(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 388 421**

(51) Int. CI.:
H04L 9/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **10197119 .0**
(96) Fecha de presentación: **28.12.2010**
(97) Número de publicación de la solicitud: **2341657**
(97) Fecha de publicación de la solicitud: **06.07.2011**

(54) Título: **Método para controlar el acceso a datos digitales cifrados**

(30) Prioridad:
29.12.2009 IT MI20092326

(45) Fecha de publicación de la mención BOPI:
15.10.2012

(45) Fecha de la publicación del folleto de la patente:
15.10.2012

(73) Titular/es:
Antares S.r.l.
Via A. Volta, 94
20033 Desio, IT

(72) Inventor/es:
Corradi, Vincenzo

(74) Agente/Representante:
Sugrañes Moliné, Pedro

DESCRIPCIÓN

Método para controlar el acceso a datos digitales cifrados

Campo de la invención

La presente invención se refiere a un método para controlar el acceso a datos digitales cifrados contenidos en un medio de almacenamiento.

Se conoce que, en el sector técnico relacionado con la gestión de datos por medio de ordenadores, existe la necesidad de usar sistemas para registrar el acceso por los administradores del sistema a los datos almacenados en el ordenador, con el fin de evitar una manipulación aleatoria y/o fraudulenta.

En particular, estos sistemas de registro deben tener las características de ser completos, no modificables y adecuados para permitir la verificación de su integridad.

También se conoce a partir de “Key Management in an Encrypting File System” por Matt Blaze (AT&T Laboratories) y “Put Your Syslog Messages in a Database Over the Network” por Martin Ben (LINUXFOUNDATION.ORG) que han desarrollado sistemas de seguridad, basándose estos sistemas, por ejemplo, en el uso de claves para acceder a dichos datos que se distribuyen a varias personas dentro de una empresa autorizada para guardar dichas claves; estos procedimientos, sin embargo, no son adecuados para los objetos definidos anteriormente puesto que la ocultación de un posible acto ilícito puede ser en el interés de la propia empresa y, por tanto, dar como resultado que todos los miembros de dicha empresa estén implicados en la defensa de un interés común y/o estar aconsejados para actuar según reglas definidas especialmente. Asimismo, es inaceptable que cualquier tercera parte (compañías de software, consultores, ingenieros de instalación, etc.) que se llama para implementar un software dedicado pueda tener conocimiento de estos procedimientos y posea las claves para acceder a los mismos con la posibilidad de manipular los datos; la relación económica entre cliente y proveedor puede dar como resultado, de hecho, la estipulación de acuerdos que violan la ley.

Una solución conocida adicional es que cuando la empresa se compromete a llevar a cabo diariamente el guardar todos los datos clasificados como no modificables en un medio óptico no reescribible; este procedimiento, sin embargo, da lugar a un problema adicional asociado con una operación diaria realizada por personas que, antes de guardar los datos, podrían modificar de manera inapropiada dichos datos y generar un gran número de discos que a su vez crean problemas y costes adicionales que surgen a partir de la necesidad de mantenimiento, certificación de autenticidad y almacenamiento de los mismos; además, no es posible impedir el acceso a cualquier dato almacenado sensible por custodios no autorizados, cuando se requiera.

El problema técnico que se plantea, por tanto, debe desarrollar un procedimiento que garantice, por un lado, la imposibilidad efectiva de modificar datos contenidos en los archivos, carpetas o discos completos por cualquier usuario dentro o fuera de la empresa, que tiene acceso a dichos datos y, por otro lado, que el procedimiento sea tal que el acceso a los datos cifrados originales para cualquier comprobación se restrinja exclusivamente a un organismo de inspección autorizado y que este acceso debe ser de naturaleza totalmente automática, es decir, sin ninguna intervención humana durante cualquier fase de dicha operación.

En relación con este problema también se requiere que este método debe ser fácil y barato de instalar en cualquier instalación de usuario a través de medios de acceso de sistemas informáticos normales.

Estos resultados se logran según la presente invención mediante un método para controlar el acceso a datos digitales cifrados según los rasgos característicos de la reivindicación 1.

Pueden obtenerse detalles adicionales a partir de la siguiente descripción de un ejemplo no limitativo de realización de un método según la presente invención, en el que los términos a continuación se entienden como que tienen el siguiente significado:

USUARIO

Persona física o persona jurídica, propietaria del ordenador en el que se almacenan los datos cifrados o datos que van a cifrarse;

CUSTODIO

Persona física o persona jurídica (notario o similar), independiente del USUARIO y autorizada para tener la custodia de las claves de descifrado;

ORGANISMO DE INSPECCIÓN

Persona física o persona jurídica (policía postal, policía financiera, juez o similares) independientes del USUARIO y el CUSTODIO y exclusivamente con el poder para solicitar y/o autorizar la retirada de la clave privada del CUSTODIO;

INGENIERO DE INSTALACIÓN

Persona física o persona jurídica que tiene la experiencia técnica y de procedimiento para gestionar el traspaso/retirada de la clave privada para el descifrado a petición del ORGANISMO DE INSPECCIÓN y para activar en las instalaciones del USUARIO los procedimientos para cifrar y descifrar los datos. Con estas definiciones el método comprende las siguientes etapas:

a) ejecutar operaciones preliminares realizadas por el INGENIERO DE INSTALACIÓN;

b) traspasar y recuperar la clave a/desde el CUSTODIO

c) ejecutar operaciones en las instalaciones del USUARIO

d) descifrar, lo que puede realizarse únicamente por el ORGANISMO DE INSPECCIÓN

En mayor detalle:

a) Operaciones preliminares llevadas a cabo por el INGENIERO DE INSTALACIÓN

a1) creación de las claves de cifrado/descifrado;

durante esta etapa se crean los siguientes:

- una clave de cifrado, denominada clave pública, por medio de la que los propietarios pueden realizar el cifrado de los archivos disponibles en texto plano; y

- una clave de descifrado, denominada clave privada, por medio de la que el único poseedor puede realizar el descifrado de los archivos; durante la creación de la clave privada se asigna un número de serie único a la clave para los fines de identificación de la misma;

las claves pública y privada pueden ser únicas en el sentido de que se crea un único par de las mismas válido para todos los usuarios, previéndose que se realice la habilitación del acceso/el descifrado únicamente en presencia de ambas claves, una de las cuales (clave privada), sin embargo, nunca es accesible para el USUARIO, como quedará más claro a continuación;

a2) creación de un medio físico para almacenar la clave privada;

durante esta etapa se usa una tarjeta inteligente o un testigo como medio físico para la clave privada que se escribe en el propio el dispositivo, dotándose dicho dispositivo de un microprocesador útil para adquirir automáticamente y almacenar información relacionada con la fecha cuando la clave privada se usó la última vez y toda aquella información que pueda certificar la gestión correcta del dispositivo limitada a las ocasiones reales previstas por el procedimiento y descritas a continuación;

a3) verificación e impresión del número de serie, que puede leerse por medio del programa de descifrado en el momento de la retirada/traspaso de la clave privada, de modo que las partes implicadas en el traspaso/la retirada del medio pueden comprobar que la clave no se ha cambiado;

a4) creación de un diario de registro para almacenar los datos (número de serie, fecha y hora, persona que efectúa la retirada) relacionados con el traspaso/la retirada del medio físico, de modo que pueda llevarse a cabo una comprobación cruzada de los datos de usuario de clave privada almacenados en el microprocesador del medio físico con los datos contenidos en el diario de registro mencionado anteriormente;

durante esta etapa y tras realizar las comprobaciones operativas necesarias,

a5) la tarjeta inteligente o testigo con, adjunta, la contraseña para proteger los archivos de instrucciones contenidos en el archivo de descifrado se inserta dentro de un sobre que contiene también: la impresión del número de serie verificado y firmado por el CUSTODIO tras una comprobación llevada a cabo *in situ*, los datos de referencia del

INGENIERO DE INSTALACIÓN y la indicación de que el sobre puede entregarse sólo al ORGANISMO DE INSPECCIÓN o a la persona indicada por ellos, mostrado en diario de entregas todas las operaciones de retirada y depósito que permanecerán durante toda la vida de la clave.

b) Traspaso de la clave privada al CUSTODIO

El INGENIERO DE INSTALACIÓN puede no entregar el sobre al CUSTODIO, por ejemplo un notario u organismo de certificación, cuyos datos se almacenarán en texto plano en el archivo de texto contenido en una carpeta de descifrado presente en las instalaciones de cada USUARIO.

Durante el depósito inicial, se rellenará la primera línea en el diario de registro, certificando por tanto oficialmente el traspaso de la clave y la activación del procedimiento.

c) Operaciones realizadas en las instalaciones del USUARIO

c1) La instalación de cualquier programa de aplicación dedicado para la recogida y centralización de los archivos que van a procesarse posteriormente

Durante esta etapa, el INGENIERO DE INSTALACIÓN instala en el ordenador que contiene los datos que van a protegerse, o en uno de los ordenadores conectados al mismo en una red, de modo que pueda en cualquier caso gestionarse los datos mencionados anteriormente, los programas que tienen la función de recoger los archivos que van a someterse al procedimiento y enviarlos a la unidad designada para el procesamiento de cifrado;

c2) Creación de una carpeta que contiene los archivos requeridos para el descifrado

La carpeta está protegida por medio de cifrado simétrico y es accesible por medio de una contraseña adjunta en texto plano en el sobre que contiene el medio físico en el que se registra la clave privada y guardado por el CUSTODIO.

La carpeta de descifrado contiene en particular un archivo en texto plano y cuatro archivos protegidos por una contraseña, concretamente:

-) un archivo de instrucciones en texto plano para activar el procedimiento para acceder a los datos cifrados;

-) un archivo protegido que contiene las instrucciones reservadas para el ORGANISMO DE INSPECCIÓN;

-) un archivo protegido que contiene una primera aplicación propietaria que permite la identificación, mediante el programa de descifrado, de los archivos que contienen los datos;

-) un archivo protegido que contiene una aplicación propietaria que procesa los archivos de datos cifrados, convirtiéndolos de la condición en la que pueden identificarse mediante los programas de descifrado a la condición anterior en la que no pueden identificarse mediante dichos programas;

-) un archivo protegido que puede instalar un controlador para la lectura de la clave privada por el ORGANISMO DE INSPECCIÓN que autoriza el programa de descifrado;

c3) Cifrado de los archivos que van a protegerse

Tras el traspaso inicial del medio físico que contiene la clave privada al CUSTODIO que garantiza que la clave privada se hace inaccesible a terceras partes, es posible iniciar la etapa para el cifrado de los datos en texto plano en las instalaciones del USUARIO o USUARIOS;

durante esta etapa:

- se activa un programa de cifrado, que carga los archivos que van a cifrarse y que genera en segundo plano, es decir sin ninguna acción por parte del operario, una copia cifrada de los mismos, guardando el original en texto plano para la libre consulta, o que los elimina cuando también se requiere que los datos almacenados no deban poder consultarse; se genera la copia cifrada usando algoritmos de impenetrabilidad probada, usando, respectivamente, como clave de cifrado y clave de descifrado, la clave pública y clave privada generadas durante la etapa a);

d) Operaciones de descifrado que pueden realizarse únicamente por el ORGANISMO DE INSPECCIÓN

Si es necesario, y únicamente a petición de un ORGANISMO DE INSPECCIÓN, iniciación del procedimiento para

acceder a los datos cifrados y para el descifrado automático.

Si se requiere el acceso a los datos cifrados por el ORGANISMO DE INSPECCIÓN para el análisis de los mismos, el método prevé las siguientes etapas:

d1) Acceso al ordenador que va a inspeccionarse por el ORGANISMO DE INSPECCIÓN y apertura del archivo de texto que se genera inicialmente en texto plano en el servidor de recogida y que contiene una instrucción para ponerse en contacto con el INGENIERO DE INSTALACIÓN con el fin de obtener la posesión de la contraseña de modo que se abran los archivos que están cifrados de forma sencilla; la carpeta está, de hecho, en texto plano, pero los archivos de soporte contenidos en la misma están cifrados y sólo pueden abrirse por medio de una contraseña suministrada verbalmente por el INGENIERO DE INSTALACIÓN;

entretanto, con el fin de proteger el almacenamiento físico de los datos cifrados, la persona designada para llevar a cabo la comprobación será responsable de extraer dichos archivos, almacenarlos en un medio asociado por medio de una medida de seguridad sencilla de modo que, en el caso de un acto fraudulento conocido, dichos archivos no se borren de los registros internos del USUARIO que esté verificándose. Los archivos extraídos no serán legibles en ningún caso hasta que la clave privada esté físicamente en la posesión del organismo autorizado.

d2) presentación de la autorización al CUSTODIO y retirada del medio físico que contiene la clave privada;

d3) registro, en el diario que registra las operaciones de traspaso/retirada, de lo siguiente: número de serie de la clave privada, fecha y hora de retirada; datos del ORGANISMO DE INSPECCIÓN que efectúa la retirada y, cuando esté permitido por las leyes de privacidad, el nombre del USUARIO que esté verificándose.

d4) acceso del ORGANISMO DE INSPECCIÓN al ordenador que contiene los archivos que van a verificarse e inserción de la clave privada en un lector correspondiente;

d5) verificación de que los datos almacenados en la memoria de la tarjeta inteligente o testigo, recogidos automáticamente y relacionados con la última operación de acceso coinciden con los datos contenidos en el diario que registra las operaciones de acceso;

d6) registro automático, realizado por la tarjeta inteligente, del último acceso;

d7) iniciación del procedimiento para el descifrado a través de las instrucciones y los programas contenidos en la carpeta de descifrado;

d8) extracción del medio físico y por tanto de la clave privada.

Al final de la inspección realizada en las instalaciones del USUARIO, se extraerá la clave privada, se desinstalará el programa de descifrado y se cerrará de nuevo la carpeta que contiene todos los datos, usando la contraseña de texto plano.

La generación de los archivos almacenados cifrados entretanto no se ha interrumpido y el sistema continúa operando automáticamente;

d9) devolución de la clave privada al CUSTODIO tras la identificación previa del mismo y registro del traspaso en el diario de registro de accesos usando los mismos procedimientos operativos que los usados para la retirada.

Entretanto, con el fin de proteger el almacenamiento físico de los archivos que están ahora descifrados y, por tanto, legibles en texto plano, la persona designada para realizar la verificación será responsable de extraer los mismos, almacenándolos en un medio asociado de modo que estén disponibles para las operaciones de inspección necesarias.

Por tanto, queda claro cómo prevé el método según la invención como medidas esenciales para garantizar que no puede accederse a los datos cifrados por personas que podrían estar decididas a manipularlos:

-) custodia del medio físico que contiene la clave privada por un CUSTODIO neutro;

-) identificación de un solo ORGANISMO DE INSPECCIÓN autorizado legalmente para recuperar la clave privada;

-) la necesidad de una autorización emitida por el ORGANISMO DE INSPECCIÓN para obtener el traspaso del medio físico que contiene la clave privada;

-) el registro simultáneo, en el medio físico, de la clave privada y en un diario de registro separado guardado por el ORGANISMO DE INSPECCIÓN, de los datos relacionados con la secuencia de operaciones para acceder a los datos cifrados;

garantizando esto que la posesión de la tarjeta inteligente o testigo para el descifrado de los archivos de diario no puede transferirse en modo alguno, restringiéndose dicha posesión exclusivamente al ORGANISMO DE INSPECCIÓN.

Además de la generación del par de claves pública y privada que permiten el acceso sólo si se usan en pares y la posesión exclusiva de la clave privada por un CUSTODIO tal como se describió anteriormente, puede generarse un único par de claves que pueden usarse para una pluralidad de USUARIOS diferentes, de modo que es posible garantizar la custodia y disponibilidad de una única clave privada que activa el procedimiento de inspección cuando se usa junto con la clave pública en posesión de cada USUARIO.

Debido a las características intrínsecas de inviolabilidad ofrecidas por el procedimiento, incluso en el caso de un robo en que está implicado el CUSTODIO o la destrucción de la clave privada, los archivos cifrados, durante el periodo de almacenamiento mínimo estipulado por los reglamentos, será completamente inutilizable.

Es posible, sin embargo, realizar el cifrado paralelo de los mismos datos, cuya custodia se asigna a un CUSTODIO diferente y remoto del CUSTODIO que salvaguarda el primer cifrado. La imposibilidad de poder interpretar los datos cifrados gestionados por la primera clave se compensará por el posible descifrado del archivo duplicado.

Una clave privada perdida ocasionalmente y el medio asociado se regenerarán y a partir de ese momento y en adelante se reactivará el procedimiento de alta fiabilidad.

Aunque se ha descrito con relación a determinadas formas de construcción y determinados ejemplos preferidos de realización de la invención, se entiende que el alcance de protección de la presente patente está definido únicamente por las siguientes reivindicaciones.

REIVINDICACIONES

1. Método para controlar el acceso a datos digitales cifrados guardados en un medio de almacenamiento de un USUARIO, que comprende las siguientes etapas:

a1) crear una clave de cifrado pública y una clave de descifrado privada;

a2) almacenar de manera cifrada la clave de descifrado privada en un medio físico;

a3) asignar un número de serie único que identifica la clave de descifrado privada en el momento en que se crea;

a4) crear un diario para registrar las operaciones para el traspaso/retirada del medio físico;

a5) depositar la clave de descifrado privada con un CUSTODIO externo e independiente;

b1) instalar programas de aplicación dedicados para el cifrado de los datos en un ordenador disponible en las instalaciones del USUARIO;

b2) crear, en las instalaciones del USUARIO, una carpeta que contiene programas de descifrado dedicados;

c) iniciar, en las instalaciones del USUARIO, el procedimiento automático para el cifrado de archivos por medio de programas de cifrado, usando la clave de cifrado pública y la clave de descifrado privada generadas durante la etapa a1) como clave de cifrado y clave de descifrado, respectivamente;

d) acceder un ORGANISMO DE INSPECCIÓN al ordenador que va a inspeccionarse;

e) iniciar el procedimiento de descifrado automático;

caracterizado porque comprende las etapas adicionales, de:

d1) solicitar, por el ORGANISMO DE INSPECCIÓN, la verificación en las instalaciones del USUARIO;

d2) emitir, por el ORGANISMO DE INSPECCIÓN, una autorización para la retirada de la clave de descifrado privada;

d3) solicitar la liberación de la clave de descifrado privada por el CUSTODIO con la presentación de la petición recibida desde el ORGANISMO DE INSPECCIÓN y la consiguiente compilación del diario que registra las operaciones para el acceso a los datos cifrados;

d4) traspasar la clave de descifrado privada al ORGANISMO DE INSPECCIÓN autorizado, tras la verificación del número de serie de la clave de descifrado privada

e implicando las etapas de descifrado adicionalmente:

e1) comprobar por el ORGANISMO DE INSPECCIÓN que los datos contenido en el medio físico de la clave de descifrado privada coinciden con los datos contenidos en el diario de registro;

e2) registrar la nueva operación de acceso en el medio físico de la clave de descifrado privada insertada durante el acceso de los datos cifrados;

e3) abrir los archivos para el descifrado de los datos cifrados y descifrar los mismos;

e4) extraer la clave de descifrado privada y cerrar los archivos de soporte usados para implementar el procedimiento;

e5) devolver el medio físico al CUSTODIO con verificación renovada del número de serie de la clave de descifrado privada y registrar los datos relacionados con el traspaso en el diario de registro.

2. Método según la reivindicación 1, caracterizado porque el medio físico para almacenar la clave de descifrado privada es una tarjeta inteligente o un testigo.

3. Método según la reivindicación 1, caracterizado porque dicha carpeta de descifrado contiene al menos:

un archivo en texto plano y cuatro archivos protegidos por una contraseña y, respectivamente:

-) un archivo de instrucciones en texto plano para activar el procedimiento para acceder a los datos cifrados;

-) un archivo protegido que contiene las instrucciones reservadas para el ORGANISMO DE INSPECCIÓN;

-) un archivo protegido que contiene una primera aplicación propietaria que permite la identificación, mediante el programa de descifrado, de los archivos que contienen los datos;

-) un archivo protegido que contiene una aplicación propietaria que procesa los archivos de datos cifrados, convirtiéndolos de la condición en la que pueden identificarse mediante los programas de descifrado a la condición anterior en la que no pueden identificarse mediante dichos programas;

-) un archivo protegido que puede instalar un controlador para la lectura de la clave privada por el ORGANISMO DE INSPECCIÓN que autoriza el programa de descifrado.

4. Método según la reivindicación 1, caracterizado porque el procedimiento de cifrado se realiza en modo en segundo plano.