Agence Nationale
de la Sécurité des
Systèmes d'Information

Mémo : Rôle et gestion des certificats dans Clip

Mots-clés : certificat, infrastructure de gestion de clé, client, passerelle

Table des matières

~~DIFFUSION LIMITÉE~~

1 Pré-requis

Cette documentation ne nécessite aucun prérequis.

2 Rôle et gestion des certificats dans Clip

Le poste Clip fait utilisation d'un nombre important de certificats pour sécuriser ses communications (aussi bien IPsec que TLS). Cette section s'attache à lister les différents certificats, leurs usages et leur emplacement sur le système.

Il est à noter que le niveau de sécurité de Clip implique que le système fera confiance à aucune autorité de certification par défaut pour les fonctionnalités IPsec et les tunnels TLS. En d'autres termes, il n'y a pas, pour ces applications du système de magasin de certificats. Les autorités de certifications donc être placée dans le système, soit via le profil d'installation, ou après l'installation via les procédures adéquates.

Les certificats utilisés par les applicatifs (authentification client sur un navigateur Web par exemple) ne seront pas ici abordés.

A noter que certaines IGC délivrent les certificats au format *PKCS#12* ou *PFX*. Il est important de convertir ces certificats au format PEM pour leur utilisation dans Clip. Cela peut être réalisé via la commande *OpenSSL*.

2.1 Certificats pour les tunnels IPsec

Il s'agit de certificat qui sont utilisés pour la réalisation des tunnels IPsec. Ils peuvent porter les noms suivants [1] :

- « gw.pem » (partie publique) et « gw.key » (partie privée) : utilisé par le tunnel qui accueille les clients (sur une passerelle uniquement) ;
- « rmh.pem » (partie publique) et « rmh.key » (partie privée) : utilisé par le tunnel niveau haut (sur un client uniquement) ;
- « rmb.pem » (partie publique) et « rmb.key » (partie privée) : utilisé par le tunnel niveau bas (sur un client uniquement) ;
- « audit.pem » (partie publique) et « audit.key » (partie privée) : utilisé par le tunnel associé à la cage « AUDIT » ;
- « admin.pem » (partie publique) et « admin.key » (partie privée) : utilisé par le tunnel associé à la cage « ADMIN » ;
- « update.pem » (partie publique) et « update.key » (partie privée) : utilisé par le tunnel de mise à jour.

La partie clé privée doit absolument être au format **RSA PRIVATE KEY**.

Ces certificats se trouvent dans le répertoire « /etc/admin/ike2/cert » depuis une cage « ADMIN ». Ils peuvent être remplacés à chaud depuis la cage « ADMIN » via la commande « install_ccsd ». Il n'est pas possible de les éditer autrement. Notament, il n'est pas possible de lire leur contenu pour éviter toute extraction.

2.2 Autorités de certification pour les tunnels IPsec

Les autorités certifications sont nécessaires pour qu'un client puisse valider une passerelle, et inversement. Ces autorités ne sont pas nécessairement les mêmes sur un couple client/passerelle. Ainsi, un client peut ne posséder une autorité de certification pour sa passerelle, mais n'a pas beosin de

1. Il s'agit ici des noms des certificats en cas d'utilisation de cryptographie civile. Le poste Clip est également capable d'utiliser la cryptographie gouvernementale. Dans ce cas, le nom des certificats diffère.

pouvoir l'autorité de certification qui a émis ses certificats. Ces certificats se trouvent dans le répertoire « /etc/ike2/cert ». Celui-ci n'est accessible que depuis un installeur.

Le remplacement des autorités de certification n'est pas prévu à chaud, et doit donc se faire depuis un installeur. Il est important de placer les bons droits lors de la création des fichiers.

2.3 Certificat client pour la mise à jour via HTTPS

Ce certificat se trouve dans le répertoire « /etc/admin/clip_download/private » de la cage « ADMIN ». La partie publique doit porter le nom « apt.cert.pem » et la partie privée le nom « apt.key.pem ».

Ces fichiers sont éditables via les méthodes habituelles et peuvent être librement écrasés (depuis la cage « ADMIN »).

2.4 Autorités de certification pour la mise à jour via HTTPS

Ce certificat se trouve dans le répertoire « /etc/admin/clip_download/cacerts » de la cage « ADMIN ». Ces fichiers sont éditables via les méthodes habituelles et peuvent être librement écrasée (depuis la cage « ADMIN »).

A noter que ce répertoire contient également des liens symboliques qu'il convient de rafraichir lors de l'ajout de nouveaux certificats via la commande « c_rehash ».

2.5 Certificat utilisateur pour l'utilisation de tunnel TLS (stunnel)

Les certificats utilisateurs se trouvent dans le répertoire « .vault » du répertoire maison de l'utilisateur. Ce répertoire ne lui est toutefois pas accessible et les opérations sur les certificats se font via la commande « vault ». Cela permet d'éviter l'extraction du certificat par un utilisateur. Cette commande à deux rôles :

- fournir les certificats à *stunnel* lors de son lancement ;
- injecter des nouveaux certificats utilisateur.

2.6 Autorités de certification pour l'utilisation de tunnel TLS (stunnel)

Les répertoires « /etc/admin/rm_h/tls/cacerts » et « /etc/admin/rm_b/tls/cacerts » sont utilisés quand le programme *stunnel* fait parti de la distribution Clip. L'ajout de certificat dans ce répertoire peut se faire via la cage « ADMIN » et nécessite de rafraichir les liens symboliques via la commande « c_rehash ».

3 Mécanisme de protection des certificats

Lors de son fonctionnement, les certificats sont protégés par les mécanismes de cloisonnement et accessibles depuis un nombre minimal de compartiments afin de limiter leurs expositions à un attaquant. D'un point de vue disque, toutefois, les choses sont plus simple. Selon l'usage, un certificat peut être situé :

- sur l'une des partitions systèmes ; celle-ci peut alors être protégée par la fonction de chiffrement du disque (qui peut être choisie durant l'installation) ;
- sur l'un des partitions utilisateurs ; le secrêt est alors protégé par le mot de passe de l'utilisateur ou la carte à puce (quand celle-ci est activée pour le login).

Il est donc important de noter que les certificats peuvent être située sur une zone exposée du poste (si aucun chiffrement n'est choisi durant l'installation) et donc facilement extractible.

Le tableau suivant liste les emplacements des différents certificats sur un poste Clip.

Nom du certificat	*Emplacement*	*Lisible depuis par un utilisateur*	*Modifiable à chaud*
Certificats IPsec	système	non	oui
Certificat client pour mise à jour via HTTPS	système	oui	oui
Certificat pour l'utilsation de TLS dans une cage utilisateur	cage utilisateur	non	oui