétés du certificat indiquent qu'il délivré à l'utilisateur u2, autosigné, avec une validité de 100 ans, dispose d'une clé publique et est lié à une clé privée.

Validez la possibilité de lire et de modifier le fichier de u2.

Partage du fichier chiffré de u1 avec u2

Connecté avec l'utilisateur u1, essayons de partager son fichier chiffré avec les utilisateurs u2 et u3.

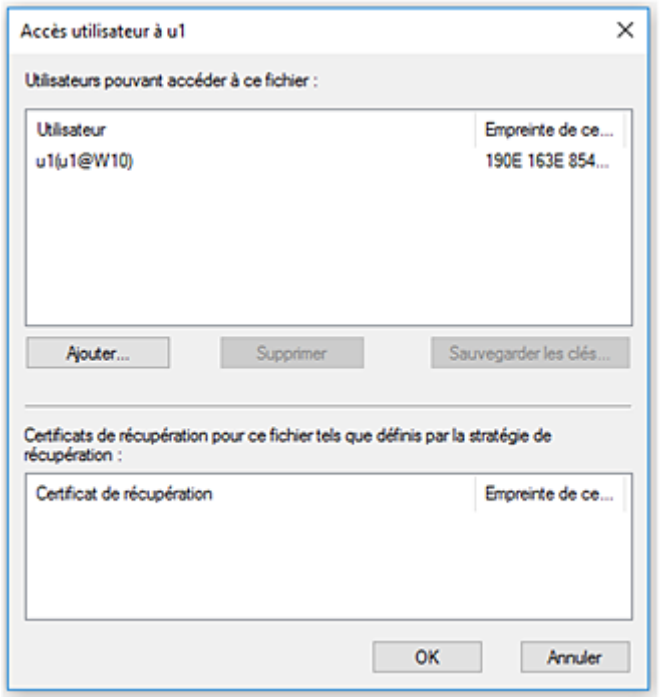
Connectez-vous avec l'utilisateur local u1.

Faites un clic droit sur le fichier u1 et sélectionnez le menu **Propriétés** puis cliquez sur le bouton **Avancé** puis cliquez sur le bouton **Détails**.

Dans la boîte de dialogue Accès utilisateur à u1, cliquez sur **Ajouter** puis cliquez sur le lien **Autre choix**.

Sélectionnez le certificat de l'utilisateur u2 et cliquez sur le bouton **OK**.

Cliquez trois fois sur les boutons **OK** pour valider toutes les boîtes de dialogue.



L'utilisateur u3 n'ayant pas encore chiffré de fichier ne dispose encore d'un certificat EFS. Sans ce certificat, le système ne dispose pas d'une clé publique associée à l'utilisateur u3 qui lui permettrait de chiffrer son en-tête symétrique du chiffrement (voir la section Partage de fichiers EFS dans ce même chapitre).

Connectez-vous avec l'utilisateur local u2.

Validez la possibilité de lire le fichier partagé de l'utilisateur u1.

Le système utilise la clé privée de l'utilisateur u2 pour déchiffrer la clé symétrique contenue dans son en-tête, puis utilise cette clé symétrique pour déchiffrer le document.

Partage du fichier chiffré de u1 avec u3

Nous allons maintenant chiffrer un fichier avec l'utilisateur u3, de façon à ce qu'il dispose également d'un certificat EFS autosigné. Nous pourrons alors partager le fichier chiffré de l'utilisateur u1 avec u3.

Reprenez les manipulations décrites dans cet atelier pour :

- Vous connecter avec l'utilisateur local u3 puis chiffrer son fichier (celui crée par u3).
- Partager le fichier chiffré de l'utilisateur local u1 avec l'utilisateur local u3.
- Valider l'accès au fichier partagé par l'utilisateur local u3.

3. Sauvegarde de certificats

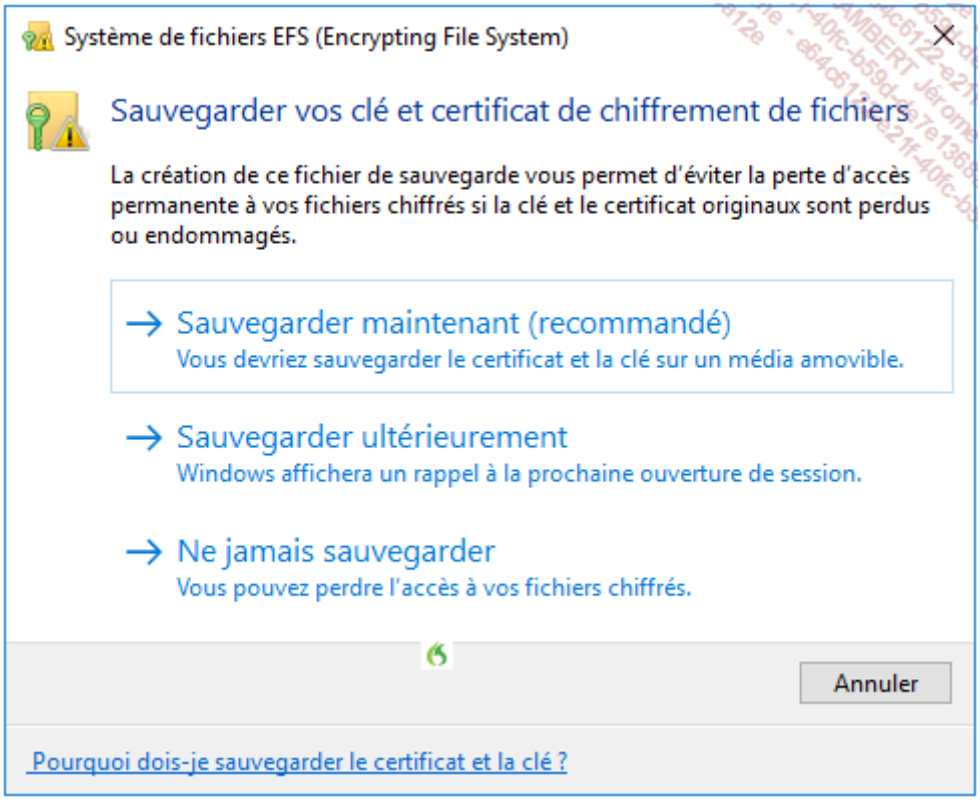
Objectif : sauvegarder et restaurer les certificats d'un utilisateur. Comprendre les différents formats de fichiers de certificats.

Connectez-vous avec l'utilisateur local u1.

Cliquez sur l'icône ˆ (icône **Afficher les icônes cachées** à gauche de la zone de notification dans la barre de tâches) puis cliquez sur l'icône **Système de fichiers chiffrés - Sauvegardez votre clé de chiffrement des fichiers**.

Cette icône n'est plus disponible au bout d'un certain nombre de connexions. Dans ce cas, sautez cette étape et reprenez à l'étape suivante Sauvegarde par la console MMC personnalisée.

Dans la boîte de dialogue Système de fichiers EFS (Encrypting File System), cliquez sur le menu **Sauvegarder maintenant (recommandé)**.



Le menu de sauvegarde permet une sauvegarde immédiate des clés et certificats associés.

Dans la boîte de dialogue Assistant exportation du certificat, cliquez sur le bouton **Suivant**.

Le seul format de fichier proposé ici est le format .pfx. Ce format de fichier inclut le certificat (qui inclut lui-même la clé publique) ainsi que la clé privée associée.

Cliquez sur le bouton **Annuler** pour quitter l'assistant.

Nous allons relancer une sauvegarde des certificats mais avec une version de l'assistant plus complète.

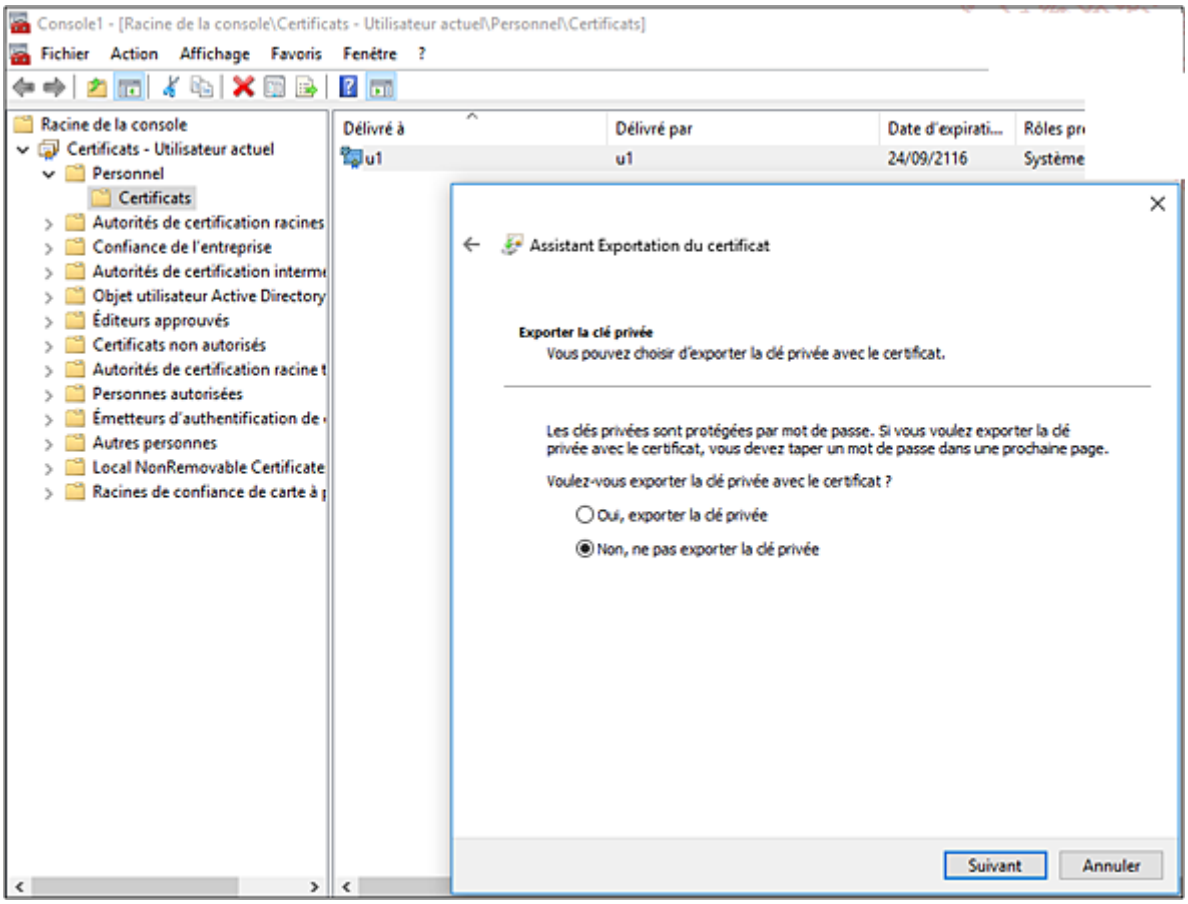
Sauvegarde par la console MMC personnalisée

Ouvrez la console MMC personnalisée Certificats u1 créée sur le bureau de l'utilisateur.

Développez **Certificats\Utilisateur actuel\Personnel\Certificats**.

Faites un clic droit sur le certificat, sélectionnez le menu **Toutes les tâches** puis le menu **Exporter**.

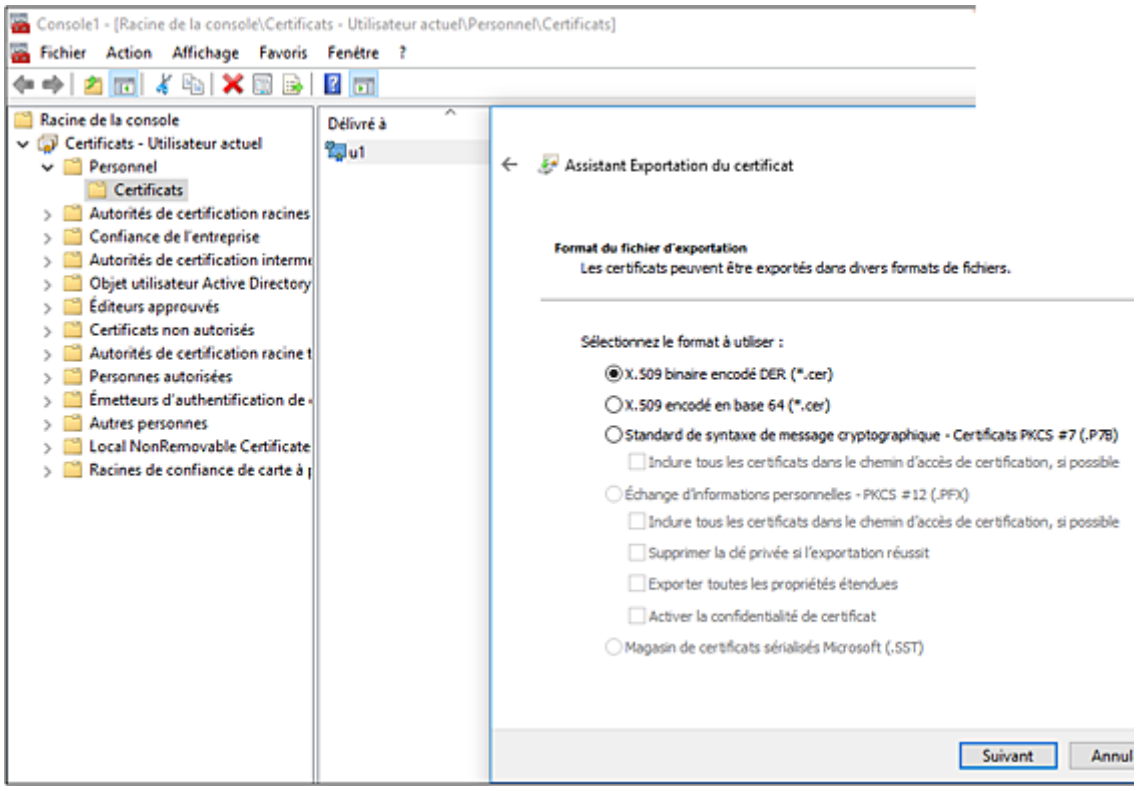
La boîte de dialogue Assistant exportation du certificat s'ouvre, cliquez sur le bouton **Suivant**.



Lancer la sauvegarde depuis la console MMC personnalisée offre plus de choix que par l'assistant de sauvegarde de la barre de tâches.

Sélectionnez **Non, ne pas exporter la clé privée** puis cliquez sur le bouton **Suivant**.

Les trois formats proposés ici ne sauvegarderont que le certificat et sa clé publique (sans la clé privée associée).

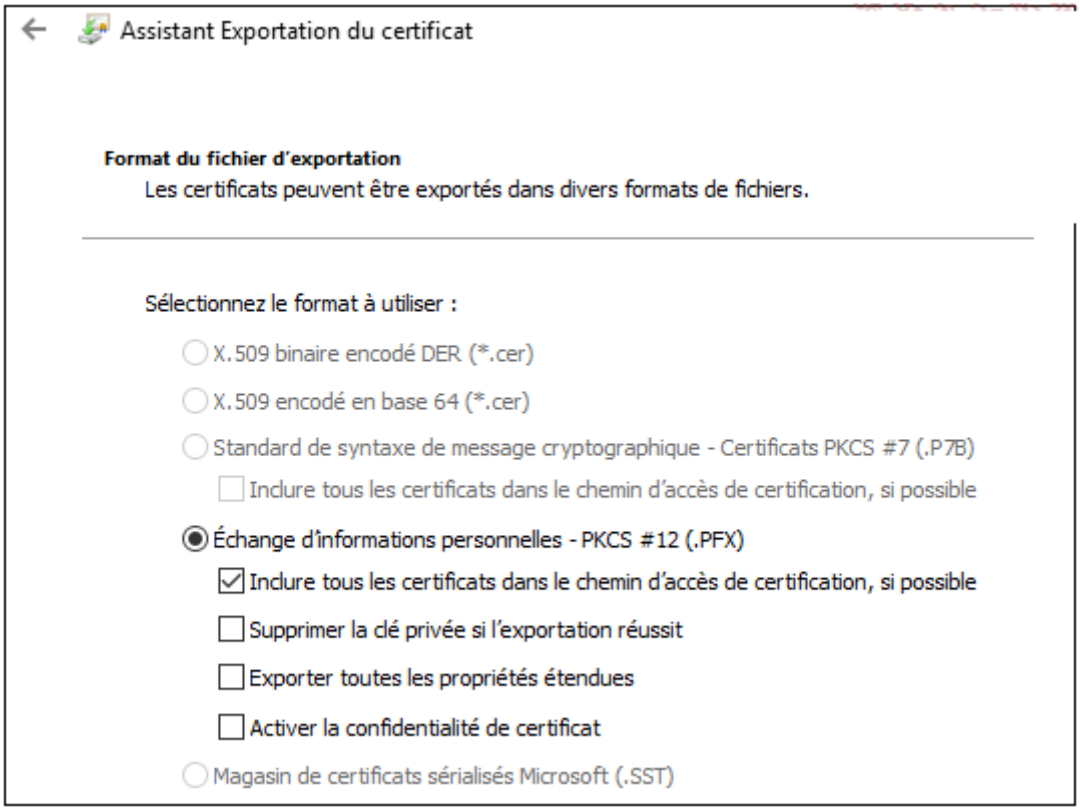


Les formats en encodage DER ou base 64 (.cer) n'incluent que le certificat et sa clé publique. Le format PKCS #7 (.P7B) peut inclure également les certificats du chemin d'accès de certification (les certificats des autorités de certification qui ont délivré ce certificat).

Cliquez sur **Annuler** pour annuler l'assistant et exécutez-le à nouveau.

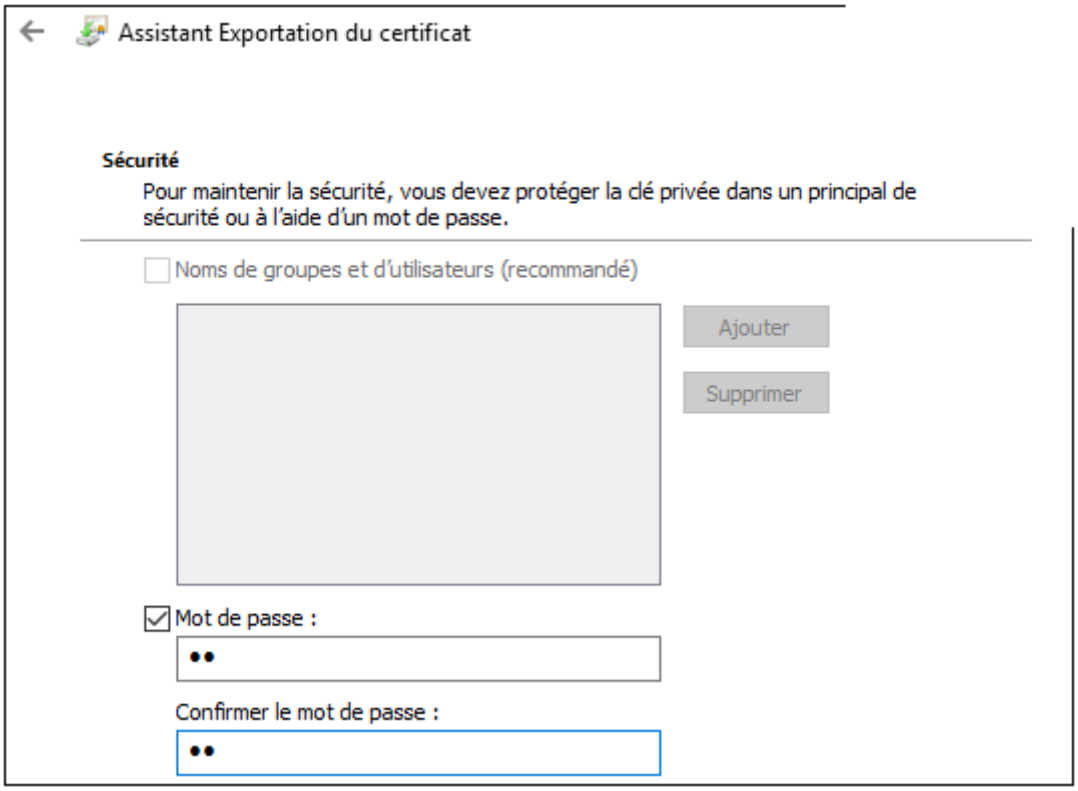
La boîte de dialogue Assistant exportation du certificat s'ouvre, cliquez sur le bouton **Suivant**.

Sélectionnez **Oui, exporter la clé privée** puis cliquez sur le bouton **Suivant**.



Le format proposé ici PKCS #12 (.PFX) permet une sauvegarde aussi bien du certificat (avec sa clé publique intégrée) que de la clé privée associée. On peut également choisir d'inclure les certificats du chemin de certification (les certificats des autorités de certification qui ont délivré ce certificat), demander la suppression de la clé privée après exportation, exporter toutes les propriétés étendues du certificat ou activer la confidentialité du certificat.

Cochez la case **Mot de passe** et saisissez deux fois un mot de passe personnalisé dans les zones **Mot de passe** et **Confirmer le mot de passe** puis cliquez sur le bouton **Suivant**.



Il est également possible de protéger un fichier de sauvegarde de certificat en cochant l'option **Noms de groupes et d'utilisateurs (recommandé)** pour n'autoriser la restauration qu'au(x) groupe(s) ou utilisateur(s) indiqué(s). Cette option requiert cependant une intégration de l'ordinateur à un domaine Active Directory.

Cliquez sur le bouton **Parcourir**, sélectionnez l'emplacement **Bureau**, saisissez **CertificatEfsU1** dans la zone **Nom de fichier**, cliquez sur le bouton **Enregistrer** puis sur le bouton **Suivant** et sur le bouton **Terminer**.

Un message indique que l'exportation a réussi.

Supprimer le certificat EFS

Cliquez sur le bouton **OK** pour fermer le message.

Faites un clic droit sur le certificat et sélectionnez le menu **Supprimer**.

Cliquez sur le bouton **Oui** sur le message indiquant "vous ne pourrez plus lire les données chiffrées à l'aide de ce certificat. Voulez-vous supprimer ce certificat ?".

Le certificat est supprimé.

Fermez la console MMC personnalisée Certificats u1.

Validez que vous ne pouvez plus lire votre fichier chiffré.

Si vous pouvez toujours le lire, redémarrez physiquement l'ordinateur et validez l'impossibilité de lire le fichier chiffré.

Restaurer un certificat

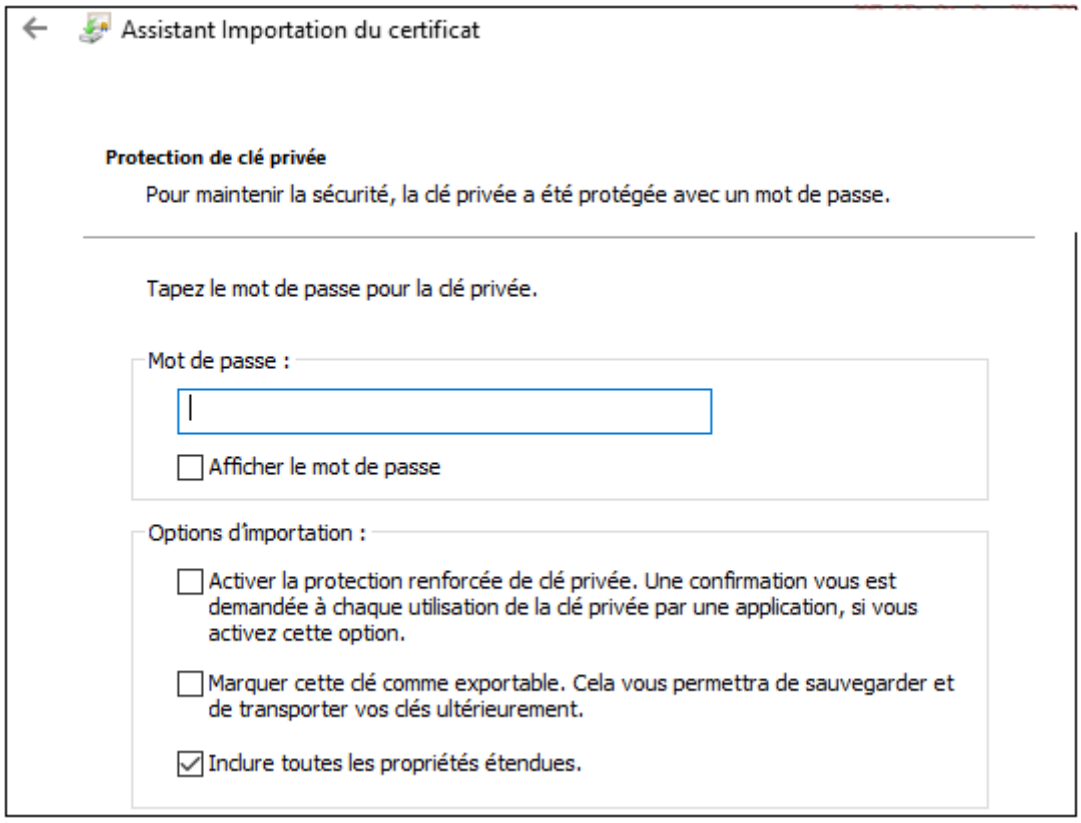
Double cliquez sur le fichier (.PFX) sauvegardé sur le bureau.

La boîte de dialogue Assistant importation du certificat, sélectionnez **Utilisateur local** puis cliquez sur le bouton **Suivant**.

Dans la zone **Nom du fichier**, validez le chemin d'accès au fichier .pfx puis cliquez sur le bouton **Suivant**.

Dans la zone **Mot de passe**, saisissez le mot de passe utilisé lors de la sauvegarde du certificat.

Cochez les options **Marquer cette clé comme exportable** et **Inclure toutes les propriétés étendues** puis cliquez sur le bouton **Suivant**.



N'oubliez pas de cocher **Marquer cette clé comme exportable**. Cela vous permettra de sauvegarder et de transporter vos clés ultérieurement sinon le certificat importé ne pourrait plus être à nouveau exporté avec sa clé privée !

Dans la boîte de dialogue Magasin de certificats, sélectionnez **Sélectionnez automatiquement le magasin de certificats en fonction du type de certificat**, puis cliquez sur le bouton **Suivant** et sur le bouton **Terminer**.

Un message indique que l'importation a réussi.

Cliquez sur le bouton **OK** pour fermer le message.

Validez que le certificat EFS de l'utilisateur u1 est à nouveau disponible dans sa console MMC personnalisée Certificat u1.

Validez que l'utilisateur peut à nouveau lire le contenu de son fichier texte chiffré.

4. Agent de récupération EFS

Objectif : Implémenter le compte utilisateur adminw10 en tant qu'agent de récupération EFS local et tester la récupération de fichiers chiffrés.

a. Méthodologie

La méthodologie suivante est appliquée :

- Génération des certificats de l'agent de récupération EFS local
- Déclaration de l'agent de récupération sur l'ordinateur local
- Récupération des fichiers chiffrés des utilisateurs

b. Génération des certificats d'agent de récupération

Connectez-vous avec l'utilisateur local adminw10.

Créez un nouveau dossier CertifsAR sous le disque local C:.

Ce nouveau dossier hébergera les certificats de l'agent de récupération EFS local.

Créer les certificats pour le rôle d'agent de récupération

Ouvrez une invite PowerShell en tant qu'administrateur.

Exécutez la commande :

```
cipher /r:c:\certifisAR\certificatAr
```

Saisissez deux fois le mot de passe.

Validez la création de deux certificats dans le dossier C: \CertificatsAR.

Un certificat certificatAr.cer et un certificat certificatAr.pfx sont créés dans le dossier C: \CertificatsAR.

Question : Pourquoi l'utilitaire cipher.exe a-t-il généré deux certificats ?

Réponse :

- Le certificat au format DER (.cer) sera déployé sur les ordinateurs pour indiquer la présence d'un agent de récupération. Pour ce rôle, seule la clé publique de l'agent de récupération est nécessaire. Cette clé publique chiffrera la clé de chiffrement symétrique, réservé à l'agent de récupération.
- Le certificat en format PKCS #12 (.PFX) ne sera utile que dans un contexte de récupération de fichiers chiffrés. Lui seul contient la clé privée qui permettra de déchiffrer la clé symétrique de chiffrement du fichier.

Validation de la présence d'un agent de récupération EFS

Faites un clic droit sur le fichier u1 et sélectionnez le menu **Propriétés** puis cliquez sur le bouton **Avancé** puis cliquez sur le bouton **Détails**.

Validez que la zone Certificats de récupération pour ce fichier tels que définis par la stratégie de récupération est pour le moment vide.

Cela signifie qu'il n'y a pas pour le moment d'agent de récupération EFS déclaré sur cet ordinateur.

Cliquez sur les boutons **Annuler** pour refermer toutes les boîtes de dialogue.

Déclarer un agent de récupération EFS sur l'ordinateur

Méthodologie : la déclaration d'un agent de récupération EFS sur un ordinateur consiste simplement à déployer le certificat (.cer) de l'agent de récupération sur l'ordinateur. Cette tâche est effectuée au moyen d'une stratégie de groupe.

Connectez-vous en tant qu'Adminw10.

Ouvrez une invite PowerShell en tant qu'administrateur et exécutez la commande :

```
Gpedit.msc
```

La console de gestion Editeur de stratégies de groupe locales s'ouvre.

Développez l'arborescence **Configuration ordinateur\Paramètres Windows\Parametres de sécurité\Stratégies de clé publique**.

Faites un clic droit sur **Systeme de fichier EFS (Encrypting File system)** puis sélectionnez le menu **Ajouter un agent de récupération de données**.

Dans la boîte de dialogue Assistant ajout d'un agent de récupération, cliquez sur le bouton **Suivant**.

Dans la boîte de dialogue Sélectionner des agents de récupération, cliquez sur le bouton **Parcourir les dossiers** et sélectionnez le fichier **C: \certifsAR\certificatAR.cer**.

L'assistant sélectionne intelligemment le fichier au format DER (.cer) qui ne contient que la clé publique de l'agent de récupération EFS. Déployer sur l'ordinateur un certificat contenant la clé privée de l'agent de récupération EFS compromettrait fortement la sécurité !

Cliquez sur le bouton **Oui** sur le message indiquant que Windows n'a pas pu déterminer si ce certificat a été révoqué.

La détermination de révocation de certificats n'est possible que dans un contexte domaine et avec une autorité de certification entreprise. Ce sujet sera abordé dans d'autres chapitres.

Cliquez sur le bouton **Suivant** puis sur le bouton **Terminer**.

Le certificat d'agent de récupération EFS (adminw10) apparaît maintenant dans la stratégie de groupe locale.

Fermez la console de gestion Editeur de stratégies de groupe locales.

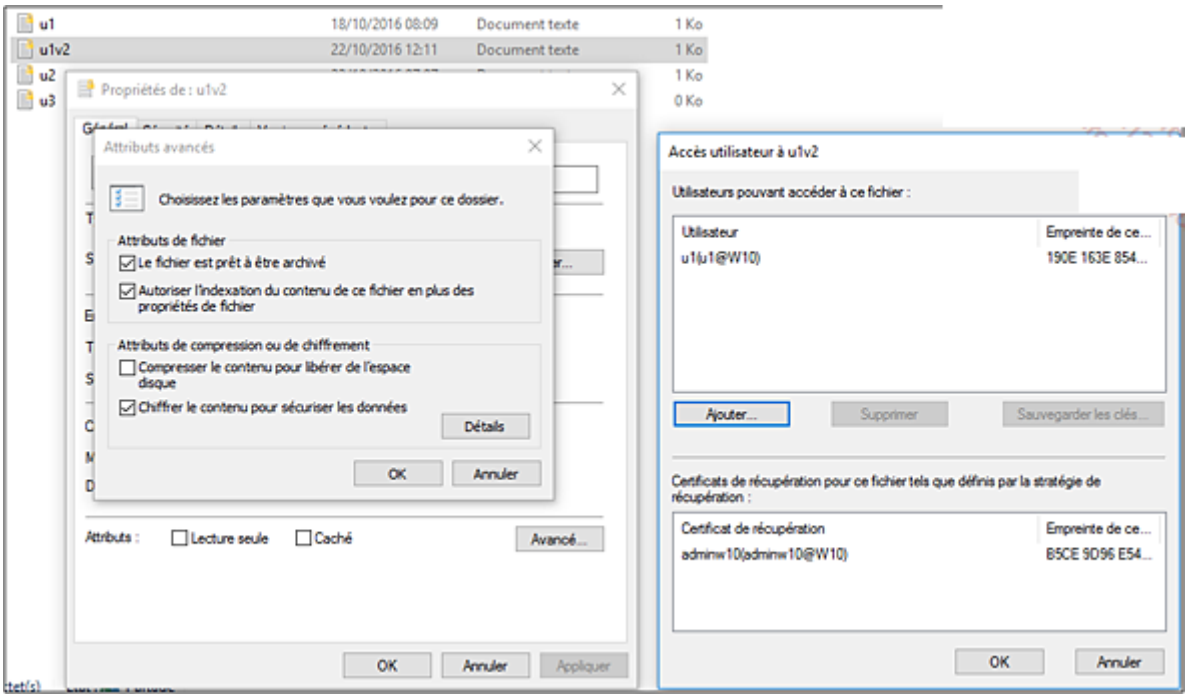
Récupération de fichiers chiffrés

Connectez-vous avec l'utilisateur local u1.

Créez un nouveau fichier texte u1V2 dans le dossier C: \TestsEfs (avec un contenu) puis chiffrez ce nouveau fichier.

Faites un clic droit sur le fichier u1V2 et sélectionnez le menu **Propriétés** puis cliquez sur le bouton **Avancé** puis cliquez sur le bouton **Détails**.

Validez que la zone **Certificats de récupération pour ce fichier tels que définis par la stratégie de récupération** affiche le certificat de l'agent de récupération EFS (adminw10).



Un certificat d'agent de récupération (adminw10) est bien déclaré et actif sur cet ordinateur.

Cliquez sur les boutons **Annuler** pour refermer toutes les boîtes de dialogue.

Prenez soin de ne modifier aucun autre fichier. Cela modifierait les résultats de notre atelier.

Connectez-vous avec l'agent de récupération EFS adminw10.

Essayez d'accéder aux fichiers cryptés par les utilisateurs u1, u2 et u3.

Question : Peut-on déchiffrer les fichiers cryptés par les utilisateurs ? Pourquoi ?

Réponse : Non. On ne peut, pour le moment, déchiffrer aucun fichier chiffré d'aucun utilisateur, car l'agent de récupération ne dispose pas de certificat incluant sa clé privée sur cet ordinateur. Ce certificat est bien disponible sous forme de fichiers, mais n'a pas encore été installé sur cet ordinateur !

Ouvrez la console Certificat Adminw10 qui se trouve sur le bureau de l'administrateur.

Développez **Certificats\Utilisateur actuel\Personnel**.

Aucun certificat n'est disponible pour le moment pour la récupération EFS.

Installer la clé privée de l'agent de récupération EFS

Double cliquez sur le fichier C: \certifsAR\CertificatAR.pfx.

L'icône des fichiers PKCS #12 (.pfx) inclut une clé. L'assistant d'importation du certificat s'affiche.

La boîte de dialogue Assistant importation du certificat, sélectionnez **Utilisateur local** puis cliquez sur le bouton **Suivant**.

Dans la zone **Nom du fichier**, validez le chemin d'accès au fichier .pfx puis cliquez sur le bouton **Suivant**.

Dans la zone **Mot de passe**, saisissez le mot de passe utilisé lors de génération du certificat avec l'utilitaire cipher.exe.

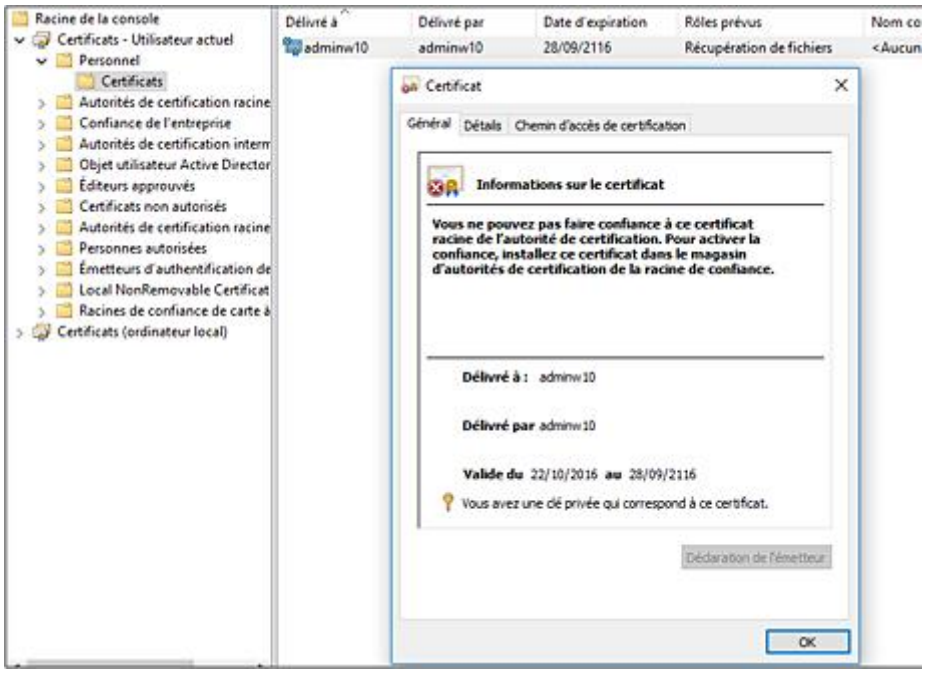
Cochez les options **Marquer cette clé comme exportable** et **Inclure toutes les propriétés étendues** puis cliquez sur le bouton **Suivant**.

Dans la boîte de dialogue Magasin de certificats, sélectionnez **Sélectionnez automatiquement le magasin de certificats en fonction du type de certificat** puis cliquez sur le bouton **Suivant** et sur le bouton **Terminer**.

Un message indique que l'importation a réussi.

Cliquez sur le bouton **OK** pour fermer le message.

Actualisez la console Certificat Adminw10 pour valider qu'un certificat d'agent de récupération EFS est maintenant correctement installé.



*Le certificat installé inclut la clé privée, la colonne **Rôles prévus** indique qu'il s'agit d'un certificat de type Récupération de fichiers !*

Essayez de lire les fichiers chiffrés par les utilisateurs u1, u2 et u3.

Question : L'agent de récupération EFS peut-il lire les fichiers chiffrés des utilisateurs ?

Réponse : Oui, mais uniquement pour les fichiers qui ont été créés après l'installation d'un agent de récupération. Donc uniquement pour le fichier texte u1v2. Les fichiers texte qui ont été créés avant l'installation de l'agent de récupération ne disposent pas de l'en-tête de l'agent de récupération, ils ne peuvent donc pas être déchiffrés !

Actualisation des en-têtes de l'agent de récupération

Connectez-vous avec l'utilisateur local u1.

Ouvrez et refermez (sans aucune modification) le fichier texte u1.

Cette opération met à jour l'en-tête de l'agent de récupération pour ce fichier !

Connectez-vous avec l'agent de récupération EFS adminw10.

Validez la possibilité de lire le fichier texte chiffré de l'utilisateur u1.

Procédez de même avec les utilisateurs u2 et u3 pour actualiser l'en-tête de l'agent de récupération sur leurs fichiers respectifs.

Connectez-vous avec l'agent de récupération EFS adminw10.

Validez la possibilité de lire les fichiers texte chiffrés des utilisateurs u2 et u3.