(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 271 129**

(51) Int. Cl.:
H04L 9/32 (2006.01)
H04K 1/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Número de solicitud europea: **02002858 .5**
(86) Fecha de presentación : **08.02.2002**
(87) Número de publicación de la solicitud: **1233571**
(87) Fecha de publicación de la solicitud: **21.08.2002**

(54) Título: **Procedimiento para la asignación de cronofechadores digitales.**

(30) Prioridad: **08.02.2001 DE 101 06 083**

(45) Fecha de publicación de la mención BOPI:
16.04.2007

(45) Fecha de la publicación del folleto de la patente:
16.04.2007

(73) Titular/es: **Jan Wendenburg**
Hammerstrasse 24
40219 Düsseldorf, DE

(72) Inventor/es: **Wendenburg, Jan y**
Dahm, Percy

(74) Agente: **Elzaburu Márquez, Alberto**

DESCRIPCIÓN

Procedimiento para la asignación de cronofechadores digitales.

La invención se refiere a un procedimiento para el encadenamiento de datos electrónicos o digitales con un sello cronofechador, en el que se crea un paquete de datos con sello cronofechador, que comprende un primer código de cifras de comprobación, que identifica los datos a sellar, así como datos del sello cronofechador.

La técnica actual de tratamiento de datos permite muy extensamente, reunir, enviar y archivar electrónicamente todas las informaciones que antes se retenían en papel. Esto se aprovecha, por ejemplo en el tráfico comercial, para intercambiar documentos por correo electrónico, o para encargar productos o prestaciones de servicios por Internet. Así se desarrollan electrónicamente, cada vez con más frecuencia, actividades comerciales y también privadas.

No obstante, en el desarrollo electrónico de negocios, el problema consiste en que los datos electrónicos son fácilmente manipulables. Por consiguiente, los datos electrónicos tienen por lo regular, un bajo carácter probatorio, por ejemplo, cuando en un encargo controvertido transmitido electrónicamente, lo que importa es cuándo y en qué extensión se ha impartido el encargo. Básicamente son necesarias, por lo tanto, comprobaciones fiables, para obtener seguridad sobre la validez de datos electrónicos, como por ejemplo, de correos electrónicos relevantes para el encargo, de una compra por Internet, o en la banca en línea.

Un problema semejante consiste en el archivo sin papel de documentos en forma electrónica. Así por ejemplo, los datos de contabilidad de una empresa, pueden manipularse posteriormente electrónicamente en forma fraudulenta, con el resultado de que, siempre y cuando no se hayan archivado los mismos datos en forma impresa, no puedan comprenderse ya más las operaciones contables verdaderas y, por tanto, se malversen posiblemente los recursos financieros de la empresa.

Hay distintos sistema de signatura del tiempo, con los que puede probarse que ha existido un determinado juego de datos en un momento determinado, y si este juego de datos se ha remitido por vía electrónica a un tercero. Aquí, un juego de datos se provee con una fecha, encadenando un código de cifras de comprobación, inequívoco para el juego de datos, con una fecha, creándose un código de signatura para la combinación de código de cifras de comprobación y fecha, y codificándose el código de signatura en una clave de signatura. La codificación se lleva a cabo con un procedimiento de cifrado en el que el código de signatura se codifica con una clave privada, y se decodifica con una clave pública correspondiente. La clave de signatura se encadena con el código de cifras de comprobación y la fecha, y forma un paquete de datos con sello cronofechador, que se archiva junto con una copia del juego de datos.

Por código de cifras de comprobación y código de signatura se entienden aquí y en lo sucesivo, datos que se crean según un algoritmo determinado a partir de un juego de datos o de un fichero, y lo identifican inequívocamente. Son por lo regular comparativamente pequeños respecto a los juegos de datos, y tienen una longitud uniforme, por ejemplo, una longitud de n bits. A causa del tamaño menor y uniforme, un programa de procesamiento de datos puede trabajar más fácil y rápidamente con un código semejante, conocido también, entre otras cosas, como código Hash, que con el fichero completo o con todo el juego de datos.

Si debe de producirse la comprobación sobre la validez del juego de datos y del tiempo en el que este juego de datos fue "sellado", o sea, se encadenó con una fecha, se decodifica la clave de signatura del paquete de datos con sello cronofechador, con la clave pública. El código de signatura decodificado de este modo, se compara con un nuevo código a calcular de signatura, produciéndose el nuevo código de signatura a calcular, a partir de un código de cifras de comprobación perteneciente al juego de datos, y de la fecha contenida en el paquete de datos con sello cronofechador. Si coincide el nuevo código calculado de signatura, y el decodificado, se ha producido la comprobación de que el juego de datos ya existía en la forma depositada en el momento del sello cronofechador. La clave de signatura está codificada de tal manera que es imposible, o al menos casi imposible, abrirla sin la necesaria clave pública, de manera que no pueda ser manipulada. Si hubiera de modificarse el paquete de datos con sello cronofechador, que contiene la clave codificada de signatura, no puede reproducirse ya más el código original de signatura, de manera que la manipulación sería evidente. Con ello, la signatura de tiempo se inutiliza e invalida en su totalidad. Así pues, está excluida una falsificación de los datos marcados.

Para que este tipo de signatura de tiempo tenga una validez oficial según el derecho alemán, conforme a la ley de sello cronofechador, hay exigencias especiales en la eficacia y seguridad de manipulación del hardware y del software, y de su entorno. Si un sistema de signatura del tiempo cumple estas exigencias para esta signatura de tiempo, después de la recepción por la TÜV-IT (inspección técnica, área de IT) existe la posibilidad de obtener un certificado oficial de signatura de tiempo. Un sistema de signatura que cumple por lo visto estas exigencias, está descrito en el documento EP 0 848 872 B1.

Básicamente es posible para una empresa gestionar un sistema semejante de signatura del tiempo, por ejemplo, incluso dentro de una red propia, y de este modo permitir fechar los datos electrónicos propios de la empresa, o también los que entren. Pero también existe la posibilidad de remitir los datos mediante una red pública de datos, como por ejemplo, Internet, a un proveedor de prestaciones de servicios, el cual devuelve de nuevo estos datos provistos con un sello cronofechador.

Un inconveniente de tales sistemas de signatura del tiempo, consiste en que son costosos y, por tanto, caros, y al mismo tiempo su capacidad para la concesión de sellos cronofechadores para juegos individuales de datos, está limitada por causa del rendimiento de computación. Si una empresa quiere protocolizar todas sus transacciones electrónicas, mediante tales sistemas de signatura de tiempo, esto apenas es posible, y económicamente insostenible, a causa de la capacidad limitada de sellado de estos sistemas.

Por Haber S. y otros: "How to time-stamp a digital document" 30 de diciembre de 1991, Advances in Cryptology - Proceedings of Crypto, Santa Bárbara, 11-15 de agosto de 1990, Berlín, editorial Springer, DE, Vol. Conf. 10, page(s) 437-455, se conoce un procedimiento en el que un fichero de protocolo, al que

están adjuntados una multitud de valores de Hash, se remiten para el sellado cronofechador, a un servidor de sellos cronofechadores ("time stamping service"). Un inconveniente de este procedimiento consiste en que los datos enviados al servidor de sellos cronofechadores, no tienen una longitud uniforme, de manera que el paquete creado de datos con sello cronofechador, puede ser comparativamente grande.

Por lo demás, por el documento US-A-5 946 396 se conoce un procedimiento con el que se debe de poder constatar dentro de qué lapsos de tiempo se han creado determinados datos de vídeo y de audio. Tanto para los datos de vídeo, como también para los de audio, se crea un código de cifras de comprobación, designado como "aggregate digest". Se propone que este código de cifras de comprobación se lleve a un procedimiento de cronofechado, para la determinación del momento más tardío antes del cual fueron creados los datos de vídeo y de audio. Como procedimiento de cronofechado se cita aquí el procedimiento de la Surety Technologies Inc. En este procedimiento, para cada uno de una multitud de códigos de cifras de comprobación se elabora por pares un código de cifras de comprobación, de orden superior, agrupándose estos códigos antepuestos de cifras de comprobación, en otro código de cifras de comprobación, y desde luego en forma arborescente, de manera que al final se cree un "composite digest" que es válido para todos los códigos antepuestos de cifras de comprobación. Este composite digest se publica en una multitud de publicaciones, para dar a conocer que los códigos de cifras de comprobación identificados con este "composite digest" han existido en el momento de la publicación. Para conducir la prueba de que un determinado juego de datos, en un momento posterior, corresponde al juego cronofechado de datos, tienen que suministrarse determinadas informaciones, a saber, el "composite digest" publicado, el "aggregate digest", así como una multitud de códigos antepuestos de cifras de comprobación, que se utilizan para la creación del "composite digest", y finalmente el algoritmo de Hash utilizado. Con este procedimiento no es posible una comprobación automatizada de la "autenticidad" de datos.

Así pues la misión de la presente invención se basa en perfeccionar un procedimiento del tipo citado en el preámbulo, de tal manera que pueda aprovecharse mejor la capacidad de tales sistemas de signatura, y sea posible poder proveer con sellos cronofechadores un número comparativa y esencialmente mayor de juegos de datos, dentro de un determinado espacio de tiempo.

Esta misión se resuelve con un procedimiento con las notas características de la reivindicación 1.

La idea fundamental de la invención consiste en proveer un código de cifras de comprobación con un sello cronofechador que identifique no sólo un juego concreto de datos, sino más bien una multitud de códigos de cifras de comprobación, cada uno de los cuales identifica al menos un juego de datos, de manera que en suma, un sello cronofechador tenga validez para una multitud de jugos de datos. Así, un segundo código de cifras de comprobación puede identificar directamente, o bien uno, o bien varios juegos de datos en su totalidad, o si no, otra pluralidad de códigos de cifras de comprobación, mediante los cuales pueden identificarse a su vez uno o varios juegos de datos.

Si debe de verificarse que un determinado juego de datos ha sido provisto en un tiempo determinado con un sello cronofechador, se comprueba por una parte, si un primer código de cifras de comprobación creado a partir de los segundos códigos de cifras de comprobación adjuntos al paquete de datos con sello cronofechador, coincide con el primer código de cifras de comprobación contenido en el paquete de datos con sello cronofechador. Además, a partir del juego de datos se elabora un segundo código de cifras de comprobación, y se compara con el segundo código de cifras de comprobación que está adjuntado al paquete de datos con sello cronofechador. Si los dos coinciden, el sello cronofechador es válido para el juego de datos.

Lo correspondiente es válido cuando el segundo código de cifras de comprobación no identifica directamente el juego de datos, sino que se formó a partir de uno u otros varios códigos de cifras de comprobación. En este caso, de la mano de todos los otros códigos de cifras de comprobación, necesarios para la creación de uno de los segundos códigos de cifras de comprobación, y que están adjuntos igualmente al paquete de datos con sello cronofechador, se comprueba si a partir de este puede producirse el correspondiente segundo código de cifras de comprobación, Además, se comprueba si un código de cifras de comprobación formado a partir del juego de datos, es idéntico con uno de los otros códigos de cifras de comprobación. Si puede contestarse afirmativamente a las dos cosas, el sello cronofechador es válido para el correspondiente juego de datos.

En suma se adjudica pues exactamente un sello cronofechador para una multitud de juegos de datos que pueden identificarse todos ellos mediante segundos o ulteriores códigos de cifras de comprobación, siempre y cuando el paquete de datos con sello cronofechador se ponga en comunicación de nuevo con todos los códigos de cifras de comprobación utilizados para su creación, así como con los correspondientes juegos de datos.

La capacidad de un sistema de signatura del tiempo gestionado de tal manera para la signatura por sello cronofechador, es con ello mucho mayor que en la gestión convencional conocida previamente, en la que un sello cronofechador se asigna exactamente a un juego de datos. Con independencia de una posible codificación del paquete de datos con sello cronofechador para aumentar su valor probatorio, un sistema semejante puede utilizarse para el archivo de datos electrónicos propios.

En una realización preferente del procedimiento según la invención, el paquete de datos con sello cronofechador contiene una signatura codificada con una clave privada, identificando el código de la signatura, la combinación del primer código de cifras de comprobación y los datos del sello cronofechador. Si se utiliza una signatura como sucede por lo regular en las cajas de seguridad descritas al comienzo, el paquete de datos con sello cronofechador contiene un alto valor probatorio, puesto que la creación de la signatura dentro de la caja de seguridad, está protegida muy ampliamente contra manipulación desde el exterior, y una manipulación de la signatura tendría como consecuencia su destrucción, a causa de su codificación. En este caso ya no podría comprobarse más si a partir del primer código de cifras de comprobación y de los datos del sello cronofechador, se puede calcu-

lar un código de signatura que corresponda al código cifrado de signatura.

Lo correspondiente es válido cuando, según otro procedimiento preferente, en lugar de la utilización de una signatura, o como complemento a la utilización de una signatura codificada, se cifra todo el paquete de datos con sello cronofechador, opcionalmente junto con los segundos códigos adjuntados de cifras de comprobación. Para el cifrado puede utilizarse, por ejemplo, un conocido procedimiento PGP [Pretty Good Privacy].

En especial en la utilización del procedimiento según la invención, junto con cajas de seguridad, existe la ventaja respecto a cajas de seguridad que trabajen en forma convencional, de que para la generación del código de cifras de comprobación para un determinado juego de datos, no existen las exigencias de fiabilidad y manejabilidad, como las que existen para la coordinación de un sello cronofechador a un código de cifras de comprobación. Con ello, para la generación de códigos de cifras de comprobación a partir de juegos de datos y para la agrupación de varios códigos de cifras de comprobación en uno primero, puede utilizarse un sistema sencillo de cómputo.

En otro acondicionamiento preferente del procedimiento está previsto que el paquete de datos con sello cronofechador, esté codificado con la clave pública de un receptor de sellos cronofechadores, y sólo pueda abrirse con su clave personal. De este modo puede asegurarse que solamente el receptor de sellos cronofechadores pueda analizar el paquete de datos con sello cronofechador.

Para la realización de un sistema de signatura del tiempo que trabaje en la forma según la invención, dentro de una red, en un ordenador central se calcula de preferencia para cada juego de datos a sellar, un segundo código de cifras de comprobación, y todos los segundos códigos de cifras de comprobación se remiten a un servidor de sellos cronofechadores que se encuentra en la red, y en el cual se crea el paquete de datos con sello cronofechador. Aquí el servidor de sellos cronofechadores puede presentar una caja de seguridad a la que sé preconecta un software del servidor, que recibe de un remitente los segundos códigos de cifras de comprobación de los juegos de datos o ficheros a sellar, los agrupa y para ello crea un primer código de cifras de comprobación, y alimenta el primer código de cifras de comprobación a la caja de seguridad. El paquete de datos con sello cronofechador emitido por la caja de seguridad es devuelto entonces por el software del servidor, al ordenador central, junto con los correspondientes segundos códigos de cifras de comprobación.

En otra forma de gestión según la invención, el primer código de cifras de comprobación se crea ya en el ordenador principal, y se envía al servidor de sellos cronofechadores. Entonces la coordinación de todos los segundos códigos de cifras de comprobación con el paquete creado de datos con sello cronofechador, se lleva a cabo en el calculador principal, tan pronto haya recibido el correspondiente paquete de datos con sello cronofechador, del servidor de sellos cronofechadores. De este modo se suprimen en el servidor de sellos cronofechadores, las etapas de cómputo para la creación del primer código de cifras de comprobación, y de la coordinación de los segundos códigos de cifras de comprobación con el paquete producido de datos con sello cronofechador, que se realizan descentralizadas en el respectivo ordenador central en la red, de manera que está mejor repartida la carga de cómputo. En especial en la utilización de un servidor de sellos cronofechadores con caja de seguridad, se aprovecha así la ventaja del procedimiento según la invención, de que en la creación del código de cifras de comprobación, no existen más exigencias de seguridad que las de la creación del sello cronofechador.

Con estas o similares formas de proceder, puede utilizarse una caja de seguridad mediante la intranet de una empresa, o también mediante una red pública como Internet. Pero básicamente también es posible gestionar una caja propia de seguridad con el procedimiento según la invención, cuando se modifique adecuadamente el software que trabaja en ella.

En suma, con el procedimiento según la invención se puede comprobar con gran fuerza probatoria, no sólo para ficheros electrónicos individuales especialmente importantes, que fueron registrados en un momento determinado y que no se modificaron desde entonces, sino que todos los procesos empresariales desarrollados por vía electrónica, pueden protocolizarse en forma probatoria mediante la signatura del tiempo, en forma justificable económicamente. Esto es válido en especial para el desarrollo electrónico de encargos, por ejemplo, en sistemas de compraventa en línea, sistemas de banca en línea, así como para la protocolización de la recepción y envío de correos electrónicos, y para el archivo de todos los datos electrónicos de una empresa. Aquí no importa nada el formato de los ficheros electrónicos, pueden proveerse con una signatura del tiempo, documentos de texto, datos de audio, datos de vídeo, u otros datos electrónicos. Con ello es posible hacer todos los datos de una empresa a prueba de falsificación, y proteger la empresa de las consecuencias y costes incalculables por la manipulación de sus datos digitales.

A continuación se explica en detalle la invención de la mano de dos figuras.

Se muestran:

Figura 1 Un diagrama de una red con un servidor central de sellos cronofechadores, y con un enlace correspondiente de cliente, y

Figura 2 Un diagrama de operaciones para la creación de un paquete de datos con sello cronofechador, con un procedimiento ejemplar según la invención.

El diagrama representado en la figura 1 de un sistema ejemplar servidor-cliente, muestra la unión de un servidor 1 de sellos cronofechadores que trabaja de conformidad con el procedimiento según la invención, con la red de una empresa. Los datos electrónicos relevantes de una empresa son registrados por cuatro interfaces de aplicación. A estas pertenecen, un escáner 2 de ficheros que está unido con uno o varios servidores de datos, un escáner 3 de correo electrónico que está unido con uno o varios servidores de correo electrónico, un escáner 4 de datos de un banco de datos, así como un escáner 5 para datos del desarrollo del software.

Los datos registrados por estos escáneres se llevan mediante una interfaz 6 de aplicación y una interfaz 7 de distribución, a un generador 8 de cifras de comprobación, que elabora un código de cifras de comprobación para cada juego de datos. Los códigos producidos de cifras de comprobación se hacen seguir después al servidor 1 central de sellos cronofechadores, mediante una interfaz 7 de distribución y una interfaz 9 de comunicación, a través de un enlace 10 de Inter-

net. Aquí los códigos de cifras de comprobación pueden ya agruparse en el generador 8 de cifras de comprobación, elaborando entonces para ello, el generador 8 de cifras de comprobación, un primer código de cifras de comprobación, o si no, se envía cada código de cifras de comprobación al servidor 1 central de sellos cronofechadores, que entonces asume incluso las tareas del agrupamiento y la generación de un primer código de cifras de comprobación. El servidor 1 central de sellos cronofechadores crea para el primer código de cifras de comprobación, un paquete codificado de datos con sello cronofechador, y devuelve este, en su caso junto con los correspondientes códigos de cifras de comprobación a la empresa, a través del enlace 10 de Internet, llegando los datos devueltos a través de la interfaz 9 de comunicación a la interfaz 7 de distribución. La interfaz 7 de distribución se cuida de que los paquetes de datos con sello cronofechador junto con los segundos códigos correspondientes de cifras de comprobación y los juegos de datos, se depositen en un banco 11 de datos de archivo, previsto para ello.

Con qué intervalos de tiempo se procesan de este modo, los juegos de datos y se proveen con un sello cronofechador, depende en lo esencial de las exigencias de protocolización de la empresa. Mientras que en el desarrollo electrónico de operaciones bursátiles, puede ser necesario un sello cronofechador con exactitud de minutos o incluso de segundos y, por tanto, un intercambio continuo de datos entre el servidor de sellos cronofechadores y una empresa, posiblemente es suficiente en un simple desarrollo de un encargo, que se reúnan todos los datos de un día, y se procesen juntos en un momento determinado, y se provean con un sello cronofechador.

La figura 2 muestra esquemáticamente la elaboración del paquete de datos con sello cronofechador. Así, de una multitud de juegos 21 de datos, se elabora un número correspondiente de “segundos” códigos 22 de cifras de comprobación. Estos códigos 22 de cifras de comprobación se agrupan en un juego 23 de datos, para el que se elabora un nuevo “primer” código 24 de cifras de comprobación. Este primer código 24 de cifras de comprobación se une, por ejemplo, en una caja no representada de seguridad, con un sello 25 cronofechador, o sea, con datos que contienen una fecha. Para estos datos 26 unidos unos con otros, se crea un código de signatura que se codifica en una signatura 27, y se encadena junto con los datos 26 unidos, en un paquete 28 de datos con sello cronofechador. Al paquete 28 de datos con sello cronofechador se adjuntan los “segundos” códigos de cifras de comprobación, de manera que se crea un juego 29 de datos de salida, con el que en un momento posterior puede probarse la coordinación correcta del paquete de datos con sello cronofechador, con el “segundo” código 22 de cifras de comprobación.

REIVINDICACIONES

1. Procedimiento para el encadenamiento de datos electrónicos o digitales con un sello (25) cronofechador, en el que se crea un paquete (28) de datos con sello cronofechador, que comprende un primer código (24) de cifras de comprobación, que identifica los datos a sellar, así como datos (25) del sello cronofechador, **caracterizado** porque el primer código (24) de cifras de comprobación identifica una multitud de segundos códigos (22) de cifras de comprobación, identificando cada segundo código (22) de cifras de comprobación al menos un juego (21) de datos a sellar, y adjuntándose cada uno de los segundos códigos (22) de cifras de comprobación al paquete de datos con sello cronofechador.

2. Procedimiento según la reivindicación 1, **caracterizado** porque el paquete (28) de datos con sello cronofechador contiene una clave (27) de signatura codificada con una clave privada, identificando la clave (27) de signatura, la combinación del primer código (24) de cifras de comprobación, y de los datos (25) del sello cronofechador.

3. Procedimiento según la reivindicación 1 ó 2, **caracterizado** porque todo el paquete (28) de datos con sello cronofechador, se cifra opcionalmente junto con los segundos códigos (22) adjuntos de cifras de comprobación.

4. Procedimiento según alguna de las reivindicaciones 1 a 3, **caracterizado** porque el paquete (28) de datos con sello cronofechador está codificado con la clave pública de un receptor de sellos cronofechadores, y sólo puede abrirse con su clave personal.

5. Procedimiento según alguna de las reivindicaciones 1 a 4, **caracterizado** porque existe al menos un juego (21) de datos a sellar en un ordenador central de una red, en el ordenador central se calcula para cada juego (21) de datos un segundo código (22) de cifras de comprobación, y todos los segundos códigos (22) de cifras de comprobación se remiten a un servidor (1) de sellos cronofechadores que se encuentra en la red, y en el cual se crea el paquete (28) de datos con sello cronofechador.

6. Procedimiento según alguna de las reivindicaciones 1 a 4, **caracterizado** porque existe al menos un juego (21) de datos a sellar en un ordenador central de una red, en el ordenador central se calcula para cada juego (21) de datos un segundo código (22) de cifras de comprobación, y para todas las segundas cifras de comprobación se calcula un primer código (24) de cifras de comprobación, y este primer código (24) de cifras de comprobación se remite a un servidor (1) de sellos cronofechadores que se encuentra en la red, en el que se crea el paquete (28) de datos con sello cronofechador.

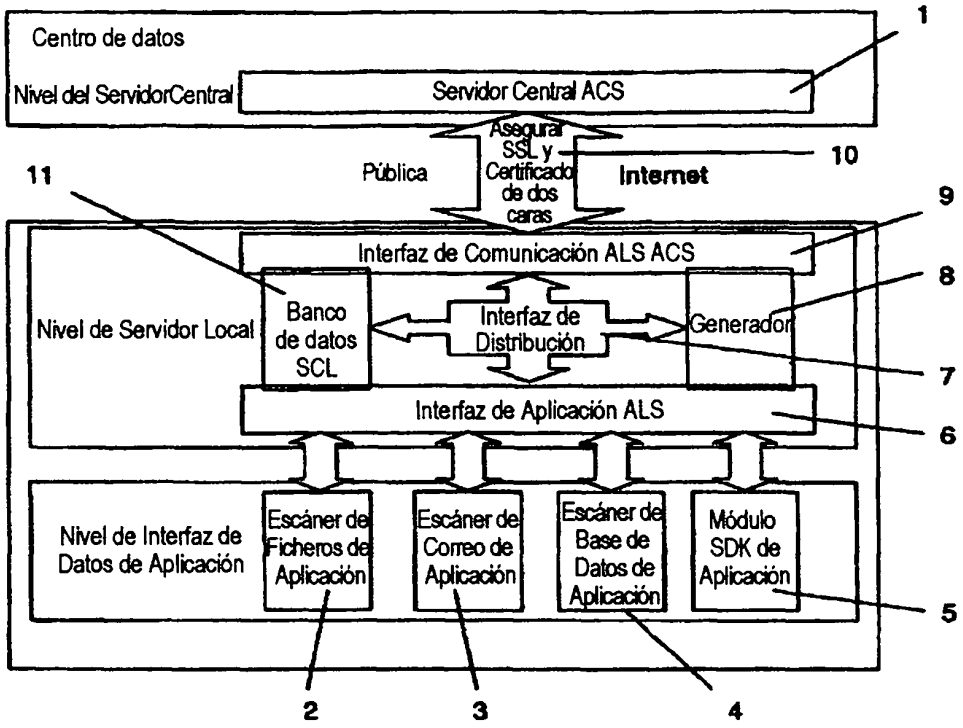

Figura 1

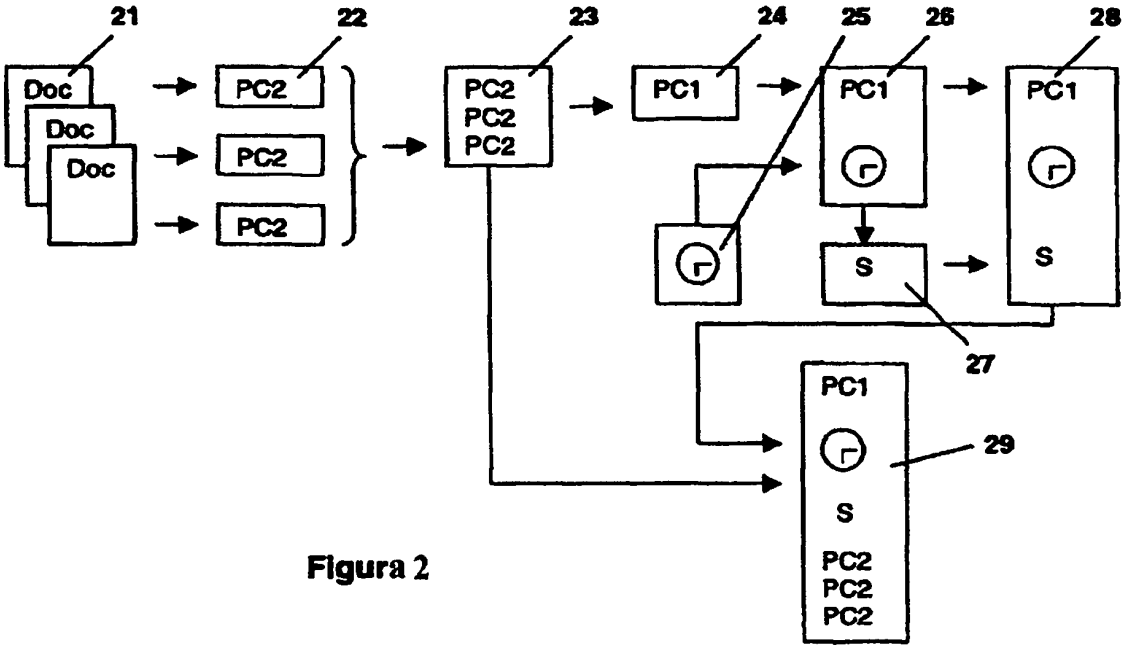

Figura 2