(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 782 329**

(51) Int. CI.:

G06F 21/00 (2013.01)
G06F 21/10 (2013.01)
H04L 29/06 (2006.01)
H04L 29/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **22.09.2009 E 09368032 (0)**

(97) Fecha y número de publicación de la concesión europea: **26.02.2020 EP 2309407**

(54) Título: **Proceso para asegurar la comunicación de un archivo digital a través de una red de comunicación**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
14.09.2020

(73) Titular/es:

AMADEUS S.A.S. (100.0%)
485 Route du Pin Montard, Sophia Antipolis
06410 Biot , FR

(72) Inventor/es:

MATHIEU, ERIC y
FRENKIEL, MICHEL

(74) Agente/Representante:

ELZABURU, S.L.P

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

DESCRIPCIÓN

Proceso para asegurar la comunicación de un archivo digital a través de una red de comunicación

Campo técnico de la invención

La invención se refiere a telecomunicaciones y más particularmente a un proceso para asegurar la comunicación de un archivo digital a través de una red de comunicación.

Técnica anterior

La red de Internet ha facilitado drásticamente la comunicación de archivos y documentos digitales, ya sea video, audio o texto básico o archivos de procesamiento de texto. Tal facilidad en la comunicación de los archivos digitales ha aumentado significativamente la necesidad de proporcionar una protección apropiada de la información contenida en ellos, ya sea material comercial con derechos de autor o más simplemente información confidencial que debería estar restringida solo a usuarios autorizados.

Claramente, la necesidad de asegurar la comunicación de documentos digitales transmitidos a través de una red de comunicación, tal como la red de Internet, aumenta constantemente con el progreso continuo de los equipos de telecomunicaciones.

Existen algunas técnicas de la técnica anterior para mejorar la seguridad en las comunicaciones de archivos digitales.

Una primera técnica conocida está basada en la utilización de un mecanismo de cifrado, ya sea basado en una clave simétrica (es decir, siendo utilizada una misma clave tanto para el cifrado como para el descifrado) o en una clave asimétrica (tal como de la RSA - Rivest-Shamir et Adleman) que utiliza dos claves públicas-privadas distintivas para el mecanismo de cifrado y descifrado). Si bien tal técnica muestra eficiencia, particularmente con el desarrollo constante de los algoritmos de cifrado, la seguridad depende claramente del estado confidencial asignado a la clave de descifrado y la protección cesa con la pérdida de la confidencialidad de esta última.

Otra solución conocida que se conoce en la técnica está más adaptada a la protección de materiales con derechos de autor, tales como archivos de video y audio, y está basada en los mecanismos conocidos de Gestión de Derechos Digitales (DRM). La protección de los archivos protegidos con derechos de autor es conseguida por medio del cifrado, antes de su transmisión a un usuario, de un documento digital con una información que identifica de forma exclusiva a dicho usuario (p. ej., la dirección MAC de este último), para evitar el uso del documento en el sistema que pertenece a otro usuario. Si tal solución demuestra ser una mejora significativa en la protección de una información digital que ha de ser reenviada a través de una red, solo proporciona flexibilidad limitada para manejar una amplia cantidad de situaciones, abarcando diferentes categorías de usuarios, diferentes derechos de uso que han de ser asignados al documento digital que ha de ser protegido.

Se conoce otra técnica de la técnica anterior bajo la designación de Adobe LiveCycle, que es un software para asegurar documentos PDF. Véase (www.adobe.com/security/pdfs/acrobat_security_wp.pdf). Esta solución conocida integra el cifrado de los archivos intercambiados dentro de una empresa y las claves de administración. Los Derechos de Uso también se administran utilizando la seguridad nativa de los documentos. Con Adobe, el documento es cifrado de una vez por todas utilizando una clave de cifrado. Esta clave es comunicada a cada usuario del documento, cifrada con el receptor. Este mecanismo tiene dos inconvenientes principales:

- Cada parte interesada debe poseer un par de claves dentro de una PKI aceptada por los aceptables dentro de una empresa pero que no se ajusta a las necesidades de Internet;

- El documento cifrado con la misma clave simétrica es enviado a todos los clientes. El anonimato facilita la difusión adicional no deseada del documento, el control apropiado sobre la gestión del ciclo de vida de la información.

El documento EP1669833 presentado por la Solicitante de la presente solicitud describe otra solución de la técnica anterior que aumenta significativamente la seguridad de una transacción basada en la generación, durante un primer procedimiento de calificación, de un Archivo de Calificación del Sistema (SQF), que es utilizado para generar una Firma de Calificación de Referencia (RQS) que puede ser utilizada, durante un segundo procedimiento de validación, con el propósito de asegurar una transacción.

Un aspecto importante de la solicitud de patente europea mencionada anteriormente se deriva del hecho de que los datos informados al Sistema Operativo (OS) – ya sea Windows (de Microsoft Corp.) o Linux o similar, por los diferentes componentes que componen los sistemas (componentes internos como el tamaño de la memoria y la estructura física, el número de serie del procesador, ... componentes externos como dispositivos “plug and play” o PnP (en español “enchufar, conectar y usar”) como claves USB, monitor, ratón, teclado ... o incluso elementos pasivos tales como una impresora o un CDROM. ... véase EP1669833), es utilizado sistemáticamente con el propósito de generar un Archivo de Calificación del Sistema completo que comprende tantos parámetros y variables que pueden ser utilizados para identificar de forma exclusiva el sistema particular que solicita una transacción. Esta técnica, que ha demostrado ser muy efectiva, está ahora designada comercialmente por la Solicitante con el nombre de "El ADN Digital".

Sin embargo, la técnica que se ha descrito en la solicitud de patente Europea mencionada anteriormente no está totalmente adaptada para asegurar la descarga de un archivo digital protegido por derechos de autor o confidencial, y particularmente para gestionar los diferentes derechos de uso o restricciones asociados con el archivo digital que ha de ser protegido.

En tal situación, los procedimientos de calificación y verificación muy generales descritos por la patente Europea mencionada anteriormente tienen que ser adaptados y mejorados con el fin de proporcionar una solución completa y poderosa que permita la protección de los archivos digitales que son descargados a través de una red de comunicación, ya sea un audio, un video o el bien conocido Archivo de Documento Portátil básico generado por el software Adobe Acrobat comercializado por Adobe Inc. La solicitud de patente internacional WO 01/79971 es otra técnica anterior.

En términos más generales, existe la necesidad de una solución mejorada para generalizar la descarga de materiales comerciales o con derechos de autor, mientras que proporciona una protección fácil y justa a los propietarios de los derechos de autor.

Este es el problema técnico que ha de ser resuelto por la presente invención.

Compendio de la invención

Es un objeto de la presente invención mejorar la seguridad en el acceso de un Sistema de Manejo de Información (I.H.S.), y particularmente mejorar el acceso a un archivo para ser descargado desde un servidor distante en un sistema local.

Es otro objeto de la presente invención proporcionar un proceso que mejore la protección de material protegido por derechos de autor, tales como archivos de video o audio, para impedir el uso no autorizado de este último en un sistema genérico.

Es un objeto adicional de la presente invención proporcionar un proceso que mejore la protección que ha de ser llevada a un archivo que contiene información sensible y confidencial, impidiendo el acceso no autorizado a dicha información.

Es todavía otro objeto de la presente invención conseguir un proceso para comunicar un documento digital en donde la comunicación de dicho archivo está asociada con la comunicación de propiedades apropiadas que están protegidas apropiadamente contra usos no autorizados.

Es un objeto adicional de la presente invención proporcionar un poderoso mecanismo de cifrado que utiliza la configuración contextual de una máquina IHS para conseguir la protección apropiada de la pareja de información-propiedades de un documento descargado.

Es todavía otro objeto proporcionar un mecanismo seguro para descargar un archivo confidencial o protegido por derechos de autor y permitir que el propietario de dicho documento autentique la apertura de dicho archivo en un entorno seguro.

Es un objetivo adicional proporcionar un mecanismo mejorado que consiga un control efectivo de documentos en archivos protegidos por derechos de autor o confidenciales que son descargados a través de una intranet o de la red de Internet.

Estos y otros objetos mediante el proceso para comunicar un archivo digital (D1) desde un servidor a un Sistema de Manejo de Información (IHS), comprendiendo el IHS un conjunto de componentes de hardware y software operados por un Sistema Operativo (OS) a través de controladores.

El proceso implica las operaciones de:

- iniciar un procedimiento de detección del sistema con el propósito de recopilar datos de dichos componentes a través de dichos controladores e informar a dicho OS;

- generar un archivo de descripción del sistema a partir de parte o de la totalidad de los datos recopilados de dicho procedimiento de detección del sistema;

- cifrar parte o la totalidad de dicho archivo de descripción del sistema con el fin de generar una Firma digital de Autenticación (ADS);

Además, el proceso está caracterizado por que implica además las operaciones de:

- utilizar dicha Firma Digital de Autenticación (ADS) para derivar una clave de cifrado/descifrado (K1);

- utilizar dicha clave para cifrar un archivo que ha de ser descargado o para descifrar un archivo cifrado previamente descargado.

La utilización de la Firma Digital de Autenticación (ADS) para generar una clave de cifrado/descifrado es particularmente ventajosa ya que permite la posibilidad de aprovechar las funcionalidades proporcionadas por los algoritmos de

cifrado/descifrado.

En particular, ya no es necesario realizar ninguna comparación entre dos firmas, una firma actual y una firma de referencia como en la solicitud de patente Europea mencionada anteriormente, aumentando así de manera significativa el nivel de seguridad del proceso.

Más particularmente, con la invención, ni si quiera será necesario comunicar la clave al cliente, una vez que la Firma Digital de Autenticación (ADS) ha sido almacenada en una base de datos, tal como una base de datos de derechos de uso.

En una realización, la clave (K1) se deriva de dicha ADS a través de un mecanismo de “hashing” (generar un valor o valores a partir de una cadena de texto utilizando una función matemática).

Preferiblemente, la clave (K1) es utilizada para generar un archivo agregado F1 que comprende la siguiente información: X1, S1 y H1:

En donde:

X1: comprende el documento D1 que ha de ser descargado, cifrado con dicha clave K1;

comprendiendo S1 un primer campo no cifrado (PS1) y un segundo campo pS1 cifrado con dicha clave K1.

H1: es un hash de X1, S1

En una realización, el archivo descargado es un archivo de texto, un archivo PDF, un archivo word, un archivo de audio o video, o un archivo multimedia, que puede ser abierto en un navegador web, por ejemplo.

Alternativamente, el archivo digital es un correo electrónico que solo puede ser abierto en la aplicación de software de correo electrónico apropiada que se ejecuta en la máquina que tiene la Firma Digital de Autenticación (ADS)

La invención también proporciona un proceso que es realizado en un servidor, y que puede ser utilizado para comunicar archivos digitales a un Sistema de Manejo de Información (IHS), comprendiendo el IHS un conjunto de componentes de hardware y software operados por un Sistema Operativo (OS) a través de controladores.

El proceso implica las operaciones de:

- recibir una solicitud de descarga en dicho servidor de un usuario;

- lanzar en dicho sistema IHS un procedimiento de detección del sistema con el propósito de recopilar datos de dichos componentes a través de dichos controladores e informar a dicho OS;

- generar un archivo de descripción del sistema a partir de parte o de la totalidad de la información recopilada de dicho procedimiento de detección del sistema;

- cifrar parte o la totalidad de dicho archivo de descripción del sistema para generar una Firma Digital de Autenticación (ADS) que identifique de forma exclusiva dicho sistema;

- generar una primera clave de cifrado (K1) a partir de dicha ADS;

- generar, en respuesta a dicha solicitud de descarga, un archivo agregado F1 que comprende los siguientes campos: X1, S1 y H1:

En donde

X1 es el archivo digital (D1) cifrado con dicha clave;

S1 son configuraciones que comprenden dos campos:

- un primer campo PS1 que es público y no cifrado;

- un segundo campo pS1 que es privado y cifrado por dicha clave;

siendo H1 un hash de X1, S1.

En una realización, el servidor está asociado con una base de datos de derechos de uso y normas de restricciones aplicadas a una lista de usuarios predeterminados, e implica las operaciones de:

- recibir una solicitud de descarga en dicho servidor de un usuario;

- acceder a una base de datos que comprende una lista de usuarios predeterminados asociados con normas de restricción o derechos de uso aplicados a dichos usuarios;

- si dicho usuario que solicita la descarga de un archivo digital no figura en dicha base de datos, iniciará entonces en dicho sistema IHS un procedimiento de detección del sistema con el propósito de recopilar datos de dichos componentes a través de dichos controladores e informar a dicho OS;

- generar un archivo de descripción del sistema a partir de parte o de la totalidad de los datos recopilados de dicho procedimiento de detección del sistema;

- cifrar parte o la totalidad de dicho archivo de descripción del sistema con el fin de generar una Firma Digital de Autenticación (ADS) que identifique de forma exclusiva dicho sistema;

- si dicho usuario está incluido en dicha base de datos, entonces recupera dichas ADS asignadas a dicho usuario;

- generar una clave de cifrado (K1) a partir de dicha ADS;

- generar, en respuesta a dicha solicitud de descarga, un archivo agregado F1 que comprende los siguientes campos: X1, S1 y H1:

En donde

X1 es el archivo digital (D1) cifrado con dicha clave;

S1 son configuraciones que comprenden dos campos:

- un primer campo pS1 que es público y no está cifrado;

- un segundo campo pS1 que es privado y cifrado por dicha clave;

- H1 es un hash de X1, S1.

Finalmente, la invención consigue un proceso que ha de ser ejecutado en un sistema IHS para descargar y explotar el archivo agregado F1 comunicado por el servidor anterior.

- recibir dicho archivo agregado F1 descargado;

- iniciar en dicho sistema IHS un proceso de Control de Documentos que implica las operaciones de:

    - realizar en dicho sistema IHS un procedimiento de detección del sistema con el propósito de recopilar datos de dichos componentes a través de dichos controladores e informar a dicho SO;

    - generar un archivo de descripción del sistema a partir de parte o de la totalidad de los datos recopilados de dicho procedimiento de detección del sistema;

    - cifrar parte o la totalidad de dicho archivo de descripción del sistema con el fin de generar una Firma Digital de Autenticación (ADS) que identifique de forma exclusiva dicho sistema;

    - generar una segunda clave de cifrado (K2) a partir dicha ADS;

    - descifrar dicho campo privado (pS1) de dicho archivo agregado con dicha segunda clave;

    - descifrar X1 con dicha segunda clave y abrir dicho documento (D1) de acuerdo con los derechos de uso y las normas de restricciones aplicadas a dicho usuario.

Se puede ver de nuevo, y esta es una gran ventaja de la presente invención con respecto a la solicitud de patente Europea (EP1669833) de la técnica anterior mencionada anteriormente que no hay absolutamente ninguna necesidad de comunicar la clave de cifrado (K1), ya que esta última es directamente calculada dentro de la máquina, ni es necesario realizar ninguna comparación entre firmas (una firma de referencia y una firma actual) que debilitaría el nivel de seguridad.

En una realización, una vez abierto, el archivo digital F1 es cargado con restricciones que cumplen con los derechos de uso incluidos en el campo S1 y extraído de la base de datos de derechos de uso.

La invención también proporciona un sistema IHS equipado con medios para realizar el proceso definido anteriormente.

Descripción de los dibujos

Ahora se describirá una realización de la invención, solo a modo de ejemplo, con referencia a los dibujos adjuntos, en donde:

La Figura 1 ilustra una realización de un Sistema de Manejo de Información (IHS) típico que se comunica con un servidor distante que proporciona acceso a archivos digitales.

La figura 2 ilustra una realización de un proceso ejecutado para registrar al cliente en la base de datos de derechos de uso o para actualizar dicha base de datos.

La figura 3 ilustra una realización de un proceso que es ejecutado dentro del servidor.

La figura 4 ilustra una realización de un proceso que es ejecutado dentro de la máquina IHS local.

La figura 5 ilustra una segunda realización de un proceso ejecutado dentro del servidor que no requiere la utilización de una base de datos de uso y derechos que enumera los clientes.

La figura 6 ilustra la arquitectura de un sistema genérico que incluye componentes que proporcionan datos CID y CDD utilizados para generar la información del ADN digital.

La figura 7 ilustra un ejemplo de la recopilación de datos para dos dispositivos USB particulares.

Descripción de la realización preferida de la invención

Ahora se describirán procedimientos nuevos y mejorados para mejorar la protección de los archivos digitales que son transmitidos y difundidos a través de una red, tal como una red de intranet o la red de Internet, y descargados en un sistema local.

Hablando en términos generales, el sistema local puede ser cualquier Sistema de Manejo de Información (IHS) o dispositivo que esté equipado con recursos de procesamiento. Esto incluye claramente, sin ninguna limitación, ordenadores de escritorio, ordenadores de escritorio y portátiles, ordenadores de mano o de bolsillo también conocidos como Personal Digital Assistant (P.D.A.), e incluso los últimos teléfonos móviles que están ahora equipados con recursos de procesamiento, así como un sistema operativo (tal como Windows CE o iPhone o Google Android, por ejemplo).

La figura 1 ilustra un primer ejemplo que muestra un sistema IHS convencional 10 que comprende un procesador 6, equipado con almacenamiento RAM 7 donde un Sistema Operativo (OS) dedicado 11 - por ejemplo Windows de Microsoft Corp. o Linux o similar, en donde las aplicaciones 12 de software pueden ejecutarse. Además de tales aplicaciones, el sistema incluye un navegador web 13 (tal como Internet Explorer de Microsoft Inc.) y un software 14 de instalación de correo electrónico (tal como Outlook del mismo fabricante).

Además, el sistema 10 puede estar asociado con componentes de E/S bien conocidos, tales como una pantalla 2, un teclado 3, un ratón 4 y otros periféricos, tales como una llave USB 20 que coopera con un enchufe USB 5.

El sistema incluye además medios para conseguir comunicaciones, por ejemplo, cumplir con los protocolos TCP/IP y particularmente el bien conocido Protocolo de Transferencia de Hipertexto (HTTP) o la versión segura HTTPS, para comunicarse con una intranet o red de Internet, representada por el número 90 en figura 1, para acceder a un servidor 91 de archivos distante y un servidor 92 de derechos de Uso. Claramente, los servidores 91 y 92 pueden estar incorporados en un mismo servidor o pueden estar dispuestos en diferentes entidades físicas. De manera similar, el servidor 91 puede ser un servidor FTP o cualquier otro servidor que proporcione acceso a un directorio de archivos digitales, mientras que el servidor 92 puede ser un servidor especializado que organiza transacciones comerciales con los usuarios. En una realización alternativa, se pueden disponer tres servidores distintivos, uno para almacenar la base de datos de derechos de uso, uno para almacenar los archivos digitales, y un servidor particular para ejecutar los procedimientos y protocolos inventivos descritos a continuación.

Por lo tanto, el sistema IHS local 10 está equipado con todos los medios necesarios para acceder a un servidor web distante 91, por ejemplo, con el propósito de solicitar la descarga de un archivo, ya sea un video, un audio o cualquier archivo multimedia.

Sin embargo, con el fin de aumentar el nivel de protección de los archivos digitales que se comunican a través de la red, se describirán ahora realizaciones de procesos ejecutados entre el servidor 91 y la máquina IHS 10.

La figura 2 muestra el proceso preliminar de registro que es ejecutado con el propósito de registrar un usuario en una base de datos.

El proceso comienza con una operación 21 durante la cual el usuario solicita acceso a una página web del servidor 92 que mantiene la base de datos de derechos de uso.

Luego, en una operación 22, el servidor autentica al cliente, por ejemplo, utilizando un nombre de usuario y contraseña convencionales.

Luego, en una operación 23, un fragmento de código es cargado luego ejecutado en el cliente para generar la Firma Digital de Autenticación (ADS), a veces designada bajo la expresión "información de ADN digital" – que identifica y autentica de manera exclusiva el sistema IHS. En una realización preferida, este fragmento de código se encuentra en un applet de Java instalado por un navegador que detecta una referencia a un código de applet de Java firmado en una página HTML del servidor 92. En otra realización, este fragmento de código se encuentra en un programa adicional del navegador como un programa adicional de Firefox™ o programa adicional de Microsoft ActiveX.

Una vez instalado, el agente de generación de ADS provoca, en una operación 24, el inicio de un procedimiento de detección con el propósito de recopilar toda la información existente proporcionada por los diferentes componentes del sistema a través de los controladores de dichos componentes, y se informa al Sistema Operativo que se ejecuta en el sistema de acuerdo, por ejemplo, con las técnicas descritas en el documento EP1669833 mencionadas en la sección de la técnica anterior.

Luego, en una operación 25, los datos que se informan durante el proceso de detección son utilizados, parcial o totalmente, para generar un **archivo de descripción del sistema IHS** que luego es cifrado, parcial o totalmente, por medio de cualquier mecanismo de cifrado conocido para generar un Firma Digital de Autenticación (ADS).

De hecho, debido a la amplia variedad de componentes, hardware y software, que componen el sistema IHS, y cada uno informando información y datos significativos al sistema operativo – al menos con el propósito del procedimiento de configuración de los controladores – uno puede garantizar que la Firma Digital de Autenticación (ADS) (información de ADN digital) identifica de forma exclusiva el sistema IHS local 10.

Alternativamente, la firma ADS se limitará a un conjunto muy limitado de componentes, e incluso a un solo componente pasivo, tal como una llave USB o un CDROM, siendo utilizada la ADS generada a partir de ese único componente para cifrar el archivo de acuerdo con el procedimiento descrito a continuación.

Luego, en una operación 26, la Firma Digital de Autenticación (ADS) (o información de ADN digital) es transmitida a través de cualquier proceso de transmisión seguro conocido al servidor distante 92, con el fin de ser almacenada dentro de la base de datos mantenida por el servidor 92.

Luego, en una operación 27, la base de datos es actualizada con la Firma Digital de Autenticación (ADS) del cliente que está asociada con el usuario considerado, junto con los derechos de uso, posiblemente definidos de acuerdo con algunas consideraciones comerciales.

Ahora se describirá el procedimiento particular que es ejecutado con el propósito de descargar un archivo, asociado con derechos de uso, a un cliente en particular.

Con ese propósito, la Firma Digital de Autenticación (ADS) (información de ADN digital) es utilizada para derivar una clave de cifrado que es utilizada ventajosamente para el cifrado/descifrado de los archivos de documentos en el procedimiento que se describirá a continuación.

De hecho, los inventores han descubierto que utilizando tal información ADS digital como una clave de cifrado permite aprovechar las funcionalidades del algoritmo de cifrado/descifrado, y particularmente el hecho de que ya no es necesario realizar ninguna comparación entre dos firmas, una firma actual y una firma de referencia, con el propósito de permitir la transacción...

Por lo tanto, la invención se desvía de la enseñanza del documento EP1669833 que requería la carga, en la memoria del sistema bajo control de las dos firmas, para completar la transacción, debilitando así el nivel de seguridad del proceso.

Con la invención, ya no será necesario realizar ninguna comparación y, además, como se hará evidente de aquí en adelante, incluso ya no será necesario intercambiar la clave de cifrado/descifrado.

Preferiblemente, la clave de cifrado se deriva de la Firma Digital de Autenticación (ADS) (información de ADN digital) por medio de un mecanismo de hash.

Con respecto a la figura 3, se describirá ahora una realización particular del proceso que es realizado en el servidor distante 91 que utiliza la base de datos actualizada en la figura 2…

El proceso comienza con una operación 31 en donde el servidor distante 91 recibe una solicitud de descarga de un usuario o cliente, por ejemplo, el sistema IHS local 10, solicitando la descarga de un documento D1.

Luego, en una operación 32, el servidor distante autentica al cliente, preferiblemente mediante el uso de un nombre de usuario y una contraseña como en los procedimientos de autenticación convencionales. En una realización, la operación 32 puede implicar la utilización de la Firma Digital de Autenticación (ADS) (información de ADN digital) generada en la operación 25 del procedimiento de registro, para proporcionar un Identificador de Cliente más completo que utiliza la información contextual relativa al sistema y, por lo tanto, un procedimiento de autenticación más fuerte.

Luego, en una operación 33, el servidor accede a la base de datos de Derechos de Uso y a las normas de restricciones almacenadas en el servidor 92 (en la figura 1), y extrae la Firma Digital de Autenticación (ADS) (información de ADN digital) asociada al cliente que está almacenada allí.

Si el cliente no figura en la base de datos mencionada anteriormente, el proceso de registro descrito en la figura 2 se iniciará antes del proceso de descarga.

Si el cliente figura en la base de datos, el proceso continúa con una operación 34 en la que el servidor 91 calcula (con una función matemática predeterminada) una clave criptográfica K1 que está basada en la Firma Digital de Autenticación

(ADS) (información de ADN digital) almacenada en el base de datos. En una realización particular, la función matemática está basada en un algoritmo hash tal como SHA-1 o MD5.

Luego, en una operación 35, el servidor distante cifra el documento D1 con la clave K1. El resultado de esta operación se llama X1.

Luego, en una operación 36, el servidor genera información S1 de configuración que comprende dos campos distintivos, un primer campo público PS1 y un segundo campo privado pS1.

El campo público PS1 comprende información pública que no está cifrada y, por lo tanto, puede estar disponible para cualquier usuario. Tal información pública PS1 puede incluir información pública general, tal como el nombre del documento, el nombre del servidor, un aviso de derechos de autos, cuando corresponda, el nombre del cliente, la referencia (U.R.L.) de la transacción de descarga, la fecha, la hora, etc… así como los derechos de uso del documento D1 asociado a la ID del cliente.

Por el contrario, el campo privado pS1 comprende información que es cifrada con la clave K1 calculada en la operación 34. Tal información puede incluir información privada general relacionada con el documento D1 (por ejemplo, la identificación de la persona que ha modificado el documento, en qué momento, la naturaleza de la modificación...), pero también propiedades de contexto relativas tanto al servidor como al cliente,

Incluyendo:

- la identificación del Servidor, p. ej. un hash de su propia Firma Digital de Autenticación (ADS) (información de ADN digital)

Luego, en una operación 37, el servidor genera un archivo F1 que comprende la siguiente información agregada X1, S1 y H1:

En donde:

X1: comprende el documento que ha de ser descargado, cifrado con la clave K1 calculada en la operación 34. Se puede utilizar cualquier algoritmo simétrico conocido para realizar tal cifrado, p. ej., un algoritmo 3DES o uno AES bien conocido.

Además de X1 y S1 = (PS1, pS1), el documento F1 comprende un hash global H1 basado en toda la información previa (X1, PS1, pS1)

Luego, en una operación 38, el archivo agregado F1 es descargado por el cliente que lo procesa de acuerdo con el procedimiento descrito en referencia con la figura 3.

Con respecto a la figura 4, se ha descrito ahora el proceso que es realizado en el sistema IHS local que recibe el archivo agregado F1 después de la ejecución del proceso de la figura 3.

En una operación 40, el sistema IHS local 10 o el cliente recibe el archivo descargado F1.

Luego, en una operación 41, el cliente ejecuta un Software de Control ADS específico (ADSCS) con el propósito de explotar el archivo F1.

En una realización particular, ADSCS toma la forma de un software de programa adicional asociado con el navegador o incluso con cualquier otro software de aplicación, tal como un correo electrónico o el software Adobe Acrobat Reader.

Alternativamente, el ADSCS puede adoptar la forma de un código java o applet.

Luego, en una operación 42, el Software de Control ADS carga el archivo descargado F1.

Luego, en una operación 43, el Software de Control ADS realiza el mismo proceso descrito con respecto a las operaciones 23-25 con el fin de calcular la Firma Digital de Autenticación (ADS) (información de ADN digital), utilizando el mismo algoritmo y funciones.

En una realización particular, el cálculo de la Firma Digital de Autenticación (ADS) se limitará a un conjunto limitado de componentes, e incluso a un solo componente pasivo, tal como una llave USB o un CDROM.

Luego, en una operación 44, el Software de Control ADS calcula una clave criptográfica K2 con la misma función matemática que se utilizó para calcular K1

Luego, en una operación 45, el Software de Control ADS calcula nuevamente el hash de los componentes X1, S1 incluidos en el archivo F1 para obtener H2.

Luego, en una operación 46, se realiza una prueba con el fin de verificar si H2 = H1

Si H2 = H1, entonces el archivo no ha sido modificado, la integridad está garantizada y entonces el proceso continúa con una operación 48.

Si H2 no es igual a H1, entonces la carga del documento es cancelada en una operación 47.

En la operación 48, el software de control ADS extrae del archivo F1 las partes X1, PS1 y pS1.

En una operación 49, el proceso realiza un proceso de descifrado, basado en la clave K2 calculada, del archivo X1 que se cifró previamente por medio de la Firma Digital de Autenticación (ADS) (información de ADN digital) almacenada dentro de la base de datos. Se puede ver que X1 solo puede ser descifrado si la información ADS digital actual calculada en la operación 25 corresponde totalmente a la información ADS digital calculada en la operación 44.

Por lo tanto, el proceso de la invención se aprovecha de la funcionalidad del algoritmo de cifrado/descifrado para evitar cualquier comparación entre una información ADS de referencia y una información ADS actual. En particular, la clave de cifrado basada en la información ADS digital almacenada en la base de datos nunca es almacenada en el sistema IHS, e incluso no está incluida en el archivo F1. El proceso muestra ser mucho más seguro que el que estaría basado en una comparación entre dos informaciones ADS digitales que son almacenadas en algún lugar de la memoria del sistema (como fue el caso en la solicitud de patente Europea mencionada anteriormente).

En una operación 50, D1 es descifrado a partir de X1 con K2. Nuevamente, si la clave K2 no es correcta, entonces el archivo no puede ser abierto...

Debería tenerse en cuenta que, en el caso particular donde la clave K1 ha sido calculada a partir de un conjunto limitado de componentes, e incluso un solo componente pasivo, tal como una llave USB o un CDROM. En este caso particular, el archivo cifrado descargado aún se abrirá si el usuario cambia su ordenador, pero aún conservará sus componentes pasivos particulares que se utilizaron para calcular la firma ADS. Más básicamente, si se utilizó una llave USB para crear la firma ADS, esto significa que el archivo descargado todavía puede ser abierto mientras la llave USB permanezca conectada en el ordenador anfitrión.

Luego, en una operación 51, el software de control ADS permite la utilización del documento D1 de acuerdo con las normas y restricciones de uso que están definidas en el campo PS1.

En particular, permite la apertura del documento D1 tantas veces como se ha definido en el campo PS1. En un caso particular, considerando que el derecho de usuario no puede imprimir, ADSCS deshabilitará el acceso a la función de impresión.

Si bien el proceso de la figura 3 se describió con respecto al acceso a una base de datos, debería tenerse en cuenta que tal acceso no es obligatorio.

De hecho, en una realización, ilustrada en la figura 5, el servidor puede realizar directamente el proceso de las figuras 2 y 3, sin implicar ninguna base de datos o servidor de derechos de uso para cifrar el archivo (D1) y generar el archivo agregado F1. En ese caso, los derechos de uso, si los hay, serán aplicados por defecto o de acuerdo con las consideraciones comerciales definidas en una transacción actualmente pendiente entre el cliente y el servidor web.

La figura 5 ilustra las diferentes operaciones que comprenden:

En una operación 61, el servidor recibe una solicitud de descarga en dicho servidor de un usuario.

Luego, en una operación 62, el servidor autentica al cliente de una manera similar a la de la operación 22 de la figura 2.

Luego, en una operación 63, el servidor descarga un agente que provoca el lanzamiento en dicho sistema IHS de un procedimiento de detección del sistema con el propósito de recopilar datos de dichos componentes a través de dichos controladores e informar a dicho SO. Esto da como resultado la generación de un archivo de descripción del sistema a partir de parte o de la totalidad de los datos recopilados de dicho procedimiento de detección del sistema. Ese archivo está cifrado con el propósito de generar una Firma Digital de Autenticación (ADS) que identifique de forma exclusiva dicho sistema.

Luego, en una operación 64, el servidor genera una primera clave de cifrado (K1) a partir de dicha ADS.

Luego, en una operación 65, el servidor cifra el documento D1 que ha de ser descargado con la clave (K1) y, en una operación posterior 66, calcula las configuraciones S1.

El servidor genera entonces en una operación 67, en respuesta a dicha solicitud de descarga, un archivo agregado F1 que comprende los siguientes campos: X1, S1 y H1;

En donde

X1 es el archivo digital (D1) cifrado con dicha clave;

S1 son configuraciones que comprenden dos campos:

- un primer campo PS1 que es público y no está cifrado;

- un segundo campo pS1 que es privado y está cifrado por dicha clave;

Siendo H1 un hash de X1, S1./

El archivo agregado F1 es entonces descargado por el cliente en una operación 68, que lo procesa de acuerdo con el procedimiento descrito en referencia con la figura 4.

Se puede ver que el proceso que se describió anteriormente con detalles puede ser utilizado con una amplia variedad de sistemas y componentes y, además, esa amplia variedad de sistemas y componentes es una ventaja clave para la presente invención, ya que garantiza la posibilidad de generar automáticamente una denominada Firma Digital de Autenticación (ADS) (información de ADN digital) a partir de la multiplicidad de componentes, particularmente detectada por el Sistema Operativo (Windows, Linux o similar) e implica datos de identificación para los procedimientos de configuración de los controladores.

Tales mecanismos demuestran ser muy efectivos ya que la clave de cifrado/descifrado no está disponible para los usuarios y, por lo tanto, no puede ser intercambiada directamente entre ellos, sino que es generada automáticamente a partir de un análisis contextual del sistema que recibe el archivo digital descargado.

Además, y esta es una gran ventaja de la presente invención, el proceso puede construir el **archivo de descripción de IHS** mencionado anteriormente utilizando el denominado proceso de calificación que se describió con detalles en la solicitud de patente Europea mencionada anteriormente, cuyo contenido es incorporado en la presente memoria por referencia simple que, en aras de la claridad, se resumirá de aquí en adelante.

Con respecto a la figura 6, se ha ilustrado la arquitectura estructural de un sistema general 100 que, en la realización preferida, es un ordenador de escritorio o portátil o cualquier ordenador de mano/PDA o teléfono móvil equipado con componentes 110 de hardware y elementos de software. Los componentes de hardware incluyen una placa base 111 equipada con un procesador, equipos de memoria, de alimentación y de batería, y un conjunto de adaptadores o controladores, así como buses y puertos de Entrada/salida. La placa base coopera con adaptadores especializados, tales como tarjetas de Red de Área Local (L.A.N.) o de Red de Área Amplia (W.A.N), o cualesquiera tarjetas o adaptadores especializados (video o audio) que proporcionen funciones especializadas y capacidades de procesamiento.

Además de la placa base, el sistema 100 incluye además un conjunto de dispositivos externos, tales como los dispositivos principales tradicionales 112, es decir, el bien conocido equipo de pantalla, teclado y mouse y algunas instalaciones de almacenamiento (discos duros, discos flexibles, unidades de Cdrom o DVD rom, etc...). El sistema puede incluir además dispositivos secundarios 113 conectados a la placa base a través de puertos de E/S apropiados, es decir, una impresora, un escáner, equipos de video y de fotografía, dispositivos de comunicación (Bluetooth, WIFI, infrarrojos, telefonía GSM-GPRS, módem), e incluso dispositivos más especializados, tales como un lector de identificación por radiofrecuencia (RFID), un lector biométrico y, de forma más general, cualquier otro equipo que pueda ser una fuente de información.

El Sistema 100 es hecho funcionar bajo el control del código de software, que está organizado en el código 121 de bajo nivel – el código conocido del Sistema Básico de Entrada y Salida (BIOS) que coopera con el Sistema Operativo (O.S.) y el código de nivel superior que incluye componentes y aplicaciones de software especiales. En la realización preferida de la invención, el sistema 100 es hecho funcionar bajo el bien conocido sistema operativo WINDOWS (TM) comercializado por MICROSOFT Corp. Un ordenador de mano puede estar equipado con el sistema operativo WINDOWS CE (Marca Registrada de Microsoft Comp.) diseñado para ordenadores de bolsillo. Claramente, el experto adaptará la invención a cualquier sistema operativo alternativo, tal como LINUX o PalmOS (TM), por ejemplo.

Considerando ahora más particularmente la información a la que puede acceder el sistema 100 a través de su propósito general y dispositivos más especializados, se puede ver que el sistema 100 tiene acceso, a través de la interfaz 130, a una amplia gama de información, tal como información contextual o ambiental 131 así como información 132 relacionada con el usuario. La información ambiental 131 puede ser, sin ninguna limitación, información sobre el Sistema de Posicionamiento Global (G.P.S.), la fecha y la hora, la temperatura relevante de la habitación en donde el sistema está siendo hecho funcionar, el número de línea telefónica proporcionado por el adaptador de módem, los Medios Control de acceso (MAC)/dirección IP asignada por el adaptador de red…La información 132 relacionada con el usuario puede incluir datos tales como datos biométricos, código PIN, nombre de usuario-contraseña, tarjeta de ID o cualquier información personal proporcionada por el usuario...

Cada componente dentro del sistema 100 está siendo identificado, registrado y validado antes de la transacción o antes de acceder a cualquier servicio seguro. En el marco de la presente invención, un componente – se entiende que abarca elementos de hardware y software que son constituyentes del sistema. De manera más precisa, un componente es un elemento constitutivo de un sistema. Puede ser una tarjeta integrada (placa base, tarjeta adaptadora de red), un chip microprocesador, un chip de memoria, un disco duro... De manera más general, un dispositivo periférico (lector biométrico) y un componente de software o programa de aplicación se considera que son componentes.

En la realización preferida de la invención, cada componente está asociado a datos de componente que incluyen, sin limitación, Datos de Identificación de Componentes (CID) y Datos Contextuales de Componentes (CCD).

Datos de Identificación de Componentes (CID) es un identificador que identifica de forma exclusiva el propio componente. Claramente, puede ser cualquier cadena alfanumérica única que identifique el componente correspondiente, ya sea hardware o software.

Debería tenerse en cuenta que, en el campo técnico de los ordenadores, es una práctica común que los fabricantes de productos y los proveedores de partes individuales asignen referencias que identifiquen individualmente un elemento en particular. Por ejemplo, cada procesador tiene un número de serie único; cada software instalado (en Windows (TM), por ejemplo) (o componente de software como Active X) tiene un Identificador Único Global (GUID) y/o un identificador de Clase (CLSID). Para el software GUID/CLSID, podría no haber colisión entre dos identificadores, ya que se están acumulando para ser únicos en un OS. Para los componentes de hardware, se podría crear una ID de ordenador concatenando el identificador del fabricante, el identificador del modelo y el número de serie del propio componente. Claramente, el experto adaptará la invención a cualquier sistema operativo alternativo, tal como LINUX.

Tales identificadores son utilizados particularmente para permitir que los diferentes controladores correspondientes a los diferentes dispositivos sean instalados dentro de un sistema operativo dado, por ejemplo, el sistema operativo tipo Windows (TM). Esto es muy ventajoso porque la gran cantidad de componentes existentes en el sistema da como resultado un gran volumen de datos (recopilados automáticamente) para generar la información contextual de ADS.

Además de los Datos de Identificación del Componente, los datos del Componente incluyen además unos Datos Contextuales de Componentes (CCD) que no identifica el propio componente, sino que son los datos devueltos por el componente cuando está en uso. Por ejemplo, los CCD son las coordenadas GPS en una solicitud específica proporcionada por un componente del dispositivo GPS. Los datos CID y CDD pueden ser combinados para crear una referencia de identificación contextual compleja que se utilizará para autorizar o denegar el acceso al sistema 100.

El procedimiento de identificación que se resumió anteriormente, y que permite la recopilación automática de una información completa sobre (CID, CCD) informada por los diferentes componentes del sistema, incluyendo los datos puestos a disposición del OS para el procedimiento de instalación de los controladores, permite la generación de una información ADS digital que toma la forma, en una realización, de un Archivo de Calificación del Sistema, p. ej. un archivo extendido de Lenguaje de Marcado (XML).

Como se ha explicado en la solicitud de patente Europea mencionada anteriormente, el archivo SQF presenta una organización estructurada que almacena datos correspondientes a los diferentes componentes detectados dentro del sistema 100, incluyendo los Datos de Identificación de Componentes (CID) y, posiblemente, los Datos Contextuales de Componentes (CCD) que pueden ser devueltos por uno o más componentes particulares.

Una vez generado, el archivo SQF es cifrado para generar una firma de Calificación del sistema (SQS) que puede ser comparada con una firma de referencia antes de validar cualquier transacción.

En la presente invención, el archivo SQS es utilizado ahora como la denominada información de ADN digital, y es codificado para proporcionar una clave de cifrado que puede ser utilizada de acuerdo con el proceso descrito en referencia a las figuras 2 y 3, y permitiendo así la protección de un archivo de descarga y su uso legítimo de acuerdo con los derechos de uso predeterminados.

Con respecto a la figura 7, se ha ilustrado un ejemplo de la información que puede ser recopilada, respectivamente, por tres sistemas operativos (MICROSOFT WINDOWS, GNU-LINUX, APPLE MAC) informados a partir de dos ejemplos de dispositivos USB, tales como un PNY Mini Attaché 2Gb y un OTi Flash Disk Media.

Aplicación de la invención

La invención puede encontrar aplicaciones de muchas maneras diferentes.

En una realización, los procedimientos descritos anteriormente pueden ser ejecutados mediante un programa adicional del navegador web preexistente para proporcionar una herramienta de navegación mejorada que permita la lectura de los archivos descargados por el servidor 91.

Alternativamente, la invención puede ser realizada por medio de un programa adicional de un software de correo electrónico para el propósito

De manera más general, la invención puede ser utilizada ventajosamente para proporcionar protección a las siguientes categorías de documentos:

- un archivo de texto, un archivo PDF, un archivo de automatización de oficina (texto, Microsoft Word, Microsoft Excel, Open Office Writer,...)
- Una página web HTML

• un archivo de audio (MP3 ...)

• un archivo de video (avi ...)

Etc ...

Como se apreciará por un experto en la técnica, la presente invención puede ser realizada como un método, un sistema de procesamiento de datos o un producto de programa. Por consiguiente, la presente invención puede adoptar la forma de una realización completamente de hardware, una realización completamente de software o una realización que combina aspectos de software y hardware. Además, la presente invención puede adoptar la forma de un producto de programa informático en un medio de almacenamiento legible por ordenador que tiene medios de código de programa legibles por ordenador incorporados en el medio. Se puede utilizar cualquier medio adecuado legible por ordenador incluyendo discos duros, CD-ROM, dispositivos de almacenamiento óptico, o dispositivos de almacenamiento magnético.

La presente invención se ha descrito a continuación con referencia a ilustraciones de diagrama de flujo de métodos, aparato (sistemas) y productos de programas informáticos de acuerdo con la invención. Se entenderá que cada bloque de las ilustraciones del diagrama de flujo, y las combinaciones de bloques en las ilustraciones del diagrama de flujo, pueden ser implementados mediante instrucciones del programa informático. Estas instrucciones de programa informático pueden ser cargadas en un ordenador u otro aparato de procesamiento de datos programable para producir una máquina, de tal manera que las instrucciones que se ejecutan en el ordenador u otro aparato de procesamiento de datos programable crean medios para implementar las funciones especificadas en el bloque o bloques de diagrama de flujo. Estas instrucciones de programa informático también pueden ser almacenadas en una memoria legible por ordenador que puede hacer que un ordenador u otro aparato de procesamiento de datos programable funcione de una manera particular, de tal manera que las instrucciones almacenadas en la memoria legible por ordenador produzcan un artículo de fabricación que incluya instrucciones significa que implementa la función especificada en el bloque o bloques del diagrama de flujo. Las instrucciones del programa informático también pueden ser cargadas en un ordenador u otro aparato de procesamiento de datos programable para causar una serie de pasos operativos que han de ser realizados en el ordenador u otro aparato programable para producir un proceso implementado por ordenador de tal manera que las instrucciones que se ejecutan en el ordenador u otro aparato programable proporcionan operaciones para implementar las funciones especificadas en el bloque o bloques de diagrama de flujo.

Por consiguiente, los bloques de las ilustraciones del diagrama de flujo admiten combinaciones de medios para realizar las funciones especificadas, combinaciones de operaciones para realizar las funciones especificadas y medios de instrucción de programa que realizan las funciones especificadas. También se entenderá que cada bloque de las ilustraciones del diagrama de flujo, y las combinaciones de bloques en las ilustraciones del diagrama de flujo, pueden ser implementados mediante hardware de propósito especial o sistemas informáticos que realizan las funciones especificadas o combinaciones de hardware de propósito especial e instrucciones de ordenador.

REIVINDICACIONES

1. Proceso para comunicar un archivo digital (D1) desde un servidor a un Sistema de Manejo de Información (IHS), comprendiendo el IHS un conjunto de componentes de hardware y software operados por un Sistema Operativo (OS) a través de controladores;

Implicando dicho proceso las operaciones de:

- iniciar un procedimiento de detección del sistema con el propósito de recopilar datos de dichos componentes a través de dichos controladores e informar a dicho OS;

- generar un archivo de descripción del sistema a partir de parte o de la totalidad de los datos recopilados de dicho procedimiento de detección del sistema;

- cifrar parte o la totalidad de dicho archivo de descripción del sistema para generar una Firma Digital de Autenticación (ADS);

- utilizar dicha Firma Digital de Autenticación (ADS) para derivar una clave de cifrado/descifrado (K1);

- utilizar dicha clave para cifrar un archivo que ha de ser descargado o para descifrar un archivo cifrado que se está descargando.

2. Proceso según la reivindicación 1, caracterizado por que dicha firma ADS es calculada a partir de los datos informados por un conjunto limitado de dispositivos conectados a dicho sistema HIS.

3. Proceso según la reivindicación 2, caracterizado por que dicha firma ADS es calculada a partir de un único dispositivo USB, tal como un dispositivo de almacenamiento USB.

4. Proceso según la reivindicación 1, caracterizado por que dicha Firma Digital de Autenticación es almacenada en una base de datos que comprende derechos de uso y normas de restricciones asociadas a una lista de usuarios.

5. Proceso según cualquiera de las reivindicaciones 1 a 4, caracterizado por que dicha clave (K1) se deriva de dicha ADS a través de un mecanismo de “hashing”.

6. Proceso según las reivindicaciones 1 a 5, caracterizado por que dicha clave (K1) es utilizada para generar un archivo agregado F1 que comprende la siguiente información: X1, S1 y H1:

En donde:

X1: comprende el documento D1 que ha de ser descargado, cifrado con dicha clave K1;

Comprendiendo S1 un primer campo (PS1) no cifrado y un segundo campo pS1 cifrado con dicha clave K1.

H1: es un hash de X1, S1

7. Procedimiento según cualquiera de las reivindicaciones 1 a 6, caracterizado por que dicho archivo descargado es un archivo de texto, un archivo PDF, un archivo word, un archivo de audio o video, o un archivo multimedia.

8. Proceso según cualquiera de las reivindicaciones 1 a 7, caracterizado por que dicho servidor es un servidor pop y dicho proceso es ejecutado en un software de aplicación de correo electrónico, tal como Outlook.

9. Proceso para comunicar un archivo (D1) desde un servidor a un Sistema de Manejo de Información (IHS) comprendiendo el IHS un conjunto de componentes de hardware y software operados por un Sistema Operativo (OS) a través de controladores, implicando dicho proceso las operaciones de:

- recibir una solicitud de descarga en dicho servidor de un usuario;

- iniciar en dicho sistema IHS un procedimiento de detección del sistema con el propósito de recopilar datos de dichos componentes a través de dichos controladores e informar a dicho OS;

- generar un archivo de descripción del sistema a partir de parte o de la totalidad de los datos recopilados de dicho procedimiento de detección del sistema;

- cifrar parte o la totalidad de dicho archivo de descripción del sistema para generar una Firma Digital de Autenticación (ADS) que identifique de forma exclusiva dicho sistema;

- generar una primera clave de cifrado (K1) a partir de dicho ADS;

- generar, en respuesta a dicha solicitud de descarga, un archivo agregado F1 que comprende los siguientes campos: X1, S1 y H1;

En donde

X1 es el archivo digital (D1) cifrado con dicha clave;

S1 son configuraciones que comprenden dos campos:

- un primer campo PS1 que es público y no está cifrado;

- un segundo campo pS1 que es privado y está cifrado por dicha clave;

Siendo H1 un hash de X1, S1.

10. Proceso para comunicar un archivo (D1) desde un servidor a un Sistema de Manejo de Información (IHS), comprendiendo el IHS un conjunto de componentes de hardware y software operados por un Sistema Operativo (OS) a través de controladores, implicando dicho proceso las operaciones de:

- recibir una solicitud de descarga en dicho servidor de un usuario;

- acceder a una base de datos que comprende una lista de usuarios predeterminados asociados con normas de restricción o derechos de uso aplicados a dichos usuarios;

- si dicho usuario que solicita la descarga de un archivo digital no figura en dicha base de datos, entonces iniciará en dicho sistema IHS un procedimiento de detección del sistema con el propósito de recopilar datos de dichos componentes a través de dichos controladores e informar a dicho sistema operativo;

- generar un archivo de descripción del sistema a partir de parte o de la totalidad de la información recopilada de dicho procedimiento de detección del sistema;

- cifrar parte o la totalidad de dicho archivo de descripción del sistema con el fin de generar una Firma Digital de Autenticación (ADS) que identifique de forma exclusiva dicho sistema;

- si dicho usuario está incluido en dicha base de datos, recuperar entonces dichas ADS asignadas a dicho usuario;

- generar una clave de cifrado (K1) a partir de dicha ADS;

- generar, en respuesta a dicha solicitud de descarga, un archivo agregado F1 que comprende los siguientes campos: X1, S1 y H1;

En donde

X1 es el archivo digital (D1) cifrado con dicha clave;

S1 son configuraciones que comprenden dos campos:

- un primer campo PS1 que es público y no está cifrado;

- un segundo campo pS1 que es privado y está cifrado por dicha clave;

Siendo H1 un hash de X1, S1.

11. Proceso ejecutado en un sistema IHS para descargar y explotar el archivo comunicado según el proceso de las reivindicaciones 9 o 10, implicando dicho proceso las operaciones de:

- recibir dicho archivo agregado descargado F1;

- iniciar en dicho sistema IHS un proceso de Control de Documentos que implica las operaciones de:

- realizar en dicho sistema IHS un procedimiento de detección del sistema con el propósito de recopilar datos de dichos componentes a través de dichos controladores e informar a dicho OS;

- generar un archivo de descripción del sistema a partir de parte o de la totalidad de la información recopilada de dicho procedimiento de detección del sistema;

- cifrar parte o la totalidad de dicho archivo de descripción del sistema con el fin de generar una Firma Digital de Autenticación (ADS) que identifique de forma exclusiva dicho sistema;

- generar una segunda clave de cifrado (K2) a partir de dicha ADS;

- descifrar dicho campo privado (pS1) de dicho archivo agregado con dicha segunda clave;

- descifrar X1 con dicha segunda clave y abrir dicho documento (D1) de acuerdo con los derechos de uso y normas de restricciones aplicadas a dicho usuario.

12. Proceso según cualquiera de las reivindicaciones 1 a 4, caracterizado por que dicha información de control público define normas de restricciones relativas a una de las siguientes funciones:

- LEER el archivo;

- LEER el archivo un número predeterminado de veces;

- IMPRIMIR el archivo

- IMPRIMIR el archivo un número predeterminado de veces;

- IMPRIMIR el archivo con un tono específico de "filigrana";

- COPIAR el archivo.

13. Sistema de Manejo de información que comprende un conjunto de componentes de hardware y software operados por un sistema operativo (OS) a través de controladores y que comprende además medios de comunicación para comunicarse con un servidor, comprendiendo dicho sistema:

- medios para iniciar un procedimiento de detección del sistema con el propósito de recopilar datos de dichos componentes a través de dichos controladores e informados a dicho OS;

- medios para generar un archivo de descripción del sistema a partir de parte o de la totalidad de la información recopilada de dicho procedimiento de detección del sistema;

- medios para cifrar parte o la totalidad de dicho archivo de descripción del sistema para generar una Firma Digital de Autenticación (ADS);

- medios para utilizar dicha Firma Digital de Autenticación (ADS) para derivar una primera clave de cifrado/descifrado (K1);

- medios para utilizar dicha clave para cifrar un archivo que ha de ser descargado o para descifrar un archivo cifrado que se está descargando.

14. El sistema HIS según la reivindicación 13 que incluye además:

- medios para recibir dicho archivo agregado descargado F1 que comprende los siguientes campos: X1, S1 y H1;

En donde

X1 es el archivo digital (D1) cifrado con dicha clave;

S1 son configuraciones que comprenden dos campos:

- un primer campo PS1 que es público y no está cifrado;

- un segundo campo pS1 que es privado y está cifrado por dicha clave;

Siendo H1 un hash de X1, S1;

- medios para realizar en dicho sistema IHS un procedimiento de detección del sistema con el propósito de recopilar datos de dichos componentes a través de dichos controladores e informar a dicho OS;

- medios para generar un archivo de descripción del sistema a partir de parte o de la totalidad de la información recopilada de dicho procedimiento de detección del sistema;

- medios para cifrar parte o la totalidad de dicho archivo de descripción del sistema para generar una Firma Digital de Autenticación (ADS) que identifique de forma exclusiva dicho sistema;

- medios para generar una segunda clave de cifrado (K2) a partir de dicha ADS, siendo utilizada dicha segunda clave (K2) para descifrar dicho campo privado (pS1) de dicho archivo agregado con dicha segunda clave;

- medios para descifrar X1 con dicha segunda clave y abrir dicho documento (D1) de acuerdo con los derechos de uso y las normas de restricciones aplicadas a dicho usuario.

- medios para abrir dicho documento (D1) de acuerdo con los derechos de uso definidos en dicho campo S1.

15. Un programa informático de seguridad para asegurar la descarga de un archivo digital, teniendo dicho producto de programa informático de seguridad elementos de código de programa para llevar a cabo un método según se ha reivindicado en cualquiera de las reivindicaciones 1 a 12.

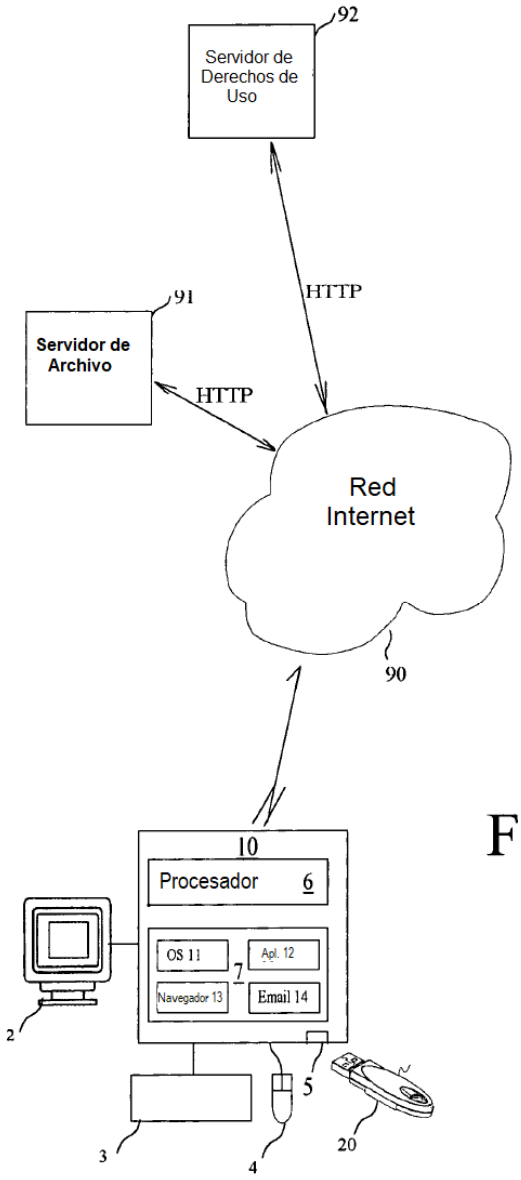
92
Servidor de Derechos de Uso
HTTP
91
Servidor de Archivo
HTTP
Red Internet
90
10
Procesador 6
OS 11
Apl. 12
7
Navegador 13
Email 14
2
3
4
5
20

Fig. 1

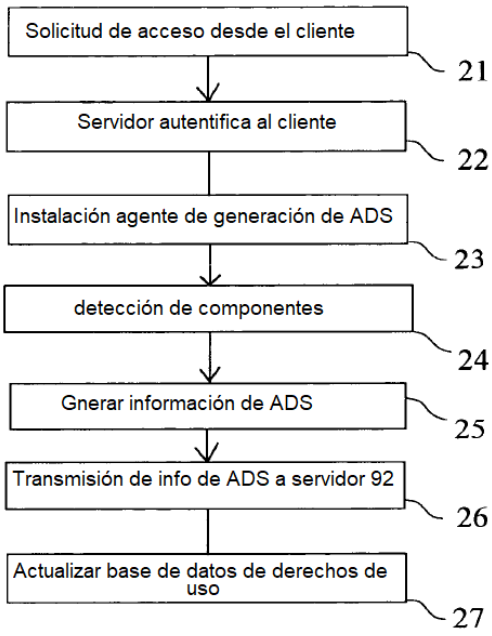
Solicitud de acceso desde el cliente
21
Servidor autentifica al cliente
22
Instalación agente de generación de ADS
23
detección de componentes
24
Gnerar información de ADS
25
Transmisión de info de ADS a servidor 92
26
Actualizar base de datos de derechos de uso
27

Fig. 2

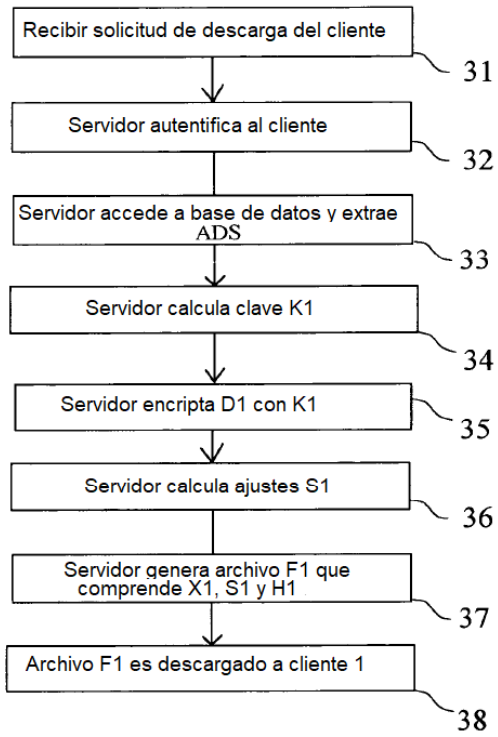
Recibir solicitud de descarga del cliente
31
Servidor autentifica al cliente
32
Servidor accede a base de datos y extrae ADS
33
Servidor calcula clave K1
34
Servidor encripta D1 con K1
35
Servidor calcula ajustes S1
36
Servidor genera archivo F1 que comprende X1, S1 y H1
37
Archivo F1 es descargado a cliente 1
38

Fig. 3

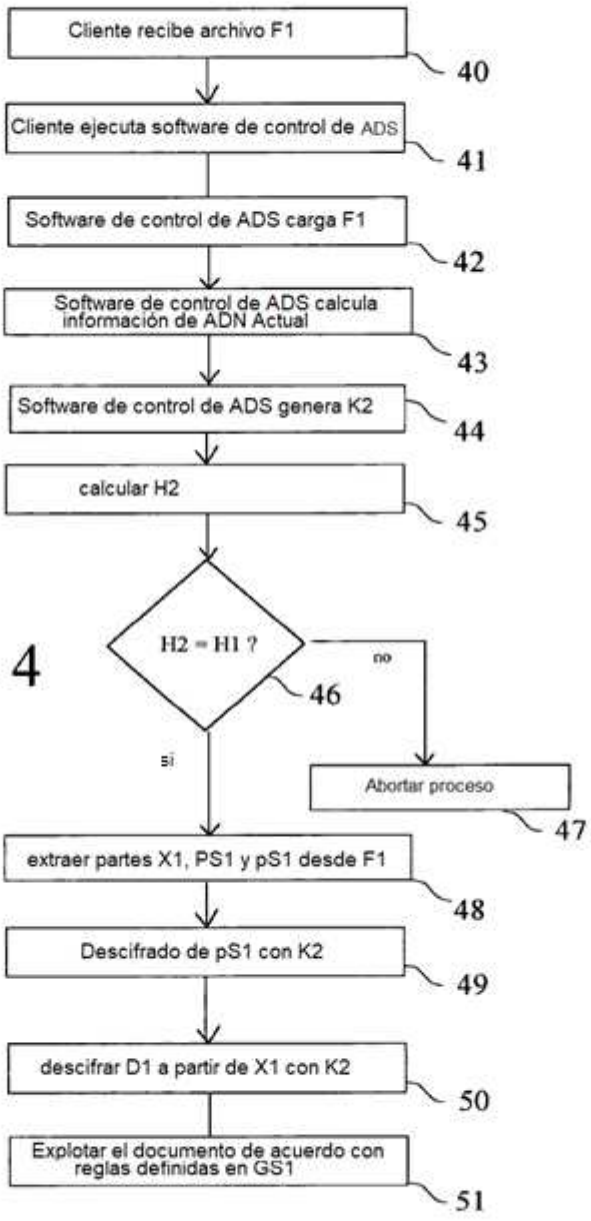
Cliente recibe archivo F1
40
Cliente ejecuta software de control de ADS
41
Software de control de ADS carga F1
42
Software de control de ADS calcula información de ADN Actual
43
Software de control de ADS genera K2
44
calcular H2
45
H2 = H1 ?
46
no
si
Abortar proceso
47
extraer partes X1, PS1 y pS1 desde F1
48
Descifrado de pS1 con K2
49
descifrar D1 a partir de X1 con K2
50
Explotar el documento de acuerdo con reglas definidas en GS1
51

Fig. 4

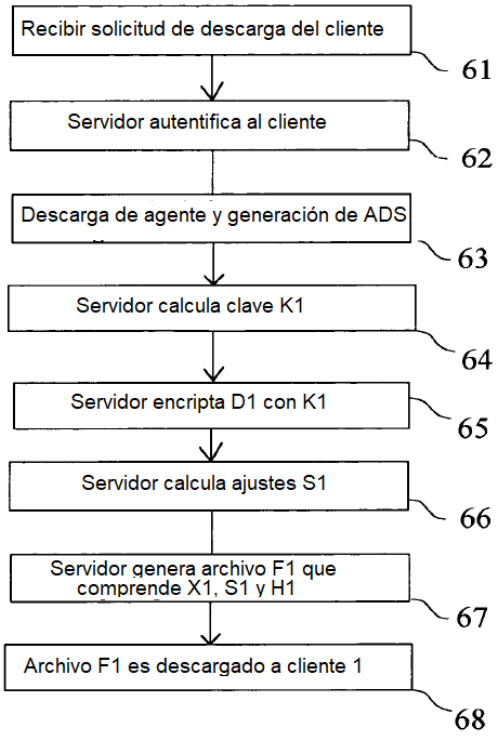
Recibir solicitud de descarga del cliente
61
Servidor autentifica al cliente
62
Descarga de agente y generación de ADS
63
Servidor calcula clave K1
64
Servidor encripta D1 con K1
65
Servidor calcula ajustes S1
66
Servidor genera archivo F1 que comprende X1, S1 y H1
67
Archivo F1 es descargado a cliente 1
68

Fig. 5

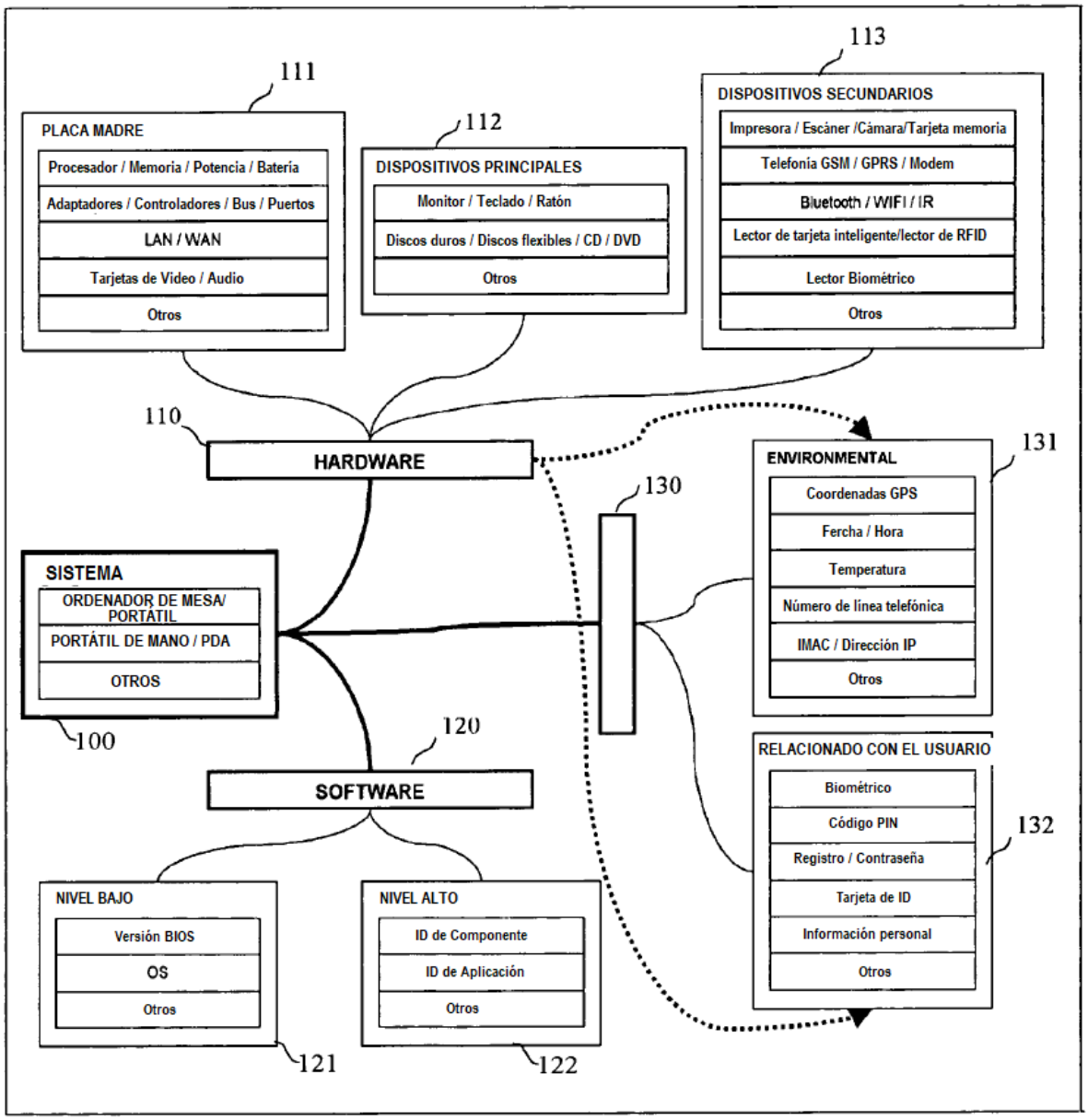
111
PLACA MADRE
Procesador / Memoria / Potencia / Batería
Adaptadores / Controladores / Bus / Puertos
LAN / WAN
Tarjetas de Video / Audio
Otros
112
DISPOSITIVOS PRINCIPALES
Monitor / Teclado / Ratón
Discos duros / Discos flexibles / CD / DVD
Otros
113
DISPOSITIVOS SECUNDARIOS
Impresora / Escáner /Cámara/Tarjeta memoria
Telefonía GSM / GPRS / Modem
Bluetooth / WIFI / IR
Lector de tarjeta inteligente/lector de RFID
Lector Biométrico
Otros
110
HARDWARE
130
131
ENVIRONMENTAL
Coordenadas GPS
Fercha / Hora
Temperatura
Número de línea telefónica
IMAC / Dirección IP
Otros
SISTEMA
ORDENADOR DE MESA/ PORTÁTIL
PORTÁTIL DE MANO / PDA
OTROS
100
120
SOFTWARE
RELACIONADO CON EL USUARIO
Biométrico
Código PIN
Registro / Contraseña
Tarjeta de ID
Información personal
Otros
132
NIVEL BAJO
Versión BIOS
OS
Otros
121
NIVEL ALTO
ID de Componente
ID de Aplicación
Otros
122

Fig. 6

Dispositivo	Información	Microsoft Windows	GNU-Linux	Apple Mac OS
PNY Mini Attaché 2Gb	ID de Producto	0x653e	0x653e	0x653e
	Nombre de Producto	"USB Flash Memory"	"USB Flash Memory"	"USB Flash Memory"
	ID de Vendedor	0x0930	0x0930	0x930
	Nombre de Vendedor	""	""	""
	Capacidad	2 023 418 880	2 026 373 120	2 026 373 120
	Número de serie	"0611162202231"	"0611162202231"	"0611162202231"
	Revisión	"1.00"	"1.00"	"1.00"
OTi Flash Disk Media 128Mb	ID de Producto	0x2168	0x2168	0x2168
	Nombre de Producto	"Flash Disk"	"Flash Disk"	"Flash Disk"
	ID de Vendedor	0x0ea0	0x0ea0	0xea0
	Nombre de Vendedor	"OTi"	"OTi"	"OTi"
	Capacidad	123 379 200	131 072 000	131 072 000
	Número de serie	"67282C406A1578BD"	"67282C406A1578BD"	"67282C406A1578BD"
	Revisión	"2.00"	"2.00"	"2.00"

Fig. 7