

Sécurisation Cryptage Windows – sys 30 – Cours T.P. -

Cryptage AxCrypt Veracrypt Windows Michel Cabaré – Ver 1.0 – Mai 2017-

Sécurisation Cryptage Windows

Cours et T.P.

Michel Cabaré – Ver 1.0 – Mai 2017

www.cabare.net©



TABLE DES MATIERES

BITLOCKER VS EFS	3
CRYPTAGE LOGICIEL	3
EFS	5
Fonctionnement d'EFS	5
VOIR LES CERTIFICATS UTILISATEUR	7
CRYPTAGE DE FICHIER	9
VERIFICATION CERTIFICATS UTILISATEUR	10
AGENT RECUPERATEUR	11
EXPORT CLE ET CERTIFICAT EFS DE L'UTILISATEUR	
DECRYPTAGE DE FICHIER EFS	15
COMMANDE EN LIGNE CIPHER	16
EFS – Securiser un poste autonome	17
AXCRYPT	19
TELECHARGEMENT DE AXCRYPT.NET	
INSTALLER AXCRYPT 2.0	20
1° LANCEMENT - PARAMETRAGE	
LANCER AXCRYPT 2.0 VIA CLIC DROIT	
DEMONTER LE CRYPTAGE	
OUVRIR LE FICHIER SUR UNE AUTRE MACHINE	23
SUPPRIMER DEFINITIVEMENT UN FICHIER CRYPTE	23
VERACRYPT	24
TELECHARGEMENT DE VERACRYPT	24
DECOMPACTER VERACRYPT 1.19	
CREATION CONTAINER CRYPTE – FICHIER DISQUE VIRTUEL	
MONTAGE VOLUME SUR CONTAINER VERACRYPT	
DEMONTAGE VOLUME SUR CONTAINER VERACRYPT	
CREATION VOLUME CRYPTE	
MONTAGE VOLUME CRYPTE	
SIGNATURE ET ENCRYPTAGE	
DIFFERENCE ENTRE UNE SIGNATURE, ET L'ENCRYPTAGE :	
MECANISME DE CLE SECRETE (SYMETRIQUE) :	
MECANISME DE CLE PUBLIQUE – CLE PRIVEE (ASYMETRIQUE):	
MECANISME DE CERTIFICAT :	



BITLOCKER VS EFS

Cryptage Logiciel

BitLocker est conçu pour protéger la totalité des fichiers personnels et des fichiers système d'un lecteur logique. Vous pouvez utiliser **BitLocker** pour chiffrer tous les fichiers sur des lecteurs de données fixes (tels que des disques durs internes) et utiliser **BitLocker To Go** pour chiffrer les fichiers sur des lecteurs de données amovibles (disques durs externes ou disques flash ou USB).

Le **système de fichiers EFS** permet de protéger des fichiers individuels sur tout lecteur, en fonction de l'utilisateur.

N.B: Le chiffrement <u>est perdu</u> en cas de transmission par mail ou via le réseau.

BitLocker (logiciel et materiel)

- BitLocker chiffre tous les fichiers personnels et système sur un lecteur de données fixe et sur des lecteurs de données amovibles.
- BitLocker ne dépend pas des comptes d'utilisateurs individuels associés aux fichiers. BitLocker est activé ou désactivé, pour tous les utilisateurs ou groupes.
- BitLocker peut utiliser le module de plateforme sécurisée (TPM), une puce spéciale présente sur de nombreux ordinateurs et qui prend en charge des fonctionnalités de stockage et de chiffrement.
- Vous devez être un administrateur pour activer ou désactiver le chiffrement BitLocker

EFS, Système de fichiers EFS (logiciel)

- EFS chiffre les fichiers personnels et système un par un et ne chiffre pas le contenu complet d'un lecteur.
- Le système de fichiers EFS chiffre des fichiers en fonction du compte d'utilisateur associé. Si un ordinateur comporte plusieurs utilisateurs ou groupes, chacun peut chiffrer ses propres fichiers individuellement.
- Le système de fichiers EFS ne requiert ou n'utilise pas de matériel spécial.
- Il n'est pas nécessaire que vous soyez un administrateur pour pouvoir utiliser le système de fichiers EFS.



Si cette clef USB n'est pas présente dans un des ports USB de votre ordinateur, Windows ne démarrera pas, à moins que vous saisissiez la clef de recouvrement Bitlocker(numéro super long de secours). La clef USB devient en quelque sorte votre puce TPM, mais avec moins de fonctionnalités. La puce TPM possède des fonctionnalités avancées permettant de ne pas démarrer Windows du tout, si le disque dur n'est pas dans le même ordinateur, que le BIOS, le MBR, ou le Gestionnaire de démarrage ont changés.



Fonctionnement d'EFS

Le système **EFS** inclus dans windows permet à un utilisateur de chiffrer un fichier de manière à ce que celui-ci ne puisse pas être lu par quelqu'un d'autre que lui (saut un compte particulier, appelé **agent de récupération**, généralement un administrateur...)

Sans la «clé», le fichier est <u>véritablement indécryptable</u>, même par l'administrateur. Seul un agent de récupération peut être alors utilisé pour relire le fichier. POUR LIRE UN FICHIER EFS, même si on dispose de tous les droits NTFS, même si on s'est approprié le fichier, <u>IL EST NECESSAIRE DE DISPOSER DE LA CLE PRIVEE (ou d'être AGENT DE RECUPERATION</u>). Ainsi un disque « démonté et remonté sur un autre système » ou un portable reste protégé.

EFS fonctionne en arrière plan, et stocke dans le fichier lui-même un certain nombre d'informations (qui a chiffré, avec quelle clé, liste des agents de récupération...).

N.B: certaines applications peuvent sauvegarder des fichiers temporaires, et donc risquent de laisser des traces lisibles de vos fichiers, il vaut mieux pour éviter cela **demander de crypter tout un dossier, plutôt que uniquement un fichier**.... (dans ce cas, chaque fichier posé dans ce dossier sera automatiquement chiffré avec la clé de son propriétaire...)

Pour qu'EFS fonctionne il est nécessaire que :

- Vous soyez sur un volume NTFS
- L'utilisateur ait un certificat valide d'utilisateur EFS
- Un compte d'agent de récupération d'EFS au moins ait un certificat valide de récupération d'EFS. (une autorité de certification n'est pas nécessaire, EFS produit automatiquement ses propres certificats pour les utilisateurs et les comptes d'agent de récupération...)

Lorsque EFS chiffre un fichier :

Lorsqu'un utilisateur chiffre un fichier, les opérations suivantes sont exécutées :

- Production d'une clé de chiffrement
- Chiffrage du fichier avec cette clé de chiffrement
- Chiffrage de cette clé de chiffrement avec la clé publique de l'utilisateur (si besoin création de cette clé et du certificat associé)
- Stockage de cette « clé de chiffrage chiffrée » dans le fichier dans une zone nommée DDF (une par fichier)



Résultat : lorsque l'on essayera de lire un fichier chiffré, seul le possesseur de la clé privée de cet utilisateur, peut déchiffrer la clé de chiffrage employée lors du codage. Ce ne peut être que l'utilisateur

Mais n'oublions pas que EFS permet à des comptes définis d'agent de récupération de déchiffrer et de récupérer le fichier, au cas où la clé privée serait détruire (exemple, un utilisateur renvoyé crypte tous ses fichiers avent de partir...) donc lorsqu'un utilisateur chiffre un fichier les opérations suivantes sont aussi exécutées :

- Chiffrage de cette clé de chiffrement avec la clé publique de chaque agent de récupération
- Stockage de cette « clé de chiffrage chiffrée » dans le fichier dans une zone nommée DRF (une ou plusieurs par fichier)
- Chaque fois que l'on manipule ce fichier, copie, ouverture, modification, la zone DRF est mise à jour selon les besoins

Résultat: seul le possesseur de la clé privée des agents de récupération peu lire le fichier



Voir les Certificats Utilisateur

Soit 2 utilisateurs locaux sur un poste Windows 10, andré et bruno, respectivement avec comme mot de passe Local10

Nom	Nom complet	Description
Administrateur		Compte d'utilisateur d'administra
🛃 andré	andré	
🜉 Bruno	Bruno	

Vérifions d'abords par exemple pour andré que celui-ci ne possède pas de certificat permettant de stocker une clé publique (il n'a jamais chiffré de fichier, et n'a donc jamais eut besoin d'une clé privée+clé publique...)

Plusieurs méthodes existent

En invite de commande **certmgr.msc**, lance la gestion du **certificat utilisateur** pour l'utilisateur courant



On peut créer une mmc avec le composant Certificats

Ajout d'un composant logiciel enfichal	ole autonome	? ×
Composants logiciels enfichables disponible	es :	
Composant logiciel enfichable	Vendeur	
Certificats	Microsoft Corporation	
🛛 🗊 Configuration et analyse de la sécurité	Microsoft Corporation	
al Contrôle ActiveX		

Si on est simple utilisateur, on ne pourra que voir les du **certificat utilisateur** pour l'utilisateur courant , mais si on est administrateur, on pourrait choisir

Ajouter ou supprimer des	composants log	icie	ls enfichables			
Vous pouvez sélectionner des composants logiciels enfichables parmi ceux disponibles sur votre ordinateur, et les configurer. composants logiciels enfichables extensibles, vous pouvez spécifier quelles extensions doivent être activées.						
Composants logiciels enficha	bles disponibles :		Composant logiciel enfichable Certificats			
Composant logiciel enfi	Fournisseur	^				
Analyseur de perfor	Microsoft Cor		Ce composant logiciel enfichable gérera toujours les certificats pour :			
Certificats	Microsoft Cor		O Mon compte d'utilisateur			
Contiguration et an	Microsoft Cor		O Un compte de service			
Contrôle WMI	Microsoft Cor		 Un compte d'ordinateur 			



Sous windows 10, en tant qu'administrateur, une recherche **Cortana** avec le mot *certificat* propose assez rapidement **Gérer les certificats de chiffrement de fichiers**







Suivant

Annuler

Cryptage de fichier

Dans	un dossier	🕳 data (D:)	^	Nom
nommé	stock-efs,	\$RECYCLE.BIN		doc de andré.txt
andré c	rée un fichier	stock-efs		
doc de o	andré			

puis il le chiffre via EFS... par **propriété** sur ce fichier, et **avancée**





Sécuriser AxCrypt VeraCrypthttp://www.cabare.netPage 9 / 38- SYS 30 Cours et T.P. - ver 1.0- Michel Cabaré -

Si on crypte que le fichier, les conséquences sont claires

Si on crypte le dossier alors on aura :

- Tous les fichiers existants sont protégés par notre clé (mais que si on peut écrire dedans au niveau des ACL)
- Tout ce qui sera crée ou copié plus tard dans ce dossier par nous sera protégé par notre clé
- Tout ce qui sera crée par un autre utilisateur sera protégé par sa clé
- Tout ce qui sera déplacé restera inchangé (au niveau cryptage)

IL VAUT MIEUX POSER UN CRYPTAGE PAR DOSSIER VIDE AVANT TOUTE UTILISATION

Vérification Certificats Utilisateur

Automatiquement, lors du premier appel à EFS de la part de André, une création de clé a été effectuée, et un certificat a été délivré...

Vérifions nos méthodes, En invite de commande **certmgr.msc**, lance la gestion du **certificat utilisateur** pour l'utilisateur courant



 \times

Via Cortana, avec la recherche...

🗧 🚽 Système de fichiers EFS (Encrypting File System)

Sélectionner ou créer un certificat de chiffrement de fichiers

Les certificats permettent de vérifier votre identité. Ainsi, lorsque vous chiffrez ou déchiffrez un fichier, nous savons qu'il s'agit bien de vous. Si vous avez déjà chiffré certains fichiers, vous pouvez les mettre à jour pour qu'ils utilisent ce certificat.

Otiliser	се	certificat
----------	----	------------

Si vous utilisez une carte à puce, sélectionnez le certificat sur la carte à puce.

Détails du certificat:

Délivré à : andré	Afficher le certificat
Délivré par : andré Expiration : 20/05/2117	Sélectionner un certificat





Agent Récupérateur

Par ailleurs il y a forcément un agent de récupération, on peut le connaître en via les **propriétés** puis **avancées** du fichier, où l'on voit

Certificats de récupération pour ce fichier tels que définies par la stratégie de récupération

Utilisateur		Empreinte de ce.
andré(andré@WIN10-1	71)	E4B4 81B0 418
Aio: tor	Supplier	Courseseder los dás
Ajouter	Supprimer	Sauvegarder les clés
Ajouter	Supprimer	Sauvegarder les clés

Dans un Domaine, c'est l'Administrateur de domaine qui possède ce rôle,

<u>Sur une machine en Workgroup</u>, c'est l'Administrateur du poste qui possède ce rôle

on peut par conséquent afficher les certificats personnels de l'administrateur, et on devrait voir

🚡 certmgr - [Certificats - Utilisateu	r actuel\Personnel\Cert	ificats]				_	
Fichier Action Affichage ?							
🗢 🔿 🙋 💼 🔏 🖬	1 🗟 🛛 🖬						
Certificats - Utilisateur actuel	Délivré à	Délivré par	Date d'expirati	Rôles prévus	+	Nom convivial	
 Personnel Certificats 	Administrateur	Administrateur	15/05/2117	Récupération	de fichiers	<aucun></aucun>	

N.B : Si une machine de domaine sort du domaine, les fichiers crytpés se retrouvent sans agent récupérateur.



Export clé et certificat EFS de l'utilisateur

Plusieurs cas pour lesquels il peut être intéressant d'exporter la clé privée de l'utilisateur

- Avoir une copie de sauvegarde de la clé
- Si l'on souhaite qu'un autre utilisateur (à part l'agent de récupération) puisse modifier le fichier, il faut exporter la clé privée de l'utilisateur qui a chiffré le fichier, et l'importer pour l'utilisateur à qui on veut fournir l'accès

Par exemple, pour pouvoir faire en sorte que **paul** puisse modifier le fichiers cryptés par **pierre**, il faut <u>exporter</u> le certificat de **pierre**, et l'<u>importer</u> pour **paul**

Exportation du certificat de pierre sur disquette

Ayant une session pour pierre, on crée une mmc certificats



On se place sur certificats à gauche, puis menu contextuel sur le certificat de pierre sur lequel on va enclencher l'exportation de certificat avec la clé privée de Pierre

Les étapes sont claires

Assistant Exportation de certificat	×
Exportation de la clé privée Vous pouvez choisir d'exporter la clé privée avec le certificat.	
Les clés privées sont protégées par mot de passe. Pour pouvoir exporter la clé privée avec le certificat, vous devez entrer son mot de passe dans une des pages suivantes.	
Voulez-vous exporter la clé privée avec le certificat ?	
 Oui, exporter la dé privée 	
🔿 Non, ne pas exporter la clé privée	

Avec exportation de la clé privée



Sélec	tionnez le format à utiliser :
(Bioaire codé DER X 509 (cer)
ć	Codé à base 64 X 509 (cer)
ć	Code a base of misor (real) Standard de cyntaxe de mescage cryntographique - Certificats PKCS #7 (p7)
	Inclure tous les certificats dans le chemin d'accès de certification si possibilité
(Échange d'informations personnelles - PKCS #12 (.pfx)
	Inclure tous les certificats dans le chemin d'accès de certification si possible
	Activer la protection renforcée (nécessite IE 5.0, NT 4.0 SP4 ou supérieur
	Effacer la clé privée si l'exportation s'est terminée correctement
Pour Pour pass	prose maintenir la sécurité, vous devez protéger la clé privée en utilisant un mot de e.
Pour pass	passe maintenir la sécurité, vous devez protéger la clé privée en utilisant un mot de e.
Pour pass Entr	rmaintenir la sécurité, vous devez protéger la clé privée en utilisant un mot de e. ez et confirmez le mot de passe.
Pour pass Entr	rmaintenir la sécurité, vous devez protéger la clé privée en utilisant un mot de le. ez et confirmez le mot de passe. 1ot de passe :
Entr	rmaintenir la sécurité, vous devez protéger la clé privée en utilisant un mot de e. ez et confirmez le mot de passe. 1ot de passe :
Entr	rmaintenir la sécurité, vous devez protéger la clé privée en utilisant un mot de le. ez et confirmez le mot de passe. 1ot de passe : Confirmer le mot de passe :
Entr	rmaintenir la sécurité, vous devez protéger la clé privée en utilisant un mot de e. ez et confirmez le mot de passe. Not de passe : Confirmer le mot de passe :
Entr Pour Entr M	rmaintenir la sécurité, vous devez protéger la clé privée en utilisant un mot de le. ez et confirmez le mot de passe. Not de passe : confirmer le mot de passe :

A partir de là, on dispose du certificat de pierre (et de sa clé privée) sur une clé ou tout autre emplacement. Il reste à les donner à paul...

Importation du certificat de pierre pour paul

Ayant accès à l'emplacement contenant le certificat de pierre,

pierre.pfx Échange d'informations personnelles



et ayant ouvert une session pour paul, on crée une mmc certificats



🎢 Console1 - [Racine de la console\Certifi	cats - Utilisateur actu	el\Personnel\	Certificats]		_ 8 ×
∫ 🚰 ⊆onsole Fe <u>n</u> être <u>?</u>] 🗅 🖨 🖬	: <u>-</u> #×
$Action Affichage Eavoris 4 \Rightarrow 1$	t 🖪 🖪 🕼) 2			
Arbre Favoris	Délivré à 🛛	Délivré par	Date d'expiration	Rôles prévus	Nom complet
Racine de la console Gertificats - Utilisateur actuel Gertificats - Utilisateur actuel Gertificats	- Depaul	paul	25/04/2102	Système de fichiers de cryptage	<aucun></aucun>
🔁 🕀 🛄 Autorités de c 👘 Toutes les tâches	•	Demander un no	ouveau certificat		
	▶ Dartir d'ici	Importer			

On se place sur certificats à gauche, puis avec le menu contextuel

on va enclencher l'importation de certificat avec la clé privée de Pierre...

istant Importation de certificat	
Spécifiez le fichier à importer.	
Nom du fichier :	-
A:\pierre.pfx Parcourir	
Remarque : plusieurs certificats peuvent être stockés dans un seul fichier aux formats suivants	:
Échange d'informations personnelles - PKCS #12 (.PFX, .P12)	
Standard de syntaxe de message cryptographique - Certificats PKCS #7 (.p7b)	
Magasin de certificats sérialisés Microsoft (.sst)	
istant Importation de certificat Mot de passe Pour maintenir la sécurité : la dé privée a été proténée avec up mot de passe	
	_
Entrez le mot de passe de la clé privée.	
Mot de passe :	
Activer la protection renforcée de clés privées. La clé privée vous sera demandée chaque fois qu'elle est utilisée par une application si vous activez cette option.	
🔽 Marquer la clé privée comme étant exportable	

Lorsque l'assistant se termine on devrait avoir

Arbre Favoris	Délivré à 🗠	Délivré par	Date d'expiration	Rôles prévus
Racine de la console	Egaul	paul	25/04/2102	Système de fichiers de cryptage
🖻 👹 Certificats - Utilisateur actuel	pierre	pierre	25/04/2102	Système de fichiers de cryptage
Personnel Certificats				

et paul peut désormais modifier les documents de pierre



Annulation non rétro-active de l'import de certificat

Le temps passe, et paul se fâche avec pierre, comment peut on empêcher paul d'accéder aux fichiers de pierre ? Il faut ouvrir une session en tant que Paul, aller dans les certificats...

Arbre Favoris	Délivré à 🛆	Délivré par	Date d'expiration	Rôles prévus
Racine de la console	🔛 paul	paul	25/04/2102	Système de fichiers de cryptage
💼 🐻 Certificats - Utilisateur actuel	🔤 pierre	pierre	25/04/2102	Système de fichiers de cryptage
÷ Personnel	◀			
Certificats	/			

et supprimer le certificat de pierre dans sa liste de certificats...

N.B : par défaut Pierre peut toujours modifier les documents déjà existant de pierre ? s'il les a déjà ouvert, leur champs liste DRF (liste des agents récupérateurs) inclus l'utilisateur Pierre comme personne habilité à les gérer.

Par contre, si maintenant Paul crée d'autres documents, ceux-ci sont inutilisables à Pierre

Decryptage de Fichier EFS

Décryptage EFS et gestion des fichiers:

Donc un fichier crypté dans un domaine, pourra être "lu" sur n'importe quelle machine, à partir du moment où l'on ouvre une session du domaine... Si on se transfère sur une autre machine (autre domaine ou chez soi) il faut emporter aussi le certificat avec la clé privée, ou bien être repéré comme agent de récupération !

SI la clé privée est inutilisable, (utilisateur inexistant) l'agent de récupération peut ouvrir le fichier en utilisant sa propre clé cryptée. Si l'agent de récupération se trouve sur un autre ordinateur, il faut lui envoyer le fichier à décrypter, plutôt que l'agent vous envois sa propre clé cryptée...

Décryptage d'un fichier

De manière générale, lors d'une manipulation, pour décrypter un fichier il suffit <u>de décocher la case</u> crypter le contenu... dans avancée

Attrib	uts avancés 🤶 🕺
<u>=</u>	Choisissez les paramètres que vous désirez pour ce dossier Lorsque vous appliquerez ces modifications, vous devrez indiquer si elles s'appliqueront aussi à tous les sous-dossiers et fichiers.
Att	ributs d'archivage et d'indexation
	Le dossier est prêt à être archivé
	Autoriser l'indexation de ce dossier pour la recherche rapide
Attr	ributs de compression ou de cryptage
	Compresser le contenu pour minimiser l'espace disque nécessaire
	Crypter le contenu pour sécuriser les données
	OK Annuler



Manipuler un fichier crypté

Lorsque l'on effectue les manipulations sur les fichiers cryptés, de manière générale, le fichier est décrypté, modifié, puis recrypté sous sa nouvelle forme ou destination si cela est possible

Ainsi lorsque l'on :

le chiffrage est

- Change le nom maintenu
- Déplace Copie le fichier maintenu si cible sur NTFS2000
- Déplace vers un autre PC si la cible accepte EFS, maintenu avec la clé publique de l'expediteur. L'ordinateur cible doit être approuvé pour la délégation (voir dans Utilisateur et Ordinateur Active Directory, dossier Computer, propriété de l'ordinateur sur lequel on veut effectuer le transfert, onglet Général, la case à cocher Approuver l'ordinateur pour la délégation
- Sauvegarde avec l'outil backup maintenu

Commande en ligne cipher

On peut aussi utiliser une commande en ligne **cipher** dont l'aide est complète...

Sous sa forme la plus simple, cipher indique si les fichiers – dopssiers sont cryptés ou non

Utilisé sans paramètres, CIPHER affiche l'état de chiffrement du répert. actuel et des fichiers qu'il contient. Vous pouvez utiliser plusieurs noms de répert. et des caractères génériques. Vous devez insérer des espaces entre plusieurs paramètres.

ainsi **cipher** donnerait:



N.B : l'attribut E peut apparaître aussi dans l'explorateur de fichier

Il faut demander dans l'explorateur sur les colonnes via le menu contextuel **Autres**, et demander **Attributs** :



Nom		Modifié le	Туре	Taille			
doc de andré.	.t	Ajuster la taille Ajuster la taille	de la colonne de toutes les colonnes	1 Ko			
	\checkmark	Nom					
	~	Modifié le		Choisir les détails			×
	Š	Type Taille		Sélectionnez les dét éléments de ce dos	ails que vous souhaitez sier.	afficher pour les	1
		Date de créatio Auteurs Mots clés Titre	n	Détails :	e mariage ou fête	A Mo	nter endre
		Autres		Auteurs		Aff	icher
ur obtenir							*
			~				
🕳 data (D:)		^	Nom	Modifié le	Туре	Taille	Attribut
🕳 data (D:) > 📑 \$RECYCLE.BIN		^	Nom	Modifié le 13/06/2017 12:02	Type Document texte	Taille 1 Ko	Attribut

EFS – Sécuriser un poste autonome

Vol d'un poste (portable ?) :

Si on a compris le principe de la sécurisation, on a compris que sur une machine, par défaut le Compte de l'Agent de récupération par défaut est celui de l'Administrateur de Domaine (dans le cas d'une machine faisant partie d'un domaine) ou le compte de l'Administrateur Local...

Pour sécuriser au maximum une machine autonome, il suffit d'exporter le certificat du compte de l'agent de récupération, en exportant sa clé privée en un endroit sûr ! A partir de la, l'agent de récupération n'existe plus !!!!! il faut pour le « reconstruire » que l'on importe le certificat et sa clé privée, ce qui suppose d'avoir accès aux fichiers

Export du certificat de l'agent de récupération d'un poste autonome :

Le poste étant autonome (hors Domaine), il faut ouvrir une session en tant qu'administrateur local...

📸 certificats - [Racine de la console\Certificats - Utilisateur actuel\Personnel\Certificats]							
∫ <u>C</u> onsole Fe <u>n</u> être <u>?</u>				D 🖨 🖬 🔲 💷			
Action Affichage Eavoris ↓ ← → 1 🔁 💽	% ⊫ × @ I	5 2					
Arbre Favoris	Délivré à 🔺	Délivré par	Date d'expiration	Rôles prévus			
Racine de la console	Administrateur	Administrateur	26/04/2102	Récupération de fichier			
🗄 🗐 Certificats - Utilisateur actuel	🕮 Administrateur	Administrateur	26/04/2102	Système de fichiers de cryptage			
🚊 ··· 🧰 Personnel							
Certificats							

et demander d'exporter, dans l'assistant il faut indiquer alors





et surtout effacer la clé localement

	Assistant Exportation de certificat	۱
Sinon la clé est	Format de fichier d'exportation Les certificats peuvent être exportés sous plusieurs formats de fichier.	
laissée	Sélectionnez le format à utiliser :	
localement	C Binaire codé DER X.509 (.cer)	
	C Codé à base 64 X.509 (.cer)	
	C Standard de syntaxe de message cryptographique - Certificats PKCS #7 (.p7b)	
	\square Inclure tous les certificats dans le chemin d'accès de certification si possible	
	Échange d'informations personnelles - PKCS #12 (.pfx)	
	$\overline{\square}$ Inclure tous les certificats dans le chemin d'accès de certification si possible	
	🔽 Activer la protection renforcée (nécessite IE 5.0, NT 4.0 SP4 ou supérieur)	
	Ffacer la clé privée si l'exportation s'est terminée correctement	

Vérifier que désormais l'administrateur n'est plus agent de récupération (ou plutôt il est toujours agent de récupération, mais ne dispose plus de la clé privée...)

Import du certificat de l'agent de récupération d'un poste autonome :

En cas de problème, on ouvre une session en tant qu'administrateur et on demande d'importer la clé

👘 🟦 certificats - [Racine de la console\Certificats - Ut	tilisateur actuel\Pe	rsonnel\Certificat	s]		<u> X</u>
🚰 Console Fenêtre <u>?</u>] D 🖨 🖬 🔲 💷	P×
Action Affichage Eavoris ↓ ← → 1 €	n 🗗 🖪 🖻				
Arbre Favoris	Délivré à 🛆	Délivré par	Date d'expiration	Rôles prévus	Nom
Racine de la console	📟 Administrateur	Administrateur	26/04/2102	Récupération de fichier	<al< td=""></al<>
🗄 🗐 Certificats - Utilisateur actuel	🕮 Administrateur	Administrateur	26/04/2102	Système de fichiers de cryptage	<ÅL
Personnel					
Certificats					
🕀 👘 🛄 Autorités de c 🔤 Toutes les tâches	Demand	ler un nouveau certif	icat		
🗄 🛄 Approbation d	Importe	r			

N.B : pour que cela marche, la clé ne suffit pas, il faut la réimporter dans le compte qui est agent de récupération par défaut... (ici administrateur local).



AXCRYPT

Téléchargement de AxCrypt.net

Depuis le site https://www.axcrypt.net/fr/download/

AxCrypt	TÉLÉCHARGER	PRIX	DOCUMENTATION	AIDE	A PROPOS	SE CONNECTER	Q	••
AxCrypt Mobile Des applications mobiles sont disponi mobile est une application devisualisa documents chiffrés avec l'application o En lire plus ici.	bles pour les app tion qui vous per de bureau.	areils And met d'our	droid et iOS. La version vrir et de lire les fichie	n rs et		H		
Télécharger AxCry Version 2	pt pour \	Wind	lows		D	ownload AxCryp for Winckws	t	

On récupère un executable

Nom	Modifié le	Туре	Taille
AxCrypt-2.1.1494.0-Setup.exe	19/05/2017 13:35	Application	5 884 Ko

Propriétés de : AxCrypt-2.1.1494.0-Setup.exe

Général	Compatibilité	Signatures numériques	Sécurité	Détails
Propri	été	Valeur		
Descr Type	iption du fichier	AxCrypt 2.1.1494.0 Application		
Versio Nom o	n du fichier du produit	2.1.1494.0 AxCrypt 2.1.1494.0		
Versio	n du produit	2.1.1494.0 Copyright (c) AxCount Al	8 All riabts	reserved
Taille	ignit.	5,74 Mo	5.74 fights	
Modifi Langu	é le Je	19/05/2017 13:35 Anglais (États-Unis)		
Fichie	r d'origine	AxCrypt.NET.Bootstrapp	per.exe	



Installer AxCrypt 2.0

On accepte la licence

▲ AxCrypt 2.1.1494.0 Paramètres - ×	
AxCrypt 2.1.1494.0	
GNU GENERAL PUBLIC LICENSE Version 2, June 1991 Copyright (C) 1989, 1991 Free Software Foundation, Inc. 59 Temple Place, Suite 330, Boston, MA 02111- 1307 USA Everyone is permitted to copy and distribute verbatim copies of this license document, but changing v	
J'accepte les termes de la license et les conditions	
Pour obtenir	
AxCrypt 2.1.1494.0 Paramètres	>
AxCrypt 2.1.1494.0	
Installation réussie avec succès	
Lancer	nent Fermer

1° lancement - paramétrage

Au premier lancement une adresse mail est requise

AxCrypt 2.1.1494.0 -		_
Fichier Aide		
AxCrypt	AxCrypt ID ? X	
Fichiers récents Dossiers Proté	Lors du premier lancement d'AxCrypt, une connexion internet et une adresse mail valide sont requises. Cliquez sur Aide pour plus	
Fichier Heur	Email	
	ОК	



Cela permet de recevoir par email un code de vérification



Vous venez de créer un compte AxCrypt. Veuillez confirmer votre inscription pour finaliser la création.

Ce code permettra de réponde a la boite de dialogque suivante

Vérifier votre AxCr	ypt ID		-		×
Email					
michel@cabare.	net				
Code de vérificat	ion				
736xxx	Vérifiez vos	s boîtes de ré	ceptio	n et de s	spam!
Nouveau Mot de	Passeo				
Nouveau Mot de					
Nouveau Mot de					
Nouveau Mot de	asse				
Nouveau Mot de	asse	_			
Vérifier Mot de P	asse oot de passe	_			

et de démarrer AxCrypt

🖪 Débuter avec AxCrypt	\times				
Bienvenue à AxCrypt!					
AxCrypt est très simple à utiliser. Démarrez avec la fenêtre principale, ou utilisez le clic droit et le double-clic dans Windows Explorer.					
Pour commencer à protéger vos fichiers, cliquez l'icône + dans la barre d'outils.					
Pour plus d'information, cliquez sur OK pour naviguer sur notre site web.					
OK Annuler					



lancer AxCrypt 2.0 via Clic Droit

On se met sur un fichier à crypter

🖳 Nouveau Doo	ument Microsoft Word.docx	19/05/2017 13:56	Doci	ument Micros	0 Ko
	Ouvrir Edition Nouveau Imprimer				
	AxCrypt Numériser avec Windo Ouvrir avec	ws Defender	> -	Crypter Avancé Brouiller et suppri	mer
	 IZArc Rechercher les menace 	5	> -	Se déconnecter A propos	

On demande Crypter, on rentre le mot de passe AxCrypt et on obtient

1	AxCrypt 2	2.1.1494	4.0 - Gratuit					_	_		\times	
	Fichier	Aide										
	P	Ax	Cryp	t	6 + 🙎			Essayez Premium!	000) -(Ş.	
	Fichiers réo	ents	Dossiers	Protégés								
	Fichier Nouve	au Doo	cument	Heure 19/05/20	17 13:58:13	Protégé C:\Users\Administrateur	Algorit AES-128					

Et si on regarde le fichier, on retrouve en fait maintenant à la place de notre fichier Word un fichier crypté **.axx**

Nom	Modifié le	Туре
Mouveau Document Microsoft Word-docx.axx	19/05/2017 13:58	AxCrypt

Démonter le cryptage

Si on veut rendre de nouveau un fichier accessible, sans besoin de décryptage, alors il faut demander sur le fichier un clic contextuel, puis **AxCrypt / Décrypter**

secret-docx.axx		
AxCrypt	\rightarrow	Décrypter

Et il faut faire attention car on crée alors un nouveau document de toutes pièce (avec le nom du document d'origine)

🕙 secret.docx

N.B : attention si on a renommé le fichier crypté entre temps, cela peut provoquer quelques surprises..



Ouvrir le fichier sur une autre machine

Si le logiciel AxCrypt n'est pas installé (avec le même mot de passe paramétré) alors le fichier est inutilisable.

On ne peut l'ouvrir car aucune application ne reconnait le format de fichier **axx.**

Supprimer définitivement un fichier crypté

Si on veut effacer définitivement un fichier alors il faut demander sur le fichier un clic contextuel, puis **AxCrypt / Brouiller et supprimer**

B	secret-docx.axx			
Μ	AxCrypt		>	Décrypter
	Numériser avec Windows	Defender		Ouvrir
	Ouvrir avec			Retitrez
2	IZArc	>		Avancé
۵	Rechercher les menaces			Brouiller et supprimer



VERACRYPT

Téléchargement de Veracrypt



Veracrypt s'installe de 2 façon :

• Installation complète sur une machine

Toujours possible en environnement Windows, si on a les droits. On procède dans ce cas à une vrai installation du soft sur la machine, et ensuite on s'en sert

• Installation « portable mode»

On procède dans ce cas à une unitlisation « à la volée » du fichier executable **veracrypt.exe**. Ce qui peut déclancher à chaque fois l'UAC, et parfois poser quelques problemes de compatibilité car le driver utilisé n'est pas toujours compatible.

Veracrypt peut s'utiliser de 3 manières

- Encryptage de la prtition système
- Encryptage d'une partition de données
- Création dans un fichier d'un disque dur virtuels cryptés (caché ou non)

décompacter Veracrypt 1.19

🧤 VeraCrypt Setup 1.19.exe

22/05/2017 14:45

Application

24 256 Ko

On accepte la licence









Création container crypté – fichier disque virtuel

Utilisons Veracrypt pour créer un fichier « disque dur virtuels cryptés »

On lance veracrypt via veracrypt.exe et on demande Create Volume

🖌 VeraCryp	ot					_		×
/olumes S	ystem Favorit	tes Tools	Settings	Help			Home	epag
Drive Vol L: M: N: O: P: Q: U: V: W:	ume			Size	Encryption Algorithm	Туре		
X: Y: Z: Crea	te Volume		Volume	Propert	ies	Wipe	e Cache	
Volume	Never save	history		V	✓	Sele Select	ct File Device	
Мс	unt	Auto-Mour	nt Devices		Dismount All		Exit	

Le 1° choix est le bon « create an ecrypted file container »







On donne un emplacement (ici D:\) et un nom au fichier (ici volume-crypté)

VeraCrypt Volume Creation Wizard	-		\times
	 Volume Location D:\volume-crypté Never save history A VeraCrypt volume can reside in a file (called Ve which can reside on a hard disk, on a USB flash of VeraCrypt container is just like any normal file (it moved or deleted as any normal file). Click 'Select filename for the container and to select the locat the container to be created. 	Select File eraCrypt container), irive, etc. A can be, for example t File' to choose a tion where you wish]] ;, 1

On choisit un niveau de cryptage

-	Encrypticn Options
	Encryption Algorithm
	AES V Test
	FIPS-approved cipher (Rijndael, published in 1998) that may be used by U.S. government departments and agencies to protect classified information up to the Top Secret level. 256-bit key, 128-bit block, 14 rounds (AES-256). Mode of operation is XTS.
	More information on AES Benchmark
	Hash Algorithm
VeraCrypt	SHA-512 V Information on hash algorithms



La taille du disque dynamique crypté

😉 VeraCrypt Volume Creation Wizard		-		×
	Volume Size			
	100 KB MB Free space on drive D:\ is 858.07 GB	● GB	⊖тв	
VeraCrypt	Please specify the size of the container you w	vant to crea	ate.	
	If you create a dynamic (sparse-file) container specify its maximum possible size.	r, this parar	neter will	
	Note the minimum possible size of a FAT The minimum possible size of an exFAT volum minimum possible size of an NTFS volume is 33	volume is ie is 424 KE 792 KB.	292 KB. 3. The	

Le choix du mot de passe de 20 caractères minimum est CAPITAL ! (Min, Maj, lettre , chiffre, caractère spéciaux)

Х VeraCrypt Volume Creation Wizard Volume Password Password: 2 Confirm: Use keyfiles Keyfiles... Display password Use PIM It is very important that you choose a good password. You should avoid choosing one that contains only a single word that can be found in a dictionary (or a combination of 2, 3, or 4 such words). It should not contain any names or dates of birth. It should not be easy to guess. A good password is a random combination of upper and lower case letters, numbers, and special characters, such as @ $^=$ \$ * + et + etc. We recommend choosing a password consisting of 20 or more characters (the longer, the better). The maximum possible length is 64 characters. VeraCrypt

On répond

✓ VeraCrypt Volume Creation Wizard –
 ✓ Yes
 ✓ Yes
 ✓ No
 Do you intend to store files larger than 4 GB in this VeraCrypt volume?
 Note: Depending on your choice above, VeraCrypt will choose a suitable default file system for the VeraCrypt volume (you will be able to select a file system in the next step).



Sécuriser AxCrypt VeraCrypthttp://www.cabare.netPage 28 / 38- SYS 30 Cours et T.P. - ver 1.0- Michel Cabaré -

On clique Format et on attend

VeraCrypt Volume Creation Wizard		-\
	Options Filesystem NTFS V Cluster D	lefault 🗸 🗸 Dynamic
3	Random Pool: -***+-/-+, , -* Header Key: ************ Master Key: ************	+.+*,*+,*.+-,
VeraCrypt	Done Speed IMPORTANT: Move your mouse as rat window. The longer you move it, the increases the cryptographic strength Format to create the volume.	Left Left Idomly as possible within this better. This significantly of the encryption keys. Then click
	Randomness Collected From Mouse	Movements
	Help < Back	Format Cancel
la confirmation		
VeraCrypt Volume Creation Wizard	×	
The VeraCrypt volume has been such	cessfully created.	

OK

Puis une information importante sur la gestion de ces fichiers

• La taille réelle d'un volume crypté ne s'obtient que par ses propriétés, et non pas par son affichage direct dans Windows

> Ainsi un fichier qui annonce 100 Go Peut faire réellement 89 Mo

Propr	riétés de :	volume	-crypté
Général	Sécurité	Détails	Versions précédentes
		v	olume-crypté
Type du	ı fichier :	F	chier
Descript	tion :	V	olume-crypté
Emplace	ement:	D	l:
Taille :		1(00 Go (107 374 182 400 octets)
Sur disq	ue:	8	9,3 Mo (93 716 480 octets)



On à

• Si on déplace un disque crypté sur un autre volume, il peut prendre sa taille réelle ! Si nécessaire on crée plutôt un autre volume Dynamique crypté, et ensuite on recopie les fichiers dedans !!!

Х

VeraCrypt Volume Creation Wizard

Note that the size of the dynamic container reported by Windows and by VeraCrypt will always be equal to its maximum size. To find out current physical size of the container (actual disk space it uses), right-click the container file (in a Windows Explorer window, not in VeraCrypt), then select 'Properties' and see the 'Size on disk' value.

Also note that if you move a dynamic container to another volume or drive, the physical size of the container will be extended to the maximum. (You can prevent that by creating a new dynamic container in the destination location, mounting it and then moving the files from the old container to the new one.)

Montage Volume sur container Veracrypt

Il faut maintenant monter un volume logique sur notre fichier-container précédamment construit. (c.a.d. le fichier contenant notre disque crypté)

On choisit un lecteur (ici X :) , le fichier-container (ici **volume-crypté**), et on demande **Mount**

Σc	VeraCr	/pt		*0				_		×
Vo	olumes	System	Favorites	Tools	Settings	Help			Home	oage
	Drive V L: M: N: O: P: Q: T: U: V:	olume				Size	Encryption Algorithm	Туре		^
	X: Y: Z:									~
	Cr	eate Volun	ne		Volume	Propert	ies	Wipe	Cache	
	Volume	D:\vo	olume-crypté ver save histo	ory		V	Volume Tools	Selec Select	t File Device	
[I	lount	A	uto-Moun	t Devices		Dismount All		Exit	



On donne le mot de passe

Enter password fo	or D:\volume-crypté		
Password:	•••••		ОК
PKCS-5 PRF:	Autodetection ~	TrueCrypt Mode	Cancel
	Use PIM		
	Cache passwords and keyfiles	in memory	
	Display password		
	Use keyfiles	Keyfiles	Mount Options

Et c'est fini

	-W:						
	X:	D:\volume-crypté	99 GB	AES	Normal		
	🚔 Y:						
	Z :					$\overline{\mathbf{v}}$	
L							

C'est un disque X : utilisable normalement

\leftarrow \rightarrow \checkmark \uparrow \backsim Ce PC \rightarrow Disque local (X:) \rightarrow	>			
> 🐳 data (\\nas-1) (S:)	^	Nom	Modifié le	Туре
> 🥪 Disque local (X:)		System Volume Information	22/05/2017 18:09	Dossier de fichiers

Démontage Volume sur container Veracrypt

Le démontage se fait

- automatiquement lors de l'arrêt machine,
- mais peut aussi être fait via le lacement de Veracrypt.exe, puis Dismount

₩: ₩: ₩: ₩: ¥: Z:	olume-crypté	99 GB AES	Normal
Volume	e Volume	Volume Properties	Wipe Cache
VeraCrypt	Never save history	Volume Tools	Select Device
Dismo	unt Auto-Mount D	evices Dismount All	Exit



Création Volume crypté



Il suffit dans l'assistant de demander de créer un volume Create Volume

Puis Encrypt a non system partition drive





L'assistant ensuite est similaire...



Encore faut il choisir la partiion – lecteur à crypter





Lorsque le lecteur est crée<u>, tant qu'il n'est pas « monté »</u>, il apparaît comme non formaté...

 Périphér 	iques et lecteurs (5)			
	47,1 Go libres sur 73,2 Go	-	data (D:) 174 Go libres sur 174 Go	
	doc-perso (X:) NTFS			
^{Microsoft Windows} Vous devez formater le disque c avant de l'utiliser. ऄ	Emplacement X:\n du lecteur X: Le vo systè do fi	t non disponible 'est pas accessible. plume ne contient pas de me	e système de fichiers connu. Vérifíez si tous les pilo	tes de
Voulez-vous le formater ? Formater le disq	ue Annuler	chiers necessaries sont c	narges et si le volume n'est pas endominage.	ОК

 \times

Montage Volume crypté

N.B : on ne peut plus utiliser la lette X : qui est désormais plus disponible

Donc par exemple **K** : puis **Select Device** puis **Mount**

olumes System	Favorites Tools	Settings	Help			Home	epag
Drive Volume			Size End	ryption Algorithm	Туре		
A:							
B:							
I:							
i]:							
🚔 К:							
🛁 L:							
■ M:							
■ N: → O:							
P:							
Q:							
							-
Create Volum		Volume	Properties		Wipe	e Cache	
Create Volum	ne	Volume	Properties		Wipe	e Cache	
Create Volum Volume	ne	Volume	Properties		Wipe	e Cache	
Create Volum Volume		Volume	Properties	~	Wipe	e Cache	
Create Volum Volume		Volume	Properties		Wipe	e Cache ct File	
Create Volum Volume	ne	Volume	Properties	ne Tools	Wipe Selec	e Cache ct File Device	
Create Volum Volume	ever save history	Volume	Properties Volun	ne Tools	Wipe Select	e Cache ct File Device	
Create Volum Volume	ever save history	Volume	Properties Volun	ne Tools	Wipe Select	e Cache ct File Device	
Create Volum Volume	ever save history	Volume	Properties Volun	ne Tools	Wipe Select	e Cache ct File Device Exit	



Evidemment à ce moment là le mot de passe d'encryptage est demandé

Enter password fo	or \Device\Harddisk0\Partitio	on3	
Password:	•••••		ОК
PKCS-5 PRF:	Autodetection ~	TrueCrypt Mode	Cancel
	Use PIM		
	Cache passwords and keyfiles	in memory	
	Display password		
	Use keyfiles	Keyfiles	Mount Options

Et le disque K : devient utilisable

os-systeme (C:)	data (D:)
47,1 Go libres sur 73,2 Go	174 Go libres sur 174 Go
Disgue local (K)	
Disque local (K.)	Disque local (X:)

N.B : il sera démontable comme l'est un «fichier – container », c'est-à-dire soit via Veracrypt, soit automatiquement lors de l'arrêt du poste. Ou lors de l'arrêt de la session..

Les conditions de démontages peuvent être affinées via le menu veracrypt Setting / preferences

VeraCrypt - Preferences	×
Default Mount Options	Mount volumes as removable media
VeraCrypt Background Task	Exit when there are no mounted volumes
Actions to perform upon logon to Windows Start VeraCrypt Background Task Mount all device-hosted VeraCrypt volumes	
Auto-Dismount Dismount all when: User logs off User session locked Screen saver is launched Entering power saving mode Auto-dismount volume after no data has been read/written to it for 60 minutes Force auto-dismount even if volume contains open files or directories	



SIGNATURE ET ENCRYPTAGE

Différence entre une signature, et l'encryptage :

Une signature numérique, c'est un système qui assure que l'identité de l'expéditeur est bien celle supposée, est c'est un système qui vérifie que l'intégrité du message a été respectée (autrement dit on sait que le message nous vient bien de "untel" est qu'il n'a pas été modifié " en route")

Mais un message signé numériquement reste lisible par un éventuel pirate... (non modifiable, mais lisible...). Le cryptage, permet d'éviter à une tierce personne de lire le message au passage.

Mécanisme de clé secrète (symétrique) :

La même clé est utilisée pour coder – décoder le fichier. Elle doit rester forcément secrète pour assurer la fiabilité. Environ 1000 fois plus rapide que la clé symétrique. EFS crypte les fichiers avec une clé symétrique, amis crypte cette clé symétrique avec une clé asymétrique dans les certificats...

Mécanisme de clé publique - clé privée (asymétrique):

En effet comme il est impossible de prévenir d'une interception frauduleuse des données il faut donc rendre ces informations illisibles par son intercepteur. Pour cela RSA a développé en 1977 un système de cryptage dit "a clé publique" qui répond parfaitement à ce besoin

Il est important de bien comprendre le fonctionnement d'un tel algorithme de cryptage : Cet algorithme fonctionne a l'aide de 2 clés une publique et une privée, tout phrase cryptée par la clé publique ne peut être décryptée que par la clé privée et vice-versa.



Grâce a ce principe, nous pouvons établir une transmission sécurisée (**voir schéma 1**) de Alice a Bob.

- Bob diffuse sa clé publique
- Alice crypte le message qu'elle désire envoyer à Bob avec cette clé.
- Bob pourra décrypter ce message. (et que lui)



Transmission de Alice a Bob sécurisée

N.B: Bien sur il faut s'assurer que la clé présente dans la zone publique est bien celle de Bob pour cela il existe un **mécanisme de certificat**

Il est aussi possible grâce a ce principe de signer électroniquement (**voir** schéma 2).

- En effet si Alice crypte un message avec sa clé privée
- seulement sa clé publique pourra le décrypter...
- Bob est donc sûr que c'est Alice qui a signé ce message.



Signature électronique d'Alice



Mécanisme de Certificat :

Comme nous avons vu, il n'est pas possible de garantir qu'une clé présente dans la zone publique appartient bien à la personne que vous désirez contacter de manière sécurisée. Pour cela nous avons besoin d'un tiers de confiance qui va lui assurer l'appartenance des clés publiques

Donc il vous faut impérativement un certificat. Le format des certificats est défini par la norme **X509**.

Le procédé de certification est assez simple : vous contactez **un tiers** certificateur, vous lui transmettez vos coordonnées et votre clé publique et celui-ci, après s'être assuré de la validité de ces informations, vous donne une chaîne de caractère qui est en fait le certificat crypté par la clé privée de ce **tiers** (sa signature électronique lisible avec sa clé publique...)

Donc pour récupérer votre clé publique, il faut que votre « contact » montre patte blanche auprès de **ce tiers**, afin que celui-ci le reconnaisse et lui délivre votre clé publique, c'est la rançon à payer pour être sûr de votre clé publique

Donc en fait les deux interlocuteurs doivent passer par un tiers auprès duquel il se sont enregistrés, de manière à être surs des provenances des clé publiques respectives. Ces deux interlocuteurs s'assurent de l'identité du tiers car toutes les informations qu'ils reçoivent de ce tiers (et notamment leurs clés publiques respectives) sont cryptée et décodables uniquement avec la ... clé publique du tiers !

