(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 743 611**

(51) Int. CI.:

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: **06.09.2006 PCT/US2006/034581**

(87) Fecha y número de publicación internacional: **22.03.2007 WO07032968**

(96) Fecha de presentación y número de la solicitud europea: **06.09.2006 E 06814178 (7)**

(97) Fecha y número de publicación de la concesión europea: **12.06.2019 EP 1922650**

(54) Título: **Directiva de firma digital**

(30) Prioridad:

09.09.2005 US 223255

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
20.02.2020

(73) Titular/es:

MICROSOFT TECHNOLOGY LICENSING, LLC (100.0%)
One Microsoft Way
Redmond, WA 98052, US

(72) Inventor/es:

DE MELLO, MARCIO y
DHALLA, MAHMOOD, A.

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

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

Directiva de firma digital

Antecedentes

La adopción de tecnologías sin papel se ha visto entorpecida por la reticencia de muchos usuarios a utilizar firmas digitales para firmar documentos. Muchos de estos usuarios están confundidos con respecto a lo que quiere decir en realidad una firma digital de un documento. Los usuarios también perciben una carencia de control sobre el documento firmado una vez que el documento ha abandonado el control directo del usuario. Por ejemplo, una tercera parte maliciosa puede manipular el documento mientras el documento porta la firma digital del usuario. Como resultado, a menudo los documentos digitales se imprimen y entonces se firman de una forma habitual con pluma y tinta. En ese punto, si se explora el documento o se maneja una copia física, se pierden muchas de las ventajas potenciales.
El documento US 2003/0105950 A1 desvela un procedimiento de distribución de documentos usando información de control de acceso separada en datos invisibles insertados como una marca de agua electrónica y datos visibles descritos en un documento estructurado para lograr la prevención de una alteración no autorizada de datos de documento, la autenticación de los mismos y la prevención de un acceso no autorizado a los mismos. Se designa un intervalo de firma que se va a firmar digitalmente en los datos de documento y el intervalo designado se describe dentro de una etiqueta. El documento EP 0 798 892 A2 desvela un procedimiento y aparato para crear, distribuir y controlar el acceso a documentos digitales usando sobres criptográficos seguros.

Sumario

Se describen técnicas en relación con una directiva de firma digital dirigida. En un caso, un sistema incluye unos medios para almacenar un documento como una pluralidad de partes lógicas. El sistema también incluye unos medios para establecer una configuración de documento cuando una firma digital se aplica al documento, y unos medios para indicar si la configuración de documento se altera subsiguientemente.

Este resumen se proporciona para introducir una selección de conceptos en una forma simplificada, que se describen adicionalmente a continuación en la descripción detallada. No se pretende que este sumario identifique características clave o esenciales de la materia objeto reivindicada, ni se pretende que se use como una ayuda para determinar el ámbito de la materia objeto reivindicada. Un objeto de la invención es la provisión de un control mejorado sobre un documento firmado, incluso cuando el documento abandona el control directo del usuario. Este problema es solucionado por el sistema de la reivindicación 1 y el medio legible por ordenador de la reivindicación 7. En las reivindicaciones dependientes se abordan algunas realizaciones preferidas.

Breve descripción de los dibujos

La figura 1 ilustra un sistema ilustrativo sobre el que se puede materializar una directiva de firma digital de acuerdo con una implementación.
Las figuras 2-6 ilustran configuraciones de documento ilustrativas en las que una directiva de firma digital se puede materializar de acuerdo con una implementación.
La figura 7 ilustra sistemas, dispositivos y componentes ilustrativos en un entorno sobre el que se puede materializar una directiva de firma digital de acuerdo con una implementación.
La figura 8 ilustra un diagrama de procedimiento ilustrativo en relación con una directiva de firma digital de acuerdo con una implementación.

Descripción detallada

VISTA GENERAL

Las técnicas descritas se refieren a una directiva de firma digital para mantener un documento electrónico como firmado digitalmente. Por ejemplo, un usuario publicador puede componer un documento y decidir firmar digitalmente el documento cuando este está satisfecho con su configuración. La directiva de firma digital sirve al nivel de datos subyacente para establecer qué partes del documento englobar con la firma digital para mantener el documento en la configuración firmada por el usuario. Cuando una firma digital se aplica de acuerdo con la directiva de firma digital, cualquier manipulación subsiguiente del documento que viola la directiva invalida la firma digital. Por consiguiente, la presencia continuada de la firma digital representa una evidencia de que el documento no se ha alterado debido a que este se firmó digitalmente. Por lo tanto, la directiva de firma digital facilita un nivel superior de certidumbre acerca de los contenidos de un documento firmado, es decir, ¿tiene, o no, el documento la misma configuración que tenía en el instante en el que se aplicó la firma digital? Este nivel aumentado de certidumbre en relación con la configuración de documento puede contribuir a una productividad aumentada en escenarios tan variados como negociaciones contractuales y composición colaborativa de documentos.

La directiva de firma descrita se utiliza con paquetes de documento y/o tipos de documento que almacenan los datos de un documento dentro de partes o entidades lógicas discretas. Un ejemplo de una configuración de este tipo es una estructura de árbol que tiene una parte raíz identificable y unas partes asociadas para un procesamiento válido de la parte raíz. En una configuración de este tipo, algunas partes almacenan datos en relación con el contenido mientras

que otras partes, tales como la parte raíz, almacenan datos que portan interrelaciones de otras partes. Por ejemplo, una parte se puede referir a un contenido de una página dada, mientras que otra parte se puede referir a una posición de la página dada en relación con otras páginas. A la luz de lo anterior, la directiva de firma digital especifica qué partes subyacentes de un documento o paquete se van a englobar con el fin de que se mantenga la configuración de documento presentada al usuario. Expresado de otra forma, la directiva de firma digital sirve para registrar eficazmente una configuración del documento en el instante en el que el documento se firmó digitalmente de tal modo que la configuración se puede utilizar para detectar cambios subsiguientes al documento. La directiva de firma digital puede detectar tales cambios e invalidar en respuesta la firma del usuario. Al menos algunas implementaciones permiten adicionalmente que el usuario especifique qué otras partes del documento pueden ser alteradas por un usuario futuro y de qué forma. Por ejemplo, un usuario publicador, cuando se firma el documento, puede especificar que un usuario consumidor puede, por ejemplo, añadir anotaciones al documento sin invalidar la firma del usuario publicador.

SISTEMAS ILUSTRATIVOS

La figura 1 muestra un sistema ilustrativo 100 configurado para implementar directivas de firma para determinar si un documento electrónico 101 sigue siendo consistente con una configuración del documento cuando este se firmó digitalmente. El sistema 100 incluye un publicador 102 acoplado con un consumidor 104 por medio de una plataforma de intercambio de datos digitales 106. La plataforma de intercambio de datos digitales puede incluir cualquier medio para transferir los datos digitales. Por ejemplo, se pueden utilizar diversos tipos de redes para transferir el documento electrónico 101. En otro ejemplo, el documento electrónico se puede almacenar en un cierto tipo de medio de almacenamiento, tal como un disco o un dispositivo flash, y se puede transferir físicamente de una persona a otra. En este caso, el publicador 102 incluye programas o software que operan en un dispositivo informático físico para crear una interfaz de usuario para un usuario publicador 114. De forma similar, el consumidor 104 incluye programas o software que operan en un dispositivo informático físico para crear una interfaz de usuario para un usuario consumidor 124.

El sistema 100 está configurado para permitir que el usuario publicador 114 interaccione con el publicador 102 para generar el documento 101 que se puede presentar subsiguientemente al usuario consumidor 124. En algún punto durante el procedimiento de composición de documentos, el usuario publicador puede lograr una configuración de documento que desea firmar digitalmente el usuario publicador. La directiva de firma digital que opera en el publicador 102 especifica qué partes de documento subyacentes son englobadas por la firma digital del usuario publicador suficientemente para mantener la configuración del documento 101. El usuario consumidor 124 puede acceder subsiguientemente al documento 101. El consumidor 104 abre el documento 101 y examina el documento de acuerdo con la directiva de firma digital. En un caso en el que la firma digital del usuario publicador sigue siendo válida, la presencia de la firma válida asegura al usuario consumidor que el documento sigue siendo consistente con la configuración prevista del usuario publicador. En un caso en el que la firma digital se ha invalidado, el usuario consumidor puede actuar en consecuencia basándose en el conocimiento de que el documento se ha alterado. De forma similar, si el documento se devuelve subsiguientemente al usuario publicador, el publicador puede evaluar si la firma digital del usuario publicador sigue siendo válida. El usuario publicador puede entonces actuar en consecuencia sabiendo si el documento se ha alterado o no.

La figura 2 ilustra un ejemplo general de un formato de documento 200 ilustrativo sobre el que se puede implementar una directiva de firma digital de acuerdo con una implementación. En este caso, el formato de documento 200 almacena datos en una pluralidad de partes lógicas discretas. Cuando son analizadas por un publicador o consumidor, las partes lógicas crean colectivamente la configuración del documento tal como se presenta a un usuario, como se indica en general en 202. El documento puede incluir texto, imágenes y/o cualquier otro contenido de documento habitual. En este caso, las partes lógicas se ilustran como una primera parte de documento 204, una segunda parte de documento 206 y una tercera parte de documento 208. Por supuesto, más allá de este ejemplo, otros formatos de documento ilustrativos pueden organizar las partes lógicas de una forma diferente. Por ejemplo, un ejemplo de una organización de tipo árbol de partes lógicas se describe posteriormente.

Considérese, para fines de explicación, un escenario en el que el autor o usuario publicador desea aplicar su firma digital al documento 202 en su presente forma o configuración. La directiva de firma digital especifica qué partes del documento son englobadas por la firma digital para establecer la presente configuración. Por ejemplo, supóngase que, en este ejemplo, la directiva de firma digital engloba la totalidad de las tres partes de documento 204, 206 y 208 con la firma digital. Cualquier alteración subsiguiente de cualquiera de las partes especificadas da lugar a que se invalide la firma digital del usuario publicador. Por consiguiente, una firma digital válida indica que el documento existe en la configuración en la que este se firmó. En algunas implementaciones, la directiva de firma digital puede permitir que el usuario publicador especifique datos adicionales que se pueden añadir al documento sin invalidar su firma digital. Ejemplos de tales implementaciones se describen posteriormente en relación con la figura 4. Alternativa o adicionalmente, en algunas implementaciones, la directiva de firma digital define un número reducido o mínimo de partes de documento que necesitan ser englobadas por una firma digital para garantizar que la configuración del documento no se altere sin invalidar la firma digital del usuario firmante.

Las figuras 3-4 ilustran documentos que son ilustrativos de un formato de documento sobre el que se puede implementar una directiva de firma digital de acuerdo con una realización. Un formato de documento de este tipo sobre el que se pueden implementar estos documentos es un formato de documento de Especificación de Papel XML (XPS),

desarrollado por Microsoft Corporation de Redmond, Washington. Detalles con respecto al formato de documento XPS se encuentran públicamente disponibles al menos en http://www.microsoft.com/whdc/Device/print/metro.mspx.

En este ejemplo particular, la directiva de firma digital especifica qué partes de documento van a ser englobadas por una firma digital para que el documento se considere firmado. Si la firma digital engloba menos que las partes de documento especificadas, el documento se puede alterar subsiguientemente sin invalidar la firma digital y, en este sentido, crear ambigüedad acerca de la configuración del documento en el instante en el que se aplicó la firma digital. Expresado de otra forma, la función de la directiva de firma digital es designar qué partes son englobadas por una firma digital para crear eficazmente una instantánea de la configuración de documento en el instante de la firma. Las figuras 3-4 proporcionan ejemplos específicos de cómo la directiva de firma digital se puede implementar en escenarios específicos. El experto debería reconocer otros escenarios.

La figura 3 ilustra un documento 300 que incluye una parte de relación de paquetes 301, una parte de secuencia de documentos 302 y una parte de relación de secuencia de documentos (DS) 303 asociada y al menos una parte de documento fijo. Las partes de documento fijo individuales están asociadas con las partes de relaciones de documento fijo (FD) individuales. En este ejemplo, se ilustran tres partes de documento fijo 304, 306 y 308, pero otros ejemplos podrían tener cualquier número de partes de documento fijo. Debido a las restricciones físicas de la hoja en la que aparece la figura 3, una parte de relación de FD 309 solo se ilustra para la parte de documento fijo 304.

La relación de paquetes 301 es una relación cuyo objetivo es una parte y cuya fuente es un paquete como un todo. La parte de secuencia de documentos 302 contiene un marcado que hace referencia a las partes de documento fijo 304, 306 y 308. Expresado de otra forma, la secuencia de documentos es una parte que enumera qué documentos fijos están contenidos en el documento 300. Cualquier borrado de una o más de las partes de documento fijo 304, 306 o 308 se refleja en la parte de secuencia de documentos 302. De forma similar, cualquier adición de una nueva parte de documento fijo se refleja en la parte de secuencia de documentos.

Las partes de documento fijo individuales hacen referencia a partes de página fija. Expresado de otra forma, las partes de documento fijo contienen una lista de sus páginas fijas respectivas. Debido a las restricciones de espacio de la página física sobre la que aparece la figura 3, las partes de página fija solo se ilustran en relación con la parte de documento fijo 304. En este caso, se ilustran dos partes de página fija 310, 312, pero una parte de documento fijo individual podría hacer referencia a cualquier número de partes de página fija. Cualquier borrado o adición de una parte de página fija se refleja en la parte de documento fijo asociada.

Una parte de página fija individual está vinculada a su parte o partes de recursos a través de una parte de relación que especifica la totalidad de los recursos a los que está vinculada una página individual. Por ejemplo, la parte de página fija 310 está asociada a través de la parte de relaciones de página fija (FP) 320 a las partes de recursos 322, 324. Debido a las limitaciones físicas de la página de dibujo, las partes de relación y las partes de recursos no se ilustran en relación con la parte de página fija 312. Cualquier borrado o adición de contenido de una parte de página fija se refleja en la parte de página fija y/o en la parte de relación asociada. Lo que es más, cualquier cambio a un recurso dado se refleja en ese recurso.

La directiva de firma digital sirve para establecer la configuración o contenido del documento 300 en el instante en el que se aplica la firma digital. En este ejemplo particular, la directiva de firma digital especifica que la firma digital ha de englobar la parte de relación de paquetes 301, la parte de secuencia de documentos 302, las partes de documento fijo 304, 306 y 308, las partes de página fija 310, 312, la parte de recursos 322, 324 y las partes de relación asociadas 303, 309 y 320. Las reglas de directiva de firma digital proporcionan un mecanismo para garantizar que un documento que almacena datos como una pluralidad de partes lógicas se mantenga en una configuración que fue firmada digitalmente por un usuario. En un caso en el que el documento se almacena como partes lógicas, la configuración de documento se establece a partir de las interrelaciones de las partes así como los datos dentro de las partes. En este sentido, la directiva de firma digital sirve para establecer tanto las interrelaciones de partes como los datos intra-parte. En un caso en el que la configuración de documento se altera al alterar una cualquiera o ambas de las interrelaciones de partes y los datos intra-parte, la directiva de firma digital da lugar a que se invalide la firma digital. Un mecanismo de directiva de firma digital de este tipo permite que el autor o un usuario subsiguiente determine si el documento sigue siendo consistente con la configuración asociada con la firma digital.

Para fines de explicación, supóngase que el documento 300 se firma digitalmente de conformidad con la directiva de firma digital especificada anteriormente por un usuario publicador de tal modo que la firma digital engloba la parte de relación de paquetes 301, la parte de secuencia de documentos 302 así como su parte de relación de secuencia de documentos 303, las partes de documento fijo 304, 306 y 308 y sus partes de relación de documento fijo respectivas (solo se designa específicamente la parte de relación de FD 309), las partes de página fija 310, 312 y la parte de relaciones de página fija 320 y la parte de recursos 322, 324. En un caso de este tipo, la configuración de documento que se representa para el usuario publicador en el instante de la firma es englobada eficazmente por las partes firmadas especificadas por la directiva de firma digital. Supóngase adicionalmente que un usuario subsiguiente intenta añadir un nuevo documento fijo al documento 300. El nuevo documento se representará en la parte de secuencia de documentos 302. Este cambio a la parte de secuencia de documentos dará lugar a que se invalide la firma digital del usuario publicador de forma consistente con la directiva de firma digital. En esta implementación particular, el hecho de que la firma digital se invalide se puede representar visualmente de una forma que es percibida fácilmente por los

usuarios. Otras implementaciones pueden proporcionar una advertencia al usuario de que la acción que este está a punto de realizar invalidará la firma digital del documento. No obstante, en esta implementación, la directiva de firma digital no evita que el usuario consumidor añada el nuevo documento e invalide la firma digital. Más bien, una acción de este tipo simplemente invalida la firma digital y el sistema otorga esta información a un usuario para que actúe según estime oportuno. Por ejemplo, si un usuario consumidor recibe un documento con una firma invalidada del usuario publicador, el usuario consumidor puede tratar el documento como si hubiera sido manipulado indebidamente y solicitar un nuevo documento firmado a un usuario publicador.

De una forma similar al ejemplo anterior, considérese un escenario en el que un usuario subsiguiente intenta eliminar un recurso al que hace referencia una parte de página fija particular y sustituir el recurso con un recurso diferente. Por ejemplo, el recurso puede ser una imagen que el usuario intenta sustituir con una segunda imagen diferente. Una acción de este tipo da lugar a que se invalide la firma digital del usuario publicador debido a que la acción intenta alterar (en este caso, borrar una parte firmada del documento). En este ejemplo, invalidar la firma digital en respuesta a cambiar una imagen a la que se hace referencia es consistente con la función de la directiva de firma digital. Supóngase, para fines de ejemplo, que el documento 300 es una oferta, por parte de un constructor, para construir una casa por una cantidad económica dada. Supóngase adicionalmente que la imagen a la que se hace referencia es un plano técnico de la casa incluido en la oferta. La cantidad económica de la oferta se presupuesta según ese plano técnico particular. En este sentido, el constructor no desea que alguien, tal como el propietario del inmueble, sea capaz de sustituirlo por un plano técnico diferente de tal modo que pareciese que el constructor realizara la oferta basándose en el plano técnico sustituto. La directiva de firma digital sirve para notificar al constructor y/o al propietario del inmueble que la oferta sigue estando en la configuración firmada por el constructor en la oferta o que la oferta se ha alterado de tal modo que ya no es consistente con la configuración firmada por el constructor.

La figura 4 ilustra otro documento 400 para el cual la directiva de firma digital especifica qué partes de documento van a ser englobadas por una firma digital para que el documento se considere firmado. Si el documento se firma digitalmente de conformidad con la directiva de firma digital la firma digital captura la configuración del documento en el instante en el que este se firmó digitalmente. Expresado de otra forma, en esta implementación, la directiva de firma digital especifica qué porciones de un paquete no han de cambiar con el fin de que el contenido sea considerado intacto. Para garantizar la validez, algunas aplicaciones de cliente y/o sus usuarios pueden requerir que se firme y se valide la totalidad de las partes y relaciones en un paquete. Otras pueden requerir que solo se firmen y se validen partes o relaciones seleccionadas para indicar que el contenido no ha cambiado. La directiva de firma digital proporciona flexibilidad en la definición del contenido que se firmará al tiempo que se permite que algunas partes del paquete sigan pudiendo cambiarse. El documento 400 proporciona un ejemplo para escenarios en los que un usuario firmante puede especificar casos en los que un contenido específico del documento se puede cambiar sin dañar la firma digital del usuario.

El documento 400 incluye una parte de relación de paquetes 402, una parte de definiciones de firma digital 404 y una parte de propiedades principales 406. En este caso, la parte de definiciones de firma digital, la parte de propiedades principales y la parte de relación de paquetes se definen a nivel de paquete y, en este sentido, se heredan a nivel de documento y son mantenidas por la directiva de firma digital. La relación de paquetes 402 es una relación cuyo objetivo es una parte y cuya fuente es un paquete como un todo. La parte de definiciones de firma digital 404 permite que un usuario publicador defina un conjunto solicitado de personas para firmar digitalmente el documento y las condiciones o definiciones asociadas con cada firma digital solicitada. La parte de propiedades principales se refiere a una o más propiedades que un usuario puede definir en el documento. Por ejemplo, una propiedad principal de este tipo puede ser 'autor de documento', que el usuario es libre de designar con cualquier nombre o seudónimo que desee.

El documento 400 incluye adicionalmente una parte de secuencia de documentos 410 con una parte de relación de secuencia de documentos (DS) 412 asociada y una parte de documento fijo 414 con una parte de relaciones de documento fijo (FD) 416 asociada. La parte de documento fijo 414 hace referencia a una parte de página fija 418 y una parte de anotaciones 420. La parte de página fija 418, como se indica en una parte de relaciones de página fija (FP) 422, está vinculada a la parte de recursos 424. Esta implementación particular también incluye una parte de imagen en miniatura 426 que se analizará con más detalle posteriormente.

La directiva de firma digital sirve para establecer el contenido del documento 400 en el instante en el que se aplica la firma digital. En esta implementación, la directiva de firma digital especifica, para que el documento sea de conformidad con la directiva de firma digital, que la firma digital englobe la parte de relación de paquetes 402, la parte de secuencia de documentos 410 y su parte de relación de DS 412, la parte de documento fijo 414 y su parte de relación de FD 416, la parte de página fija 418 y su parte de relación de FP 422 así como la parte de recursos 424. La directiva de firma digital expresa adicionalmente que la firma digital engloba la imagen en miniatura 426 cuando se encuentra presente. Por supuesto, aunque solo se ilustra un único ejemplo de cada una de las partes anteriores, muchas implementaciones tendrán múltiples casos de las partes 414-426.

En este caso, firmar la relación de paquetes 402 evita que un usuario subsiguiente cambie la relación de paquetes sin invalidar la firma digital del usuario firmante. De forma similar, firmar la parte de secuencia de documentos 410 y su parte de relación de DS 412 evita la eliminación de un documento fijo existente o la adición de nuevos documentos fijos sin invalidar la firma digital. Firmar la parte de documento fijo 414 y su parte de relación de FD 416 evita cambios al orden de las páginas en un documento fijo o la adición o borrado de páginas fijas. Firmar la parte de página fija 418

y su parte de relación de FP 422 sirve para evitar que se cambie el contenido de una página. Firmar la parte de recursos 424 evita la eliminación o sustitución de la parte de recursos. De forma similar, firmar la parte de imagen en miniatura cuando se encuentra presente, tal como en esta implementación ilustrada, evita una sustitución o borrado de la imagen en miniatura 426 sin dañar la firma. De forma similar, si se encuentra presente la parte de definiciones de firma digital 404, tal como se indica en el presente caso, la directiva de firma digital engloba la parte de definiciones de firma digital con la firma digital. La directiva de firma digital firma funcionalmente cada uno de estos componentes para proporcionar colectivamente una indicación con respecto a si el documento se ha alterado con respecto a la configuración firmada.

En esta implementación, la directiva de firma digital permite que el usuario firmante decida si el contenido de partes específicas del documento se puede manipular sin invalidar la firma digital del usuario firmante. Por ejemplo, ¿desea el usuario firmante que un usuario subsiguiente sea capaz de añadir contenido al documento sin invalidar la firma digital del usuario firmante? En un caso de este tipo, el usuario firmante puede decidir si permitir que un usuario subsiguiente añada firmas digitales al documento. En otro caso, el usuario firmante puede decidir si permitir que un usuario subsiguiente cambie propiedades principales en el documento. En otro caso más, el usuario firmante puede decidir si permitir que un usuario subsiguiente añada anotaciones al documento. Cada una de estas opciones es independiente de las otras y el usuario firmante puede no permitir ninguna de las adiciones opcionales al documento, o cualquier combinación deseada.

La figura 5 ilustra un ejemplo de directiva de firma digital en forma de una tabla lógica 500 en relación con propiedades principales. La tabla lógica 500 se refiere a dos escenarios mutualmente exclusivos. En el primer escenario, el usuario firmante desea permitir cambios de propiedades principales como se indica en 502. En el segundo escenario, el usuario firmante no desea permitir cambios de propiedades principales como se indica en 504. En relación con los dos escenarios 502, 504, existe una de dos situaciones. O bien la parte de propiedades principales existe como se indica en 506, o bien la parte de propiedades principales no existe, como se indica en 508.

Como se indica en 510, en un caso en el que el usuario firmante desea permitir cambios de propiedades principales y existe una parte de propiedades principales, entonces la directiva de firma digital deja la parte de propiedades principales sin firmar cuando el usuario firma digitalmente el documento pero la directiva aplica la firma digital del usuario a la relación de paquetes descrita en relación con la figura 4. La relación de paquetes contiene un vínculo a la parte de propiedades principales de modo que un usuario subsiguiente puede cambiar las propiedades principales sin invalidar la firma del usuario.

Como se indica en 512, en un caso en el que el usuario firmante desea permitir cambios de propiedades principales y la parte de propiedades principales no existe, entonces la directiva de firma digital crea una parte de propiedades principales antes de que el usuario haya firmado digitalmente el documento. La parte de propiedades principales se puede encontrar vacía en este punto, pero crearla antes de firmar permite que se añada contenido subsiguientemente. La parte de propiedades principales se deja entonces sin firmar de tal modo que se pueden hacer cambios subsiguientes a las propiedades principales. Como anteriormente, la firma digital del usuario se aplica a la relación de paquetes para evitar que se cambie o se borre material.

Como se indica en 514, si el usuario firmante no desea permitir adiciones de propiedades principales y existe una parte de propiedades principales, entonces la directiva de firma digital firma la parte de propiedades principales con la firma digital del usuario así como la relación de paquetes. En un escenario de este tipo, la firma digital del usuario engloba la parte de propiedades principales de tal modo que cualquier cambio a la parte de propiedades principales invalida la firma del usuario.

Por último, como se indica en 516, si el usuario firmante no desea permitir adiciones de propiedades principales y una parte de propiedades principales no existe, entonces la directiva de firma digital no crea una parte de propiedades principales antes de que el usuario firme digitalmente el documento. Como con los otros escenarios, la firma digital se aplica a la relación de paquetes. En este escenario, añadir subsiguientemente propiedades principales necesita añadir una parte de propiedades principales. Añadir una parte de propiedades principales cambia la parte de relación de paquetes, lo que invalida la firma del usuario.

Haciendo referencia colectivamente a las figuras 4-5, la directiva de firma digital puede manejar anotaciones de una forma similar a la descrita anteriormente en relación con las propiedades principales. Se añaden anotaciones a una parte de anotaciones 420 a la que hace referencia la parte de documento fijo 414. Si la parte de anotaciones es englobada por la firma digital del usuario, añadir anotaciones invalidará la firma. Si una parte de anotación no existe, crear la parte después de que se haya aplicado la firma digital cambiará la parte de documento fijo e invalidará la firma. Si el usuario firmante desea permitir que se añadan anotaciones, entonces debería existir una parte de anotaciones en el instante de la firma y se debería dejar sin firmar. La parte de anotaciones se puede crear antes de firmar digitalmente el documento. En tal caso, la parte de anotaciones recién creada se puede encontrar vacía en el instante en el que se aplica la firma digital del usuario.

La figura 6 se refiere a partes de firma digital tales como las que se pueden asociar con el documento 400 representado en la figura 4. En esta implementación, las partes de firma digital incluyen una parte de origen de firma 602, unas partes de firma y partes de certificado. En este caso, se representan dos partes de firma 604, 606 así como dos partes

de certificado 608, 610. La presente implementación crea un manifiesto de las partes de certificado 608, 610 como partes separadas y distintas. En otras implementaciones, las partes de certificado se pueden insertar dentro de la parte de firma asociada. La parte de origen de firma 602 proporciona un punto de partida para explorar las firmas digitales disponibles de un documento. Una parte de firma, tal como 606 o 608, que contiene una firma digital que engloba las partes especificadas por la directiva de firma digital y que se verifica apropiadamente, se puede considerar válida. Por ejemplo, el sistema verifica que las partes correctas están firmadas de acuerdo con la directiva de firma digital. El sistema verifica adicionalmente el estado de las partes opcionalmente firmadas, tales como las propiedades principales descritas anteriormente, y cómo una condición de las partes opcionalmente firmadas afecta al usuario. El sistema también verifica, para las partes firmadas, que la firma es válida. Por ejemplo, el sistema comprueba si el cálculo de hash coincide, como debería reconocer el experto.

Expresado de otra forma, si la parte de firma engloba las partes de documento consistentes con la directiva de firma digital y la verificación de firma tiene éxito, entonces el documento se puede considerar como un documento firmado válido, tal como un documento XPS. En un caso de este tipo, un usuario puede considerar que un documento de este tipo tiene la misma configuración que existía en el instante en el que se aplicó la firma digital válida.

La directiva de firma digital proporciona una solución flexible con respecto a si se puede añadir material adicional al documento. La solución permite que el usuario publicador especifique qué material opcional, de haber alguno, se puede añadir sin invalidar su firma digital. La directiva de firma digital tiene entonces en cuenta la presente configuración del documento y actúa en consecuencia para crear o formar partes como se ha descrito anteriormente en las figuras 4-6. Al menos algunas implementaciones son análogas a los conmutadores. Por ejemplo, si el autor activa una protección de firma y alguien añade una firma digital, la directiva de firma digital daña la firma digital del autor. Si el autor no desea una protección de firma, alguien puede añadir una firma digital sin afectar a la firma digital del autor. El mismo principio se aplica a otras adiciones opcionales tales como anotaciones y propiedades principales. Por lo tanto, la solución es muy flexible ya que esta permite que el usuario firmante defina un parámetro de directiva y la directiva de firma digital actúa en consecuencia para posibilitar que usuarios subsiguientes añadan el contenido sin dañar la firma digital del usuario firmante. No obstante, a pesar de su flexibilidad, la directiva de firma digital continúa evitando que nadie altere la configuración del documento sin dañar la firma digital del usuario consumidor. A nivel de usuario final, la directiva de firma digital descrita proporciona la confianza en que un documento que porta la firma digital de un usuario sigue siendo consistente con la configuración firmada digitalmente por el usuario. La directiva de firma digital también es útil para establecer una directiva de firma digital con la que se puede cumplir, y/o que puede ser entendida por, otros productos de software que pueden interaccionar con formatos de documento y documentos conformes con directivas de firma digital. La directiva de firma digital define normas para lo que es englobado en realidad por un documento firmado, cómo generar un documento firmado conforme con directivas de firma digital, y/o cómo evaluar un documento recibido para determinar si la firma digital del documento es válida. En resumen, la directiva de firma digital define lo que quiere decir en realidad un documento digitalmente firmado.

ENTORNO INFORMÁTICO ILUSTRATIVO

La figura 7 representa un sistema o entorno informático 700 ilustrativo sobre el que se puede implementar una directiva de firma digital. El sistema 700 incluye un sistema informático de propósito general en forma de una primera máquina 701 y una segunda máquina 702.

Los componentes de la primera máquina 701 pueden incluir, pero no se limitan a, uno o más procesadores 704 (por ejemplo, cualquiera de microprocesadores, controladores, y similares), una memoria de sistema 706 y un bus de sistema 708 que acopla los diversos componentes de sistema. Los uno o más procesadores 704 procesan diversas instrucciones ejecutables por ordenador para controlar el funcionamiento de la primera máquina 701 y para comunicarse con otros dispositivos electrónicos e informáticos. El bus de sistema 708 representa cualquier número de varios tipos de estructuras de bus, incluyendo un bus de memoria o controlador de memoria, un bus de periféricos, un puerto de gráficos acelerado y un procesador o bus local usando cualquiera de una diversidad de arquitecturas de bus.

El sistema 700 incluye una diversidad de medios legibles por ordenador que pueden ser cualquier medio al que pueda acceder la primera máquina 701 e incluye medios tanto volátiles como no volátiles, medios tanto extraíbles como no extraíbles. La memoria de sistema 706 incluye un medio legible por ordenador en forma de memoria volátil, tal como una memoria de acceso aleatorio (RAM) 710 y/o memoria no volátil, tal como una memoria de solo lectura (ROM) 712. Un sistema básico de entrada/salida (BIOS) 714 mantiene las rutinas básicas que facilitan la transferencia de información entre los componentes dentro de la primera máquina 701, tal como durante el arranque, y está almacenado en la ROM 712. La RAM 710 contiene, por lo general, datos y/o módulos de programa a los que se puede acceder inmediatamente y/o que pueden estar siendo operados en la actualidad por uno o más de los procesadores 704.

La primera máquina 701 puede incluir otros medios de almacenamiento informático extraíbles/no extraíbles y volátiles/no volátiles. A modo de ejemplo, una unidad de disco duro 716 lee de y escribe en unos medios magnéticos no extraíbles y no volátiles (no mostrados), una unidad de disco magnético 718 lee de y escribe en un disco magnético extraíble y no volátil 720 (por ejemplo, un disco flexible) y una unidad de disco óptico 722 lee de y/o escribe en un disco óptico extraíble y no volátil 724, tal como un CD-ROM, un disco versátil digital (DVD) o cualquier otro tipo de medios ópticos. En este ejemplo, cada una de la unidad de disco duro 716, la unidad de disco magnético 718 y la

unidad de disco óptico 722 está conectada al bus de sistema 708 por una o más interfaces de medios de datos 726. Las unidades de disco y medios legibles por ordenador asociados proporcionan un almacenamiento no volátil de instrucciones legibles por ordenador, estructuras de datos, módulos de programa y otros datos para la primera máquina 701.

Cualquier número de módulos de programa se puede almacenar en el disco duro 716, el disco magnético 720, el disco óptico 724, la ROM 712 y/o la RAM 710, incluyendo, a modo de ejemplo, un sistema operativo 726, uno o más programas de aplicación 728, otros módulos de programa 730 y datos de programa 732. Cada uno de tal sistema operativo 726, programas de aplicación 728, otros módulos de programa 730 y datos de programa 732 (o alguna combinación de los mismos) puede incluir una realización de los sistemas y procedimientos descritos en el presente documento.

Un usuario puede interaccionar con la primera máquina 701 por medio de cualquier número de diferentes dispositivos de entrada tales como un teclado 734 y un dispositivo apuntador 736 (por ejemplo, un "ratón"). Otros dispositivos de entrada 738 (que no se muestran específicamente) pueden incluir un micrófono, una palanca de control, un controlador para juegos, un controlador, una antena parabólica, un puerto serie, un escáner y/o similares. Estos y otros dispositivos de entrada se conectan a los procesadores 704 a través de unas interfaces de entrada/salida 740 que están acopladas al bus de sistema 708, pero pueden estar conectadas por otra interfaz y estructuras de bus, tales como un puerto paralelo, un puerto de juegos y/o un bus serie universal (USB).

Un monitor 742 u otro tipo de dispositivo de pantalla también puede estar conectado al bus de sistema 708 por medio de una interfaz, tal como un adaptador de vídeo 744. Además del monitor 742, otros dispositivos periféricos de salida pueden incluir componentes tales como unos altavoces (no mostrados) y una impresora 746, que pueden estar conectados a la primera máquina 701 a través de la interfaz de entrada/salida 740.

La primera máquina 701 puede operar en un entorno de red usando conexiones lógicas a uno o más ordenadores remotos, tales como la segunda máquina 702. A modo de ejemplo, la segunda máquina 702 puede ser un ordenador personal, un ordenador portátil, un servidor, un encaminador, un ordenador de red, un dispositivo del mismo nivel u otro nodo de red común, y similares. La segunda máquina 702 se ilustra como un ordenador portátil que puede incluir muchos o la totalidad de los elementos y características descritas en el presente documento en relación con la primera máquina 701.

Las conexiones lógicas entre la primera máquina 701 y la segunda máquina 702 se representan como una red de área local (LAN) 750 y una red de área amplia (WAN) general 752. Tales entornos de red son comunes en oficinas, redes informáticas empresariales, intranets e Internet. Cuando se implementa en un entorno de red LAN, la primera máquina 701 está conectada a una red local 750 a través de una interfaz o adaptador de red 754. Cuando se implementa en un entorno de red WAN, la primera máquina 701 incluye habitualmente un módem 756 u otros medios para establecer comunicaciones por la red de área amplia 752. El módem 756, que puede ser interno o externo a la primera máquina 701, puede ser conectado al bus de sistema 708 por medio de las interfaces de entrada/salida 740 u otros mecanismos apropiados. Las conexiones de red ilustradas son ilustrativas y se pueden utilizar otros medios para establecer un enlace o enlaces de comunicación entre la primera y la segunda máquinas 701, 702.

En un entorno de red, tal como el ilustrado con el Sistema 700, los módulos de programa ilustrados en relación con la primera máquina 701 o sus porciones pueden almacenarse en un dispositivo de almacenamiento en memoria remota. A modo de ejemplo, unos programas de aplicación remotos 758 se mantienen con un dispositivo de memoria de la segunda máquina 702. Para fines de ilustración, los programas de aplicación y otros componentes de programa ejecutables, tales como el sistema operativo 726, se ilustran en el presente documento como bloques discretos, aunque se reconoce que tales programas y componentes residen en diversos instantes en diferentes componentes de almacenamiento de la primera máquina 701, y son ejecutados por los procesadores 704 de la primera máquina.

PROCEDIMIENTOS ILUSTRATIVOS

La figura 8 ilustra un procedimiento ilustrativo 800 en relación con una directiva de firma digital. No se pretende que el orden en el que se describe el procedimiento se interprete como una limitación, y cualquier número de los bloques de procedimiento descritos pueden combinarse en cualquier orden para implementar el procedimiento. Además, el procedimiento puede implementarse en cualquier hardware, software, firmware, o combinación de los mismos adecuada.

En el bloque 802, el procedimiento determina partes de un documento para englobar con una firma digital de un usuario de conformidad con una directiva de firma digital. En algunas implementaciones, la directiva de firma digital puede especificar que todas las partes del documento se firmen digitalmente. En otras implementaciones, la directiva de firma digital puede especificar un subconjunto de las partes a firmar digitalmente. Por ejemplo, en una implementación, la directiva de firma digital se aplica a partes que contribuyen a una configuración de documento como se representa en el instante de la firma. En un caso de este tipo, la directiva de firma digital sirve para notificar al usuario y/o a otros usuarios si el documento se ha alterado subsiguientemente a la firma, de una forma tal como para cambiar la configuración de documento con respecto a la configuración de documento que el usuario firmó.

En el bloque 804, el procedimiento aplica la firma digital a las partes determinadas en el bloque 802. La firma digital

del usuario se aplica eficazmente a la totalidad de las partes especificadas por la directiva de firma digital de tal modo que, si se altera cualquiera de las partes, la firma digital se daña o se invalida. Dañar la firma digital en relación con cualquiera de las partes daña la firma digital para el documento como un todo. El razonamiento subyacente es que alterar cualquiera de las partes especificadas puede cambiar la configuración de documento.

El procedimiento puede representar si la firma digital sigue siendo, o no, válida de tal modo que el usuario y/o usuarios subsiguientes pueden tomar unas decisiones mejor informadas con respecto a cómo tratar el documento. La directiva de firma digital crea eficazmente un entorno con un grado más alto de certidumbre para el usuario. Por ejemplo, si un usuario publicador se encuentra a gusto con una configuración de documento particular y firma digitalmente el documento, la directiva de firma digital garantiza que, siempre que su firma digital siga siendo válida, tanto el usuario publicador como cualquier usuario consumidor pueden actuar con confianza en que estos están viendo la configuración de documento que fue firmada digitalmente por el usuario publicador. Esto puede ser especialmente valioso en un escenario en el que el usuario publicador firma digitalmente una configuración de documento deseada y envía entonces el documento a una parte consumidora adversa, tales como las que se pueden encontrar en negociaciones contractuales. Si el usuario consumidor envía entonces el documento de vuelta al usuario publicador, el usuario publicador puede mostrarse muy receloso de que la parte consumidora realizara algún cambio difícil de detectar pero importante al documento. La funcionalidad de directiva de firma digital permite que el usuario publicador determine fácilmente si el documento devuelto tiene la misma configuración que este firmó digitalmente. Debido a que la directiva de firma digital crea un nivel superior de certidumbre para los usuarios, esta puede fomentar un nivel superior de aceptación de documentos digitales, en especial en cuestiones consideradas importantes por los usuarios. Además, cuando se observa desde una perspectiva de sistema, la directiva de firma digital promueve la interoperabilidad entre productos de software que pueden interaccionar con o soportar documentos conformes con directivas de firma digital.

Aunque las implementaciones en relación con la directiva de firma digital se han descrito en lenguaje específico a características estructurales y/o procedimientos, se ha de entender que el sujeto de las reivindicaciones adjuntas no está necesariamente limitado a las características o procedimientos específicos descritos. Más bien, las características y procedimientos específicos proporcionan ejemplos de implementaciones para los conceptos descritos anterior y posteriormente. La invención se define mediante las reivindicaciones adjuntas.

REIVINDICACIONES

1. Un sistema (100), que comprende:

unos medios para almacenar un documento (400) como una pluralidad de partes lógicas;
unos medios para establecer una configuración de documento cuando una firma digital de un usuario firmante se aplica al documento (400), en el que los medios de establecimiento definen cuáles de la pluralidad de partes lógicas están firmadas con la firma digital;
unos medios para indicar si la configuración de documento se altera subsiguientemente; y
unos medios para aplicar la firma a las partes, la pluralidad de partes lógicas incluye

una parte de documento fijo (414),
una parte de propiedades principales (406), que se deja sin firmar;
una parte de definiciones de firma digital (404) que permite que el usuario firmante defina otro usuario para firmar adicionalmente el documento y que defina condiciones asociadas con la firma del otro usuario, y
una parte de relación de paquetes (402), en el que la parte de relación de paquetes contiene un vínculo a la parte de propiedades principales, de modo que un usuario subsiguiente puede cambiar las propiedades principales sin invalidar la firma del usuario firmante y en el que firmar la parte de relación de paquetes (402) evita que un usuario subsiguiente cambie el vínculo sin invalidar la firma digital del usuario firmante; y

los medios de establecimiento comprenden una regla de directiva de firma digital que permite que el otro usuario añada un contenido de documento y una firma del otro usuario al documento sin invalidar la firma del usuario firmante de acuerdo con la definición de dicho usuario firmante en la parte de definiciones de firma digital (404).

2. El sistema según la reivindicación 1, en el que los medios de almacenamiento comprenden un formato de documento XPS.

3. El sistema según la reivindicación 1, en el que los medios de establecimiento comprenden un conjunto de reglas de directiva de firma digital que definen un subconjunto de las partes lógicas que contribuyen a la configuración de tal modo que, si se alteran partes lógicas individuales del subconjunto, se considera que la configuración de documento se ha alterado.

4. El sistema según la reivindicación 1, en el que los medios de establecimiento comprenden un conjunto de reglas de directiva de firma digital que definen un primer subconjunto de partes lógicas que contribuyen a la configuración de tal modo que, si se alteran partes lógicas individuales del subconjunto, se considera que la configuración se ha alterado, y un segundo subconjunto de partes que se pueden alterar sin alterar la configuración.

5. El sistema según la reivindicación 5, en el que los medios de establecimiento permiten adicionalmente que un usuario que aplica la firma digital especifique partes individuales del segundo subconjunto que, cuando se alteran, se considera que alteran la configuración.

6. El sistema según la reivindicación 1, en el que los medios de indicación comprenden una interfaz configurada para indicar que la firma digital es no válida en un caso en el que se altera la configuración.

7. Un medio legible por ordenador que comprende unas instrucciones ejecutables por ordenador que, cuando se ejecutan, realizan actos, que comprenden:

determinar (802) partes lógicas de un documento (400) para englobar con una firma digital de un usuario firmante de conformidad con una directiva de firma digital; y
aplicar (804) la firma digital a las partes, las partes lógicas incluyen

una parte de documento fijo (414),
una parte de propiedades principales (406), que se deja sin firmar;
una parte de definiciones de firma digital (404) que permite que el usuario firmante defina otro usuario para firmar adicionalmente el documento y que defina condiciones asociadas con la firma del otro usuario, y
una parte de relación de paquetes (402), en el que la parte de relación de paquetes contiene un vínculo a la parte de propiedades principales, de modo que un usuario subsiguiente puede cambiar las propiedades principales sin invalidar la firma del usuario firmante y en el que firmar la parte de relación de paquetes (402) evita que un usuario subsiguiente cambie la relación sin invalidar la firma digital del usuario firmante;

comprendiendo adicionalmente los actos: aplicar una regla de directiva de firma digital que permite que el otro usuario añada un contenido de documento y una firma del otro usuario al documento sin invalidar la firma del usuario firmante de acuerdo con la definición de dicho usuario firmante en la parte de definiciones de firma digital (404).

8. El medio legible por ordenador de la reivindicación 7, en el que las partes comprenden todas las partes de secuencia de documentos y las partes de relación asociadas, todas las partes de documento fijo y las partes de relación asociadas, todas las partes de página fija y las partes de relaciones de página fija asociadas, todas las partes de

recursos y todas las partes de definiciones de firma digital contenidas en el documento (400).

9. El medio legible por ordenador de la reivindicación 7, que comprende adicionalmente verificar la firma digital.

10. El medio legible por ordenador de la reivindicación 7, que comprende adicionalmente invalidar la firma digital del usuario si cualquiera de las partes se altera subsiguientemente.

11. El medio legible por ordenador de la reivindicación 7, que comprende adicionalmente permitir que el usuario especifique si una o más cualesquiera de las propiedades principales, anotaciones y firmas digitales se pueden cambiar sin invalidar la firma digital del usuario.

12. Un procedimiento que comprende:

determinar (802) partes lógicas de un documento (400) para englobar con una firma digital de un usuario firmante de conformidad con una directiva de firma digital; y
aplicar (804) la firma digital a las partes, las partes lógicas incluyen

una parte de documento fijo (414),
una parte de propiedades principales (406), que se deja sin firmar;
una parte de definiciones de firma digital (404) que permite que el usuario firmante defina otro usuario para firmar adicionalmente el documento y que defina condiciones asociadas con la firma del otro usuario, y
una parte de relación de paquetes (402), en el que la parte de relación de paquetes contiene un vínculo a la parte de propiedades principales, de modo que un usuario subsiguiente puede cambiar las propiedades principales sin invalidar la firma del usuario firmante y en el que firmar la parte de relación de paquetes (402) evita que un usuario subsiguiente cambie la relación sin invalidar la firma digital del usuario firmante;

comprendiendo adicionalmente los actos: aplicar una regla de directiva de firma digital que permite que el otro usuario añada un contenido de documento y una firma del otro usuario al documento sin invalidar la firma del usuario firmante de acuerdo con la definición de dicho usuario firmante en la parte de definiciones de firma digital (404).

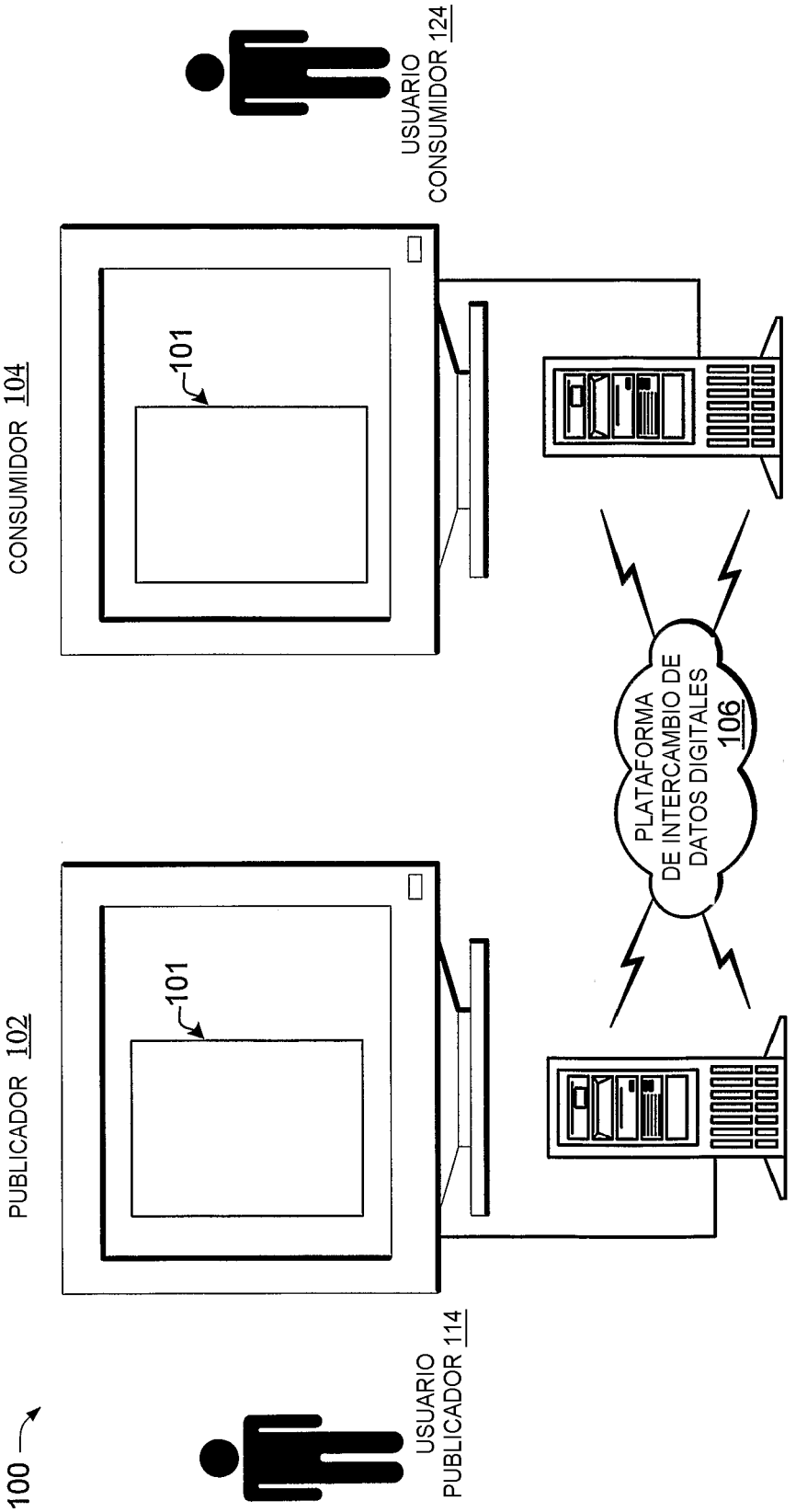
100
USUARIO PUBLICADOR 114
PUBLICADOR 102
101
PLATAFORMA DE INTERCAMBIO DE DATOS DIGITALES 106
CONSUMIDOR 104
101
USUARIO CONSUMIDOR 124

FIG. 1

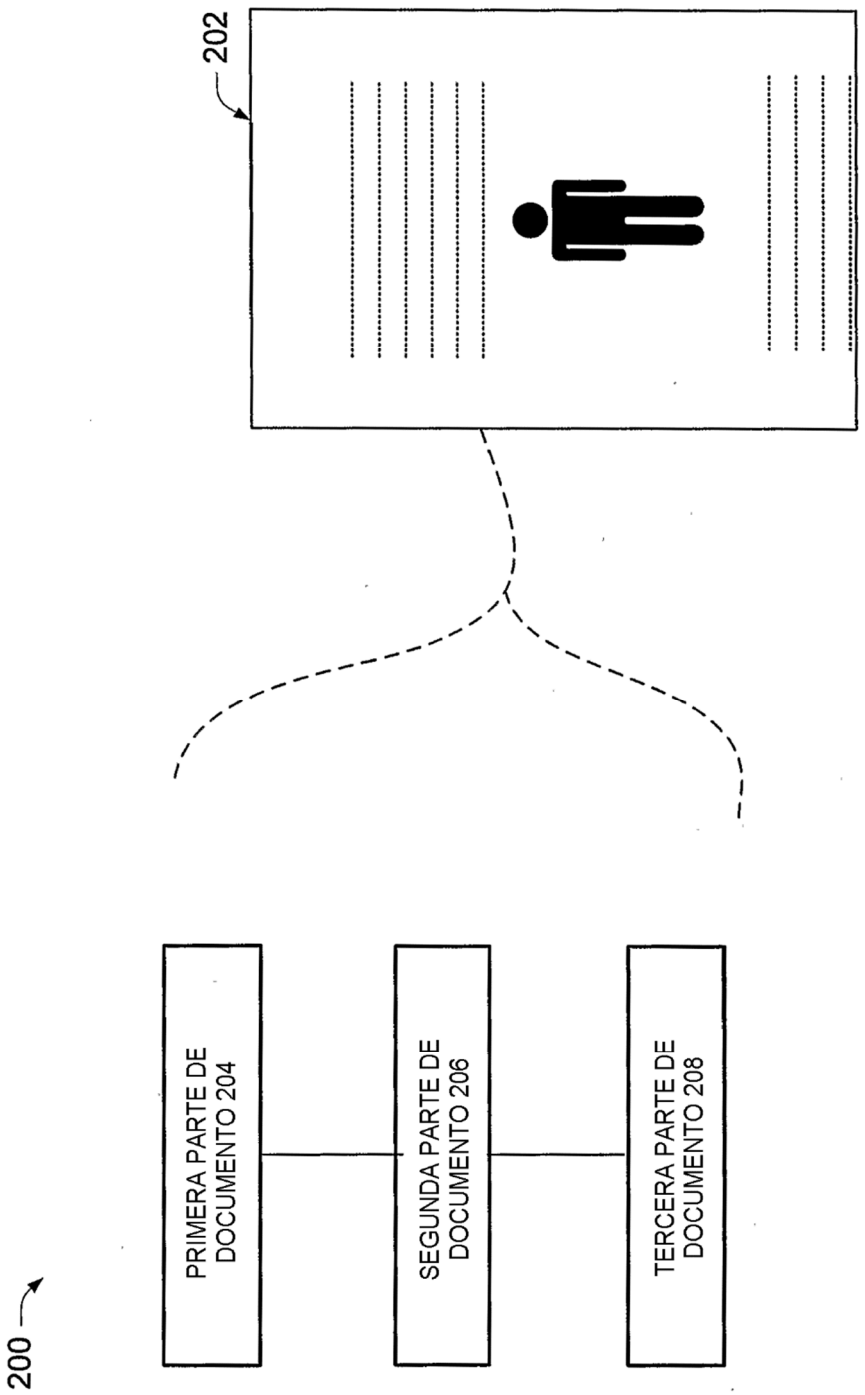
202
200
PRIMERA PARTE DE DOCUMENTO 204
SEGUNDA PARTE DE DOCUMENTO 206
TERCERA PARTE DE DOCUMENTO 208

FIG. 2

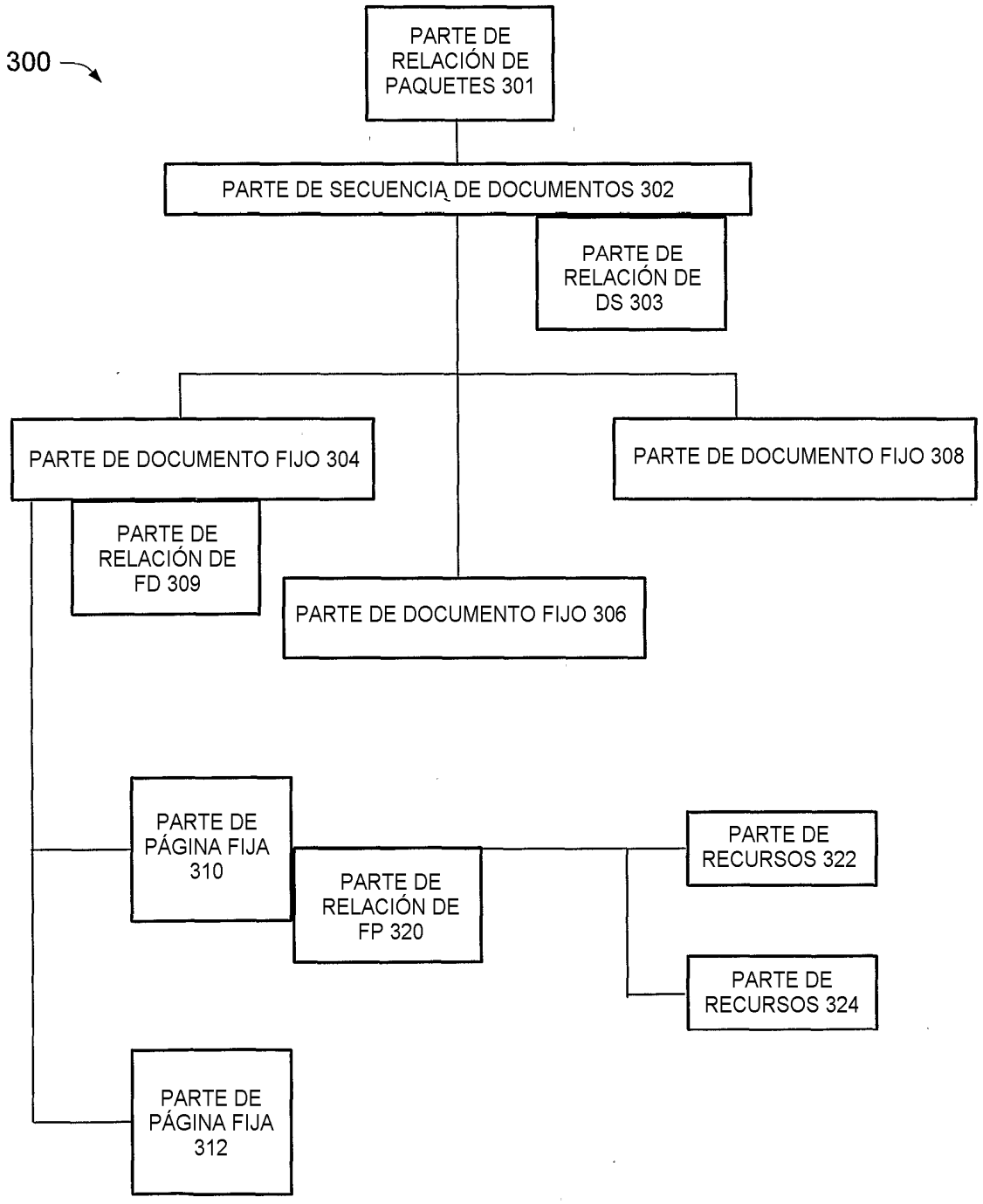
300
PARTE DE RELACIÓN DE PAQUETES 301
PARTE DE SECUENCIA DE DOCUMENTOS 302
PARTE DE RELACIÓN DE DS 303
PARTE DE DOCUMENTO FIJO 304
PARTE DE DOCUMENTO FIJO 308
PARTE DE RELACIÓN DE FD 309
PARTE DE DOCUMENTO FIJO 306
PARTE DE PÁGINA FIJA 310
PARTE DE RELACIÓN DE FP 320
PARTE DE RECURSOS 322
PARTE DE RECURSOS 324
PARTE DE PÁGINA FIJA 312

FIG. 3

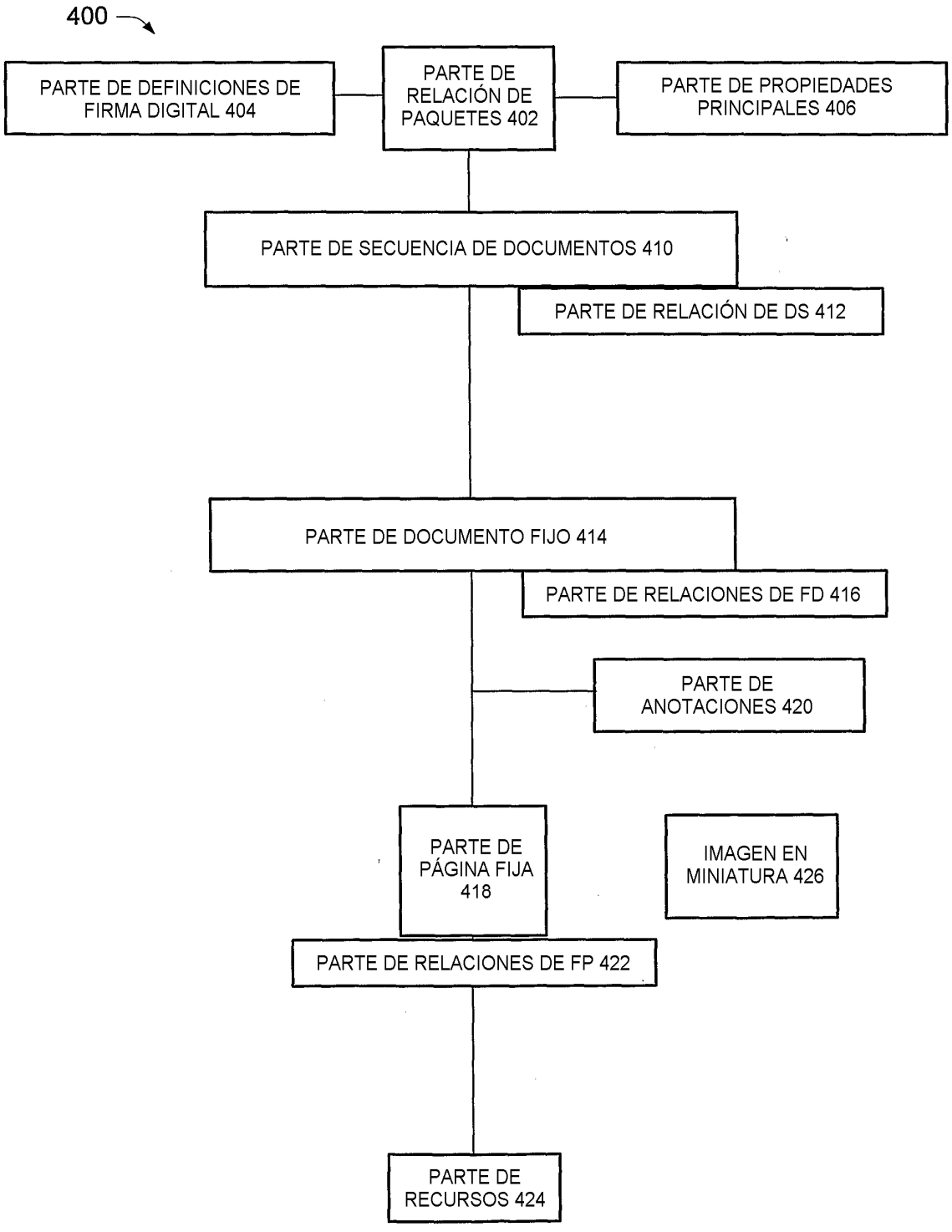
400
PARTE DE DEFINICIONES DE FIRMA DIGITAL 404
PARTE DE RELACIÓN DE PAQUETES 402
PARTE DE PROPIEDADES PRINCIPALES 406
PARTE DE SECUENCIA DE DOCUMENTOS 410
PARTE DE RELACIÓN DE DS 412
PARTE DE DOCUMENTO FIJO 414
PARTE DE RELACIONES DE FD 416
PARTE DE ANOTACIONES 420
PARTE DE PÁGINA FIJA 418
IMAGEN EN MINIATURA 426
PARTE DE RELACIONES DE FP 422
PARTE DE RECURSOS 424

FIG. 4

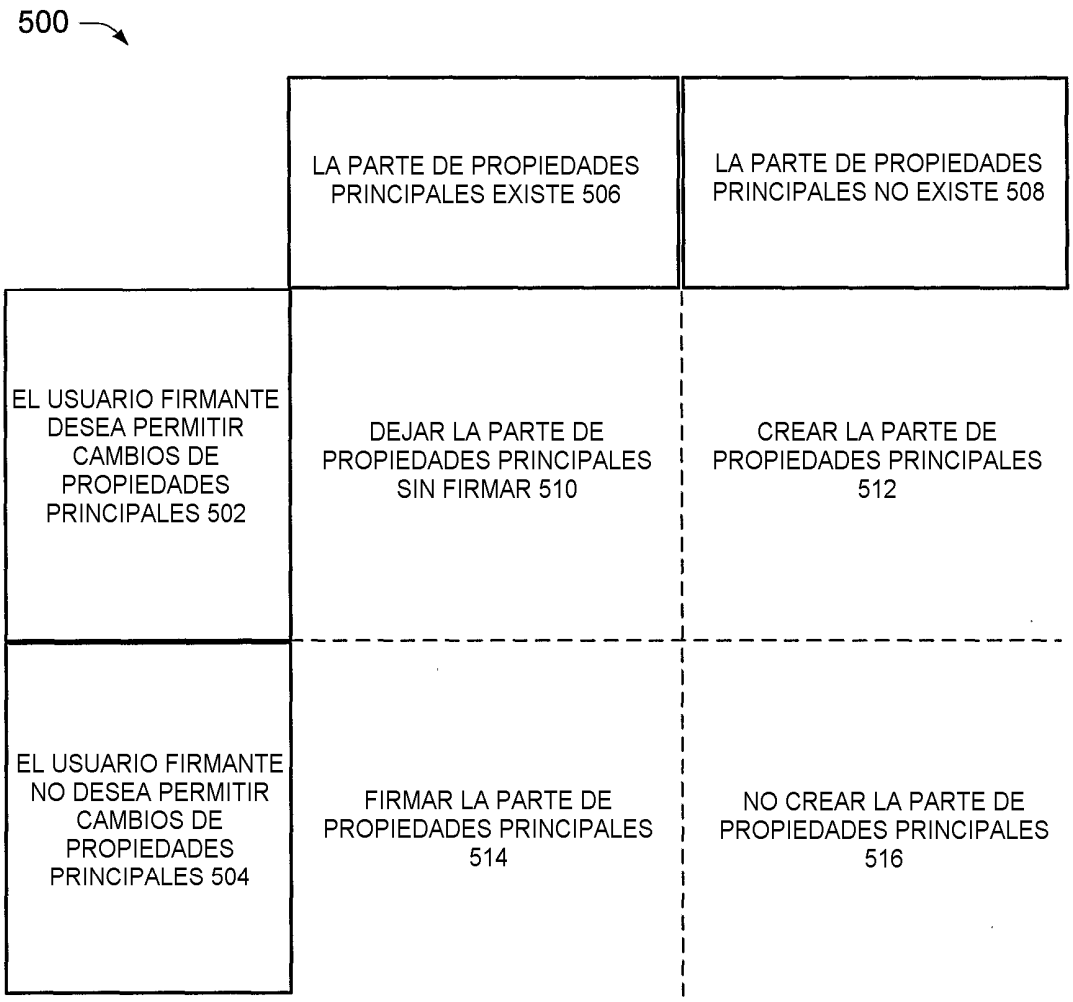
500
LA PARTE DE PROPIEDADES PRINCIPALES EXISTE 506
LA PARTE DE PROPIEDADES PRINCIPALES NO EXISTE 508
EL USUARIO FIRMANTE DESEA PERMITIR CAMBIOS DE PROPIEDADES PRINCIPALES 502
DEJAR LA PARTE DE PROPIEDADES PRINCIPALES SIN FIRMAR 510
CREAR LA PARTE DE PROPIEDADES PRINCIPALES 512
EL USUARIO FIRMANTE NO DESEA PERMITIR CAMBIOS DE PROPIEDADES PRINCIPALES 504
FIRMAR LA PARTE DE PROPIEDADES PRINCIPALES 514
NO CREAR LA PARTE DE PROPIEDADES PRINCIPALES 516

FIG. 5

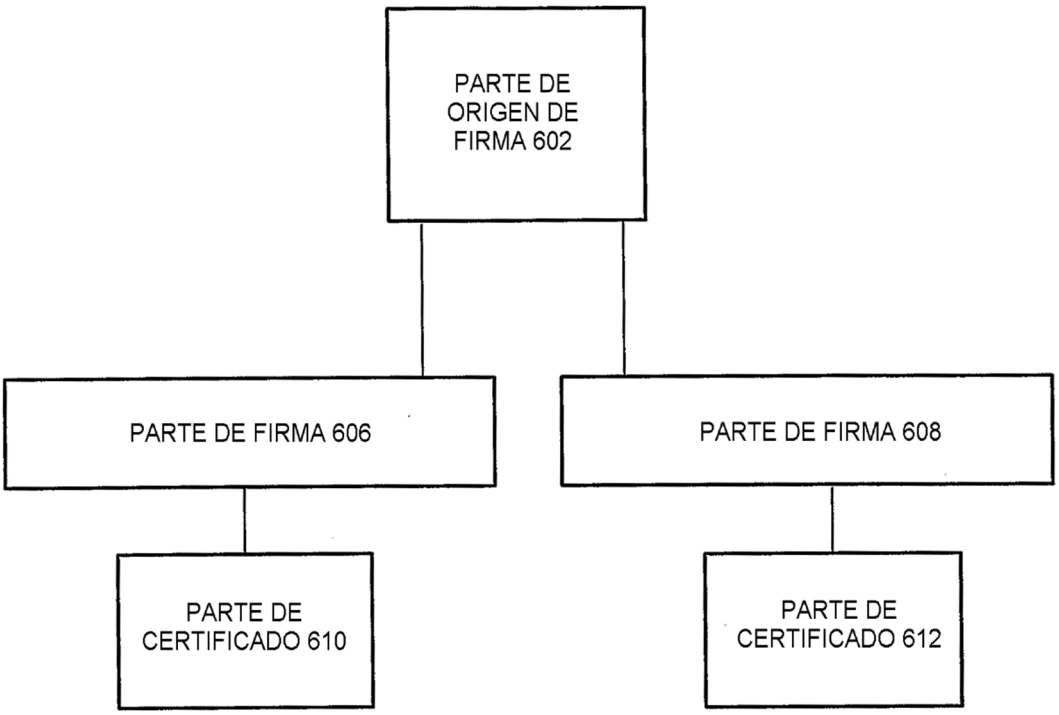
PARTE DE ORIGEN DE FIRMA 602
PARTE DE FIRMA 606
PARTE DE FIRMA 608
PARTE DE CERTIFICADO 610
PARTE DE CERTIFICADO 612

FIG. 6

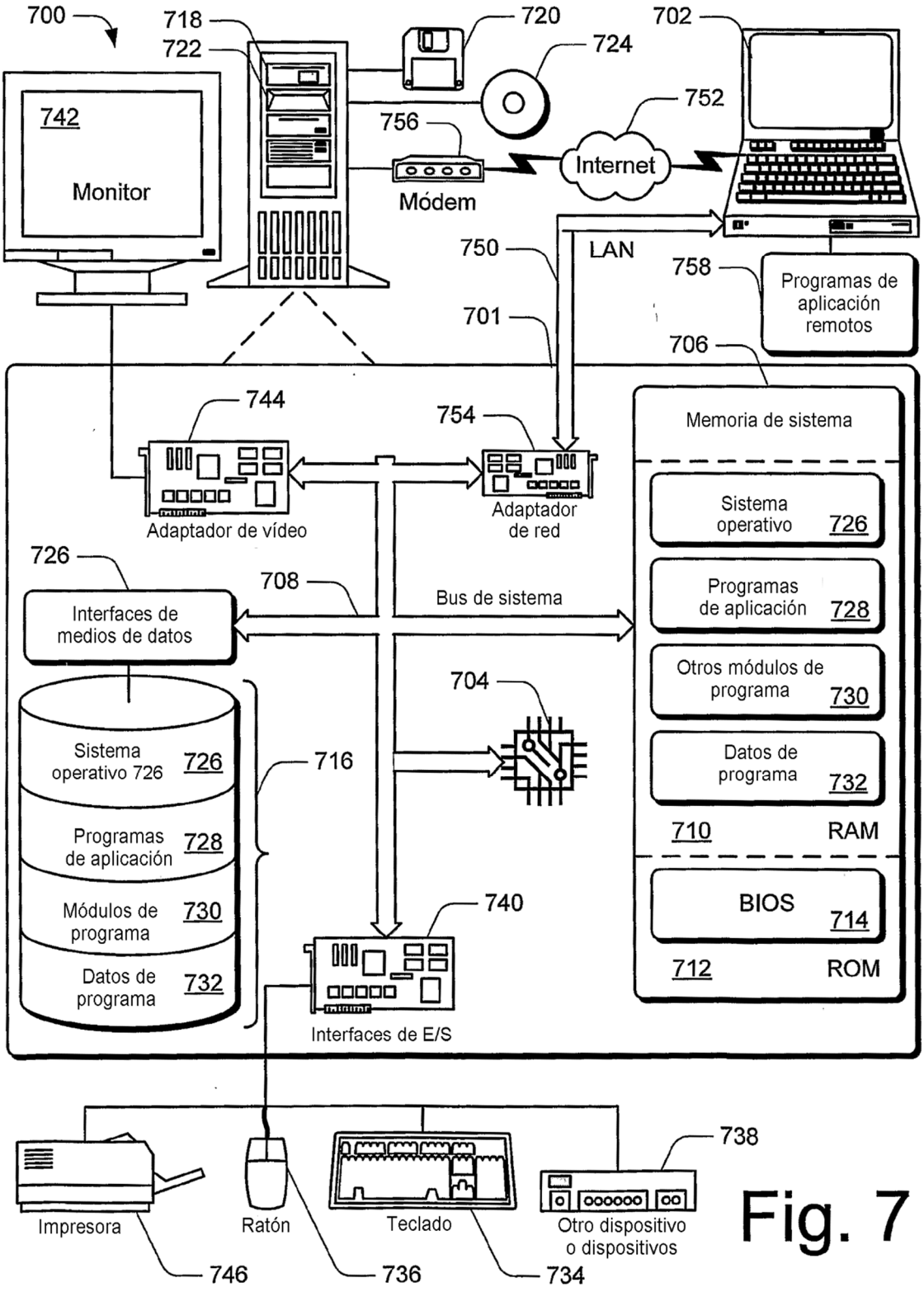
700
718
722
720
724
702
742
Monitor
752
756
Internet
Módem
750
LAN
758
Programas de aplicación remotos
701
706
744
754
Memoria de sistema
Adaptador de vídeo
Adaptador de red
Sistema operativo 726
726
Programas de aplicación 728
728
Otros módulos de programa 730
730
Datos de programa 732
732
708
Bus de sistema
Interfaces de medios de datos
704
716
Sistema operativo 726
Programas de aplicación
Módulos de programa
Datos de programa
710
RAM
740
BIOS 714
714
712
ROM
Interfaces de E/S
738
Impresora
Ratón
Teclado
Otro dispositivo o dispositivos
746
736
734

Fig. 7

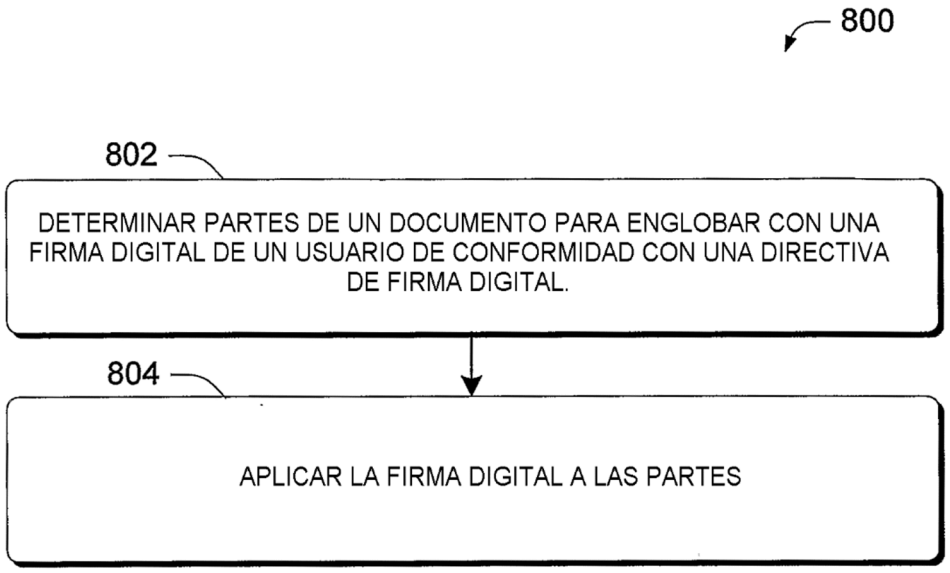
800
802
DETERMINAR PARTES DE UN DOCUMENTO PARA ENGLOBAR CON UNA FIRMA DIGITAL DE UN USUARIO DE CONFORMIDAD CON UNA DIRECTIVA DE FIRMA DIGITAL.
804
APLICAR LA FIRMA DIGITAL A LAS PARTES

Fig. 8