Documentation CLIP

2001

Procédure d'installation

Version	Date	Auteur	Commentaires
1.1.0	18/11/2009	Vincent Strubel	Mise à jour pour CLIP4 (*clip-installer-2.5.1*).
1.0.5	10/02/2009	Vincent Strubel	Prise en compte de remarques AQL (FDC17) : ajout de l'annexe A sur les exigences de sécurité sur l'environnement, ajout de précisions sur les arguments de *full-install.sh*.
1.0.4	03/02/2009	Vincent Strubel	Prise en compte de remarques AQL (FDC16) : matériel sur lequel se fait l'installation nominale, et avertissement sur les installations personnalisées.
1.0.3	09/10/2008	Vincent Strubel	Compléments sur la vérification d'intégrité des supports et de la version installée par un support.
1.0.2	29/09/2008	Vincent Strubel	Convention plus lisible pour les références.
1.0.1	29/08/2008	Olivier Levillain	Mise à jour de détails concernant les scripts d'installation.
1.0	20/06/2008	Vincent Strubel	Version initiale, adaptée pour CLIP v.03.00.02 (et *clip-installer* version 1.10).

Table des matières

Introduction

Le présent document décrit, à destination des administrateurs et intégrateurs de réseaux CLIP, les procédures à appliquer pour installer de manière sécurisée un poste CLIP, à partir d'un support d'installation de type CD-ROM / DVD-ROM ou clé USB. Deux cas sont distingués : soit l'administrateur d'un réseau CLIP procède lui-même à l'installation et à la configuration des postes CLIP qu'il déploie (procédure décrite en section 2), soit cet administrateur délègue à un intégrateur tierce-partie l'essentiel du travail d'installation et de configuration initiale des postes CLIP, en employant une procédure adaptée permettant de ne pas communiquer à l'intégrateur les éléments secrets de la configuration de chaque poste (procédure décrite en section 3).

1 Principe des procédures d'installation

1.1 Définitions

Outre les paquetages, communs à tous les postes CLIP d'une configuration donnée, chaque poste CLIP est composé d'un ensemble de Paramètres et de Données. La distinction entre ces deux derniers éléments est établie par convention comme suit :

- Un **Paramètre** est un élément propre à un poste CLIP donné, qui peut être initialisé par des données externes au poste lors de l'installation de ce poste (mais qui reste éventuellement susceptible d'évoluer après l'installation). Par exemple, les clés d'authentification IPsec, les clés de vérification de signatures de paquetages, le fichier de configuration des adresses IP et la définition des comptes utilisateurs sont tous des Paramètres de chaque poste CLIP.
- Une **Donnée** est un élément propre à un poste CLIP donné, qui ne peut pas être initialisé lors de l'installation de ce poste. Les Données ne peuvent être générées ou importées sur un poste CLIP qu'en cours d'utilisation normale du poste, après l'installation. Il s'agit par exemple des données manipulées par les utilisateurs, mais aussi des clés privées[1] associées aux comptes utilisateurs, qui ne sont pas manipulables directement par ces comptes et sont uniquement générées sur le poste CLIP lui-même.

La catégorie des Paramètres est par ailleurs sub-divisée selon les caractéristiques suivantes :

- Un **Paramètre Secret** est un paramètre qui doit être protégé en confidentialité vis-à-vis de la plupart des acteurs (cf. 1.2).
- Un **Paramètre Intègre** est un paramètre qui ne peut pas être modifié au sein du système pendant le fonctionnement normal de celui-ci[2]. Ainsi, un Paramètre Intègre ne peut être défini que lors de l'installation du système.

Un Paramètre pourrait naturellement être à la fois Intègre et Secret, bien que le système CLIP ne comporte aucun tel paramètre à ce stade. Par défaut, un Paramètre est supposé non Intègre (c'est-à-dire modifiable après l'installation du poste, dans la plupart des cas par un Administrateur du Poste – cf. 1.2) et non Secret (on pourra également préciser « Paramètre Public » en cas d'ambiguité).

1.2 Rôles

La procédure d'installation CLIP distingue plusieurs types d'acteurs, ou rôles, caractérisés notamment par des besoins d'en connaître différents vis-à-vis des éléments secrets installés sur le poste CLIP. Ces rôles sont les suivants :

- **Fabricants** : fabricants des postes matériels sur lesquels doivent être installés les systèmes CLIP, postes qu'ils fournissent aux Administrateurs de Réseaux ou aux Intégrateurs. Ils sont

[1] Clés de signature et de chiffrement de supports amovibles USB, ou encore clés d'authentification SSH pour les profils administrateurs ou auditeurs.

[2] Il reste cependant théoriquement possible (bien que cela ne soit pas fait dans la pratique) de modifier tout Paramètre Intègre, de manière non interactive, durant une mise à jour du système. Une telle modification ne peut être réalisée que par un paquetage, et est donc réservée aux Développeurs et Validateurs.

supposés de confiance pour la fourniture de postes matériels intègres (y compris les BIOS et *firmwares*), mais n'ont en aucun cas à manipuler les supports d'installation CLIP, ni à accéder aux Paramètres et Données des systèmes CLIP.

- **Développeurs** : ils sont chargés du développement de CLIP, de la génération et de la signature « Développeur » (cf. [CLIP_DCS_12007]) des paquetages binaires, et de la génération du CD-ROM d'installation (cf. [CLIP_1102]). Ils sont supposés de confiance (sous réserve d'un contrôle par les Validateurs), vis-à-vis de tous les déploiements CLIP, pour la production de paquetages et de supports d'installation intègres, mais n'ont pas à connaître les Paramètres Secrets ni les Données des postes CLIP.

  Les Développeurs sont des personnels habilités au niveau Confidentiel Défense, de nationalité française.

- **Validateurs** : ils sont chargés du contrôle et de la validation des paquetages binaires produits par les Développeurs. Cette validation est concrétisée, dans le cas des paquetages binaire, par l'apposition d'une deuxième signature dite « Validateur » (cf. [CLIP_DCS_12007]). Les Validateurs sont par ailleurs seuls habilités à remettre les supports d'installation produits par les Développeurs aux Administrateurs de Réseaux et aux Intégrateurs. Ils sont supposés de confiance, vis-à-vis de tous les déploiements CLIP, pour la fourniture de paquetages et de supports d'installation intègres, mais n'ont pas à connaître les Paramètres Secrets ni les Données des postes CLIP.

  Les Validateurs sont des personnels habilités au niveau Confidentiel Défense, de nationalité française.

- **Administrateurs de Réseaux** : ils sont en charge d'un réseau de déploiement CLIP, comportant plusieurs postes clients, au moins une passerelle et un serveur de mise à jour CLIP, ainsi que les serveurs de services (messagerie, *web*, annuaire, etc...) et éventuelles passerelles associés au déploiement. Ils sont responsables de la génération des Paramètres d'installation (Secrets et Publics), et sont seuls habilités à manipuler en clair ces éléments pour l'ensemble des postes de leur réseau. Ils peuvent par ailleurs être directement responsables de l'installation des postes CLIP de leur réseau, ou alternativement déléguer cette tâche à des Intégrateurs. Dans ce dernier cas, ils sont seuls habilités à fournir les Paramètres Publics d'Installation aux Intégrateurs. Les Administrateurs de Réseaux sont supposés de confiance, vis-à-vis du déploiement CLIP dont ils ont la responsabilité, pour la fourniture de postes CLIP installés intègres (y compris les Paramètres d'installation) aux Administrateurs de Postes, et pour le maintien de la confidentialité[3] des Paramètres Secrets d'installation. Ils n'ont en revanche pas à connaître les Données des postes CLIP de leur déploiement.

  Les Administrateurs de Réseaux sont des personnels habilités au niveau Confidentiel Défense, de nationalité française.

- **Intégrateurs** : ils peuvent être chargés par les Administrateurs de Réseaux de l'installation de postes CLIP. Ils reçoivent dans ce cas les supports d'installation des Validateurs, et les Paramètres (Publics) d'installation des Administrateurs de Réseaux. Ils sont supposés de confiance, vis-à-vis des déploiements CLIP pour lesquels ils réalisent l'installation, pour le maintien de l'intégrité des postes CLIP (y compris leurs Paramètres d'installation) qu'ils installent, et fournissent aux Administrateurs de Réseaux.

[3] On notera qu'il est ici question de la confidentialité en dehors du périmètre propre au système CLIP, qui met en oeuvre des mesures techniques spécifiques pour maintenir cette confidentialité en son sein.

Les Intégrateurs sont des personnels habilités au niveau Confidentiel Défense, de nationalité française.

- **Administrateurs de Postes** : ils sont en charge de l'administration locale, après installation, d'un ou plusieurs postes CLIP au sein d'un déploiement donné. Ils reçoivent les postes pré-installés des Administrateurs de Réseaux de leur déploiement, et sont chargés de la gestion des Paramètres de ces postes. Ils disposent d'un compte utilisateur, avec le profil administrateur (*core_admin*) ou utilisateur privilégié (*priv_user*)[4], sur chacun des postes CLIP dont ils ont la charge. Ils sont habilités à manipuler en clair les Paramètres Secrets de ces postes, et disposent en général de ces éléments (clés privées d'export USB en particulier). Ils sont supposés de confiance pour le maintien de la confidentialité de ces Paramètres Secrets, et pour le maintien de l'intégrité physique des postes qu'ils manipulent. Ils n'ont en revanche pas à connaître les Données des Utilisateurs, en dehors de celles manipulées par leur propre compte utilisateur au sein du système. Ils ne sont de plus pas considérés de confiance pour la modification des Paramètres des postes CLIP, ces derniers assurant par des mesures techniques le maintien de leurs propriétés de sécurité même en présence de Paramètres inadaptés.
- **Auditeurs de Postes** : ils sont en charge de la supervision locale d'un ou plusieurs postes CLIP au sein d'un déploiement donné. Ils reçoivent les postes pré-installés des Administrateurs de Postes, qui créent pour eux un compte utilisateur, avec le profil auditeur (*core_audit*) ou utilisateur privilégié (*priv_user*). Ils sont supposés de confiance pour le maintien de l'intégrité physique des postes CLIP qu'ils manipulent, mais n'ont pas à connaître les Paramètres Secrets, ni les Données des autres utilisateurs.
- **Utilisateurs** : ils sont les utilisateurs des postes CLIP au sein d'un déploiement donné. Ils reçoivent les postes pré-installés des Administrateurs de Postes, qui créent pour eux un compte utilisateur, avec le profil utilisateur, ou utilisateur nomade (*nomad_user*), ou encore utilisateur privilégié (*priv_user*). Ils sont supposés de confiance pour le maintien de l'intégrité physique des postes CLIP qu'ils manipulent, mais n'ont pas à connaître les Paramètres Secrets, ni les Données des autres utilisateurs.

1.3 Infrastructures de Gestion de Clés

Plusieurs infrastructures de gestion de clé (IGC) interviennent dans la configuration d'un poste CLIP. Ces IGC sont, selon leur utilisation, sous la responsabilité de différents rôles.

1.3.1 IGC Développeur

Cette IGC ACID (cf. [CEC_ACID]) fournit les clés de signature « Développeur » des paquetages (cf. [CLIP_DCS_12007]). Elle est commune à tous les déploiements CLIP, et sous la responsabilité d'un acteur spécifique, choisi parmi les Développeurs. Les clés privées de cette IGC ne sont fournies qu'aux Développeurs, à raison d'une clé valide par Développeur actif. Ces derniers sont responsables de la confidentialité de leurs clés individuelles. L'IGC Développeur fournit de plus une clé de vérification de

[4] Les comptes « utilisateurs privilégiés » combinent sous une seule identité les privilèges d'Administrateur de Poste, d'Auditeur de Poste et d'Utilisateur. La mise en oeuvre de tels types de comptes est normalement à réserver à des postes mono-utilisateur.

signature (permettant uniquement la vérification, et non la création, de signature) qui est déployée sur chaque poste CLIP comme un Paramètre Intègre.

1.3.2 IGC Validateur

Cette IGC ACID (cf. [CEC_ACID]) fournit les clés de signature 'Validateur' des paquetages (cf. [CLIP_DCS_12007]). Elle est commune à tous les déploiements CLIP, et sous la responsabilité d'un acteur spécifique, choisi parmi les Validateurs. Les clés privées de cette IGC ne sont fournies qu'aux Validateurs, à raison d'une clé valide par Validateur actif. Ces derniers sont responsables de la confidentialité de leurs clés individuelles. L'IGC Validateur fournit de plus une clé de vérification de signature (permettant uniquement la vérification, et non la création, de signature) qui est déployée sur chaque poste CLIP comme un Paramètre Intègre.

1.3.3 IGC IPsec

Cette IGC ACID (cf. [CEC_ACID]) fournit les clés d'authentification IPsec (IKEv2) des clients et passerelles CLIP. Elle est spécifique à un déploiement CLIP, et sous la responsabilité des Administrateurs de Réseau de ce déploiement. L'IGC IPsec fournit une clé privée d'authentification pour chaque poste CLIP, installée comme un Paramètre Secret sur ce poste. Par ailleurs, la clé publique de chaque passerelle est installée , comme un Paramètre Intègre, sur tous les clients et passerelles qui ont à établir des associations IPsec avec cette passerelle. Enfin, sur chaque passerelle, les clés publiques de tous les clients et passerelles avec lesquels la passerelle doit établir des associations IPsec sont installés comme de simples Paramètres (ni Secrets, ni Intègres).

La mise en oeuvre d'une IGC IPsec n'est nécessaire que dans le cas de déploiements en ligne (postes CLIP connectés au réseau, établissant des tunnels IPsec pour le téléchargement de leur mises à jour ou l'accès à des réseaux de service), elle n'est pas requise dans le cas de postes déployés hors-ligne, ou de postes déployés en ligne mais sans mise en oeuvre d'IPsec (pas de mises à jour en ligne).

1.3.4 IGC HTTPS

Cette IGC *Openssl* (cf. [IGC_OPENSSL]) fournit les clés et certificats d'authentification des serveurs de service (mises à jour, messagerie, web, annuaire, etc...) d'un déploiement CLIP. Elle est propre à un déploiement, et sous la responsabilité des Administrateurs de Réseau de ce déploiement. Elle fournit une clé privée d'authentification par service du déploiement (au minimum, une clé pour le service de téléchargement de mises à jour). Le certificat associé à l'autorité de certification de l'IGC HTTPS est installé comme un Paramètre (ni Secret, ni Intègre) sur chaque poste CLIP.

La mise en oeuvre d'une IGC OpenSSL n'est nécessaire que dans le cas de déploiements en ligne (postes CLIP connectés au réseau, réalisant leurs mises à jour en ligne), elle n'est pas requise dans le cas de postes déployés hors-ligne, ou de postes déployés en ligne mais sans mise en oeuvre de SSL (pas de mises à jour en ligne).

1.3.5 Clés d'export USB

Ces clés, permettant l'export des clés de chiffrement et d'authentification de supports amovibles USB,

ne sont pas gérées par une IGC, mais sont générées comme de simples bi-clés RSA. Leur génération est à la charge des Administrateurs de Réseau de chaque déploiement, à raison d'un bi-clé par poste et par niveau (soit un par poste pour CLIP-single ou CLIP-GTW, et trois par poste pour CLIP-RM, par exemple). Seules les parties publiques de ces bi-clés sont installées sur les postes CLIP, comme des Paramètres Intègres. Les parties privées des bi-clés de chaque poste sont communiquées par d'autres moyens à tous les utilisateurs de ce poste (Administrateurs de Postes, Auditeurs et Utilisateurs). La génération d'un bi-clé d'export peut être réalisée à l'aide des commandes suivantes sur un poste Linux (les utilitaires *ssh-keygen* et *openssl* étant fournis respectivement par *openssh* et *openssl*) :

```
PASS="$(tr -cd [:graph:] < /dev/urandom | head -c 12)"
echo -n "${PASS}"  > "<niveau>.pwd"
ssh-keygen -t rsa -b 2048 -C "<niveau>@clip" \
           -N "${PASS}" -f "<niveau>.prv"
openssl rsa -in "<niveau>.prv" -pubout \
           -out "<niveau>.pub" -passin pass:"${PASS}"
rm -f "<niveau>.prv.pub"
```

avec *<niveau>* le niveau du bi-clé (*clip* pour le socle, *rm_h* pour RM_H, etc...). Les deux premières lignes créent un mot de passe aléatoire de douze caractères, la suivante crée une clé privée RSA de 2048 bits, protégée par ce mot de passe, la quatrième ligne crée la clé publique, et la cinquième supprime une clé publique temporaire.

Après cette séquence de commandes, le fichier *<niveau>.pub* contient la clé publique d'export, installable sur le poste CLIP, tandis que les fichiers *<niveau>.prv* et *<niveau>.pwd* contiennent respectivement la clé privée et son mot de passe, qui doivent être communiqués à tous les utilisateurs du poste, mais pas installés sur le poste lui-même. Voir aussi [CLIP_1306] pour l'utilisation qui est faite de ces clés par le système.

1.4 Scripts d'installation et arborescences de configuration

1.4.1 Support d'installation, scripts d'installation

Le support d'installation CLIP se présente normalement comme un CD-ROM / DVD-ROM ou clé USB apparenté à un *Live CD Gentoo*, sur lequel il est possible de démarrer et d'obtenir une console sous l'identité *root*. Le support d'installation incorpore notamment un ou plusieurs « miroirs » CLIP, constitués chacun d'un ensemble de paquetages CLIP indexés selon le format de miroir *Debian*. Chaque miroir permet l'installation d'une configuration CLIP complète. De plus, le support d'installation inclut plusieurs scripts spécifiques qui peuvent être lancés depuis la console *root* du support, pour procéder à une installation complète. Les deux principales commandes sont les suivantes :

- *aide* fournit une aide en ligne concernant la procédure d'installation.
- *full-install.sh -t <type> -c <config> -H <matériel> <device(s)>*, avec *<type>* le type de configuration (*rm, gtw-update, gtw-rmh, single*) à installer, *<config>*, le répertoire contenant la configuration du poste client ou de la passerelle à installer, *<matériel>* le nom de la configuration matérielle et *<device(s)>* le ou les périphériques[5] où installer CLIP. Ce script

[5] Dans le cas d'une installation d'une passerelle CLIP, deux disques de même taille et de même géométrie sont nécessaires

procède à une installation complète, en réalisant successivement :

- Le partitionnement du disque dur du poste, en déterminant automatiquement les tailles de partitions optimales pour la taille du disque concerné. Le disque est intégralement utilisé pour CLIP, et partitionné de manière à supporter l'installation de deux systèmes CLIP complets, partageant leurs données (ce qui permet de garantir la disponibilité dans tous les cas d'un système « de secours », en cas par exemple de mise à jour interrompue du système).
- Le formatage des partitions du disque dur.
- L'installation d'un premier système CLIP complet, et sa configuration initiale en important différents Paramètres depuis une arborescence de configuration (voire plus bas).
- L'installation d'un deuxième système CLIP, reprenant la configuration du premier, sur un jeu de partitions alternatif.
- L'installation d'un chargeur de démarrage, permettant à l'utilisateur de démarrer par défaut sur la première installation CLIP, ou en option sur la deuxième.

Alternativement à *full-install.sh*, le support d'installation permet de réaliser des installations personnalisées, en invoquant directement et avec des options supplémentaires les scripts de plus bas niveau qui réalisent les différentes étapes du traitement de *full-install.sh*. Ces installations personnalisées permettent en particulier :

- D'installer CLIP en utilisant un miroir disponible par le réseau plutôt que celui intégré au support. *Cette approche est normalement réservée au développement et au test du système CLIP, et ne doit pas être employée, pour des raisons de sécurité, sur un poste de production.*
- D'installer CLIP sur un matériel non spécifiquement supporté par le système, en créant directement une nouvelle configuration matérielle.

Le lecteur est invité à se référer à l'aide en ligne du support d'installation (commande *aide*) pour connaître le détail de ces possibilités d'installation personnalisée.

Dans tous les cas, l'étape d'installation utilise, pour la configuration initiale des Paramètres des systèmes CLIP installés, une arborescence de fichiers de configuration qui est cherchée dans le chemin <*config*> passé par l'option *-c* de *full_install.sh,* et une configuration matérielle (liste de pilotes à charger au démarrage, paramétrage de l'affichage par défaut), définie par le nom <*matériel*> passé par l'option *-H*. Le détail de la constitution de l'arborescence de configuration est donné en 1.4.2. L'arborescence de configuration est spécifique à une installation de poste CLIP donnée, et n'est pas souvent pas incluse sur le support d'installation lui-même. Elle est généralement importée à l'aide d'un support amovible dédié, qui est typiquement monté sur */root/removable* dans l'environnement du support d'installation.

Une installation complète à l'aide de *full_install.sh* dure environ 25 minutes.

pour installer CLIP, puisque les partitions seront créées en RAID 1.

1.4.2 Arborescence de configuration

L'arborescence de configuration peut contenir un certain nombre de fichiers et répertoires prédéfinis, correspondant à autant de Paramètres du système CLIP. On notera que l'absence de certains fichiers n'est pas nécessairement problématique : dans ce cas, le système CLIP après installation sera dépourvu de certains fichiers de configuration, ou utilisera les fichiers de configuration par défaut fournis par les paquetages. La plupart de ces fichiers de configuration peuvent être modifiés par l'Administrateur du Poste après l'installation, à l'exception des Paramètres Intègres. L'absence d'un Paramètre Intègre de l'arborescence de configuration entraînera la perte irrémédiable de certaines fonctionnalités pour le système CLIP ainsi installé. Les fichiers d'une arborescence de configuration sont répartis entre deux sous-répertoires principaux :

- *conf/* pour les Paramètres non Intègres
- *params/* pour les Paramètres Intègres

Les fichiers de Paramètres non Intègres supportés sont les suivants :

- *conf/cert/cacert.pem* : certificat de l'autorité de certification de l'IGC HTTPS ([IGC HTTPS]), au format PEM.
- *conf/clip-download/** : répertoire de configuration des téléchargements de mises à jour. Tous les fichiers de ce répertoire sont installés dans le répertoire */etc/admin/clip_download* de l'arborescence CLIP. Les fichiers présents dans ce répertoire doivent comporter a minima les fichiers de définitions de sources de mises à jour (fichiers *sources.list.**) pour les différentes distributions installées sur le poste CLIP : *sources.list.clip* sur tous les types de postes, auquel s'ajoutent *sources.list.rm_b* et *sources.list.rm_h* sur un poste CLIP-RM. On pourra facultativement y ajouter un fichier *clip_download.conf*, déterminant si le téléchargement de mise à jour doit être réalisé une première fois pendant le démarrage du poste (le fichier par défaut désactive ce téléchargement initial, ce qui est généralement préférable), ainsi que des fichiers *clip_download_<cage>.conf* (avec *<cage>* égal à *clip, rm_b* ou *rm_h*) définissant les paramètres de rejets de configurations trop vieilles ou trop jeune pour chaque distribution (le paramétrage par défaut est généralement adapté).
- *conf/admin_ike2_cert/** : tous les fichiers de ce répertoire sont installés dans */etc/admin/ike2/cert/* au sein de l'arborescence CLIP. On placera dans ce fichier les clés CCSD d'authentification IPsec (et leurs mots de passe dans le cas de clés privées) qui ne constituent pas des Paramètres Intègres du poste. En particulier, la clé privée d'authentification IPsec du poste et son mot de passe (Paramètres Secrets) pourront être placés dans ce répertoire (dans le cas d'une installation par l'Administrateur de Réseau uniquement, cf. 2 et 3), dans des fichiers *ccsd.pvr* et *ccsd.pwd* respectivement. Ces clés doivent être au format KLNv2, tel que généré par le CEC ACID ([CEC_ACID]).
- *conf/logfiles* : configuration de la rotation des fichiers de journaux au démarrage (taille minimale déclenchant la rotation, nombre d'archives à conserver) (optionnel).
- *conf/ntp* : configuration de la synchronisation horaire NTP (optionnel).
- Pour un poste CLIP-RM uniquement :

- *optional.rm_b* : liste (un par ligne) de noms de paquetages optionnels à installer initialement sur le poste dans la cage RM_B. On pourra placer dans ce fichier des noms de paquetages qui pourraient également être sélectionnés ultérieurement dans l'interface de gestion des mises à jour du poste CLIP après installation.
- *optional.conf.rm_h* : idem pour RM_H.

- *conf/netconf.d/default/** : fichiers de la configuration réseau par défaut qui doit être définie. L'organisation d'une telle configuration est décrite ci-dessous.
- *conf/netconf.d/<conf>/** : autres configurations réseau prédéfinies, optionnelles, organisées de la même manière que la configuration par défaut.

Chaque répertoire de configuration réseau, placé dans *conf/netconf.d/<conf>* (y compris la configuration *default*) doit à son tour contenir les fichiers suivants (dont les contenus sont détaillés dans le document de référence [CLIP_1501]) :

- *net* : configuration de l'adressage (obligatoire)
- *netfilter* : configuration du pare-feu (obligatoire)
- *hostname* : configuration du nom d'hôte (obligatoire)
- *hosts* : résolution de nom statique pour le socle et les cages CLIP (obligatoire)
- *resolv.conf* : résolution de nom dynamique pour les cages CLIP (optionnel)
- *umts* : configuration d'une connexion téléphonique 3G (optionnel)
- *wireless* : configuration d'une connexion *Wifi* (optionnel)
- optionnellement, pour chaque cage RM *rm_X* (*rm_b* ou *rm_h*) d'un poste CLIP-RM
  - *rm_X/hosts* : résolution de nom statique pour la cage *rm_X* (optionnel)
  - *rm_X/proxy* : configuration des proxys (HTTP, HTTPS, …) pour la cage *rm_X* (optionnel)
  - *rm_X/resolv.conf* : résolution de nom dynamique pour la cage *rm_X* (optionnel)

Par ailleurs, l'arborescence de Paramètres Intègres supportés est la suivante :

- *params/ike2_cert/* : tous les fichiers de ce répertoire sont installés dans */etc/ike2/cert/* au sein de l'arborescence CLIP. On placera dans ce répertoire les clés publiques CCSD d'authentification IPsec qui constituent des Paramètres Intègres du poste, c'est-à-dire les clés publiques des passerelles avec lesquelles ce poste sera amené à dialoguer. Ces clés doivent être au format KLNv2, tel que généré par le CEC ACID ([CEC_ACID]).
- *params/chroot-commands* : liste de commandes (à raison d'une par ligne) à lancer (moyennant un appel *chroot*) au sein de la première installation CLIP (premier jeu de partitions) à la fin de l'installation de cette dernière. Peut typiquement être utilisé pour créer des comptes utilisateurs initiaux au sein du système. Les utilitaires disponibles à cette fin sont décrits plus en détail dans le paragraphe « Commandes lancées dans l'arborescence CLIP » ci-dessous.
- *params/chroot-commands-noconf* : liste de commandes similaire à *chroot-commands*, mais lancées cette fois dans la deuxième installation CLIP (deuxième jeu de partitions). Dans la mesure où cette deuxième installation reprend automatiquement l'essentiel de la configuration de la première installation, ce fichier peut généralement être laissé vide.

- *params/usb_keys/* : on placera dans ce répertoire les clés publiques d'export USB (cf. 1.3.5) du poste, à raison d'une par niveau (*clip.pub* dans tous les cas, plus *rm_h.pub* et *rm_b.pub* pour un poste CLIP-RM).
- *params/update_keys/* : on placera dans ce répertoire les clés de vérification de signatures de paquetages pour les IGC Développeur et Validateur (au format généré par le CEC lors d'un export des clés de vérification), ainsi que leur mots de passe, dans les fichiers suivants :
  - *dev.bin* : clé de vérification Développeur
  - *dev.bin.txt* : mot de passe de la clé de vérification Développeur
  - *ctrl.bin* : clé de vérification Validateur
  - *ctrl.bin.txt* : mot de passe de la clé de vérification Validateur
- *params/usbkeys.conf* : fichier de paramétrage de la gestion des supports amovibles (niveaux dans lesquels des supports non chiffrés ou non initialisés sont autorisés). Voir aussi [CLIP_1306].
- *params/conf.d/printers* : fichier de paramétrage de la gestion des imprimantes USB (chemins sous lesquels les périphériques de ce type sont exposés dans les différentes cages lors de leur branchement).
- *params/conf.d/sound* : fichier de paramétrage de la gestion de la carte son (chemins sous lesquels les périphériques associés à la carte son sont exposés dans les différentes cages lors du démarrage du poste).
- *params/conf.d/usermgmt* : fichier de paramétrage de la gestion des utilisateurs : autorisation ou non de la création de comptes de type Utilisateur Privilégié ou Utilisateur Nomade.

Commandes lancées dans l'arborescence CLIP

Les commandes utilisées dans le fichier de configuration *conf/chroot_commands-<type>* peuvent en particulier faire appel, outre les utilitaires standard UNIX installés dans le socle CLIP, à deux scripts spécifiques facilitant la création de comptes utilisateurs.

Le script ***usermod.sh*** permet de définir le mot de passe d'un utilisateur dont le compte a déjà été créé (typiquement par une commande *useradd*), en en stockant l'empreinte au format spécifique à CLIP. Il peut être invoqué sous la forme suivante :

```
usermod.sh <login> <pass> <rounds>
```

avec :

- *<login>* le nom du compte utilisateur
- *<pass>* le mot de passe à attribuer au compte
- *<rounds>* le degré de complexité du hachage à employer pour générer l'empreinte du mot de passe. La valeur conseillée est 12. Les valeurs inférieures à 12 sont à proscrire, tandis que des valeurs supérieures peuvent être choisies, pour une sécurité accrue, en portant attention au fait que le temps de vérification d'un mot de passe augmente exponentiellement en fonction de ce nombre.

Le script *makehome.sh* permet de créer et d'initialiser (notamment en créant les éventuelles clés de ré-

authentification SSH) les partitions de données chiffrées d'un utilisateur. Il peut être invoqué sous la forme suivante :

```
makehome.sh [-z] [-P <ssh-pass>] [-t <type>] [-s <taille>] -p <pass> <login>
```

avec :

- <*login*> le nom du compte utilisateur
- <*pass*> le mot de passe du compte utilisateur (doit être le même que celui passé à *usermod.sh*)
- <*taille*> la taille des partitions à créer, en Mo (16 par défaut)
- <*type*> le type de compte (*user* par défaut) :
  - *admin* pour un compte administrateur CLIP
  - *audit* pour un compte auditeur CLIP
  - *rm_admin* pour un compte administrateur RM (CLIP-RM uniquement)
  - *user* pour un compte utilisateur standard (la création de comptes utilisateurs privilégié ou nomade n'est pas supportée à ce stade par *makehome.sh*).
- <*ssh-pass*> le mot de passe à attribuer aux clés de ré-authentification SSH (uniquement pour les types autres que *user*)
- *-z* : option permettant d'initialiser les partitions chiffrées à zéro plutôt qu'à un contenu aléatoire. Cette option entraîne potentiellement une réduction minime du niveau de confidentialité des données stockées sur ces partitions, mais accélère très sensiblement la création des partitions. Son usage est recommandé dans la plupart des cas.

Les comptes utilisateurs peuvent être créés avec l'utilitaire standard *useradd*, en prenant garde aux éléments suivants :

- tous les comptes doivent être créés membres du groupe *crypthomes* pour permettre leur authentification locale sur le poste (option *-g crypthomes*)
- les comptes administrateurs CLIP doivent être membres du groupe *core_admin* (option *-G core_admin*)
- les comptes auditeurs CLIP doivent être membres du groupe *core_audit* (option *-G core_audit*)
- les comptes administrateurs RM (CLIP-RM uniquement) doivent être membres du groupe *rm_admin* (option *-G rm_admin*)

En résumé, pour créer par exemple trois comptes initiaux *admin, audit* et *toto*, respectivement administrateur, auditeur, et utilisateur normal, on inscrira dans le fichier *chroot-commands-<type>* les commandes suivantes :

```
/usr/sbin/useradd -d /home/user -g crypthomes -G core_admin  admin
/usermod.sh admin <mot de passe 1> 12
/sbin/makehome.sh -z -p <mot de passe 1> -P <ssh 1> -t admin -s 16 admin
(création de admin)
/usr/sbin/useradd -d /home/user -g crypthomes -G core_audit  audit
/usermod.sh audit <mot de passe 2> 12
/sbin/makehome.sh -z -p <mot de passe 2> -P <ssh 2> -t audit -s 16 audit
(création de audit)
```

```
/usr/sbin/useradd -d /home/user -g crypthomes toto
/usermod.sh toto <mot de passe 3> 12
/sbin/makehome.sh -z -p <mot de passe 3> -s 256 toto
(création de toto)
```

1.4.3 Configurations matérielles

Le système CLIP peut être installé, à partir d'un même miroir binaire, sur différents types de matériels. Cependant, chaque type de matériel est associé à un paramétrage spécifique de l'installation (liste de pilotes à charger, configuration par défaut de l'affichage), qui doit être fournie à l'installeur. Les différentes configurations matérielles officiellement supportées (c'est-à-dire sur lesquelles une installation a été réalisée et validée avec succès par les développeurs) sont prédéfinies dans l'installeur, et peuvent être utilisées directement en passant à ce dernier l'option *-H <matériel>* avec *<matériel>* le nom de la configuration. Pour chaque nom de configuration, l'installeur incorpore un répertoire */opt/clip-installer/hw_conf/<matériel>*, contenant deux fichiers :

- *modules* : liste de modules à intégrer dans l'*initrd* associé au noyau CLIP, et à charger automatiquement au démarrage de ce dernier. Le fichier *modules* comprend un nom de module par ligne, éventuellement suivi sur la même ligne de paramètres optionnels du module (par exemple *mon_module option1=1 option2=0* pour charger le module *mon_module* en prépositionnant ses options *option1* et *option2* à 1 et 0 respectivement). Les modules à intégrer dans ce fichier comportent a minima :
  - le pilote permettant d'accéder au disque d'installation
  - le pilote de la carte réseau utilisée par défaut (filaire de préférence)
  - les pilotes d'éventuelles autres cartes réseau, y compris *Wifi* (les cartes téléphoniques 3G supportées par CLIP ne nécessitent en revanche pas d'ajout de module spécifique).
  - les pilotes de contrôleur USB adaptés (*uhci / ohci, ehci*)
  - les pilotes son
  - les éventuels pilotes ACPI (batterie, alimentation secteur, etc).
- *bootargs* : paramètres supplémentaires à passer au noyau lors du démarrage, sur une seule ligne. Ce fichier doit en particulier définir le mode d'affichage *framebuffer* (*uvesafb*) à utiliser par défaut, par exemple *video=uvesafb:1280x800-32,mtrr:3,ywrap* pour un affichage par défaut un 1280x800[6].

Les noms des configurations matérielles sont normalement définit selon le schéma *<FABRICANT>_<Modèle>*, par exemple *DELL_Latitude_D530* ou *TOSHIBA_SatellitePro_U400*. La liste des configurations supportées par un installeur CLIP peut être obtenue par la commande :

```
full_install.sh -v
```

Ajout manuel d'une configuration matérielle

Les configurations matérielles sont normalement intégrées dans l'installeur par les développeurs CLIP.

[6] Le système proposera automatiquement des résolutions inférieures au démarrage, par exemple dans ce cas 1024x768 et 800x600.

Cependant, il reste possible d'ajouter dynamiquement une configuration à l'installeur lors de son fonctionnement, afin typiquement de tenter l'installation sur une configuration matérielle pas encore officiellement supportée. L'ajout d'une nouvelle configuration consiste simplement à ajouter un répertoire dans */opt/clip-installer/hw_conf/*, portant le nom de la configuration et contenant les fichiers *modules* et *params* adaptés.

Cependant, il est généralement plus complexe de faire cela depuis l'environnement d'installation lui-même (après avoir démarré sur l'installeur), car le répertoire */opt/clip-installer/hw_conf* est en lecture seule dans ce cas. Un contournement possible consiste à monter en *bind* un répertoire inscriptible sur ce répertoire de configuration, par exemple par la suite de commandes suivantes :

```
cp -a /opt/clip-installer/hw_conf /root/hw_conf
mount --bind -o rw /root/hw_conf /opt/clip-installer/hw_conf
```

On peut ensuite accéder en écriture au nouveau répertoire *hw_conf*, en gardant à l'esprit le fait que ces modifications résident en mémoire uniquement (le répertoire monté en *bind* sur *hw_conf* réside en réalité dans un *tmpfs,* système de fichier en RAM qui constitue la racine de l'environnement d'installation), et seront donc perdues lors de l'arrêt de l'installeur, si elles n'ont pas été auparavant sauvegardées sur un support amovible.

2 Procédure d'installation par un Administrateur de Réseau

La procédure décrite dans la présente section est adaptée à tout cadre d'emploi dans lequel l'administrateur d'un réseau de déploiement CLIP procède sous sa responsabilité directe (sans faire appel à un intégrateur tierce partie) à l'installation des postes CLIP qu'il déploie.

2.1 Acheminement des supports d'installation

Les supports d'installation sont générés par un Développeur, et contrôlés par un Validateur. Ce dernier génère un haché SHA256 (ou si possible CCSD) de l'ensemble du support (image ISO), puis transmet le support à l'Administrateur de Réseau, par un moyen (courrier recommandé avec des enveloppes de sécurité appropriées, courrier électronique chiffré, remise de la main à la main) adapté au niveau de sensibilité du support (Diffusion Restreinte – Spécial France). Il transmet par ailleurs au destinataire le haché du support, par une autre voie de communication (téléphonique par exemple). L'Administrateur de Réseau vérifie avant utilisation du support le haché de celui-ci, puis stocke le support conformément à son niveau de sensibilité.

Le calcul du haché du support peut être réalisé par exemple par la commande suivante (lancée sur un poste Linux sur lequel le support d'installation serait accessible à travers le *device* <*dev*>, par exemple */dev/sdb* ou */dev/sr0*) :

```
Pour SHA256 :
openssl dgst -sha256 < <dev>

Pour CCSD :
ccsd-hash <dev>
```

2.2 Génération des paramètres

Un Administrateur de Réseau génère les éléments secrets suivants :

- clé privée d'authentification IPsec, au sein de l'IGC IPsec (sauf cas d'un poste hors-ligne).
- un bi-clé d'export USB par niveau (un pour CLIP-GTW et CLIP-single, trois pour CLIP-RM), cf. 1.3.5. Ces bi-clés sont générés soit sur des postes dédiés hors-ligne (un par niveau), soit sur un poste traitant en mode dominant des informations de niveau supérieur ou égal au niveau maximal des informations manipulées par le poste CLIP. Une copie des clés privées ainsi générées est conservée sur le poste de génération.

Il crée ensuite une arborescence complète de configuration, comportant :

- la clé privée d'authentification IPsec et son mot de passe (fichiers *ccsd.pvr* et *ccsd.pwd* dans *conf/ike2_cert/*).
- éventuellement, pour une passerelle, les clés publiques des clients avec lesquels elle aura à négocier (dans *conf/ike2_cert/*, dans des fichiers <*SN*>*.ppr* avec <*SN*> le *SubjectName* du certificat ACID.

- les clés publiques des passerelles IPsec avec lequel le poste aura a communiquer (dans *params/ike2_cert/,* avec les conventions de nommage suivantes : *update.ppr* pour une passerelle de mise à jour, *rmh.ppr* pour une passerelle RM_H). (sauf poste hors ligne)
- le certificat racine de l'IGC HTTPS (sauf poste hors ligne)
- les clés de vérification de l'IGC Développeur et de l'IGC Validateur
- les fichiers de configuration réseau et de mise à jour pour le type de configuration (cf. 1.4) à installer (dans *conf/*)
- les clés publiques d'export USB
- un fichier de configuration *params/chroot-commands* permettant la création d'un compte utilisateur *config*, avec un mot de passe *config*.

Enfin, l'Administrateur Réseau initialise une clé USB vide et la formate au format FAT32, puis copie sur cette clé l'ensemble de l'arborescence de configuration (répertoires *conf* et *params*). Si la clé à été « effacée » selon la procédure décrite en 2.3, l'initialisation peut être réalisée par les deux commandes suivantes (en supposant la clé visible sous */dev/sdb*) :

```
fdisk /dev/sdb
(créer une partition primaire,
 occupant tout l'espace, sauver)
mkfs.vfat /dev/sdb1
```

2.3 Installation

L'Administrateur de Réseau démarre le poste CLIP sur le support d'installation. Il vérifie dans un premier temps la ou les versions (type de système, par exemple passerelle ou client, et numéro de version pour chaque type) qui peuvent être installées à partir du support en lançant la commande :

```
full-install.sh -v
```

Il monte ensuite la clé USB de configuration sur */root,* par une commande :

```
mount -t auto <device> /root
```

où <*device*> désigne le périphérique associé à la clé USB, variable selon les postes :

- sur un poste client typique, intégrant un unique disque SATA : */dev/sdb1* si l'installeur a été démarré sur un CD-ROM, */dev/sdc1* si l'installeur est lui-même une clé USB (*/dev/sdb1*)
- sur un poste de type passerelle, possédant deux disques SATA ou SCSCI : */dev/sdc1* (installeur sur CD-ROM) ou */dev/sdd1* (installeur sur clé USB)

Le périphérique associé à la clé USB peut dans tous les cas être déterminé par lecture des messages noyaux après branchement de la clé, par une commande

```
dmesg | tail
```

Puis il lance l'installation complète par défaut, par la commande :

```
full-install.sh -t <type> -c /root -H <matériel> <disque(s)>
```

Dans cette commande, <*type*> désigne le type de système CLIP à installer, par exemple *rm* pour un poste CLIP-RM, et <*disque*> désigne le ou les disques sur lesquels le système doit être installé. Un poste de type client (CLIP-RM) est installé sur un disque unique, et <*disque*> sera dans ce cas défini comme */dev/sda* (disque SCSI ou SATA) ou éventuellement */dev/hda* (disque IDE). D'autres configurations, par exemple les passerelles CLIP, utilisent typiquement deux disques combinés en RAID. L'argument <*disque*> sera dans ce cas typiquement passé comme */dev/sda /dev/sdb* (deux premiers disques SATA ou SCSI). L'argument *-c /root* désigne le chemin de montage de l'arborescence de configuration. Si la clé USB de configuration est montée ailleurs, ou contient l'arborescence de configuration dans un sous-répertoire plutôt qu'à la racine, ce chemin devra être adapté en conséquence.

L'aide en ligne des outils d'installation peut par ailleurs être consultée par la commande :

```
aide
```

Une fois l'installation complétée, l'Administrateur de Réseau démonte et retire la clé USB de configuration, et redémarre le poste CLIP en prenant soin de retirer le support d'installation. Lors de ce redémarrage, il procède à la configuration du BIOS du poste conformément à [CLIP_2002], si un tel guide est applicable. L'Administrateur de Réseau éteint immédiatement le poste CLIP après avoir vérifié qu'il démarre, sans ouvrir de session.

A l'issue de la procédure d'installation, le support USB utilisé pour importer l'arborescence de configuration est effacé par l'Administrateur de Réseau (au niveau logique uniquement) par la commande (en supposant la clé visible sous */dev/sdb,* et démontée) :

```
dd if=/dev/zero of=/dev/sdb
(attendre que l'écriture se termine faute de place)
```

L'effacement du support est également réalisable directement sur le poste CLIP, en applicant la procédure suivante, par exemple au cours de la session *config* :

- Branchement du support au poste CLIP, et annulation du montage lorsque celui-ci est proposé par un *« pop-up »*.
- Effacement du support : « Menu principal » > « Supports amovibles » > « Effacer un support USB ».

Remarque 1 : installation personnalisée

Les outils d'installation permettent, alternativement à la méthode par défaut présentée ici, une installation plus configurable en lançant directement les scripts individuels normalement appelés par full-install. *Cette approche, qui est également décrite dans l'aide en ligne, est principalement utile dans le cadre du développement, et ne doit pas être utilisée pour l'installation d'un poste de production.*

Remarque 2 : utilisation d'un support commun pour plusieurs configurations

Il est acceptable de copier plusieurs configurations de postes clients dans autant de répertoires du support USB utilisé pour les rendre disponible lors de l'installation, et de réutiliser ce même support pour plusieurs installations successives, sous réserve que le

support soit effectivement effacé au terme de son utilisation.

2.4 Configuration initiale

Au terme de l'installation, l'Administrateur de Réseau remet à un Administrateur de Poste en charge du poste nouvellement installé les éléments suivants :

- poste installé
- clés privées d'export USB et leurs mots de passe (générées en 2.2)

L'Administrateur de Poste démarre le poste, et réalise les opérations suivantes :

- Génération d'un jeu de mots de passe les comptes *admin*, *audit*, et d'un mot de passe pour chaque compte utilisateur (standard ou nomade) à créer, ou alternativement génération d'un mot de passe pour un unique compte utilisateur privilégié (si l'Administrateur est également l'auditeur et le seul utilisateur du poste).
- Authentification comme utilisateur *config.*
- Création d'un nouveau compte d'administration, *admin,* à travers l'interface graphique de gestion des utilisateurs: « menu administration (icône de clé plate) »> « Avancé » > « Gérer les utilisateurs ».
- Déconnexion de la session *config*.
- Authentification comme utilisateur *admin* (ou utilisateur privilégié) et lancement de l'interface de gestion des utilisateurs.
- Suppression du compte *config*
- Création d'un compte d'audit, *audit.*
- Création d'un compte utilisateur ou utilisateur nomade par Utilisateur du système.
- Déconnexion du compte *admin.*

Après déconnexion, l'Administrateur de Poste remet à l'Auditeur de Poste et aux éventuels Utilisateurs leurs mots de passe initiaux respectifs. L'Auditeur de Poste et chaque Utilisateur se connectent successivement sur leurs comptes respectifs (en vérifiant qu'aucune connexion précédente n'a eu lieu sur ses comptes), et modifient leur mot de passe, pour lui donner une valeur inconnue de l'Administrateur de Poste. La modification du mot de passe est possible dans le menu principale (icône « cage »), sous-menu « Configuration », action « Changer de mot de passe ».

3 Procédure d'installation par un Intégrateur

La procédure décrite dans la présente section est adaptée au cas où l'installation des postes est déléguée à un Intégrateur tierce-partie (par exemple entreprise dans le cadre d'un contrat d'assistance au déploiement), qui n'a pas vocation à connaître les éléments secrets liés au déploiement.

3.1 Génération des paramètres

Un Administrateur de Réseau génère les éléments secrets suivants :

- clé privée d'authentification IPsec, au sein de l'IGC IPsec (sauf poste hors-ligne)
- un bi-clé d'export USB par niveau (un pour CLIP-GTW et CLIP-single, trois pour CLIP-RM), cf. 1.3.5. Ces bi-clés sont générés soit sur des postes dédiés hors-ligne (un par niveau), soit sur un poste traitant en mode dominant des informations de niveau supérieur ou égal au niveau des informations manipulées par le poste CLIP. Une copie des clés privées ainsi générées est conservée sur le poste de génération.

Il crée ensuite une arborescence de configuration **limitée aux Paramètres non Secrets**, comportant :

- éventuellement, pour une passerelle, les clés publiques des clients avec lesquels elle aura à négocier (dans *conf/ike2_cert/*, dans des fichiers *<SN>.ppr* avec *<SN>* le *SubjectName* du certificat ACID.
- les clés publiques des passerelles IPsec avec lequel le poste aura a communiquer (dans *params/ike2_cert/,* avec les conventions de nommage suivantes : *update.ppr* pour une passerelle de mise à jour, *rmh.ppr* pour une passerelle RM_H) (sauf poste hors-ligne).
- le certificat racine de l'IGC HTTPS (dans *conf/cert/cacert.pem*) (sauf poste hors-ligne)
- les clés de vérification de l'IGC Développeur et de l'IGC Validateur (dans *params/update_keys/*, fichiers *dev.bin* et *ctrl.bin* respectivement, accompagnés des fichiers de mot de passe)
- les fichiers de configuration réseau et de mise à jour pour le type de configuration (cf. 1.4) à installer (dans *conf/*)
- les clés publiques d'export USB (dans *params/usb_keys/)*
- un fichier de configuration *conf/chroot-commands* permettant la création d'un utilisateur *install,* avec le mot de passe *install*.

Cette arborescence est ensuite communiquée à l'Intégrateur selon les modalités précisées en 3.2.

3.2 Acheminement des supports d'installation et paramètres publics

Les supports d'installation sont générés par un Développeur, et contrôlés par un Validateur. Ce dernier génère un haché SHA256 (ou si possible CCSD) de l'ensemble du support (image ISO), puis transmet le support à l'Intégrateur, par des moyens (courrier recommandé avec des enveloppes de sécurité appropriées, remise de la main à la main) adaptés au niveau de sensibilité du support (Diffusion Restreinte – Spécial France). Il transmet par ailleurs à chaque destinataire du support le haché du

support, par une autre voie de communication (téléphonique par exemple). L'Intégrateur vérifie avant utilisation du support le haché de celui-ci, puis stocke le support conformément à son niveau de sensibilité.

De la même manière, l'Administrateur de Réseau crée une archive unique (de type *tar, zip* ou équivalent) à partir de l'arborescence de configuration publique, et calcule un haché SHA256 ou CCSD de cette archive. L'archive de configuration doit être protégée au niveau Diffusion Restreinte – Spécial France. L'Administrateur de Réseau transmet à l'Intégrateur cette archive, par un moyen adapté à son niveau de protection. Il transmet par une autre voie le haché de l'archive, que l'Intégrateur vérifie avant utilisation de l'archive.

Le calcul des hachés du support et de l'archive de configuration peuvent être réalisés par exemple par des commandes de la forme suivante (lancée sur un poste Linux sur lequel le fichier ou support à hacher serait accessible à travers le fichier <*file*>, correspondant par exemple à */dev/sdb* ou */dev/sr0* pour un support d'installation, ou *config.tar.gz* pour une archive de configuration) :

```
Pour SHA256 :
openssl dgst -sha256 < <file>

Pour CCSD :
ccsd-hash <file>
```

3.3 Installation

L'Intégrateur démarre le poste CLIP sur le support d'installation. Il vérifie dans un premier temps la ou les versions (type de système, par exemple passerelle ou client, et numéro de version pour chaque type) qui peuvent être installées à partir du support en lançant la commande :

```
full-install.sh -v
```

Il monte ensuite la clé USB de configuration sur */root,* par une commande :

```
mount -t auto <device> /root
```

où <*device*> désigne le périphérique associé à la clé USB.

Puis il lance l'installation complète par défaut, par la commande :

```
full-install.sh -t <type> -c /root -H <matériel> <disque(s)>
```

Dans cette commande, <*type*> désigne le type de système CLIP à installer, par exemple *rm* pour un poste CLIP-RM, et <*disque(s)*> désigne le ou les disques sur lesquels le système doit être installé. Un poste de type client (CLIP-RM) est installé sur un disque unique, et <*disque(s)*> sera dans ce cas défini comme */dev/sda* (disque SCSI ou SATA) ou éventuellement */dev/hda* (disque IDE). D'autres configurations, par exemple les passerelles CLIP, utilisent typiquement deux disques combinés en RAID. L'argument <*disque(s)*> sera dans ce cas typiquement passé comme */dev/sda /dev/sdb* (deux premiers disques SATA ou SCSI). L'argument *-c /root* désigne le chemin de montage de l'arborescence de configuration. Si la clé USB de configuration est montée ailleurs, ou contient l'arborescence de configuration dans un sous-répertoire plutôt qu'à la racine, ce chemin devra être adapté en conséquence.

L'aide en ligne des outils d'installation peut par ailleurs être consultée par la commande :

```
aide
```

Une fois l'installation complétée, l'Intégrateur démonte et retire la clé USB de configuration, et redémarre le poste CLIP en prenant soin de retirer le support d'installation. Lors de ce redémarrage, il procède à la configuration du BIOS du poste conformément à [CLIP_2002], si un tel guide est applicable. L'Intégrateur éteint immédiatement le poste CLIP après avoir vérifié qu'il démarre, sans ouvrir de session.

A l'issue de la procédure d'installation, le support USB utilisé pour importer l'arborescence de configuration est effacé (au niveau logique uniquement) par l'Intégrateur par la commande (en supposant la clé montée sous */root*) :

```
rm -fr /root/*
```

3.4 Acheminement du poste CLIP installé

Après installation, les postes CLIP doivent être transmis par l'Intégrateur à l'Administrateur de Réseau, par des moyens compatibles d'un niveau de protection supérieur ou égal à Diffusion Restreinte – Spécial France (transporteur accrédité ou remise de la main à la main, dans les deux cas en utilisant des emballages scellés adaptés). Si le niveau de classification des informations qui ont vocation à être manipulées par le poste CLIP justifie une classification plus élevée du poste lui-même (par exemple Confidentiel Défense, ACSSI, …), les contraintes liées à cette classification doivent également être respectés lors de l'acheminement du poste CLIP installé.

3.5 Installation des éléments secrets et configuration initiale

Après réception du poste installé, l'Administrateur de Réseau réalise les opérations suivantes :

- Authentification sur le poste CLIP comme utilisateur *install.* Aucune connexion précédente ne doit être signalée.
- Création d'un nouveau compte d'administrateur, *config* (mot de passe *config*).
- Déconnexion du compte *install* et connexion sur le compte *config*.
- Suppression de l'utilisateur *install*.
- Si des éléments secrets (clés privées IPsec et mot de passe associé) doivent être installés :
  - Copie des éléments secrets éventuels sur un support amovible (initialisé au besoin sur le poste CLIP) : fichiers *ccsd.pvr* et *ccsd.pwd*.
  - Montage du support USB contenant les éléments secrets sur le poste CLIP, et installation de la clé et du mot de passe (« Menu Administration » > « Avancé » > « Gestion des clés » > « Installer une clé IKE », opération à reproduire deux fois – une pour *ccsd.pvr* et une pour *ccsd.pwd*)
- Déconnexion du compte *config*.

Au terme de cette pré-configuration, l'Administrateur de Réseau efface au besoin le support USB utilisé pour importer les éléments secrets, par la procédure suivante :

- Débranchement du support du poste CLIP
- Branchement du support au poste CLIP, et annulation du montage lorsque celui-ci est proposé par un *« pop-up »*.
- Effacement du support : « Menu principal » > « Supports amovibles » > « Effacer un support USB ».

Remarque 3 : utilisation d'un support commun pour plusieurs configurations

Tout comme dans le cas de l'installation directement par l'Administrateur de Réseau, il est acceptable d'utiliser un support unique pour l'import des éléments secrets de plusieurs postes CLIP, sous réserve que le support soit effectivement effacé au terme de son utilisation.

Puis il remet à un Administrateur de Poste en charge du poste nouvellement installé les éléments suivants :

- poste installé
- clés privées d'export USB et leurs mots de passe (générées en 2.2)

L'Administrateur de Poste démarre le poste, et réalise les mêmes opérations de création de comptes que celles décrites en section 2.4.

Annexe A Conditions d'usage du poste CLIP

L'utilisation d'un poste CLIP est soumise à un certain nombre de contraintes de sécurité portant sur l'environnement. Ces exigences, qui sont détaillées dans le document de référence [CLIP_2101], doivent être respectées dès le début de la phase d'installation.

Annexe B Références

[CLIP_1102] *Documentation CLIP – 1102 – Génération du CD-ROM d'installation*

[CLIP_1305] *Documentation CLIP – 1305 – Gestion des mises à jour* (à rédiger)

[CLIP_1306] *Documentation CLIP – 1306 – Gestion des supports amovibles* (à rédiger)

[CLIP_1501] *Documentation CLIP – 1501 – Configuration réseau*

[CLIP_2002] *Documentation CLIP – 2002 – Guide de configuration du BIOS (document 2002x correspondant au matériel considéré)*

[CLIP_2003] *Documentation CLIP – 2003 – Guide TEMPEST (document 2003x correspondant au matériel considéré)*

[CLIP_2101] *Documentation CLIP – 2101 – Guide utilisateur CLIP (document 2101x correspondant au matériel et type de système considérés)*

[CLIP_DCS_12007] *Régles et procédures de développement – CLIP-MA-12000-007-DCS Ed0 Rev 1*

[CEC_ACID] *Documentation utilisateur du Centre d'Elaboration des Clés ACID*

[IGC_OPENSSL] *IGC Openssl, http://openssl.org/docs/apps/ca.html*