Logiciel IBM Client Security Guide de déploiement Version 5.4.0

Mis à jour le : 18 novembre 2004

Quatrième édition - octobre 2004

Ce document est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. Les informations qui y sont fournies sont susceptibles d'être modifiées avant que les produits décrits ne deviennent eux-mêmes disponibles. En outre, il peut contenir des informations ou des références concernant certains produits, logiciels ou services non annoncés dans ce pays. Cela ne signifie cependant pas qu'ils y seront annoncés.

Pour plus de détails, pour toute demande d'ordre technique, ou pour obtenir des exemplaires de documents IBM, référez-vous aux documents d'annonce disponibles dans votre pays, ou adressez-vous à votre partenaire commercial.

Vous pouvez également consulter les serveurs Internet suivants :

- http://www.fr.ibm.com (serveur IBM en France)
- http://www.can.ibm.com (serveur IBM au Canada)
- http://www.ibm.com (serveur IBM aux Etats-Unis)

Compagnie IBM France
Direction Qualité
Tour Descartes
92066 Paris-La Défense Cedex 50

Avant-propos

Le déploiement du Logiciel IBM Client Security exige des administrateurs informatiques une bonne connaissance et la planification de nombreux éléments. Le présent manuel n'a pas pour objet d'expliquer l'utilisation de la puce de sécurité intégrée ou du Logiciel Client Security ; il s'agit plutôt d'un guide relatif au déploiement du logiciel sur des ordinateurs d'entreprise dotés d'une puce de sécurité intégrée.

A qui s'adresse ce manuel

Ce manuel est destiné aux administrateurs informatiques ou aux personnes responsables du déploiement du Logiciel IBM Client Security (CSS) version 5.4 sur les ordinateurs de leur entreprise. Il fournit les informations nécessaires à l'installation du Logiciel IBM Client Security sur un ou plusieurs ordinateurs. Vous devez avoir lu le manuel *Logiciel Client Security version 5.4 - Guide d'administration et d'utilisation* avant de lire le présent manuel. IBM fournit le manuel *Logiciel Client Security version 5.4 - Guide d'administration et d'utilisation* et une aide, que vous pouvez consulter si vous souhaitez plus d'informations sur l'utilisation de l'application.

Bibliographie

La bibliothèque du Logiciel Client Security version 5.4 comporte les documents suivants :

- *Logiciel Client Security version 5.4 - Guide d'administration et d'utilisation*

  Ce guide contient des informations concernant l'installation et l'utilisation des fonctions de sécurité du Logiciel Client Security ainsi que des informations concernant l'exécution des tâches du Logiciel Client Security telles que l'utilisation de la fonction de protection de connexion UVM, la configuration d'un écran de veille Client Security, la création d'un certificat numérique et l'utilisation de l'utilitaire de configuration utilisateur.
- *Logiciel Client Security version 5.4 - Guide d'installation*

  Ce guide contient des informations relatives à l'installation du Logiciel Client Security sur des ordinateurs de réseau IBM dotés de puces de sécurité intégrées IBM.

Informations complémentaires

Vous pouvez obtenir des informations complémentaires et des mises à jour du produit de sécurité, lorsqu'elles sont disponibles, à partir du site Web IBM http://www.pc.ibm.com/us/security/index.html.

Table des matières

Chapitre 1. Considérations préalables au déploiement du Logiciel IBM Client Security

Le déploiement dy Logiciel IBM Client Security version 5.4.0 s'effectue en mode Configuration évoluée à l'aide de l'assistant de configuration du Logiciel IBM Client Security. La version 5.4 du Logiciel IBM Client Security ne prend pas en charge la première génération (non TCPA) des puces de sécurité. Les utilisateurs de ces systèmes doivent se procurer la version 5.3 du Logiciel Client Security.

Il existe différentes façons de déployer le Logiciel IBM Client Security qui utilise le Sous-système de sécurité intégré (ESS) des ordinateurs personnels IBM. Le présent document va vous aider à déterminer le type de déploiement à effectuer dans votre environnement. Il est important que vous connaissiez le processus mis en oeuvre par votre entreprise pour le déploiement d'ordinateurs, depuis la création d'une image d'installation jusqu'à la remise du PC à un utilisateur final. Ce processus va en effet influer énormément sur la manière dont votre entreprise va déployer le Sous-système de sécurité intégré (ESS). IBM ESS se compose essentiellement de deux éléments, comme illustré dans la figure 1 :

1. Logiciel Client Security
2. Puce de sécurité intégrée

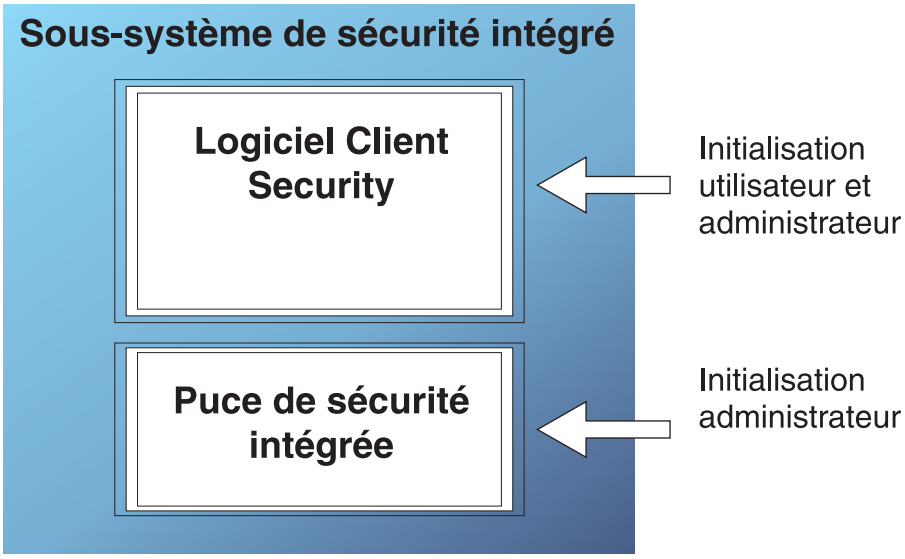

Figure 1. Composants du Logiciel IBM Client Security

Configuration requise et spécifications pour le déploiement

Si vous planifiez d'installer le Logiciel IBM Client Security sur des ordinateurs équipés de la puce de sécurité intégrée, prévoyez l'espace de stockage serveur ainsi que les téléchargements et temps d'installation suivants :

1. PC IBM doté d'une puce de sécurité intégrée
2. Espace de stockage serveur pour le code installable : environ 12 Mo
3. Espace de stockage moyen requis par utilisateur pour les données de clé d'archive : 200 ko par utilisateur pour le stockage des archives

Chapitre 2. Installation du Logiciel IBM Client Security

Le présent chapitre décrit deux types d'installation différents du Logiciel Client Security : l'installation standard et l'installation en mode administration.

Installation standard

Le fichier z046zis2018usaa.exe est un module d'installation auto-extractible qui extrait les fichiers source d'installation puis lance l'installation. Ce fichier accepte un ensemble de paramètres de lancement, lesquels sont décrits ci-après. Les options de ligne de commande qui nécessitent un paramètre doivent être indiquées en n'insérant aucun espace entre l'option et son paramètre. Par exemple, `z046zis2018usaa.exe /s /v"/qn REBOOT="R""` est correct, alors que `Setup.exe /s /v "/qn REBOOT="R""` ne l'est pas (**"/qn REBOOT="R""** est un paramètre de l'option **/v**. les guillemets entourant un paramètre ne sont obligatoires que si ce paramètre comporte des espaces.

Le comportement par défaut de ce mode d'installation, lorsque vous exécutez simplement le fichier Setup.exe sans préciser de paramètres, lequel lance l'installation avec une interface utilisateur, est de vous inviter à réamorcer le système à l'issue de l'installation. Lorsque l'installation ne comporte pas d'interface utilisateur, le comportement par défaut est d'effectuer un réamorçage à l'issue de l'installation. Cependant, ce réamorçage peut être reporté grâce à la propriété REBOOT, comme indiqué plus haut ainsi que dans la section contenant des exemples.

/a Ce paramètre force le fichier exécutable à effectuer une installation en mode administration. Dans le cas d'une installation en mode administration, vos fichiers de données sont copiés dans un répertoire spécifié par l'utilisateur, mais il n'y a aucune création de raccourcis, d'enregistrement de serveurs COM ou de création d'un historique de désinstallation.

/x Ce paramètre force le fichier exécutable à désinstaller un produit préalablement installé.

/s Mode automatique
Ce paramètre force le fichier exécutable à s'exécuter en mode automatique.

/v Le paramètre **/v** permet de transmettre des commutateurs de ligne de commande et des valeurs de propriété publique à Msiexec.exe.

/w Ce paramètre force le fichier exécutable à attendre la fin de l'installation avant de quitter. Si vous utilisez ce paramètre dans un fichier par lots, vous pouvez faire précéder l'argument de ligne de commande du fichier exécutable de `start /WAIT`. Voici un exemple correctement mis en forme d'utilisation de ce paramètre :

```
start /WAIT z046zis2018usaa.exe /w
```

Installation en mode administration

Le programme d'installation de Microsoft Windows peut procéder à une installation en mode administration d'une application ou d'un produit sur un réseau en vue de son utilisation par un groupe de travail ou d'une personnalisation. Dans le cas du module d'installation du Logiciel Client Security, l'installation en mode administration décompresse les fichiers source d'installation

à un emplacement spécifique. L'installation en mode administration n'est possible que si le module d'installation est exécuté à partir d'une ligne de commande en précisant le paramètre **/a** :

```
z046zis2018usaa.exe /a
```

Il est possible de choisir un emplacement différent sur une unité autre que C:, comme d'autres unités locales, des unités réseau, etc. De nouveaux répertoires peuvent également être créés au cours de cette étape.

Dans le cas d'une installation automatique en mode administration, la propriété publique TARGETDIR peut être définie en ligne de commande afin d'indiquer l'emplacement d'extraction :

```
Setup.exe /s /v"/qn TARGETDIR=F:\IBMCSS"
```

ou

```
msiexec.exe /i "IBM Client Security Software.msi" /qn TARGERDIR=F:\IBMCSS
```

Pour lancer une installation à partir des fichiers source décompressés après l'application de personnalisations, il suffit d'appeler msiexec.exe à partir de la ligne de commande. La section «Paramètres de ligne de commande» explique comment utiliser les paramètres de commande disponibles avec msiexec.exe et fournit un exemple d'utilisation. Des propriétés publiques peuvent également être directement définies dans l'appel de la ligne de commande de msiexec.

Paramètres de ligne de commande

/i *module* **ou** *code produit*

Utilisez le format suivant pour installer le produit :

```
msiexec /i "C:\DossierWindows\Profiles\NomUtilisateur\Personal\MySetups\Othello\
Trial\Version\Release\DiskImages\Disk1\produitOthello Beta.msi"
```

Le code produit correspond au GUID qui est généré automatiquement dans la propriété de code produit de la vue de projet de votre produit.

Remarque : L'exemple ci-dessus figure sur deux lignes pour des raisons d'espace limité sur la page. Lorsque vous entrez la commande, elle doit figurer sur une seule ligne.

/a *module*

Le paramètre **/a** permet aux utilisateurs disposant de droits d'administrateur d'installer un produit en réseau.

/x *module* **ou** *code produit*

Ce paramètre permet de désinstaller un produit.

/L [i | w | e | a | r | u | c | m | p | v | +] *fichier historique*

Ce paramètre permet d'indiquer le chemin d'accès au fichier historique. Les indicateurs suivants permettent de préciser les informations à enregistrer dans le fichier historique :

- **i**

  Consignation des messages d'état
- **w**

  Consignation des messages d'avertissement de faible gravité
- **e**

  Consignation des messages d'erreur

- **a**
  Consignation du début des séquences d'action
- **r**
  Consignation d'enregistrements spécifiques à une action
- **u**
  Consignation des demande utilisateur
- **c**
  Consignation des paramètres d'interface utilisateur initiaux
- **m**
  Consignation des messages indiquant une mémoire insuffisante
- **p**
  Consignation des paramètres de terminal
- **v**
  Consignation des paramètres de données prolixes
- **+**
  Ajout à un fichier existant
- *
  Caractère générique permettant de consigner toutes les informations dans l'historique à l'exception des paramètres de données prolixes

/? ou /h
Permet d'afficher ou pas les informations de droit d'auteur du programme d'installation de Windows

TRANSFORMS
Le paramètre de ligne de commande TRANSFORMS permet d'indiquer les transformations que vous souhaitez appliquer à votre module de base. Voici un exemple d'appel de ligne de commande comportant le paramètre TRANSFORM :

```
msiexec /i "C:\DossierWindows\Profiles\NomUtilisateur\Personal\MySetups\
Nom Projet\Version Evaluation\Mon Edition-1\DiskImages\Disk1\NomProduit.msi"
TRANSFORMS="New Transform 1.mst"
```

Les signes deux-points pouvant être utilisés pour distinguer différentes transformations, il est déconseillé d'en utiliser dans le nom d'une transformation, car ils ne seront pas correctement interprétés par le programme d'installation de Windows.

Remarque : L'exemple ci-dessus figure sur trois lignes pour des raisons d'espace limité sur la page. Lorsque vous entrez la commande, elle doit figurer sur une seule ligne.

Propriétés
Toutes les propriétés publiques peuvent être définies ou modifiées en ligne de commande. Les propriétés publiques se distinguent des propriétés privées dans la mesure ou elles sont intégralement indiquées en lettres majuscules. COMPANYNAME, par exemple, est une propriété publique.

Pour définir une propriété à partir de la ligne de commande, utilisez la syntaxe suivante : `PROPRIETE=VALEUR`. Si vous souhaitez modifier la valeur de *COMPANYNAME*, vous pouvez entrer, par exemple :

```
msiexec /i "C:\DossierWindows\Profiles\NomUtilisateur\Personal\MySetups\
NomProjet\Trial Version\My Release-1\DiskImages\Disk1\NomProduit.msi"
COMPANYNAME="InstallShield"
```

Remarque : L'exemple précédent figure sur trois lignes pour des raisons d'espace limité sur la page. Lorsque vous entrez la commande, elle doit figurer sur une seule ligne.

Propriétés publiques personnalisées du Logiciel Client Security

Le module d'installation du Logiciel Client Security contient un ensemble de propriétés publiques personnalisées qui peuvent être définies en ligne de commande lors de l'exécution de l'installation. Les propriétés publiques personnalisées actuellement disponibles sont les suivantes :

INSTALLPWM
Cette propriété permet de contrôler l'installation de Password Manager au cours de l'installation initiale. La valeur 1 indique que Password Manager doit être installé, et la valeur 0 indique que Password Manager ne doit pas être installé. La valeur par défaut est 1.

CFGFILE
Cette propriété peut être utilisée au cours d'une installation automatique pour spécifier l'emplacement d'un fichier de configuration. Ce fichier de configuration peut contenir la valeur du mot de passe en vigueur pour la puce de sécurité. Elle permet à l'installation de s'effectuer jusqu'au bout sans interaction de l'utilisation même si un mot de passe existe déjà pour la puce. Exemple :

```
CFGFILE=C:\csec.ini
```

Installation des fonctions du Logiciel Client Security

Le mode d'installation ″One-Click″ du Logiciel Client Security comporte deux fonctions principales : *Security* (Logiciel IBM Client Security) et *PWManager* (IBM Password Manager). Ces deux fonctions sont installées par défaut. Néanmoins, comme vous disposez de plusieurs options lors du lancement de l'installation, il se peut que seule la fonction Security soit installée (la fonction Security est obligatoire alors que la fonction PWManager ne l'est pas). Si vous lancez l'installation à partir d'une interface utilisateur et que la version 1.3 ou une version antérieure d'IBM Password Manager n'est pas déjà installée, un écran vous invitera à indiquer si vous souhaitez installer le Logiciel IBM Client Security uniquement ou à la fois le Logiciel IBM Client Security et IBM Password Manager. Si vous lancez l'installation sans passer par une interface utilisateur (dans le cas d'une installation automatique, notamment), vous pouvez contrôler l'installation de Password Manager au moyen de la propriété INSTALLPWM (à laquelle vous affectez la valeur 0 si vous ne voulez pas installer Password Manager). Si vous choisissez d'installer uniquement IBM Client Security lors de l'installation initiale et décidez ultérieurement d'ajouter IBM Password Manager, il vous suffit de relancer le module source d'origine. Lorsque l'installation est lancée via une interface utilisateur, un écran de maintenance comportant le bouton "Modification" s'affiche si Password Manager n'est pas déjà installé. Ce bouton permet d'accéder à un écran à partir duquel vous pouvez choisir de réinstaller Client Security uniquement ou modifier vos choix concernant l'installation du Logiciel IBM Client Security et d'IBM Password Manager. Il est possible également de réinstaller le produit à partir de la source sans passer par une interface utilisateur afin d'ajouter IBM Password Manager. Des exemples de commande sont fournis ci-après.

Exemples d'utilisation de la commande Setup.exe

Le tableau 1 comporte des exemples d'utilisation de la commande z046zis2018usaa.exe.

Tableau 1. Exemples d'installation à l'aide de la commande z046zis2018usaa.exe

Type	Exemple
Installation automatique avec réamorçage à l'issue de l'installation	`z046zis2018usaa.exe /s /v/qn`
Installation automatique sans réamorçage	`z046zis2018usaa.exe /s /v"/qn REBOOT="R""`
Installation automatique sans réamorçage et sans installation de Password Manager	`z046zis2018usaa.exe /s /v"/qn REBOOT="R" INSTALLPWM=0"`
Installation automatique sans réamorçage avec indication du répertoire d'installation	`z046zis2018usaa.exe /s /v"/qn REBOOT="R" INSTALLDIR=C:\ibmcss"`
Installation automatique sans réamorçage avec indication du fichier de configuration	`z046zis2018usaa.exe /s /v"/qn REBOOT="R" CFGFILE=C:\csec.ini"`
Installation automatique en mode administration	`z046zis2018usaa.exe /a`
Installation automatique en mode administration avec indication de l'emplacement d'extraction	`z046zis2018usaa.exe /a /s /v"/qn TARGETDIR="F:\CSS""`
Installation sans réamorçage et création d'un historique d'installation dans un répertoire temp	`z046zis2018usaa.exe /v"REBOOT="R" /L*v %temp%\css.log"`
Réinstallation automatique d'un produit pour l'ajout de Password Manager	`z046zis2018usaa.exe /s /v"/qn ADDLOCAL=PWManager"`

Le tableau 2 comporte des exemples d'utilisation de la commande msiexec.exe.

Tableau 2. Installation à l'aide de msiexec.exe

Type	Exemple
Installation avec fichier historique	`msiexec /i "C:\IBM Client Security Software.msi" /L*v %temp%\css.log`
Installation automatique sans réamorçage	`msiexec /i "C:\IBM Client Security Software.msi" /qn REBOOT="R"`
Installation automatique sans réamorçage et sans installation de Password Manager	`msiexec /i "C:\IBM Client Security Software.msi" /qn REBOOT="R" INSTALLPWM=0`
Réinstallation automatique d'un produit pour l'ajout de Password Manager	`msiexec /i "C:\IBM Client Security Software.msi" /qn ADDLOCAL=PWManager`

Chapitre 3. Fonctionnement de la puce de sécurité intégrée

La puce de sécurité intégrée IBM est représentée à la figure 2. Elle contient trois composants essentiels :

1. Mot de passe administrateur
2. Clé matérielle publique
3. Clé matérielle privée

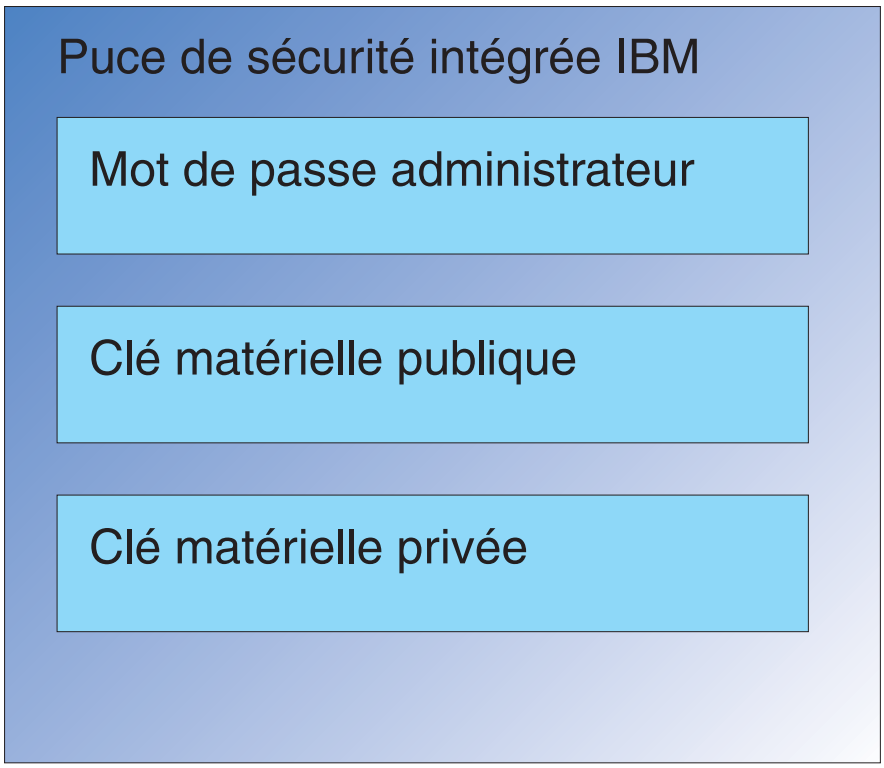

Figure 2. Données contenues dans la puce de sécurité intégrée IBM

Les clés matérielles publique et privée sont uniques sur chaque ordinateur. La clé matérielle privée ne peut en aucun cas être extraite de la puce. Vous pouvez générer de nouvelles paires de clés en procédant comme suit :

- Via l'Assistant du Logiciel Client Security
- Via l'utilitaire d'administration
- En utilisant des scripts

Remarque : Les clés matérielles ne peuvent en aucun cas être extraites de la puce.

L'administrateur se sert du mot de passe administrateur pour accéder, entre autres, aux fonctions suivantes :

- Ajout d'utilisateurs
- Définition d'une stratégie de sécurité
- Définition d'une stratégie de mot de passe composé
- Enregistrement de cartes à puce

- Enregistrement d'appareils de mesure biométrique

Un administrateur peut, par exemple, avoir à ajouter un utilisateur supplémentaire pour l'accès aux fonctions de la puce de sécurité intégrée. Le mot de passe administrateur est défini au moment de l'installation du Logiciel Client Security. La procédure de définition des mots de passe par l'administrateur est décrite plus loin dans le présent document.

Important : Vous devez développer une stratégie pour la gestion des mots de passes administrateur, à établir lors de la configuration initiale d'ESS (Sous-système de sécurité intégré). Il est possible que chaque ordinateur doté d'une puce de sécurité intégrée utilise le même mot de passe administrateur, si l'administrateur informatique ou l'administrateur de la sécurité l'a décidé ainsi. Néanmoins, chaque service ou chaque immeuble peut également se voir attribuer des mots de passe administrateur différents.

Les autres composants de la puce de sécurité intégrée IBM sont la clé matérielle publique et la clé matérielle privée. La paire de clés RSA est générée au moment de la configuration du Logiciel Client Security.

Chaque ordinateur dispose d'une clé matérielle publique et d'une clé matérielle privée uniques. Grâce à la fonction de génération aléatoire de nombres de la puce de sécurité intégrée IBM, chaque paire de clés matérielles est statistiquement unique.

La figure 3 à la page 11 illustre deux composants supplémentaires de la puce de sécurité intégrée IBM. Une bonne connaissance de ces deux composants est essentielle pour une gestion efficace de l'infrastructure de votre Sous-système de sécurité intégré IBM. La figure 3 à la page 11 indique les clés publique et privée de l'administrateur et de l'utilisateur. Voici un récapitulatif des informations relatives aux clés publique et privée :

- Les clés publique et privée sont considérées comme une ″paire de clés.″
- Les clés publique et privée sont mathématiquement reliées comme suit :
  - Tout élément chiffré avec la clé publique ne peut être déchiffré qu'à l'aide de la clé privée.
  - Tout élément chiffré avec la clé privée ne peut être déchiffré qu'à l'aide de la clé publique.
  - Le fait de connaître la clé privée ne vous autorise pas à déduire la clé publique.
  - Le fait de connaître la clé publique ne vous autorise pas à déduire la clé privée.
  - La clé publique est généralement connue de tous les utilisateurs.
- La clé privée doit être hautement protégée.
- Les clés publique et privée constituent la base de l'infrastructure PKI (Public Key Infrastructure).

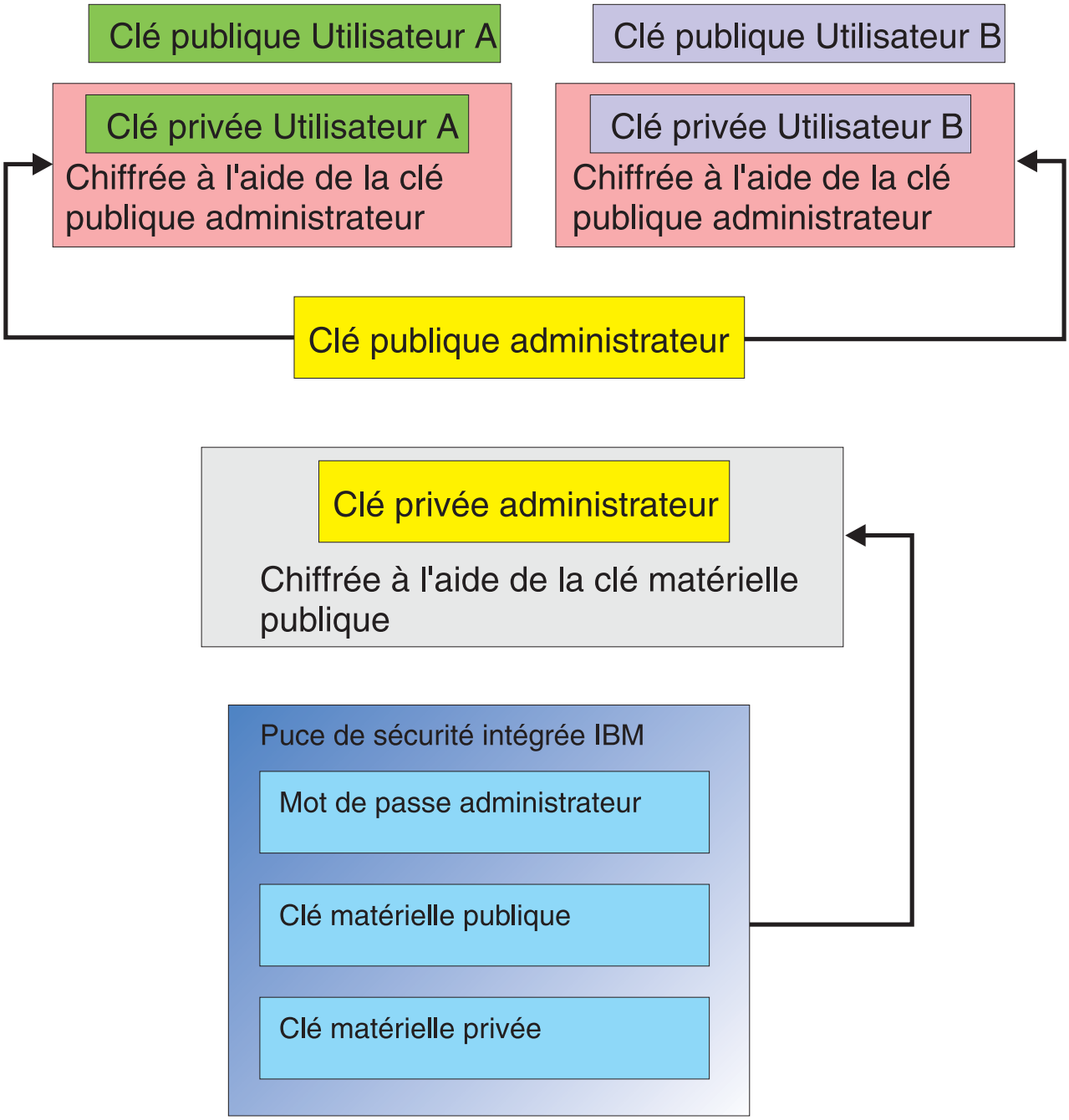

Figure 3. Plusieurs couches de chiffrement offrent une sécurité renforcée

Hiérarchie de substitution de clés

L'architecture d'IBM ESS se compose en grande partie d'une hiérarchie de "substitution de clés". Le mode de fonctionnement de cette hiérarchie est décrit en détail dans le *Logiciel Client Security - Guide d'administration et d'utilisation* ; ce concept est néanmoins introduit ici car il s'applique à la configuration, au déploiement et à la gestion de masse. La Figure 3 illustre la clé matérielle publique et la clé matérielle privée. Comme indiqué précédemment, ces clés sont créées par le Logiciel Client Security et sont statistiquement uniques sur chaque client.

Au-dessus de la puce de sécurité intégrée IBM figure, comme vous pouvez le constater, la paire de clés publique et privée de l'administrateur. Cette paire de clés peut être unique sur tous les ordinateurs ou être identique sur l'ensemble (ou un sous-ensemble) des clients. Les avantages et les inconvénients d'une telle configuration sont présentés plus loin dans le présent document. Les clés publique et privée de l'administrateur permettent d'effectuer les opérations suivantes :

- Protection des clés publique et privée des utilisateurs
- Activation de l'archivage et de la restauration des accréditations utilisateur
- Activation de l'itinérance des accréditations, opération décrite dans le manuel *IBM Client Security Software Administrator and User Guide*

Définition de la permutation de clés

Dans les sections ci-après, vous trouverez des informations concernant le rôle des utilisateurs dans l'environnement IBM ESS. Vous y trouverez également des détails concernant la configuration du Logiciel IBM Client Security et du sous-système de sécurité (ESS) ainsi que la définition de ces utilisateurs. Dans le cas présent, nous indiquerons simplement que chaque utilisateur dispose d'une clé publique et d'une clé privée. La clé privée de l'utilisateur est chiffrée à l'aide de la clé publique de l'administrateur. A partir de la figure 3 à la page 11, vous pouvez constater que la clé privée de l'administrateur est chiffrée à l'aide de la clé matérielle publique. Alors, pourquoi chiffrer ces différentes clés privées ?

La raison est l'existence de cette hiérarchie mentionnée plus haut. En raison d'un espace de stockage restreint dans la puce de sécurité intégrée IBM, seul un nombre limité de clés peut figurer dans la puce à un moment donné. Les clés matérielles publique et privée sont les seules clés persistantes (entre deux amorçages) dans le cadre de se scénario. Afin de permettre l'activation de plusieurs clés et de plusieurs utilisateurs, IBM ESS met en oeuvre une hiérarchie de substitution de clés. Une clé n'est "substituée" vers la puce de sécurité intégrée IBM que lorsqu'elle est nécessaire. De cette façon, la clé privée ne peut être déchiffrée et utilisée que dans l'environnement protégé de la puce.

La clé privée de l'administrateur est chiffrée à l'aide de la clé matérielle publique. La clé matérielle privée (disponible uniquement dans la puce) permet de déchiffrer la clé privée de l'administrateur. Une fois que la clé privée de l'administrateur a été déchiffrée dans la puce, la clé privée d'un utilisateur (chiffrée à l'aide de la clé publique de l'administrateur) peut être transférée dans la puce à partir du disque dur et déchiffrée à l'aide de la clé privée de l'administrateur. A partir de la figure 3 à la page 11, vous pouvez constater qu'il est possible de chiffrer plusieurs clés privées d'utilisateurs à l'aide de la clé publique de l'administrateur. Vous pouvez ainsi définir autant d'utilisateurs que nécessaire sur un ordinateur doté d'IBM ESS.

Chapitre 4. Considérations relatives à l'archivage de clés

Les mots de passe et les clés fonctionnent ensemble, ainsi qu'avec d'autres unités d'authentification, pour vérifier l'identité des utilisateurs système.

La figure 4 illustre le fonctionnement entre le Sous-système de sécurité intégré IBM et le Logiciel IBM Client Security. La fenêtre d'ouverture de session Windows invite tout d'abord l'Utilisateur A à ouvrir une session. L'Utilisateur A s'exécute. Le Logiciel IBM Client Security détermine ensuite la nature de l'utilisateur en cours à partir des informations fournies par le système d'exploitation. La clé privée administrateur, qui est chiffrée à l'aide de la clé matérielle publique, est chargée dans la puce de sécurité intégrée.

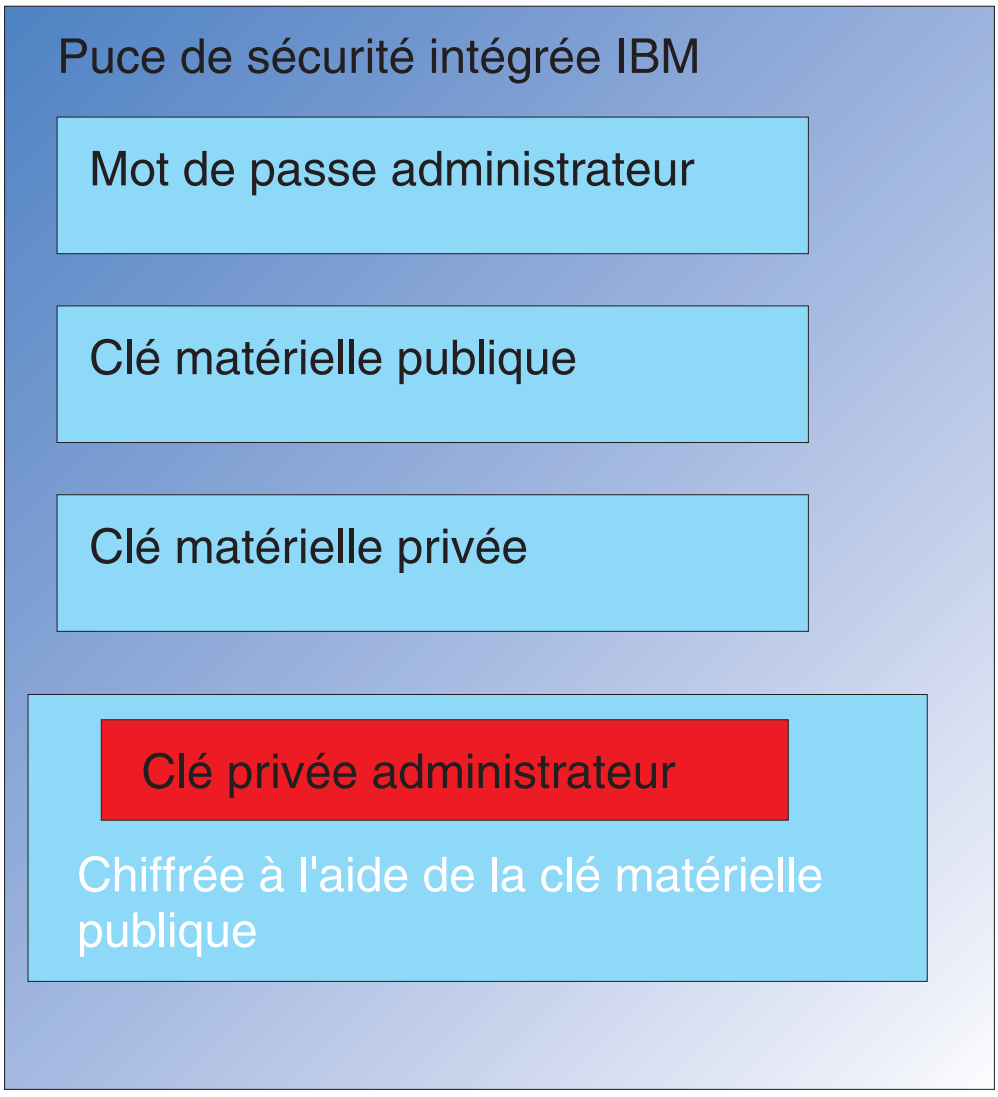

Figure 4. La clé privée administrateur, qui est chiffrée à l'aide de la clé matérielle publique. est chargée dans la puce de sécurité intégrée.

La clé matérielle privée (disponible uniquement dans la puce) permet de déchiffrer la clé privée administrateur. La clé privée administrateur est désormais disponible pour être utilisée dans la puce, comme illustré dans la figure 5.

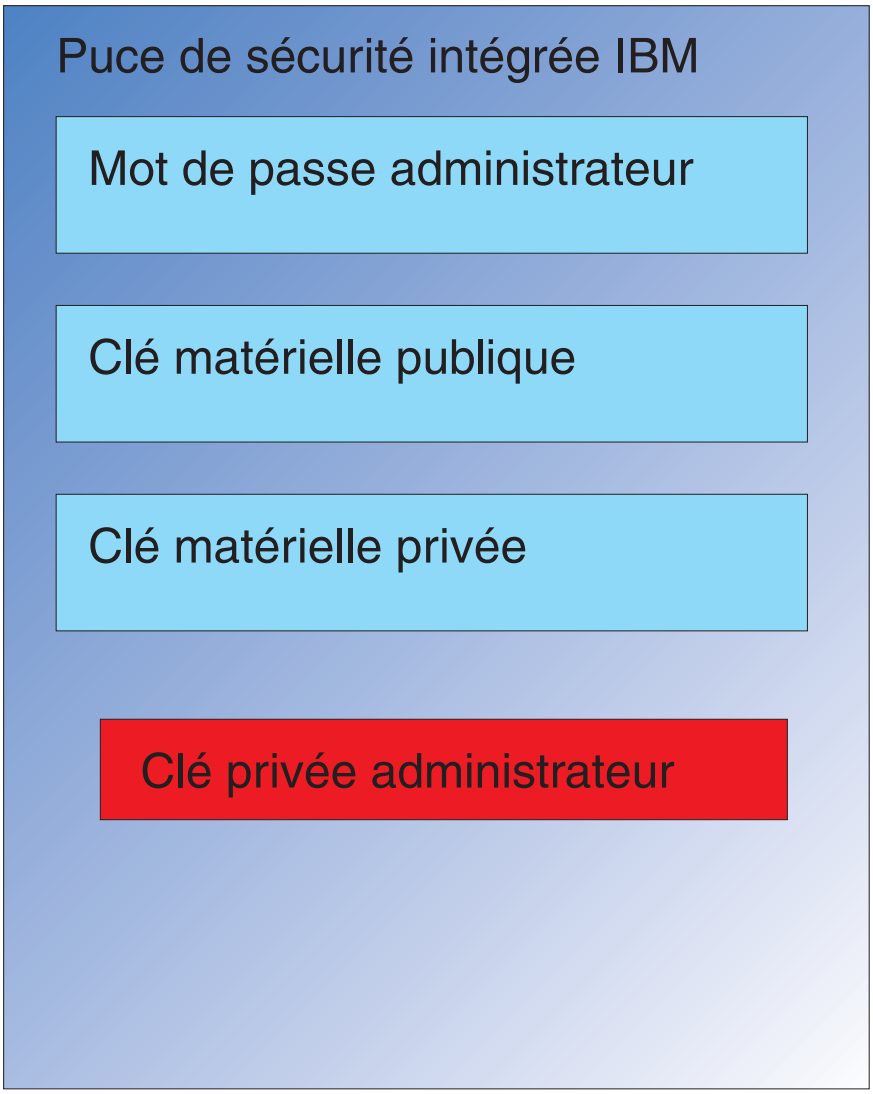

Figure 5. La clé privée administrateur est disponible pour utilisation dans la puce de sécurité.

Puisque l'Utilisateur A est connecté à l'ordinateur, la clé privée de cet utilisateur (chiffrée à l'aide de la clé publique administrateur) est transférée dans la puce, comme illustré à la figure 6.

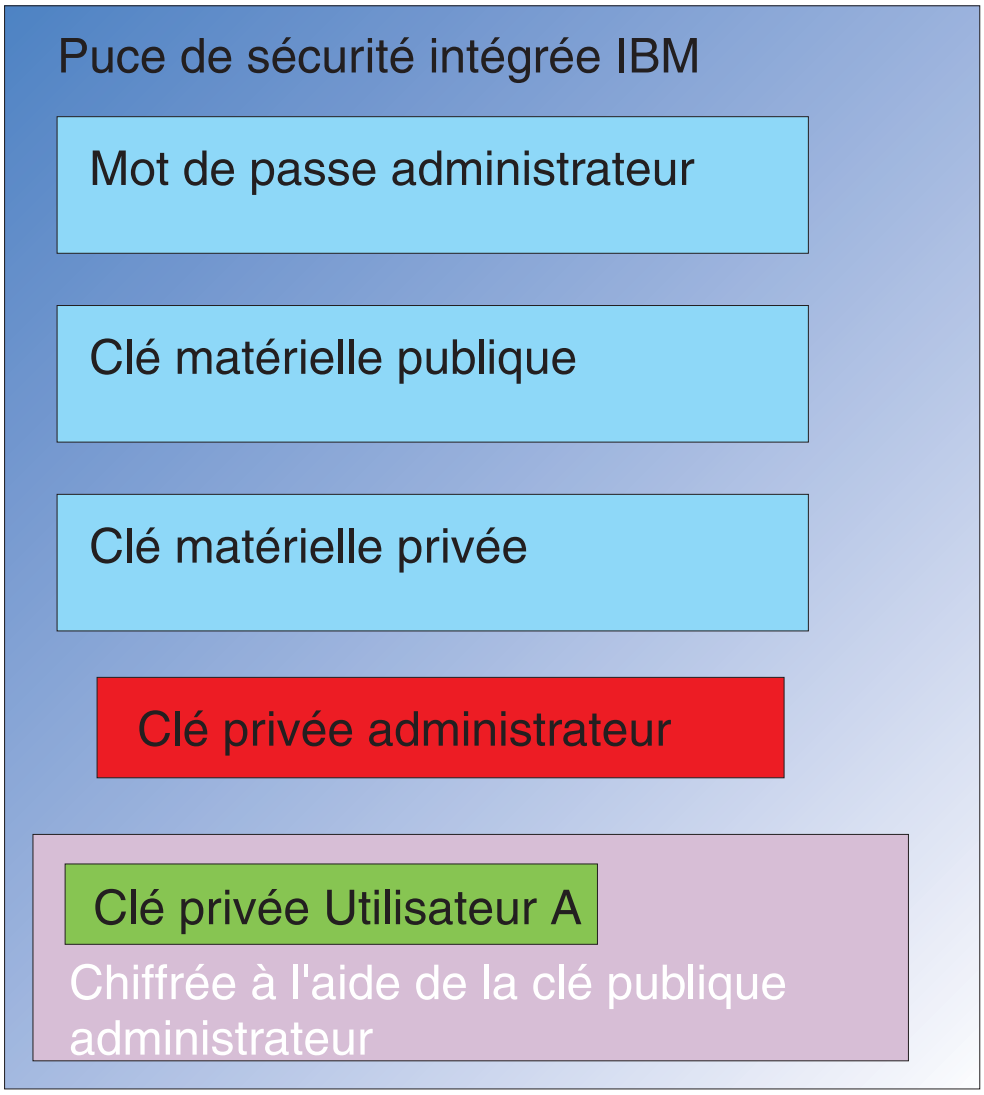

Figure 6. La clé privée de l'Utilisateur A, qui est chiffrée à l'aide de la clé publique administrateur, est transférée dans la puce de sécurité.

La clé privée administrateur est utilisée pour déchiffrer la clé privée de l'Utilisateur A. La clé privée de l'Utilisateur A est alors prête pour utilisation (voir la figure 7).

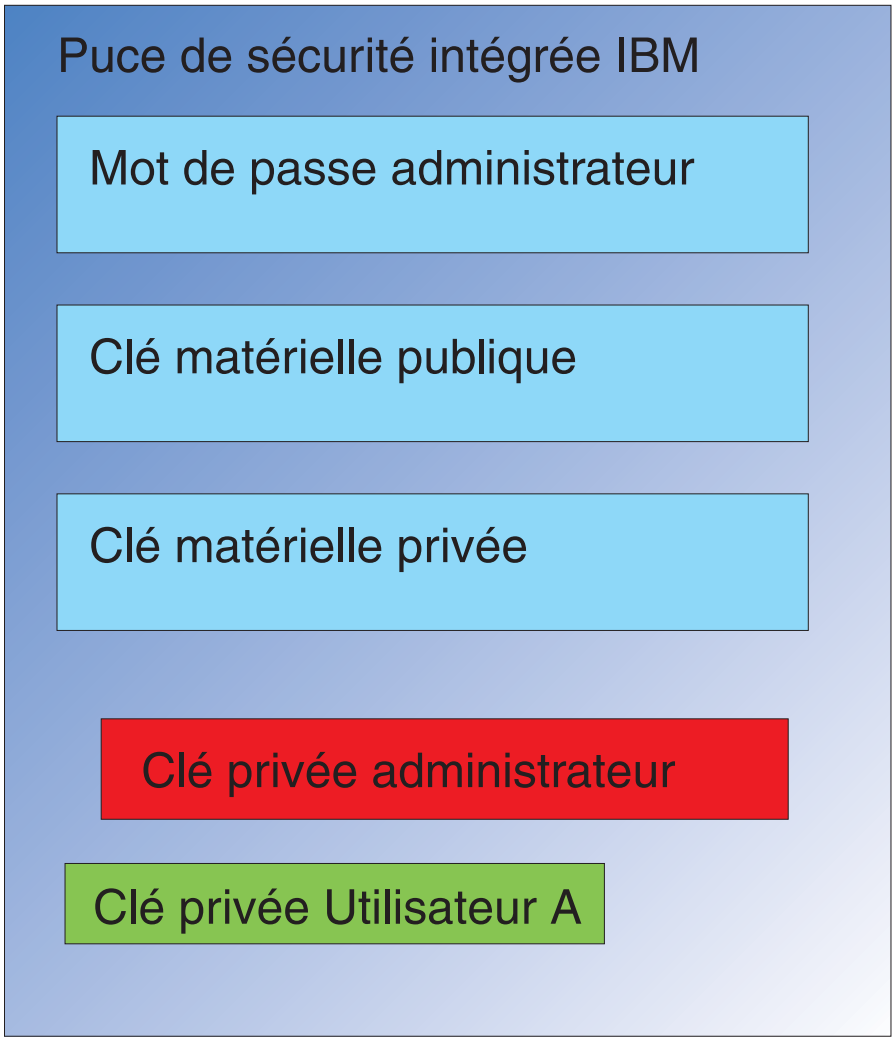

Figure 7. La clé privée de l'Utilisateur A est prête pour utilisation.

D'autres clés peuvent être chiffrées à l'aide de la clé publique de l'Utilisateur A. C'est le cas, par exemple, d'une clé privée utilisée pour la signature des courriers électroniques. Lorsque l'Utilisateur A va envoyer un courrier électronique signé, la clé privée utilisée pour la signature (chiffrée à l'aide de la clé publique de l'Utilisateur A) est transférée dans le puce. La clé privée de l'Utilisateur A (déjà dans la puce) est utilisée pour déchiffrer la clé de signature privée de l'Utilisateur A. Cette dernière est alors disponible dans la puce pour effectuer l'opération souhaitée, dans ce cas la création d'une signature numérique (chiffrement de hachage). Il est à noter que le même processus de déplacement des clés à l'intérieur et à l'extérieur de la puce serait mis en oeuvre si un Utilisateur B se connectait à l'ordinateur.

Pourquoi utiliser une paire de clés administrateur ?

Il est nécessaire de disposer d'une paire de clés administrateur pour des raisons de capacité d'archivage et de restauration. La paire de clés administrateur sert de couche d'abstraction entre la puce et les accréditations utilisateur. Les informations de clé privée spécifiques d'un utilisateur sont chiffrées à l'aide de la clé publique de l'administrateur, comme illustré dans la figure 8.

Important : Vous devez développer une stratégie pour la gestion des paires de clés administrateur. Il est possible que chaque ordinateur doté d'une puce de sécurité intégrée utilise la même paire de clés administrateur, si l'administrateur informatique ou l'administrateur de la sécurité l'a décidé ainsi. Néanmoins, chaque service ou chaque immeuble peut également se voir attribuer des paires de clés administrateur différentes.

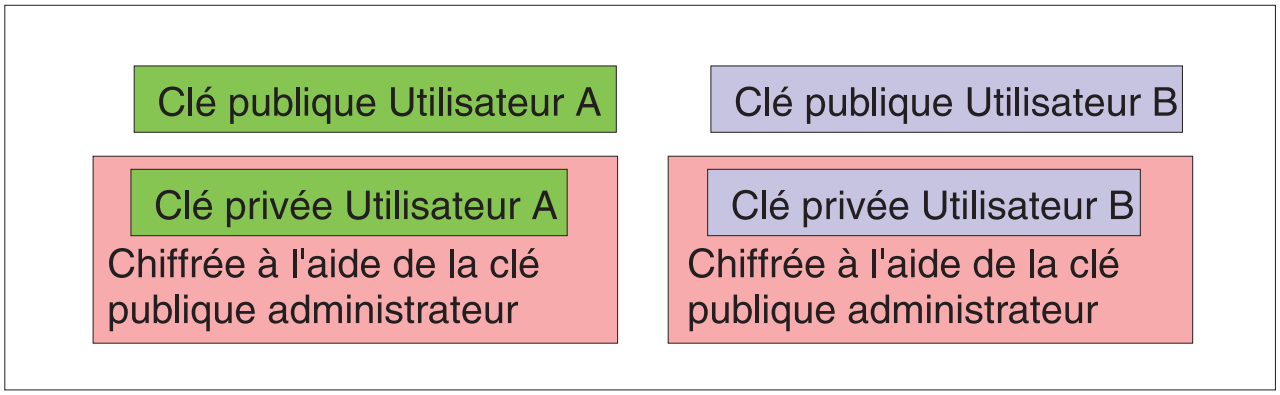

Figure 8. Les informations de clé privée spécifiques à un utilisateur sont chiffrées à l'aide de la clé publique de l'administrateur.

La nécessité de signer le fichier de stratégie de Client Security constitue une autre bonne raison de disposer d'une paire de clés administrateur. Cela permet d'empêcher quiconque, à l'exception de l'administrateur, de modifier la stratégie de sécurité. Si vous souhaitez définir un degré de sécurité élevé pour le fichier de stratégie de sécurité client, vous pouvez scinder la clé privée administrateur entre plusieurs individus (cinq au maximum). Dans ce cas, la présence des cinq individus, détenant chacun une portion de la clé privée, est requise pour la signature et le chiffrement de fichiers tels que le fichier de stratégie de sécurité client. Cela permet d'éviter qu'une seule personne puisse exécuter des fonctions d'administrateur de manière unilatérale. Pour plus d'informations concernant la scission de la clé privée administrateur, reportez-vous au paramètre Keysplit=1 dans le tableau 6 à la page 43.

Pendant l'initialisation du Logiciel IBM Client Security, les paires de clés administrateur peuvent être créées par le logiciel ou importées à partir d'un fichier externe. Si vous souhaitez utiliser une paire de clés administrateur standard, vous devez indiquer l'emplacement des fichiers nécessaires pendant l'installation du client.

Les informations spécifiques de l'utilisateur sont sauvegardées (écrites) dans un emplacement d'archive défini par l'administrateur, comme illustré à la figure 8. Cet emplacement d'archive peut être tout type de support physiquement ou logiquement connecté au client. La section relative à l'installation du Logiciel IBM Client Security fournit des informations concernant les emplacements d'archive les plus couramment définis.

Les clés publique et privée de l'administrateur ne sont pas archivées. Les données utilisateur stockées dans l'emplacement d'archive sont chiffrées à l'aide de la clé publique administrateur. Disposer des données archivées ne vous sera d'aucune utilité si vous ne possédez pas la clé privée d'archive nécessaire pour les déverrouiller. La clé publique administrateur et la clé privée d'archive sont souvent appelées "paire de clés d'archive" dans la documentation relative au Logiciel IBM Client Security. Il est à noter que la clé privée d'archive n'est pas chiffrée. Il importe donc de stocker et de protéger avec soin la paire de clés d'archive.

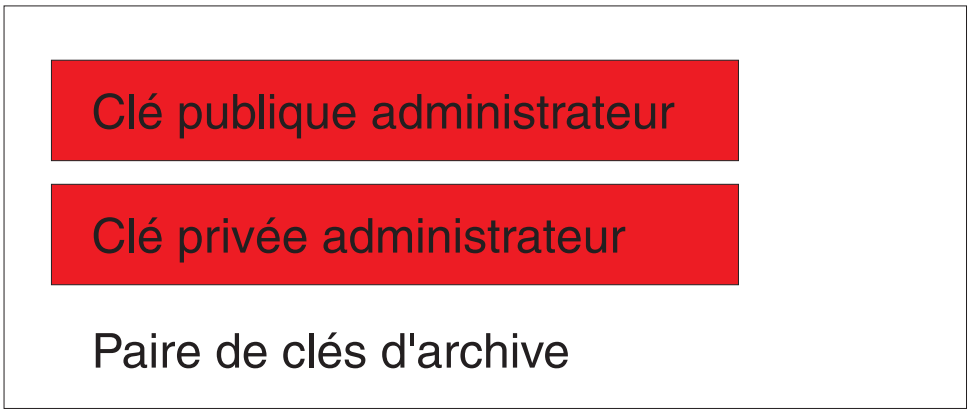

Figure 9. Les clés publique et privée de l'administrateur constituent la paire de clés d'archive.

Comme indiqué précédemment, l'une des plus importantes fonctions des clés publique et privée de l'administrateur consiste à sauvegarder et à restaurer le contenu des disques. Cette capacité est illustrée dans les figures 10 à 15. Les étapes nécessaires à l'exécution d'une telle opération sont les suivantes :

1. Le Client A, pour une raison quelconque, devient inutilisable pour l'Utilisateur A. Dans cet exemple, l'ordinateur, Client A, a été frappé par la foudre. Voir la figure 10 à la page 19.

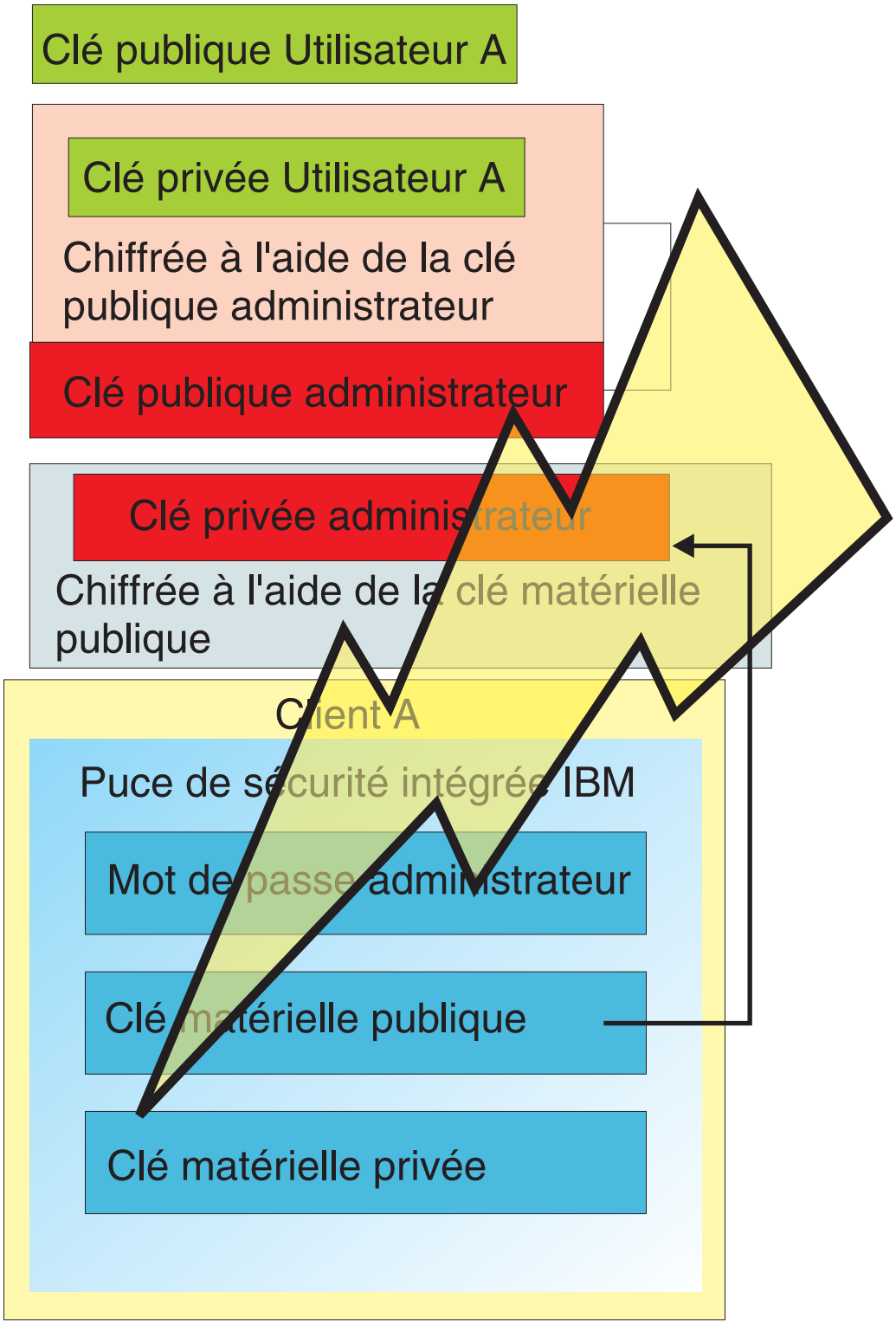

Figure 10. L'ordinateur de l'Utilisateur A est frappé par la foudre, ce qui le rend inutilisable.

2. L'Utilisateur A reçoit un nouvel ordinateur IBM de type amélioré, appelé Client B. Le Client B est différent du Client A en ce sens que ses clés matérielles publique et privée sont différentes de celles du Client A. Cette différence est visuellement représentée par les clés sur fond gris sur le Client B et les clés sur fond vert sur le Client A. Néanmoins, le mot de passe administrateur est identique sur le Client B et le Client A.

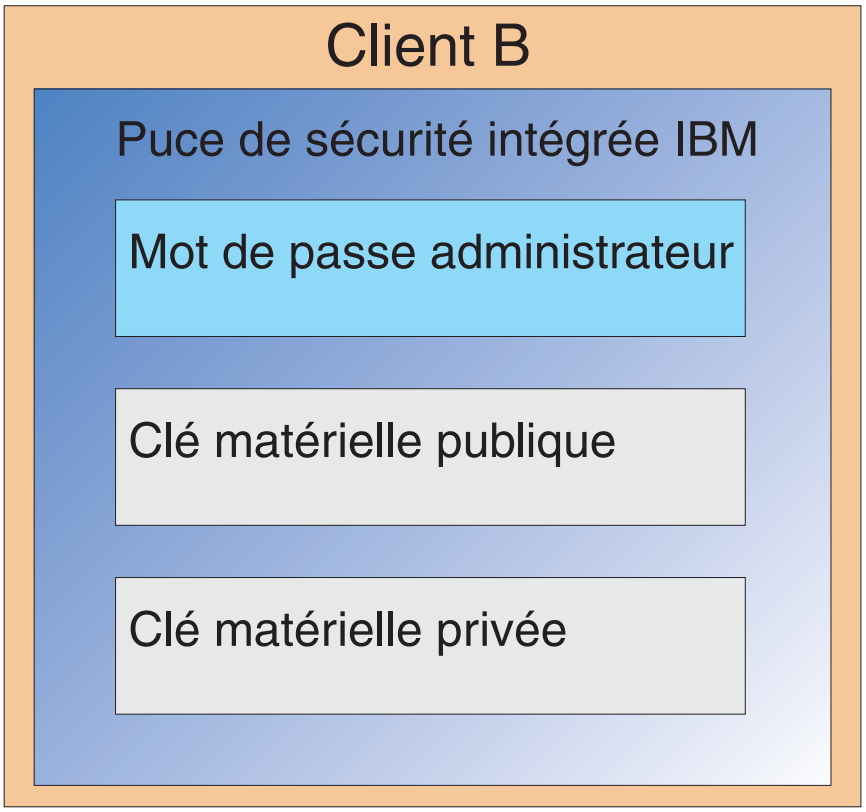

Figure 11. L'Utilisateur A reçoit un nouvel ordinateur, le Client B, doté d'une nouvelle puce de sécurité intégrée.

3. Le Client B nécessite à présent les mêmes accréditations utilisateur que celles qui figuraient sur le Client A. Ces informations ont été archivées sur le Client A. Si vous retournez à la figure 8 à la page 17, vous verrez que les clés de l'utilisateur sont chiffrés à l'aide de la clé publique administrateur et stockées dans un emplacement d'archive. Pour que les accréditations utilisateur soient disponibles sur le Client B, il est nécessaire de transférer les clés publique et privée de l'administrateur sur cette machine. La Figure 12 illustre l'extraction par le Client B des clés publique et privée de l'administrateur afin de procéder à la récupération de données utilisateur à partir de l'emplacement d'archive.

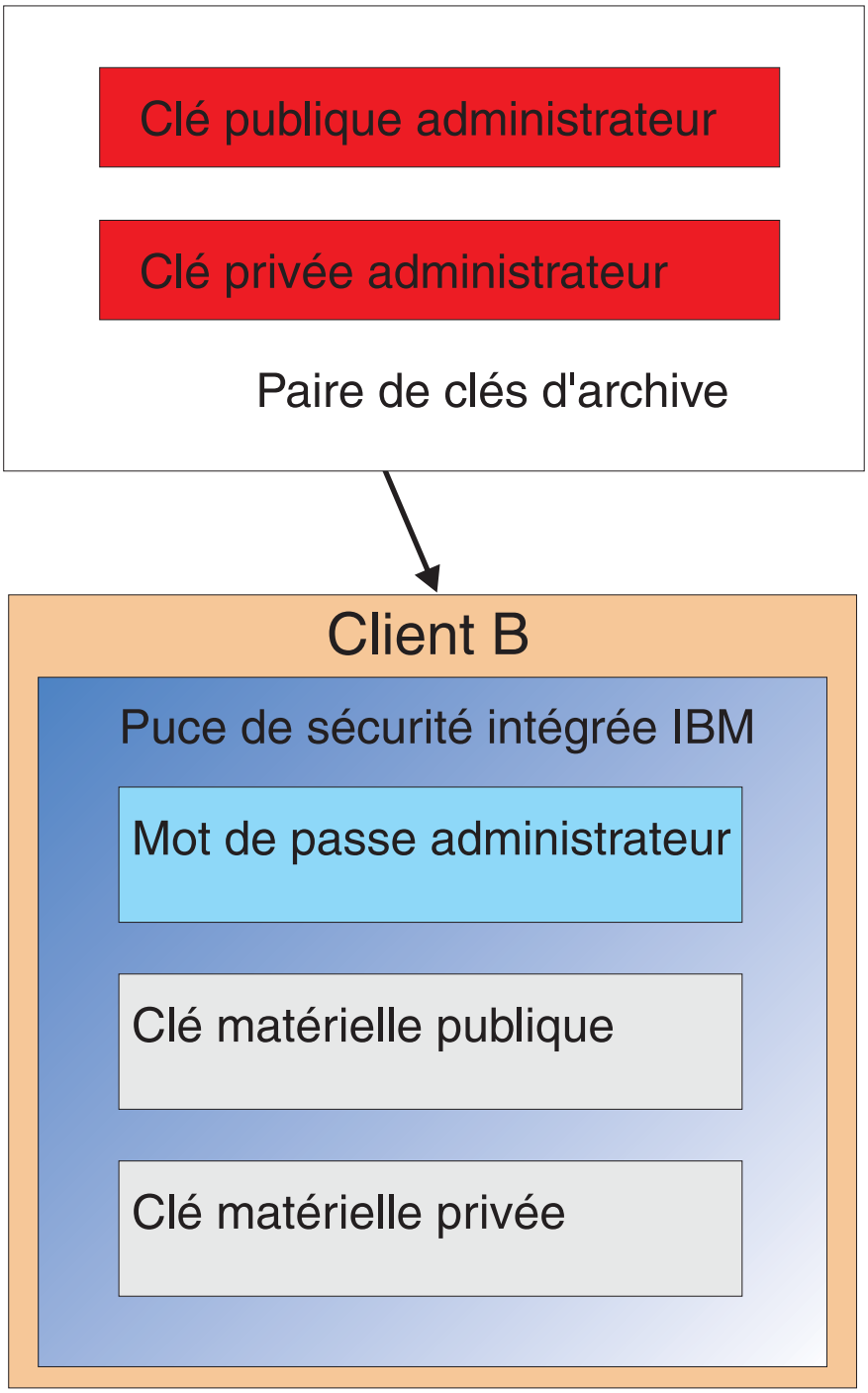

Figure 12. Le Client B extrait les clés publique et privée de l'administrateur à partir de l'emplacement d'archive.

4. La figure 13 illustre le chiffrement de la clé privée administrateur à l'aide de la clé matérielle publique du Client B.

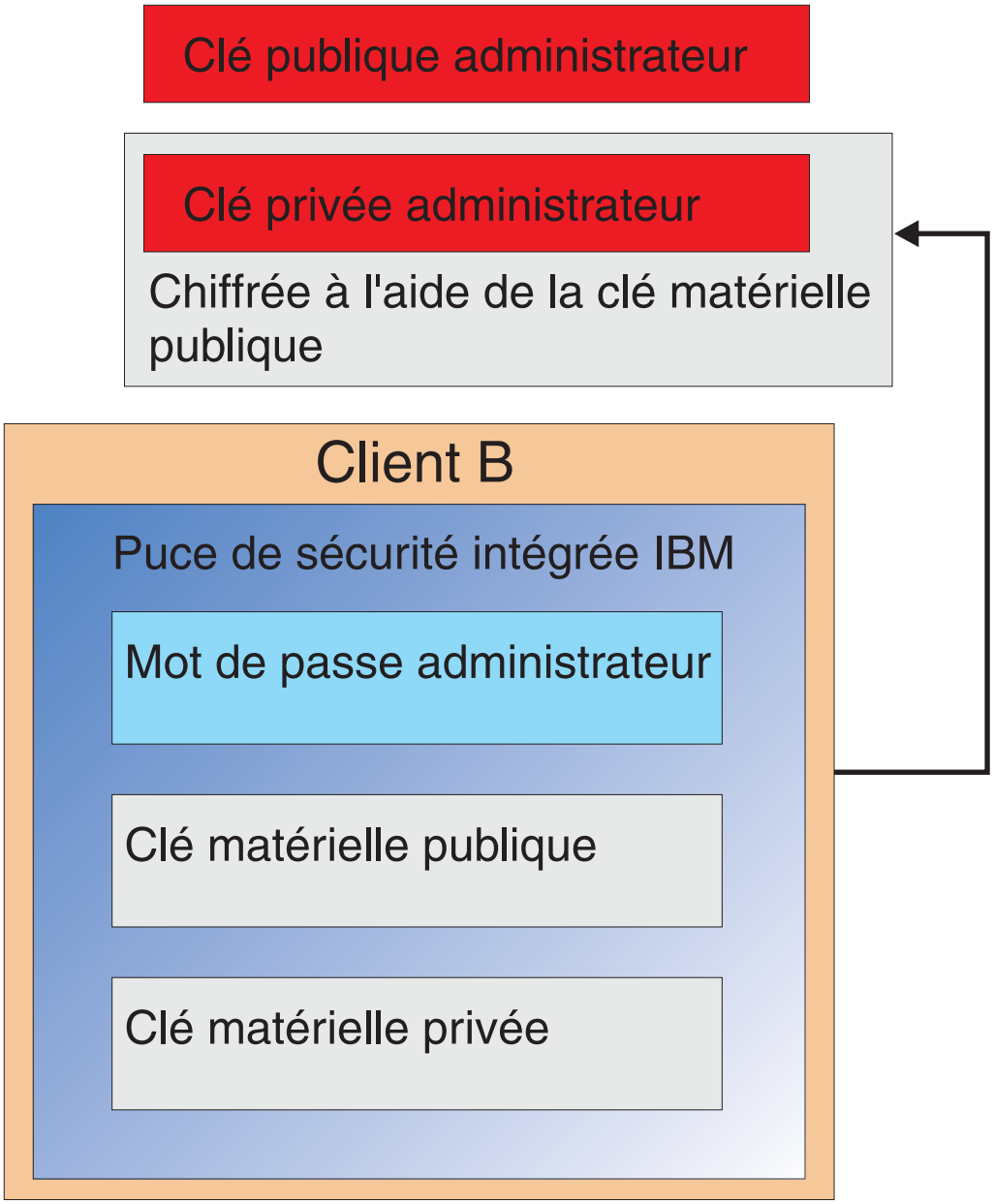

Figure 13. La clé privée de l'administrateur est chiffrée à l'aide de la clé matérielle du Client B.

A présent que la clé privée de l'administrateur a été chiffrée à l'aide de la clé matérielle publique, les accréditations de l'Utilisateur A peuvent être transférées sur le Client B. Cette opération est illustrée dans la figure 14.

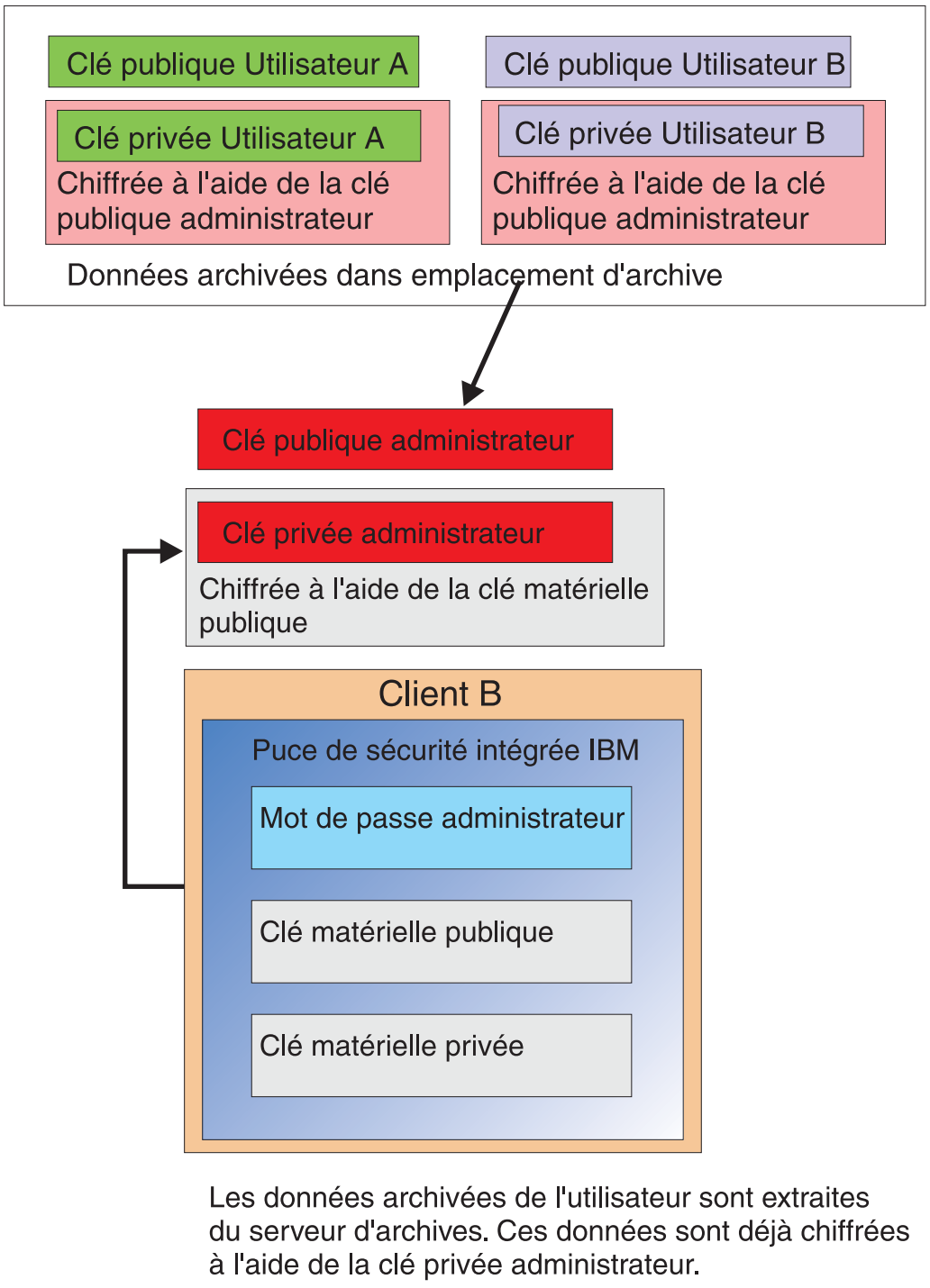

Figure 14. Les accréditations de l'Utilisateur A peuvent être chargées sur le Client B une fois que la clé privée de l'administrateur a été chiffrée.

La figure 15 à la page 25 illustre la restauration complète de l'Utilisateur A sur le Client B. Remarque : La clé privée de l'Utilisateur A a été chiffrée à l'aide de la clé publique de l'administrateur sur le serveur d'archives. La clé publique de l'administrateur est une clé RSA 2048 bits virtuellement impossible à briser. Cela signifie qu'il n'est pas nécessaire que l'emplacement d'archive soit protégé ou ou qu'il dispose d'une liste de contrôle d'accès renforcée. Tant que la paire de clés d'archive (clés publique et privée de l'administrateur) et plus spécifiquement la clé privée de l'administrateur, sont conservées en lieu sûr, l'emplacement d'archive des accréditations de l'utilisateur importe peu.

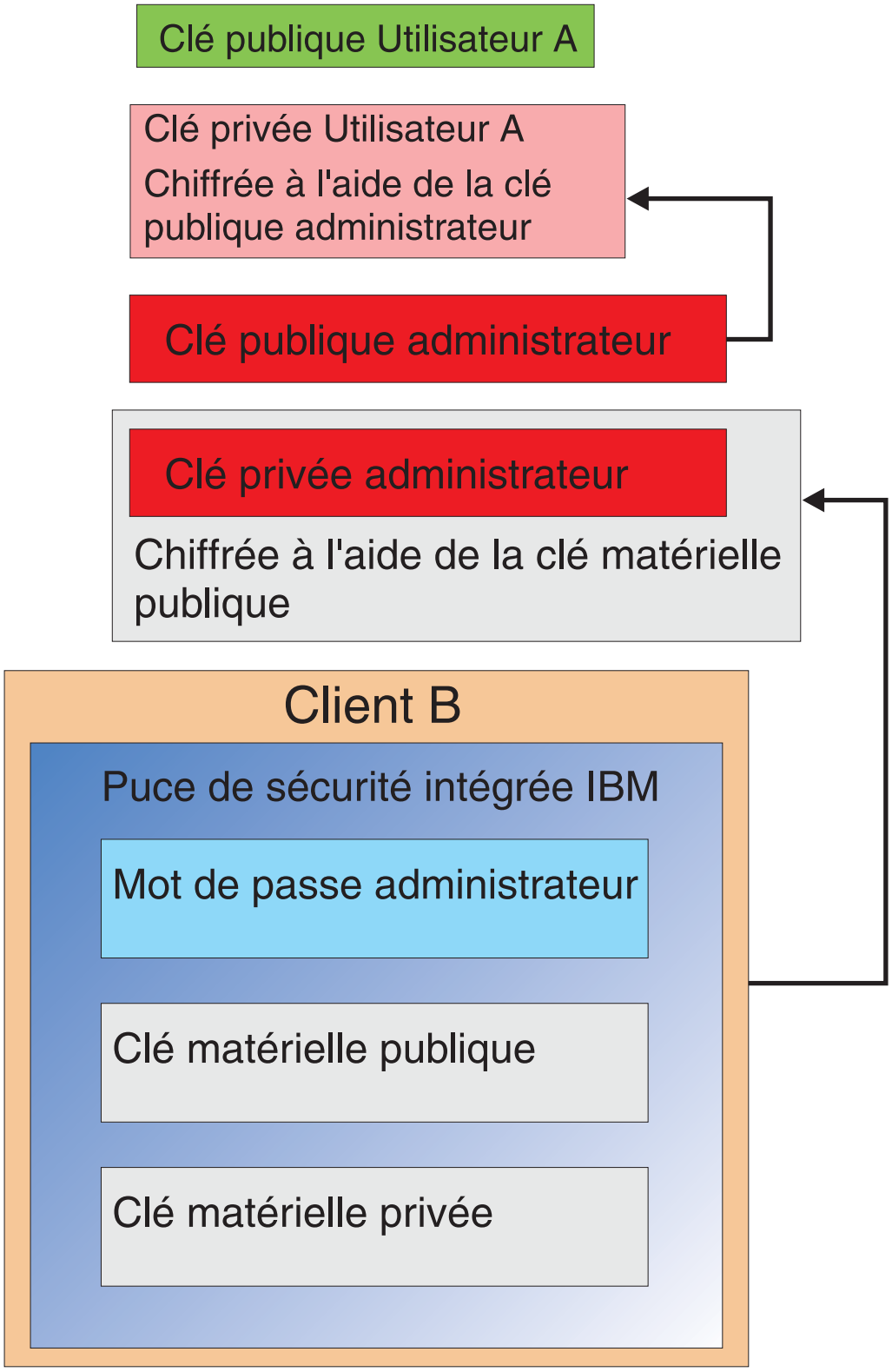

Figure 15. Restauration complète de l'Utilisateur A sur le Client B

La définition du mot de passe administrateur, les emplacements d'archive, etc., sont présentés de façon plus détaillée dans la section relative à l'installation du logiciel. La Figure 16 illustre une vue d'ensemble des composants dans un environnement de sous-système intégré (ESS). Elle indique clairement que chaque

client est unique du point de vue des clés matérielles privée et publique, mais que ses clés publique et privée administrateur sont communes. Les clients disposent d'un emplacement d'archive commun mais ce dernier peut être pour un segment ou un groupe d'utilisateurs.

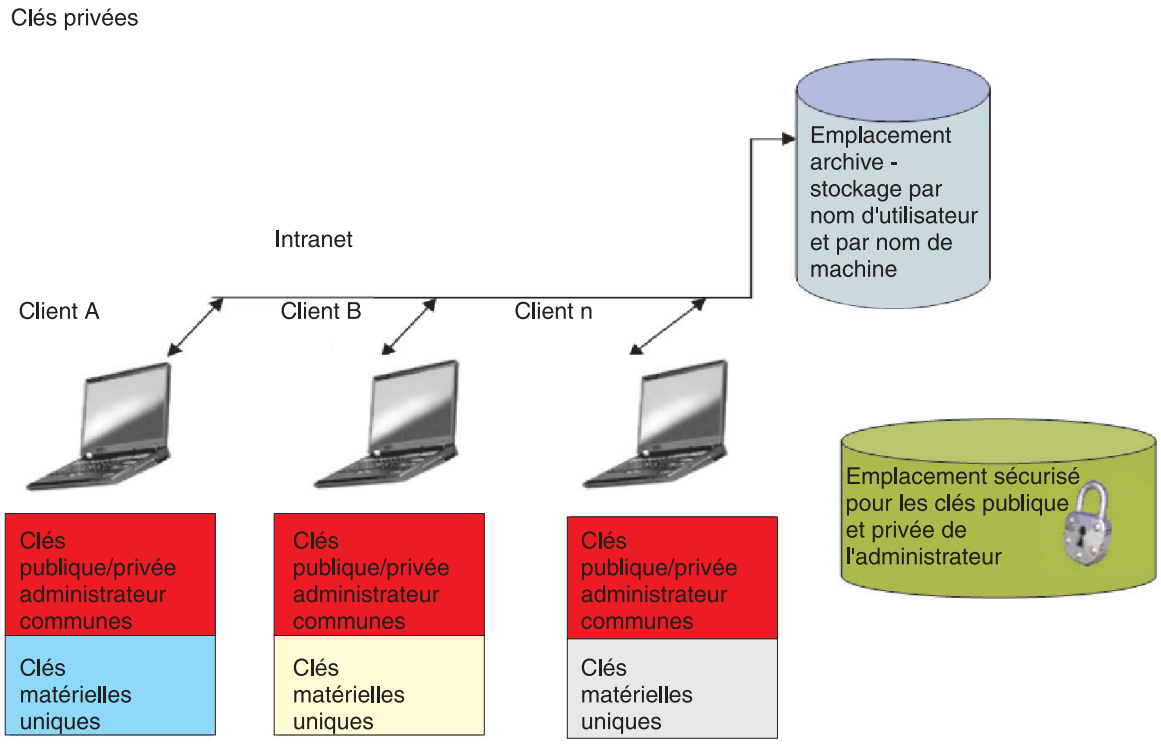

Figure 16. Principaux composants du Logiciel IBM Client Security.

Prenons l'exemple qui suit. Supposons que le service des Ressources humaines dispose d'un emplacement d'archive distinct au niveau du service Informatique. L'archivage est effectué par nom d'utilisateur et par nom d'ordinateur. Le Logiciel IBM Client Security archive les données utilisateur d'un système à l'emplacement d'archive défini, sur la base du nom d'utilisateur et du nom d'ordinateur, comme indiqué plus haut pour l'Utilisateur A et l'Utilisateur B. Notez également que les clés publique et privée de l'administrateur figurent dans un emplacement sécurisé.

Remarque : Chaque nom d'ordinateur et chaque nom d'utilisateur à archiver dans un même emplacement doit être unique. Tout nom d'ordinateur ou nom d'utilisateur en double remplace toute archive portant le même nom.

Chapitre 5. Logiciel IBM Client Security

Le Logiciel IBM Client Security constitue la connexion entre les applications et la puce de sécurité intégrée IBM, ainsi que l'interface pour l'inscription des utilisateurs, la définition de stratégies, et l'exécution de fonctions d'administration de base. Le Logiciel IBM Client Security est constitué essentiellement des composants suivants :

- Utilitaire d'administration
- Utilitaire de configuration utilisateur
- Console d'administration
- Assistant d'installation
- Gestionnaire UVM (User Verification Manager)
- Cryptographic Service Provider
- Module PKCS #11

Le Logiciel IBM Client Security permet d'exécuter plusieurs fonctions essentielles :

- Inscription d'utilisateurs
- Définition de stratégies
- Définition de stratégies de mot de passe composé
- Restauration de mots de passe composés oubliés
- Restauration d'accréditations utilisateur

Par exemple, si l'Utilisateur A se connecte au système d'exploitation, IBM Client Security en tient compte pour toutes les prises de décision. (**Remarque :** La stratégie de sécurité dépend du poste et non de l'utilisateur ; elle concerne tous les utilisateurs d'un seul ordinateur.) Si l'Utilisateur A tente d'agir au niveau d'IBM ESS, IBM Client Security met en oeuvre les stratégies de sécurité telles qu'elles sont définies pour l'Utilisateur A sur cet ordinateur (authentification par mot de passe ou empreinte digitale, par exemple). Si la personne connectée sous le profil Utilisateur A ne peut pas fournir le mot de passe composé correct ou l'empreinte digitale requise pour l'authentification, IBM ESS ne l'autorise pas à effectuer l'action demandée.

Inscription d'utilisateurs et gestion des inscriptions

Les utilisateurs IBM ESS sont simplement des utilisateurs Windows inscrits dans l'environnement IBM ESS. Plusieurs méthodes, décrites plus loin dans ce manuel, sont proposées pour l'inscription des utilisateurs. La présente section décrit uniquement le processus d'inscription. Une bonne compréhension de ce processus vous permettra de mieux cerner le fonctionnement d'IBM ESS et à terme de l'adapter à votre environnement.

Le Logiciel Client Security utilise le Gestionnaire UVM (User Verification Manager) pour gérer les mots de passe composés et d'autres éléments pour authentifier les utilisateurs système. Le logiciel UVM permet d'activer les fonctions suivantes :

- Protection de stratégie client UVM
- Protection de la connexion au système par UVM
- Protection de l'écran de veille du Logiciel Client Security par UVM

A chaque utilisateur de l'environnement IBM ESS est associé au moins un objet de personnalisation utilisé à des fins d'authentification. Le minimum requis est un mot de passe composé. Chaque utilisateur défini dans le composant UVM au sein de l'environnement d'IBM ESS (pour l'utilisateur, UVM gère l'authentification et met en oeuvre une stratégie de sécurité) doit disposer d'un mot de passe composé, lequel doit être fourni au moins une fois à chaque démarrage de l'ordinateur. Les sections qui suivent vous indiquent pourquoi un mot de passe composé est nécessaire, comment le définir et comment l'utiliser.

Raisons pour lesquelles un mot de passe composé est nécessaire

Un mot de passe composé est en premier lieu nécessaire pour de simples raisons de sécurité. Disposer d'un composant matériel tel que le Sous-système de sécurité intégré IBM (IBM ESS) représente un énorme avantage car il offre un emplacement sécurisé et autonome pour les accréditations utilisateur. Néanmoins, la protection assurée par ce type de puce ne sera que de courte durée si le niveau d'authentification requis pour y accéder est très faible. Imaginons, par exemple, que vous disposiez d'une puce matérielle dédiée à l'exécution de fonctions de sécurité. Cette puce ne nécessite, pour un appel d'opération, que d'un seul chiffre pour s'authentifier. Un éventuel pirate informatique n'aurait alors qu'à deviner un chiffre unique (de 0 à 9) pour appeler des opérations à l'aide de vos accréditations. L'authentification par chiffre unique réduit le niveau de sécurité de la puce dans la mesure où elle n'apporte aucune valeur ajoutée par rapport à une solution logicielle. Aucune amélioration du niveau de sécurité ne pourra être obtenue si vous n'associez pas une authentification renforcée à la protection matérielle. L'exigence d'un mot de passe composé par IBM ESS permet ainsi d'authentifier un utilisateur avant qu'il n'exécute des actions au niveau matériel à l'aide d'accréditations utilisateur. Le mot de passe composé UVM ne peut être récupéré que via la paire de clés administrateur. Par conséquent, il ne peut pas être extrait d'un système volé.

Définition d'un mot de passe composé

Chaque utilisateur sélectionne un mot de passe composé destiné à protéger leurs accréditations. La Chapitre 3, «Fonctionnement de la puce de sécurité intégrée», à la page 9 vous indique qu'une clé privée utilisateur est chiffrée en même temps que la clé publique administrateur. Un mot de passe composé est également associé à cette clé privée utilisateur. Il permet d'authentifier l'utilisateur à partir de ses accréditations. La figure 17 indique le mot de passe composé et la clé privée chiffrée à l'aide de la clé publique administrateur.

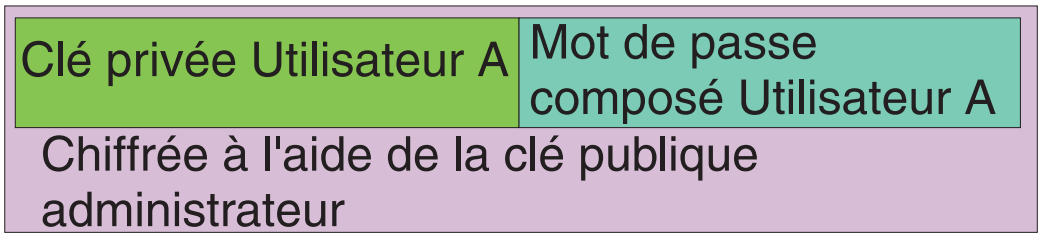

Figure 17. L'Utilisateur A doit fournir le mot de passe composé pour pouvoir effectuer les fonctions nécessitant la clé privée Utilisateur A.

Le mot de passe illustré à la figure 17 à la page 28 est sélectionné par l'utilisateur sur la base de la stratégie existante, autrement dit, sur les règles mises en oeuvre pour contrôler la création de mot de passe. Il s'agit entre autres du nombre de caractères et du nombre de jours de validité. Le mot de passe composé est créé au moment de l'inscription d'un utilisateur dans le gestionnaire UVM. Ce dernier processus, qui a lieu lors de la mise en oeuvre d'IBM Client Security, est décrit plus loin dans le présent document.

La clé privée de l'Utilisateur A est chiffrée en même temps que la clé publique administrateur, car le déchiffrement de la clé privée n'est possible qu'à l'aide de la clé privée administrateur. Ainsi, en cas d'oubli du mot de passe composé par un Utilisateur A, l'administrateur peut redéfinir un nouveau mot de passe composé.

Utilisation d'un mot de passe composé

Le traitement du mot de passe composé utilisateur sur la puce est illustré de la figure 18 à la page 30 à la figure 20 à la page 32. Un mot de passe composé doit toujours être entré en début et au moins une fois par session. De plus, l'indication d'un mot de passe composé est obligatoire. Vous pouvez choisir des unités d'authentification supplémentaires ; cependant, aucune de ces unités ne peut remplacer la saisie initiale obligatoire d'un mot de passe composé utilisateur. En règle générale, les informations biométriques et autres données d'authentification sont chiffrées à l'aide de la clé publique de l'utilisateur. Un accès à la clé privée est nécessaire pour le déchiffrage de données de sécurité supplémentaires.

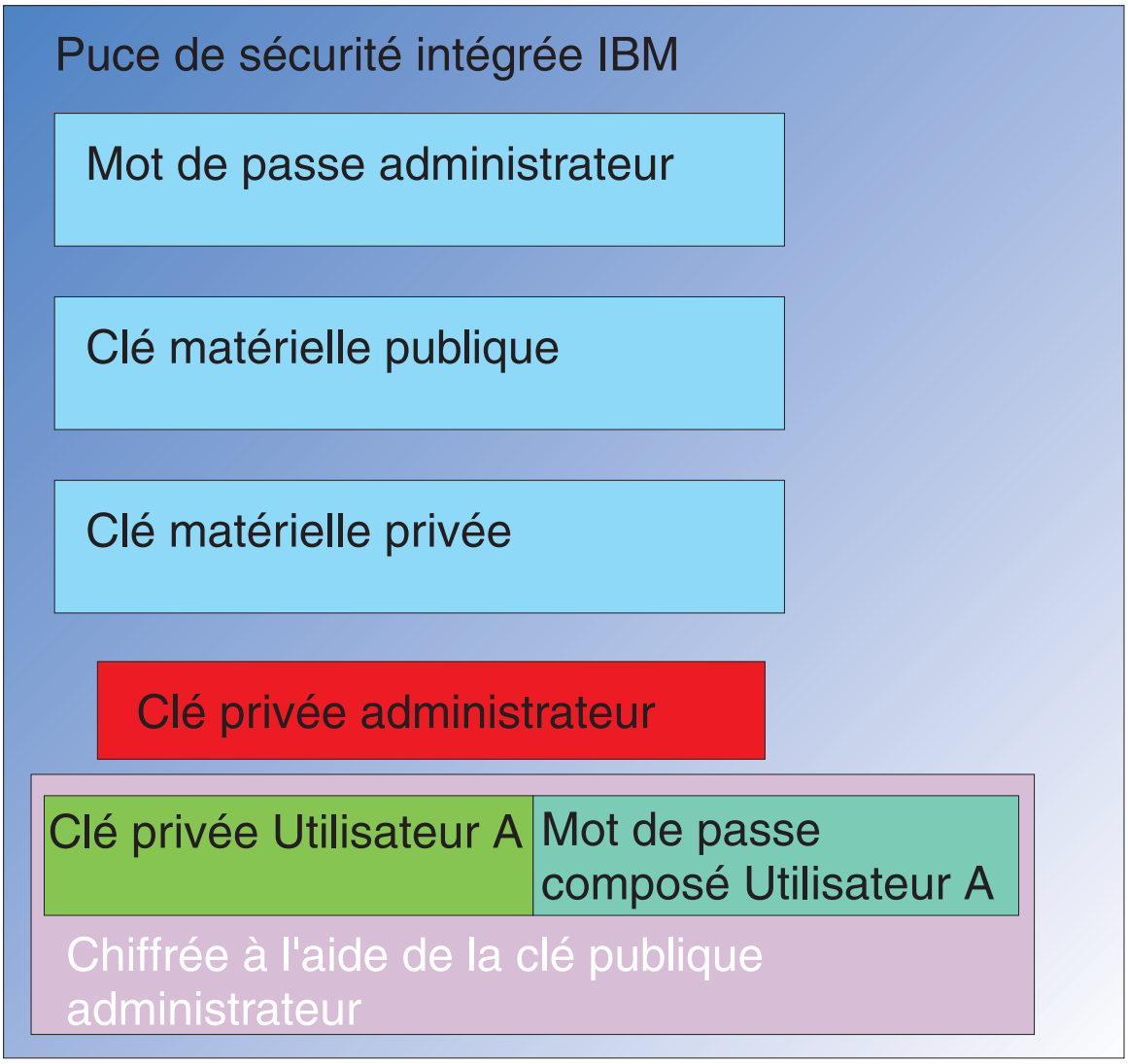

Figure 18. La clé privée de l'administrateur est déchiffrée dans la puce.

La saisie au moins une fois par session du mot de passe composé est donc obligatoire pour le déchiffrage de ces données supplémentaires. Les accréditations qui composent le clé privée et le mot de passe composé de l'Utilisateur A et qui sont chiffrées à l'aide de la clé publique de l'administrateur sont transférées dans la puce de sécurité intégrée IBM. La clé privée de l'administrateur est elle-même déjà déchiffrée dans la puce comme indiqué plus haut. Les accréditations sont transférées comme illustré à la figure 19 à la page 31.

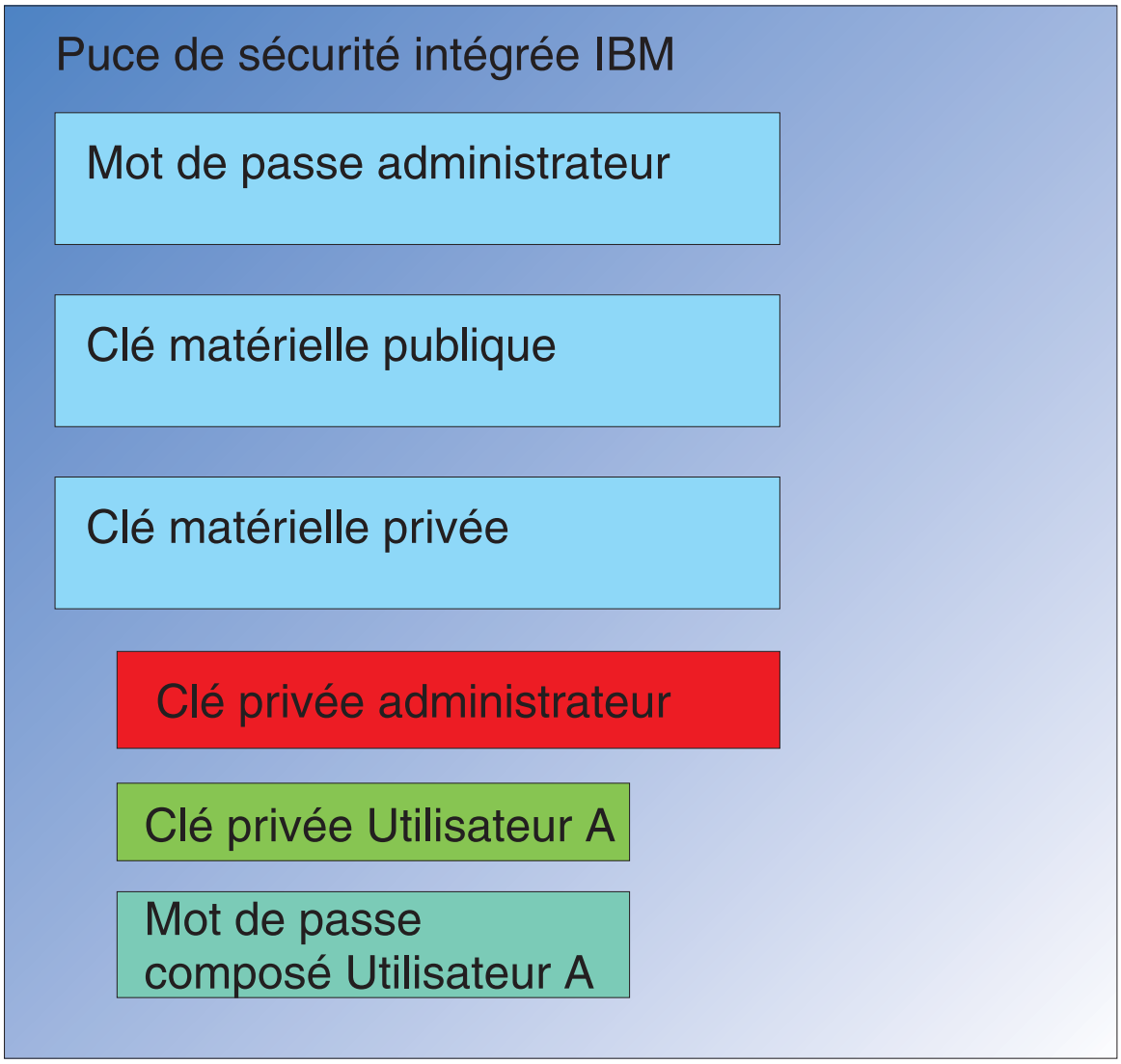

Figure 19. La clé privée ainsi que le mot de passe composé de l'Utilisateur A sont disponibles dans la puce.

Les accréditations sont déchiffrées, rendant ainsi disponibles la clé privée ainsi que le mot de passe composé de l'Utilisateur A dans la puce. Lorsque l'utilisateur connecté, identifié par IBM Client Security comme étant l'Utilisateur A, tente d'utiliser les accréditations de l'Utilisateur A, une boîte de dialogue de saisie du mot de passe composé s'affiche, comme illustré à la figure 20 à la page 32.

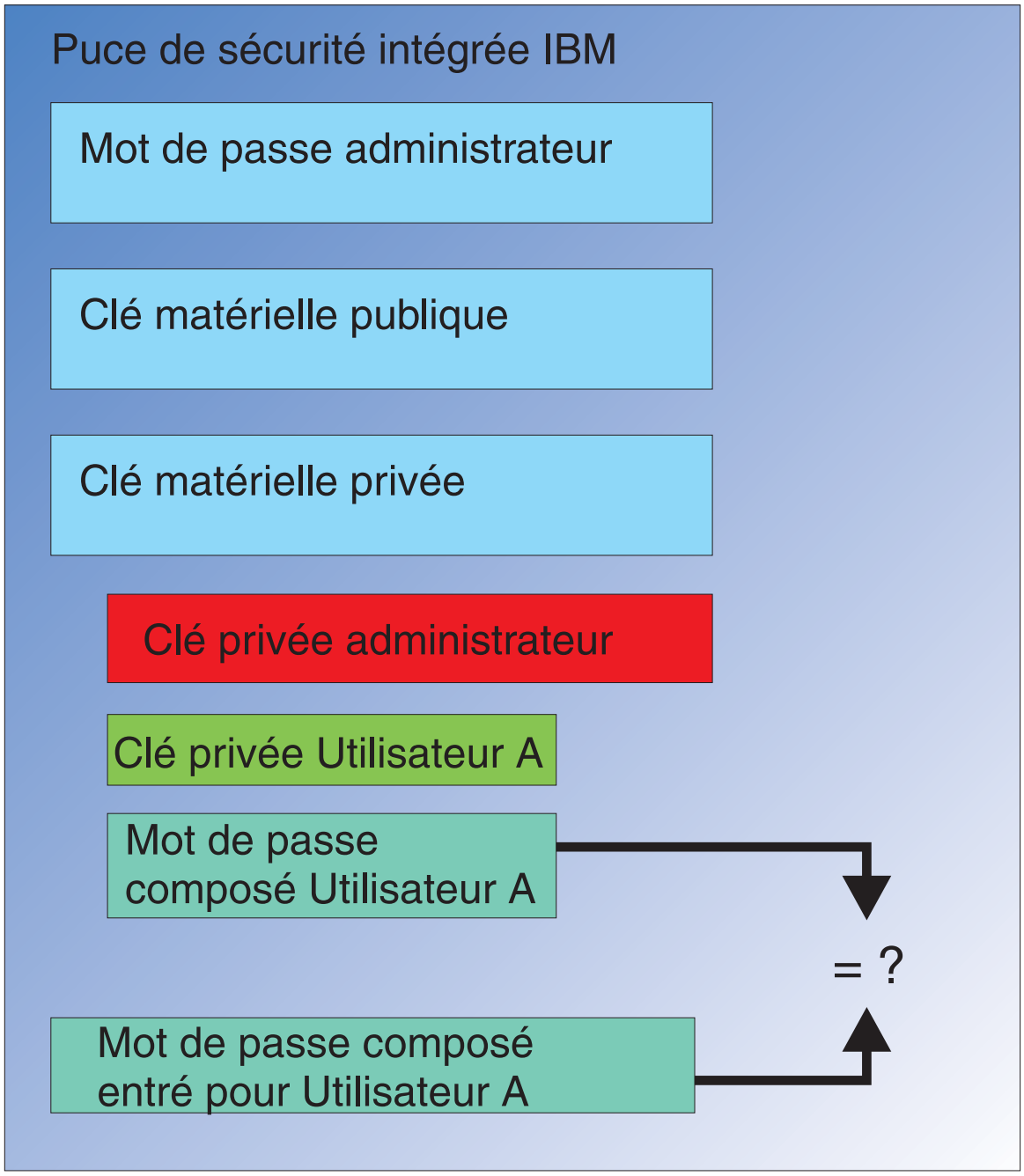

Figure 20. Lorsque l'utilisateur l'Utilisateur A essaie d'utiliser les accréditations de l'Utilisateur A, une boîte de dialogue de saisie du mot de passe composé s'affiche.

Le mot de passe composé saisi est transféré dans la puce et comparé à la valeur du mot de passe composé déchiffré. Si les valeurs coïncident, les accréditations de l'Utilisateur A peuvent alors être utilisées pour l'exécution de fonctions (signatures numériques ou déchiffrement d'e-mails, par exemple). Il est à noter que cette comparaison est effectuée dans l'environnement sécurisée de la puce. Celle-ci est dotée de fonctions permettant de détecter les échecs répétés de tentatives d'accès. De plus, le mot de passe composé enregistré de l'Utilisateur A n'est jamais accessible à l'extérieur de la puce. Par ailleurs, l'inscription des utilisateurs a lieu au cours de l'installation du Logiciel IBM Client Security. La création du mot de passe composé de l'utilisateur constitue l'une des étapes de ce processus

d'inscription. La procédure de définition de ce caractéristiques ainsi que l'application de règles de mot de passe composé sont décrites plus loin.

La figure 1 à la page 1 illustrait la puce de sécurité intégrée IBM ainsi que le Logiciel IBM Client Security. La figure 1 à la page 1 illustre également l'initialisation entreprise et l'initialisation utilisateur. L'initialisation entreprise est associée au Sous-système de sécurité intégré, l'initialisation utilisateur étant associée au Logiciel IBM Client Security. Cette initialisation a été brièvement décrite dans les sections précédentes afin que vous en compreniez le concept général. Dans les sections ci-après, le processus d'initialisation est décrit de façon plus détaillée.

Initialisation TPM

L'initialisation TPM est un processus qui consiste essentiellement à ajouter des clés matérielles publique et privée ainsi qu'un mot de passe administrateur. La machine générique qui vous a été livrée par IBM devient ainsi unique pour votre entreprise. Le tableau ci-après indique les méthodes mises en oeuvre pour l'initialisation des clés publique et privée et des mots de passe administrateur.

Tableau 3. Méthodes d'initialisation du matériel

Action	Création possible dans le BIOS	Création manuelle possible par l'administrateur dans le Logiciel CSS	Création possible dans un script
Clé matérielle publique/privée	Non	Oui	Oui
Mot de passe administrateur	Oui, sur certains clients compatibles TCPA. Vérifier entrée du BIOS.	Oui	Oui

Le tableau 3 indique clairement que les clés matérielles privée et publique ne sont pas créées lors de l'installation du logiciel. Leur création doit être effectuée manuellement dans le logiciel ou à l'aide d'un script. Le mot de passe administrateur peut être créé dans le BIOS, dans le Logiciel IBM Client Security, ou à l'aide d'un script. La puce contrôle les valeurs définies pour les clés matérielles privée et publique ; vous ne pouvez en aucun cas définir ces valeurs. Une fonction de génération aléatoire de nombre permet de produire des paires de clés publique et privée statistiquement aléatoires. En revanche, c'est à vous qu'il revient de définir le mot de passe administrateur.

Le mot de passe administrateur est différent car sa valeur doit être définie par l'administrateur. Plusieurs questions doivent ainsi être posées concernant ce mot de passe :

- Qu'allez-vous définir comme mot de passe ou mots de passe administrateur ?
- Allez-vous utiliser plusieurs mots de passe pour différents groupes ? Le cas échéant, comment allez-vous déterminer le mot de passe à associer à chaque ordinateur ?
- Quel administrateur aura accès au mot de passe ? Si vous disposez de plusieurs mots de passe pour des groupes d'utilisateurs distincts, quel administrateur aura accès à quels mots de passe ?
- Les utilisateurs finals auto-administrés auront-ils accès au mot de passe administrateur ?

Pour vous aider à trouver les réponses appropriées aux questions ci-dessus, il est important que vous sachiez ce qu'un mot de passe administrateur permet de faire :

- Accès aux utilitaires de l'administrateur
- Ajout/suppression d'utilisateurs
- Définition des applications/fonctions du Logiciel IBM Client Security pouvant être utilisées

Les sections ci-après décrivent la relation qui existe entre le fichier de stratégie et la clé privée administrateur. Il est important de savoir que la clé privée administrateur est nécessaire pour modifier une stratégie. Le tableau 4 récapitule les capacités que confère le mot de passe administrateur et/ou la clé privée administrateur.

Tableau 4. Actions administrateur nécessitant un mot de passe et une clé privée

Action	Mot de passe administrateur	Clé privée administrateur
Accès aux utilitaires de l'administrateur	Oui	Non
Ajout/Retrait/Restauration d'utilisateurs	Oui	Non
Définition des applications/fonctions CSS pouvant être utilisées	Oui	Non
Définition/modification de stratégies	Oui	Oui
Création d'un fichier permettant de réinitialiser le mot de passe composé d'un utilisateur	Oui	Oui

Le processus d'initialisation TPM fait également référence à la clé publique et privée administrateur. Le tableau ci-dessus indique les capacités associées à cette clé. La définition des clés publique et privée de l'administrateur constitue donc une étape importante. Cette paire de clés peut en effet être unique pour chaque ordinateur ou identique pour toutes les machines. L'administrateur a le choix entre utiliser une paire de clés existante ou créer une nouvelle paire de clés pour le client lors de l'initialisation du Logiciel IBM Client Security. Encore une fois, la configuration la mieux adaptée à votre entreprise doit être déterminée par un modèle d'utilisation.

Méthodes éprouvées

Les grandes entreprises peuvent utiliser une clé unique pour chaque machine ou une clé unique pour chaque service. Vous pouvez, par exemple, définir un mot de passe administrateur et/ou une clé privée administrateur pour tous les ordinateurs utilisés au sein du service des ressources humaines, un autre pour le service informatique, etc. Vous pouvez également utiliser un processus de différenciation de type physique, comme l'emplacement d'un immeuble ou d'un site. Il devient ensuite facile de déterminer la clé privée administrateur à utiliser lors de la création d'un fichier de réinitialisation de mot de passe en fonction de l'utilisateur qui demande cette réinitialisation. Comme l'indiquent le tableau 3 à la page 33 et le tableau 5 à la page 37, une initialisation utilisateur et entreprise, ou matérielle, doit également avoir lieu.

Définition de la stratégie de sécurité avant le déploiement de CSS

Chaque entité de votre entreprise concernée par le déploiement de CSS a des exigences en matière de sécurité et d'authentification. Bien que les utilisateurs possédant un droit d'accès administrateur puissent modifier la stratégie de sécurité et forcer la transmission de ces modifications sur les ordinateurs client (voir Chapitre 8, «Déploiement à distance de fichiers de stratégie de sécurité nouveaux ou modifiés», à la page 61), une configuration des paramètres de stratégie de sécurité préalable au déploiement permettra d'obtenir de meilleurs résultats. Pour de plus amples informations sur la définition de la stratégie, reportez-vous à la section relative à la gestion de la stratégie UVM du manuel *Logiciel Client Security - Guide d'administration*.

Préparation en prévision des oublis de mots de passe composés ou des dysfonctionnements des unités d'authentification

Il est inévitable que certains utilisateurs oublient leur mot de passe composé et il peut arriver que les unités d'authentification, telles que les unités biométriques d'enregistrement d'empreinte ou les cartes à puce, ne fonctionnent pas correctement.

Oubli du mot de passe composé : Le mot de passe composé de l'utilisateur n'est pas stocké sur le disque dur client ou dans la puce de sécurité intégrée sous une forme lisible par un être humain. Il est conservé en sécurité dans la mémoire de l'utilisateur et dans l'archive protégée par la paire de clés administrateur. L'administrateur devra déchiffrer les informations utilisateur contenues dans l'archive à l'aide de sa clé privée administrateur. Il pourra ensuite fournir unn nouveau mot de passe composé à l'utilisateur.

Lorsque l'utilisateur modifie son mot de passe composé, la nouvelle information est archivée dans l'emplacement d'archive spécifié.

Au cas où l'unité d'authentification présenterait des dysfonctionnements, vous pouvez configurer le logiciel IBM Client Security afin qu'il affiche un bouton de contournement **Cliquez ici pour continuer**. Si l'utilisateur clique sur ce bouton, il lui suffit pour pouvoir poursuivre de saisir le mot de passe composé correct. L'utilisateur peut ensuite exécuter des tâches sécurisées.

Pour configurer CSS afin que ce bouton de contournement soit affiché, procédez comme suit :

1. Dans le fichier CSEC.INI (situé dans le répertoire racine), localisez l'entrée `AllowBypass= 0`. Si cette entrée est définie par la valeur par défaut `0`, CSS masque le bouton de contournement.
2. Donnez la valeur 1 à `AllowBypass`. Le bouton de contournement s'affichera lorsqu'une fenêtre CSS demandera à un utilisateur, outre de fournir le mot de passe composé, de s'authentifier.
3. Enregistrez le fichier CSEC.INI.

Remarques :

1. Pour que cette information puisse être archivée, il est essentiel que l'emplacement d'archive soit indiqué dans le fichier CSEC.INI `kal=c:\jgk\archive`. En outre, si c:\jgk\archive est une unité réseau, cette unité doit être mappée sur l'ordinateur client pour que le mot de passe composé puisse être archivé.

2. Si vous ne spécifiez pas d'emplacement d'archive ou que l'emplacement n'est pas mappé sur l'ordinateur client, les mots de passe composés ne peuvent pas être récupérés.

Initialisation utilisateur

Avec IBM ESS, plusieurs utilisateurs peuvent effectuer simultanément des transactions indépendantes et sécurisées sur un seul ordinateur. Ces utilisateurs doivent utiliser un mot de passe composé ainsi que d'autres méthodes d'authentification (empreintes digitales ou cartes à puce, par exemple). Il s'agit de l'*autorisation multi-facteur*. Le processus d'initialisation utilisateur constitue une étape essentielle lors de la configuration d'ordinateurs client destinés à utiliser IBM ESS. Il se compose de deux parties :

1. Inscription
2. Personnalisation

Inscription

L'inscription consiste simplement à ajouter, ou à enregistrer, un utilisateur dans IBM Client Security. La figure 21 illustre la fonction du gestionnaire UVM (User Verification Manger) dans le Logiciel IBM Client Security. UVM contrôle les accréditations de chaque utilisateur et applique les stratégies.
Un fichier de stratégie, tel que celui représenté dans la figure 21, contient les

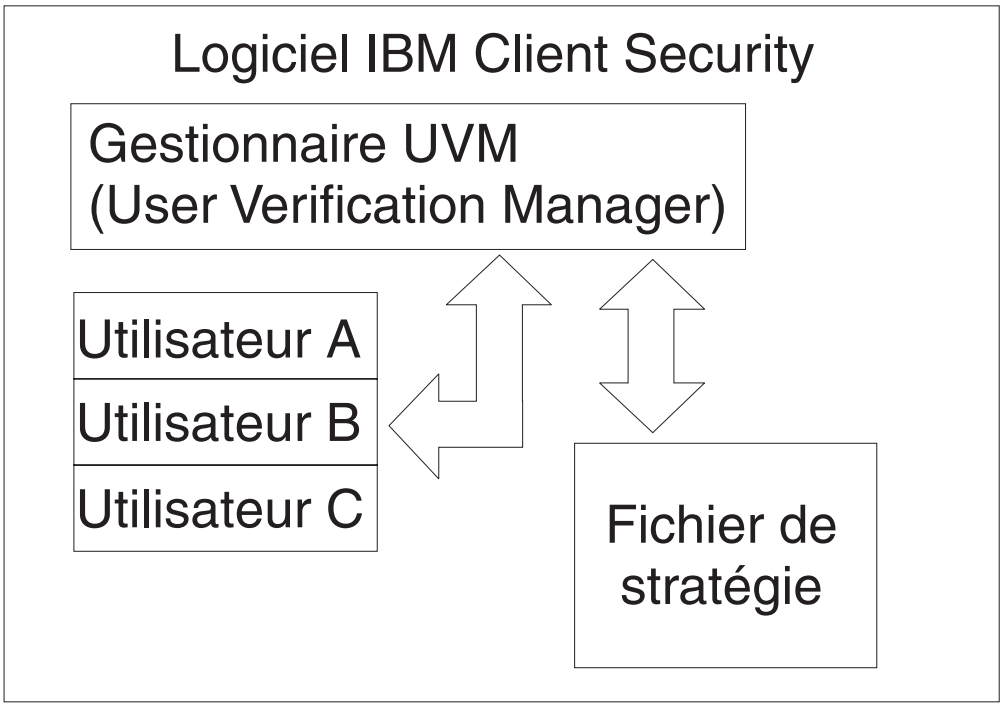

Figure 21. Le gestionnaire UVM (User Verification Manager) contrôle les accréditations de chaque utilisateur et applique les stratégies.

procédures d'authentification requises pour chacun des utilisateurs gérés par UVM. Les utilisateurs UVM sont simplement des utilisateurs Windows (local ou domaine). UVM gère ainsi les accréditations des utilisateurs effectivement connectés sur l'ordinateur et au système d'exploitation. Par exemple, si l'Utilisateur A ouvre une session Windows et que cet Utilisateur A fait également partie d'UVM, ce dernier appliquera la stratégie associée à cet utilisateur lorsque celui-ci tentera d'effectuer des opérations qui nécessitent des accréditations. Dans un autre exemple, l'Utilisateur se connecte à l'ordinateur. Cet Utilisateur A lance ensuite

l'application Microsoft Outlook et envoie un courrier électronique avec une signature numérique. La clé privée utilisée pour l'envoi de ce courrier électronique avec signature numérique est protégée dans le Sous-système de sécurité intégré IBM. Avant que la gestionnaire UVM n'autorise l'exécution de cette opération, il applique la stratégie définie dans le fichier de stratégie associé à l'utilisateur. Dans cet exemple, une authentification par mot de passe composé est requise pour que l'opération puisse être exécutée. UVM invite donc l'utilisateur à entrer le mot de passe composé requis et si le processus de vérification aboutit, l'opération nécessitant l'utilisation de la clé privée peut alors être exécutée dans la puce.

Initialisation personnelle

Le processus d'initialisation personnelle consiste simplement à définir un mot de passe composé UVM personnel d'un individu. Différentes personnes peuvent intervenir au cours des différentes étapes du processus. Le mot de passe composé UVM personnel d'un individu ne doit être connu que de lui. Néanmoins, si chaque individu ne participe pas au processus d'initialisation, cet individu devra peut-être effectuer une opération supplémentaire. Vous pouvez également configurer UVM pour qu'il force l'utilisateur à modifier le mot de passe composé à la première connexion.

Supposons que l'Utilisateur A soit initialisé par l'administrateur informatique. Cet administrateur sélectionne l'Utilisateur A à partir d'une liste d'utilisateurs Windows (au sein d'un domaine, par exemple). UVM lui demande ensuite le mot de passe composé UVM à associer a l'Utilisateur A. L'administrateur entre alors une "valeur par défaut" correspondant à un "mot de passe composé administrateur". A des fins de sécurité du système, l'Utilisateur A qui reçoit le système doit personnaliser ce mot de passe composé afin que personne d'autre que lui ne puisse effectuer des transactions sécurisées à l'aide du mot de passe composé par défaut.

Tableau 5. Méthodes d'initialisation utilisateur

Méthode	Processus	Conditions
Manuelle	L'administrateur peut personnaliser manuellement CSS pour l'utilisateur à l'aide de l'utilitaire d'administration.	La présence de l'administrateur est requise lors de la configuration sur chaque ordinateur.
Fichier de configuration administrateur	L'administrateur peut créer un fichier de configuration qui contient une version chiffrée du mot de passe administrateur. Ce fichier est envoyé à l'utilisateur, lequel peut alors s'inscrire individuellement sans l'intervention ou la présence de l'administrateur.	L'utilisateur effectue la configuration.
*.ini	L'administrateur crée un script qui exécute le fichier .ini et insère un mot de passe par défaut ou personnalisé.	La présence de l'administrateur ou de l'utilisateur est facultative.

Scénarios de déploiement

Vous déployez 1000 clients pour 1000 utilisateurs finals. L'un des scénarios décrits ci-après correspond peut-être à la méthode de déploiement que vous envisagez de mettre en oeuvre :

- Vous savez exactement quelle machine doit être affectée à quel utilisateur final. Par exemple, vous savez que la machine 1 est destinée à Bob et vous l'enregistrez. Bob doit ensuite personnaliser (définir son mot de passe composé personnel) son ordinateur à réception. Nicolas reçoit l'ordinateur, lance le Logiciel IBM Client Security, puis définit son mot de passe composé.
- Vous ne savez pas quelle machine doit être affectée à quel utilisateur final. Vous prenez le client 1 et le livrez à un utilisateur final X.

En raison de ces deux facteurs variables, le déploiement d'IBM ESS va être un peu différent de celui d'une application classique. Il existe néanmoins plusieurs options qui offrent suffisamment de souplesse pour le déploiement d'IBM ESS.

Voici un exemple classique de schéma de livraison de PC dans une entreprise :

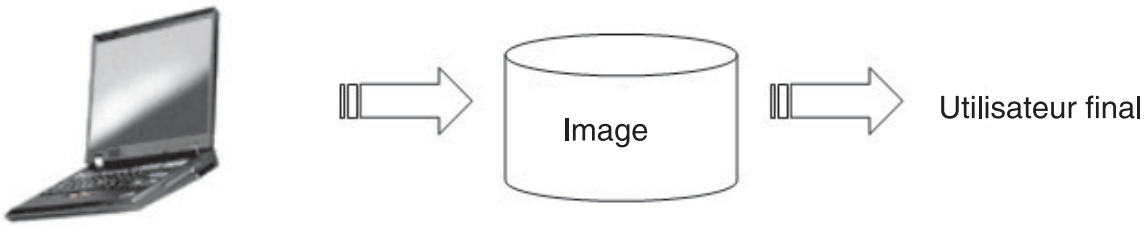

Figure 22. Schéma de livraison classique de PC

Six scénarios de déploiement

Vous disposez de six méthodes de déploiement pour le Logiciel IBM Client Security :

1. **Composant ajouté**—Le code du Logiciel IBM Client Security ne fait pas partie de l'image de disque. Il est installé, initialisé et personnalisé une fois les ordinateurs déployés.
2. **Composant de l'image**—Le code du Logiciel IBM Client Security fait partie de l'image de disque mais il n'est pas installé. Aucune personnalisation, entreprise ou utilisateur, n'a encore été initiée. (Voir figure 23 à la page 40.)
3. **Installation simple**—Le code du Logiciel IBM Client Security est installé et a été personnalisé pour l'entreprise de l'utilisateur final. (Voir figure 24 à la page 41.)
4. **Personnalisation partielle**—Le code du Logiciel IBM Client Security est installé et une personnalisation entreprise uniquement a été effectuée. Aucune personnalisation utilisateur final n'a été initiée. (Voir figure 24 à la page 41.)
5. **Personnalisation temporaire**—Le code du Logiciel IBM Client Security est installé et une personnalisation, entreprise et utilisateur, a été effectuée. L'utilisateur doit réinitialiser son mot de passe composé et, si nécessaire, fournir des données d'authentification supplémentaires, telles que l'association des données scannérisées de ses empreintes digitales ou de sa carte à puce. (Voir figure 25 à la page 42.)
6. **Personnalisation intégrale**—Le code du Logiciel IBM Client Security est installé et une personnalisation, entreprise et utilisateur, a été effectuée. L'administrateur définit le mot de passe composé de l'utilisateur. Si des données d'authentification par empreintes digitales ou autres sont requises, l'utilisateur doit procéder à une personnalisation. (Voir figure 25 à la page 42.)

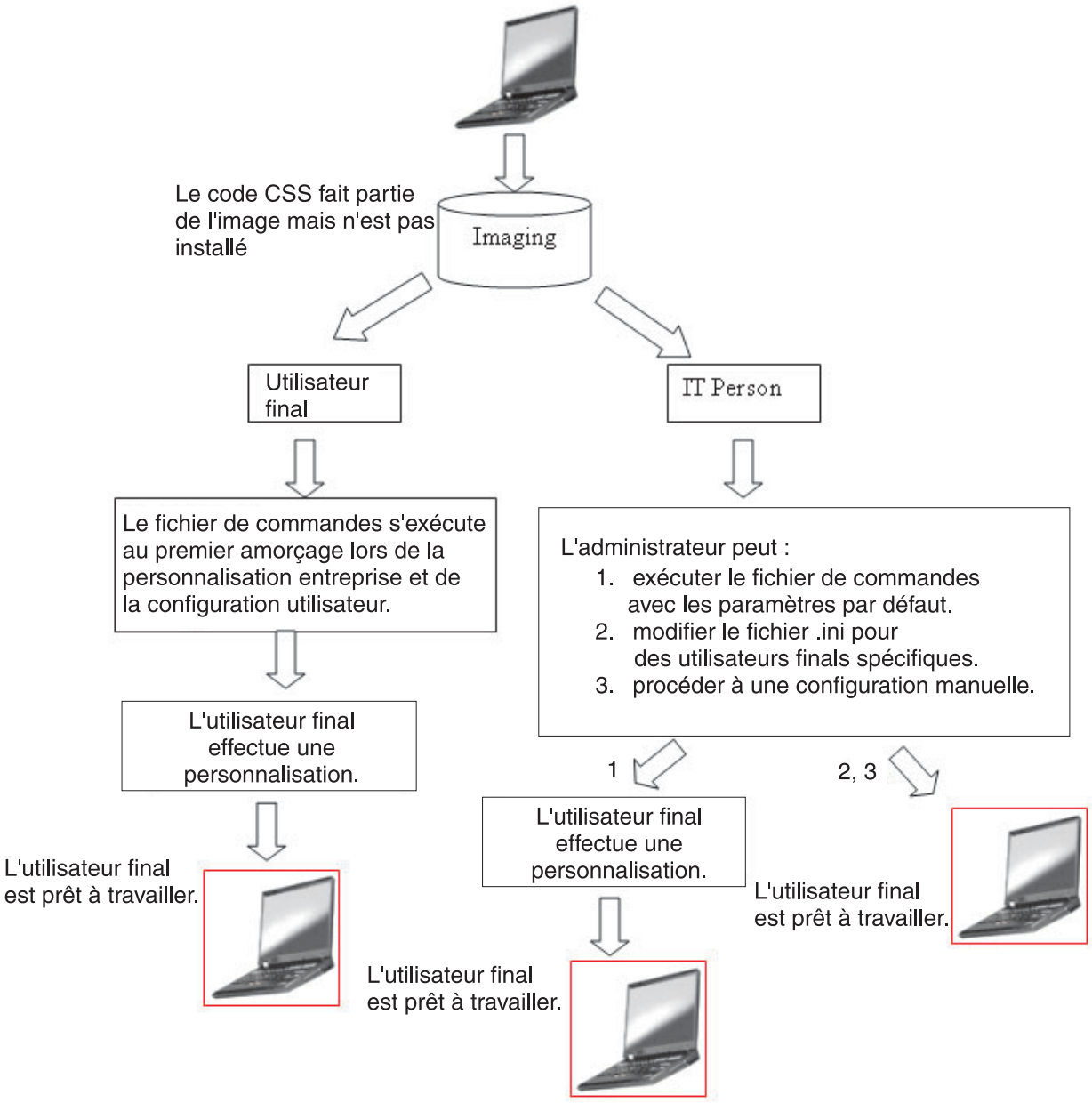

Figure 23. Le code du Logiciel IBM Client Security fait partie de l'image de disque mais il n'est pas installé.

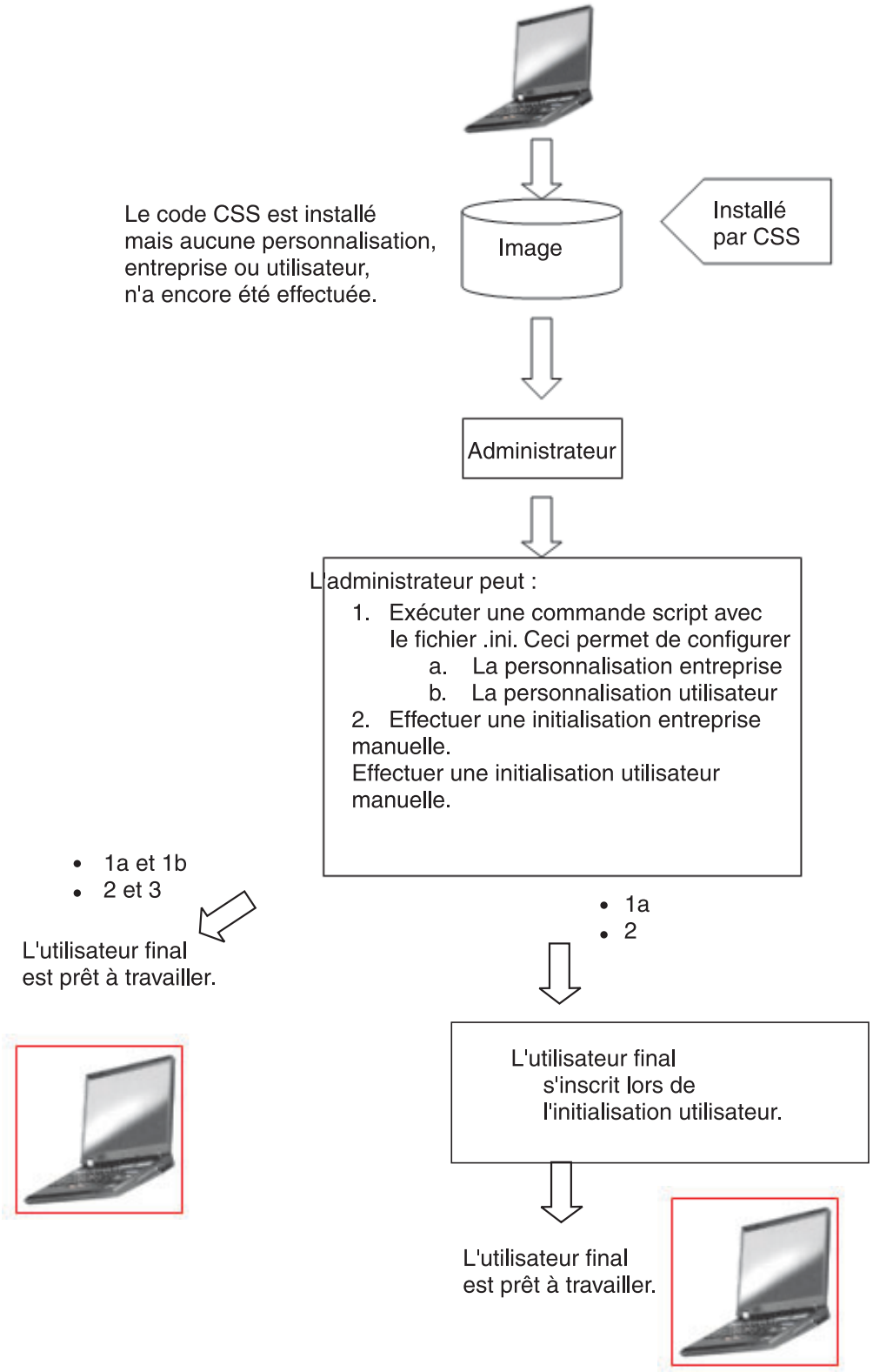

Figure 24. Le code du Logiciel IBM Client Security est installé, mais aucune personnalisation, entreprise ou utilisateur, n'a encore été effectuée.

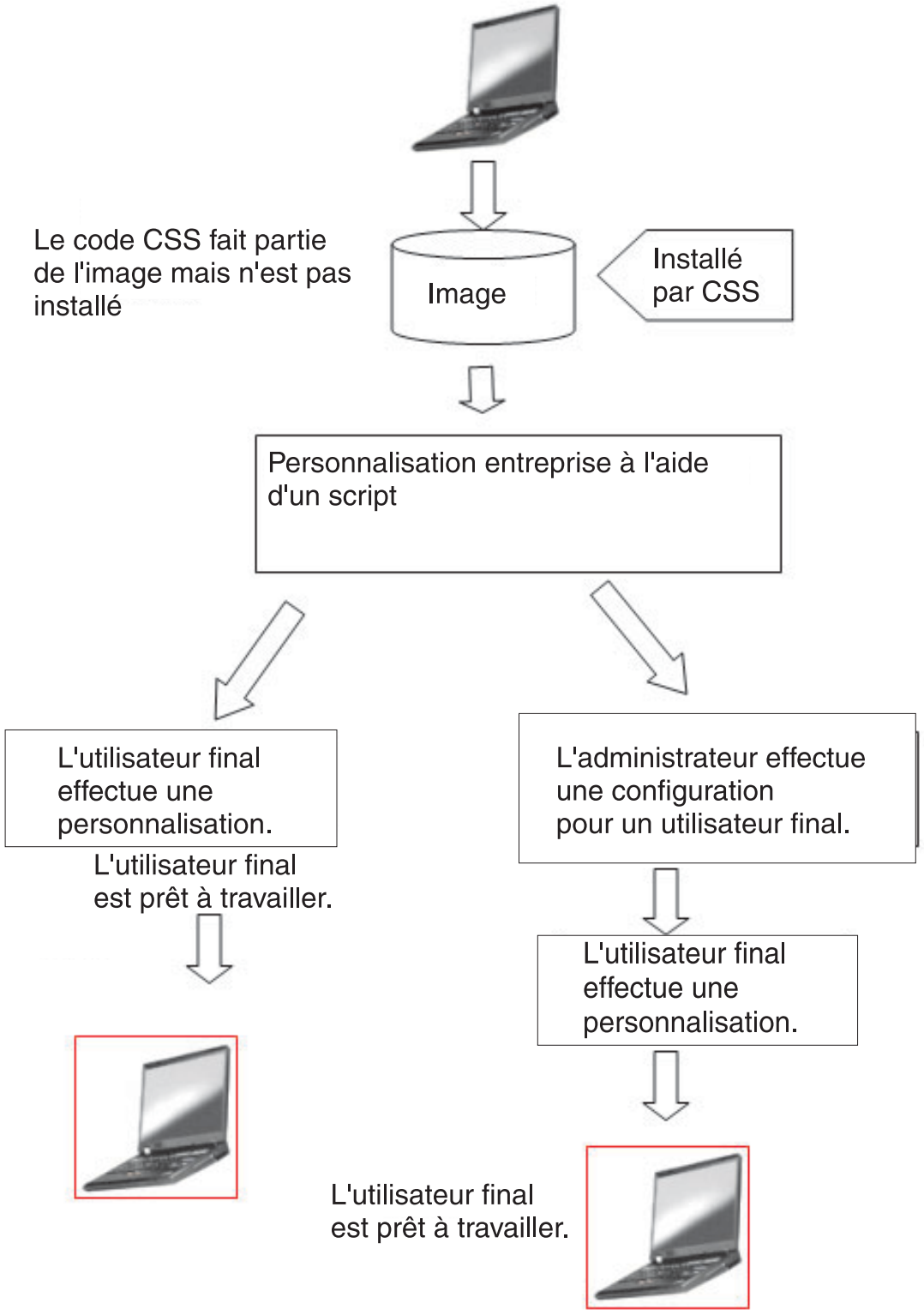

Figure 25. Le code du Logiciel IBM Client Security est installé et une personnalisation, entreprise et utilisateur, a été effectuée.

Dans le scénario 1, le Logiciel IBM Client Security est déployé une fois l'image de disque installée sur l'ordinateur. Le Logiciel IBM Client Security est installé et configuré et la puce de sécurité intégrée est configurée une fois l'image de disque installée.

Les scénarios 2 à 6 correspondent aux différentes options de déploiement et de configuration des logiciels et de configuration de puce. Vous pouvez choisir le scénario et la méthode d'installation les mieux adaptés à votre entreprise en fonction de ses contraintes et de son environnement.

Détails du fichier de configuration

Pour ce faire, vous pouvez lancer l'assistant Client Security : CSECWIZ.EXE dans le répertoire Security. A l'issue de l'assistant, cochez la case en regard de l'option **Sauvegardez les paramètres mais ne configurez pas le sous-système. (Les paramètres vont être sauvegardés dans c:\\csec.ini)**

Configuration

Le fichier cscc.ini est essentiel lors du lancement d'une configuration de masse. Ce fichier peut porter n'importe quel nom, pourvu qu'il ait l'extension .ini. La liste ci-après contient les paramètres et des explications concernant ces paramètres figurant dans le fichier .ini que vous devez créer. Avant d'ouvrir et de modifier le fichier CSEC.INI, vous devez d'abord le déchiffrer, à l'aide de la commande CONSOLE.EXE qui figure dans le dossier Security.

Tableau 6. Paramètres de configuration Client Security

[CSSSetup]	En-tête de section pour la configuration de CSS.
suppw=bootup	Mot de passe administrateur/superviseur BIOS. N'indiquez aucune valeur si aucun mot de passe n'est requis.
hwpw=11111111	Mot de passe matériel CSS. Il doit comporter huit caractères et est toujours requis. Vous devez indiquer la valeur correcte si le mot de passe matériel a déjà été défini.
newkp=1	1 pour générer une nouvelle paire de clés administrateur 0 pour utiliser une paire de clés administrateur existante.
keysplit=1	Lorsque le paramètre newkp a pour valeur 1, ce paramètre détermine le nombre de composants de clé privée. **Remarque :** Si la paire de clés existante utilise plusieurs éléments de clé privée, tous les éléments de clé privée doivent être stockés dans le même répertoire.
kpl=c:\jgk	Emplacement de la paire de clés d'administrateur lorsque le paramètre newkp a pour valeur 1. S'il s'agit d'une unité réseau, un identificateur doit lui être affecté.
kal=c:\jgk\archive	Emplacement de l'archive de clés utilisateur. S'il s'agit d'une unité réseau, un identificateur doit lui être affecté.
pub=c:\jk\admin.key	Emplacement de la clé publique d'administrateur lorsque vous utilisez une paire de clés d'administrateur existante. S'il s'agit d'une unité réseau, un identificateur doit lui être affecté.
pri=c:\jk\private1.key	Emplacement de la clé privée d'administrateur lorsque vous utilisez une paire de clés d'administrateur existante. S'il s'agit d'une unité réseau, un identificateur doit lui être affecté.

Tableau 6. Paramètres de configuration Client Security (suite)

wiz=0	Détermine si ce fichier a été généré par l'assistant de configuration CSS. Cette entrée n'est pas nécessaire. Si vous l'incluez dans ce fichier, elle doit avoir la valeur 0.
clean=0	Indiquez la valeur 1 pour supprimer le fichier .ini après l'initialisation, ou la valeur 0 pour conserver le fichier .ini après l'initialisation.
enableroaming=1	Indiquez la valeur 1 pour activer l'itinérance pour le client, ou la valeur 0 pour la désactiver.
username= [promptcurrent]	Indiquez [promptcurrent] pour inviter l'utilisateur en cours à entrer le mot de passe d'inscription système. Indiquez [current] si le mot de passe d'inscription système pour l'utilisateur en cours est fourni par l'entrée sysregpwd et que cet utilisateur est autorisé à enregistrer le système auprès du serveur itinérant. Indiquez [<specific user account>] si l'utilisateur désigné est autorisé à enregistrer le système auprès du serveur itinérant et si le mot de passe d'inscription système de cet utilisateur est fourni par l'entrée sysregpwd. N'utilisez pas cette entrée si la valeur enableroaming est définie par 0, ou si l'entrée enableroaming est absente.
sysregpwd=12345678	Mot de passe enregistrement système. Indiquez le mot de passe approprié pour cette valeur afin de permettre l'enregistrement du système auprès du serveur itinérant. N'utilisez pas cette entrée si la valeur username est définie par [promptcurrent], ou si l'entrée username est absente.
[UVMEnrollment]	En-tête de section pour l'inscription des utilisateurs.
enrollall=0	Indiquez la valeur 1 pour enregistrer tous les comptes utilisateur locaux dans UVM, ou la valeur 0 pour enregistrer des comptes utilisateur spécifiques dans UVM.
defaultuvmpw=top	Lorsque le paramètre enrollall a pour valeur 1, cette valeur est le mot de passe composé UVM de tous les utilisateurs.
defaultwinpw=down	Lorsque le paramètre enrollall a pour valeur 1, cette valeur est le mot de passe Windows enregistré dans UVM pour tous les utilisateurs.
defaultppchange=0	Lorsque le paramètre enrollall a pour valeur 1, cette valeur permet d'établir la stratégie de modification des mots de passe composé UVM pour tous les utilisateurs. Indiquez la valeur 1 pour que l'utilisateur soit obligé de modifier le mot de passe composé UVM à la connexion suivante, ou la valeur 0 dans le cas contraire.
defaultppexppolicy=1	Lorsque le paramètre enrollall a pour valeur 1, cette valeur permet d'établir la stratégie de péremption des mots de passe composé UVM pour tous les utilisateurs. Indiquez la valeur 0 pour spécifier que le mot de passe composé UVM arrive à expiration, ou la valeur 1 dans le cas contraire.

Tableau 6. Paramètres de configuration Client Security (suite)

defaultppexpdays=0	Lorsque le paramètre enrollall a pour valeur 1, cette valeur permet d'établir le nombre de jours avant expiration du mot de passe composé UVM pour tous les utilisateurs. Lorsque le paramètre ppexppolicy a pour valeur 0, cette valeur permet d'établir le nombre de jours avant expiration du mot de passe composé UVM.
enrollusers=*x*, où x est le nombre total d'utilisateurs que vous allez inscrire sur l'ordinateur.	La valeur de cette instruction indique le nombre total d'utilisateurs que vous allez inscrire. Lorsque le paramètre enrollall a pour valeur 0, cette valeur indique le nombre d'utilisateurs qui seront inscrits dans UVM.
user1=jknox	Fournit les informations concernant chaque utilisateur à inscrire, en commençant par l'utilisateur 1. (Il n'y a pas d'utilisateur 0.) Les noms d'utilisateur doivent correspondre à des noms de compte. Pour obtenir le nom de compte réel sous Windows XP, procédez comme suit : 1. Lancez la Gestion de l'ordinateur (Gestionnaire de périphériques). 2. Développez le noeud Utilisateurs et groupes locaux. 3. Ouvrez le dossier Utilisateurs. Les éléments répertoriés dans la colonne Nom sont les noms de compte.
user1uvmpw=chrome	Indiquez le mot de passe composé UVM pour l'utilisateur 1 UVM.
user1winpw=spinning	Indiquez le mot de passe composé Windows pour l'utilisateur 1 à inscrire dans UVM.
user1domain=0	Indiquez si le compte de l'utilisateur 1 est locale ou sur le domaine. Indiquez la valeur 0 pour indiquer que ce compte est local, ou la valeur 1 pour indiquer que ce compte se trouve sur le domaine.
user1ppchange=0	Indiquez si l'utilisateur 1 va devoir modifier le mot de passe composé UVM à la connexion suivante, Indiquez la valeur 1 pour que l'utilisateur soit obligé de modifier le mot de passe composé UVM à la connexion suivante, ou la valeur 0 dans le cas contraire.
user1ppexppolicy=1	Indiquez si le mot de passe composé UVM de l'utilisateur 1 expire. Indiquez la valeur 0 pour spécifier que le mot de passe composé UVM arrive à expiration, ou la valeur 1 dans le cas contraire.
user1ppexpdays=0	Lorsque le paramètre user1ppexppolicy=0, cette valeur permet d'indiquer le nombre de jours avant expiration du mot de passe composé UVM.
Pour chaque utilisateur, fournissez un jeu complet de paramètres de configuration dans l'ordre indiqué dans la partie grisée du tableau. Fournissez d'abord tous les paramètres d'un utilisateur, puis du suivant, etc. Si, par exemple, le paramètre enrollusers a pour valeur 2, vous devrez ajouter le groupe de paramètres de configuration ci-après.	
user2=chrome	
user2uvmpw=left	
user2winpw=right	

Tableau 6. Paramètres de configuration Client Security (suite)

user2domain=0	
user2ppchange=1	
user2ppexppolicy=0	
user2ppexpdays=90	
[UVMAppConfig]	En-tête de section pour la configuration des modules et des applications compatibles avec UVM.
uvmlogon=0	Indiquez la valeur 1 pour utiliser la protection à la connexion UVM, ou la valeur 0 pour utiliser la connexion Windows.
entrust=0	Indiquez la valeur 1 pour utiliser UVM pour l'authentification Entrust, ou la valeur 0 pour utiliser l'authentification Entrust
notes=1	Indiquez la valeur 1 pour utiliser la protection UVM pour Lotus Notes, ou la valeur 0 pour utiliser la protection par mot de passe Lotus Notes.
netscape=0	Indiquez la valeur 1 pour signer et chiffrer les courriers électroniques à l'aide du module IBM PKCS #11, ou la valeur 0 dans le cas contraire.
passman=0	Indiquez la valeur 1 pour utiliser Password Manager, ou la valeur 0 dans le cas contraire.
folderprotect=0	Indiquez la valeur 1 pour utiliser le support de chiffrement des fichiers et des dossiers, ou la valeur 0 dans le cas contraire.

Remarques :

1. Au fur et à mesure des améliorations et des mises à jour du Logiciel IBM Client Security, il est possible que le fichier *.ini soit modifié.
2. Si des chemins ou des fichiers se trouvent sur une unité réseau, un identificateur doit être affecté à cette unité.
3. Le fichier CSEC.ini doit être chiffré pour que le logiciel charge le contenu. Il doit être chiffré via CONSOLE.EXE dans le répertoire Security. La commande suivante peut également être utilisée pour chiffrer un fichier INI via un script. (Vous devez utiliser des guillemets pour les noms de chemin longs) : *dossier d'installation de CSS*\console.exe /q /ini : *chemin d'accès absolu vers un fichier ini non chiffré*
4. La commande suivante permet d'exécuter le fichier .ini à partir de la ligne de commande lorsque la configuration de masse n'est pas effectuée conjointement à une installation de masse :

   dossier d'installation de CSS\acamucli /ccf:c:\csec.ini
5. Le fichier INI prend en charge l'ajout de nouveaux utilisateurs après la configuration du sous-système, ce qui peut être utile pour l'inscription d'utilisateurs. Exécutez un fichier INI comme décrit précédemment, sans inclure les valeurs ″pub=″ et ″pri=″. Le code considère l'inscription d'utilisateurs uniquement et ne réinitialise pas le sous-système.

Le Logiciel IBM Client Security vous permet d'exécuter le fichier CSEC.INI une seconde fois sans affecter l'installation en cours. Vous pouvez, par exemple, exécuter ce fichier une seconde fois pour inscrire d'autres utilisateurs.

Tableau 7. Paramètres de configuration du Logiciel Client Security lors de la seconde exécution

[CSSSetup]	En-tête de section pour la configuration de CSS.
suppw=	Mot de passe administrateur/superviseur BIOS. N'indiquez aucune valeur si aucun mot de passe n'est requis.
hwpw=11111111	Mot de passe matériel CSS. Il doit comporter huit caractères et est toujours requis. Vous devez indiquer la valeur correcte si le mot de passe matériel a déjà été défini.
newkp=0	Indiquez 0 pour utiliser une paire de clés administrateur existante.
keysplit=1	Lorsque le paramètre newkp a pour valeur 1, ce paramètre détermine le nombre de composants de clé privée. **Remarque :** Si la paire de clés existante utilise plusieurs éléments de clé privée, tous les éléments de clé privée doivent être stockés dans le même répertoire.
pub=	Laisser à blanc
pri=	Laisser à blanc
kal=c:\archive	Emplacement de l'archive de clés utilisateur. S'il s'agit d'une unité réseau, un identificateur doit lui être affecté.
wiz=0	Détermine si ce fichier a été généré par l'assistant de configuration CSS. Cette entrée n'est pas nécessaire. Si vous l'incluez dans ce fichier, elle doit avoir la valeur 0.
clean=0	Indiquez 0 pour conserver le fichier .ini après l'initialisation.
enableroaming=0	Indiquez 0 pour désactiver la délocalisation du client.
[UVMEnrollment]	En-tête de section pour l'inscription des utilisateurs.
enrollall=0	Indiquez la valeur 1 pour enregistrer tous les comptes utilisateur locaux dans UVM, ou la valeur 0 pour enregistrer des comptes utilisateur spécifiques dans UVM.
enrollusers=1	La valeur de cette instruction indique le nombre total d'utilisateurs que vous allez inscrire.
user1=*eddy*	Il s'agit du nom du nouvel utilisateur inscrit.
user1uvmpw=pass1word	Indiquez le mot de passe composé UVM pour l'utilisateur 1 UVM.
user1winpw=	Indiquez le mot de passe composé Windows pour l'utilisateur 1 à inscrire dans UVM.
user1domain=0	Indiquez si le compte de l'utilisateur 1 est locale ou sur le domaine. Indiquez la valeur 0 pour indiquer que ce compte est local, ou la valeur 1 pour indiquer que ce compte se trouve sur le domaine.
user1ppchange=0	Indiquez si l'utilisateur 1 va devoir modifier le mot de passe composé UVM à la connexion suivante, Indiquez la valeur 1 pour que l'utilisateur soit obligé de modifier le mot de passe composé UVM à la connexion suivante, ou la valeur 0 dans le cas contraire.

Tableau 7. Paramètres de configuration du Logiciel Client Security lors de la seconde exécution (suite)

user1ppexppolicy=1	Indiquez si le mot de passe composé UVM de l'utilisateur 1 expire. Indiquez la valeur 0 pour spécifier que le mot de passe composé UVM arrive à expiration, ou la valeur 1 dans le cas contraire.
user1ppexpdays=0	Lorsque le paramètre user1ppexppolicy=0, cette valeur permet d'indiquer le nombre de jours avant expiration du mot de passe composé UVM.

Chapitre 6. Installation du composant Client Security sur un serveur Tivoli Access Manager

L'authentification des utilisateurs finals au niveau du client est un élément essentiel en matière de sécurité. Le Logiciel Client Security fournit l'interface requise pour gérer la stratégie de sécurité sur un client IBM. Cette interface fait partie du logiciel d'authentification, UVM (User Verification Manager), qui est le principal composant du Logiciel Client Security.

Il existe deux façons de gérer la stratégie de sécurité UVM pour un client IBM :

- Au niveau local, à l'aide d'un éditeur de stratégie résidant sur le client IBM
- Au sein d'une entreprise, à l'aide de Tivoli Access Manager

Avant de pouvoir utiliser Client Security avec Tivoli Access Manager, vous devez installer le composant Client Security de Tivoli Access Manager. Vous pouvez le télécharger depuis le site Web IBM http://www.pc.ibm.com/us/security/index.html.

Conditions préalables

Avant de pouvoir établir une connexion sécurisée entre le client IBM et le serveur Tivoli Access Manager, vous devez installer les composants suivants sur le client IBM :

- IBM Global Security Toolkit
- IBM SecureWay Directory Client
- Tivoli Access Manager Runtime Environment

Pour plus de détails sur l'installation et l'utilisation de Tivoli Access Manager, consultez la documentation présente sur le site Web http://www.tivoli.com/products/index/secureway_policy_dir/index.htm.

Téléchargement et installation du composant Client Security

Le composant Client Security peut être téléchargé gratuitement à partir du site Web IBM.

Pour télécharger et installer Client Security sur le serveur Tivoli Access Manager et sur le client IBM, procédez comme suit :

1. A partir des informations figurant sur le site Web, assurez-vous que la puce de sécurité intégrée IBM figure sur votre système en vérifiant la correspondance de votre numéro de modèle avec celui fourni dans le tableau des composants système requis, puis cliquez sur **Continue**.
2. Sélectionnez le bouton d'option qui correspond à votre type de machine et cliquez sur **Continue**.
3. Créez un ID utilisateur, enregistrez-le auprès d'IBM en remplissant le formulaire en ligne, puis lisez le Contrat de licence et cliquez sur **Yes** pour accepter la licence.

   Vous serez automatiquement redirigé vers la page de téléchargement de Client Security.

4. Suivez les étapes indiquées dans la page de téléchargement pour installer les pilotes de périphérique nécessaires, fichiers readme, logiciels, documents de référence et autres utilitaires complémentaires.
5. Installez le Logiciel Client Security en procédant comme suit :
   a. A partir du bureau Windows, cliquez sur **Démarrer > Exécuter**.
   b. Dans la zone Exécuter, entrez `d:\répertoire\csec53.exe`, où d:\répertoire\ représentent l'indicatif d'unité et le répertoire dans lequel se trouve le fichier.
   c. Cliquez sur **OK**.

      La fenêtre de bienvenue de l'assistant d'installation InstallShield pour IBM Client Security s'affiche.
   d. Cliquez sur **Suivant**.

      L'assistant extrait les fichiers et installe le logiciel. Une fois l'installation terminée, vous avez le choix entre redémarrer l'ordinateur immédiatement ou ultérieurement.
   e. Sélectionnez le bouton d'option approprié et cliquez sur **OK**.
6. Une fois le système redémarré, à partir du bureau Windows, cliquez sur **Démarrer > Exécuter**.
7. Dans la zone Exécuter, entrez *d:*`\`*répertoire*`\TAMCSS.exe`, où *d:\répertoire* représente l'indicatif d'unité et le répertoire dans lequel se trouve le fichier. Vous pouvez aussi cliquer sur **Parcourir** afin de localiser le fichier.
8. Cliquez sur **OK**.
9. Indiquez un dossier cible et cliquez sur **Unzip**.

   L'assistant extrait les fichiers dans le dossier indiqué. Un message indique que les fichiers ont été décompressés.
10. Cliquez sur **OK**.

Ajout des composants Client Security sur le serveur Tivoli Access Manager

L'utilitaire pdadmin est un outil de ligne de commande que l'administrateur peut utiliser pour effectuer la plupart des tâches d'administration de Tivoli Access Manager. L'exécution de plusieurs commandes permet à l'administrateur d'utiliser un fichier contenant plusieurs commandes pdadmin pour exécuter une tâche entière ou une série de tâches. La communication entre l'utilitaire pdadmin et le serveur de gestion (pdmgrd) est sécurisée via SSL. L'utilitaire pdadmin est installé avec le progiciel Tivoli Access Manager Runtime Environment.

L'utilitaire pdadmin accepte un argument de nom de chemin qui identifie l'emplacement de ce fichier, par exemple :

```
MSDOS>pdadmin [-a util-admin][-p motdepasse ]fichier-nomchemin
```

La commande ci-après illustre le mode de création de l'espace objet IBM Solutions, d'actions Client Security et d'entrées ACL individuelles sur le serveur Tivoli Access Manager.

```
MSDOS>pdadmin -a resp_sécurité -p mot_de_passe
C:\TAM_Add_ClientSecurity.txt
```

Pour plus d'informations sur l'utilitaire pdadmin et sa syntaxe de commande, reportez-vous au manuel *Tivoli Access Manager Base Administrator Guide*.

Etablissement d'une connexion sécurisée entre le client IBM et le serveur Tivoli Access Manager

Le client IBM doit définir sa propre identité authentifiée au sein du domaine sécurisé Tivoli Access Manager afin de demander des décisions d'autorisation au service Tivoli Access Manager Authorization.

Une identité unique doit être créée pour l'application dans le domaine sécurisé Tivoli Access Manager. Pour que l'identité authentifiée effectue des vérifications d'authentification, l'application doit être membre du groupe d'utilisateurs ACL éloignés. Lorsque l'application veut prendre contact avec l'un des services du domaine sécurisé, elle doit d'abord ouvrir une session sur le domaine.

L'utilitaire svrsslcfg permet aux applications IBM Client Security de communiquer avec le serveur de gestion Tivoli Access Manager et avec le serveur d'autorisation.

L'utilitaire svrsslcfg permet aux applications IBM Client Security de communiquer avec le serveur de gestion Tivoli Access Manager et avec le serveur d'autorisation.

Il permet d'exécuter les tâches suivantes :

- Création d'une identité utilisateur pour l'application. Par exemple, UtilDémo/NOMHOTE
- Création d'un fichier de clés SSL pour cet utilisateur. Par exemple, UtilDemo.kdb et UtilDemo.sth
- Ajout de l'utilisateur dans un groupe d'utilisateurs ACL éloignés

Les paramètres suivants sont nécessaires :

- **-f fichier_cfg** Chemin et nom du fichier de configuration. Utilisez TAMCSS.conf.
- **-d rép_kdb** Répertoire devant contenir les fichiers de base de données de fichiers de clés pour le serveur.
- **-n nom_serveur** Nom réel Windows/UVM de l'utilisateur client IBM voulu.
- **-P mdp_admin** Mot de passe de l'administrateur de Tivoli Access Manager.
- **-s type_serveur** Vous devez indiquer qu'il s'agit d'un serveur éloigné.
- **-S mdp_serveur** Mot de passe du nouvel utilisateur. Ce paramètre est obligatoire.
- **-r n°_port** Définit le numéro de port d'écoute pour le client IBM. Il s'agit du paramètre indiqué comme port du serveur SSL variable de Tivoli Access Manager Runtime pour le serveur de gestion de Tivoli Access Manager.
- **-e pwd_life** Définit le délai d'expiration (en nombre de jours) du mot de passe.

Pour établir une connexion sécurisée entre le client IBM et le serveur Tivoli Access Manager, procédez comme suit :

1. Créez un répertoire et placez-y le fichier TAMCSS.conf.

   Par exemple, `MSDOS> mkdir C:\TAMCSS MSDOS> move C:\TAMCSS.conf C:\TAMCSS\`
2. Exécutez svrsslcfg pour créer l'utilisateur.

   MSDOS> svrsslcfg -config -f C:\TAMCSS\TAMCSS.conf -d C:\TAMCSS\ -n <nom_serveur> - s remote -S <mdp_serveur> -P <mdp_admin> -e 365 -r 199

   Remarque : Remplacez <nom_serveur> par le nom d'utilisateur et le nom d'hôte UVM du client IBM. Par exemple : –n UtilDémo/NomHôte. Pour trouver le nom d'hôte du client IBM, vous pouvez taper la commande

"hostname" à l'invite MSDOS. L'utilitaire svrsslcfg va créer une entrée correcte sur le serveur Tivoli Access Manager et fournir un fichier de clés SSL unique pour les communications chiffrées.

3. Exécutez svrsslcfg pour ajouter l'emplacement de ivacld dans le fichier TAMCSS.conf.

   Par défaut, le serveur Tivoli Access Manager Authorization écoute sur le port 7136. Vous pouvez le vérifier en recherchant la valeur du paramètre tcp_req_port dans le paragraphe ivacld du fichier ivacld.conf sur le serveur Tivoli Access Manager. Il est important que vous disposiez du nom d'hôte ivacld correct. Pour obtenir cette information, utilisez la commande de liste de serveurs pdadmin. Les serveurs portent le nom : **nom_serveur-nom_hôte**. Voici un exemple d'exécution de commande de liste de serveurs pdadmin :

```
MSDOS> pdadmin server list   ivacld-MonHôte.ibm.com
```

La commande ci-après permet ensuite d'ajouter une entrée réplique pour le serveur ivacld affiché précédemment. Il est entendu que ivacld écoute sur le port par défaut 7136.

```
svrsslcfg -add_replica  -f chemin fichier config -h nom_hôte
MSDOS>svrsslcfg -add_replica  -f C:\TAMCSS\TAMCSS.conf -h MonHôte.ibm.com
```

Configuration des clients IBM

Pour pouvoir utiliser Tivoli Access Manager afin de contrôler les objets d'authentification pour les clients IBM, vous devez configurer chaque client à l'aide de l'utilitaire d'administration, composant fourni avec le logiciel Client Security. Dans la présente section, sont décrites les conditions requises et les instructions relatives à la configuration des clients IBM.

Conditions préalables

Vérifiez que les logiciels ci-après sont installés sur le client IBM, dans l'ordre suivant :

1. **Système d'exploitation Microsoft Windows pris en charge.** Vous pouvez utiliser Tivoli Access pour contrôler les conditions d'authentification des clients IBM dotés de Windows XP, Windows 2000 ou Windows NT Workstation 4.0.
2. **Logiciel Client Security version 3.0 ou supérieure.** Après avoir installé le logiciel et activé la puce de sécurité intégrée IBM, vous pouvez utiliser l'utilitaire d'administration de la sécurité client pour configurer l'authentification d'utilisateur et éditer la stratégie de sécurité UVM. Pour connaître toutes les instructions d'installation et d'utilisation du logiciel Client Security, reportez-vous aux manuels *Logiciel Client Security – Guide d'installation* et *Logiciel Client Security – Guide d'administration*.

Définition des informations de configuration de Tivoli Access Manager

Une fois Tivoli Access Manager installé sur le client local, vous pouvez définir les informations de configuration d'Access Manager à l'aide de l'utilitaire d'administration, composant fourni par le logiciel Client Security. Ces informations sont constituées des éléments suivants :

- Choix du chemin d'accès complet aux fichiers de configuration
- Choix de la fréquence de régénération de la mémoire cache locale

Pour définir les informations de configuration de Tivoli Access Manager sur le client IBM, suivez la procédure ci-après.

1. Cliquez sur **Démarrer > Paramètres > Panneau de configuration > Sous-système de sécurité intégré IBM**.
2. Tapez le mot de passe administrateur et cliquez sur **OK**.

   Une fois le mot de passe saisi, la fenêtre principale de l'utilitaire d'administration s'ouvre.
3. Cliquez sur le bouton **Configuration du support d'application et des stratégies**.

   L'écran Configuration des applications UVM et des stratégies s'affiche.
4. Sélectionnez la case à cocher **Remplacement de la fenêtre de connexion standard de Windows par la fenêtre de connexion sécurisée UVM**.
5. Cliquez sur le bouton **Stratégie d'application**.
6. Dans la zone d'information de configuration de Tivoli Access Manager, sélectionnez le chemin d'accès complet au fichier de configuration TAMCSS.conf. Par exemple, `C:\TAMCSS\TAMCSS.conf`

   Tivoli Access Manager doit être installé sur le client pour que cette zone soit disponible.
7. Cliquez sur le bouton **Edition de la stratégie**.

   L'écran Saisie du mot de passe administrateur s'affiche.
8. Tapez le mot de passe administrateur dans la zone prévue à cet effet et cliquez sur **OK**.

   L'écran Stratégie UVM s'affiche.
9. Sélectionnez les actions que vous voulez voir contrôlées par Tivoli Access Manager à partir du menu déroulant Actions.
10. Cochez la case en regard de l'option Access Manager contrôle l'objet sélectionné.
11. Cliquez sur **Validation**.

    Les modifications entrent en vigueur à la régénération suivante de la mémoire cache. Si vous souhaitez que les modifications soient immédiatement appliquée, cliquez sur le bouton **Régénération de la mémoire cache locale**.

Configuration et utilisation du dispositif de mémoire cache locale

Après avoir sélectionné le fichier de configuration de Tivoli Access Manager, vous pouvez définir la fréquence de régénération de la mémoire cache locale. Une réplique locale des informations de stratégie de sécurité, telles qu'elles sont gérées par Tivoli Access Manager, est conservée sur le client IBM. Vous pouvez planifier une régénération automatique de la mémoire cache locale par incréments de mois (0-12) ou de jours (0-30).

Pour définir ou régénérer la mémoire cache locale, suivez la procédure ci-après.

1. Cliquez sur **Démarrer > Paramètres > Panneau de configuration > Sous-système de sécurité intégré IBM**.
2. Tapez le mot de passe administrateur et cliquez sur **OK**.

   La fenêtre Utilitaire d'administration s'ouvre. Pour connaître les informations relatives à l'utilisation de l'utilitaire d'administration, reportez-vous au manuel *Logiciel Client Security – Guide d'administration*.
3. Dans l'utilitaire d'administration, cliquez sur le bouton **Configuration du support d'application et des stratégies**, puis sur **Stratégies d'application**.

L'écran Modification de la configuration de stratégie de Client Security s'affiche.

4. Effectuez l'une des opérations suivantes :
   - Pour régénérer la mémoire cache locale immédiatement, cliquez sur **Régénération de la mémoire cache**.
   - Pour définir la fréquence de régénération automatique, tapez le nombre de mois (de 0 à 12) et de jours (de 0 à 30) voulus dans les zones affichées et cliquez sur **Régénération de la mémoire cache locale**. La mémoire cache locale et la date de péremption du fichier seront mises à jour afin d'indiquer la date de la prochaine régénération automatique.

Activation de Tivoli Access Manager pour contrôler les objets du client IBM

La stratégie UVM est contrôlée par le biais d'un fichier de stratégie globale. Le fichier de stratégie globale, appelé fichier de stratégie UVM, contient des conditions d'authentification requises pour les actions effectuées sur le système client IBM, telles que l'ouverture de session sur le système, la désactivation de l'économiseur d'écran ou la signature de messages de courrier électronique.

Pour pouvoir activer Tivoli Access Manager afin de contrôler les objets d'authentification pour un client IBM, éditez le fichier de stratégie UVM à l'aide de l'éditeur de stratégie UVM. L'éditeur de stratégie UVM fait partie de l'utilitaire d'administration.

Important : L'activation de Tivoli Access Manager pour contrôler un objet donne le contrôle sur les objets à l'espace objet Tivoli Access Manager. Si vous l'activez, vous devez réinstaller le logiciel Client Security pour rétablir le contrôle local sur cet objet.

Edition d'une stratégie UVM locale

Avant de tenter d'éditer la stratégie UVM pour le client local, vérifiez qu'un utilisateur au moins est inscrit dans le gestionnaire UVM. Dans le cas contraire, un message d'erreur s'affiche lorsque l'éditeur de stratégie tente d'ouvrir le fichier de stratégie local.

Après avoir édité une stratégie UVM locale, vous ne pouvez l'utiliser que sur le client sur lequel elle a été éditée. Si vous avez installé Client Security dans le répertoire par défaut, la stratégie UVM locale est stockée sous le nom \Program Files\IBM\Security\UVM_Policy\globalpolicy.gvm Seuls les utilisateurs ajoutés au gestionnaire UVM peuvent utiliser l'éditeur de stratégie UVM.

Remarque : Si vous définissez dans la stratégie UVM que les empreintes digitales sont obligatoires pour un objet d'authentification (tel que l'ouverture de session sur le système d'exploitation), les empreintes des utilisateurs qui sont ajoutés à UVM doivent être enregistrées pour que ceux-ci puissent utiliser cet objet.

Pour démarrer l'éditeur de stratégie UVM, suivez la procédure de l'utilitaire d'administration ci-après.

1. Cliquez sur le bouton **Configuration du support d'application et des stratégies**, puis sur **Stratégies d'application**.

   L'écran Modification de la configuration de stratégie de Client Security s'affiche.
2. Cliquez sur le bouton **Edition de la stratégie**.

L'écran Saisie du mot de passe administrateur s'affiche.

3. Tapez le mot de passe administrateur dans la zone prévue à cet effet et cliquez sur **OK**.

   L'écran Stratégie UVM s'affiche.

4. Cliquez sur l'onglet Sélection d'objet, puis sur **Action** ou sur **Type d'objet**, puis sélectionnez l'objet auquel vous voulez affecter des conditions d'authentification.

   Exemples d'actions admises : ouverture de session sur le système, déverrouillage du système, déchiffrement du courrier électronique ; exemple de type d'objet : acquisition de certificat numérique.

5. Pour chaque objet que vous sélectionnez, choisissez **Tivoli Access Manager contrôle l'objet sélectionné** pour activer Tivoli Access pour cet objet.

   Important : Si vous activez Tivoli Access Manager pour contrôler un objet, vous donnez le contrôle sur les objets à l'espace objet Tivoli Access Manager. Si vous voulez, par la suite, rétablir le contrôle local sur cet objet, vous devez réinstaller le logiciel Client Security.

   Remarque : Lorsque vous éditez la stratégie UVM, vous pouvez visualiser le récapitulatif de la stratégie en cliquant sur **Récapitulatif de la stratégie**.

6. Cliquez sur **Validation** pour sauvegarder vos modifications.
7. Cliquez sur **OK** pour sortir.

Edition et utilisation de stratégies UVM pour des clients éloignés

Pour utiliser une stratégie UVM sur plusieurs clients IBM, éditez et sauvegardez la stratégie UVM pour un client éloigné, puis copiez le fichier de stratégie sur les autres clients. Si vous installez Client Security dans le répertoire par défaut, le fichier de stratégie UVM est stocké sous le nom \Program Files\IBM\Security\UVM_Policy\remote\globalpolicy.gvm.

Copiez les fichiers suivants sur les autres clients IBM éloignés qui utiliseront cette stratégie UVM :

- \IBM\Security\UVM_Policy\remote\globalpolicy.gvm
- \IBM\Security\UVM_Policy\remote\globalpolicy.gvm.sig

Si vous avez installé le logiciel Client Security dans son répertoire par défaut, le répertoire racine pour les chemins précédents doit être le répertoire \Program Files. Copiez les deux fichiers dans le répertoire \IBM\Security\UVM_Policy\ sur les clients éloignés.

Tableaux d'identification des incidents

La section ci-après contient des tableaux d'identification des incidents qui peuvent s'avérer utiles en cas d'incident avec le Logiciel Client Security.

Identification des incidents relatifs à un certificat numérique

Les informations ci-après peuvent s'avérer utiles en cas d'incident lors de l'obtention d'un certificat numérique.

Incident	Solution possible
La fenêtre de mot de passe composé UVM ou la fenêtre d'authentification d'empreinte digitale s'affiche plusieurs fois lors de la demande d'un certificat numérique	**Action**
La stratégie de sécurité UVM impose qu'un utilisateur fournisse le mot de passe composé UVM ou l'authentification d'empreinte digitale avant de pouvoir acquérir un certificat numérique. Si l'utilisateur tente d'acquérir un certificat, la fenêtre d'authentification demandant le mot de passe composé UVM ou le scannage d'empreinte digitale peut s'afficher plusieurs fois	Tapez votre mot de passe composé UVM ou scannez votre empreinte digitale chaque fois que la fenêtre d'authentification s'ouvre.
Un message d'erreur VBScript ou JavaScript s'affiche	**Action**
Lorsque vous demandez un certificat numérique, un message d'erreur relatif à VBScript ou JavaScript peut s'afficher.	Redémarrez l'ordinateur et redemandez le certificat.

Identification des incidents relatifs à Tivoli Access Manager troubleshooting information

Les informations ci-après peuvent s'avérer utiles en cas d'incident lors de l'utilisation de Tivoli Access Manager avec le Logiciel Client Security.

Incident	Solution possible
Les paramètres de stratégie locaux ne correspondent pas à ceux du serveur	**Action**
Tivoli Access Manager autorise certaines configurations de bit qui ne sont pas prises en charge par UVM. Les exigences de stratégie locales peuvent donc remplacer les paramètres définis par un administrateur lors de la configuration du serveur Tivoli Access Manager.	Il s'agit d'une limite connue.
Les paramètres de configuration de Tivoli Access Manager ne sont pas accessibles	**Action**
Les paramètres de configuration de Tivoli Access Manager et de la mémoire cache locale ne sont pas accessibles sur la page Définition de stratégie de l'utilitaire d'administration.	Installez l'environnement d'exécution de Tivoli Access Manager. Si l'environnement d'exécution n'est pas installé sur le client IBM, les paramètres de Tivoli Access Manager sur la page Définition de stratégie ne seront pas disponibles

Incident	Solution possible
Une commande utilisateur est admise à la fois pour l'utilisateur et le groupe	**Action**
Lors de la configuration du serveur Tivoli Access Manager, si vous définissez un utilisateur par rapport à un groupe, la commande utilisateur est admise à la fois pour l'utilisateur et le groupe si l'option **Traverse bit** est activée.	Aucune action n'est requise.

Identification des incidents relatifs à Lotus Notes

Les informations ci-après peuvent s'avérer utiles en cas d'incident lors de l'utilisation de Lotus Notes avec le Logiciel Client Security.

Incident	Solution possible
Une fois que la fonction de protection UVM pour Lotus Notes a été activée, Notes ne peut pas finir sa configuration	**Action**
Lotus Notes ne peut pas finir sa configuration une fois que la fonction de protection UVM a été activée à l'aide de l'utilitaire d'administration.	Il s'agit d'une limite connue. Lotus Notes doit être configuré et en cours d'exécution pour que le support Lotus Notes puisse être activé dans l'utilitaire d'administration.
Un message d'erreur s'affiche lorsque vous tentez de modifier le mot de passe Notes	**Action**
La modification du mot de passe Notes lors de l'utilisation du Logiciel Client Security risque de provoquer l'affichage d'un message d'erreur.	Essayez de modifier à nouveau le mot de passe. Si l'opération n'aboutit pas, redémarrez le client.
Un message d'erreur s'affiche une fois que vous avez généré un mot de passe de façon aléatoire	**Action**
Un message d'erreur peut s'afficher lorsque vous exécutez les opérations suivantes : • Utilisation de l'outil de configuration de Lotus Notes pour définir la protection UVM pour un ID Notes • Ouverture de Notes et utilisation de la fonction fournie par Notes pour modifier le mot de passe pour un fichier d'ID Notes • Fermeture immédiate de Notes après la modification du mot de passe	Cliquez sur **OK** pour faire disparaître le message d'erreur. Aucune autre action n'est requise. Contrairement aux indications du message d'erreur, le mot de passe a été modifié. Le nouveau mot de passe est généré de façon aléatoire par le Logiciel Client Security. Le fichier d'ID Notes est désormais chiffré à l'aide du mot de passe généré de façon aléatoire et l'utilisateur n'a pas besoin d'un nouveau fichier d'ID utilisateur. Si l'utilisateur final modifie à nouveau le mot de passe, UVM génère un nouveau mot de passe de façon aléatoire pour l'ID Notes.

Identification des incidents relatifs au chiffrement

Les informations ci-après peuvent s'avérer utiles en cas d'incident lors du chiffrement de fichiers à l'aide du Logiciel Client Security version 3.0 ou suivante.

Incident	Solution possible
Les fichiers précédemment chiffrés ne sont pas déchiffrés	**Action**
Les fichiers chiffrés à l'aide de versions précédentes du Logiciel Client Security ne peuvent pas être déchiffrés après la mise à niveau vers Client Security version 3.0 ou suivante.	Il s'agit d'une limite connue. Vous devez déchiffrer tous les fichiers qui ont été chiffrés à l'aide de versions précédentes du Logiciel Client Security *avant* d'installer Client Security version 3.0 ou suivante. Le logiciel Client Security 3.0 ne peut pas déchiffrer des fichiers qui ont été chiffrés à l'aide de versions précédentes du Logiciel Client Security en raison de modifications effectuées dans l'implémentation du chiffrement de fichiers.

Chapitre 7. Installation de pilotes de périphérique matériel tiers en complément du logiciel IBM Client Security

L'utilisation du logiciel Client Security et de solutions provenant de fournisseurs tiers vous permet de protéger la totalité de votre infrastructure en intégrant des offres complémentaires qui vous permettent d'adapter le niveau de protection à votre environnement informatique.

La compatibilité du sous-système de sécurité intégré IBM avec certaines offres matérielles d'authentification et de sécurité a été testée. Les marques compatibles sont les suivantes :

- Targus pour les programmes de lecture d'empreintes digitales
- Gemplus pour les solutions de carte à puce
- Ensure Technologies pour les badges de proximité

Afin d'en savoir plus sur les offres qui vous sont proposées par ces différentes marques, consultez le site Web suivant qui contient des liens vers les sites de chaque marque : http://www.pc.ibm.com/us/security/index.html

Comme c'est le cas avec les nombreux composants faisant partie des images de disquette, la séquence d'installation est extrêmement importante. Si vous envisagez de déployer les unités d'authentification mentionnées précédemment, ainsi que les logiciels et pilotes associés, vous devez installer le Logiciel IBM Client Security en premier. Les pilotes et logiciels associés à ces unités ne peuvent pas être correctement installés si CSS n'est pas copié sur le disque dur avant les fichiers de pilote de périphérique.

Pour obtenir des informations spécifiques à jour sur l'installation des logiciels et des pilotes qui permettent d'utiliser le matériel d'authentification, reportez-vous à la documentation fournie avec ces unités.

Chapitre 8. Déploiement à distance de fichiers de stratégie de sécurité nouveaux ou modifiés

Que vous procédiez à la mise à jour de stratégies de sécurité ou à la création de nouvelles stratégies pour d'autres ordinateurs, vous pouvez, en tant qu'administrateur informatique doté de droits de signature, modifier et déployer des fichiers de stratégie. Pour ce faire, éditez le fichier de stratégie à l'aide de l'exécutable ACAMUCLI.EXE. (Vous pouvez également cliquer deux fois de suite sur l'icône Sous-système de sécurité IBM dans le panneau de configuration).

Signez le fichier de stratégie en suivant les instructions affichées à l'écran, puis cliquez sur Validation. (**Remarque :** Si la clé privée de l'administrateur a été partagée, tous les composants doivent être entrés pour la signature du fichier de stratégie.) Les fichiers édités sont les suivants : GLOBALPOLICY.GVM et GLOBPOLICY.GVM.SIG. Distribuez ces fichiers aux utilisateurs appropriés et assurez-vous qu'ils sont sauvegardés dans le dossier Security\UVM_Policy.

Vous pouvez opérer une mise à jour à distance des stratégies de mots de passe composés à l'issue du déploiement. Cette mise à jour vous permet de modifier les règles lorsque (ou si) l'utilisateur modifie son mot de passe composé. L'administrateur peut ainsi définir un délai au terme duquel l'utilisateur est obligé de modifier son mot de passe composé. Ce délai est défini lors de l'inscription de l'utilisateur. Par exemple : L'administrateur crée l'utilisateur Jeanne pour lequel la stratégie initiale indique qu'un mot de passe de huit caractères doit être créé et qu'il doit expirer au bout de 30 jours. L'administrateur a pu modifier le fichier de stratégie et indiquer qu'à la prochaine modification du mot de passe composé par Jeanne, le nouveau mot de passe composé devra contenir 12 caractères. L'administrateur a pu également modifier le délai de péremption de ce mot de passe. Par exemple, au lieu d'une modification tous les 30 jours, l'administrateur peut demander à ce que Jeanne modifie ses mots de passe composés tous les 15 jours. Que va-t-il se passer dans le scénario suivant ? Nous sommes le 10ème jour d'une période au cours de laquelle le mot de passe composé doit être modifié tous les 30 jours. Un nouveau fichier de stratégie indiquant que le mot de passe composé doit être modifié tous les 15 jours est envoyé sur l'ordinateur client. Dans ce cas, le mot de passe composé expire-t-il dans 5 ou 20 jours ? Le mot de passe composé expire dans 20 jours comme indiqué dans la première stratégie. En effet, cette stratégie entre en vigueur dès l'instant où elle est définie. La stratégie de péremption du mot de passe composé au bout de 15 jours commence à s'appliquer lorsque Jeanne modifie son mot de passe composé 20 jours plus tard.

Si vous souhaitez modifier les caractéristiques obligatoires du mot de passe composé, suivez les instructions ci-dessus. Distribuez ensuite les fichiers suivants du dossier SECURITY\UVM_POLICY : UVM_PP_POLICY.DAT et UVM_PP_POLICY.DAT.SIG.

Annexe. Remarques

Le présent document peut contenir des informations ou des références concernant certains produits, logiciels ou services IBM non annoncés dans ce pays. Pour plus de détails, référez-vous aux documents d'annonce disponibles dans votre pays, ou adressez-vous à votre partenaire commercial IBM. Toute référence à un produit, logiciel ou service IBM n'implique pas que seul ce produit, logiciel ou service puisse être utilisé. Tout autre élément fonctionnellement équivalent peut être utilisé, s'il n'enfreint aucun droit d'IBM. Il est de la responsabilité de l'utilisateur d'évaluer et de vérifier lui-même les installations et applications réalisées avec des produits, logiciels ou services non expressément référencés par IBM.

IBM peut détenir des brevets ou des demandes de brevet couvrant les produits mentionnés dans le présent document. La remise de ce document ne vous donne aucun droit de licence sur ces brevets ou demandes de brevet. Si vous désirez recevoir des informations concernant l'acquisition de licences, veuillez en faire la demande par écrit à l'adresse suivante :

IBM EMEA Director of Licensing
IBM Europe Middle-East Africa
Tour Descartes
92 066 Paris-La Défense CEDEX 50
France

LE PRESENT DOCUMENT EST LIVRE «EN L'ETAT». IBM DECLINE TOUTE RESPONSABILITE, EXPLICITE OU IMPLICITE, RELATIVE AUX INFORMATIONS QUI Y SONT CONTENUES, Y COMPRIS ET DE FACON NON LIMITATIVE, TOUTE GARANTIE IMPLICITE DE NON-CONTREFACON OU D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE. Certaines juridictions n'autorisent pas l'exclusion des garanties implicites, auquel cas l'exclusion ci-dessus ne vous sera pas applicable.

Le présent document peut contenir des inexactitudes ou des coquilles. Il est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. IBM peut modifier sans préavis les produits et logiciels décrits dans ce document.

Les produits décrits dans ce document ne sont pas conçus pour être implantés ou utilisés dans un environnement où un dysfonctionnement pourrait entraîner des dommages corporels ou le décès de personnes. Les informations contenues dans ce document n'affectent ni ne modifient les garanties ou les spécifications des produits IBM. Rien dans ce document ne doit être considéré comme une licence ou une garantie explicite ou implicite en matière de droits de propriété intellectuelle d'IBM ou de tiers. Toutes les informations contenues dans ce document ont été obtenues dans des environnements spécifiques et sont présentées en tant qu'illustration. Les résultats peuvent varier selon l'environnement d'exploitation utilisé.

IBM pourra utiliser ou diffuser, de toute manière qu'elle jugera appropriée et sans aucune obligation de sa part, tout ou partie des informations qui lui seront fournies.

Sites Web non IBM

Les références à des sites Web non IBM sont fournies à titre d'information uniquement et n'impliquent en aucun cas une adhésion aux données qu'ils contiennent. Les éléments figurant sur ces sites Web ne font pas partie des éléments du présent produit IBM et l'utilisation de ces sites relève de votre seule responsabilité.

Marques

Les termes qui suivent sont des marques d'International Business Machines Corporation aux Etats-Unis et/ou dans certains autres pays :

IBM
ThinkPad
ThinkCentre
Tivoli

Microsoft, Windows et Windows NT sont des marques de Microsoft Corporation aux Etats-Unis et/ou dans certains autres pays.

D'autres sociétés sont propriétaires des autres marques, noms de produits ou logos qui pourraient apparaître dans ce document.