EFS (Encrypting File System)

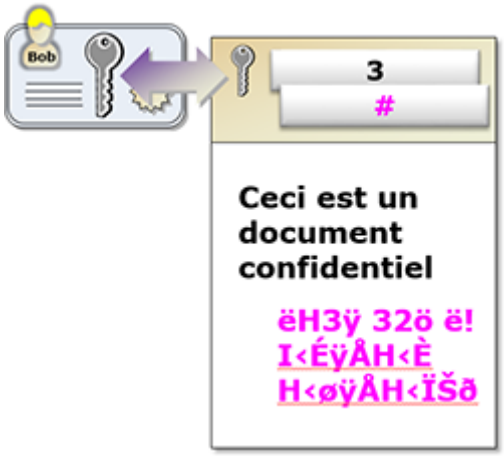
Avec le système EFS (*Encrypting File System*), Microsoft propose une solution simple, efficace, totalement intégrée et gratuite pour le chiffrement de vos fichiers. Ainsi, en cas de vol de l'ordinateur, la confidentialité des données sensibles reste préservée.

Le premier exemple d'utilisation de la cryptographie associée à des chiffrements et déchiffrements de fichiers (voir atelier Chiffrement EFS ci-après) nous permettra de comprendre clairement et par la pratique le fonctionnement des algorithmes de chiffrement et le rôle des certificats et clés privées/publiques associées.

1. Fonctionnement

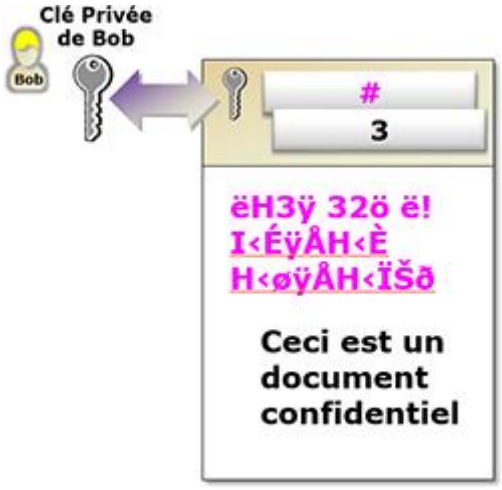
Le système de chiffrement de fichiers EFS (*Encrypting File System*) combine les systèmes de chiffrement symétrique et asymétrique.

Lorsque l'utilisateur demande à chiffrer un fichier, le système génère une clé symétrique aléatoire à l'aide de laquelle il chiffre le fichier (performance), cette clé est ensuite stockée dans un en-tête du fichier ou elle est chiffrée en asymétrique à l'aide de la clé publique de l'utilisateur (sécurité maximale).



Chiffrement du texte avec la clé symétrique, chiffrée elle-même dans un en-tête, avec la clé publique de l'utilisateur.

Lorsqu'un utilisateur demande à déchiffrer le fichier, le système accède à la clé privée de l'utilisateur, à l'aide de laquelle il déchiffre la clé symétrique qui est dans l'entête du fichier, le système déchiffre alors le fichier à l'aide de la clé symétrique.



Déchiffrement de la clé symétrique à l'aide de la clé privée puis déchiffrement du texte avec la clé symétrique.

Pour pouvoir chiffrer des fichiers à l'aide du système EFS, l'utilisateur doit donc disposer d'un certificat avec une clé publique et une clé privée. Ce certificat peut être généré de façon automatique par le système (on parle de certificat autogénéré) lorsque l'ordinateur est en Workgroup. Ce type de certificat peut être distribué plus simplement et plus sûrement par une autorité de certification lorsque l'ordinateur de l'utilisateur fait partie d'un domaine Active Directory (cf. chapitre Autorité de certification entreprise).

2. Partage de fichiers chiffrés

Le chiffrement utilisant un certificat utilisateur est, de ce fait, plutôt lié à un usage strictement personnel. Microsoft introduit cependant la possibilité étonnante, pour un utilisateur, de pouvoir partager ses fichiers chiffrés.

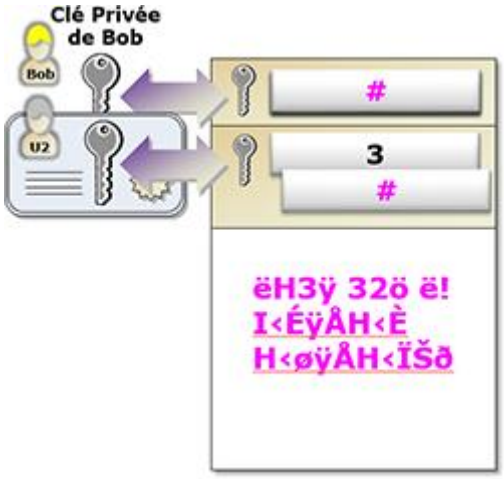
Si l'on en voit clairement l'utilité (travail collaboratif par exemple sur le même fichier), on ne perçoit pas le mécanisme par lequel d'autres utilisateurs pourraient accéder aux fichiers chiffrés. Il n'est bien sûr pas question de partager avec eux notre clé privée. Comment alors cela est-il possible ?

Ici, la difficulté est de trouver une solution technique pour qu'un utilisateur puisse partager des fichiers chiffrés avec d'autres utilisateurs, sans pour autant (et c'est bien là tout le challenge) leur donner accès à la clé privée de l'utilisateur qui partage le fichier. Donner accès à cette clé privée complexifierait la procédure et surtout donnerait accès à … tous … les fichiers chiffrés par l'utilisateur qui aurait partagé sa clé privée. C'est donc inacceptable !

Une solution simple et élégante existe pourtant et c'est celle implémentée par Microsoft. Voilà comment cela fonctionne :

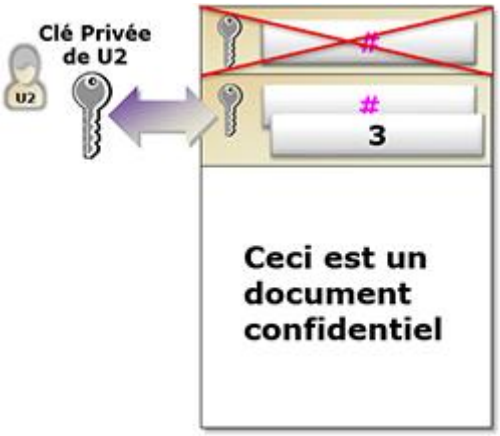
L'utilisateur qui a chiffré le fichier ne partage pas (jamais) sa clé privée. Ce n'est pas nécessaire ! Pour déchiffrer le fichier, il suffit que les autres utilisateurs aient accès à la clé de chiffrement/déchiffrement symétrique.

Lorsque l'utilisateur qui a chiffré le fichier demande à le partager avec un autre utilisateur. Le système duplique l'en-tête contenant la clé de chiffrement/déchiffrement symétrique pour créer un en-tête supplémentaire. Ce nouvel en-tête est chiffré avec la clé publique de l'utilisateur avec lequel vous partagez le fichier chiffré.



L'utilisateur u2, avec lequel Bob a partagé son fichier, dispose de son en-tête contenant la clé symétrique (3 ici, par exemple) qu'il chiffre avec sa clé publique (celle de l'utilisateur u2).

Lorsque l'utilisateur, avec lequel vous avez partagé votre fichier, souhaite le déchiffrer, il utilise sa clé privée pour déchiffrer la clé symétrique qui se trouve dans son en-tête, il utilise ensuite cette clé symétrique pour déchiffrer le document.



L'utilisateur u2, avec lequel Bob a partagé son fichier, n'accède pas à l'en-tête de Bob, mais il déchiffre son propre en-tête à l'aide de sa clé privée puis déchiffre le fichier à l'aide de la clé symétrique (3 ici, par exemple).

Et ainsi de suite pour chaque utilisateur avec lequel vous partagerez vos fichiers chiffrés…

Ainsi, si vous partagez votre fichier chiffré avec 10 utilisateurs, le fichier contiendra 11 en-têtes, le vôtre plus 10 autres pour les utilisateurs avec qui vous partagez le fichier chiffré, chaque en-tête étant protégé avec les clés privées/publiques de chaque utilisateur. Chaque utilisateur n'accède donc qu'à son propre en-tête. Astucieux et élégant, non ?

Les ateliers de ce chapitre présentent de façon détaillée et pratique l'implémentation du partage de fichiers EFS.

3. Agent de récupération EFS

Un autre challenge intéressant serait de pouvoir disposer en interne d'un moyen de récupération de fichiers chiffrés.

Imaginez par exemple qu'un employé quitte l'entreprise, ou pire qu'un événement grave l'empêche de reprendre son travail. Comment l'entreprise peut-elle récupérer l'accès à ses fichiers chiffrés ?

Autoriser ce type de récupération est souvent souhaitée et souhaitable en interne. Rappelez-vous que le système EFS est principalement conçu pour préserver la confidentialité de fichiers en externe (vol d'un portable lors d'un déplacement de collaborateurs par exemple).

La solution technique passe par la mise en place d'un ou de plusieurs agents de récupération EFS.

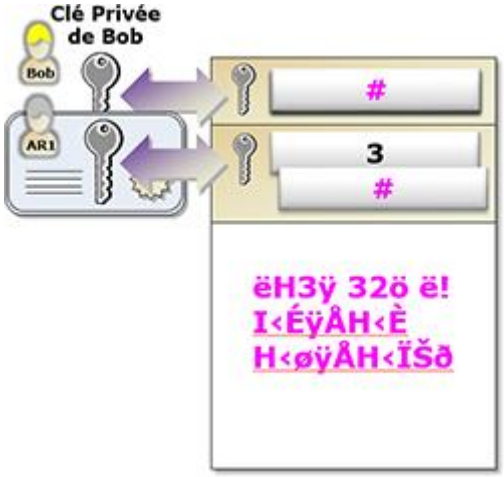
a. Fonctionnement

Ici, la difficulté est de trouver une solution technique pour qu'un utilisateur, qui sera l'agent de récupération EFS, puisse accéder à tous les fichiers chiffrés de tous les utilisateurs de l'entreprise. Sans que ceux-ci lui aient communiqué leur clé privée !

Une solution simple et élégante existe là aussi et elle est très proche de celle utilisée pour le partage de fichiers chiffrés.

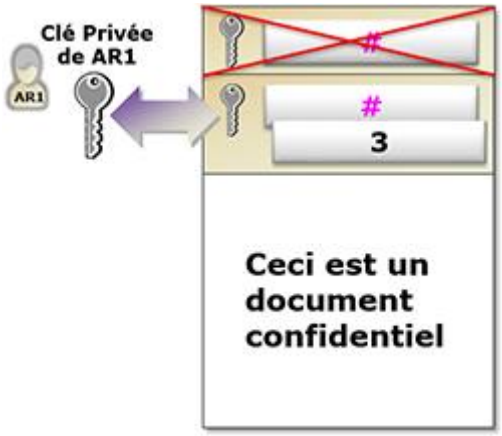
Voilà comment cela fonctionne :

Lorsque l'utilisateur chiffre un fichier, si un agent de récupération est déclaré sur l'ordinateur de l'utilisateur, l'en-tête contenant la clé de chiffrement symétrique est automatiquement dupliqué et chiffré avec la clé publique de l'agent de récupération EFS.



Un en-tête est automatiquement créé pour l'agent de récupération EFS (ar1). La clé de chiffrement symétrique (3 ici, par exemple) est chiffrée avec la clé publique de l'agent de récupération EFS.

Lorsque l'agent de récupération EFS souhaite accéder au fichier, il utilise sa clé privée pour déchiffrer l'en-tête contenant la clé de chiffrement symétrique, à l'aide de laquelle il déchiffre le contenu du document.



L'agent de récupération (ar1) utilise sa clé privée pour déchiffrer l'en-tête symétrique (3 ici, par exemple) avec laquelle il déchiffre le document.

Les ateliers de ce chapitre présentent de façon détaillée et pratique l'implémentation d'un agent de récupération EFS.