ISEC Labs #11

Despliegue y restauración segura de volúmenes cifrados con TrueCrypt

Javier Moreno
jmoreno<arroba>isecauditors.com

1. RESUMEN 2

2. INTRODUCCIÓN 2

3. RESTAURACIÓN DE VOLÚMENES CIFRADOS 3

4. CONCLUSIÓN 14

5. REFERENCIAS 14

1. Resumen

En este nuevo ISec Lab tratamos una de las herramientas más útiles a la hora de proteger la información en nuestros equipos. Se trata de TrueCrypt una herramienta de cifrado open-source y gratuita que nos proporciona la posibilidad de crear una unidad de disco virtual donde toda la información que se almacene en ella quedará cifrada y protegida por una contraseña.

El artículo hace hincapié en una de las más características más desconocidas pero quizás más útiles de TrueCrypt: la posibilidad, en entornos corporativos, de restauración de volúmenes cifrados cuya clave ha sido perdida, olvidada o extraviada. Esta funcionalidad permite a las entidades disponer de una herramienta de cifrado completamente gratuita, cuya eficacia ha sido altamente demostrada y con la posibilidad de recuperar información cifrada en caso de pérdida de contraseñas por parte de los usuarios.

2. Introducción

TrueCrypt es una aplicación de cifrado open-source y libre. TrueCrypt funciona en sistemas operativos Windows, Linux y Mac OS X. Permite crear volúmenes cifrados dentro de un archivo y montarlos como si fueran una unidad de disco real e independiente.

Las principales funcionalidades de TrueCrypt son las siguientes

- Posibilidad de cifrar una partición entera o un dispositivo de almacenamiento (tipo memoria USB o disco duro)
- Posibilidad de cifrar la partición donde Windows está instalado obteniendo así una autenticación anterior al arranque del equipo.
- El cifrado que realiza TrueCrypt es:
    a. ***Automático:*** Los datos se cifran automáticamente. El volumen TrueCrypt se encuentra cifrado de manera completa incluyendo nombres de archivos, tablas de asignación, espacio libre, etc.
    b. ***En tiempo real (on-the-fly):*** El descifrado de datos se produce en memoria mientras los datos son leídos o copiados desde la unidad TrueCrypt. Del mismo modo, los datos son cifrados en tiempo real, justo antes de ser escritos en el disco.
    c. ***Transparente:*** No es necesaria la intervención del usuario en ningún punto del proceso de cifrado/descifrado.
- Los datos pueden ser copiados a/desde una unidad TrueCrypt exactamente igual que son copiados a/desde un disco normal (copiar/pegar, arrastrar y soltar, etc.)
- Los volúmenes TrueCrypt pueden ser cifrados utilizando algoritmos (o combinaciones de algoritmos) como: AES, Serpent, Twofish, AES-Twofish, AES-Twofish-Serpent, Serpent-AES, Serpent-Twofish-AES y Twofish-Serpent.
- TrueCrypt tiene un sistema de volúmenes ocultos que permite anular potenciales extorsiones para revelar la contraseña de un usuario (plausible deniability o negación demostrable)
- TrueCrypt también cuenta con un modelo para despliegue de unidades cifradas masivas en entornos empresariales. Los usuarios finales podrán generar sus propias contraseñas para los volúmenes cifrados y el administrador dispondrá de claves maestras para utilizar en caso de emergencia (perdida de la contraseña por parte del usuario, abandono de la empresa por parte del empleado, etc.)

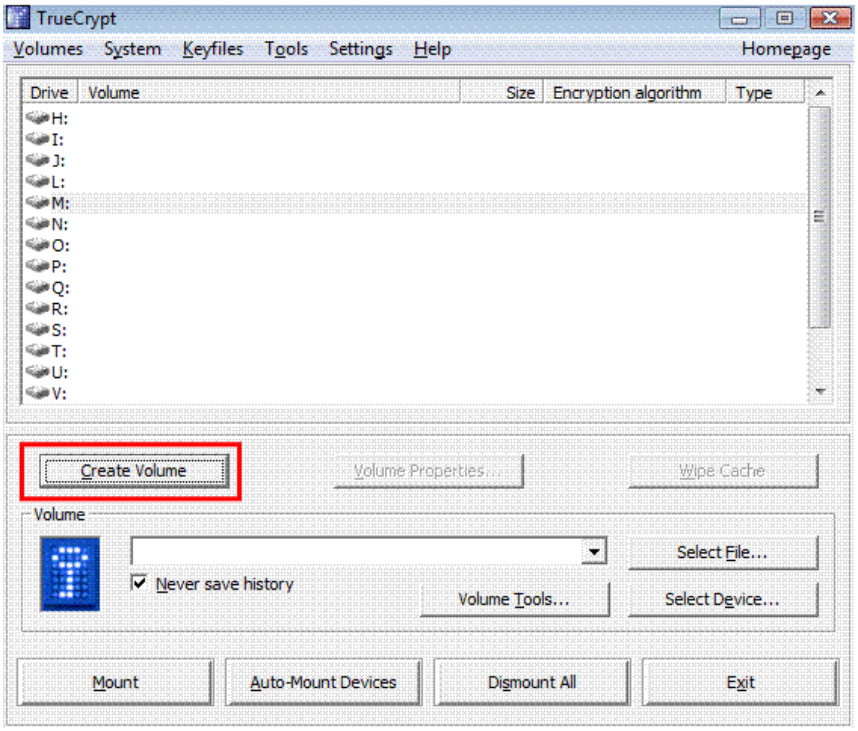
Una de las medidas de seguridad que implementa TrueCrypt es que nunca descifra los datos en el disco, sino que sólo lo hace en memoria. Cuando un usuario quiere utilizar un archivo que está ubicado en la unidad cifrada, TrueCrypt se encarga de ir descifrándolo poco a poco en memoria según el sistema operativo y la aplicación asociada a ese tipo de archivos se lo va solicitando. De este modo se evita que datos no cifrados residan en el disco aunque sólo fuera de una forma temporal.

3. Restauración de volúmenes cifrados

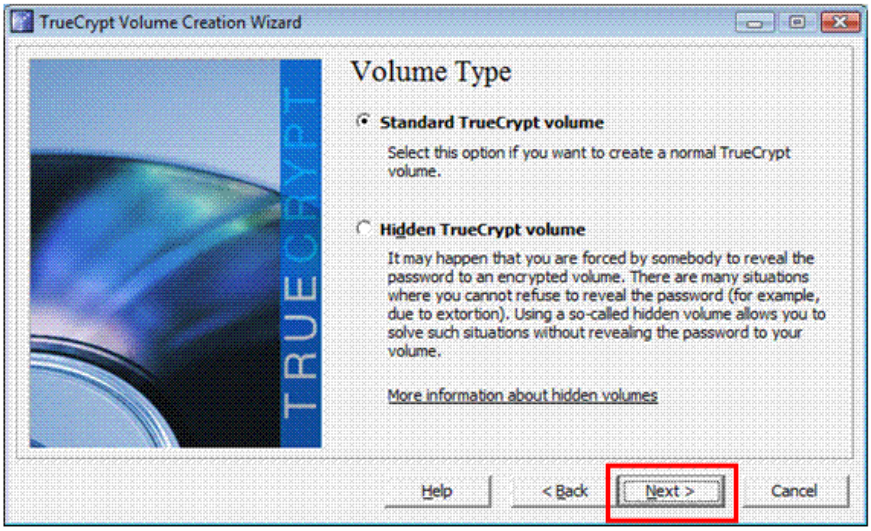
El caso que se va a exponer en este apartado corresponde a la situación en la que la política de seguridad de una entidad exige a sus empleados que toda la información de trabajo se almacene cifrada en los ordenadores corporativos. En esta situación al plataforma cada equipo antes de entregárselo al usuario, el administrador de sistemas debe crear una partición cifrada donde se almacenará la información corporativa. El usuario debe poder cambiar la contraseña de dicho volumen cifrado y además, el administrador de sistemas debe ser capaz de recuperar la información cifrada en caso de que el usuario pierda u olvide la contraseña utilizada.

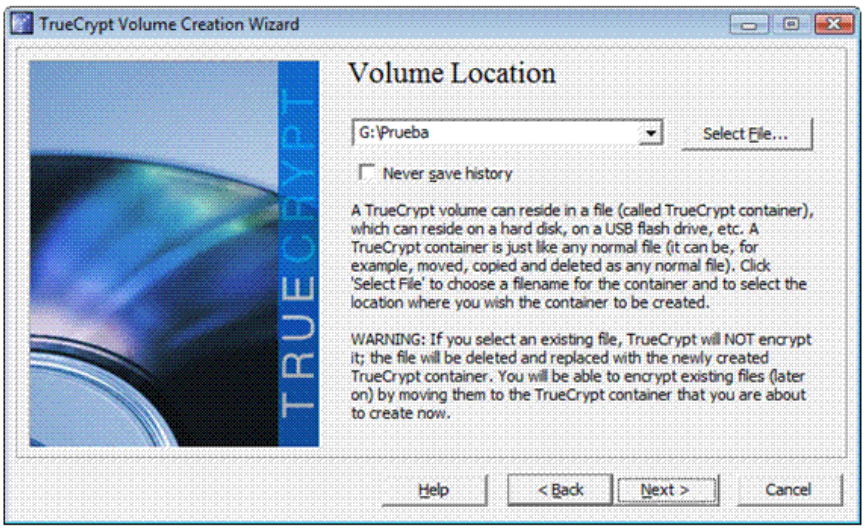
Los pasos a dar para alcanzar la situación descrita en el párrafo anterior serían los siguientes:

Paso 1. El Administrador crea un volumen cifrado en el ordenador del usuario.

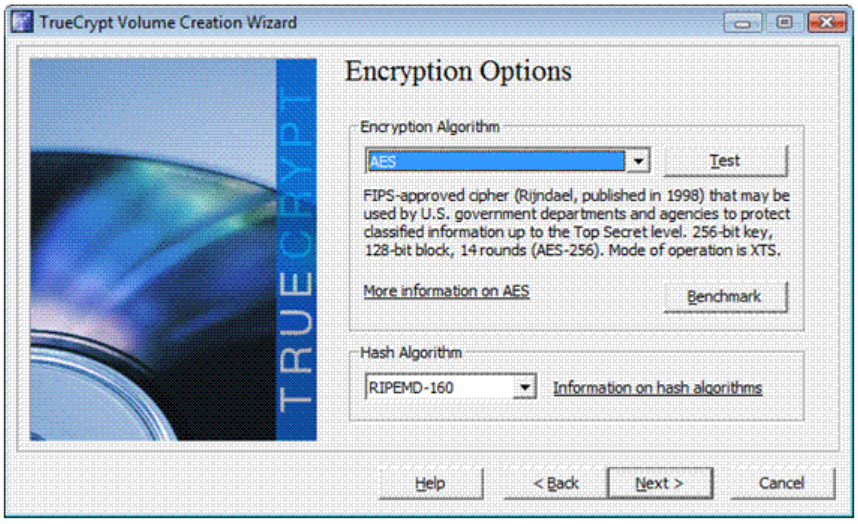


Paso 2. Elige crear el volumen dentro de un archivo, el tipo de volumen, el nombre y la ubicación del archivo que contendrá el volumen.

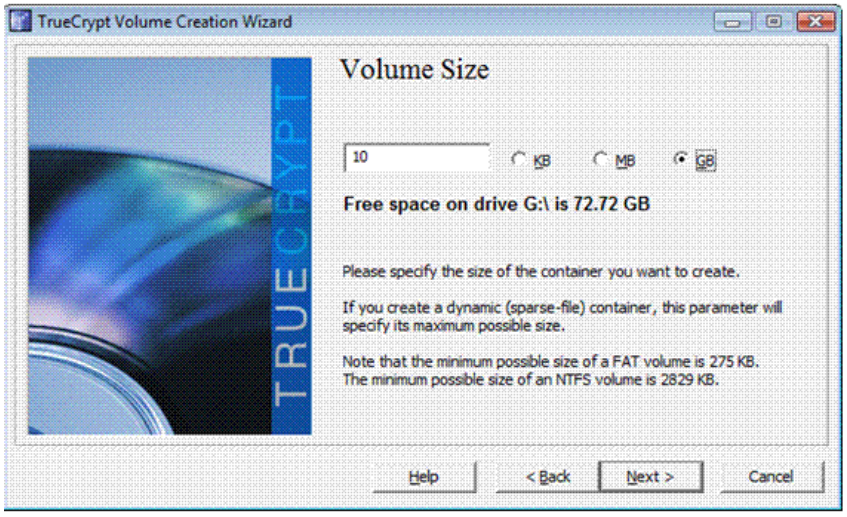




Paso 3. También es necesario seleccionar el algoritmo de cifrado así como la función Hash a utilizar.

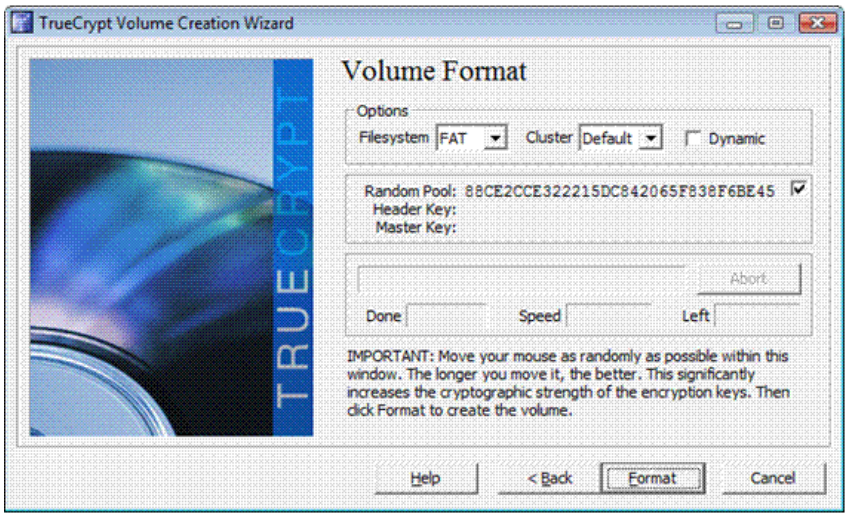


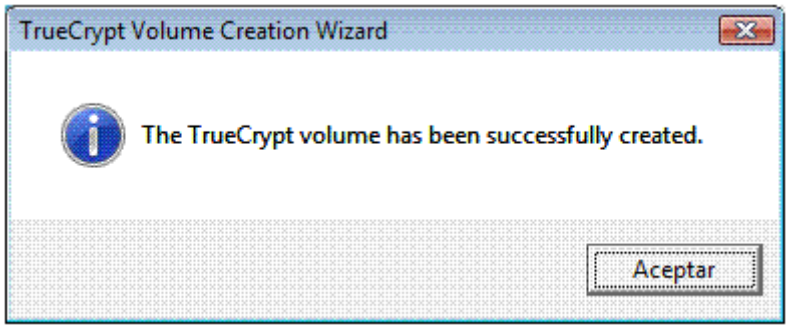
Paso 4. Debe seleccionar además el tamaño que tendrá el nuevo volumen.



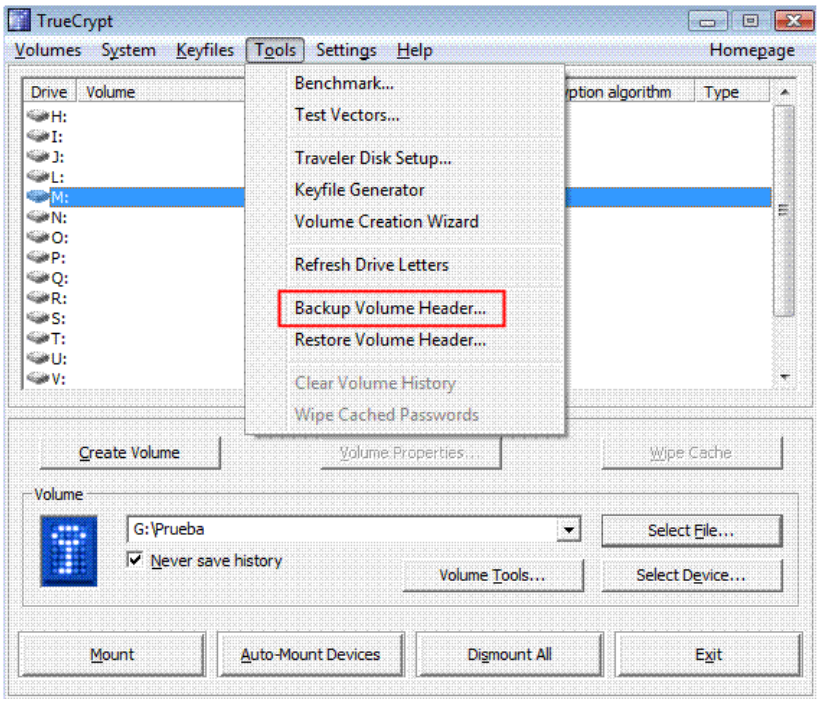
Paso 5. Se selecciona la contraseña de este nuevo volumen.

Paso 6. Finalmente se formatea el volumen y de este modo se obtiene un nuevo volumen TrueCrypt cifrado.

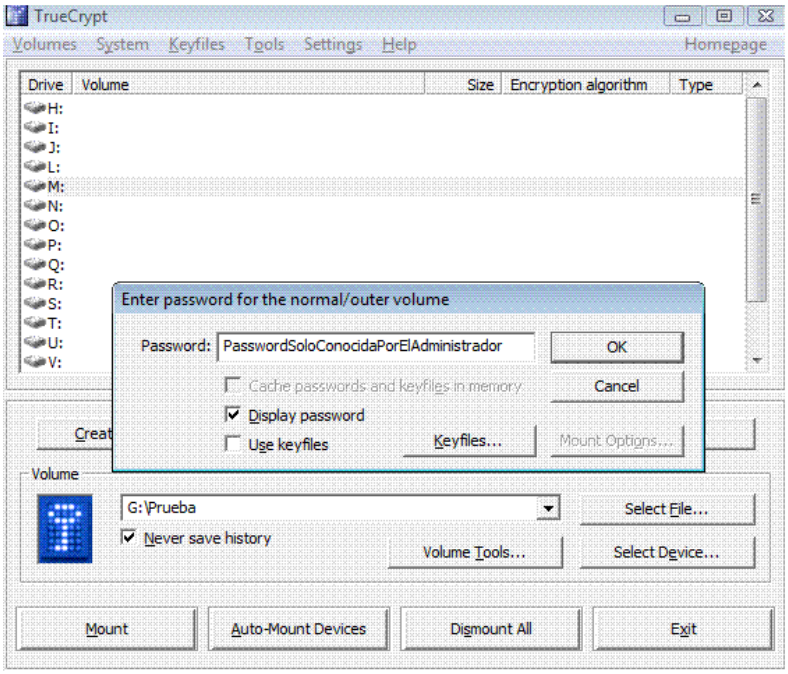




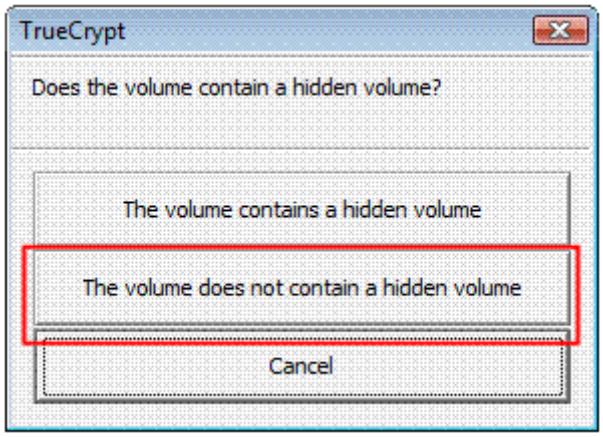
Paso 7. Una vez el volumen cifrado ha sido creado, el administrador de sistemas debe realizar un backup de la cabecera de dicho volumen:



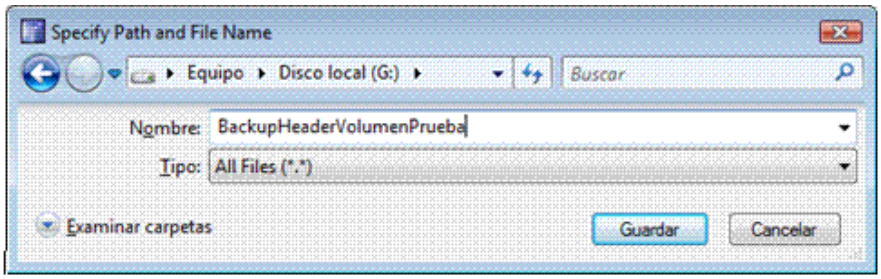
Paso 8. TrueCrypt, como medida de seguridad, solicitará la contraseña del volumen cuya cabecera estamos guardando. Esta medida asegura que solo el creador del volumen puede realizar un backup de la cabecera de dicho volumen.

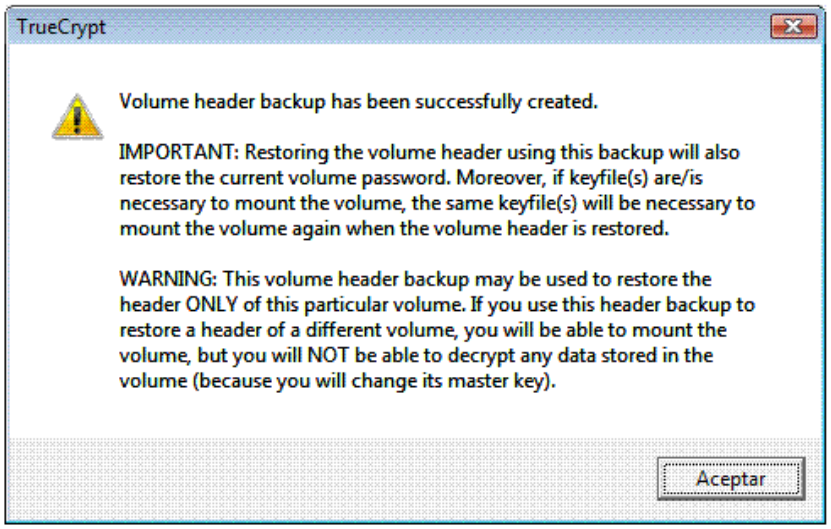


Paso 9. Se debe seleccionar si el volumen de cuya cabecera vamos a hacer un backup, contiene o no un volumen oculto.

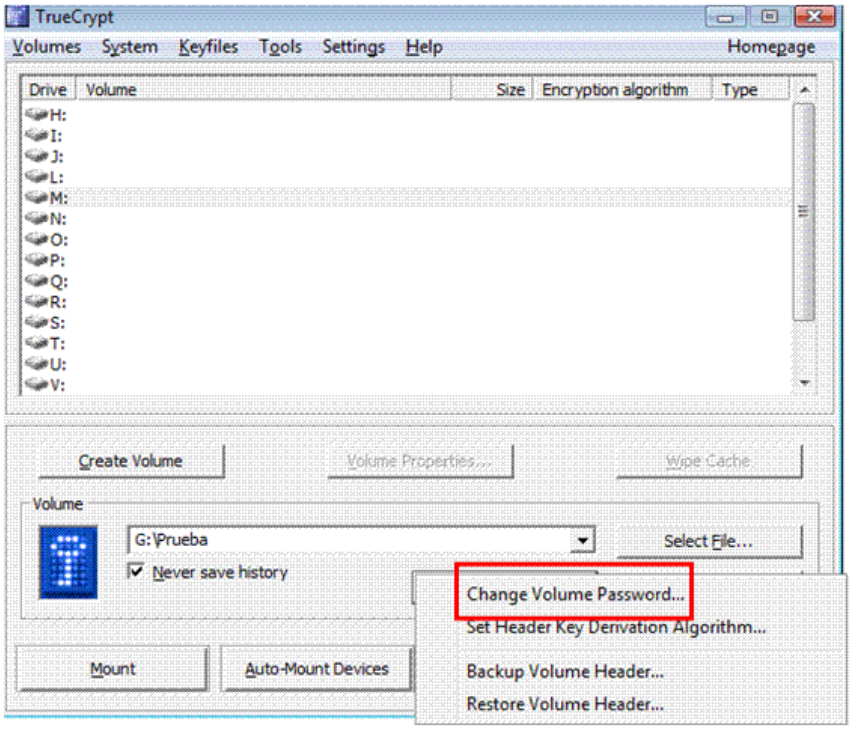


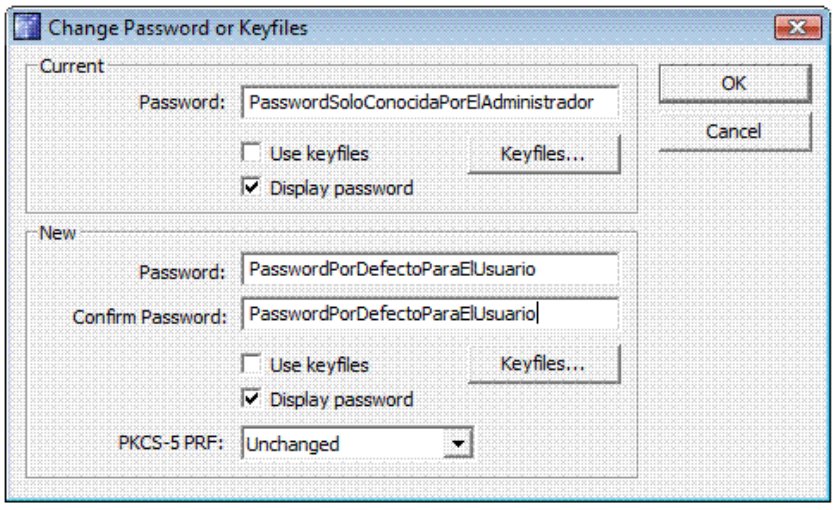
Paso 10. Por último, se debe indicar el nombre que asignaremos a este backup y estará lista la copia de seguridad de la cabecera del volumen creado.

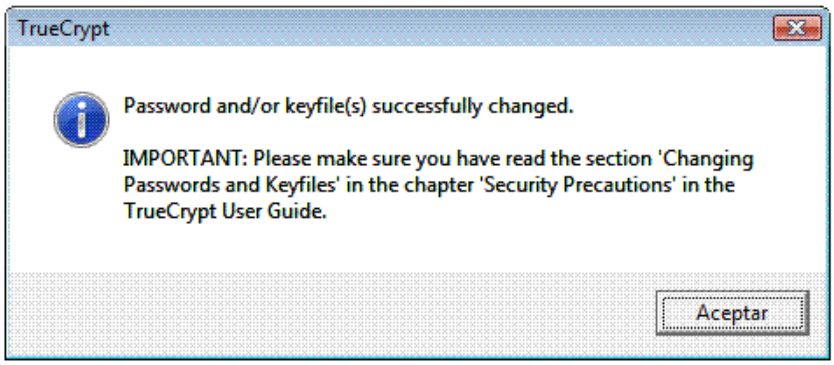




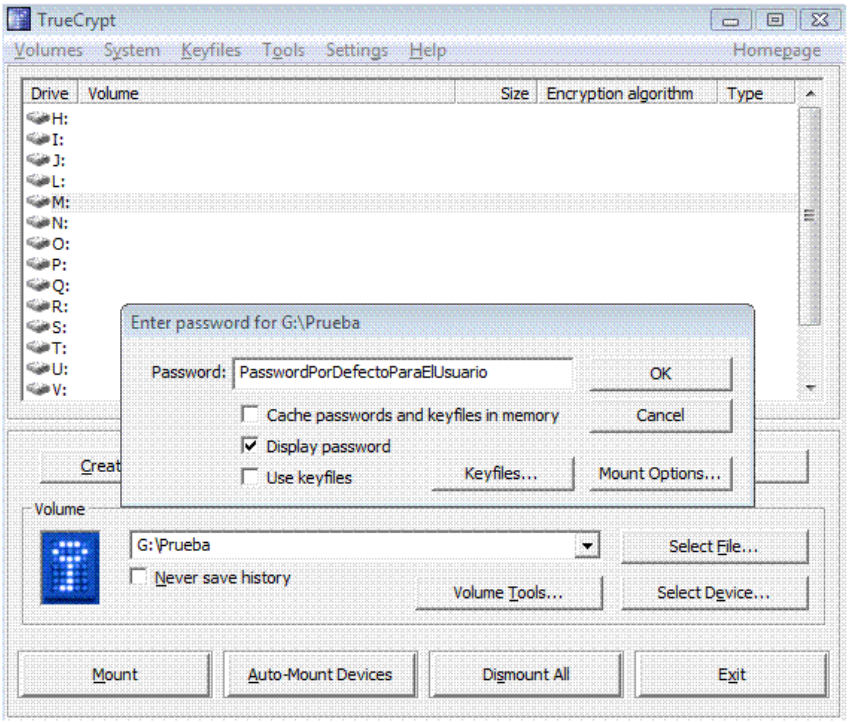
Paso 11. Antes de entregar el PC al usuario el administrador de sistemas debe cambiar la contraseña del volumen (con la intención de que el usuario final no conozca la contraseña inicial, que será la que nos permite recuperar el volumen cifrado en caso de emergencia):



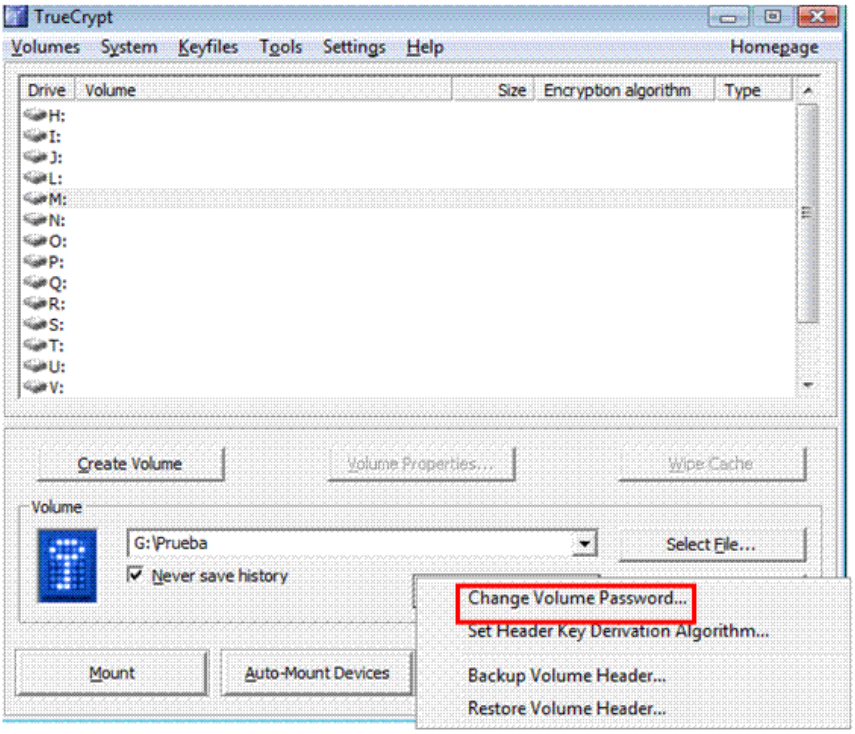


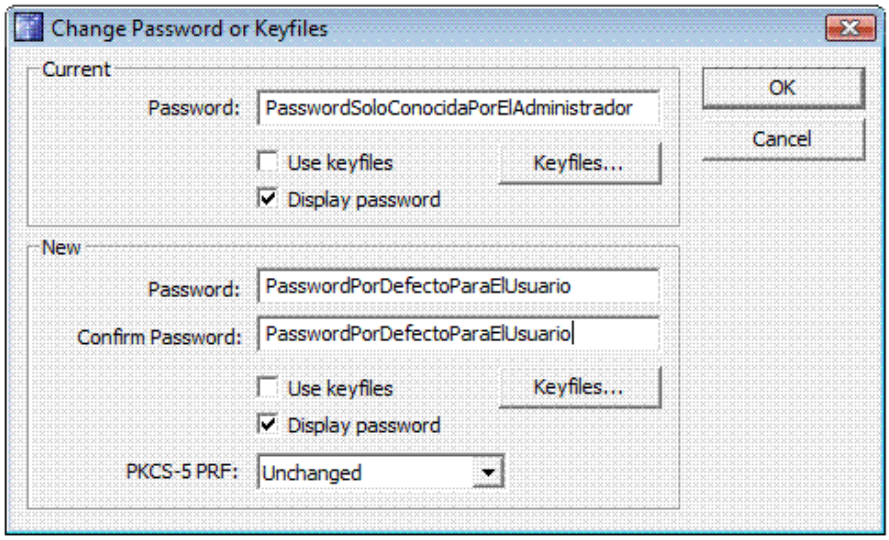


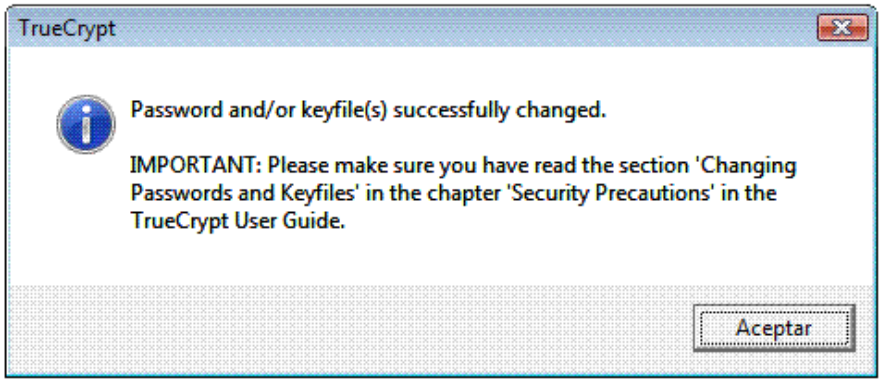
Paso 12. Ahora sí, el Administrador de Sistemas ya puede entregar el equipo al usuario final indicándole la clave necesaria para montar el volumen cifrado. Con esa contraseña el usuario podrá montar la unidad cifrada.



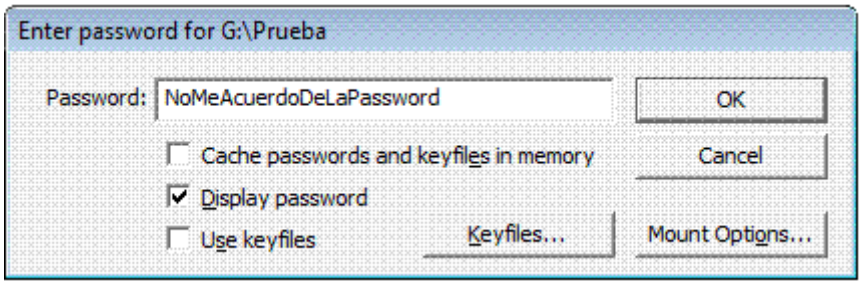
Por supuesto, el usuario final también puede cambiar esta contraseña tantas veces como quiera:

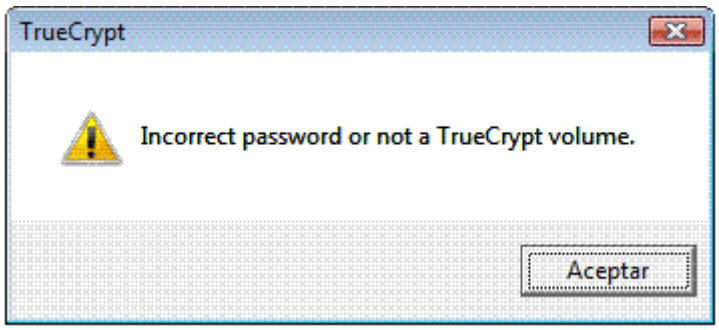






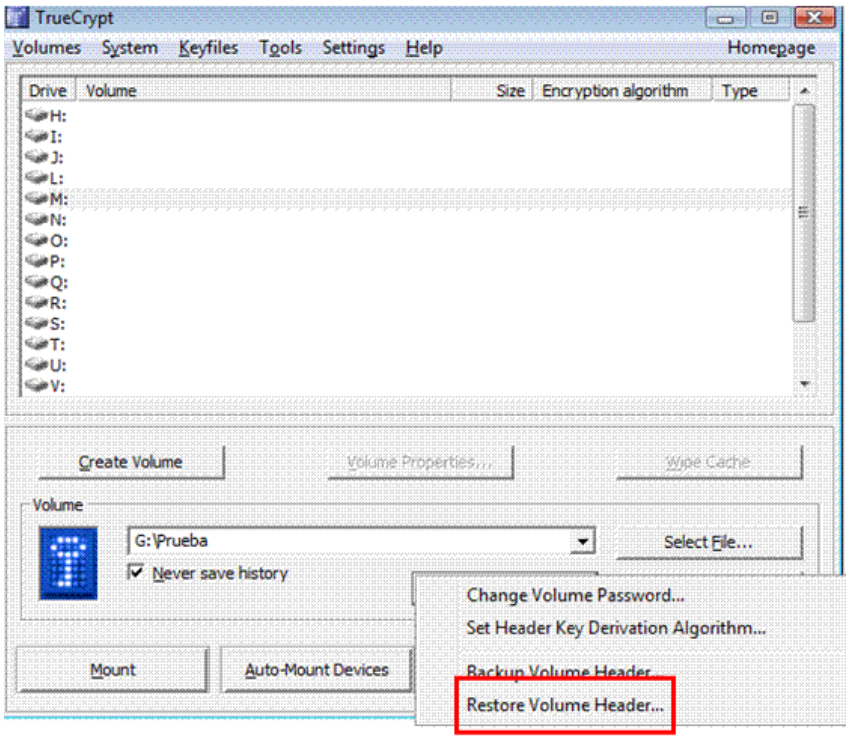
Si el usuario final pierde la contraseña o no la recuerda,



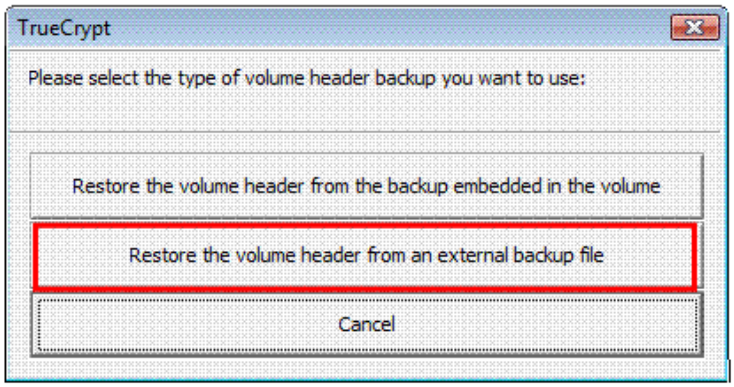


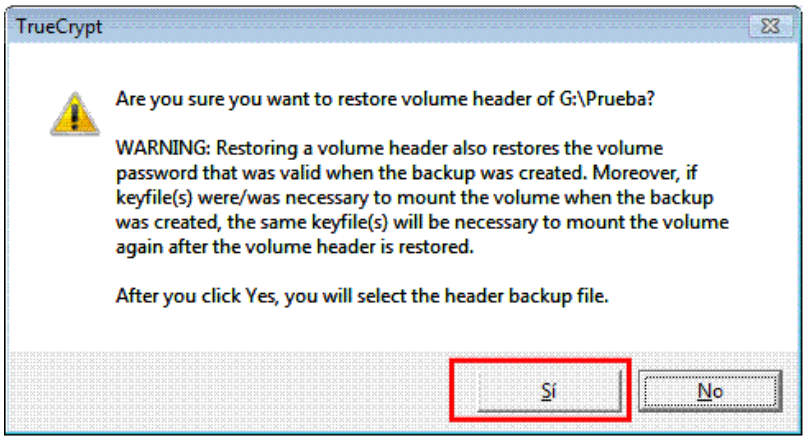
La copia de seguridad de la cabecera realizada por el Administrador de Sistemas permitirá a éste recuperar ese volumen para el usuario. Para ello los pasos a dar serían los siguientes:

Paso 1. Seleccionar el volumen problemático y elegir la opción Restaurar Cabecera de Volumen dentro del menú Volume Tool:

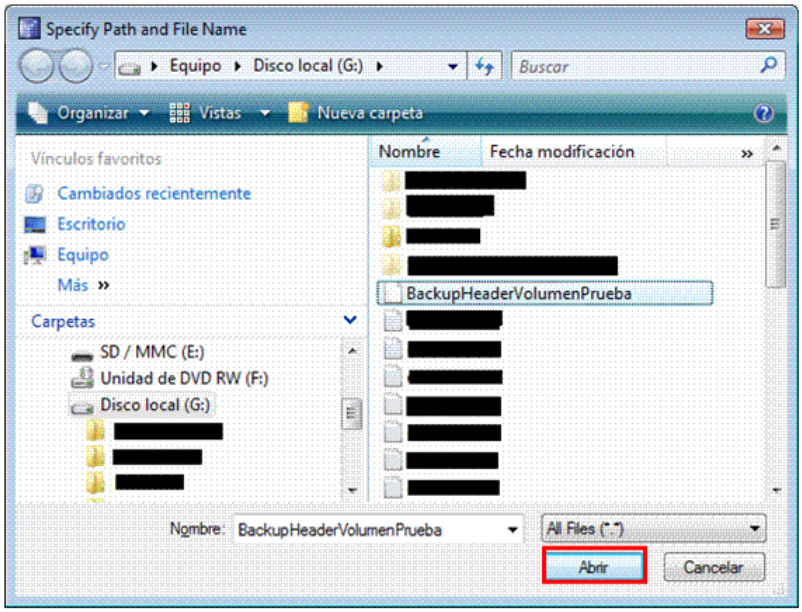


Paso 2. Seleccionar restaurar la cabecera desde un archivo de backup externo:

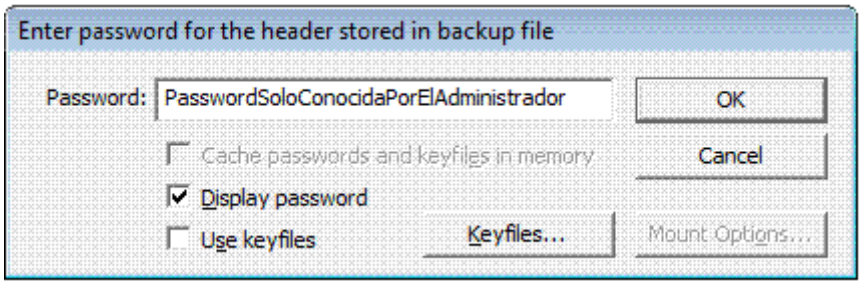


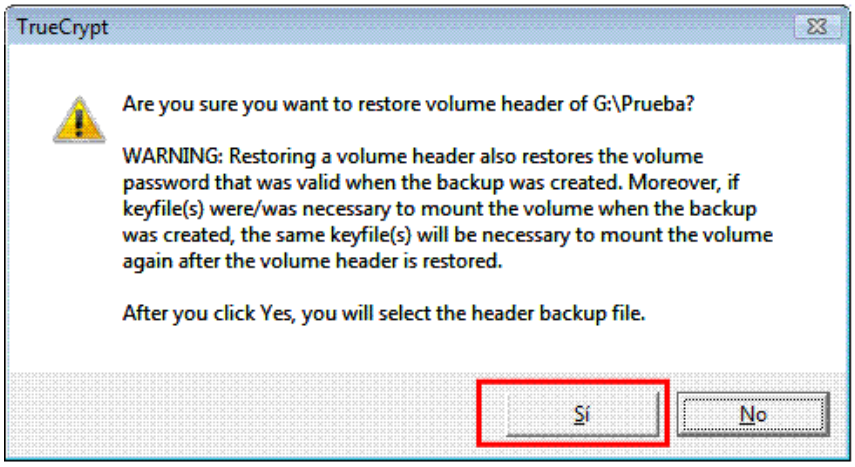


Paso 3. Buscar y seleccionar el archivo correspondiente al backup de la cabecera:

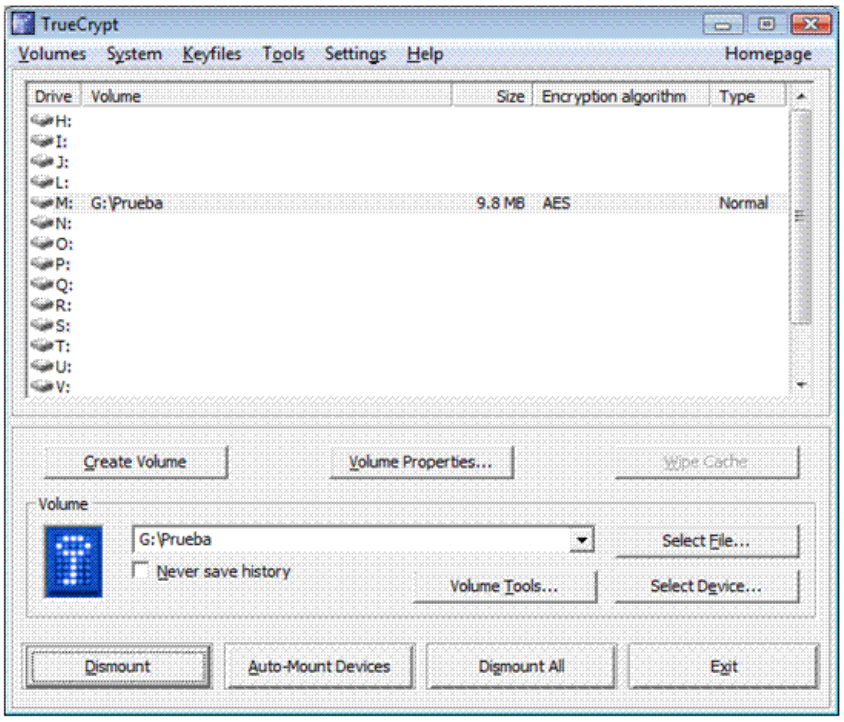


Paso 4. Para finalizar se debe introducir la contraseña inicialmente asignada a este volumen.

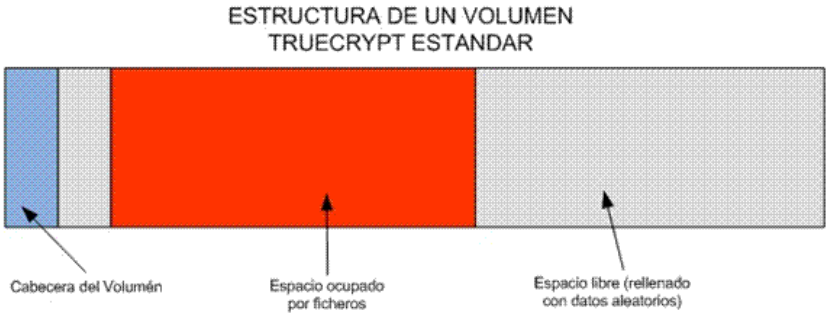




Paso 6. Utilizando esa contraseña se podría volver montar el volumen, y por supuesto cambiar la contraseña para asignarle una nueva al usuario.



La clave de este proceso de restauración de claves se encuentra en la estructura que tienen los volúmenes TrueCrypt:



La cabecera del volumen TrueCrypt ocupa 512 bytes. Sus primeros 64 bytes son denominados SALT y son un conjunto aleatorio de caracteres generados durante el proceso de creación del volumen. El SALT no está cifrado (bytes 0 a 63). El resto de la cabecera (bytes 64 a 511) está cifrada con la llamada clave de cabecera (header key).

Dentro de la cabecera se encuentra la clave maestra (master key) con la que se encuentran cifrada el resto de los datos.

Por lo tanto lo primero que TrueCrypt tiene que hacer para descifrar una unidad cifrada es averiguar la clave de cabecera. Este clave de cabecera se calcula mediante unas funciones criptográficas que tienen como parámetros de entrada la password introducida por el usuario y la propia SALT.

Una vez descifrada la clave de cabecera se puede acceder a la master key y por tanto descifrar los datos contenidos en el volumen TrueCrypt.

Al cambiar la password de un volumen lo único que se consigue es cambiar la clave de la cabecera (y no la master key). Este cambio permite al usuario utilizar una nueva clave para acceder al volumen. Por lo tanto si hacemos un backup de la cabecera del volumen en el momento de crearlo, estaremos salvaguardando la master key (solo descifrable con la header key original). Y da igual cuantas veces cambie el usuario la contraseña (la header key) que simplemente con sustituir la cabecera actual por la original, impondremos la header key original, recuperando el acceso a la master key y con ella el acceso a los datos.

4. Conclusiones

Como hemos mostrado, disponer se soluciones eficientes de cifrado con el grado de seguridad que un entorno corporativo puede no implicar el desembolso de grandes capitales. Confiar en el software libre, si además es de código abierto, debe ofrecer toda la confianza que un software comercial con el valor añadido de las reducciones de coste. Añadido a que su uso sea relativamente masivo puede ser un aliciente más para no tener la sensación de estar haciendo un experimento que un error no pudiera justificar. Pero no olvidemos las copias de seguridad.

5. Referencias

[1] Documentación Oficial de TrueCrypt. Accesible en: http://www.truecrypt.org/docs/