Guía de despliegue de IBM Client Security Software
Versión 5.4.0

Actualizada: 18 Noviembre 2004

Cuarta edición (octubre de 2004)

Esta publicación es la traducción del original inglés *IBM Client Security Software Deployment Guide Version 5.4.0*.

Prefacio

Los administradores de TI deben conocer y planificar numerosos factores cuando despliegan IBM Client Security Software. Esta guía no pretende explicar cómo utilizar Embedded Security Subsystem. Más bien se trata de una guía sobre cómo desplegar el software en sistemas equipados con el chip IBM Security Chip incorporado en una empresa.

Público objetivo

Esta guía va dirigida a administradores de TI o a aquellas personas responsables del despliegue de IBM Client Security Software Versión 5.4 (CSS) en los sistemas de su organización. El objetivo de la guía es proporcionar la información necesaria para la instalación de IBM Client Security Software en uno o varios sistemas. Lea la *Guía del administrador y el usuario de IBM Client Security Software Versión 5.4* como requisito previo antes de leer este manual. IBM proporciona la *Guía del administrador y el usuario de IBM Client Security Software Versión 5.4* y la ayuda de la aplicación, en la que puede buscar información sobre el uso de la aplicación.

Publicaciones del producto

Los documentos siguientes está disponibles en la biblioteca de Client Security Software Versión 5.4:

- *Guía del administrador y el usuario de Client Security Software Versión 5.4*

  Proporciona información para configurar y utilizar las características de seguridad que se proporcionan con Client Security Software, y contiene información sobre cómo efectuar tareas de Client Security Software, como la utilización de la protección de inicio de sesión de UVM, la configuración del protector de pantalla de Client Security, la creación de un certificado digital y la utilización de User Configuration Utility.
- *Guía de instalación de Client Security Software Versión 5.4*

  Contiene información sobre la instalación de Client Security Software en sistemas en red de IBM con chips IBM Security Chip incorporados.

Información adicional

Puede obtener información adicional y actualizaciones de productos de seguridad, cuando estén disponibles, desde el sitio Web de IBM en http://www.pc.ibm.com/us/security/index.html.

Contenido

Capítulo 1. Consideraciones antes de desplegar IBM Client Security Software

El despliegue central de IBM Client Security Software Versión 5.4.0 se obtiene con la modalidad de configuración avanzada en el asistente de configuración de IBM Client Security Software. IBM Client Security Software Versión 5.4 no da soporte a los chips de seguridad de primera generación (no TCPA). Los usuarios de estos sistemas deben utilizar Client Security Software Versión 5.3.

Existen varias formas de desplegar IBM Client Security Software (CSS), que utiliza el hardware IBM Embedded Security Subsystem (ESS) integrado en sistemas personales IBM. Este documento le ayudará a determinar cómo distribuir ESS en su entorno. Es importante conocer el proceso que utiliza su empresa para distribuir los sistemas, desde la creación de la imagen hasta la forma en que el PC se entrega al usuario final. Este proceso influirá enormemente en la forma en que su empresa distribuye ESS. IBM ESS está compuesto fundamentalmente de dos partes, como se muestra en la Figura 1:

1. Client Security Software
2. Chip IBM Security Chip incorporado

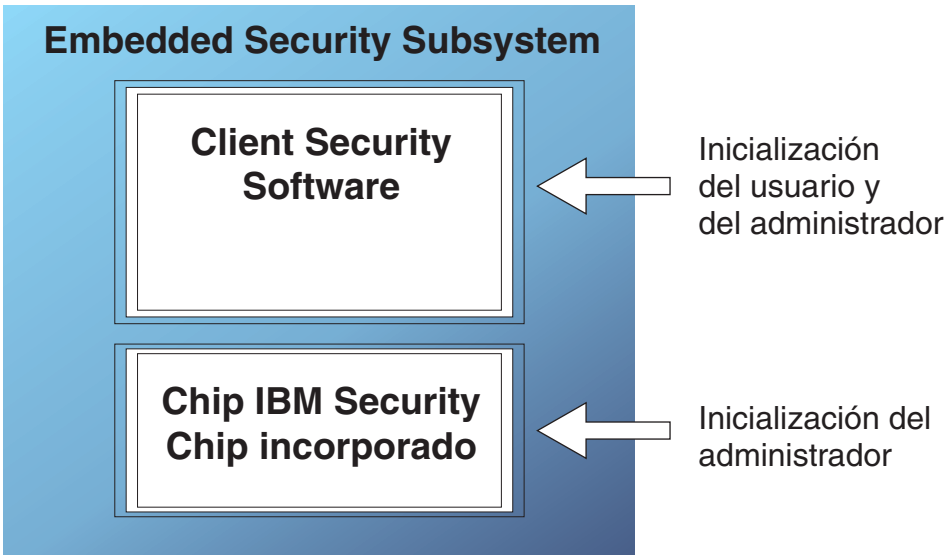

Figura 1. Componentes de IBM Client Security System

Requisitos y especificaciones de distribución

Si tiene previsto instalar IBM Client Security Software en sistemas que estén equipados con el chip IBM Security Chip incorporado, cuente con los siguientes requisitos de almacenamiento y bajada del servidor y en los tiempos de instalación:

1. IBM PC con Embedded Security Chip
2. Requisitos de almacenamiento en el servidor para código instalable: aproximadamente 12 MB
3. Promedio de requisitos de almacenamiento por usuario para los datos del archivo de claves: 200 KB por usuario y para almacenamiento del archivador

Capítulo 2. Instalación de Client Security Software

En este capítulo se describen dos formas diferentes de instalar Client Security Software: la instalación estándar y la instalación administrativa.

Instalación estándar

El archivo z046zis2018usaa.exe es un paquete de instalación de extracción automática que extrae los archivos de origen de instalación y ejecuta la instalación. Este archivo acepta un conjunto de parámetros de línea de mandatos que se describen a continuación. Las opciones de línea de mandatos que necesitan un parámetro se deben especificar sin ningún espacio entre la opción y el parámetro. Por ejemplo, `z046zis2018usaa.exe /s /v"/qn REBOOT="R""` es válido, mientras que `Setup.exe /s /v "/qn REBOOT="R""` no lo es (**"/qn REBOOT="R""** es un parámetro de la opción **/v**). Sólo se deben utilizar comillas en el parámetro de una opción si el parámetro contiene espacios.

El comportamiento por omisión de la instalación cuando se ejecuta Setup.exe sin parámetros, que ejecuta la instalación con una interfaz de usuario, es solicitar un reinicio del sistema al final de la instalación. El comportamiento por omisión cuando se ejecuta la instalación sin interfaz de usuario es reiniciar el sistema al final de la instalación. No obstante, el reinicio se puede retrasar con la propiedad REBOOT, tal como se ha descrito anteriormente en el apartado de ejemplo.

/a Este parámetro hace que el archivo ejecutable realice una instalación administrativa. Una instalación administrativa copia los archivos de datos en un directorio especificado por el usuario, pero no crea accesos directos, ni registra servidores COM, ni crea anotaciones cronológicas de desinstalación.

/x Este parámetro hace que el archivo ejecutable desinstale un producto instalado previamente.

/s Modalidad silenciosa
Este parámetro hace que el archivo ejecutable se ejecute en modalidad silenciosa.

/v El parámetro **/v** se utiliza para pasar conmutadores de línea de mandatos y valores de propiedades públicas a través de Msiexec.exe.

/w Este parámetro obliga al archivo ejecutable a esperar hasta que finalice la instalación antes de salir. Si utiliza este parámetro en un archivo por lotes, puede colocar delante del argumento completo de línea de mandatos del archivo ejecutable `start /WAIT`. A continuación se proporciona un ejemplo de este uso con un formato correcto:

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

Instalación administrativa

El instalador de Microsoft Windows puede realizar una instalación administrativa de una aplicación o un producto en una red para un grupo de trabajo o para la personalización. Para el paquete de instalación de Client Security Software, una instalación administrativa desempaqueta los archivos de origen de instalación en una ubicación especificada. Para ejecutar una instalación administrativa, el paquete de configuración se debe ejecutar desde la línea de mandatos utilizando el parámetro **/a**:

```
z046zis2018usaa.exe /a
```

Se puede elegir una nueva ubicación que puede incluir unidades distintas de C: como, por ejemplo, otras unidades locales, unidades de red correlacionadas, etc. También se pueden crear nuevos directorios durante este paso.

Si una instalación administrativa se ejecuta de forma silenciosa, la propiedad pública TARGETDIR se puede establecer en la línea de mandatos para especificar la ubicación de extracción:

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

o bien

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

Para realizar la instalación desde el origen desempaquetado después de realizar las personalizaciones, el usuario invoca msiexec.exe desde la línea de mandatos. En el apartado "Parámetros de línea de mandatos" se describen los parámetros de línea de mandatos disponibles que se pueden utilizar con msiexec.exe, así como un ejemplo de como utilizarlos. También se pueden establecer propiedades públicas directamente en la invocación de línea de mandatos de msiexec.

Parámetros de línea de mandatos

/i *paquete* **o** *producto*
Utilice este formato para instalar el producto:

```
msiexec /i
"C:\CarpetaWindows\Profiles\NombreUsuario\Personal\MySetups\Othello\Trial
Version\Release\DiskImages\Disk1\productoOthello Beta.msi"
```

El código del producto hace referencia al GUID que se genera automáticamente en la propiedad de código de producto de la vista del proyecto del producto.

Nota: El ejemplo anterior se ha dividido en dos líneas para que entre en la página. Cuando especifique este mandato, escríbalo en una línea.

/a *paquete*
El parámetro **/a** permite a los usuarios con privilegios de administrador instalar un producto en la red.

/x *paquete* **o** *código del producto*
Este parámetro desinstala un producto.

/L [i | w | e | a | r | u | c | m | p | v | +] *archivo anotaciones cronológicas*
Este parámetro especifica la vía de acceso del archivo de anotaciones cronológicas. Los siguientes distintivos indican qué información se registra en el archivo de anotaciones cronológicas:

- **i**
  Anota mensajes de estado
- **w**
  Anota mensajes de aviso no graves
- **e**
  Anota cualquier mensaje de error
- **a**
  Anota las secuencias de comienzo de acciones

- **r**

  Anota registros específicos de acciones
- **u**

  Anota peticiones de usuario
- **c**

  Anota parámetros de la interfaz de usuario inicial
- **m**

  Anota mensajes de falta de memoria
- **p**

  Anota valores de terminal
- **v**

  Anota el valor de salida verbosa
- **+**

  Añade en un archivo existente
- *

  Es un carácter comodín que le permite anotar toda la información, excepto el valor de salida verbosa

/? o /h

Cualquiera de estos mandatos muestra la información de copyright del instalador de Windows

TRANSFORMS

Utilice el parámetro de línea de mandatos TRANSFORMS para especificar las transformaciones que desea que se apliquen al paquete base. La invocación de línea de mandatos de transformación será parecida a la siguiente:

```
msiexec /i
"C:\CarpetaWindows\Profiles\NombreUsuario\Personal\MySetups\Nombre
Proyecto\
Versión Prueba\Mi
Release-1\DiskImages\Disk1\NombreProducto.msi"
TRANSFORMS="Nueva Transformación 1.mst"
```

Como puede utilizar un punto y coma para separar varias transformaciones, se recomienda no utilizar el punto y coma en el nombre de la transformación, ya que el servicio del instalador de Windows no los interpretará correctamente.

Nota: El ejemplo anterior se ha dividido en tres líneas para que entre en la página. Cuando especifique este mandato, escríbalo en una línea.

Propiedades

Desde la línea de mandatos se pueden establecer o modificar todas las propiedades públicas. Las propiedades públicas se diferencian de las propiedades privadas en que están en mayúsculas. Por ejemplo, COMPANYNAME es una propiedad pública.

Para establecer una propiedad desde la línea de mandatos, utilice la sintaxis siguiente: `PROPIEDAD=VALOR`. Si desea cambiar el valor de *COMPANYNAME*, deberá entrar:

```
msiexec /i
"C:\CarpetaWindows\Profiles\NombreUsuario\Personal\MySetups\Nombre Proyecto\
Trial Version\Mi Release-1\DiskImages\Disk1\ProductName.msi"
COMPANYNAME="InstallShield"
```

Nota: El ejemplo anterior se ha dividido en tres líneas para que entre en la página. Cuando especifique este mandato, escríbalo en una línea.

Propiedades públicas personalizadas de Client Security Software

El paquete de instalación de Client Security Software contiene un conjunto de propiedades públicas personalizadas que se pueden establecer en la línea de mandatos cuando se ejecute la instalación. Las propiedades públicas personalizadas disponibles actualmente son:

INSTALLPWM
Se utiliza para controlar si Password Manager se instala durante la instalación inicial. Establézcala como 1 para instalar Password Manager, o como 0 para que no se instale Password Manager. El valor por omisión es 1.

CFGFILE
Esta propiedad se puede utilizar durante la instalación silenciosa para especificar la ubicación de un archivo de configuración. El archivo de configuración puede contener el valor de la contraseña existente del chip de seguridad. Esto permite finalizar la instalación sin la interacción del usuario, aunque exista previamente una contraseña en el chip. Por ejemplo:

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

Características de instalación de Client Security Software

La instalación con una sola pulsación de Client Security Software contiene dos características principales: *Security* (IBM Client Security Software) y *PWManager* (IBM Password Manager). Por omisión, se instalan las dos características, aunque existen varias opciones para ejecutar la instalación de forma que sólo se instale la característica Security (la característica Security es necesaria, mientras que PWManager no lo es). Si el usuario ejecuta la instalación con una interfaz de usuario y no está instalado IBM Password Manager Versión 1.3 o inferior, aparecerá una pantalla para elegir si desea instalar sólo IBM Client Security Software, o IBM Client Security Software e IBM Password Manager. Si el usuario ejecuta la instalación sin una interfaz de usuario (silenciosa), puede controlar si se instala Password Manager utilizando la propiedad INSTALLPWM (si se establece como 0, no se instala Password Manager). Si el usuario instala sólo IBM Client Security durante la instalación inicial y más tarde decide añadir IBM Password Manager, puede hacerlo ejecutando de nuevo el paquete de origen original. Si vuelve a ejecutar la instalación con una interfaz de usuario, aparecerá una pantalla de mantenimiento donde puede seleccionar el botón "Modificar" si no se ha instalado todavía Password Manager. Aparecerá una pantalla para que elija si desea reinstalar sólo Client Security o instalar conjuntamente IBM Client Security Software e IBM Password Manager. El usuario también puede reinstalar el producto desde el origen sin ninguna interfaz de usuario para añadir IBM Password Manager. A continuación se muestran algunos mandatos de ejemplo para realizar esta operación.

Ejemplos de utilización de Setup.exe

En la Tabla 1 se muestran algunos ejemplos de instalación en los que se utiliza z046zis2018usaa.exe.

Tabla 1. Ejemplos de instalación en los que se utiliza z046zis2018usaa.exe

Tipo	Ejemplo
Instalación silenciosa con reinicio y fin de la instalación	`z046zis2018usaa.exe /s /v/qn`
Instalación silenciosa sin reinicio	`z046zis2018usaa.exe /s /v"/qn REBOOT="R""`
Instalación silenciosa sin reinicio y sin instalar Password Manager	`z046zis2018usaa.exe /s /v"/qn REBOOT="R" INSTALLPWM=0"`
Instalación silenciosa sin reinicio, especificando el directorio de instalación	`z046zis2018usaa.exe /s /v"/qn REBOOT="R" INSTALLDIR=C:\ibmcss"`
Instalación silenciosa sin reinicio, especificando el archivo de configuración	`z046zis2018usaa.exe /s /v"/qn REBOOT="R" CFGFILE=C:\csec.ini"`
Instalación administrativa silenciosa	`z046zis2018usaa.exe /a`
Instalación administrativa silenciosa, especificando la ubicación de extracción	`z046zis2018usaa.exe /a /s /v"/qn TARGETDIR="F:\CSS""`
Instalar sin reinicio y crear un archivo de anotaciones cronológicas de instalación en un directorio temp	`z046zis2018usaa.exe /v"REBOOT="R" /L*v %temp%\css.log"`
Reinstalación silenciosa del producto para añadir Password Manager	`z046zis2018usaa.exe /s /v"/qn ADDLOCAL=PWManager"`

En la Tabla 2 se muestran algunos ejemplos de instalación en los que se utiliza msiexec.exe.

Tabla 2. Ejemplos de instalación en los que se utiliza msiexec.exe

Tipo	Ejemplo
Instalar con archivo de anotaciones cronológicas	`msiexec /i "C:\IBM Client Security Software.msi" /L*v %temp%\css.log`
Instalación silenciosa sin reinicio	`msiexec /i "C:\IBM Client Security Software.msi" /qn REBOOT="R"`
Instalación silenciosa sin reinicio y sin instalar Password Manager	`msiexec /i "C:\IBM Client Security Software.msi" /qn REBOOT="R" INSTALLPWM=0`
Reinstalación silenciosa del producto para añadir Password Manager	`msiexec /i "C:\IBM Client Security Software.msi" /qn ADDLOCAL=PWManager`

Capítulo 3. Cómo funciona el chip IBM Security Chip incorporado

El chip IBM Security Chip incorporado está representado gráficamente en la Figura 2. Existen tres componentes principales:

1. Contraseña del administrador
2. Clave pública de hardware
3. Clave privada de hardware

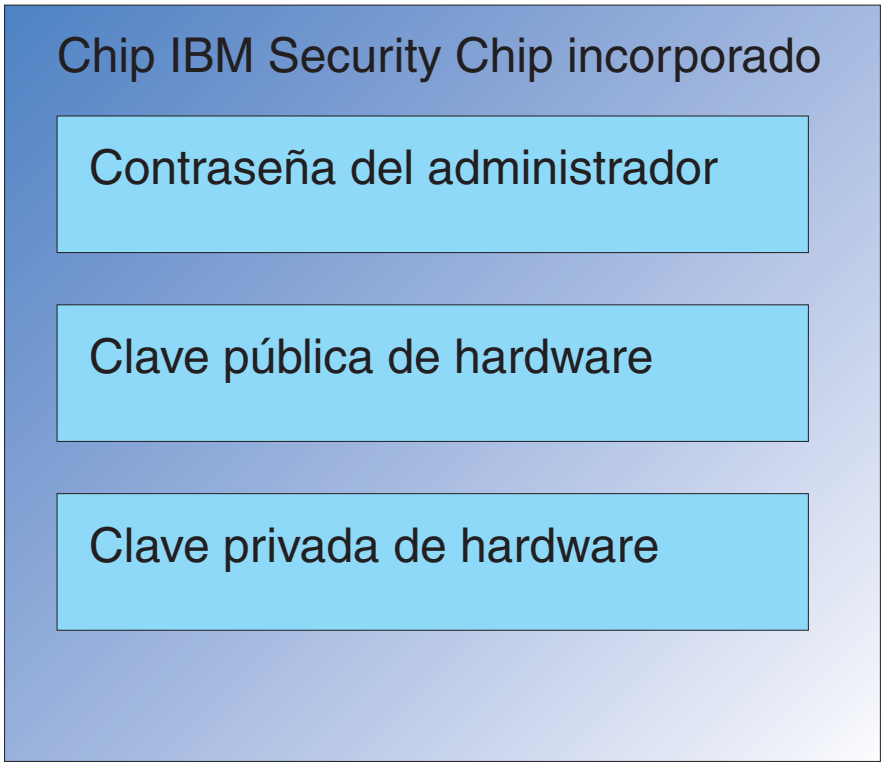

Figura 2. Datos contenidos en el chip IBM Security Chip incorporado

Las claves pública y privada de hardware son únicas en cada sistema. La clave privada de hardware nunca se puede extraer del chip. Se puede generar pares de claves de las siguientes formas:

- Mediante el asistente de Client Security Software
- Mediante Administrator Utility
- Mediante scripts

Tenga en cuenta que las claves de hardware no se pueden extraer del chip.

El administrador utiliza la contraseña del administrador para acceder a las funciones siguientes, incluidas:

- Adición de usuarios
- Establecimiento de políticas de seguridad
- Establecimiento de políticas de frases de paso

- Inscripción de smart cards
- Inscripción de dispositivos biométricos

Por ejemplo, un administrador puede necesitar permitir que un usuario aproveche las ventajas de las características y funciones del chip IBM Security Chip incorporado. La contraseña del administrador se establece cuando se instala Client Security Software. Los detalles sobre cómo y cuándo se establecen las contraseñas del administrador, se tratan más adelante en este documento.

Importante: desarrolle una estrategia de mantenimiento de las contraseñas del administrador, que deben establecerse cuando se configura ESS por primera vez. Es posible que cada sistema con chip IBM Security Chip incorporado tenga la misma contraseña del administrador, si el administrador de TI o el administrador de seguridad así lo determina. Alternativamente, cada departamento o edificio puede tener asignado una contraseña del administrador diferente.

Los otros componentes del chip IBM Security Chip incorporado son la clave pública de hardware y la clave privada de hardware. Este par de claves RSA se genera cuando se configura Client Security Software.

Cada sistema tendrá una clave pública de hardware única y una clave privada única. La posibilidad de números aleatorios del chip IBM Security Chip incorporado garantiza que cada par de claves de hardware es estadísticamente único.

La Figura 3 en la página 11 describe dos componentes adicionales del chip IBM Security Chip incorporado. Conocer estos dos componentes es fundamental para una gestión eficaz de la infraestructura de IBM Embedded Security Subsystem. La Figura 3 en la página 11 muestra las claves pública y privada del administrador así como las claves pública y privada del usuario. A continuación hay un resumen de las claves pública y privada.

- Las claves pública y privada se consideran un ″par de claves″.
- Las claves privada y pública están relacionadas matemáticamente de tal forma que:
  - Cualquier cosa cifrada con la clave pública sólo puede descifrarse con la clave privada.
  - Cualquier cosa cifrada con la clave privada sólo puede descifrarse con la clave pública.
  - Conocer la clave privada no le permite obtener la clave pública.
  - Conocer la clave pública no le permite obtener la clave privada.
  - Generalmente, la clave pública está disponible para todos.
- La clave privada debe protegerse enérgicamente.
- Las claves pública y privada son las bases para la infraestructura de claves públicas (PKI).

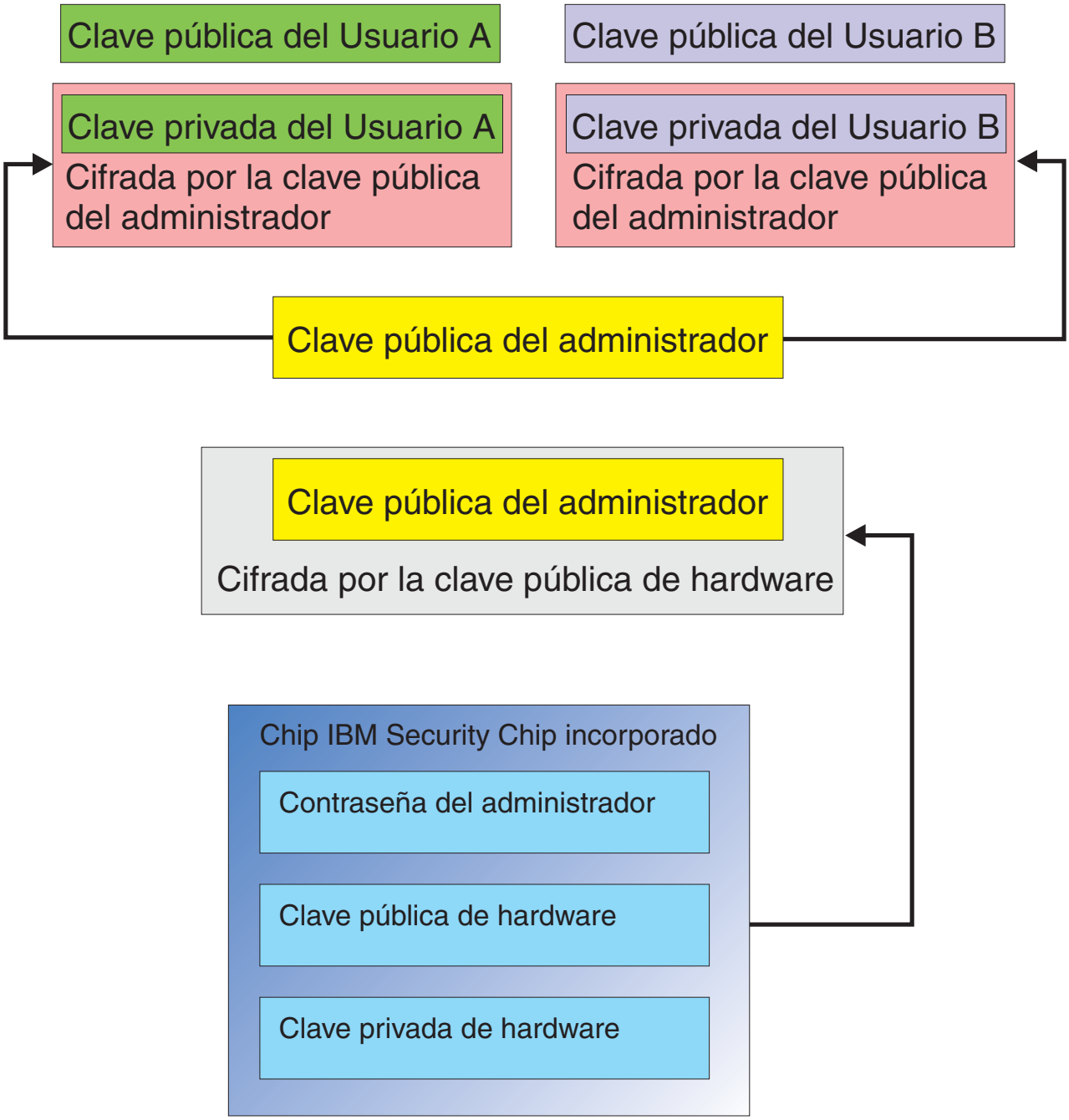

Figura 3. Varias capas de cifrado proporcionan una fuerte seguridad

Jerarquía de intercambio de claves

Parte de la arquitectura de IBM ESS es la jerarquía de "intercambio de claves". Los detalles precisos de su funcionamiento se tratarán en la *Guía del administrador y el usuario de IBM Client Security Software*; sin embargo, introducimos aquí el concepto ya que se aplica a la configuración, despliegue y gestión masivas. En la Figura 3, puede ver las claves pública y privada de hardware. Como se mencionaba anteriormente, estas claves son creadas por Client Security Software y son estadísticamente únicas en cada cliente. Sobre el chip IBM Embedded Security

incorporado puede ver el par de claves pública y privada del administrador. El par de claves pública y privada del administrador puede ser único en todos los sistemas o puede ser el mismo en todos los clientes o subconjunto de clientes. Las ventajas y desventajas se tratarán más adelante en este documento. Las claves pública y privada del administrador hacen lo siguiente:

- Proteger las claves pública y privada del usuario
- Permitir el archivo y restauración de credenciales de usuario
- Permitir la itinerancia de credenciales de usuario, descrita en la *Guía del administrador y el usuario de IBM Client Security Software*

¿Por qué el intercambio de claves?

En los apartados siguientes se hablará sobre los usuarios del entorno IBM ESS. En estos apartados se cubrirán los detalles de cómo configurar IBM y ESS para alojar a estos usuarios. En este caso simplemente estipularemos que cada usuario tiene una clave pública y privada. La clave privada del usuario se cifra con la clave pública del administrador. En la Figura 3 en la página 11, puede ver que la clave privada del administrador se cifra con la clave pública de hardware. ¿Por qué nos tenemos que preocupar en cifrar estas diferentes claves privadas?

Esta razón nos lleva de nuevo a la jerarquía mencionada anteriormente. Debido al espacio de almacenamiento limitado del chip IBM Security Chip incorporado, sólo puede haber un número limitado de claves en el chip en un momento dado. Las claves pública y privada de hardware son las únicas claves persistentes (de arranque a arranque) en este escenario. Para permitir varias claves y varios usuarios, IBM ESS implementa una jerarquía de intercambio de claves. Siempre que se necesite una clave, ésta se ″intercambia″ dentro del chip IBM Security Chip incorporado. Mediante el intercambio de claves privadas cifradas dentro del chip, la clave privada puede descifrarse y utilizarse sólo en el entorno protegido del chip.

La clave privada del administrador se cifra con la clave pública de hardware. La clave privada de hardware, que sólo está disponible en el chip, se utiliza para descifrar la clave privada del administrador. Una vez descifrada la clave privada del administrador en el chip, puede pasarse dentro del chip una clave privada de usuario desde el disco duro (cifrada con la clave pública del administrador) y descifrarla con la clave privada del administrador. En la Figura 3 en la página 11 puede ver que puede disponer de varias claves privadas de usuario cifradas con la clave pública del administrador. Esto proporciona la capacidad de configurar tantos usuarios como sean necesarios en un sistema con IBM ESS.

Capítulo 4. Consideraciones clave para archivar

Las contraseñas y la claves trabajan juntas, junto con otros dispositivos de autenticación opcionales, para verificar la identidad de los usuarios del sistema.

La Figura 4 muestra cómo funcionan de forma conjunta IBM Embedded Security Subsystem y Client Security Software. El inicio de sesión de Windows solicita al Usuario A que inicie la sesión y el Usuario A lo hace. IBM Client Security System determina quién es el usuario actual mediante información proporcionada por el sistema operativo. La clave privada del administrador, cifrada con la clave pública de Hardware, se carga en el chip IBM Security Chip incorporado.

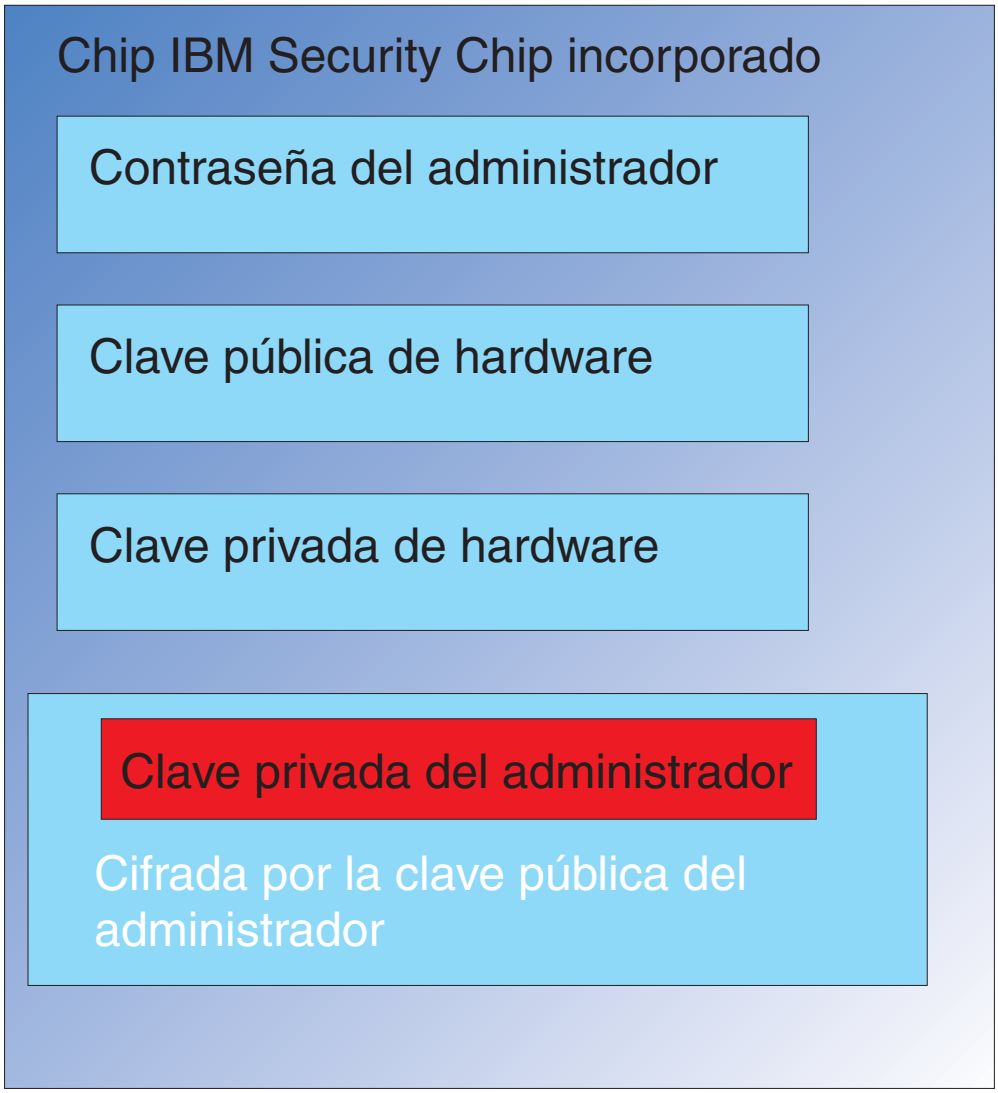

Figura 4. La clave privada del administrador, cifrada por la clave pública de hardware, se carga en el chip IBM Security Chip incorporado.

La clave privada de hardware (que sólo está disponible en el chip) descifra la clave privada del administrador. Ahora, la clave privada del administrador está disponible para su utilización en el chip, tal como se muestra en la Figura 5.

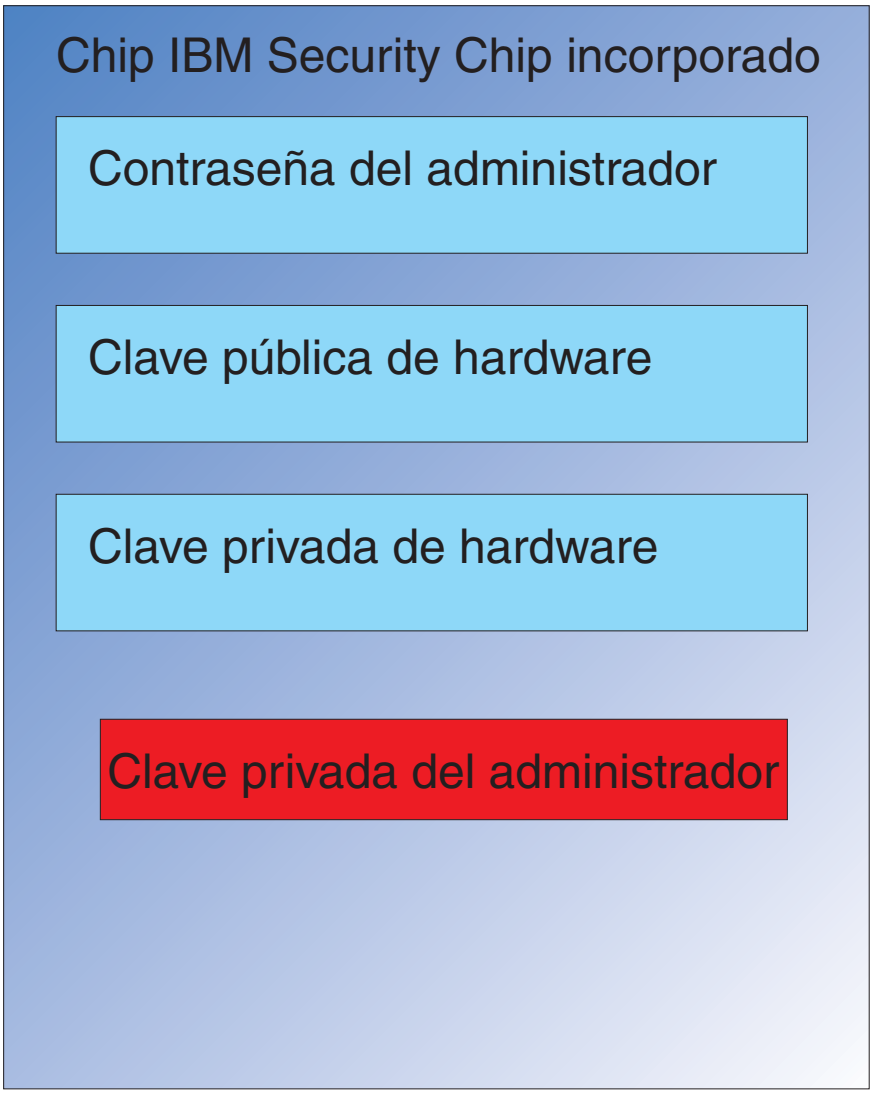

Figura 5. La clave privada del administrador está disponible para su utilización en el chip.

Como el Usuario A ha iniciado la sesión en el sistema, la clave privada del Usuario A (cifrada con la clave pública del administrador) se pasa al chip, como se muestra en la Figura 6 en la página 15.

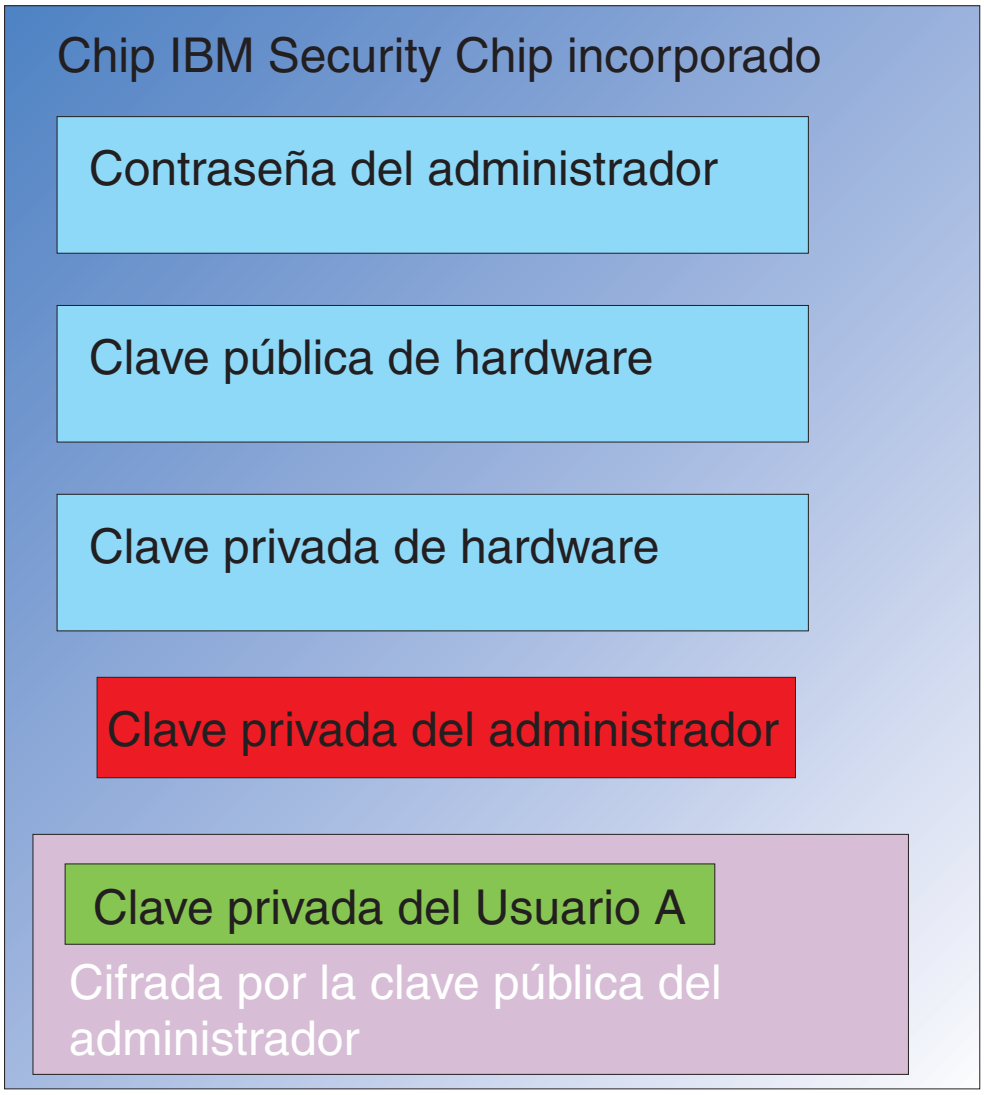

Figura 6. La clave privada del Usuario A, cifrada por la clave pública del administrador, se pasa al chip de seguridad.

La clave privada del administrador se utiliza para descifrar la clave privada del Usuario A. Ahora, la clave privada del Usuario A está lista para su utilización, como se muestra en la Figura 7 en la página 16.

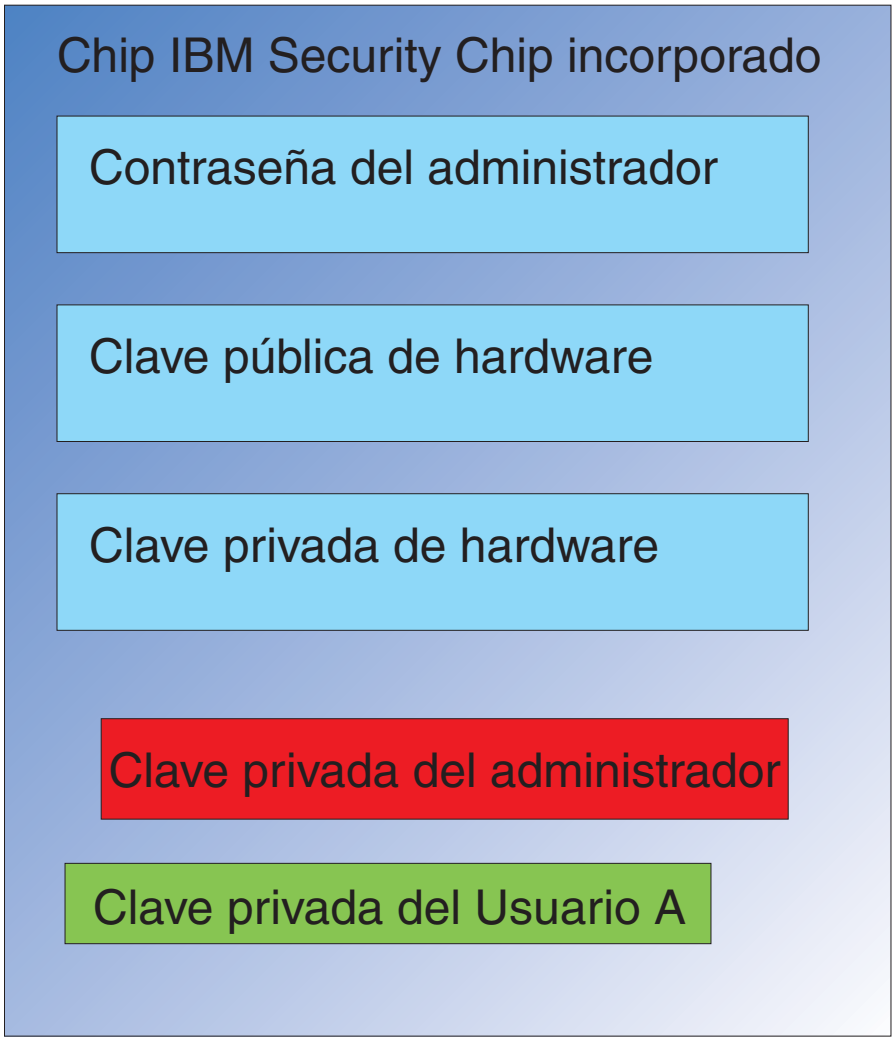

Figura 7. La clave privada del Usuario A está lista para su utilización.

Hay otras claves que pueden cifrarse con la clave pública del Usuario A. Un ejemplo sería una clave privada utilizada para firmar correo electrónico. Cuando el Usuario A va a enviar un correo electrónico firmado, la clave privada utilizada para firmar (cifrada con la clave pública del Usuario A) se pasa al chip. La clave privada del Usuario A (ya en el chip) descifrará la clave de firma privada del Usuario A. Ahora la clave de firma privada del Usuario A está disponible en el chip para realizar la operación deseada, en este caso crear una firma digital (cifrado de un hash). Tenga en cuenta que se utilizará el mismo proceso de traslado de claves dentro y fuera del chip cuando el Usuario B inicie la sesión en el sistema.

¿Por qué un par de claves del administrador?

La razón principal para disponer de un par de claves del administrador es por tener posibilidades de archivo y restauración. El par de claves del administrador sirve como capa de abstracción entre el chip y las credenciales de usuario. La información de la clave privada específica del usuario se cifra con la clave pública del administrador como se muestra en la Figura 8 en la página 17.

Importante: desarrolle una estrategia de mantenimiento de los pares de claves del administrador. Es posible que cada sistema con chip IBM Security Chip incorporado tenga el mismo par de claves del administrador, si el administrador de TI o el administrador de seguridad así lo determina. Alternativamente, cada departamento o edificio puede tener asignado un par de claves del administrador diferente.

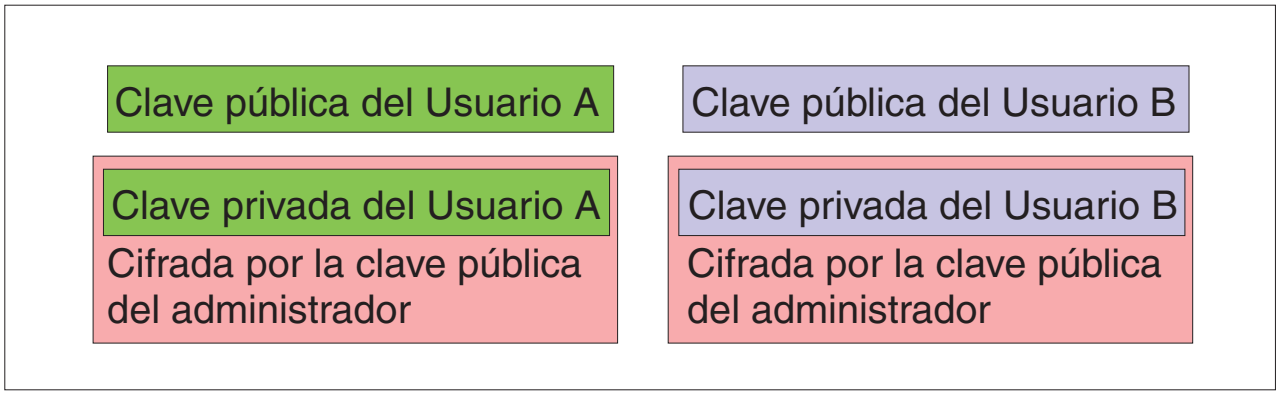

Figura 8. La información de clave privada específica del usuario se cifra con la clave pública del administrador.

Otra razón para tener un par de claves del administrador es el firmar el archivo de políticas de seguridad del cliente, evitando por lo tanto que nadie salvo el administrador pueda cambiar la política de seguridad. Para poder alcanzar un alto nivel de seguridad del archivo de políticas de seguridad del cliente, puede dividir la clave privada del administrador hasta entre cinco individuos. En ese caso, los cinco individuos que tienen parte de la clave privada, deben estar todos presentes para firmar y cifrar archivos, como el archivo de políticas de seguridad del cliente. Esto evita que un solo individuo realice funciones de administración unilateralmente. Para obtener información sobre la división de la clave privada del administrador, consulte el valor Keysplit=1 en Tabla 6 en la página 41.

Durante la inicialización de IBM Client Security Software, los pares de claves del administrador pueden crearse por el software o pueden importarse de un archivo externo. Si desea utilizar un par de claves del administrador común, especificará la ubicación de los archivos necesarios durante la instalación del cliente.

Se hace copia de seguridad (graba) esta información específica del usuario en una ubicación de archivo definida por el administrador como se muestra en la Figura 8. Esta ubicación de archivo puede ser cualquier tipo de soporte que esté conectado físicamente o lógicamente con el cliente. El apartado de instalación de IBM Client Security System tratará sobre las recomendaciones para esta ubicación de archivo.

Las claves pública y privada del administrador no se archivan. Los datos del usuario situados en la ubicación de archivo se cifran con la clave pública del administrador. Disponer sólo de los datos de archivo del usuario no sirve de nada si no tiene la clave privada del administrador para desbloquear los datos. A menudo se hace referencia a las claves pública y privada del administrador en la documentación de IBM Client Security Software como "par de claves del archivador". Tenga en cuenta que el par de claves del archivador no está cifrado. Debe tenerse especial cuidado a la hora de almacenar y proteger el par de claves del archivador.

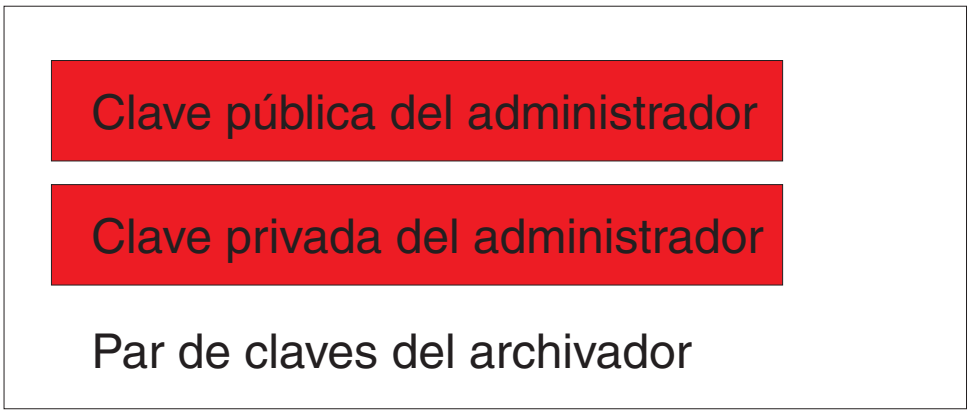

Figura 9. Las claves pública y privada del administrador forman el par de claves del archivador

Como se ha mencionado anteriormente, una de las funciones más importantes de las claves pública y privada del administrador es la de copia de seguridad y restauración del contenido del disco. Esta funcionalidad se muestra de la 10 a la 15. Los pasos son los siguientes:

1. El Cliente A, por alguna razón, deja de estar disponible para el Usuario A. En este ejemplo, diremos que al sistema, Cliente A, le ha caído un rayo, como se muestra en la Figura 10 en la página 19.

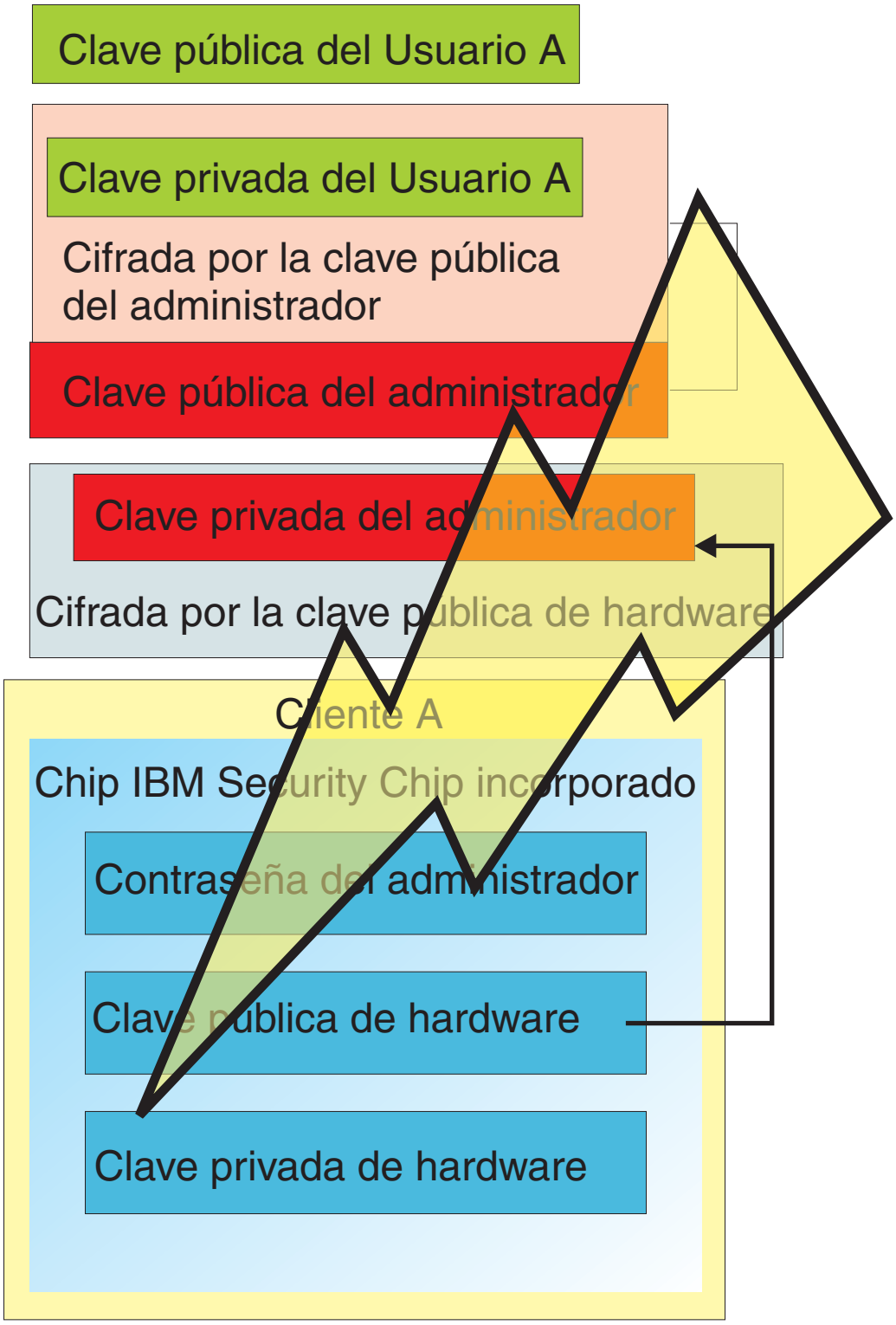

Figura 10. Al sistema del Usuario A le ha caído un rayo, por lo que ya no puede utilizarse.

2. El Usuario A obtiene un sistema de IBM nuevo y mejorado, que llamaremos Cliente B, como se muestra en la Figura 11 en la página 20. El Cliente B es distinto del Cliente A y las claves pública y privada de hardware son diferentes de las del Cliente A. Esta diferencia está representada visualmente por las claves de color gris en el Cliente B y las claves de color verde en el Cliente A.

Sin embargo, tenga en cuenta que la contraseña del administrador es la misma en el Cliente B y en el A.

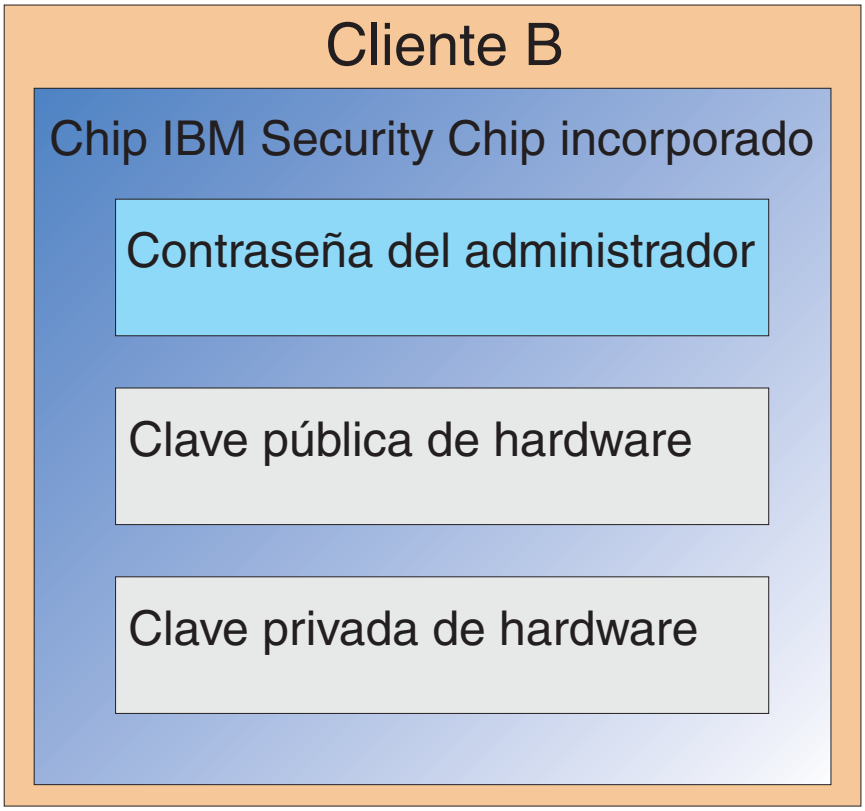

Figura 11. El Usuario A recibe un nuevo sistema, el Cliente B, con un chip IBM Security Chip incorporado.

3. El Cliente B ahora necesita las mismas credenciales de usuario que había en el Cliente A. Esta información se archivó para el Cliente A. Si vuelve a la Figura 8 en la página 17, recordará que las claves del usuario se cifraron con la clave pública del administrador y se almacenaron en la ubicación de archivo. Para que las credenciales de usuario estén disponibles en el Cliente B, las claves pública y privada del administrador deben transferirse a esta máquina. La Figura 12 muestra al Cliente B recuperando las claves pública y privada del administrador para recuperar datos del usuario de la ubicación de archivo.

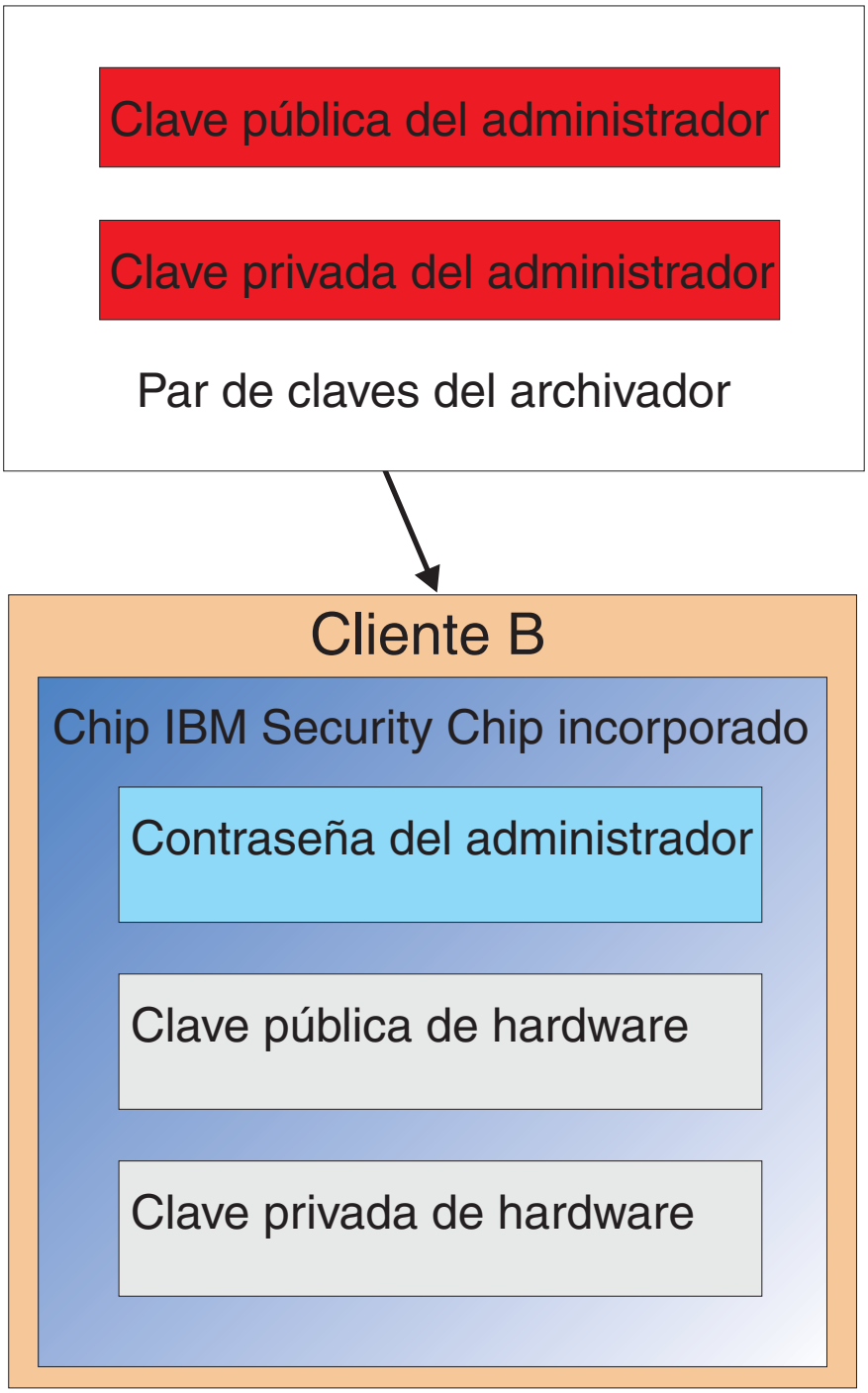

Figura 12. El Cliente B recupera las claves pública y privada del administrador de la ubicación de archivo.

4. La Figura 13 en la página 22 muestra la clave privada del administrador que se está cifrando con la clave pública de hardware del Cliente B.

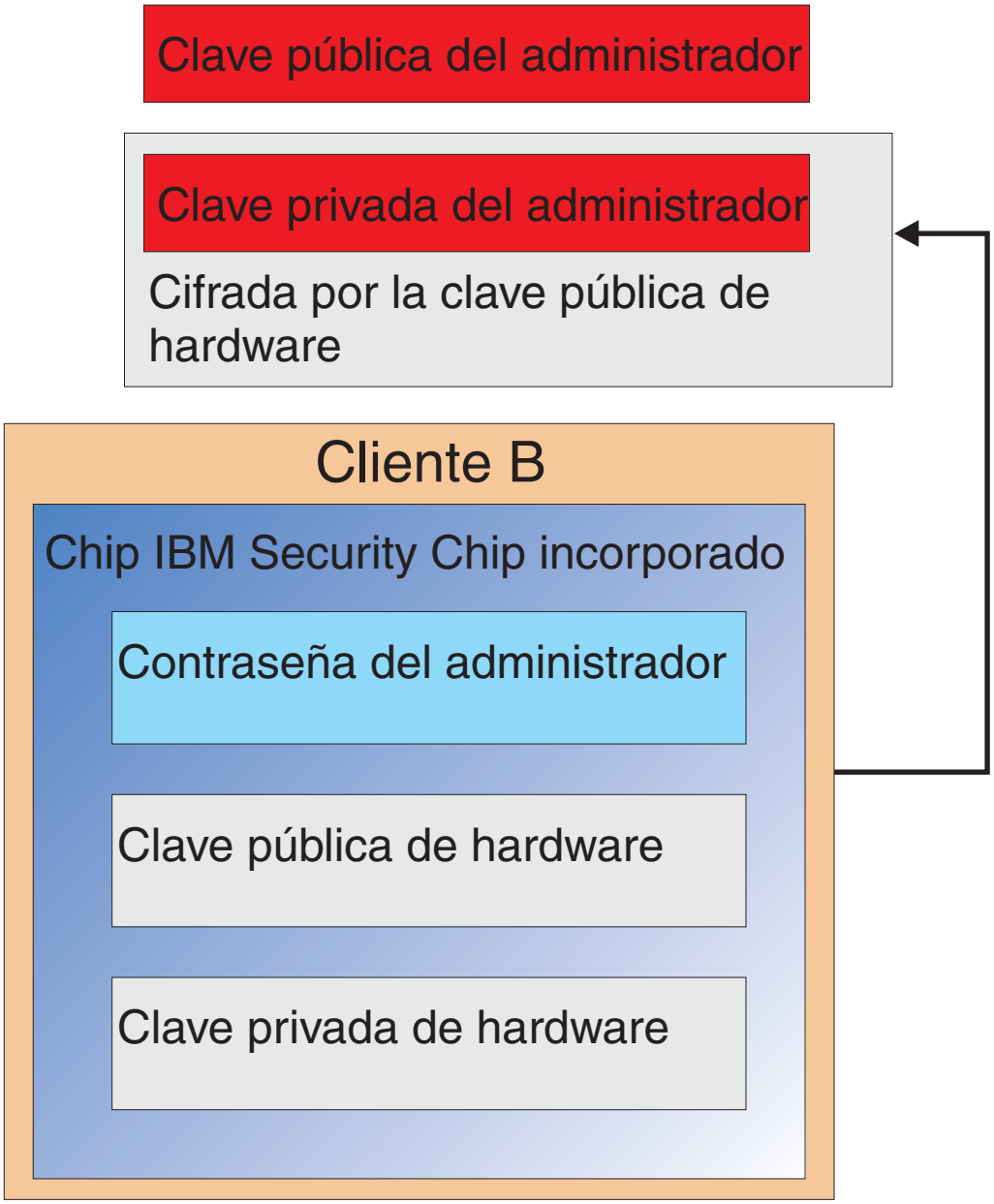

Figura 13. La clave privada del administrador se cifra con la clave de hardware del Cliente B.

Ahora que la clave privada del administrador se ha cifrado con la clave pública de hardware, las credenciales de usuario pueden cargarse en el Cliente B para el Usuario A, como se muestra en la Figura 14 en la página 23.

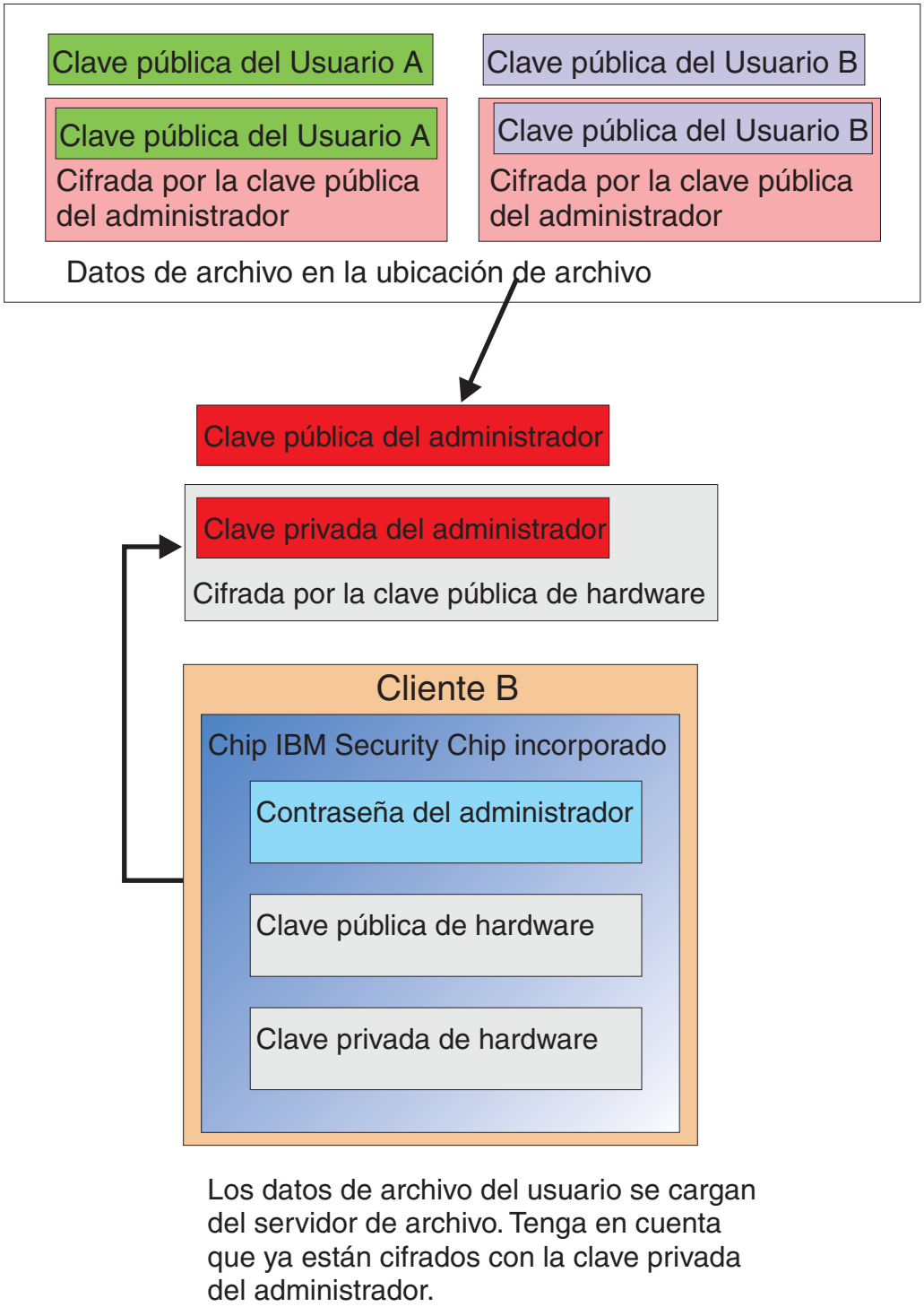

Figura 14. Las credenciales del Usuario A pueden cargarse en el Cliente B después de haberse cifrado la clave privada del administrador.

La Figura 15 en la página 24 muestra el Usuario A totalmente restaurado en el Cliente B. Tenga en cuenta que la clave privada del Usuario A se ha cifrado con la clave pública del administrador mientras estaba en el servidor de archivo. La clave pública del administrador es una clave RSA de 2048 bits y es virtualmente imposible de descifrar. Esto significa que no es totalmente necesario que la ubicación de archivo esté protegida o tenga un fuerte control de acceso. Mientras

que el par de claves de archivador (las claves pública y privada del administrador) y más específicamente la clave privada del administrador se mantengan seguras, la ubicación de archivo de las credenciales de usuario puede estar casi en cualquier sitio.

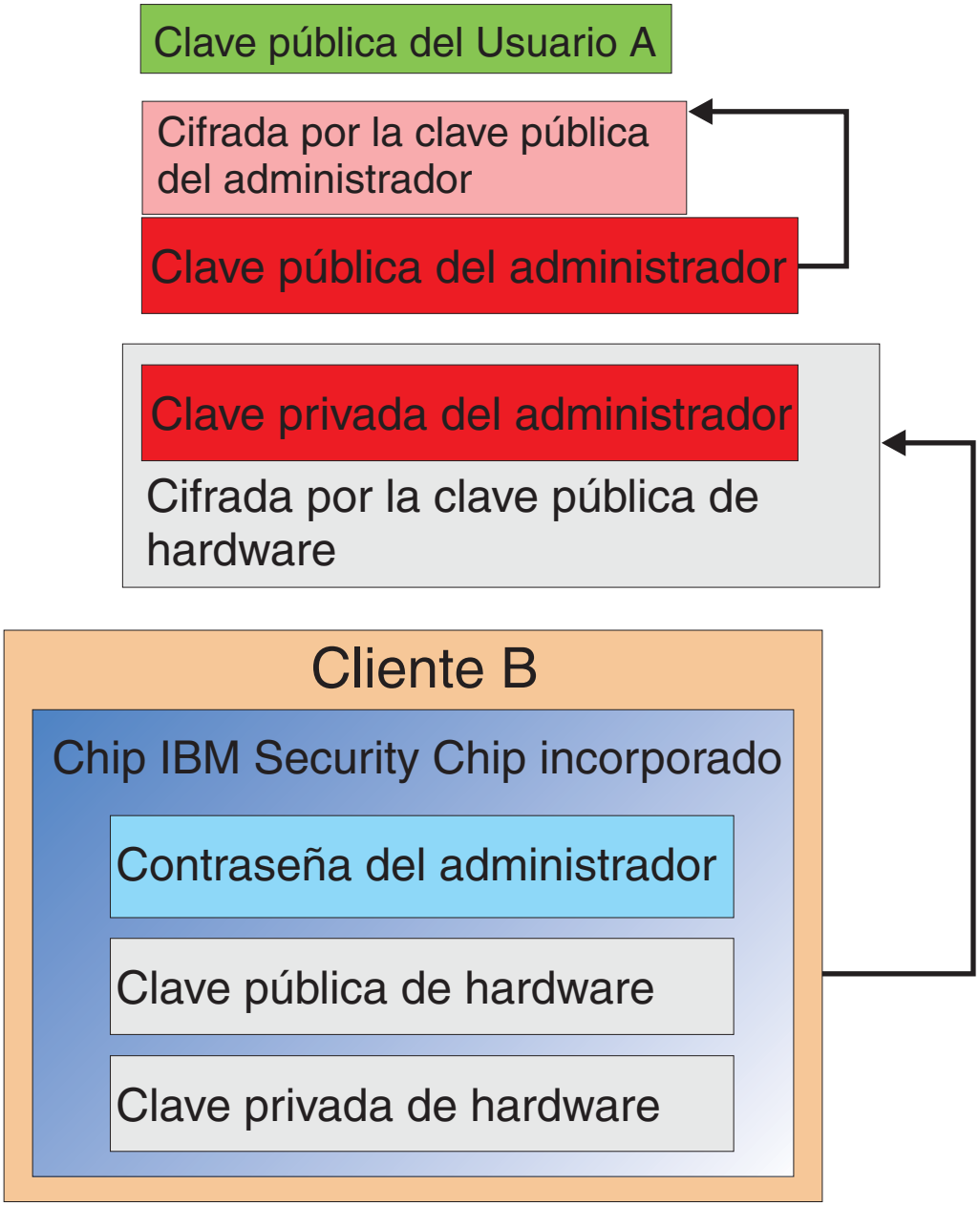

Figura 15. El Usuario A está totalmente restaurado en el Cliente B.

Los detalles de cómo se establece la contraseña del administrador, dónde deben estar las ubicaciones de archivo, etc. se tratará con mayor detalle cuando lleguemos al apartado de instalación del software. La Figura 16 muestra una visión general de los componentes de un entorno ESS. Los puntos principales son que cada cliente es único desde la perspectiva de una clave pública y privada, pero tiene una clave pública y privada del administrador común. Los clientes tienen una ubicación de

archivo común pero esta ubicación de archivo puede ser para un segmento o grupo de usuarios.

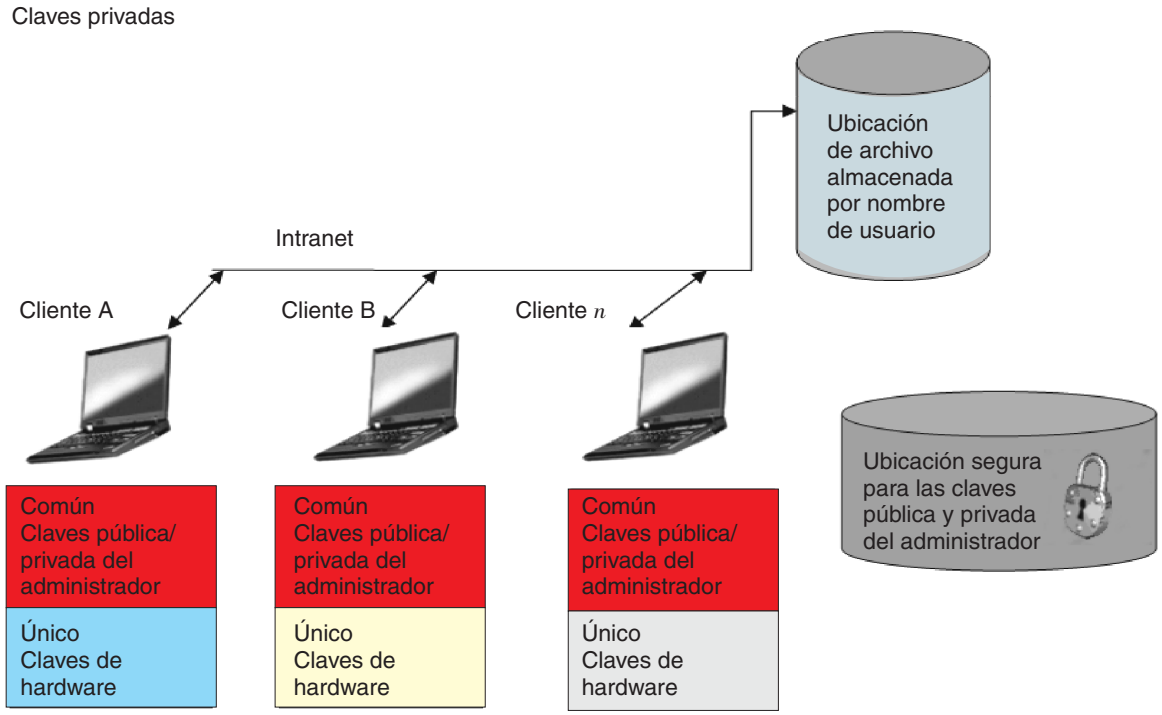

Figura 16. Componentes principales de IBM Client Security System.

Considere el ejemplo siguiente. El departamento de Recursos humanos tiene una ubicación de archivo distinta de la del departamento de Ingeniería. El archivo se realiza por nombre de usuario y de sistema. IBM Client Security Software archivará los usuarios de un sistema en la ubicación de archivo definida basándose en el nombre del usuario y en el nombre del sistema, como se mostraba anteriormente en el Usuario A y Usuario B. Tenga en cuenta también la ubicación segura de las claves pública y privada del administrador.

Nota: Cada nombre de sistema y nombre de usuario que se archivan en una misma ubicación deben ser únicos. Un nombre de sistema o nombre de usuario duplicado se escribirá encima del mismo nombre.

Capítulo 5. IBM Client Security Software

IBM Client Security Software es la conexión entre las aplicaciones y el chip IBM Security Chip incorporado, así como la interfaz para inscribir usuarios, establecer políticas y realizar las funciones básicas de administración. IBM Client Security System está compuesto principalmente de los siguientes componentes:

- Administrator Utility
- User Configuration Utility
- Administrator Console
- Asistente de instalación
- User Verification Manager (UVM)
- Proveedor de servicios criptográficos
- Módulo PKCS#11

IBM Client Security System le permite realizar varias funciones clave:

- Inscribir usuarios
- Establecer políticas
- Establecer políticas de frases de paso
- Restablecer frases de paso olvidadas
- Restablecer credenciales de usuario

Por ejemplo, si el Usuario A inicia la sesión en el sistema operativo, IBM basa todas las decisiones asumiendo que el Usuario A ha iniciado la sesión. **Nota:** la política de seguridad se basa en la máquina, no en el usuario; la política se aplica a todos los usuarios de una sola máquina. Si el Usuario A intenta utilizar IBM Embedded Security Subsystem, IBM Client Security System impondrá las políticas de seguridad establecidas para el Usuario A en ese sistema, como la frase de paso y la autenticación de la huella dactilar. Si la persona que inicia la sesión como Usuario A no puede suministrar la frase de paso correcta ni la huella dactilar correcta para la autenticación, IBM ESS prohibirá al usuario realizar la acción solicitada.

Inscripción de usuarios y gestión de las inscripciones

Los usuarios de IBM ESS son simplemente usuarios de Windows que están inscritos en el entorno IBM ESS. Los usuarios pueden inscribirse de varias formas, que se tratarán en detalle más adelante en este documento. En este apartado, trataremos lo que ocurre cuando se inscribe un usuario. Entender lo que ocurre durante este proceso le permitirá conocer mejor cómo funciona IBM ESS y, en ultima instancia, cómo gestionarlo con éxito en su entorno.

El software Client Security utiliza UVM (User Verification Manager) para gestionar las frases de paso y otros elementos para autenticar los usuarios del sistema. El software UVM permite utilizar las características siguientes:

- Protección de política de cliente de UVM
- Protección de inicio de sesión del sistema de UVM
- Protección de protector de pantalla de Client Security de UVM

Cada usuario del entorno IBM ESS tiene al menos un objeto de personalización asociado que se utiliza para cuestiones de autenticación. El requisito mínimo es una frase de paso. Todos los usuarios del componente UVM del entorno ESS (desde la perspectiva de usuario, UVM gestiona la autenticación y hace cumplir la política de seguridad) debe tener una frase de paso y esta frase de paso debe proporcionarse una vez por arranque del sistema, como mínimo. En los apartados siguientes se explicará por qué se utiliza una frase de paso y cómo utilizarla.

Necesidad de una frase de paso

Expuesto de forma sencilla, la frase de paso se necesita por razones de seguridad. Disponer de un elemento de hardware como IBM Embedded Security Subsystem es una ventaja tremenda porque proporciona una ubicación segura y autónoma para trabajar sobre las credenciales de usuario. Sin embargo, la protección que proporciona un chip de hardware es de poca utilidad si la autenticación que se necesita para acceder al chip es débil. Por ejemplo, supongamos que tiene un chip de hardware que realiza funciones de seguridad. Sin embargo, la autenticación necesaria para invocar una acción del chip es un solo dígito. En este caso, un hacker potencial tendría que averiguar un sólo dígito numérico (0 a 9) para poder invocar acciones con sus credenciales. La autenticación de un solo dígito debilita la seguridad del chip porque proporciona muy pocas o ninguna ventaja frente a una solución basada en software. Si no tiene una autenticación fuerte junto con la protección de hardware, no habrá ganado nada en seguridad. La frase de paso que necesita IBM se utiliza para autenticar al usuario antes de realizar cualquier acción en el hardware con las credenciales de usuario. La frase de paso de UVM sólo es recuperable mediante el par de claves del administrador, pos tanto no se puede recuperar de un sistema robado.

Configuración de una frase de paso

Cada usuario selecciona una frase de paso para proteger sus credenciales. En la Capítulo 3, “Cómo funciona el chip IBM Security Chip incorporado”, en la página 9 vio que la clave privada del usuario se cifraba con la clave pública del administrador. La clave privada del usuario también tiene asociada una frase de paso. Esta frase de paso se utiliza para autenticar el usuario con sus credenciales. La Figura 17 muestra la frase de paso más el componente de clave privada cifrado con la clave pública del administrador.

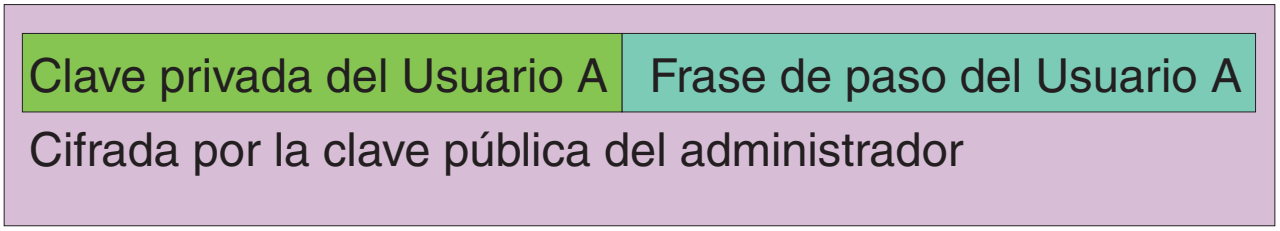

Figura 17. El Usuario A debe proporcionar la frase de paso para poder realizar cualquier función que requiera la clave privada del Usuario A.

El usuario selecciona la frase de paso mostrada en la Figura 17 según la política existente, es decir, las reglas especificadas para controlar la creación de contraseñas, como el número de caracteres y el número de días que es válida la contraseña. La frase de paso se crea cuando un usuario se inscribe en UVM. Una vez más veremos más adelante en este documento cómo ocurre realmente esto en IBM Client Security Software.

La clave privada del Usuario A se cifra con la clave pública del administrador, porque para descifrar la clave privada se necesita la clave privada del administrador. Por tanto, si el Usuario A olvida la frase de paso, el administrador puede restablecer una nueva frase de paso.

Utilización de una frase de paso

Desde la Figura 18 a la Figura 20 en la página 31, se muestra cómo se procesa la frase de paso en el chip. Una frase de paso debe utilizarse siempre la primera vez y al menos una vez por sesión. La frase de paso siempre es necesaria. Puede elegir añadir dispositivos de autenticación adicionales, pero ninguno de ellos puede sustituir al requisito de la frase de paso del usuario inicial. Brevemente, los datos biométricos u otros datos de autenticación se cifran con la clave pública del usuario. Es necesario acceder a la clave privada para descifrar estos datos de seguridad adicionales.

Figura 18. La clave privada del administrador se descifra en el chip.

Por tanto, es necesario proporcionar la frase de paso al menos una vez por sesión para descifrar los datos adicionales. Las credenciales que constituyen la clave privada del Usuario A y la frase de paso del Usuario A cifrados con la clave pública del administrador se pasan al chip IBM Security Chip incorporado. La clave privada del administrador ya está descifrada en el chip como se ha descrito

anteriormente. Las credenciales se pasan como se describe en la Figura 19. Las credenciales se descifran, lo que hace que estén disponibles en el chip la clave

Figura 19. La clave privada del Usuario A y la frase de paso del Usuario A están disponibles en el chip.

privada del Usuario A y la frase de paso del Usuario A. Cuando el usuario que ha iniciado actualmente la sesión, identificado por IBM Client Security System como Usuario A, intenta utilizar las credenciales del Usuario A, se abre el diálogo de la frase de paso, como se muestra en la Figura 20 en la página 31.

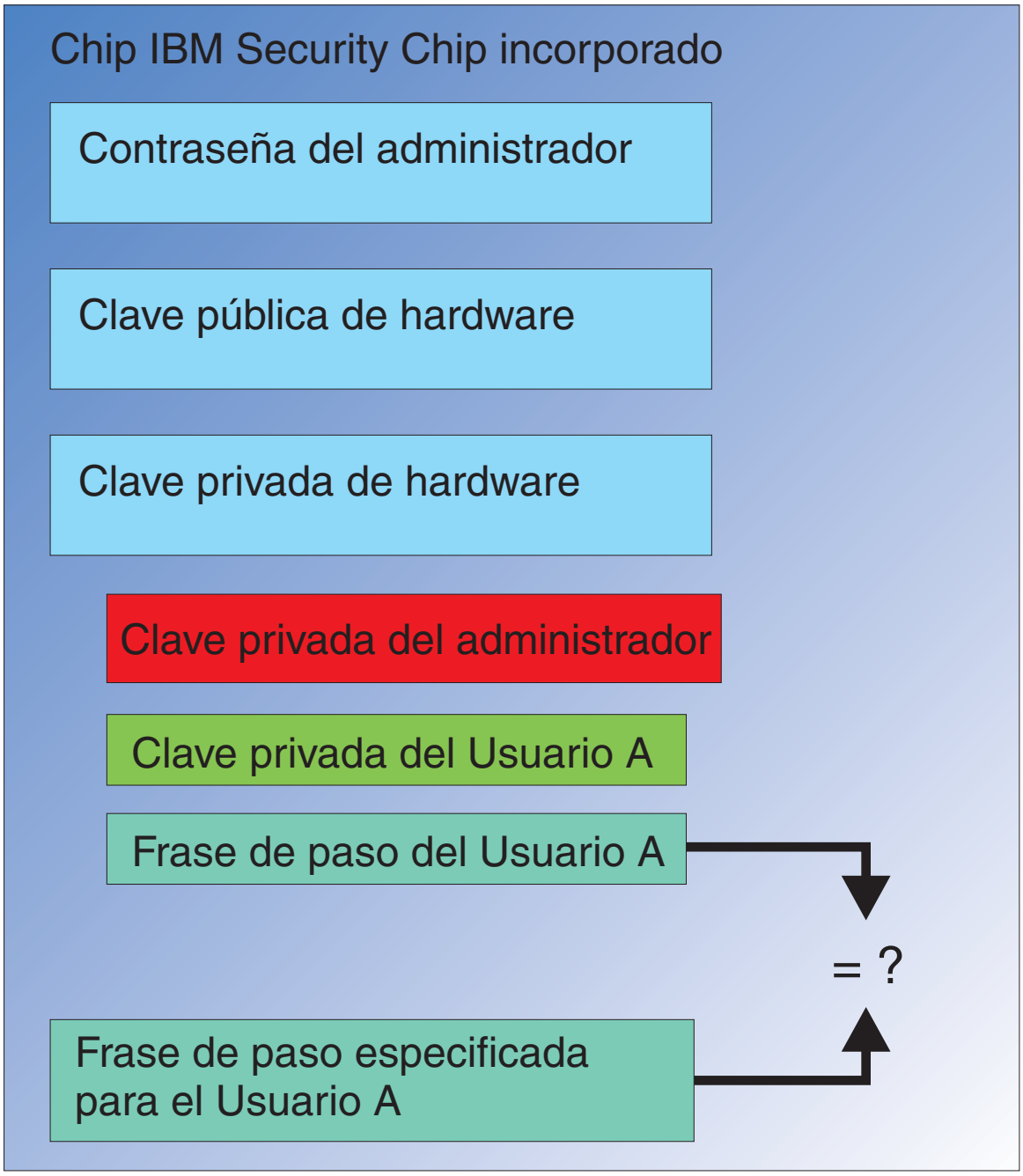

Figura 20. Cuando el Usuario A intenta utilizar las credenciales del Usuario A se abre el diálogo de la frase de paso.

La frase de paso especificada se pasa al chip y se compara con el valor de la frase de paso descifrada. So coinciden, pueden utilizarse las credenciales del Usuario A para diversas funciones como firmas digitales o descifrar correos electrónicos. Tenga en cuenta que esta comparación de frases de paso se realiza en el entorno seguro del chip. El chip tiene capacidades para no permitir los intentos de acceso repetitivos fallidos. Tenga también en cuenta que la frase de paso registrada del Usuario A nunca se expone fuera del chip. Como parte de la instalación de IBM Client Security Software, los usuarios se inscriben. Parte de este proceso de inscripción es la creación de la frase de paso del usuario. Trataremos los detalles de cómo se establece esta frase de paso y como pueden imponerse las normas de la frase de paso.

La Figura 1 en la página 1 mostraba el chip IBM Security Chip incorporado así como IBM Client Security System. La Figura 1 en la página 1 también describe la inicialización de la empresa y del usuario. La inicialización de la empresa está asociada con Embedded Security Subsystem y la inicialización del usuario está asociada con IBM Client Security Software. En los apartados anteriores se describía la inicialización que tiene lugar con el fin de conocer el concepto general. En los apartados siguientes se darán más detalles sobre el proceso de inicialización.

Inicialización de TPM

La inicialización de TPM es fundamentalmente el proceso de añadir las claves pública y privada de hardware y una contraseña del administrador. Este proceso toma una máquina genérica, tal y como viene de IBM, y la convierte en única para la empresa. El diagrama siguiente muestra los métodos de inicialización de las claves pública y privada así como las contraseñas del administrador.

Tabla 3. Métodos de inicialización de hardware

Acción	Puede crearse en el BIOS	Puede crearse manualmente por el administrador en el software CSS	Puede crearse en un script
Creación de la clave pública/privada de hardware	No	Sí	Sí
Creación de la contraseña del administrador	En algunos clientes compatibles con TCPA, sí. Comprobar la entrada del BIOS.	Sí	Sí

La Tabla 3 demuestra que las claves pública y privada de hardware no se crean automáticamente cuando se instala el software. La creación de las claves pública y privada de hardware debe iniciarse manualmente en el software o mediante el script. La contraseña del administrador puede crearse en el BIOS, en la aplicación IBM Client Security Software o mediante un script. El chip controla los valores establecidos para las claves pública y privada de hardware; usted no puede establecer los valores. Las capacidades de generación de números aleatorios del chip se utilizan para producir pares de claves pública y privada estadísticamente aleatorias. Sin embargo, usted si establece la contraseña del administrador.

La contraseña del administrador, no obstante, es diferente porque el administrador debe establecer este valor. Debemos determinar varios temas relacionados con la contraseña del administrador:

- ¿Qué establecerá como contraseña o contraseñas del administrador?
- ¿Tendrá más de una para varios grupos? En ese caso, ¿cómo determinará de forma lógica que sistemas tienen qué contraseña?
- ¿Qué administrador tendrá acceso a la contraseña? Si tiene más de una contraseña para grupos separados de usuarios, ¿quién tendrá acceso a esas contraseñas?
- ¿Qué usuarios finales autoadministrados tienen acceso a la contraseña del administrador?

Para tomar decisiones efectivas sobre los temas anteriores, es importante conocer qué es lo que permite hacer la contraseña del administrador:

- Poder acceder a los programas de utilidad del administrador

- Añadir/eliminar usuarios
- Definir qué aplicaciones/características de IBM Client Security Software se pueden utilizar

En los apartados siguientes explicaremos la conexión entre el archivo de políticas y la clave privada del administrador. De momento tenga en cuenta que la clave privada del administrador se necesita para cambiar políticas. La Tabla 4 resume las posibilidades que se obtienen al disponer de la contraseña del administrador o la clave privada del administrador.

Tabla 4. Acciones del administrador basadas en la contraseña y en la clave privada

Acción	Contraseña del administrador	Clave privada del administrador
Poder acceder al programa de utilidad del administrador	Sí	No
Añadir/Eliminar/Restaurar usuarios	Sí	No
Definir qué aplicaciones/características de CSS se pueden utilizar	Sí	No
Definir/Cambiar políticas	Sí	Sí
Crear archivos para restablecer las frases de paso de los usuarios	Sí	Sí

La inicialización de TPM también hace referencia a las claves pública y privada del administrador. En el diagrama anterior puede ver las posibilidades asociadas con esta clave. Pensemos un poco en cómo se establecen las claves pública y privada del administrador. Este par de claves puede ser único para cada sistema o puede ser el mismo para todas las máquinas. Cuando el administrador inicializa IBM Client Security Software tiene la opción de utilizar un par de claves existente o de crear un nuevo par de claves para el cliente. De nuevo, el modelo de uso determinará qué es lo mejor para su empresa.

Recomendaciones

Las grandes empresas pueden utilizar una clave única para cada máquina o una clave única para cada departamento. Por ejemplo, establecer una contraseña y/o clave privada del administrador para todos los sistemas utilizados en el departamento de recursos humanos, otra para el departamento de ingeniería, etc. También puede diferenciar sobre un elemento físico, como por edificio o por emplazamiento. La capacidad de determinar qué clave privada de administrador utilizar cuando se crea un archivo para restablecer la frase de paso debería ser un proceso sencillo basado en quién solicita restablecerla. Como se indica en la Tabla 3 en la página 32 y en la Tabla 5 en la página 36, también debe realizarse la inicialización del usuario y de la empresa, o del hardware.

Establecimiento de políticas de seguridad antes de desplegar CSS

En los requisitos de seguridad y autenticación intervendrán varias partes de su organización. Aunque las personas con acceso de administrador pueden realizar cambios en las políticas y "pasarlas" a los sistemas clientes (consulte el Capítulo 8, "Despliegue remoto de archivos de políticas de seguridad nuevos o revisados", en la página 59), se obtiene mejores resultados si se configuran los valores de las

políticas antes del despliegue. Para obtener información adicional sobre el establecimiento de políticas, consulte "Trabajo con la política de UVM" en el manual *Guía del administrador de Client Security Software*.

Preparación para las frases de paso olvidadas o el mal funcionamiento de dispositivos de autenticación

Inevitablemente, los usuarios olvidarán una frase de paso, y existe la posibilidad que los dispositivos de autenticación, como los dispositivos biométricos de lectura de huellas o las smart cards, no funcionen correctamente.

Frase de paso olvidada: La frase de paso del usuario no se almacena de forma legible en ninguna parte del disco duro del cliente ni en el chip de seguridad incorporado. Sólo está segura en la memoria del usuario y en otra ubicación: el archivo protegido por el par de claves del administrador. El administrador necesitará descifrar la información del usuario contenida en el archivador, utilizando la clave privada del administrador. A continuación el administrador puede suministrar una nueva frase de paso al usuario.

Cuando el usuario cambia la frase de paso, la nueva información se archivará en la ubicación específica del archivador.

En caso de que de mal funcionamiento un dispositivo de autenticación, puede configurar IBM Client Security Software para que presente un botón **Pulsar aquí para cancelar**. Al pulsar el botón de cancelación, únicamente se indica al usuario que escriba la frase de paso correctamente. A continuación el usuario puede llevar a cabo tareas seguras.

Para configurar CSS de forma que muestre el botón de cancelación, haga lo siguiente:

1. En el archivo CSEC.INI (situado en el directorio raíz), localice la entrada `AllowBypass= 0`. El valor por omisión, `0`, indica a CSS que oculte el botón de cancelación.
2. Establezca el valor de `AllowBypass` en 1. El botón de cancelación aparecerá cuando la ventana de CSS indique al usuario que proporciona autenticación además de la frase de paso.
3. Guarde el archivo CSEC.INI.

Notas:

1. Para conservar archivada esta información, es esencial que se especifique la ubicación del archivador en la entrada `kal=c:\jgk\archive` del archivo CSEC.INI. Además, si c:\jgk\archive es una unidad de red, esa unidad debe correlacionarse en el sistema cliente para archivar la frase de paso.
2. Si no especifica una ubicación para el archivador y esa ubicación no se correlaciona con el sistema cliente, no se podrán recuperar las frases de paso.

Inicialización del usuario

IBM ESS proporciona la posibilidad de que varios usuarios lleven a cabo transacciones independientes y seguras en un solo sistema. Estos usuarios deben tener asociada una frase de paso y pueden tener otros elementos de autenticación, como huellas dactilares y/o smart cards. Esto se conoce como *Autorización de factor múltiple*. La inicialización del usuario es un paso crítico en la configuración de los sistemas cliente que utilizan IBM ESS. Tenga en cuenta que la inicialización del usuario es un proceso de dos partes:

1. Registro

2. Personalización

Registro

El registro consiste simplemente en añadir un usuario o en registrarlo con IBM Client Security System. En la Figura 21, puede ver el componente User Verification Manager (UVM) de IBM Client Security Software. UVM controla las credenciales de cada usuario e impone la política.
Un archivo de políticas, como el descrito en la Figura 21, contiene los requisitos de

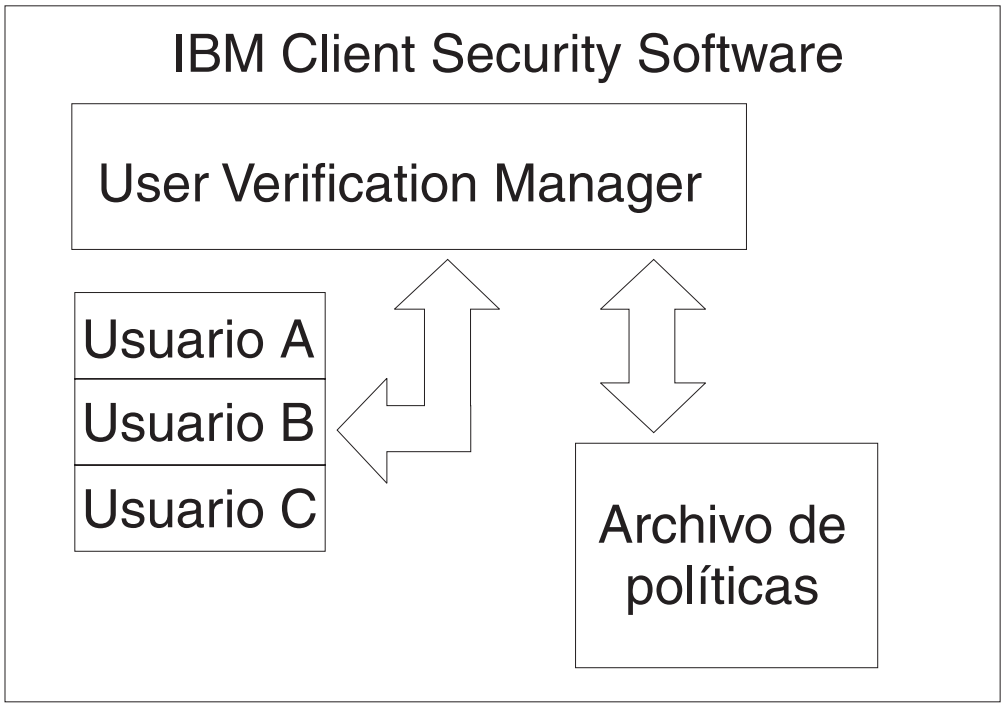

Figura 21. User Verification Manager controla las credenciales de cada usuario e impone las políticas de seguridad.

autenticación de cada usuario gestionado por UVM. Tenga en cuenta que los usuarios de UVM son simplemente usuarios de Windows (locales o de dominio). UVM gestiona las credenciales basándose en quién ha iniciado actualmente la sesión en el sistema y en el sistema operativo. Por ejemplo, si el Usuario A inicia la sesión en Windows y el Usuario A también forma parte de UVM, UVM impone la política cuando el Usuario A intenta realizar operaciones que requieren credenciales. En otro ejemplo, el Usuario A inicia la sesión en el sistema. El Usuario A entra en Microsoft Outlook y envía un correo electrónico firmado digitalmente. La clave privada utilizada para enviar el correo firmado digitalmente está protegida en IBM Embedded Security Subsystem. Antes de que UVM permita realizar la operación, impondrá la política como se ha definido en el archivo de políticas. En este ejemplo, el requisito es autenticar una frase de paso antes de realizar la operación. UVM solicitará al usuario la frase de paso y si se verifica correctamente se llevará a cabo la operación de la clave privada en el chip.

Inicialización personal

La inicialización personal es simplemente establecer una frase de paso de UVM personal del individuo. Diferentes personas pueden llevar a cabo las distintas partes del proceso. La frase de paso de UVM del individuo sólo deberá conocerla el individuo. Sin embargo, si algún individuo no realiza el proceso de inicialización podría tener que realizar un paso adicional. UVM también se puede configurar para obligar al usuario a cambiar la frase de paso la primera vez que inicie la sesión.

Por ejemplo, el administrador de TI inicializa al Usuario A. El administrador de TI selecciona al Usuario A en una lista de usuarios de Windows (de un dominio por ejemplo). UVM solicita que la frase de paso de UVM esté asociada con el Usuario A. El administrador de TI entre un ″valor por omisión″ de ″Frase de paso del administrador de TI″. Para garantizar la seguridad del sistema, después de que el Usuario A recibe el sistema debe personalizar la frase de paso para que nadie pueda llevar a cabo transacciones seguras utilizando la frase de paso por omisión.

Tabla 5. Métodos de inicialización de usuario

Método	Proceso de mandatos	Requisitos del proceso
Manual	El administrador puede personalizar manualmente CSS para el usuario mediante Administration Utility	El administrador debe estar presente en cada sistema para su configuración.
Archivo de configuración del administrador	El administrador puede crear un archivo de configuración, que contiene una versión cifrada de la contraseña del administrador. El archivo se envía al usuario, quien a continuación se inscribe individualmente sin la intervención ni la presencia del administrador.	El usuario pasa por el proceso de configuración.
*.ini	El administrador crea un script que ejecuta el archivo .ini y pone una contraseña por omisión o personalizada.	La presencia del administrador o del usuario es opcional.

Escenarios de despliegue

Imagine que va a desplegar 1.000 clientes a 1.000 usuarios finales. Una de las afirmaciones siguientes podría describir su planteamiento de despliegue:

- Sabe exactamente qué máquina corresponde a cada usuario final. Por ejemplo, sabe que la máquina 1 es para Roberto, así que registra a Roberto en la máquina 1. Roberto debe personalizar (establecer su frase de paso individual) cuando reciba el sistema. Roberto recibe el sistema, inicia IBM Client Security Software, y después establece su frase de paso.
- No sabe qué máquina corresponde a cada usuario. Envía el cliente 1 al usuario final X.

Estos dos factores variables hacen que el despliegue de IBM ESS sea diferente al despliegue de una aplicación típica. Sin embargo, existen varias opciones de despliegue que proporcionan flexibilidad para desplegar IBM ESS.

Un diagrama de flujo típico de entrega de los PC de su empresa podría ser similar al siguiente:

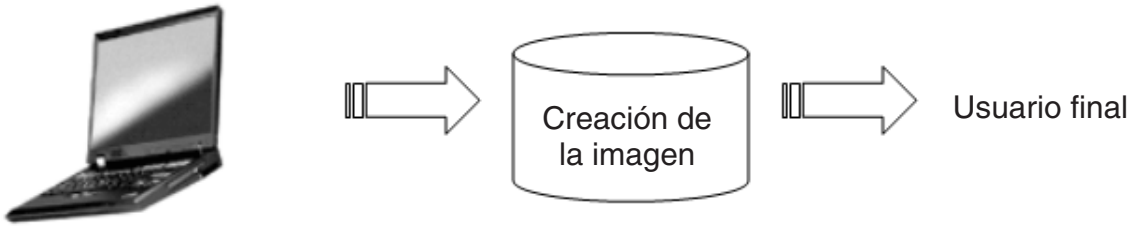

Figura 22. Diagrama de flujo típico de despliegue de los PC

Seis escenarios de despliegue

Existen seis métodos de despliegue de IBM Client Security Software:

1. **Componente añadido** — El código de IBM Client Security Software no forma parte de la imagen del disco. Se instala, inicializa y personaliza después de desplegar los sistemas.
2. **Componente de la imagen** — El código de IBM Client Security Software forma parte de la imagen, pero no está instalado. No se ha iniciado ni la personalización de la empresa ni la personalización del usuario. Consulte la Figura 23 en la página 38.
3. **Instalación sencilla** — IBM Client Security Software está instalado y se ha personalizado para la empresa o el usuario final. Consulte la Figura 24 en la página 39.
4. **Personalización parcial** — IBM Client Security Software está instalado y se ha realizado la personalización de la empresa, pero no la del usuario. Consulte la Figura 24 en la página 39.
5. **Personalización temporal** — IBM Client Security Software está instalado y se ha realizado la personalización de la empresa y del usuario. El usuario tendrá que restablecer la frase de paso del usuario y, si es necesario, proporcionar otra información de autenticación, como exploraciones de huellas dactilares o una asociación de smart card. Consulte la Figura 25 en la página 40.
6. **Personalización completa** — IBM Client Security Software está instalado y se ha realizado la personalización de la empresa y del usuario. El administrador establece la frase de paso del usuario. Si se necesita una exploración de huella dactilar u otra autenticación, el usuario debe proporcionar esa personalización. Consulte la Figura 25 en la página 40.

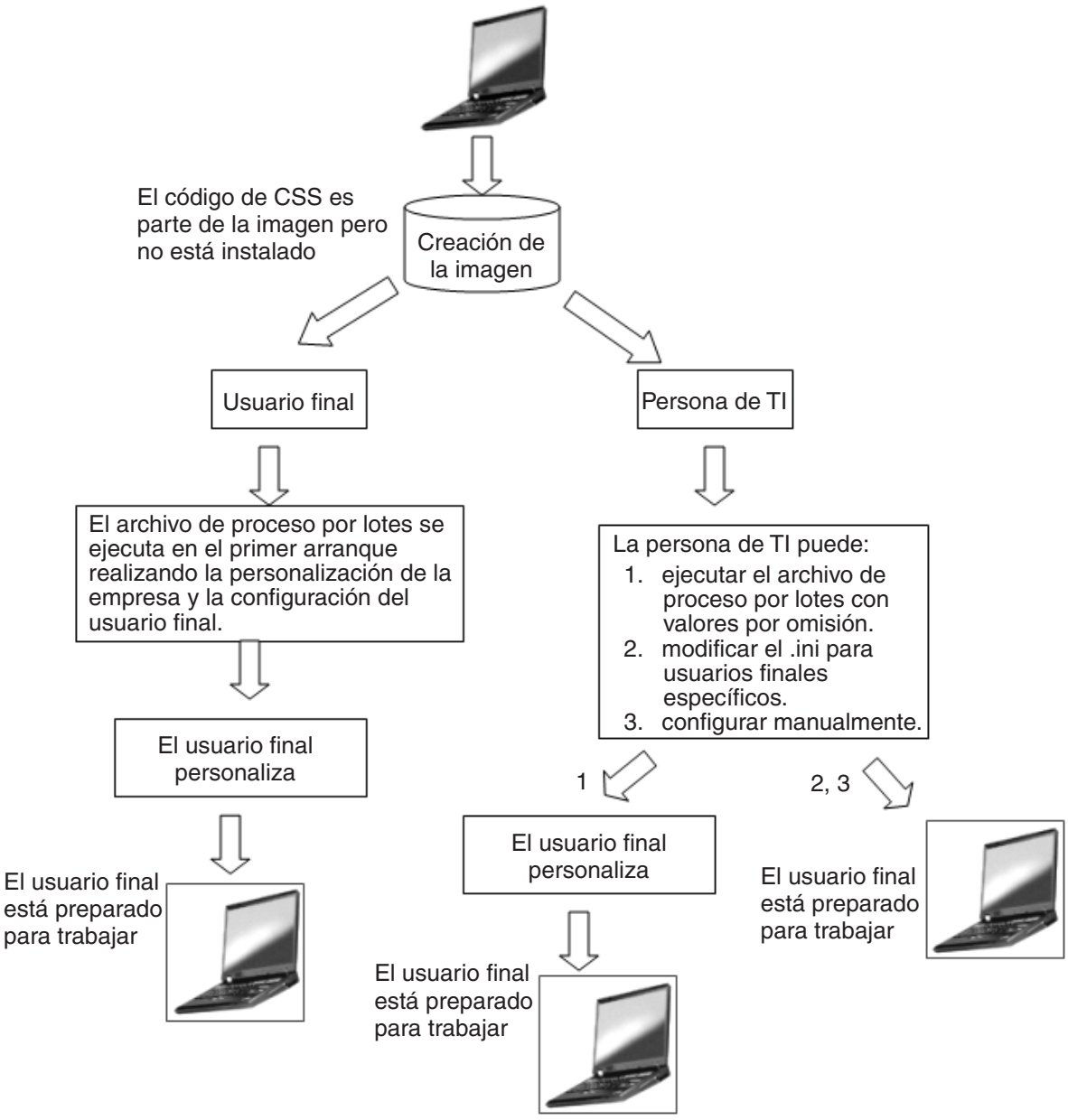

Figura 23. El código de IBM Client Security forma parte de la imagen, pero no está instalado.

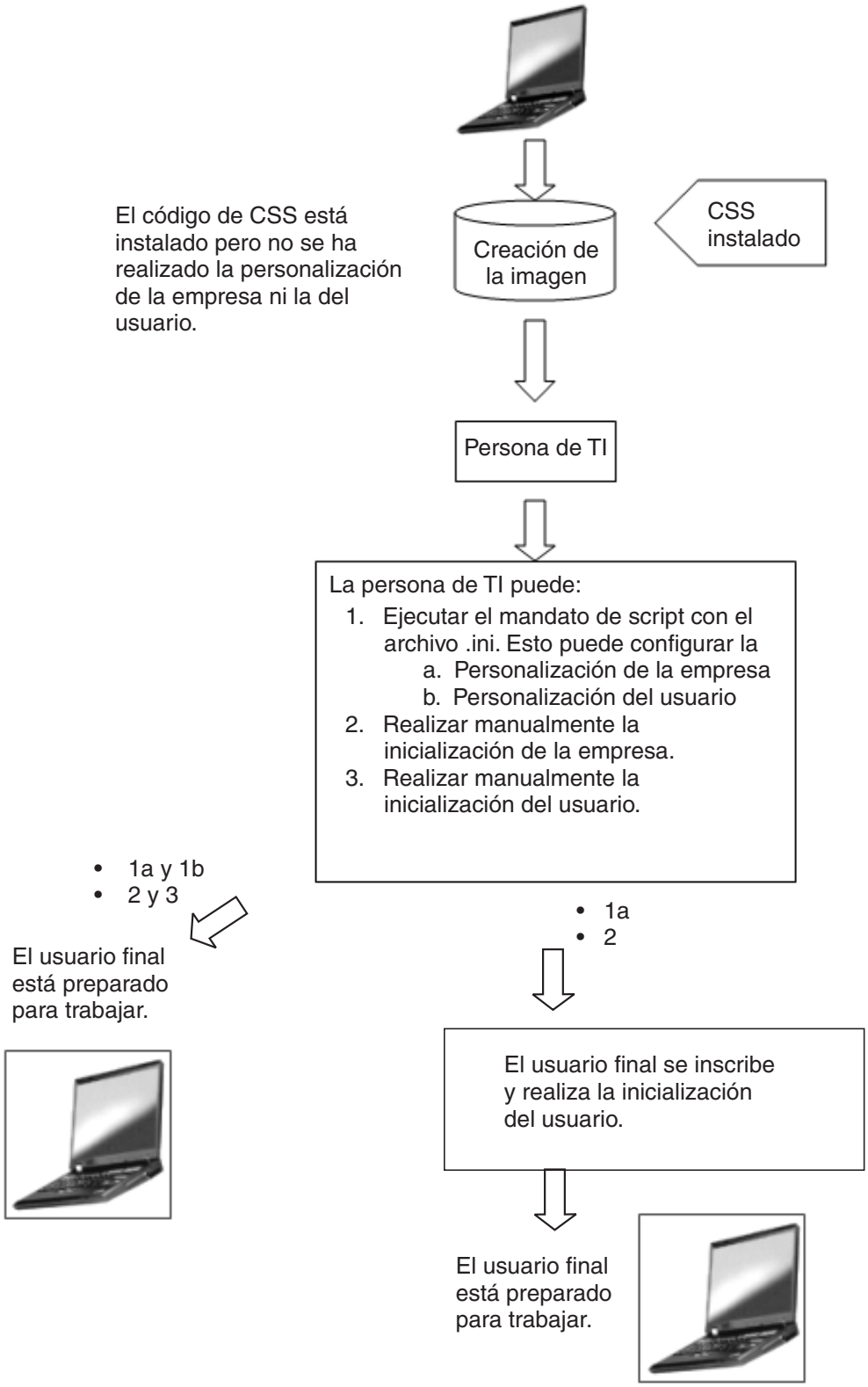

Figura 24. El código de IBM Client Security Software está instalado pero no se ha realizado la personalización de la empresa ni del usuario.

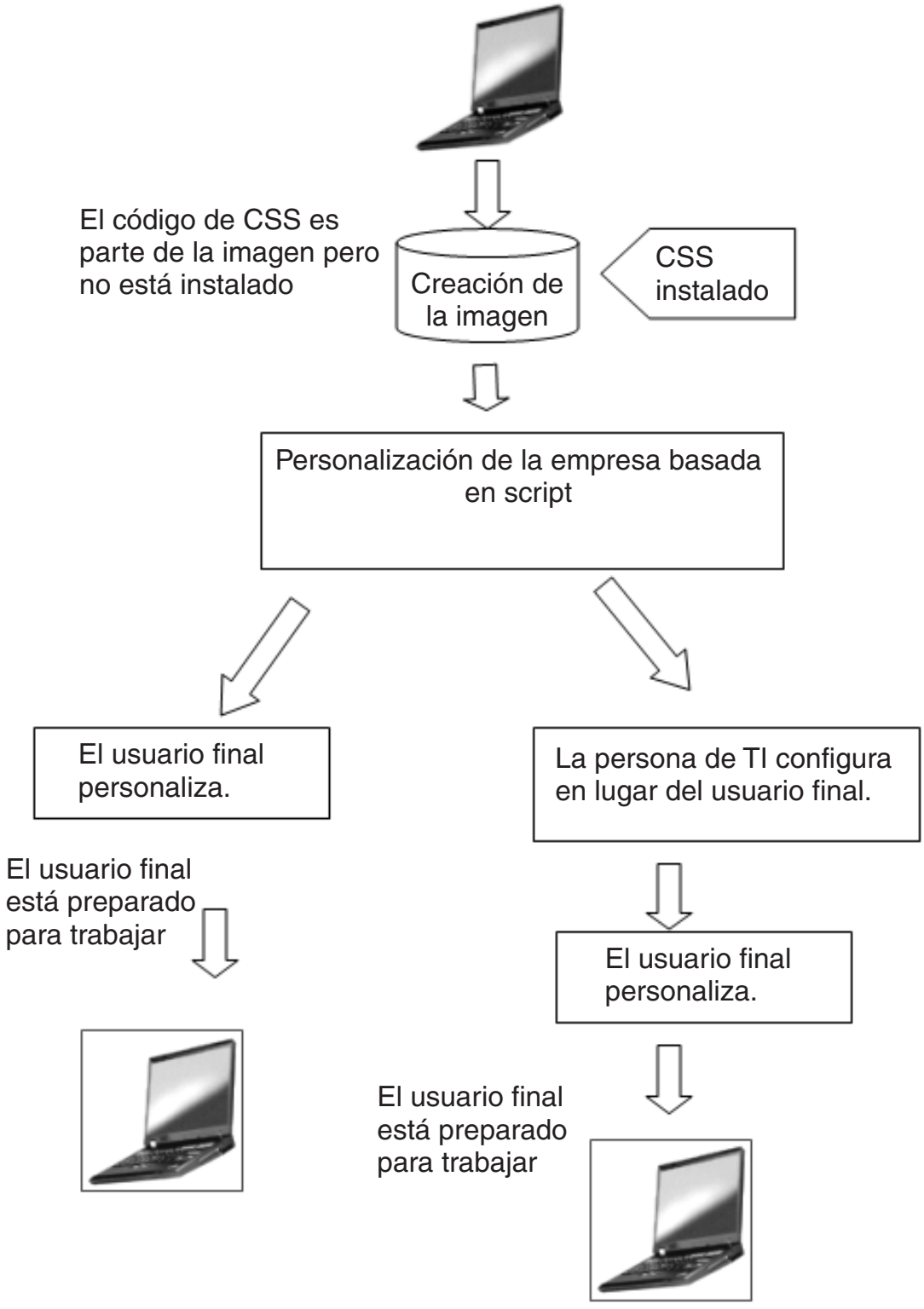

Figura 25. IBM Client Security Software está instalado y se ha realizado la personalización de la empresa y del usuario.

En el escenario 1, IBM Client Security Software se despliega después de situar la imagen del disco en el sistema. Después de instalar la imagen del disco se instala y configura IBM Client Security Software y se configura el chip Security Chip incorporado.

Los escenarios 2-6 representan diversas opciones de despliegue y configuración del software y de configuración del chip. Dependiendo de sus necesidades y del entorno, puede seleccionar el escenario y el método de instalación que mejor cumpla sus requisitos.

Detalles del archivo de configuración

Puede crear el archivo CSEC.INI utilizando el Asistente de Client Security: CSECWIZ.EXE en el directorio Security. Después de completar el asistente, seleccione el recuadro de selección situado junto a **Guardar los valores, pero no configurar el subsistema. (Los valores se guardarán en C:\CSEC.INI)**.

Configuración

El archivo cscc.ini es esencial cuando se inicia una configuración masiva. El archivo puede tener cualquier nombre siempre que su extensión sea .ini. La lista siguiente detalla los valores y sus explicaciones para el archivo .ini que debe crear. Antes de que pueda abrir y revisar el archivo CSEC.INI, deberá descifrarlo utilizando CONSOLE.EXE de la carpeta Security.

Tabla 6. Valores de configuración de Client Security System

[CSSSetup]	Cabecera de la sección para la configuración de CSS.
suppw=bootup	Contraseña del BIOS del administrador/supervisor. Déjela en blanco si no es necesaria.
hwpw=11111111	Contraseña del hardware de CSS. Debe tener ocho caracteres. Es siempre necesaria. Debe ser correcta si ya se ha establecido una contraseña de hardware.
newkp=1	1 para generar un nuevo par de claves del administrador 0 para utilizar un par de claves del administrador ya existente.
keysplit=1	Cuando newkp es 1, este parámetro determina el número de componentes de la clave privada. **Nota:** Si el par de claves existente utiliza varias partes de la clave privada, todas deben almacenarse en el mismo directorio.
kpl=c:\jgk	Ubicación del par de claves del administrador cuando newkp es 1, si es una unidad de red debe estar correlacionada.
kal=c:\jgk\archive	Ubicación del archivo de claves del usuario, si es una unidad de red debe estar correlacionada.
pub=c:\jk\admin.key	Ubicación de la clave pública del administrador cuando se utiliza un par de claves del administrador ya existente, si es una unidad de red debe estar correlacionada.
pri=c:\jk\private1.key	Ubicación de la clave privada del administrador cuando se utiliza un par de claves del administrador ya existente, si es una unidad de red debe estar correlacionada.
wiz=0	Determina si el asistente de configuración de CSS ha generado este archivo. Esta entrada no es necesaria. Si la incluye en el archivo el valor debe ser 0.
clean=0	1 para suprimir el archivo .ini después de la inicialización, 0 para conservar el archivo .ini después de la inicialización.

Tabla 6. Valores de configuración de Client Security System (continuación)

enableroaming=1	1 para habilitar la itinerancia del cliente, 0 para inhabilitar la itinerancia del cliente.
username= [promptcurrent]	[promptcurrent] para solicitar al usuario actual la contraseña de registro del sistema. [current] cuando la contraseña de registro del sistema del usuario actual la proporciona la entrada sysregpwd y el usuario actual tiene autorización para registrar el sistema en el servidor de itinerancia. [<cuenta específica del usuario>] si el usuario designado tiene autorización para registrar el sistema en el servidor de itinerancia y si la contraseña de registro del sistema del usuario se proporciona en la entrada sysregpwd. No utilice esta entrada si el valor de enableroaming es 0 o si la entrada enableroaming no está presente.
sysregpwd=12345678	Contraseña de registro del sistema. Establezca este valor con la contraseña correcta para permitir que el sistema se registre en el servidor de itinerancia. No incluya esta entrada si el valor de username está establecido como [promptcurrent] o si la entrada username no está presente.
[UVMEnrollment]	Cabecera de la sección para la inscripción de usuarios.
enrollall=0	1 para inscribir todas las cuentas de usuarios locales en UVM, 0 para inscribir cuentas de usuarios específicos en UVM.
defaultuvmpw=top	Cuando enrollall es 1, esta será la frase de paso de UVM para todos los usuarios.
defaultwinpw=down	Cuando enrollall es 1, esta será la contraseña de Windows registrada en UVM para todos los usuarios.
defaultppchange=0	Cuando enrollall es 1, se establecerá la política de cambio de frase de paso de UVM para todos los usuarios. 1 para solicitar al usuario que cambie la frase de paso de UVM en el próximo inicio de sesión, 0 para no solicitar al usuario que cambie la frase de paso de UVM en el próximo inicio de sesión.
defaultppexppolicy=1	Cuando enrollall es 1, se establecerá la política de caducidad de frase de paso de UVM para todos los usuarios. 0 para indicar que la frase de paso de UVM caduca 1 para indicar que la frase de paso de UVM no caduca
defaultppexpdays=0	Cuando enrollall es 1, se establecerá el número de días en que caduca la frase de paso de UVM para todos los usuarios. Cuando ppexppolicy se establece en 0, establezca este valor para establecer el número de días en que caduca la frase de paso de UVM.
enrollusers=*x*, donde x es el número total de usuarios que inscribirá en el sistema.	El valor de esta sentencia especifica el número total de usuarios que inscribirá. Cuando enrollall es 0, este es el número de usuarios que se inscribirán en UVM.

Tabla 6. Valores de configuración de Client Security System (continuación)

user1=jknox	Proporciona la información para inscribir a cada usuario comenzando por el usuario 1. No hay usuario 0. Los nombres de usuario deben ser nombres de cuenta. Para obtener el nombre de cuenta real en XP, haga lo siguiente 1. Inicie Administración de equipos (Administrador de dispositivos). 2. Expanda el nodo Usuarios locales y grupos. 3. Abra la carpeta Usuarios. Los elementos listados en la columna Nombre son los nombres de cuenta.
user1uvmpw=chrome	Especifica la frase de paso de UVM para el usuario 1 de UVM.
user1winpw=spinning	Especifica la frase de paso de Windows para registrar el usuario 1 en UVM.
user1domain=0	Especifica si la cuenta del usuario 1 es local en está en un dominio. 0 para indicar que esta cuenta es local, 1 para indicar que esta cuenta está en el dominio.
user1ppchange=0	Especifica si el usuario 1 tiene que cambiar la frase de paso de UVM en el próximo inicio de sesión. 1 para solicitar al usuario que cambie la frase de paso de UVM en el próximo inicio de sesión, 0 para no solicitar al usuario que cambie la frase de paso de UVM en el próximo inicio de sesión.
user1ppexppolicy=1	Especifica si la frase de paso de UVM del usuario 1 caduca. 0 para indicar que la frase de paso de UVM caduca. 1 para indicar que la frase de paso de UVM no caduca.
user1ppexpdays=0	Si user1ppexppolicy=0, establezca este valor para indicar el número de días en que caduca la fase de paso de UVM.
Proporcione para cada usuario un conjunto completo de valores de configuración en el orden especificado en la parte sombreada de la tabla. Proporcione todos los parámetros para un usuario y después proporcione los parámetros para el siguiente usuario. Si por ejemplo enrollusers se ha establecido en 2, debería añadir el grupo siguiente de valores de configuración.	
user2=chrome	
user2uvmpw=left	
user2winpw=right	
user2domain=0	
user2ppchange=1	
user2ppexppolicy=0	
user2ppexpdays=90	
[UVMAppConfig]	Cabecera de la sección para la configuración de aplicaciones y módulos preparados para UVM.
uvmlogon=0	1 para utilizar la protección de inicio de sesión de UVM, 0 para utilizar el inicio de sesión de Windows.
entrust=0	1 para utilizar UVM para la autenticación de Entrust, 0 para utilizar la autenticación de Entrust.
notes=1	1 para utilizar la protección de UVM para Lotus Notes, 0 para utilizar la protección de contraseña de Notes.

Tabla 6. Valores de configuración de Client Security System (continuación)

netscape=0	1 para firmar y cifrar correos electrónicos con el módulo IBM PKCS#11, 0 para no firmar ni cifrar correos electrónicos con el módulo IBM PKCS#11.
passman=0	1 para utilizar Password Manager, 0 para no utilizar Password Manager
folderprotect=0	1 para utilizar Cifrado de archivos y carpetas, 0 para no utilizar Cifrado de archivos y carpetas.

Notas:

1. A medida que IBM Client Security Software se mejore y actualice, los parámetros de *.ini pueden cambiar.
2. Si algún archivo o vía de acceso está en una unidad de red, la unidad debe estar correlacionada con una letra de unidad.
3. Debe descifrarse el archivo CSEC.ini para que el software cargue los contenidos. Debe descifrarse con CONSOLE.EXE, en el directorio Security. También se puede utilizar el mandato siguiente para cifrar un archivo INI con un script. (Son necesarias las comillas para los nombres de vía de acceso largos): *carpeta de instalación de CSS*\console.exe /q /ini: *vía de acceso completa a un archivo ini sin cifrar*
4. El mandato siguiente ejecuta el archivo .ini desde la línea de mandatos cuando la configuración masiva no se realiza junto con la instalación masiva:

   carpeta de instalación de CSS\acamucli /ccf:c:\csec.ini
5. Se pueden añadir nuevos usuarios al archivo INI después de que el subsistema esté configurado, lo que resulta útil para realizar la inscripción del usuario. Ejecute un archivo INI como se ha descrito anteriormente, pero no incluya los valores ″pub=″ ni ″pri=″. El código asumirá que se trata sólo de una inscripción de usuario y no reinicializará el subsistema.

IBM Client Security Software le permite ejecutar el archivo CSEC.INI una segunda vez sin afectar a la instalación actual de Client Security Software. Podría ejecutar este archivo una segunda vez para inscribir usuarios adicionales, por ejemplo.

Tabla 7. Valores de configuración de Client Security System al ejecutar por segunda vez

[CSSSetup]	Cabecera de la sección para la configuración de CSS.
suppw=	Contraseña del BIOS del administrador/supervisor. Déjela en blanco si no es necesaria.
hwpw=11111111	Contraseña del hardware de CSS. Debe tener ocho caracteres. Es siempre necesaria. Debe ser correcta si ya se ha establecido una contraseña de hardware.
newkp=0	Entre 0 para utilizar un par de claves del administrador ya existente.
keysplit=1	Cuando newkp es 1, este parámetro determina el número de componentes de la clave privada. **Nota:** Si el par de claves existente utiliza varias partes de la clave privada, todas deben almacenarse en el mismo directorio.
pub=	Dejar en blanco
pri=	Dejar en blanco
kal=c:\archive	Ubicación del archivo de claves del usuario, si es una unidad de red debe estar correlacionada.

Tabla 7. Valores de configuración de Client Security System al ejecutar por segunda vez (continuación)

wiz=0	Determina si el asistente de configuración de CSS ha generado este archivo. Esta entrada no es necesaria. Si la incluye en el archivo el valor debe ser 0.
clean=0	Entre 0 para conservar el archivo .ini después de la inicialización.
enableroaming=0	Entre 0 para inhabilitar la itinerancia del cliente.
[UVMEnrollment]	Cabecera de la sección para la inscripción de usuarios.
enrollall=0	1 para inscribir todas las cuentas de usuarios locales en UVM, 0 para inscribir cuentas de usuarios específicos en UVM.
enrollusers=1	El valor de esta sentencia especifica el número total de usuarios que inscribirá.
user1=*eddy*	Es el nombre del nuevo usuario que se va a inscribir.
user1uvmpw=pass1word	Especifica la frase de paso de UVM para el usuario 1 de UVM.
user1winpw=	Especifica la frase de paso de Windows para registrar el usuario 1 en UVM.
user1domain=0	Especifica si la cuenta del usuario 1 es local en está en un dominio. 0 para indicar que esta cuenta es local, 1 para indicar que esta cuenta está en el dominio.
user1ppchange=0	Especifica si el usuario 1 tiene que cambiar la frase de paso de UVM en el próximo inicio de sesión. 1 para solicitar al usuario que cambie la frase de paso de UVM en el próximo inicio de sesión, 0 para no solicitar al usuario que cambie la frase de paso de UVM en el próximo inicio de sesión.
user1ppexppolicy=1	Especifica si la frase de paso de UVM del usuario 1 caduca. 0 para indicar que la frase de paso de UVM caduca. 1 para indicar que la frase de paso de UVM no caduca.
user1ppexpdays=0	Si user1ppexppolicy=0, establezca este valor para indicar el número de días en que caduca la fase de paso de UVM.

Capítulo 6. Instalación del componente Client Security en un servidor Tivoli Access Manager

La autenticación de los usuarios finales en el nivel del cliente es una cuestión de seguridad importante. Client Security Software proporciona la interfaz necesaria para gestionar la política de seguridad de un cliente de IBM. Esta interfaz forma parte del software de autenticación, User Verification Manager (UVM), que es el componente principal de Client Security Software.

La política de seguridad de UVM para un cliente de IBM puede gestionarse de dos formas:

- Localmente, utilizando un editor de política que esté en el cliente de IBM
- En toda una corporación, utilizando Tivoli Access Manager

Antes de utilizar Client Security con Tivoli Access Manager, debe estar instalado el componente Client Security de Tivoli Access Manager. Este componente se puede descargar desde el sito Web de IBM http://www.pc.ibm.com/us/security/index.html.

Requisitos previos

Antes de poder establecer una conexión segura entre el cliente de IBM y el servidor Tivoli Access Manager, deben estar instalados los componentes siguientes en el cliente de IBM:

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

Para obtener información detallada sobre la instalación y utilización de Tivoli Access Manager, consulte la documentación proporcionada en el sitio http://www.tivoli.com/products/index/secureway_policy_dir/index.htm.

Cómo bajar e instalar el componente Client Security

El componente Client Security está disponible para bajarlo gratuitamente del sitio Web de IBM.

Para bajar e instalar el componente Client Security en el servidor Tivoli Access Manager y el cliente de IBM, complete el procedimiento siguiente:

1. Utilizando la información del sitio Web, compruebe si su máquina tiene instalado el chip IBM Security Chip integrado; para ello busque su número de modelo en la tabla de requisitos del sistema; después pulse **Continue** (Continuar).
2. Seleccione el botón de selección que se corresponda con su tipo de máquina y pulse **Continue** (Continuar).
3. Cree un ID de usuario, regístrese con IBM rellenando el formulario en línea y revise el Acuerdo de licencia; después pulse **Accept Licence** (Acepto la licencia).

   Se le redirigirá automáticamente a la página para bajarse Client Security.

4. Siga los pasos de esta página para instalar todos los controladores de dispositivo necesarios, los archivos readme, el software, los documentos de referencia y los programas de utilidad adicionales.
5. Instale Client Security Software completando el procedimiento siguiente:
   a. En el escritorio de Windows, pulse **Inicio > Ejecutar**.
   b. En el campo Ejecutar, escriba `d:\directorio\csec53.exe`, donde d:\directorio\ es la letra de la unidad y el directorio donde se encuentra el archivo.
   c. Pulse **Aceptar**.

      Se abre la ventana Bienvenido al Asistente de InstallShield para IBM Client Security Software.
   d. Pulse **Siguiente**.

      El asistente extraerá los archivos e instalará el software. Cuando se haya completado la instalación, se le dará la opción de reiniciar el sistema en ese momento o hacerlo más tarde.
   e. Seleccione el botón de selección adecuado y pulse **Aceptar**.
6. Cuando se reinicie el sistema, en el escritorio de Windows, pulse **Inicio > Ejecutar**.
7. En el campo Ejecutar, escriba *d:*`\`*directorio*`\TAMCSS.exe`, donde *d:\directorio* es la letra de la unidad y el directorio donde se encuentra el archivo, o pulse **Examinar** para localizar el archivo.
8. Pulse **Aceptar**.
9. Especifique una carpeta de destino y pulse **Unzip** (Descomprimir).

   El asistente extraerá los archivos en la carpeta especificada. Un mensaje indica si los archivos se han descomprimido satisfactoriamente.
10. Pulse **Aceptar**.

Adición de componentes Client Security en el servidor Tivoli Access Manager

El programa de utilidad pdadmin es una herramienta de línea de mandatos que el administrador puede utilizar para efectuar la mayoría de las tareas de administración de Tivoli Access Manager. La ejecución de varios mandatos permite al administrador utilizar un archivo que contenga varios mandatos de pdadmin para efectuar una tarea completa o una serie de tareas. La comunicación entre el programa de utilidad pdadmin y Management Server (pdmgrd) está protegida sobre SSL. El programa de utilidad pdadmin se instala como parte del paquete Tivoli Access Manager Runtime Environment (PDRTE).

El programa de utilidad pdadmin acepta un argumento de nombre de archivo que identifique la ubicación de tal archivo, por ejemplo:

```
MSDOS>pdadmin [-a usuario-admin][-p contraseña]nombrevía-archivo
```

El mandato siguiente es un ejemplo de cómo crear el espacio de objetos IBM Solutions, las acciones de Client Security y las entradas ACL individuales en el servidor Tivoli Access Manager:

```
MSDOS>pdadmin -a director_seg -p contraseña C:\TAM_Add_ClientSecurity.txt
```

Consulte el manual *Tivoli Access Manager Base Administrator Guide* para obtener más información sobre el programa de utilidad pdadmin y su sintaxis de mandatos.

Establecimiento de una conexión segura entre el cliente de IBM y el servidor Tivoli Access Manager

El cliente de IBM debe establecer su propia identidad autenticada dentro del dominio seguro de Tivoli Access Manager para solicitar decisiones de autorización del Servicio de autorización de Tivoli Access Manager.

Se debe crear una identidad exclusiva para la aplicación en el dominio seguro de Tivoli Access Manager. Para que la identidad autenticada efectúe las comprobaciones de autenticación, la aplicación debe ser miembro del grupo remote-acl-users. Cuando la aplicación desee contactar con uno de los servicios del dominio seguro, primero debe iniciar una sesión en éste.

El programa de utilidad svrsslcfg permite a las aplicaciones IBM Client Security comunicarse con Tivoli Access Manager Management Server y Authorization Server.

El programa de utilidad svrsslcfg permite a las aplicaciones IBM Client Security comunicarse con el servidor Tivoli Access Manager Management y el servidor de autorización.

El programa de utilidad svrsslcfg efectúa las tareas siguientes:

- Crea una identidad de usuario para la aplicación. Por ejemplo, UsuarioDemo/NOMBRESISTPPAL
- Crea un archivo de claves de SSL para ese usuario. Por ejemplo, UsuarioDemo.kdb y UsuarioDemo.sth
- Añade el usuario al grupo remote-acl-users

Se necesitan los parámetros siguientes:

- **-f archivo_cfg**: vía de acceso y nombre del archivo de configuración, utilice TAMCSS.conf
- **-d dir_bdc**: el directorio que contiene los archivos de la base de datos del conjunto de claves para el servidor.
- **-n nombre_servidor**: el nombre de usuario de Windows/UVM real del usuario que va a ser el cliente de IBM.
- **-P contraseña_admin**: la contraseña del administrador de Tivoli Access Manager.
- **-s tipo_servidor**: debe especificarse como ″remote″.
- **-S contraseña_servidor**: la contraseña para el usuario recién creado. Este parámetro es necesario.
- **-r núm_puerto**: establece el número de puerto de escucha para el cliente de IBM. Este es el parámetro especificado en la variable de puerto del servidor SSL para Tivoli Access Manager Management Server de Tivoli Access Manager Runtime.
- **-e duración_contraseña**: establece el período de caducidad de la contraseña en número de días.

Para establecer una conexión segura entre el cliente de IBM y el servidor Tivoli Access Manager, complete el procedimiento siguiente:

1. Cree un directorio y mueva el archivo TAMCSS.conf al directorio nuevo.

   Por ejemplo, `MSDOS> mkdir C:\TAMCSS MSDOS> move C:\TAMCSS.conf C:\TAMCSS\`
2. Ejecute svrsslcfg para crear el usuario.

MSDOS> svrsslcfg -config -f C:\TAMCSS\TAMCSS.conf -d C:\TAMCSS\ -n <nombre_servidor> - s remote -S <contraseña_servidor> -P <contraseña_admin> -e 365 -r 199

Nota: sustituya <nombre_servidor> por el nombre de usuario de UVM y el nombre de sistema principal del cliente de IBM. Por ejemplo: –n UsuarioDemo/MiNombreSistPpal. El nombre de sistema principal del cliente de IBM puede averiguarse escribiendo "hostname" en el indicador de MSDOS. El programa de utilidad svrsslcfg creará una entrada válida en el servidor Tivoli Access Manager y proporcionará un archivo de claves SSL exclusivo para la comunicación cifrada.

3. Ejecute svrsslcfg para añadir la ubicación de ivacld al archivo TAMCSS.conf.

   Por omisión, PD Authorization Server escucha en el puerto 7136. Esto puede verificarse mirando el parámetro tcp_req_port en la sección ivacld del archivo ivacld.conf en el servidor Tivoli Access Manager. Es importante que obtenga el nombre de sistema principal correcto de ivacld. Utilice el mandato pdadmin server list para obtener esta información. Los servidores se denominan: **nombre_servidor- nombre_sistppal**. A continuación se incluye un ejemplo de ejecución de pdadmin server list:

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

Después se utiliza el mandato siguiente para añadir una entrada de duplicación para el servidor ivacld mostrado abajo. Se asume que ivacld escucha en el puerto por omisión 7136.

```
svrsslcfg -add_replica  -f vía acceso archivo config -h nombre_sistppal
MSDOS>svrsslcfg -add_replica  -f C:\TAMCSS\TAMCSS.conf -h
MiSistPpal.ibm.com
```

Configuración de los clientes de IBM

Antes de poder utilizar Tivoli Access Manager para controlar los objetos de autenticación para los clientes de IBM, debe configurar cada cliente mediante Administrator Utility, un componente que se proporciona con Client Security Software. Esta sección contiene los requisitos previos y las instrucciones para configurar los clientes de IBM.

Requisitos previos

Asegúrese de que se instala el software siguiente en el cliente de IBM en el orden siguiente:

1. **Sistema operativo Microsoft Windows soportado.** Puede utilizar Tivoli Access Manager para controlar los registros de autenticación para los clientes de IBM que tengan Windows XP, Windows 2000 o Windows NT Workstation 4.0.
2. **Client Security Software versión 3.0 o posterior.** Después de instalar el software y habilitar el chip IBM Security Chip incorporado, puede utilizar Client Security Administrator Utility para configurar la autenticación de usuarios y editar la política de seguridad de UVM. Para obtener instrucciones completas sobre la instalación y utilización de Client Security Software, consulte la *Guía de instalación de Client Security Software* y la *Guía del administrador de Client Security Software*.

Definición de la información de configuración de Tivoli Access Manager

Después de haber instalado Tivoli Access Manager en el cliente local, puede definir la información de configuración de Access Manager mediante Administrator Utility, un componente de software que se proporciona con Client Security Software. La información de configuración de Access Manager consta de los valores siguientes:

- Selección de la vía de acceso completa al archivo de configuración
- Selección del intervalo de renovación de la antememoria local

Para definir la información de configuración de Tivoli Access Manager en el cliente de IBM, complete el procedimiento siguiente:

1. Pulse **Inicio > Configuración > Panel de control > IBM Client Security Subsystem**
2. Escriba la contraseña del administrador y pulse **Aceptar**.

   Después de entrar la contraseña, se abrirá la ventana principal de Administrator Utility.
3. Pulse el botón **Configurar soporte de aplicaciones y políticas**.

   Se mostrará la pantalla Configuración de aplicaciones y políticas de UVM.
4. Pulse el recuadro de selección **Sustituir el inicio de sesión estándar de Windows con el inicio de sesión seguro de UVM**.
5. Pulse el botón **Política de aplicaciones**.
6. En el área Información de configuración de Tivoli Access Manager, seleccione la vía de acceso completa al archivo de configuración TAMCSS.conf. Por ejemplo, `C:\TAMCSS\TAMCSS.conf`

   Tivoli Access Manager debe estar instalado en el cliente para que esta área esté disponible.
7. Pulse el botón **Editar política**.

   Se muestra la pantalla Entre la contraseña del administrador.
8. Escriba la contraseña del administrador en el campo proporcionado y pulse **Aceptar**.

   Se muestra la pantalla Política de IBM UVM.
9. Seleccione las acciones que desea que controle Tivoli Access Manager en el menú desplegable Acciones.
10. Seleccione el recuadro de selección Access Manager controla el objeto seleccionado para que aparezca una marca de selección en él.
11. Pulse el botón **Aplicar**.

    Estos cambios tendrán lugar en la próxima renovación de la antememoria. Si desea que los cambios tengan lugar inmediatamente, pulse el botón **Renovar antememoria local**.

Establecimiento y utilización de la característica de antememoria local

Después de seleccionar el archivo de configuración de Tivoli Access Manager, puede establecerse el intervalo de renovación de la antememoria local. En el cliente de IBM se mantiene una duplicación local de la información de política de seguridad gestionada por Tivoli Access Manager. Puede planificar una renovación automática de la antememoria local en incrementos de meses (0-12) o días (0-30).

Para establecer o renovar la antememoria local, complete el procedimiento siguiente:

1. Pulse **Inicio > Configuración > Panel de control > IBM Client Security Subsystem**
2. Escriba la contraseña del administrador y pulse **Aceptar**.

   Se abre la ventana Administrator Utility. Para obtener información completa sobre la utilización de Administrator Utility, consulte la *Guía del administrador de Client Security Software*.
3. En Administrator Utility, pulse el botón **Configurar soporte de aplicaciones y políticas** y después pulse el botón **Política de aplicaciones**.

   Se mostrará la pantalla Modificar la configuración de políticas de Client Security.
4. Efectúe una de las acciones siguientes:
   - Para renovar la antememoria local ahora, pulse **Renovar antememoria local**.
   - Para establecer la cadencia de renovación automática, escriba el número de meses (0-12) y días (0-30) en los campos proporcionados y pulse **Renovar antememoria local**. Se renovará la antememoria local y se actualizará la fecha de caducidad del archivo para indicar la fecha en la que se efectuará la próxima renovación automática.

Habilitación de Tivoli Access Manager para controlar los objetos del cliente de IBM

La política de UVM se controla mediante un archivo de políticas globales. El archivo de políticas globales, llamado archivo de políticas de UVM, contiene requisitos de autenticación para acciones que se efectúan en el sistema cliente de IBM, como iniciar una sesión en el sistema, quitar el protector de pantalla o firmar los mensajes de correo electrónico.

Antes de poder habilitar Tivoli Access Manager para controlar los objetos de autenticación para un cliente de IBM, utilice el editor de política de UVM para editar el archivo de políticas de UVM. El editor de política de UVM forma parte de Administrator Utility.

Importante: si se habilita Tivoli Access Manager para que controle un objeto, se da el control del objeto al espacio de objetos de Tivoli Access Manager. Si lo hace, deberá reinstalar Client Security Software para volver a establecer el control local sobre ese objeto.

Edición de una política local de UVM

Antes de intentar editar la política de UVM para el cliente local, asegúrese de que hay inscrito al menos un usuario en UVM. De lo contrario, se mostrará un mensaje de error cuando el editor de política intente abrir el archivo de políticas locales.

Cuando se edita la política local de UVM sólo se utiliza en el cliente para el que se ha editado. Si ha instalado Client Security en su ubicación por omisión, la política local de UVM está almacenada como \Archivos de programa\IBM\Security\UVM_Policy\globalpolicy.gvm. Sólo los usuarios que se hayan añadido a UVM pueden utilizar el editor de política de UVM.

Nota: si establece que la política de UVM necesita huellas dactilares para un objeto de autenticación (como el inicio de sesión del sistema operativo), los usuarios que se añadan a UVM deben tener registradas sus huellas dactilares para utilizar ese objeto.

Para iniciar el editor de política de UVM, complete el procedimiento siguiente de Administrator Utility:

1. Pulse el botón **Configurar soporte de aplicaciones y políticas** y después pulse el botón **Política de aplicaciones**.

   Se mostrará la pantalla Modificar la configuración de políticas de Client Security.
2. Pulse el botón **Editar política**.

   Se muestra la pantalla Entre la contraseña del administrador.
3. Escriba la contraseña del administrador en el campo proporcionado y pulse **Aceptar**.

   Se muestra la pantalla Política de IBM UVM.
4. En la pestaña Selección de objetos, pulse **Acción** o **Tipo de objeto** y seleccione el objeto al que desea asignar requisitos de autenticación.

   Entre los ejemplos de acciones válidas se incluyen Inicio de sesión del sistema, Desbloqueo del sistema, Descifrado de correo electrónico; un ejemplo de un tipo de objeto es Obtener un certificado digital.
5. Para cada objeto que seleccione, tiene que seleccionar **Tivoli Access Manager controla el objeto seleccionado** para habilitar Tivoli Access Manager para ese objeto.

   Importante: si se habilita Tivoli Access Manager para que controle un objeto, se da el control del objeto al espacio de objetos de Tivoli Access Manager. Si posteriormente desea volver a establecer el control local sobre ese objeto, deberá reinstalar Client Security Software.

   Nota: mientras edita la política de UVM, puede ver información sobre el resumen de políticas pulsando **Resumen de políticas**.
6. Pulse **Aplicar** para guardar los cambios.
7. Pulse **Aceptar** para salir.

Edición y utilización de la política de UVM para clientes remotos

Para utilizar la política de UVM en varios clientes de IBM, edite y guarde la política de UVM para clientes remotos y después copie el archivo de políticas de UVM en otros clientes de IBM. Si instala Client Security en la ubicación por omisión, se almacenará el archivo de políticas de UVM como \Archivos de programa\IBM\Security\UVM_Policy\remote\globalpolicy.gvm.

Copie los archivos siguientes en los otros clientes de IBM remotos que vayan a utilizar esta política de UVM:

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

Si ha instalado Client Security Software en la ubicación por omisión, el directorio raíz de las vías de acceso anteriores es \Archivos de programa. Copie ambos archivos en la vía de acceso del directorio \IBM\Security\UVM_Policy\ de los clientes remotos.

Tablas de resolución de problemas

La sección siguiente contiene tablas de resolución de problemas que podrían serle útiles si experimenta problemas con Client Security Software.

Información de resolución de problemas de certificados digitales

La información de resolución de problemas siguiente podría serle útil si experimenta problemas al obtener un certificado digital.

Síntoma del problema	Posible solución
La ventana de frase de paso de UVM o la ventana de autenticación de huellas dactilares se muestran varias veces durante la petición de un certificado digital	**Acción**
La política de seguridad de UVM define que un usuario debe proporcionar la frase de paso de UVM o la autenticación de huellas dactilares antes de que se pueda obtener un certificado digital. Si el usuario intenta obtener un certificado, la ventana de autenticación que solicita la frase de paso de UVM o la exploración de huellas dactilares se muestra más de una vez.	Escriba la frase de paso de UVM o explore su huella dactilar cada vez que se abra la ventana de autenticación.
Se muestra un mensaje de error de VBScript o JavaScript	**Acción**
Cuando solicita un certificado digital, puede mostrarse un mensaje de error relacionado con VBScript o JavaScript.	Reinicie el sistema y obtenga el certificado de nuevo.

Información de resolución de problemas de Tivoli Access Manager

La información de resolución de problemas siguiente podría serle útil si experimenta problemas al utilizar Tivoli Access Manager con Client Security Software.

Síntoma del problema	Posible solución
Los valores de política local no se corresponden con los del servidor	**Acción**
Tivoli Access Manager permite ciertas configuraciones de bits que no son soportadas por UVM. En consecuencia, los requisitos de política local pueden prevalecer sobre los valores definidos por un administrador al configurar el servidor Tivoli Access Manager.	Se trata de una limitación conocida.
No se puede acceder a los valores de configuración de Tivoli Access Manager	**Acción**
No se puede acceder a la configuración de Tivoli Access Manager ni a los valores de configuración de la antememoria local en la página Configuración de política en Administrator Utility.	Instale Tivoli Access Manager Runtime Environment. Si no está instalado Runtime Environment en el cliente de IBM, no se podrá acceder a los valores de Tivoli Access Manager en la página Configuración de política.
El control de un usuario es válido tanto para el usuario como para el grupo	**Acción**

Síntoma del problema	Posible solución
Al configurar el servidor Tivoli Access Manager, si define un usuario en un grupo, el control del usuario es válido tanto para el usuario como para el grupo si está activo **Traverse bit** (Bit cruzado).	No se precisa ninguna acción.

Información de resolución de problemas de Lotus Notes

La información de resolución de problemas siguiente podría serle útil si experimenta problemas al utilizar Lotus Notes con Client Security Software.

Síntoma del problema	Posible solución
Después de habilitar la protección de UVM para Lotus Notes, Notes no puede completar su configuración	**Acción**
Lotus Notes no puede completar la configuración después de habilitar la protección de UVM utilizando Administrator Utility.	Se trata de una limitación conocida. Lotus Notes debe estar configurado y en ejecución antes de habilitar el soporte de Lotus Notes en Administrator Utility.
Se muestra un mensaje de error al intentar cambiar la contraseña de Notes	**Acción**
Si se cambia la contraseña de Notes cuando se utiliza Client Security Software, puede aparecer un mensaje de error.	Vuelva a intentar cambiar la contraseña. Si no funciona, reinicie el cliente.
Se muestra un mensaje de error después de generar aleatoriamente una contraseña	**Acción**
Puede aparecer un mensaje de error cuando hace lo siguiente: • Utiliza la herramienta Configuración de Lotus Notes para establecer la protección de UVM para un ID de Notes • Abre Notes y utiliza la función proporcionada por Notes para cambiar la contraseña para el archivo de ID de Notes • Cierra Notes inmediatamente después de cambiar la contraseña	Pulse **Aceptar** para cerrar el mensaje de error. No se precisa ninguna otra acción. Contrariamente al mensaje de error, la contraseña se ha cambiado. La contraseña nueva es una contraseña generada aleatoriamente creada por Client Security Software. El archivo de ID de Notes está cifrado ahora con la contraseña generada aleatoriamente y el usuario no necesita un archivo de ID de usuario nuevo. Si el usuario final cambia la contraseña de nuevo, UVM generará una nueva contraseña aleatoria para el ID de Notes.

Información de resolución de problemas de cifrado

La información de resolución de problemas siguiente podría serle útil si experimenta problemas al cifrar archivos utilizando Client Security Software 3.0 o posterior.

Síntoma del problema	**Posible solución**
Los archivos cifrados previamente no se descifrarán	**Acción**
Los archivos cifrados con versiones anteriores de Client Security Software no se descifran después de actualizar a Client Security Software 3.0 o posterior.	Se trata de una limitación conocida. Debe descifrar todos los archivos que fueron cifrados utilizando versiones anteriores de Client Security Software *antes* de instalar Client Security Software 3.0 o posterior. Client Security Software 3.0 no puede descifrar los archivos que fueron cifrados utilizando versiones anteriores de Client Security Software debido a cambios en su implementación de cifrado de archivos.

Capítulo 7. Instalación de dispositivos de hardware de otros fabricantes como complemento de IBM Client Security Software

Con Client Security y soluciones de otros fabricantes, puede proteger toda su infraestructura integrando ofertas adicionales, que le permiten adaptar el nivel de protección de sus entorno informático.

Se ha comprobado la conformidad de IBM Embedded Security Subsystem con ofertas específicas de autenticación de seguridad de estas organizaciones:

- Targus para lectores de huellas dactilares
- Gemplus para soluciones de smart card
- Ensure Technologies para tarjetas de identificación por contacto

Visite este sitio Web que contiene enlaces a estas organizaciones para conocer más sobre las ofertas de cada organización:
http://www.pc.ibm.com/us/security/index.html

Al igual que con numerosos componentes de las imágenes de disco, el orden de instalación es de vital importancia. Si desea desplegar los dispositivos de autenticación de la lista anterior , sus controladores asociados y otro software, debe instalar antes IBM Client Security Software. Los controladores y el software de estos dispositivos no funcionarán correctamente si CSS no se instala en el disco duro antes que los archivos de controlador de dispositivo.

Para obtener información específica y actualizada sobre cómo instalar el software y los controladores que habilitan el hardware de autenticación, consulte la documentación que acompaña a los dispositivos.

Capítulo 8. Despliegue remoto de archivos de políticas de seguridad nuevos o revisados

Tanto si actualiza políticas de seguridad como si crea políticas diferentes para sistemas diferentes, el administrador de TI con autorización de firma puede revisar y desplegar los archivos de políticas. Edite el archivo de políticas mediante ACAMUCLI.EXE. También puede editar la política efectuando una doble pulsación en el icono IBM Security Subsystem del Panel de control.

Firme el archivo de políticas siguiendo las instrucciones que aparecen en pantalla después de pulsar Aplicar. **Nota:** si la clave privada del administrador está dividida, todos los componentes deben entrarse en orden para firmar el archivo de políticas. Los archivos que ha editado son GLOBALPOLICY.GVM y GLOBPOLICY.GVM.SIG. Distribuya estos archivos a los usuarios apropiados, asegurándose de que se guardan en la carpeta Security\UVM_Policy.

Puede actualizar las políticas de frases de paso remotamente después del despliegue. La actualización del archivo de políticas de frases de paso le permite cambiar los requisitos de frase de paso cuando (o si) el usuario cambia su frase de paso. El administrador puede definir un periodo de tiempo después del cual el usuario se verá forzado a cambiar la frase de paso. Este periodo de tiempo se define durante la inscripción o el registro del usuario. Un ejemplo sería el siguiente: el administrador inscribe al usuario, Juan, y la política inicial indica que el usuario Juan tiene que tener una contraseña de ocho caracteres que caduca cada 30 días. El administrador puede actualizar el archivo de políticas y exigir que la próxima vez que Juan cambie su frase de paso la nueva frase de paso tenga 12 caracteres. El administrador también podría cambiar el periodo de caducidad. Por ejemplo, en lugar de cada 30 días, el administrador podría exigir que Juan cambie su frase de paso cada 15 días. ¿Qué ocurre en el escenario siguiente? Estamos en el día 10 de la ″vida″ de la frase de paso de 30 días. Se envía un nuevo archivo de políticas de frases de paso al sistema cliente que indica que la frase de paso debe cambiarse cada 15 días. ¿La frase de paso caduca dentro de 5 días o dentro de 20 días? La frase de paso caduca dentro de 20 días como indicaba la política original. La política de caducidad de frases de paso entra en vigor cuando se establece la frase de paso. La política de cambio de 15 días comenzará cuando Juan cambie su frase de paso dentro de 20 días.

Si desea cambiar las características necesarias de la frase de paso, siga las instrucciones anteriores. Después, distribuya los siguientes archivos de la carpeta SECURITY\UVM_POLICY: UVM_PP_POLICY.DAT y UVM_PP_POLICY.DAT.SIG.

Apéndice. Avisos

Puede que IBM no ofrezca en todos los países los productos, los servicios o las funciones que se describen en este documento. Consulte al representante local de IBM para obtener información sobre los productos y servicios que actualmente pueden adquirirse en su zona geográfica. Las referencias a un producto, programa o servicio de IBM no pretenden afirmar ni implicar que sólo pueda utilizarse este producto, programa o servicio de IBM. En su lugar se puede utilizar cualquier producto, programa o servicio funcionalmente equivalente que no vulnere ningún derecho de propiedad intelectual de IBM. Sin embargo, la evaluación y verificación del funcionamiento de cualquier producto, programa o servicio no IBM son responsabilidad del usuario.

IBM puede tener patentes o solicitudes de patentes en tramitación que hacen referencia a temas tratados en este documento. La posesión de este documento no otorga ninguna licencia sobre dichas patentes. Puede realizar consultas sobre licencias escribiendo a:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

INTERNATIONAL BUSINESS MACHINES CORPORATION PROPORCIONA ESTA PUBLICACIÓN "TAL CUAL" SIN GARANTÍAS DE NINGUNA CLASE, YA SEAN EXPRESAS O IMPLÍCITAS, INCLUYENDO, PERO SIN LIMITARSE A, LAS GARANTÍAS IMPLÍCITAS DE NO INFRACCIÓN, COMERCIALIZACIÓN O IDONEIDAD PARA UN PROPÓSITO DETERMINADO. Algunas jurisdicciones no permiten declaraciones de limitación de responsabilidad de garantías explícitas o implícitas en algunas transacciones, por tanto, es posible que esta declaración no se aplique al usuario.

La presente publicación puede contener inexactitudes técnicas o errores tipográficos. Periódicamente se efectúan cambios en la información aquí contenida; estos cambios se incorporarán en nuevas ediciones de la publicación. IBM puede realizar mejoras o cambios en los productos o programas descritos en esta publicación cuando lo considere oportuno y sin previo aviso..

Los productos descritos en este documento no están pensados para que se utilicen en implantaciones u otras aplicaciones para mantenimiento de la vida donde un mal funcionamiento pueda ocasionar lesiones o, incluso, la muerte. La información contenida en este documento no afecta ni altera las especificaciones o garantías del producto de IBM. Nada de lo que aparezca en este documento puede utilizarse como una licencia implícita o explícita o inmunidad ante los derechos de propiedad intelectual de IBM u otros proveedores. Toda la información que aparece en este documento se obtuvo en entornos específicos y se utiliza con fines ilustrativos. El resultado obtenido en otros entornos operativos puede variar.

IBM puede utilizar y distribuir cualquier parte de la información que proporcione cualquier cliente de la forma que considere más apropiada sin incurrir en ningún tipo de obligación con el cliente.

Sitios Web no IBM

Las referencias hechas en esta publicación a sitios Web no IBM se proporcionan sólo por comodidad del usuario y en ningún modo constituyen un respaldo de dichos sitios Web. Los materiales de dichos sitios Web no forman parte de los materiales para este producto de IBM y el uso de dichos sitios Web es a cuenta y riesgo del usuario.

Marcas registradas

Los términos siguientes son marcas registradas de International Business Machines Corporation en los Estados Unidos y/o en otros países:

IBM
ThinkPad
ThinkCentre
Tivoli

Microsoft, Windows y Windows NT son marcas registradas de Microsoft Corporation en los Estados Unidos o en otros países.

Otros nombres de compañías, productos o servicios pueden ser marcas registradas o marcas de servicio de otras empresas.