Sistema de encriptación de archivos para Windows 2000

Documento estratégico

Resumen

El presente documento proporciona un resumen ejecutivo y una descripción general técnica sobre el sistema de encriptación de archivos (EFS) que se incluye en el sistema operativo Microsoft® Windows® 2000.

EFS brinda la tecnología principal de encriptación de archivos para almacenar los archivos NTFS encriptados en disco. EFS se dirige particularmente a los problemas de seguridad que surgen por las herramientas disponibles en otros sistemas operativos, que permiten a los usuarios acceder archivos desde un volumen NTFS sin una verificación de acceso. Con EFS, los datos en los archivos NTFS se encriptan en el disco. La tecnología de encriptación utilizada se basa en la clave pública y se ejecuta como un servicio de sistema integrado, lo cual facilita su administración, lo protege contra ataques y lo hace transparente para el usuario. Si un usuario que intenta acceder un archivo NTFS encriptado tiene la clave privada para dicho archivo, el usuario puede abrir el archivo y trabajar con él de manera transparente, como un documento normal. Se le niega el acceso a un usuario que no cuenta con la clave privada para el archivo.

Microsoft Corporation • One Microsoft Way • Redmond, WA 98052-6399 • USA

0399

TABLA DE CONTENIDOS

RESUMEN EJECUTIVO

Una medida de seguridad estándar en un sistema de computadora personal es intentar iniciar desde un disco flexible antes de intentarlo desde el disco duro. Esto protege a los usuarios contra fallas en el disco duro y particiones de inicio dañadas. Lamentablemente, también agrega la conveniencia de iniciar diferentes sistemas operativos. Esto podría significar que alguien con acceso físico a un sistema pudiera desviar las funciones de seguridad integradas del control de acceso al sistema de archivos Microsoft® Windows NT®, utilizando una herramienta para leer las estructuras en disco Windows NTFS. Varias configuraciones de hardware proporcionan funciones como una contraseña para restringir este tipo de acceso. Dichas funciones no se utilizan comúnmente, y en un ambiente típico, donde varios usuarios comparten una estación de trabajo, no funcionan adecuadamente. Incluso si estas funciones fueran universales, la protección que brinda una contraseña no es muy sólida.

Entre los escenarios típicos donde el acceso a datos no autorizado se vuelve un problema, se incluyen:

- **Una *laptop* robada**—En tan solo un instante alguien puede llevarse una *laptop* no vigilada. ¿Qué pasa si el ladrón no pretende revender la computadora, sino que está interesado en la información importante almacenada en su disco duro?
- **Acceso no restringido**—Los sistemas de escritorio Office se dejan sin atender y cualquiera puede llegar y robar información rápidamente en una computadora que se ha dejado desatendida.

La raíz de estas preocupaciones de seguridad es la información sensible, la cual existe por lo regular en archivos no protegidos de su disco duro. Puede restringir el acceso a la información importante almacenada en una partición NTFS si Windows NT es el único sistema operativo que se puede ejecutar y si el disco duro no se puede retirar físicamente. Si alguien desea realmente obtener la información, no es difícil que pueda tener acceso físico a la computadora o al disco duro. La disponibilidad de las herramientas que permiten acceder a los archivos NTFS desde los sistemas operativos MS-DOS® y UNIX hace que el desvío de seguridad de NTFS sea aún más sencillo.

La encriptación de datos es la única solución para este problema. Existen varios productos en el mercado que permiten la encriptación de archivos a nivel de aplicaciones, utilizando claves derivadas de las contraseñas. Sin embargo, existen ciertas limitantes con la mayoría de estos enfoques:

- **Encriptación y desencriptación manual en cada uso.** Los servicios de encriptación no son transparentes para el usuario en la mayoría de los productos. El usuario tiene que desencriptar el archivo antes de cada uso y volver a encriptarlo al terminar. Si el usuario olvida encriptar un archivo, el archivo queda sin protección. Debido a que el usuario debe especificar que un archivo va a ser encriptado (y desencriptado) en cada uso, esto puede omitirse.
- **Fugas de archivos temporales y de búsqueda.** Varias aplicaciones crean

archivos temporales mientras el usuario edita un documento (por ejemplo, Microsoft Word). Estos archivos temporales se dejan sin encriptar en el disco, aún cuando el documento original esté encriptado, haciendo que el robo de los datos es muy fácil. La encriptación a nivel de aplicaciones se ejecuta en el modo de usuario Windows. Esto significa que la clave de encriptación del usuario puede almacenarse en un archivo de búsqueda. Es bastante fácil tener acceso a todos los documentos encriptados utilizando una sola clave, con solo explotar en un archivo de búsqueda.

- **Seguridad débil.** Las claves se derivan de contraseñas o frases de pase. Los ataques de diccionario fácilmente pueden abrir una brecha en este tipo de seguridad, si se utilizan contraseñas fáciles de recordar.
- **Sin recuperación de datos.** Muchos productos no proporcionan los servicios de recuperación de datos. Este es otro aspecto que desalienta a los usuarios, especialmente a quienes no desean tener que recordar otra contraseña. En los casos en que se brinda la recuperación de datos con base en una contraseña, se crea otro punto de acceso débil. El único dato que necesita un ladrón es la contraseña, para que el mecanismo de recuperación le permita acceder a los archivos encriptados.

El sistema de encriptación de archivos (EFS) resuelve todos los problemas mencionados anteriormente y más. Las cuatro secciones siguientes detallan la tecnología de encriptación, en dónde se realiza la encriptación en el sistema, la interacción del usuario y la recuperación de datos.

Tecnología de encriptación EFS

EFS se basa en la encriptación de clave pública, que aprovecha la arquitectura CryptoAPI en Windows. Cada archivo se encripta utilizando una clave generada de manera aleatoria, que es independiente del par de clave privada/pública del usuario, evitando así varias formas de ataque con base en criptoánalisis.

La encriptación de archivos puede utilizar cualquier algoritmo de encriptación simétrico. La primera versión del EFS expone DES como el algoritmo de encriptación. Las versiones futuras permitirán esquemas de encriptación alternos.

El EFS también soporta la encriptación y desencriptación en archivos almacenados en servidores de archivos remotos. **Nota:** En este caso, el EFS sólo resuelve la encriptación de datos en disco. No encripta datos que se transfieren a través de la red. Windows proporciona protocolos de red como SSL/PCT para encriptar el acceso a datos en la red.

En dónde reside el EFS

El EFS está integrado firmemente con el NTFS. Cuando se crean archivos temporales, los atributos del archivo original se copian a los archivos temporales, siempre que los archivos estén en el volumen NTFS. Si encripta un archivo, el EFS también encripta sus copias temporales. El EFS reside en el *kernel* del sistema operativo y utiliza una agrupación de no búsqueda para almacenar las claves de

encriptación de archivo lo cual asegura que nunca estén en el archivo de búsqueda.

Interacción del usuario

La configuración predeterminada del EFS permite que los usuarios inicien la encriptación de archivos sin esfuerzo administrativo. El EFS genera automáticamente un par de clave pública para la encriptación de archivos para un usuario, en caso de que no exista.

La encriptación y desencriptación de archivos se soporta sobre una base de directorio completo o por archivos. La encriptación de directorios se refuerza de manera transparente. Todos los archivos (y subdirectorios) creados en un directorio marcado para encriptación se encriptan automáticamente. Cada archivo tiene una clave de encriptación única, lo que lo hace seguro para volver a nombrarlo. Si renombra un archivo desde un directorio encriptado a un directorio no encriptado en el mismo volumen, el archivo permanece encriptado. Los servicios de encriptación y desencriptación están disponibles en Windows Explorer. Las herramientas de la línea de comandos y las interfaces administrativas también se proporcionan para usuarios avanzados y agentes de recuperación, de manera que puedan aprovechar al máximo esta capacidad.

Un archivo no necesita desencriptarse antes de utilizarse. La encriptación y desencriptación se realiza de manera transparente cuando los bytes viajan hacia y desde el disco. El EFS detecta automáticamente un archivo encriptado y coloca una clave del usuario desde el almacén de claves del sistema. Ya que el mecanismo de almacenamiento de claves se basa en CryptoAPI, los usuarios tienen la facilidad de almacenar claves en dispositivos seguros, tales como las tarjetas inteligentes.

La primera versión del EFS no soporta el compartir archivos. No obstante, la arquitectura del EFS está diseñada para poder compartir archivos entre cualquier número de personas utilizando sus claves públicas. Los usuarios pueden desencriptar entonces de manera independiente los archivos mediante sus propias claves privadas. Los usuarios pueden ser agregados fácilmente (si cuentan con un par de clave pública configurado) o eliminados de un grupo de con autorización para compartir.

Recuperación de datos

El EFS cuenta con soporte de recuperación de datos. La infraestructura de seguridad Windows 2000 refuerza la configuración de claves de recuperación de datos. Puede utilizar la encriptación de archivos sólo si el sistema está configurado con una o más claves de recuperación. El EFS permite que los agentes de recuperación configuren las claves públicas que se utilizan para habilitar la recuperación de archivos. Utilizando la clave de recuperación, sólo está disponible la clave de encriptación del archivo generada de manera aleatoria y no una clave privada de usuario. Esto asegura que ninguna otra información privada sea

revelada al agente de recuperación de manera accidental.

La recuperación de datos está pensada para la mayoría de los ambientes empresariales, en donde las organizaciones esperan poder recuperar los datos encriptados por un empleado después de que el empleado se retire, o cuando se pierdan las claves de encriptación. La política de recuperación se puede definir en el controlador de dominio de un dominio Windows. Esta política se refuerza en todas las computadoras en dicho dominio. Los administradores de dominio tienen el control de la política de recuperación y pueden delegar esto a cuentas de administradores de seguridad de datos, utilizando las funciones de delegación del Servicio de directorio Windows. Esto proporciona un control mejor y más flexible de quién está autorizado para recuperar datos encriptados. El EFS también soporta diversos agentes de recuperación, al permitir múltiples configuraciones clave de recuperación que proporcionen a las organizaciones redundancia y flexibilidad al implementar sus procedimientos de recuperación.

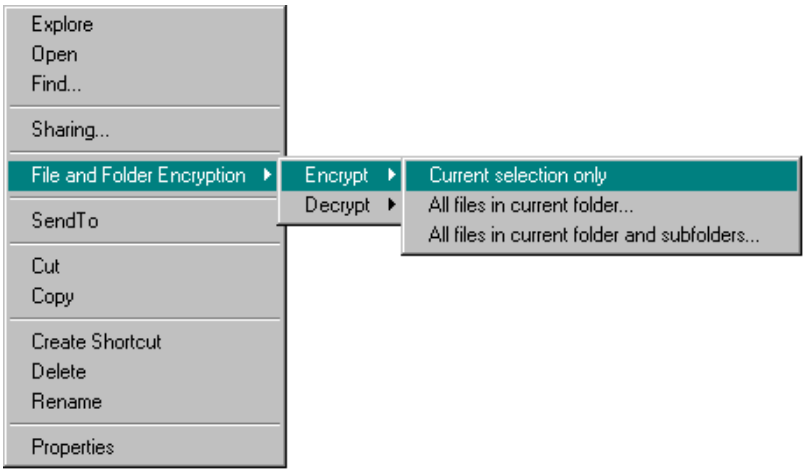
El EFS también se puede utilizar en un ambiente local. El EFS genera automáticamente claves de recuperación y las guarda como claves de la máquina en donde no hay dominio de Windows. Los usuarios locales también pueden utilizar la herramienta de línea de comandos para recuperar los datos, utilizando la cuenta del administrador. Esto reduce la sobrecarga administrativa para un usuario local.

USO DEL SISTEMA DE ENCRIPTACION DE ARCHIVOS

Las siguientes secciones brindan al usuario escenarios que demuestran cómo funciona el EFS.

Operaciones del usuario

La siguiente figura muestra el menú de contexto Windows Explorer para los servicios de encriptación de archivos.



El menú de contexto expone las siguientes funciones EFS para el usuario:

- **Encriptación**—Esta opción permite que el usuario encripte el archivo seleccionado actualmente. Si la selección actual es un directorio, permite al usuario encriptar todos los archivos (y subdirectorios) en el directorio y marcar el directorio como encriptado.
- **Desencriptación**—Esta opción es lo contrario de la encriptación. Permite que el usuario decodifique el archivo seleccionado actualmente. Si la selección actual es un directorio, permite al usuario desencriptar todos los archivos que hay en el directorio y restablece el directorio como decriptado.
- **Configuración**—Los usuarios pueden generar, exportar, importar y manejar claves públicas utilizadas para la encriptación de archivos basados en EFS. La configuración se integra con el resto de las configuraciones de seguridad del usuario. Esta función está dirigida a los usuarios avanzados que desean administrar sus propias claves. Por lo regular, los usuarios no tienen que hacer ninguna configuración. El EFS genera automáticamente claves para el usuario que no cuenta con una clave configurada para uso de encriptación de archivos.

Además de la interfaz gráfica, Windows 2000 incluye herramientas de línea de comandos para enriquecer la funcionalidad necesaria para las operaciones administrativas. Las herramientas de línea de comando son:

- **Utilidad de línea de comando *cipher***—Proporciona la capacidad de encriptar y desencriptar archivos desde un indicador de comandos.

Por ejemplo:

- Para encriptar el directorio C:\Mis documentos, el usuario escribe:

```
C:\>cipher /e "My Documents"
```

- Para encriptar todos los archivos con "cnfdl" en el nombre, el usuario escribe:

```
C:\>cipher /e /s *cnfdl*
```

El comando ***cipher*** completo soporta las siguientes opciones:

```
CIPHER [/E | /D] [/S[:dir]] [/A] [/I] [/F] [/Q] [filename [...]]
 /E    Encrypts the specified files. Directories will be marked so
that files added afterward will be encrypted.
 /D    Decrypts the specified files. Directories will be marked so
that files added afterward will not be encrypted.
 /S    Performs the specified operation on files in the given
directory and all subdirectories. Default "dir" is the current
directory.
 /I    Continues performing the specified operation even after errors
have occurred. By default, CIPHER stops when an error is encountered.
 /F    Forces the encryption operation on all specified files, even
those which are already encrypted. Already-encrypted files are
skipped by default.
 /Q    Reports only the most essential information.
 filename Specifies a pattern, file, or directory.
 Used without parameters, CIPHER displays the encryption state of the
current directory and any files it contains. You may use multiple
filenames and wildcards. You must put spaces between multiple
parameters.
```

- **Comando *copy***—Este se ampliará con las nuevas opciones para exportar e importar archivos encriptados a un formato transportable.

  Por ejemplo:

  - Para exportar un archivo encriptado a un disco flexible, el usuario escribe:

```
C:\>copy /e EncResume.doc a:
```

  Las nuevas opciones soportadas por el comando ***copy*** son:

```
copy [/E |/I] sourcefile destinationfile
 /E   exports an encrypted file (sourcefile) as an opaque encrypted
stream of bits to destinationfile. The destinationfile need not be on
an NTFS volume, it can be a FAT file on a floppy disk.
 /I   imports an opaque encrypted stream of bits from sourcefile as
an EFS encrypted file on NTFS volume. The sourcefile need not be an
NTFS file. However, destinationfile needs to be.
```

Encriptación de archivos

Todo lo que debe hacer el usuario es seleccionar uno o más archivos y elegir Encriptar del menú de contexto Encriptación de archivos. El EFS encripta los archivos seleccionados.

Una vez que el archivo se encripta, éste se almacena ya encriptado en el disco. Todas las lecturas y escrituras al archivo se desencriptan y encriptan de manera transparente. Para saber si el archivo está encriptado, el usuario puede verificar las propiedades en el archivo para ver que el bit de atributo esté activado. Ya que la encriptación es transparente, el usuario puede utilizar el archivo como antes. Por ejemplo, puede seguir abriendo el documento en Word y editarlo como antes o abrir un archivo de texto utilizando *Notepad* y hacer lo mismo. Cualquier otro

usuario que trate de abrir este archivo encriptado obtiene un error de acceso denegado, debido a que el usuario no posee la clave para desencriptar el archivo.

Los usuarios (administradores en este caso) no deberán encriptar los archivos en el directorio del sistema, pues estos archivos se necesitan para que se inicie el sistema. Durante el proceso de inicio, no hay una clave de usuario disponible para desencriptar los archivos. Dicha operación puede dejar inservible al sistema. Windows Explorer evita esto al hacer fallar los intentos de encriptación en archivos con el atributo del sistema. Las versiones futuras de Windows brindarán capacidades de inicio seguras para soportar la encriptación de los archivos del sistema.

El EFS también da a los usuarios la capacidad de transferir archivos encriptados a través de los sistemas. Las funciones de Exportar archivo encriptado e Importar archivo encriptado son extensiones del comando Copiar en un indicador de comandos Windows. Todo lo que el usuario debe hacer es especificar el archivo encriptado como la fuente y otro archivo en un directorio no encriptado como el destino con la opción de exportar. El archivo exportado continúa encriptado. El usuario puede copiar entonces este archivo exportado a diferentes sistemas de archivos, incluyendo FAT, cintas de respaldo o enviarlo como adjunto de un correo electrónico como un archivo normal. Para poder utilizar el archivo en un sistema al que se copia, el usuario especifica el archivo exportado como la fuente y un nombre de archivo nuevo en un volumen NTFS como destino para importar el archivo, con lo que el nuevo archivo se crea como un archivo encriptado. **Nota:** Con sólo copiar el archivo se hace una copia en sólo texto, a menos que el directorio en el que se copia el archivo esté marcado como encriptado, en cuyo caso la copia se reencripta. Esto se debe a que el comando de copia normal utiliza lecturas de archivo que se desencriptan de manera clara mediante el EFS. Esto se puede utilizar para crear copias de texto de un archivo encriptado para distribución.

Encriptación de directorio

Los usuarios también pueden marcar directorios como encriptados utilizando el menú de contexto Windows Explorer. Marcar un directorio como encriptado asegura que se encuiten todos los archivos futuros en dicho directorio de manera predeterminada y que todos los subdirectorios futuros del mismo se marquen como encriptados. La lista de archivos de directorio no está encintada y se pueden enumerar archivos como siempre, en caso de que tenga suficiente acceso al directorio.

Marcar los directorios para encriptación es similar a encriptar archivos. Un usuario selecciona el directorio y elige la opción de encriptación en Windows Explorer. En este caso, el usuario tiene las opciones de marcar sólo el directorio para encriptación o encriptar todos los archivos y subdirectorios bajo él. La encriptación de directorios brinda a los usuarios la capacidad de manejar sus archivos importantes copiándolos simplemente a directorios encriptados.

Desencriptación de archivo o directorio

Los usuarios no necesitan desencriptar archivos o directorios para operaciones normales debido a que el EFS brinda encriptación y desencriptación transparente durante las escrituras y lecturas de datos. No obstante, dichas operaciones pueden ser requeridas bajo circunstancias especiales en donde un usuario necesita compartir un archivo encriptado con otros usuarios.

Los usuarios pueden desencriptar archivos y marcar directorios no encriptados utilizando el menú de contexto Windows Explorer. La operación es similar a la encriptación. Realizar esta operación en uno o más archivos provoca que el EFS desencripte el archivo completo y lo marque como no encriptado. En el caso de la desencriptación de un directorio, el menú de contexto también brinda la opción de desencriptar todos los archivos y subdirectorios encriptados en dicho directorio.

Operaciones de recuperación

La política de recuperación de EFS se implementa como parte de la política de seguridad general para el sistema. Es parte de la política de seguridad de dominio para Windows Domains o parte de la política de seguridad local para las estaciones de trabajo y servidores autónomos. Como parte de la política de seguridad de dominio, aplica a todas las computadoras basadas en Windows 2000 ó Windows NT en dicho dominio. La interfaz del usuario de la Política de EFS se integra como parte de la Política de dominio y las interfaces de Política local. Esta interfaz permite que los agentes de recuperación generen, exporten, importen y respalden claves de recuperación a través de un control de administración de claves común. Integrar la política de recuperación con una política de seguridad del sistema brinda un modelo de refuerzo de seguridad coherente. El subsistema de seguridad Windows se encarga de reforzar, replicar y mandar a la memoria *caché* la política EFS. Por lo tanto, los usuarios pueden utilizar la encriptación de archivos en un sistema que esté fuera de línea temporalmente, como una *laptop*, y también pueden registrar en su cuenta de dominio, utilizando credenciales con *caché*.

- **Utilidad de línea de comando EfsRecvr**—Permite que los agentes de recuperación puedan consultar claves de recuperación y recuperar un archivo encriptado, utilizando cualquiera de las claves de recuperación.

  Por ejemplo:

  - Para recuperar todos los archivos en el directorio Mis documentos, un agente de recuperación puede escribir:

    ```
    C:\>efsrecvr /s:"My Documents" *.*
    ```

  El comando ***efsrecvr*** soporta las opciones siguientes:

```
EFSRECVR [/S[:dir]] [/I] [/Q] [filename [...]]
/S    Performs the recovery on files in the given directory and all
subdirectories. Default "dir" is the current directory.
 /I    Continues performing recovery even after errors have occurred.
By default, EFSRECVR stops when an error is encountered.
 /Q    Reports only the most essential information including the list
of recovery key identifications to help the recovery agent load
appropriate keys.
 filename Specifies a pattern, file, or directory.
```

Recuperación de encriptación

El EFS requiere que se establezca una política de recuperación de datos en un nivel de dominio (o localmente si la computadora no es miembro de un dominio) antes de que se pueda utilizar el EFS. Los administradores de dominio establecen la política de recuperación de dominio (o el personal delegado conocido como agentes de recuperación), quienes controlan las claves de recuperación para todas las computadoras en dicho dominio.

Si un usuario pierde una clave privada, un archivo protegido por dicha clave se puede recuperar exportando el archivo y enviándolo por correo electrónico a uno de los agentes de recuperación. El agente de recuperación importa el archivo en una computadora segura con las claves de recuperación privadas y utiliza la herramienta de la línea de comandos de recuperación para desencriptar el archivo. Entonces el agente de recuperación regresa el archivo de texto al usuario. En ambientes de pequeñas empresas o en ambientes de hogar, en donde no hay dominios, la recuperación se puede realizar en la computadora autónoma misma.

ARQUITECTURA DEL EFS

Esta sección proporciona una breve descripción general de la arquitectura y técnica del EFS.

Criptografía

El EFS implementa la encriptación y desencriptación de datos, utilizando un esquema basado en clave pública. Los datos del archivo se encriptan utilizando un algoritmo simétrico rápido con la clave de encriptación de archivo (FEK). FEK es una clave generada aleatoriamente de una longitud determinada por el algoritmo o por ley, si el algoritmo soporta claves de longitud variable. Los problemas de exportación relacionados con el EFS se analizan en otro documento.

FEK se encripta utilizando una o más claves públicas de encriptación para generar una lista de las FEKs encriptadas. La parte pública de un par de claves de usuario se utiliza para encriptar las FEKs. La lista de las FEKs encriptadas se almacena junto con este archivo encriptado en un atributo EFS especial denominado Campo de desencriptación de datos (DDF). La información de encriptación de archivos está muy ligada al archivo. La parte privada del par de claves del usuario se utiliza durante la desencriptación. La FEK se desencripta utilizando la parte privada del par de claves. La parte privada de un par de claves de usuario se almacena de manera segura en otro lado, en tarjetas inteligentes o en otros dispositivos de almacenamiento seguros.

Nota: Una clave de usuario también puede encriptarse utilizando un algoritmo simétrico como una clave derivada de una contraseña. El EFS no soporta esto porque los esquemas basados en contraseñas son inherentemente débiles debido a su susceptibilidad a los ataques de diccionario.

Asimismo, la FEK se encripta utilizando una o más claves públicas de encriptación de clave. Una vez más, la parte pública de cada par de claves se utiliza para encriptar las FEKs. Esta lista de FEKs encriptadas también se almacena con el archivo en un atributo EFS especial denominado Campo de recuperación de datos (DRF). Sólo las partes públicas de los pares de claves de recuperación se necesitan para la encriptación de FEK en el DRF. Estas claves públicas de recuperación se requieren en todo momento en un sistema EFS para operaciones normales de sistema de archivo. La recuperación misma espera ser una operación rara, requerida sólo cuando los usuarios dejan las empresas o pierden las claves. Por esto, los agentes de recuperación pueden almacenar las partes privadas de las claves de manera segura en otro lado (en tarjetas inteligentes y en otros dispositivos de almacenamiento seguro).

El diagrama siguiente muestra los procesos de encriptación, desencriptación y recuperación.

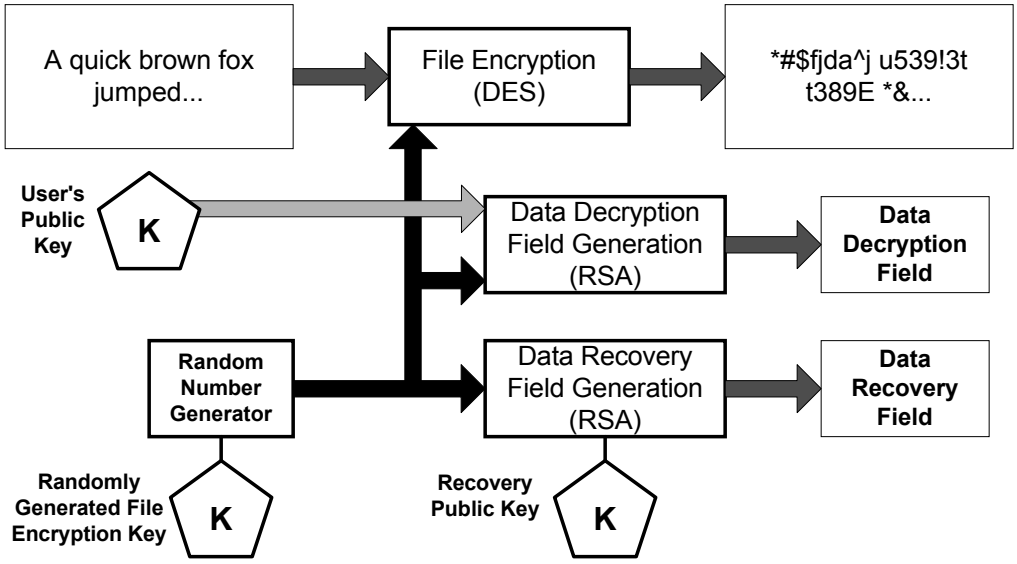


Figura 1. Proceso de encriptación de archivo

La Figura 1 muestra el proceso de encriptación. El archivo de texto del usuario se encripta utilizando una FEK generada de manera aleatoria. Esta clave de encriptación de archivo se almacena junto con el archivo encriptado bajo una clave pública de usuario en el DDF y encriptado bajo la clave pública del agente de recuperación en el DRF. **Nota:** La figura muestra sólo un usuario y un agente de recuperación, esto puede ser, de hecho, una lista de usuarios y una lista de agentes de recuperación con claves independientes. La primera versión de EFS soporta agentes de recuperación múltiples y usuarios únicos.

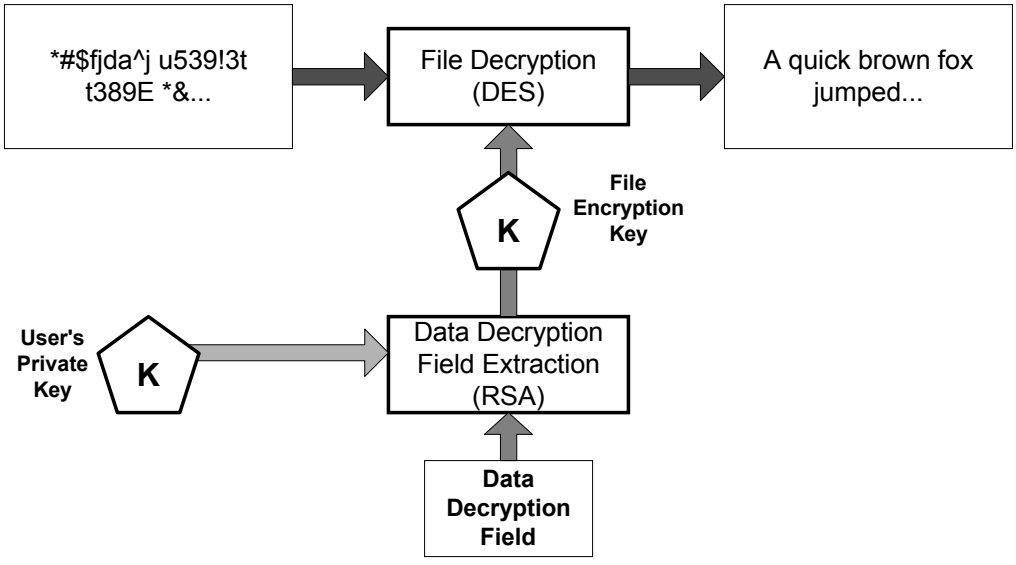


Figura 2. Proceso de desencriptación de archivos

La Figura 2 muestra el proceso de desencriptación. Una clave privada de usuario se utiliza para desencriptar la FEK, utilizando el elemento FEK encriptado

correspondiente en el DDF. La FEK se utiliza para desencriptar lecturas de datos de archivos por bloque. El acceso aleatorio a un archivo grande desencripta sólo la lectura de bloques específicos del disco para dicho archivo. El archivo completo no tiene que ser decriptado.

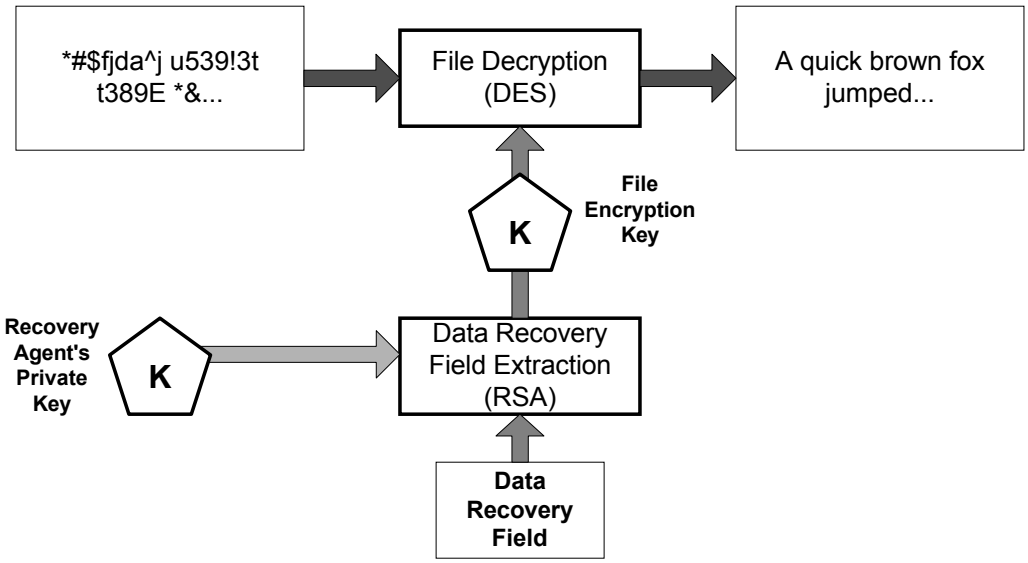


Figura 3. Proceso de recuperación de archivos

La Figura 3 muestra el proceso de recuperación. Es similar a la desencriptación, excepto que utiliza una clave privada de agente de recuperación para desencriptar la FEK en el DRF.

Este esquema simple brinda una tecnología de encriptación sólida y la capacidad de permitir a los usuarios múltiples compartir un archivo encriptado, además de proporcionar a diferentes agentes de recuperación la capacidad de recuperar el archivo, si así lo requieren. El esquema es un algoritmo completamente ágil y cualquier algoritmo criptográfico se puede utilizar en las diferentes fases de encriptación. Esto será muy importante a medida que se inventen nuevos y mejores algoritmos.

Implementación

La arquitectura del EFS se muestra en la Figura 4, a continuación.

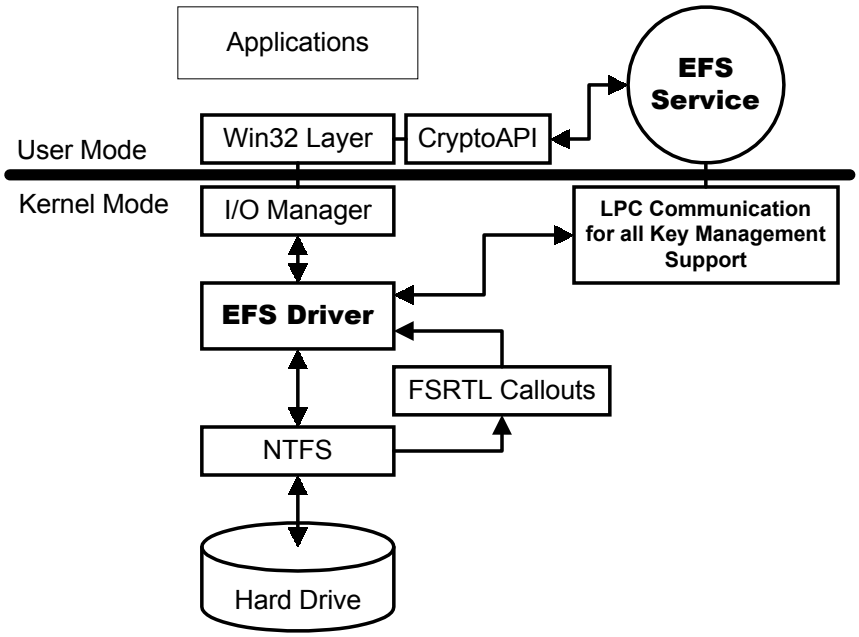


Figura 4: Arquitectura de EFS

El EFS consta de los siguientes componentes en el sistema operativo Windows 2000:

- **Controlador de EFS.** El controlador del EFS se encuentra en la parte superior del NTFS. Se comunica con el servicio del EFS para solicitar las claves de encriptación de archivos, DDF, DRF y demás servicios de administración clave. Pasa esta información a la biblioteca de tiempo de ejecución del sistema de archivo EFS (FSRTL) para realizar diversas operaciones del sistema de archivos (abrir, leer, escribir y anexar) de manera transparente.
- **FSRTL de EFS.** FSRTL es un módulo dentro del controlador EFS que implementa *callouts* NTFS para manejar diversas operaciones del sistema de archivos, como lectura, escritura y apertura en los archivos y directorios encriptados, además de operaciones para encriptar, desencriptar y recuperar datos de archivos cuando se escribe o lee desde el disco. Aún cuando el controlador EFS y la FSRTL se implementan como un solo componente, nunca se comunican directamente. Utilizan el mecanismo de *callout* de control de archivo NTFS para pasar mensajes de uno a otro. Esto asegura que el NTFS participe en todas las operaciones de archivo. Las operaciones implementadas utilizando los mecanismos de control de archivo incluyen escribir los datos de atributo EFS (DDF y DRF) como atributos de archivos y comunicar la FEK calculada en el servicio de EFS para la FSRTL, de manera que se pueda establecer en el contexto del archivo abierto. Este contexto de archivo se utiliza entonces para una encriptación y desencriptación transparente en escrituras y lecturas de datos de archivo del disco.
- **Servicio de EFS.** El servicio de EFS es parte del subsistema de seguridad. Utiliza el puerto de comunicación LPC existente entre la Autoridad de seguridad local (LSA) y el monitor de referencia de seguridad de modo *kernel*

para comunicarse con el controlador EFS. En el modo de usuario hace interfaz con CryptoAPI para brindar claves de encriptación de archivos y generar DDF y DRF. Además, el servicio EFS brinda soporte para *Win32® API* para encriptación, desencriptación, recuperación, importación y exportación.

- **APIs Win32.** Brindan interfaces de programación para encriptar archivos de texto, desencriptar o recuperar archivos de texto *cipher* e importar y exportar archivos encriptados (sin desencriptarlos primero). Estas APIs se soportan en un sistema estándar DLL, Advapi32.dll.

TEMAS DE EXPORTACION CON EFS

El EFS brinda recuperación de datos a agentes de recuperación autorizados. La arquitectura de recuperación de datos es parte del esfuerzo de Microsoft para cumplir con las reglas de la política actual para exportar encriptación y brindar encriptación más sólida que 40 bits para nuestros clientes internacionales. Enfocándose en este esfuerzo, el EFS utiliza el algoritmo de encriptación DES estándar que se basa en una clave de encriptación de 56 bits. El EFS está diseñado para soportar diferentes algoritmos de encriptación con fuerzas clave variantes para futuras mejoras.

Actualmente, Microsoft está trabajando con el gobierno de Estados Unidos para obtener la aprobación de exportación del EFS con DES de 56 bits como el algoritmo de encriptación de archivos. Mientras se realiza este proceso de revisión, Microsoft tendrá el EFS disponible para nuestros clientes internacionales en una implementación DES de 40 bits como el algoritmo de encriptación de archivos. Los productos Windows para el mercado estadounidense utilizan la encriptación DES de 56 bits estándar. Los archivos encriptados que utilizan la versión de 40 bits de EFS se pueden importar en versiones EFS que soportan DES de 56 bits. No obstante, los archivos encriptados que utilizan la versión de EFS de 56 bits no se pueden importar a versiones EFS restringidas a DES de 40 bits, para asegurar que se satisfagan las reglas de exportación de Estados Unidos. En el futuro, cuando las reglas permitan exportar una criptografía más fuerte, los clientes a nivel mundial podrán migrar de manera clara y utilizar algoritmos de encriptación con EFS nuevos y más fuertes.

CONCLUSION

EFS en Windows 2000 proporciona a los usuarios la capacidad de encriptar archivos NTFS individuales, además de directorios completos, utilizando un esquema criptográfico basado en una sólida clave pública.

- EFS soporta la encriptación de archivos remotos accesibles a través de compartir archivos.
- EFS brinda a las empresas la capacidad de establecer políticas de recuperación de datos, de manera que los datos encriptados se puedan recuperar cuando se requiera, utilizando EFS.
- La política de recuperación se integra con la política global de Seguridad de Windows. El control de esta política se puede delegar a personas con autoridad de recuperación.
- La recuperación de datos en EFS es una operación contenida. Sólo descubre los datos recuperados, no la clave de usuario individual que se utilizó para encriptar el archivo.
- La encriptación de archivos mediante el EFS no requiere que los usuarios desencripten o reencripten el archivo en cada uso. La desencriptación y encriptación sucede de manera transparente en la lectura y escritura de archivos en los discos.
- EFS soporta funciones de exportación e importación que permiten el respaldo, restablecimiento y transferencia de archivos encriptados sin desencriptación.
- EFS se integra con el sistema operativo, de manera que detiene las fugas de información clave en archivos de búsqueda y asegura que todas las copias temporales de archivos encriptados también se encripten.
- La versión estadounidense del EFS utiliza el DES como el algoritmo de encriptación de archivos con entropía clave completa de 56 bits. La versión internacional de EFS también utiliza DES como algoritmo de encriptación; no obstante, la clave de encriptación de archivo se reduce a tener sólo entropía clave de 40 bits.

Para mayores informes

Para la información más reciente sobre Windows 2000 y Windows NT Server, visite el sitio Web en http://www.microsoft.com/ntserver o Windows NT Server Forum en Microsoft Network (GO WORD: MSNTS).