(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 731 651**

(51) Int. CI.:

H04L 9/32 (2006.01)
G06F 21/64 (2013.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **08.07.2009 PCT/EP2009/058657**

(87) Fecha y número de publicación internacional: **14.01.2010 WO10003975**

(96) Fecha de presentación y número de la solicitud europea: **08.07.2009 E 09780305 (0)**

(97) Fecha y número de publicación de la concesión europea: **20.03.2019 EP 2300958**

(54) Título: **Procedimiento y sistema informático para archivar de forma duradera datos firmados certificados**

(30) Prioridad:

08.07.2008 DE 102008031890

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
18.11.2019

(73) Titular/es:

ARTEC COMPUTER GMBH (100.0%)
Robert-Bosch-Straße 38
61184 Karben, DE

(72) Inventor/es:

HETT, CHRISTIAN y
ARTISHDAD, JERRY JOHN

(74) Agente/Representante:

CONTRERAS PÉREZ, Yahel

DESCRIPCIÓN

Procedimiento y sistema informático para archivar de forma duradera datos firmados certificados

La invención se refiere a un procedimiento para archivar de forma duradera datos que son firmados de forma certificada para asegurar su capacidad probatoria así como a un sistema informático para realizar este procedimiento. El procedimiento de acuerdo con la invención realiza el archivo de tal modo que la validez legal de los datos se mantiene durante más tiempo mediante una renovación de las firmas.

Con el avance de la "oficina sin papel" y el hecho cada vez más frecuente de que los documentos para los que existe un periodo de 30 años o más durante el que deben conservarse legalmente tanto en las empresas como en la esfera privada ya no están disponibles en forma impresa, o no exclusivamente en forma impresa, sino en forma de datos electrónicos, existe una necesidad cada vez mayor de hacer posible el archivar los datos resultantes de forma segura legalmente. Dado que los documentos en forma electrónica son fácilmente modificables, se deben proporcionar medidas para asegurar que los datos archivados se encuentran en su estado original.

Dado que tales documentos constituyen pruebas que pueden ser utilizadas judicialmente, el legislador ha impuesto estrictos requisitos. El legislador alemán ha traspuesto la directiva de la Unión Europea 1999/93/EG ("directiva de firma"), que regula el uso de las firmas electrónicas, con la ley de firma alemana (SigG) y el decreto de firma alemán (Sig). De acuerdo con ello, un documento electrónico provisto de una firma electrónica certificada es considerado equivalente a la forma escrita. La firma electrónica certificada tiene en gran medida el mismo efecto legal que la firma escrita a mano. Por tanto, los documentos firmados de este modo como, por ejemplo, correos electrónicos o facturas electrónicas pueden utilizarse judicialmente a modo de prueba al igual que los correspondientes en papel.

Sin embargo, a diferencia de los documentos en papel con firma, las firmas electrónicas pierden su validez legal transcurrido cierto tiempo. Para generar las firmas se utilizan algoritmos criptográficos que, debido al desarrollo avanzado de la informática y los análisis criptográficos asociados cada vez mejores, sólo son considerados como seguros contra falsificación durante un tiempo limitado.

En general, un valor denominado valor resumen ("hash value") es calculado a partir del documento a firmar por medio de una función resumen ("hash function"), estando caracterizado por que representa una especie de huella digital del documento correspondiente, la función siendo unidireccional y resistente a colisiones. Esto significa que a partir de un documento de cualquier tamaño se calcula un valor pequeño de una longitud determinada y que permite extraer conclusiones sobre modificaciones en el documento pues dos documentos diferentes siempre proporcionan valores resumen significativamente diferentes (resistencia a colisiones) y a partir del valor resumen no se puede recalcular el documento original (unidireccionalidad). Posteriormente, el valor resumen obtenido de este modo es encriptado con una clave privada secreta, vinculado a un sello de tiempo con el momento actual y provisto con la firma del servicio de sello de tiempo. Para archivar los ficheros, los ficheros de firma pueden ser archivados separadamente del fichero original o adjuntos al mismo. Otra posibilidad es utilizar ficheros contenedores (por ejemplo, PKCS#7, etc.), que contienen tanto el original como los ficheros de firma y, en su caso, información adicional sobre la firma. Si transcurrido un cierto tiempo el aumento de la capacidad de computación o nuevos hallazgos matemáticos hicieran posible quebrantar los algoritmos resumen utilizados, el fichero firmado podría ser posteriormente manipulado. Por tanto, para tales algoritmos se estable un periodo de validez por la autoridad reguladora de correos y telecomunicaciones alemana ("Regulierungsbehörde für Telekommunikation und Post", RegTP).

Para asegurar la validez legal de los datos archivados, el límite temporal establecido para los algoritmos en el decreto de firma alemán ha de ser extendido mediante las medidas apropiadas, proporcionando el propio decreto de firma alemán medidas correspondientes. Así, "los datos deben estar provistos de una nueva firma electrónica certificada antes del momento en que el propio algoritmo o los parámetros asociados expiren. Esto debe efectuarse con nuevos algoritmos apropiados o parámetros asociados, incluyendo firmas previas y llevando un sello de tiempo certificado".

Para el usuario esto supone el inconveniente de que, por una parte, debe vigilar la validez de las firmas y, por otra parte, en caso necesario debe obtener una nueva firma. Dado que de acuerdo con la ley de firma y el decreto de firma alemanes la concesión de firmas electrónicas certificadas está sujeta a unas normas mínimas de seguridad para los centros de datos y que los correspondientes proveedores sólo son autorizados tras un examen exhaustivo, los proveedores de servicios de firma certificada son por lo general servicios de pago. Por tanto, cada firma certificada obtenida representa un coste añadido. Si, por ejemplo, todos los correos electrónicos deben ser archivados en una empresa, pueden alcanzarse cantidades significativas económicamente.

A partir del estado de la técnica son bastante conocidos procedimientos para generar valores resumen ("hash values") y árboles resumen ("hash trees") y para crear sellos de tiempo ("timestamps") certificados. El coste de un

sello de tiempo certificado, que garantiza la validez de los datos por sí solo, para un elevado volumen de datos a asegurar diariamente como, por ejemplo, correos electrónicos, facturas electrónicas, faxes, ficheros de impresión, etc., conlleva un coste considerable.

El documento DE 10 2006 025 369 B4 describe un procedimiento y un dispositivo para asegurar la integridad y/o no repudio de comunicaciones de tiempo crítico basadas en paquetes. En este caso, para aplicar procedimientos de seguridad digital técnicos, respectivamente, un número de paquetes que puede definirse son comprimidos en un intervalo y los intervalos vinculados entre sí. Los procedimientos de seguridad digitales técnicos aplicados pueden también incluir adjuntar una firma electrónica o un sello de tiempo electrónico.

El documento WO2008061389A1 describe un procedimiento para gestionar documentos para un archivado seguro a efectos de auditorías en el que en una primera etapa a) partiendo de un primer documento digital se genera un primer conjunto de datos que contiene un valor resumen del documento digital y un sello de tiempo interno, y entonces en otra etapa b) este primer conjunto de datos es registrado como una entrada de registro y las etapas a) a b) se repiten para al menos otro documento y, de este modo, se forma un fichero de registro con al menos dos entradas de registro, y el fichero de registro es completado en una organización de sellado de tiempo certificada de acuerdo con criterios de terminación predeterminados y de transmisión del valor resumen del registro o del valor resumen de una clave pública, y desde la organización de sellado de tiempo es recibida una firma de sello de tiempo, que es calculada por medio del valor resumen del registro o por medio del valor resumen de la clave pública y por medio de un sello de tiempo certificado de la organización de sellado de tiempo y de forma encriptada con una clave de la organización de sellado de tiempo, y el registro así como su firma de sello de tiempo son almacenados en un repositorio. El documento también describe un dispositivo para efectuar este procedimiento, el cual incluye un servidor para crear el sello de tiempo y/o las firmas de sello de tiempo para cada documento a almacenar, una unidad de registro para adquirir el sello de tiempo y/o las firmas de sello de tiempo para un fichero de registro único y una conexión de comunicación a una organización de sellado de tiempo certificada.

El documento “Long-term trusted preservation service using service interaction protocol and evidence records" de la revista “Computer Standards & Interfaces”, volumen 29, páginas 398-412 (2007) de la publicación ScienceDirect describe un procedimiento para archivar datos (“Trusted Archive Services”, TAS) con una función de firma duradera, que consiste en las etapas del firmado de los datos a archivar (“evidence record generation”) y en el criptografiado de los datos firmados (“evidence record maintenance”), la firma siendo obtenida por el procedimiento normalizado por el “Long-term-Archiving and Notary Service” (IETF LTANS WG) y recurriendo con ello para el criptografiado a los sistemas de la infrastructura de clave pública. El documento también describe un sistema informático, que incluye los bloques constructivos de uno o más terminales informáticos (“clients”), de una red de archivo (“long-term archive protocol”) con una interfaz a los terminales, una gestión de datos (“data management”) con un medio de almacenamiento masivo (“data storage”), un reconocimiento de datos (“data validation”), un firmado (“evidence record generation and management”) y, opcionalmente, una interpretación de datos (“data interpretation”) para mantener los datos cuando el entorno de datos cambia, por ejemplo, en una migración de datos.

El documento WO0233886A2 describe un procedimiento para la trasmisión segura de datos usando un aparato para el procesamiento de datos (COM), que es conectable a una unidad de almacenamiento (ARC), configurada de forma separada físicamente del aparato, por medio de al menos una línea de datos (DAT), a través de la cual son intercambiables datos entre el aparato para el procesamiento de datos y la unidad de almacenamiento, tal que en una etapa a) con el aparato para el procesamiento de datos (COM) datos (dat) almacenados al menos en el aparato o un archivo asociado al aparato son provisto de una firma (has*), y en una etapa posterior b) al menos los datos (dat) encriptados así como la firma (has*) digital son provistos de un encriptado de transporte (ssl) y así son transmitidos por medio de una línea de datos (DAT) a la unidad de almacenamiento (ARC). En una forma de realización del procedimiento, en la etapa b) la firma (has*) digital es encriptada junto con los datos (dat) y en la etapa c) la firma (has*) encriptada con los datos así como los datos (has*) son provistos del encriptado de transporte. El documento describe también un aparato para realizar este procedimiento.

El objeto técnico de la presente invención es proporcionar un dispositivo y un procedimiento para archivar de forma legamente segura datos electrónicos que reduzca significativamente la cantidad de los sellos de tiempo certificados a adquirir y por tanto el coste del procedimiento respecto a los procedimientos convencionales.

El objeto técnico se consigue con el procedimiento de acuerdo con la invención (reivindicación 1) para archivar de forma duradera datos firmados certificados, que comprende las siguientes etapas de procedimiento:

- resumir los datos;
- encriptar los datos por medio de un algoritmo criptográfico;
- resumir los datos encriptados;
- firmar los datos resumidos con un sello de tiempo avanzado al final de un intervalo de tiempo preseleccionado, tal que la firma incluye tanto un valor resumen de los datos como un valor resumen de los datos encriptados;

- generar un árbol resumen sobre la base de datos completa o subgrupos de la misma;
- firmar el o los árboles resumen por medio de un sello de tiempo certificado, mediante el cual el sello de tiempo avanzado es confirmado por un sello de tiempo certificado, por lo que sólo se requiere un sello de tiempo de pago en el intervalo de tiempo preseleccionado, tal que para generar las firmas se utilizan algoritmos criptográficos;
- suministrar automáticamente en el archivo los datos a archivar sin ninguna acción adicional por parte de un usuario;

tal que el procedimiento se ejecuta en un sistema informático que comprende las siguientes características:

- una y/o varias interfaces para conectar cada una a un servidor para proporcionar los sellos de tiempo y firmas avanzados y/o certificados;
- un dispositivo criptográfico;
- uno y/o varios medios de almacenamiento masivo;
- una y/o varias interfaces adecuadas para el flujo de datos a archivar, estando configurada o configuradas de tal modo que pueda efectuarse un archivado automático.

La idea básica detrás de la invención es reducir el número de los sellos de tiempo certificados requeridos remplazándolos por sellos de tiempo avanzados en un intervalo de tiempo determinado, siendo entonces los mismos confirmados por un sello de tiempo certificado para el intervalo de tiempo preseleccionado. Así, por ejemplo, durante un día el sellado de todos los datos puede realizarse con sellos de tiempo avanzados sin coste, siendo entonces los mismos confirmados al final del día conjuntamente con un sello de tiempo certificado; de este modo sólo es necesario un sello con coste por día.

Dado que los sellos de tiempo avanzados son firmados en un árbol resumen resumidamente con el sello de tiempo certificado, la fecha es asegurada con mayor valor probatorio para estos datos sellados. La hora del sello avanzado no cumple los estrictos requisitos de seguridad legal en el marco de la ley de firma alemana (SigG) o el decreto de firma alemán (SigV), no obstante dado que los sellos están provistos adicionalmente con el sello certificado, se les concede usualmente un mayor valor probatorio que a sólo los sellos de tiempo avanzados exclusivos.

Además, las principales cuestiones de seguridad se derivan sólo de una fecha segura pero no de una hora exacta.

En detalle, el procedimiento de acuerdo con la invención es como sigue. Primero, los datos son resumidos por medio de una función resumen. En una variante de realización preferible, con ello se generan inmediatamente varios valores resumen con una selección de más de un algoritmo resumen, preferiblemente de 2-10, más preferiblemente de 5-7. Estos algoritmos resumen se seleccionan de modo que pueden ser clasificados como seguros para un tiempo lo más prolongado posible. De este modo, los valores resumen son creados en cierto modo de forma anticipada, de manera que en el caso de una clasificación posterior del algoritmo resumen utilizado para la firma como no seguro no haya que recurrir a los datos archivados sino que pueda utilizarse simplemente el último válido a partir de los valores resumen. Idealmente, el sello completo requerido para el periodo de retención puede ser proporcionado a partir de la provisión de valores resumen sin tener que procesar de nuevo los datos originales.

Posteriormente, el valor resumen es firmado con un sello de tiempo avanzado. Esto puede realizarse o bien en el sistema de archivo por sí mismo, que entonces está equipado con un dispositivo correspondiente que tiene un reloj interno, con una conexión a un tiempo de referencia externo (por ejemplo, un receptor de una seña DCF77) y con el software de firma correspondiente, o bien por medio de un servidos de sellado de tiempo externo, tal que el acceso a este servidor pueda realizarse tanto por medio de una LAN como por medio de una WAN. Los árboles resumen se forman a partir de los valores resumen así obtenidos. Los árboles pueden extenderse sobre la base de datos completa o sólo sobre subgrupos de la misma, de forma preferible especialmente, sobre los nuevos datos añadidos al intervalo en cada caso.

En una forma de realización de la invención, para mantener la validez legal de la firma de uno o más ficheros el o los árboles resumen se firman de nuevo mediante una firma certificada.

En otra forma de realización de la invención, el árbol resumen se genera sobre la base de datos completa en intervalos de tiempo regulares, en particular, diariamente.

En otra forma de realización de la invención el árbol resumen es generado sobre la base de datos añadida de nuevo en intervalos de tiempo regulares, en particular, diariamente.

En otra forma de realización de la invención, los datos a archivar son correos electrónicos y la firma avanzada es generada cada vez sobre todo el correo electrónico.

En otra forma de realización de la invención, los datos a archivar son correos electrónicos y la firma avanzada es generada cada vez sólo sobre el cuerpo del correo electrónico, incluido cualquier adjunto existente pero no el encabezado.

En una configuración ventajosa de la invención, el requerimiento de la firma certificada es concentrado por el servidor para varios clientes de archivo de manera que sólo es necesario un sello para todos los clientes conjuntamente, lo que reduce adicionalmente el coste. En otra variante ventajosa, los ficheros resumen firmados son archivados en el archivo como los datos archivados, es decir, por ejemplo, como falsos correos electrónicos. Esto hace posible que sea fácil firmar de nuevo los datos resumen cuando sea necesario, simplemente resumiéndolos con los datos de fecha.

En una variante de realización especialmente preferible, los datos de árbol resumen son recopilados en un fichero binario, lo que hace posible una navegación simple y rápida en los datos, por ejemplo, mediante operaciones matemáticas (longitud de bits fija de las entradas). Al final del intervalo de tiempo preseleccionado se efectúa la firma del árbol resumen formado por medio de un sello de tiempo certificado. La petición de esto puede realizarse al proveedor de servicios de firma certificado mediante el propio sistema de archivo o por el servidor que es responsable también de proporcionar la firma avanzada.

En otra forma de realización de la invención, el árbol resumen binario, junto con el sello de tiempo certificado obtenido, es almacenado en el archivo del mismo modo que los datos a archivar.

En otra forma de realización de la invención, los valores de los árboles resumen son recopilados en un banco de datos.

En otra forma de realización de la invención, los datos son resumidos paralelamente en un paso con más de un algoritmo resumen y los valores resumen generados de este modo son almacenados junto con los datos sellados y una referencia al algoritmo utilizado para el sellado.

En otra forma de realización de la invención, el requerimiento del sello de tiempo certificado se hace para una pluralidad de clientes de archivo mediante un servidor de sello de tiempo conjunto de tal modo que los valores resumen transferidos para el sellado son recopilados por el servidor de sellado de tiempo conjunto en una ventana de tiempo regular y son vinculados después del transcurso de la ventana de tiempo, lo que tiene lugar, preferiblemente, por medio de un árbol resumen, entonces son transferidos a un servicio de sellado de tiempo certificado para el sellado y a los clientes de archivo en el siguiente contacto es devuelta una estructura de datos que está provista de un sello de tiempo certificado e incluye el valor resumen transferido.

En otra variante de realización ventajosa, las firmas son monitorizadas mediante el sistema de archivo para comprobar su validez y con la debida antelación a su expiración son enviadas de nuevo para el firmado. Especialmente preferible es una variante en la que los datos son encriptados con ayuda de un algoritmo criptográfico. De este modo no es posible acceder de forma no autorizada a los datos archivados. Por ello para almacenar los datos de archivo puede utilizarse un servicio de almacenamiento que opere a través de una página web sin que la seguridad se vea afectada. La unidad criptográfica prevista para ello en el sistema informático está configurada de modo que sólo es posible descifrar el archivo en el sistema informático utilizado para el cifrado. De este modo, puede excluirse que un sistema informático constructivamente idéntico pueda ser utilizado para descifrar datos de archivo robados.

Si los datos son archivados en el archivo de forma encriptada, la firma avanzada se efectúa en una variante de configuración de tal modo que incluya tanto el valor resumen del fichero original no encriptado como el valor resumen del fichero de archivo encriptado. Esto hace posible comprobar la integridad de los datos incluso sin tener acceso a la función criptográfica del sistema informático de archivo.

Para satisfacer los requerimientos de la ley de firma y del decreto de firma alemanes con respecto a la diligencia debida durante el archivado, en otras variantes de realización preferibles se efectúa por el sistema informático de archivo la creación de un archivo de registro (“log file”), en el que todos los accesos de archivo son registrados por el administrador, así como un examen de consistencia de todos los documentos archivados activado manualmente y/o automáticamente en intervalos determinados con la generación de un informe. Tanto los archivos de registro como ficheros de informe son también firmados y almacenados en el archivo como los propios datos (es decir, por ejemplo, como falsos correos electrónicos). Esto permite a un administrador probar que ha satisfecho su obligación de diligencia debida y que ha comprobado la pérdida de datos de su archivo con regularidad.

El procedimiento de archivo puede ser usado para cualquier tipo de ficheros. Son concebibles archivos para correos electrónicos que pueden ser añadidos automáticamente en el archivo, archivos de registro que funcionan como una solución de copia de seguridad (“backup”) y con ello pueden documentar diversos estados de procesamiento de

ficheros, archivos de documentos que representan un depósito de expedientes a partir de documentos de texto y/o dibujos creados y, además de los ficheros de documentos, por ejemplo, también pueden ser creados a partir de los datos enviados a una impresora. Además, archivos de fax o archivos de documento son posibles a partir de originales en papel. En una forma de realización preferible de la invención, los datos de archivo son archivados de forma que puedan ser buscados en el archivo. Para ello, se efectúa una indexación y depósito una estructura de banco de datos – en su caso, tras una conversión de ficheros de imágenes en ficheros de datos por medio de OCR-. El acceso tanto a las funciones de archivo administrativas y operativas como a los propios datos archivados se efectúa de forma especialmente preferible por medio de una conexión segura (SSL) a un servicio web que se ejecuta en el sistema informático de archivo. Así, son posibles tanto el acceso desde una LAN como por medio de internet. Mediante la utilización de una interfaz de usuario en el buscador web, puede efectuarse el acceso en el archivo sin una instalación de software adicional e independientemente del sistema operativo del cliente utilizado.

También se reivindica un sistema informático (reivindicación 12) para archivar de forma duradera datos firmados certificados, que está caracterizado por que el sistema informático comprende las siguientes características:

- una y/o varias interfaces para conectar cada una a un servidor para proporcionar los sellos de tiempo y firmas avanzados y/o certificados;
- un dispositivo criptográfico;
- uno y/o varios medios de almacenamiento masivo;
- una y/o varias interfaces adecuadas para el flujo de datos a archivar, estando configurada o configuradas de tal modo que pueda efectuarse un archivado automático;

y está instalado para realizar las siguientes etapas

- resumir los datos;
- encriptar los datos por medio de un algoritmo criptográfico;
- resumir los datos encriptados;
- firmar los datos resumidos con un sello de tiempo avanzado al final de un intervalo de tiempo preseleccionado, tal que la firma incluye tanto un valor resumen de los datos como un valor resumen de los datos encriptados;
- generar un árbol resumen sobre la base de datos completa o subgrupos de la misma;
- firmar el o los árboles resumen por medio de un sello de tiempo certificado, mediante el cual el sello de tiempo avanzado es confirmado por un sello de tiempo certificado, por lo que sólo se requiere un sello de tiempo de pago en el intervalo de tiempo preseleccionado, tal que para generar las firmas se utilizan algoritmos criptográficos;
- suministrar automáticamente en el archivo los datos a archivar sin ninguna acción adicional por parte de un usuario.

En una forma de realización de la invención, el dispositivo criptográfico está configurado de modo que un desencriptado de los datos sólo es posible en el sistema informático usado, respectivamente, para el encriptado.

Para la integración de acuerdo con la invención del sistema informático en el flujo de datos que hace posible suministrar en el archivo los datos a archivar automáticamente sin ninguna acción adicional por parte del usuario, hay varias posibilidades. La ejecución de las interfaces al flujo de datos depende sustancialmente del tipo de datos a archivar. Para el caso de un archivo de correo electrónico existen, entre otras, dos variantes de realización preferibles. En una de las variantes el sistema de archivo está instalado entre el servidor de correo (por ejemplo, “Sendmail”, “Microsoft Exchange”, “Lotus Notes”, “Novel GroupWise”) y la puerta de enlace de internet o un cortafuegos (“firewall”) y reenvía los correos electrónicos entrantes o salientes después de que se haya dejado una copia para el archivo. En la otra variante el sistema de archivo proporciona al servidor de correo una copia del correo electrónico transferido. Alternativamente, sería posible monitorizar el directorio de depósito del servidor de correo para los correos electrónicos y desde ahí hacer copias en el archivo. Sin embargo, este método encierra el riesgo de que los datos de correos electrónicos originales ya no se encuentren almacenados en estos directorios.

Para archivar los documentos impresos, un controlador de impresora es una interfaz adecuada para el sistema de archivo. El sistema de archivo proporciona un controlador que opera antes del propio controlador de impresora. Los datos de impresión que se envían a la impresora instalada son copiados desde el controlador de archivo en el archivo y entonces reenviados al controlador de la impresora. De este modo, todos los documentos impresos son registrados automáticamente en el archivo. Para el registro de documentos en papel puede usarse una captura manual por medio de un escáner. Pero en este caso también existe la posibilidad de establecer un controlador antes del controlador de escáner, análogamente al controlador de impresora, que suministre automáticamente todos los documentos escaneados en el archivo.

Tanto para los documentos impresos como para los documentos escaneados, se efectúa por otra parte una indexación después de la conversión en formato de papel y un almacenamiento de forma que puedan ser buscados en un sistema de banco de datos.

En otra forma de realización de la invención, en el caso de que los datos a archivar sean correos electrónicos, el sistema informático está instalado en el servidor de correo electrónico y recibe de éste copias de los correos electrónicos.

También se reivindica un programa informático (reivindicación 16) para realizar el procedimiento, con un código de programa que está almacenado en un soporte legible por máquina si el programa es ejecutado en un ordenador.

REIVINDICACIONES

1. Procedimiento para archivar de forma duradera datos firmados certificados, que comprende las siguientes etapas de procedimiento:
- resumir los datos;
- encriptar los datos por medio de un algoritmo criptográfico;
- resumir los datos encriptados;
- firmar los datos resumidos con un sello de tiempo avanzado al final de un intervalo de tiempo preseleccionado, tal que la firma incluye tanto un valor resumen de los datos como un valor resumen de los datos encriptados;
- generar un árbol resumen sobre la base de datos completa o subgrupos de la misma;
- firmar el o los árboles resumen por medio de un sello de tiempo certificado, mediante el cual el sello de tiempo avanzado es confirmado por un sello de tiempo certificado, por lo que sólo se requiere un sello de tiempo de pago en el intervalo de tiempo preseleccionado, tal que para generar las firmas se utilizan algoritmos criptográficos;
- suministrar automáticamente en el archivo los datos a archivar sin ninguna acción adicional por parte de un usuario.

2. Procedimiento según la reivindicación 1, **caracterizado por que** para mantener la validez legal de la firma de uno o más ficheros el o los árboles resumen se firman de nuevo mediante una firma certificada.

3. Procedimiento según las reivindicaciones 1 y 2, **caracterizado por que** el árbol resumen se genera sobre la base de datos completa en intervalos de tiempo regulares, en particular, diariamente.

4. Procedimiento según las reivindicaciones 1 y 2, **caracterizado por que** el árbol resumen es generado sobre la base de datos añadida de nuevo en intervalos de tiempo regulares, en particular, diariamente.

5. Procedimiento según una de las reivindicaciones 1 a 4, **caracterizado por que** los datos a archivar son correos electrónicos y la firma avanzada es generada cada vez sobre todo el correo electrónico.

6. Procedimiento según una de las reivindicaciones 1 a 4, **caracterizado por que** los datos a archivar son correos electrónicos y la firma avanzada es generada cada vez sólo sobre el cuerpo del correo electrónico, incluido cualquier adjunto existente pero no el encabezado.

7. Procedimiento según una de las reivindicaciones 1 a 6, **caracterizado por que** los valores de los árboles resumen son recopilados en un fichero binario.

8. Procedimiento según la reivindicación 7, **caracterizado por que** el árbol resumen binario, junto con el sello de tiempo certificado obtenido, es almacenado en el archivo del mismo modo que los datos a archivar.

9. Procedimiento según una de las reivindicaciones 1 a 6, **caracterizado por que** los valores de los árboles resumen son recopilados en un banco de datos.

10. Procedimiento según una de las reivindicaciones 1 a 9, **caracterizado por que** los datos son resumidos paralelamente en un paso con más de un algoritmo resumen y los valores resumen generados de este modo son almacenados junto con los datos sellados y una referencia al algoritmo utilizado para el sellado.

11. Procedimiento según una de las reivindicaciones 1 a 10, **caracterizado por que** el requerimiento del sello de tiempo certificado se hace para una pluralidad de clientes de archivo mediante un servidor de sello de tiempo conjunto de tal modo que los valores resumen transferidos para el sellado son recopilados por el servidor de sellado de tiempo conjunto en una ventana de tiempo regular y son vinculados después del transcurso de la ventana de tiempo, lo que tiene lugar, preferiblemente, por medio de un árbol resumen, entonces son transferidos a un servicio de sellado de tiempo certificado para el sellado y a los clientes de archivo en el siguiente contacto es devuelta una estructura de datos que está provista de un sello de tiempo certificado e incluye el valor resumen transferido.

12. Sistema informático para archivar de forma duradera datos firmados certificados, tal que el sistema informático comprende las siguientes características:
- una y/o varias interfaces para conectar cada una a un servidor para proporcionar los sellos de tiempo y firmas avanzados y/o certificados;
- un dispositivo criptográfico;
- uno y/o varios medios de almacenamiento masivo;
- una y/o varias interfaces adecuadas para el flujo de datos a archivar, estando configurada o configuradas de tal modo que pueda efectuarse un archivado automático;
y está instalado para realizar las siguientes etapas
- resumir los datos;

- encriptar los datos por medio de un algoritmo criptográfico;
- resumir los datos encriptados;
- firmar los datos resumidos con un sello de tiempo avanzado al final de un intervalo de tiempo preseleccionado, tal que la firma incluye tanto un valor resumen de los datos como un valor resumen de los datos encriptados;
- generar un árbol resumen sobre la base de datos completa o subgrupos de la misma;
- firmar el o los árboles resumen por medio de un sello de tiempo certificado, mediante el cual el sello de tiempo avanzado es confirmado por un sello de tiempo certificado, por lo que sólo se requiere un sello de tiempo de pago en el intervalo de tiempo preseleccionado, tal que para generar las firmas se utilizan algoritmos criptográficos;
- suministrar automáticamente en el archivo los datos a archivar sin ninguna acción adicional por parte de un usuario.

13. Sistema informático según la reivindicación 12, **caracterizado por que** la unidad criptográfica está configurada de tal como que un desencriptado de los datos sólo es posible en el sistema informático usado, respectivamente, para el encriptado.

14. Sistema informático según una de las reivindicaciones 12 y 13, **caracterizado por que**, en el caso de que los datos a archivar sean correos electrónicos, el sistema informático está instalado entre el servidor de correo electrónico y la puerta de enlace de internet.

15. Sistema informático según una de las reivindicaciones 12 y 13, **caracterizado por que**, en el caso de que los datos a archivar sean correos electrónicos, el sistema informático está instalado en el servidor de correo electrónico y recibe de éste copias de los correos electrónicos.

16. Programa informático para realizar el procedimiento según una de las reivindicaciones 1 a 11 con un código de programa que está almacenado en un soporte legible por máquina si el programa es ejecutado en un ordenador.

REFERENCIAS CITADAS EN LA DESCRIPCIÓN

Esta lista de referencias citadas por el solicitante es únicamente para la comodidad del lector. No forma parte del documento de la patente europea. A pesar del cuidado tenido en la recopilación de las referencias, no se pueden excluir errores u omisiones y la EPO niega toda responsabilidad en este sentido.

Documentos de patentes citados en la descripción

- DE 102006025369 B4
- WO 2008061389 A1
- WO 0233886 A2

Literatura diferente de patentes citada en la descripción

- Long-term trusted preservation service using service interaction protocol and evidence records. *Zeitschrift Computer Standards & Interfaces,* 2007, vol. 29, 398-412