



Agence Nationale
de la Sécurité des
Systèmes d'Information

MÉMO : CLÉS USB

Utilisation des clés USB dans CLIP.

Mots-clés : clé usb, signature, marquage, chiffrement

Table des matières

1	Pré-requis	1
2	Rappel	1
3	Branchement d'une clé quelconque (i.e. non marquée) sur un poste CLIP	1
4	Marquage d'une clé USB	1
4.1	Principe du marquage	1
4.2	Procédure de marquage	1
4.2.1	Création de la clé cryptographique nécessaire au marquage	1
4.2.2	Marquage de la clé	2
4.3	Chiffrement d'une clé USB	2
4.3.1	Principe du chiffrement	2
4.3.2	Procédure de chiffrement	2
5	Import/Export de clé	3
5.1	Export des clés	3
5.2	Import de clés	3

Ce document est placé sous la « Licence Ouverte », version 2.0 publiée par la mission Etalab

~~DIFFUSION LIMITÉE~~

1 Pré-requis

Liste des pré-requis :

- Disposer d'un poste CLIP,
- Disposer d'une clé USB, vierge ou non, marquée ou non (le sens de "marquée" est expliqué dans la fiche).

2 Rappel

Il y a deux environnements de travail dans CLIP :

- l'environnement nommé "**0**", "**1**" ou "**RMB**" (pour Réseau de Messagerie Bas) qui à l'écran est encadré de vert, et qui est destiné à ne contenir que des informations NP.
- l'environnement nommé "**2**" ou "**RMH**" (pour Réseau de Messagerie Haut) qui à l'écran est encadré de rouge, et qui est destiné à contenir des informations au plus Diffusion Restreinte.

La possibilité de lire et d'écrire sur une clé USB dépend :

- du **niveau** (RMB ou RMH) auquel on connecte cette clé ;
- et du **marquage** ou non de la clé par le poste CLIP.

3 Branchement d'une clé quelconque (i.e. non marquée) sur un poste CLIP

Le branchement d'une clé USB quelconque (i.e. non marquée) sur un poste CLIP provoque l'affichage d'une boîte de dialogue demandant à l'utilisateur de choisir à quel niveau (RMB ou RMH) connecter la clé.

On notera que :

- connectée à **RMB**, il sera **possible de lire et d'écrire** sur la clé ;
- connectée à **RMH**, il sera **uniquement possible de lire** sur la clé, mais impossible d'y écrire.

4 Marquage d'une clé USB

4.1 Principe du marquage

Pour pouvoir écrire des données sur une clé USB depuis le niveau RMH d'un poste CLIP, il est nécessaire que celle-ci ait été « marquée » pour le poste en question. Ce marquage :

- est propre à un poste CLIP donné et à une clé USB donnée ;
- rend impossible la connexion de la clé ainsi marquée au niveau RMB ;
- entraîne, lors de la procédure de marquage, le formatage de la clé USB et ainsi la suppression des données qui s'y trouvent ;
- est invisible lorsque l'on branche la clé sur un autre système d'exploitation (ex : Windows).

Le marquage d'une clé USB permet de **contrôler l'export de données sensibles** (issues du niveau haut) vers des périphériques amovibles.

4.2 Procédure de marquage

4.2.1 Création de la clé cryptographique nécessaire au marquage

Cette étape permet de **générer des informations cryptographiques liées au poste CLIP** concerné et nécessaires au marquage d'une clé USB pour ce poste.

Cette opération **n'a besoin d'être effectuée qu'une seule fois pour le poste CLIP**, et peut ensuite servir à marquer plusieurs clés USB pour ce poste.


Si elle est répétée sur un poste CLIP alors qu'une clé USB a été déjà marquée pour ce poste, cette clé USB ne sera plus reconnue par le poste.

Cette opération **n'est pas effectuée automatiquement lors de l'installation d'un poste CLIP**, elle doit être effectuée par l'utilisateur du poste lui-même.

Dans le menu « *Périphériques amovibles* »  :

- cliquer sur « *Clés cryptographiques* » ;
- cliquer sur « *Générer les clés cryptographiques* » ;
- choisir « *Niveau haut* ».

4.2.2 Marquage de la clé

Commencer par brancher la clé USB sur le poste, mais cliquer sur « *non* » à la proposition de montage de celle-ci, puis dans le menu « *Périphériques amovibles* »  :

- cliquer sur « *Initialiser une clé USB* » ;
- cliquer sur « *Formater et signer* » ;
- choisir « *Niveau haut* ».

Attention : cette opération effacera toutes les données de la clé USB.

4.3 Chiffrement d'une clé USB

4.3.1 Principe du chiffrement

Il est possible de **chiffrer le contenu d'une clé USB** depuis un poste CLIP afin de rendre son **contenu illisible sur tout autre poste (quel qu'en soit l'OS) que le poste CLIP sur lequel elle a été formatée**.

Le chiffrement d'une clé USB permet de **protéger les données présentes sur la clé**, en ne les rendant lisibles que sur un poste donné : **si la clé USB est perdue, les données présentes sur la clé seront illisibles**.

Dans le cas d'une clé marquée mais pas chiffrée, si la clé USB est perdue, les données présentes sur la clé seront lisibles sur n'importe quel poste.

4.3.2 Procédure de chiffrement

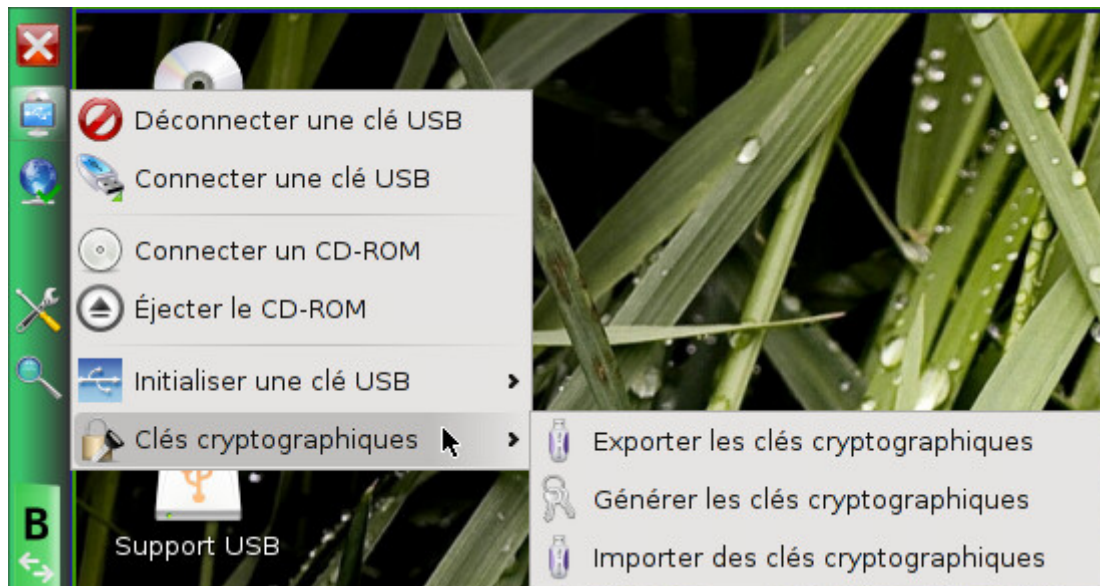
Pour cela, dans le menu « *Périphériques amovibles* »  :

- cliquer sur « *Initialiser une clé USB* » ;
- cliquer sur « *Formater et chiffrer* » ;
- choisir « *Niveau haut* ».

Cette procédure **nécessite d'avoir généré une clé cryptographique de marquage**, comme décrit à la section 2.b.i.

Attention : la répétition de cette opération fera disparaître la clé précédemment générée et rendra illisible toute clé USB chiffrée par cette dernière.

5 Import/Export de clé



5.1 Export des clés

Procédure :

- brancher une clé USB non marquée, de préférence consacrée à cet usage, **ne pas la monter sur un niveau particulier** ;
- cliquer sur *l'outil de gestion des support de stockage USB* ;
- cliquer sur « *Clés cryptographiques* » ;
- choisir « *Exporter les clés cryptographiques* ».

L'outil fournit alors un mot de passe de chiffrement généré automatiquement à conserver de manière sécurisée pour l'import futur des clés.

Les clés sont ensuite stockées sous la forme de trois fichiers au sein de la clé.

5.2 Import de clés

Procédure :

- brancher
- cliquer sur *l'outil de gestion des support de stockage USB* ;
- cliquer sur « *Clés cryptographiques* » ;
- choisir « *Importer les clés cryptographiques* ».

La clé est associée à un nom d'utilisateur. Il est possible de modifier les fichiers présents sur la clé pour s'adapter à un éventuel changement de nom d'utilisateur.

Attention Si des clés étaient déjà présentes, elles seront écrasées, rendant illisibles les supports USB chiffrés avec la clé précédente.