(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 637 251**

(51) Int. CI.:

H04L 12/58 (2006.01)
H04L 29/08 (2006.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **21.10.2002 E 02023650 (1)**

(97) Fecha y número de publicación de la concesión europea: **17.05.2017 EP 1304848**

(54) Título: **Mecanismo de seguridad flexible de mensaje electrónico**

(30) Prioridad:

19.10.2001 US 346370 P
14.08.2002 US 219898

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
11.10.2017

(73) Titular/es:

MICROSOFT TECHNOLOGY LICENSING, LLC (100.0%)
ONE MICROSOFT WAY
REDMOND, WA 98052, US

(72) Inventor/es:

KALER, CHRISTOPHER G.;
SHEWCHUK, JOHN P. y
DELLA-LIBERA, GIOVANNI M.

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

DESCRIPCIÓN

Mecanismo de seguridad flexible de mensaje electrónico

1. Campo de la invención

La presente invención se refiere a mensajería electrónica y más particularmente, a mecanismos para permitir un uso más flexible de mecanismos de seguridad cuando se comunica usando mensajes electrónicos.

2. Tecnología relacionada

La tecnología informática ha transformado el modo en que trabajamos y jugamos. Las tecnologías e infraestructuras de redes informáticas de módem permiten a diferentes aplicaciones y usuarios comunicar datos de manera electrónica incluso a grandes distancias relativamente rápido usando sistemas informáticos fácilmente disponibles. Tales sistemas informáticos pueden incluir, por ejemplo, ordenadores de escritorio, ordenadores portátiles, Asistentes Personales Digitales (PDA), teléfonos digitales o similares.

Actualmente, los sistemas informáticos están tan interconectados que un sistema informático es literalmente capaz de comunicarse con cualquier otro de los muchos millones de otros sistemas informáticos esparcidos a por todo el mundo. Esto es útil ya que ahora podemos comunicarnos más fácilmente. Sin embargo, este alto nivel de interconectividad también nos expone a problemas de seguridad. Por ejemplo, a menudo es necesario verificar que un dispositivo informático o usuario asociado es realmente la misma entidad que pretenden ser en un procedimiento llamado autenticación. También, a menudo es importante validar la integridad de un mensaje electrónico para estar seguro de que el mensaje electrónico no se ha comprometido durante la transmisión.

Las mejoras en los mecanismos de seguridad son beneficio importante ya que las brechas en seguridad pueden provocar mucho daño, económico o de otro tipo, a entidades que legalmente desean comunicaciones electrónicas seguras. Los principios de la presente invención mejoran la seguridad sobre las tecnologías de seguridad convencionales como se describirá a continuación en mayor detalle. El documento WO 97/50205 se refiere al sistema y los procedimientos para firmar digitalmente un acuerdo digital entre nodos ubicados remotamente en una manera que impide la retención fraudulenta del acuerdo digital completamente firmado; en un esfuerzo por ganar unas ventajas injustas sobre un acuerdo comercial de contratista. El sistema comprende un nodo de arbitraje y uno o más nodos signatorios acoplados juntos a través de un enlace de comunicación. Cada uno de los nodos signatarios puede incluir una clave privada que se usa para firmar digitalmente un mensaje, formar una firma digital y transmitir la firma digital sobre el enlace de comunicación al nodo servidor. Este procedimiento de firma digital permite a destinatario de la firma digital verificar la identidad de la parte que envía la firma digital. Esto puede lograrse encriptando la firma digital con una clave pública que corresponde a la clave privada de la firma. El nodo servidor transmite una señal de acuse de recibo para las firmas digitales desde las partes a cada una de estas partes al recibir todas las firmas digitales y determinar que cada una de las firmas digitales es válida.
El documento EP1 111 559 A2 se refiere a transacciones electrónicas seguras realizadas sobre redes públicas tal como Internet. Un mensaje electrónico para transmisión sobre una red se crea encriptando un primer componente con una primera clave criptográfica, que se asocia con una primera entidad de red, tal como el primer componente encriptado puede descifrarse únicamente por la primera entidad de red. Un segundo componente, que es diferente del primer componente, se encripta con una segunda clave criptográfica, que se asocia con una segunda entidad de red, de tal manera que el segundo componente puede también descifrarse por la primera entidad de red. El primer y el segundo componente encriptado se combinan para crear el mensaje electrónico.

Breve sumario de la invención

Es el objeto de la invención proporcionar un mecanismo de seguridad flexible y fiable cuando se comunica usando mensajes electrónicos, sin la necesidad de compartir un par de claves públicas/privadas entre las partes. En particular, la presente invención proporciona medios para determinar si la manipulación de un mensaje electrónico ha podido tener lugar. Se especifican las reivindicaciones preferentes en las reivindicaciones dependientes.

Los principios de la invención se refieren a mecanismos para proporcionar mecanismos de seguridad fáciles y flexibles cuando se comunica usando mensajes electrónicos. El mensaje electrónico puede tener múltiples diferentes tipos de credenciales. El mensaje electrónico puede incluir el formato codificado y tipo codificado de cada uno de las credenciales, permitiendo así acceso adecuado a la credencial por tanto el sistema informático receptor como por un sistema informático intermediario. El mensaje electrónico puede incluir también múltiples firmas que se firmaron cada una usando una credencial diferente. Las firmas pueden tener cada una referencia a una ubicación incluso externa al mensaje electrónico. El sistema informático receptor puede evaluar la credencial externa contra la firma para determinar si ha podido tener lugar la manipulación del mensaje electrónico.

Se expondrán características y ventajas adicionales de la invención en la descripción que sigue, y en parte será obvio de la descripción, o pueden aprenderse por la práctica de la invención. Las características y ventajas de la invención se pueden realizar y obtener por medio de los instrumentos y combinaciones particularmente señaladas en las reivindicaciones adjuntas. Estas y otras características de la presente invención se harán totalmente evidentes a partir de la siguiente descripción y las reivindicaciones adjuntas, o pueden aprenderse por la práctica de la invención

como se expone a continuación.

Breve descripción de los dibujos

Con el fin de describir la manera en la que las ventajas y características anteriormente citadas de la invención pueden obtenerse, una descripción más particular de la invención brevemente descrita anteriormente se mostrará por referencia a las realizaciones específicas de la misma que se ilustran en los dibujos adjuntos. Comprendiendo que estos dibujos representan solo realizaciones típicas de la invención que, por lo tanto, no deben considerarse como limitación de su ámbito, la invención se describirá y explicará con especificidad adicional y detalle a través del uso de los dibujos adjuntos en los que:

la figura 1 ilustra un sistema informático adecuado en el que los principios de la presente invención pueden emplearse; la figura 2 ilustra un diagrama de flujo de un procedimiento para transmitir de manera segura un mensaje electrónico de acuerdo con los principios de la presente invención;
la figura 3 ilustra una estructura de datos de un mensaje electrónico que tiene múltiples diferentes tipos de credenciales en el encabezado del mensaje electrónico de acuerdo con los principios de la presente invención;
la figura 4A ilustra un entorno de red en el que múltiples diferentes credenciales se usan para identificar un sistema informático fuente en un sistema informático receptor particular en un modelo llamado en el presente documento "modelo de receptor de única credencial-credenciales múltiples";
la figura 4B ilustra un entorno de red en el que diferentes credenciales en el mensaje electrónico se pueden usar para identificar el sistema informático fuente en un sistema informático intermediario y para identificar el dispositivo informático fuente en un sistema informático receptor en un modelo llamado en el presente documento el "modelo de credencial serial";
la figura 4C ilustra un entorno de red en el que diferentes credenciales en el mensaje electrónico pueden usarse para identificar el sistema informático fuente en diferentes sistemas informáticos receptores en un modelo llamado en el presente documento "modelo de credencial paralelo";
la figura 4D ilustra un entorno de red que combina todos los modelos de la figura 4A, 4B y 4C; y la figura 5 ilustra un árbol de herencia semántica de credenciales de acuerdo con los principios de la presente invención.

Descripción detallada de las realizaciones preferentes

Los principios de la presente invención se refieren a procedimientos, sistemas, productos de programas informáticos y estructuras de datos que permiten comunicaciones más seguras de un mensaje electrónico.

Múltiples diferentes credenciales y/o firmas basadas en diferentes credenciales pueden incluirse en una parte de encabezado de un único mensaje electrónico. Estas diferentes firmas y/o credenciales pueden usarse por diferentes sistemas informáticos receptores, por un único sistema informático receptor o incluso por diferentes sistemas informáticos a lo largo de una ruta de enrutamiento del mensaje electrónico.

El mensaje electrónico puede incluir una identificación de un algoritmo de codificación y el tipo de credencial incluido en el mensaje electrónico. Por consiguiente, múltiples diferentes credenciales pueden incluirse teniendo diferente codificación. El sistema informático receptor puede decodificar y procesar la credencial apropiada dado el tipo de identificación del algoritmo de codificación y el tipo de credencial.

También, el mensaje electrónico puede incluir un puntero que hace referencia a una credencial que es accesible al sistema informático receptor, tanto dentro del mismo mensaje electrónico como desde alguna otra ubicación. El sistema informático receptor puede entonces comparar las credenciales referenciadas desde las credenciales usadas para generar la firma. Si se produce una coincidencia, entonces los datos firmados pueden asociarse con las credenciales. Por consiguiente, la integridad de cualquier declaración realizada en las credenciales tales como la identidad, los derechos y así sucesivamente, pueden verificarse.

Las realizaciones dentro del ámbito de la presente invención incluyen medios legibles por ordenador para llevar o tener instrucciones ejecutables por ordenador o estructuras de datos almacenadas en los mismos. Tales medios legibles por ordenador pueden ser cualquier medio disponible al que se puede acceder por un ordenador de objetivo general o de objetivo especial. A modo de ejemplo, y sin limitación, tales medios legibles por ordenador pueden comprender medios legibles por ordenador físicos tales como RAM, ROM, EEPROM, CD-ROM u otro almacenamiento en disco óptico, almacenamiento en disco magnético u otros dispositivos de almacenamiento magnético o cualquier otro medio que se puede usar para llevar o almacenar medios de código de programas deseados en forma de instrucciones ejecutables por ordenador o estructuras de datos y a las que se pueden acceder por un ordenador de objetivo general o de objetivo especial.

Cuando la información se transfiere o proporciona sobre una red u otra conexión de comunicaciones (ya sea cableada, inalámbrica o una combinación de cableada o inalámbrica) a un ordenador, el ordenador ve correctamente la conexión como un medio legible por ordenador. De esta manera, cualquier tal conexión se denomina correctamente un medio legible por ordenador. Se deberían incluir también combinaciones de lo anterior dentro del ámbito de los medios legibles por ordenador. Las instrucciones ejecutables por ordenador comprenden, por ejemplo, instrucciones y datos que provocan que el ordenador de objetivo general, el ordenador de objetivo especial o el dispositivo de procesamiento de objetivo especial lleve a cabo una cierta función o grupo de funciones.

La figura 1 y la siguiente discusión se dirigen a proporcionar una descripción breve y general de un entorno informático adecuado en el que la invención puede implementarse. Aunque no es necesario, la invención se describirá en el contexto general de las instrucciones ejecutables por ordenador, tales como módulos de programas, que se ejecutan por ordenadores en entornos de red. Generalmente, los módulos de programa incluyen rutinas, programas, objetos, componentes, estructura de datos y similares, que llevan a cabo tareas particulares o implementan tipos de datos abstractos particulares.

Los expertos en la materia apreciarán que la invención puede practicarse en entornos informáticos de redes con muchos tipos de configuraciones de sistemas informáticos, incluyendo ordenadores personales, dispositivos de mano, sistema multiprocesador, electrónica de consumo basada en microprocesador o programable, ordenadores en red, miniordenadores, ordenadores centrales, y similares. La invención puede también practicarse en entornos informáticos distribuidos en los que las tareas se llevan a cabo por dispositivos de procesamiento local y remoto que se enlazan (ya sea por enlaces, enlaces inalámbricos o por una combinación de enlaces cableados o inalámbricos) a través de una red de comunicaciones. En un entorno informático distribuido, los módulos de programa pueden ubicarse tanto en dispositivos de almacenamiento de memoria local como en dispositivos de almacenamiento de memoria remota.

Con referencia a la figura 1, un sistema ejemplar para implementar la invención incluye un dispositivo informático de objetivo general en forma de un ordenador 120 convencional, incluyendo una unidad 121 de procesamiento, una memora 122 de sistema y un bus 123 de sistema que acopla diversos componentes de sistema que incluyen la memoria 122 de sistema a la unidad 121 de procesamiento. A lo largo de esta descripción, los números de elementos comienzan con el mismo número que la figura en la que los elementos correspondientes se introdujeron primero. Por ejemplo, todos los números de elemento en la figura 1 se enumeran de 100 mientras que los números de elemento en la figura 2 son números de 200, y así sucesivamente.

El bus 123 de sistema puede ser cualquiera de muchos tipos de estructuras de bus que incluyen un bus de memoria o un controlador de memoria, un bus periférico y un bus local que usa cualquiera de entre una variedad de arquitecturas de bus. La memoria de sistema incluye leer solo la memoria 124 de solo lectura (ROM) y la memoria 125 de acceso aleatorio (RAM). Un sistema 126 básico de entrada/salida (BIOS), que contiene las rutinas básicas que ayudan a transferir información entre los elementos dentro del ordenador 120, tal como durante la puesta en marcha, pueden almacenarse en la ROM 124.

El ordenador 120 puede incluir también un disco 127 duro informático magnético para leer desde y escribir en un disco 139 duro magnético, una unidad 128 de disco magnético para leer desde o escribir en un disco 129 magnético extraíble y una unidad 130 de disco óptico para leer desde o escribir en un disco 131 óptico, tal como un CD-ROM u otro medio óptico. La unidad 127 de disco duro magnético, la unidad 128 de disco magnético y la unidad 130 de disco óptico se conectan al sistema 123 de bus por una interfaz 132 de unidad de disco duro, una interfaz de unidad de disco magnético 133 y una interfaz 134 óptica, respectivamente. Las unidades y sus medios legibles por ordenador asociados proporcionan almacenamiento no volátil de instrucciones ejecutables por ordenador, estructuras de datos, módulos de programa y otros datos para el ordenador 120. Aunque el entorno ejemplar descrito en el presente documento emplea un disco 139 duro magnético, un disco 129 magnético extraíble y una unidad 131 óptica extraíble, otros tipos de medios legibles por ordenador para almacenar datos se pueden usar, incluyendo casetes magnéticos, tarjetas de memoria flash, discos de vídeo digitales, cartuchos de Bernoulli, RAM, ROM y similares.

Los medios de código de programa comprenden uno o más módulos de programa pueden almacenarse en el disco 139 duro, disco 129 magnético, disco 131 óptico, ROM 124 o RAM 125, incluyendo un sistema 135 operativo, uno o más programas 136 de aplicaciones, otros módulos 137 de programa y datos 138 de programa. Un usuario puede introducir comandos e información en el ordenador 120 a través del teclado 140, dispositivo 142 apuntador u otros dispositivos de entrada (no mostrados), tal como un micrófono, un mando de videojuegos, almohadilla de juego, antena parabólica, escáner o similares. Estos y otros dispositivos de entrada están a menudo conectados a la unidad 121 de procesamiento a través de una interfaz 46 de puerto en serie acoplada al bus 123 de sistema. De manera alternativa, los dispositivos de entrada pueden conectarse por otras interfaces, tales como un puerto paralelo, un puerto de juego o un bus en serie universal (USB). Un monitor 147 u otro dispositivo de visualización también se conecta al bus 123 de sistema mediante una interfaz, tal como un adaptador 148 de vídeo. Además del monitor, los ordenadores personales incluyen típicamente otros dispositivos periféricos de salida (no mostrados), tal como altavoces e impresoras.

El ordenador 120 puede operar en un entorno de red que usa conexiones lógicas a uno o más ordenadores remotos, tal como los ordenadores 149a remotos 149b. Los ordenadores 149a y 149b puede cada uno ser un ordenador personal, un servidor, un rúter, un ordenador de red, un dispositivo par u otro nodo de red común y, típicamente, incluyen muchos o todos los elementos descritos anteriormente en relación al ordenador 120, aunque solo los dispositivos 150a y 150b de almacenamiento de memoria y sus programas 136a y 136b de aplicación asociados se han ilustrado en la figura 1. Las conexiones lógicas representadas en la figura 1 incluyen una red 151 de área local (LAN) y una red 152 de área extensa (WAN) que se presentan aquí a modo de ejemplo y sin limitación. Tales entornos de red son comunes en redes informáticas de toda la oficina o en toda la empresa, intranets e Internet.

Cuando se usa en un entorno de red LAN, el ordenador 120 se conecta a la red 151 local a través de una interfaz o adaptador 153 de red. Cuando se usa en un entorno de red WAN, el ordenador 120 puede incluir un módem 154, un enlace inalámbrico u otros medios para establecer comunicaciones sobre la red 152 de área extensa, tal como Internet. El módem 154, que puede ser interno o externo, se conecta al bus 123 de sistema a través de la interfaz 146 de puerto en serie. En un entorno de red, los módulos de programa representados en relación con el ordenador 120 o partes de los mismos, pueden almacenarse en el dispositivo de almacenamiento de memoria remota. Se apreciará que las conexiones de red mostradas son ejemplares y otros medios de establecer comunicaciones sobre una red 152 de área local pueden usarse.

Mientras que la figura 1 ilustra un ejemplo de un sistema que puede implementar los principios de la presente invención, cualquier sistema informático puede implementar las características de la presente invención. En la descripción y en las reivindicaciones, un "sistema informático" se define como cualquier componente o componentes de hardware que pueden usar software para llevar a cabo una o más funciones. Ejemplos de sistemas informáticos incluyen ordenadores de sobremesa, ordenadores portátiles, Asistentes Personales Digitales (PDA), teléfonos o cualquier otro sistema o dispositivo que tenga capacidades de procesamiento.

La figura 2 ilustra un procedimiento 200 para llevar a cabo mensajería electrónica de una manera segura. Algunos de los actos en la etapa del procedimiento 200 se llevan a cabo por un sistema informático remitente que envía un mensaje electrónico. Esos actos y esa etapa se enumeran generalmente en la columna de la izquierda de la figura 2 bajo el encabezado "REMITENTE". Otros actos del procedimiento 200 se llevan a cabo por un sistema informático receptor que recibe un mensaje electrónico. Esos actos se enumeran generalmente en la columna de la derecha en la figura 2 bajo el encabezado "RECEPTOR".

El procedimiento 200 incluye una etapa funcional orientada a resultados para construir un mensaje electrónico para proporcionar una mayor seguridad (etapa 210). Esta etapa funcional orientada a resultados puede incluir cualquier acto correspondiente para lograr este resultado. Sin embargo, en la realización ilustrada, la etapa 210 incluye actos 211 a 218 correspondientes. Un ejemplo de estructura de datos de mensaje electrónico se ilustra en la figura 3 como mensaje 300 electrónico. El procedimiento de la figura 2 se describirá con referencia frecuente a la estructura de datos de mensaje electrónico de la figura 3.

El procedimiento 200 incluye un acto de designar al menos una dirección de destino en el mensaje electrónico (acto 211). La dirección de destino corresponde a uno o más sistemas informáticos receptores. En referencia a la figura 3, el mensaje electrónico incluye un campo 310 de encabezado y un campo 330 de cuerpo. El campo 330 de cuerpo puede contener el contenido de la información deseada que se comunicara al (a los) receptor(es), mientras que el campo 310 de encabezado contiene información que facilita el transporte apropiado y seguro y el procesamiento del mensaje electrónico. El campo 310 de encabezado incluye un campo 311 de dirección de destino que contiene la dirección o direcciones de destino de uno o más receptores deseados del mensaje electrónico.

El procedimiento 300 incluye entonces un acto de incluir uno o más tokens de seguridad en una parte de encabezado del mensaje electrónico (acto 212). El uno o más tokens de seguridad pueden ser, por ejemplo, una o más firmas. Por ejemplo, el campo 310 de encabezado incluye una primera firma 312, una posible segunda firma 313 y potencialmente otras firmas 314. La primera firma 312 tiene una forma oval que representa que la primera firma puede haberse firmado usando una credencial 315 correspondiente, que también se representa como con forma oval. La segunda firma 313 tiene forma trapezoidal para representar que la segunda firma puede haberse firmado usando una credencial 316 correspondiente, que también se representa como con forma trapezoidal.

Además de incluir las firmas (acto 212) u otros tokens de seguridad en el mensaje electrónico, el procedimiento 300 incluye un acto de dosificar una o más credenciales (acto 213), y entonces el acto de incluir la una o más credenciales codificadas en el mensaje electrónico (acto 214). En algunos casos, la(s) credencial(es) incluidas en el mensaje electrónico puede no codificarse en absoluto, eliminando así el acto 213. En otros casos, una credencial no se incluirá en el mensaje electrónico eliminando así el acto 214. Por ejemplo, puede no existir ninguna causa para incluir una credencial si hay una referencia a un campo de credencial asociado descrito anteriormente donde la credencial puede ser externa al mensaje electrónico.

Las credenciales pueden ser, por ejemplo, cualquier elemento de información que ayude a identificar y/o autentificar el proveedor de credenciales. Un tipo de credencial es una licencia, que contiene un conjunto de afirmaciones relacionadas firmadas por una autoridad. Algunas afirmaciones pueden ser sobre claves que pueden usarse para firmar y/o encriptar mensajes. Entre los ejemplos de licencias se incluyen los certificados X.509 y los tickets Kerberos. El propietario de una licencia es una entidad que puede usar la licencia con autoridad. Específicamente, el principio tiene el conocimiento necesario para aplicar las claves criptográficas ubicadas en la licencia o licencias adjuntas. En la figura 3, las credenciales incluidas se representan por la primera credencial 315, la segunda credencial 316 y otras credenciales 317.

El procedimiento 200 también incluye un acto de incluir, en la parte de encabezado, una identificación de un formato de codificación de la(s) credencial(es) (acto 215). Esta identificación se representa en la figura 3 por la primera credencial 315 por el campo 318A de formato de codificación. La identificación se representa en la figura 3 por la segunda credencial 316 por el campo 318B de formato de codificación. El procedimiento 300 también incluye un acto

de incluir, en la parte de encabezado, una identificación de un tipo de la credencial(es) (acto 216). Por ejemplo, el tipo de credencial puede ser un certificado X.509 o un ticket Kerberos. La identificación del tipo de credencial se representa en la figura 3 para la primera credencial 315 por el campo 319A de tipo de credencial, y para la segunda credencial 316 por el campo 319B de tipo de credencial.

En este ejemplo, existe una identificación del formato de codificación y un tipo de credencial para cada una de las credenciales incluidas en el mensaje electrónico, aunque esto no es necesario. Por ejemplo, en casos en los que el formato de codificación es el mismo para todas las credenciales en el mensaje electrónico, el formato de codificación puede enumerarse en solo una parte del mensaje electrónico. De manera similar, si el tipo de credencial es el mismo para todas las credenciales en el mensaje electrónico, el formato de credencial puede enumerarse solo una vez. Además, si una credencial particular tiene un formato de codificación predeterminado (y/o tipo de credencial), entonces el formato de codificación particular (y/o tipo de credencial) necesita no incluirse expresamente para esa credencial.

También, la identificación del formato de codificación y tipo de credencial se ilustran como incluyéndose en el campo de credencial correspondiente. Si estos campos se incluyen en el campo de credencial correspondiente, los actos 215 y 216 tendrían lugar con el acto 213 para esa credencial. Sin embargo, el formato de codificación y el campo de tipo puede, por el contrario, solo asociarse con el campo de credencial correspondiente.

El procedimiento 300 también incluye un acto de generar una referencia que indica dónde una credencial asociada con la firma puede encontrarse (acto 217) y que incluye la referencia en la parte de encabezado de un mensaje electrónico (acto 218). La referencia se representa en la figura 3 para la primera firma 312 por la referencia al campo 320A de credencial asociado y para la segunda firma 313 por la referencia al campo 320B de credencial asociado. Aunque la referencia puede incluir una referencia a una posición interna al mensaje electrónico (por ejemplo, campos 316 y 317 de credencial), la referencia puede también ser un Localizador de Recurso Uniforme (URL) que identifica una ubicación externa al mensaje electrónico donde la credencial asociada puede encontrarse.

El sistema informático de envío transmite entonces el mensaje electrónico a uno o más sistemas informáticos receptores (acto 219), que entonces recibe el mensaje electrónico (acto 220). El mensaje electrónico puede contener múltiples diferentes firmas que se generaron usando múltiples diferentes tipos de credenciales. El sistema informático receptor puede entonces seleccionar uno de entre múltiples firmas incluidas en una parte de encabezado del mensaje electrónico (acto 221), y entonces lee esa firma electrónica desde el mensaje electrónico (acto 222). Por consiguiente, el sistema informático receptor puede seleccionar una, alguna o todas las firmas incluidas que dependiendo de qué sistema informático receptor se configura para procesar y confiar.

La habilidad del mensaje 300 electrónico para contener múltiples credenciales de diferentes tipos permite muchas nuevas configuraciones de seguridad de red. Por ejemplo, la figura 4A ilustra un entorno 400A de red en el que múltiples diferentes credenciales se usan para identificar un sistema 401A informático fuente en un sistema 411A informático receptor particular en un modelo llamado en el presente documento "modelo de receptor de única credencial-credenciales múltiples". En este modelo, un sistema 411A informático receptor único usas dos credenciales 421 y 422 diferentes con el fin de autentificar el sistema 401A informático fuente. Las credenciales se ilustran en las figuras 4A a 4D como teniendo diferentes formas para enfatizar que las credenciales pueden ser de tipos diferentes.

La figura 4B ilustra un entorno 400B de red en el que diferentes credenciales en el mensaje electrónico se pueden usar para identificar un sistema 400B informático fuente en un sistema 411B informático intermediario y para identificar el dispositivo 401B informático fuente en un sistema 412B informático receptor en un modelo llamado en el presente documento el "modelo de credencial serial". En el modelo 400B de credencial serial ilustrada, el sistema 411B informático intermediario usa la credencial 421, mientras que el sistema 412B informático receptor usa la credencial 422.

La figura 4C ilustra un entorno 400C de red en el que las diferentes credenciales en el mensaje electrónico pueden usarse para identificar el dispositivo informático fuente en dispositivos 411C y 412C informáticos receptores en un modelo llamado en el presente documento el "modelo de credencial paralelo". En el modelo 400C de credencial paralelo ilustrado, el sistema 411C informático receptor usa la credencial 421, mientras que el sistema 412C informático receptor usa la credencial 422.

Existen diversas combinaciones de cada uno de los modelos de la figura 4A a 4C que forman una variedad prácticamente sin límites de configuraciones de red. Por ejemplo, la figura 4D ilustra un entorno 400D de red que combina todos los modelos de la figura 4A, 4B y 4C en una de las muchas maneras posibles. En el entorno 400D, el mensaje electrónico incluye tres credenciales 421, 422 y 423. La credencial 423 es diferente de las credenciales 421 y 422 como se representa por su forma triangular. El sistema 411C informático intermediario usa la credencial 421, el sistema 412D informático receptor usa la credencial 422 y el sistema 413D informático receptor usa las credenciales 422 y 423.

Volviendo a la figura 3, el sistema informático receptor también puede leer, la referencia que indica donde una credencial asociada puede encontrarse (acto 223), usa esta referencia para encontrar la credencial (acto 224), y

entonces determinar si la credencial corresponde con la firma electrónica, (acto 225). Si ahí la credencial referenciada corresponde a la firma, entonces los datos firmados pueden asociarse con la credencial. Por consiguiente, la integridad de cualquier declaración realizada en las credenciales tales como la identidad, los derechos y así sucesivamente, pueden estar más seguros, especialmente si la credencial referenciada fuera externa al mensaje electrónico y, por lo tanto, no se somete a las mismas instancias de manipulación a las que el mensaje electrónico puede someterse.

En una realización, el mensaje 300 electrónico puede ser una envoltura de Protocolo Simple de Acceso de Objetos (SOAP) aunque esto no es necesario. Las dos solicitudes provisionales de patentes previamente incorporadas en el presente documento por referencia proporcionan varios ejemplos de envolturas SOAP que incorporan diversos aspectos de la presente invención. La siguiente envoltura SOAP es un ejemplo de código de una realización específica de la estructura de datos del mensaje 300 electrónico. El ejemplo de código se representa en Lenguaje de Marcado extensible (XML) versión 1.0. La numeración de líneas se ha añadido para mayor claridad en la explicación de la estructura del ejemplo de código. Aunque ejemplo de código muestra una implementación específica, hay una gran variedad de diferentes implementaciones que pueden emplear los principios de la presente invención. Por ejemplo, aunque este ejemplo ilustra el uso de encabezados jerárquicos estructurados en un cierto modo y que tienen usos de encabezados particulares, otras realizaciones pueden tener una jerarquía y uso diferentes de los encabezados sin alejarse del ámbito de los principios de la presente invención.

```
1.  <?xml version-“1.0" encoding="utf-8"?>
2.  <S:Envelope
3.  xmlns:S=“http://schemas.xmlsoap.org/soap/envelope/"
4.          xmlns:xsd="http://www.w3 org/2001/XMLSchema"
5.          xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance>
6.      <Header>
7.      <m:path xmlns:m="http://schemas.xmlsoap.org/rp">
8.          PATH INFORMATION
9.      </m:path>
10.     <wssec:credentials
11.         xmlns:wssec="http://schemas.xmlsoap.org/ws/2001/10/security">
12.         <wslic:binaryLicence
13.             xmlns:wslic="http://schemas.xmlsoap.org/ws/2001/10/licenses"
14.                 wslic:valueType="wslic:x509v3"
15.                 xsi:type="xsd:base64Binary"
16.                 id="X509License">
17.                     X509LICENSE ENCODED IN BASE64BINARY
18.         </wslic:binaryLicense>
19.         <wslic:binaryCredential xmlns:tru="...">
20.                 wslic:valueType="tru:binaryCredentialFormat"
21.                 xsi:type="xsd:base64Binary"
22.                 id="BinaryCredential">
23.                     BINARY CREDENTIAL ENCODED IN BASE64BINARY
24.         </wslic:binaryCredential>
25.     </wssec:credentials>
26.     <wssec:integrity>
27.         <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
28.             <ds:SignedInfo>
29.                 <ds:CanonicalizationMethod
30.                     Algorithm="http://www.w3.org/Signature/Drafts/xml-exc-c14n"/>
31.                 <ds.SignatureMethod
32.                     Algorithm"http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
33.                 <ds:Reference>
34.                     <ds:Transforms>
35.                         <ds:Transform Algorithm="http://schemas.xmlsoap.org/
36.                             2001/10/security#RoutingSignatureTransform"/>
37.                         <ds:Transform Algorithm="http://www.w3.org/
38.                             TR/2001/REC-xml-c14n-20010315/>
39.                     </ds:Transforms>
40.                     <ds:DigestMethod Algorithm="http://www.w3.org/
41.                         2000/09/xmldsig#sha1"/>
42.                 </ds:Reference>
43.             </ds:SignedInfo>
44.             <ds:SignatureValue>
45.                 FIRST SIGNATURE VALUE
46.             </ds:SignatureValue>
47.             <ds:KeyInfo>
```

```
48.                 <wssec:LicenseLocation="#X509License"/>
49.             </ds:KeyInfo>
50.         </ds:Signature>
51.         <ds:Signature>
52.             <ds:SignedInfo>
53.                 <ds:CanonicalizationMethod
54.                     Algorithm="http://www.w3.org/Signature/Drafts/xml-exc-c14n"/>
55.                 <ds:SignatureMethod
56.                     Algorithm"http://www.w3.org/2000/09/xmldsig#rsa-sha1/>
57.                 <ds:Reference>
58.                     <ds:Transforms>
59.                         <ds:Transform Algorithm="http://schemas.xmlsoap.org/
60.                             2001/10/security#RoutingSignatureTransform"/>
61.                         <ds:Transform Algorithm="http://www.w3.org/ .
62.                             TR/2001/REC-xml-c14n-20010315/>
63.                     </ds:Transforms>
64.                     <ds:DigestMethod Algorithm="http://www.w3.org/
65.                         2000/09/xmldsig#sha1"/>
66.                 </ds:Reference>
67.             </ds:SignedInfo>
68.             <ds:SignatureValue>
69.                 SECOND SIGNATURE VALUE
70.             </ds:SignatureValue>
71.             <ds:KeyInfo>
72.                 <wssec:LicenseLocation="#BinaryCredential"/>
73.             </ds:KeyInfo>
74.         </ds:Signature>
75.     </wssec:integrity>
76. </S:Header>
77. <S:Body>
78.     BODY
79. </S:Body>
80. </S:Envelope>
```

La línea 1 define la versión XML que la envoltura SOAP sigue, así como el formato de codificación para la envoltura SOAP como un todo.

Las líneas 2 a 80 definen la envoltura SOAP que incluye dos credenciales diferentes, dos firmas diferentes firmadas usando las credenciales, y las referencias a las credenciales para cada una de las firmas. También, el tipo de codificación y el tipo de formato de cada una de las credenciales se especifica.

Las líneas 3 a 5 definen abreviaturas de nombres de espacio global usadas a través de la envoltura SOAP. Es una práctica estándar especificar la abreviatura de nombre de espacio en esta parte de la envoltura SOAP. Estas abreviaturas de nombre de espacio corresponden a un nombre de espacio que define un estándar acerca de cómo elementos particulares a los que el nombre de espacio se aplica deben interpretarse.

Las líneas 77 a 79 representan el cuerpo de la envoltura SOAP y es un ejemplo del campo 330 de cuerpo de la figura 3. Cabe señalar que el contenido del cuerpo real se reemplaza con el término en mayúsculas "BODY". Los términos en mayúsculas se usan a través del ejemplo de código para reemplazar contenido real cuyo valor no se incluye específicamente en el ejemplo de código y el valor no es importante para los principios de la presente invención. Por ejemplo, el término "BODY" en la línea 78 podría ser cualquier contenido sin afectar los principios de la presente invención.

Las líneas 6 a 76 representan la información de encabezado para la envoltura SOAP y es un ejemplo de campo 310 de encabezado de la figura 3.

Las líneas 7 a 9 expresan la ruta que el mensaje electrónico debe tomar. Los sistemas informáticos intermediarios tales como el sistema 411B informático intermediario de la figura 4B puede especificarse en esta sección.

Las líneas 10 a 25 definen un encabezado SOAP exclusivo llamado "credenciales". Este encabezado puede incluir varios tipos de credenciales deferentes. El formato de codificación y el tipo de credencial también puede especificarse en este encabezado.

Por ejemplo, las líneas 12 a 18 contienen una licencia binaria (ver línea 17) llamada "X509License" (llamada línea 16), que se define como siendo un certificado X.509 (ver línea 14), y que se identifica como codificándose usando la codificación base64binary (ver línea 15). La línea 14 es un ejemplo de campo 319A de tipo de credencial de la figura 3. La línea 15 es un ejemplo de campo 318A de formato de codificación de la figura 3. La línea 17 es un ejemplo del

primer campo 315 de credencial de la figura 3.

También, las líneas 19 a 24 contienen credenciales binarias (ver línea 23) llamadas "BinaryCredential" (ver línea 22), que se identifican como siendo un formato de credencial binario (ver línea 20), y que se identifica como codificándose también usando la codificación base64binary (ver línea 21). La línea 20 es un ejemplo de campo 319B de tipo de credencial de la figura 3. La línea 21 es un ejemplo de campo 318B de formato de codificación de la figura 3. La línea 23 es un ejemplo del segundo campo 316 de credencial de la figura 3.

Las líneas 26 a 75 definen un encabezado de "integridad" que contiene dos firmas, teniendo cada una una ubicación de referencia para encontrar una credencial correspondiente que se puede usar para verificar la integridad del mensaje electrónico (es decir, que el mensaje electrónico se envió por un firmante de la firma, y que el mensaje electrónico no se alteró en el tránsito).

En particular, un primer elemento de firma se referencia desde las líneas 27 a 50, con el segundo elemento de firma referenciándose desde las líneas 51 a 74. Cada elemento de firma sigue el esquema definido por la firma digital XML de acuerdo con el nombre de espacio "http://www.w3.org/2000/09/xmldsig#". Sin embargo, el elemento secundario KeyInfo dentro de cada firma digital XML incluye un elemento "LicenseLocation" que referencia la ubicación de una licencia (u otra credencial) que puede usarse para verificar la integridad del mensaje electrónico.

El primer elemento de firma incluye un elemento "SignedInfo" desde las líneas 28 a 43 que define procedimientos de canonicalización, algoritmo de recopilación y diversas transformaciones que se aplican a la firma. El primer valor de firma se incluye en la línea 45 y es un ejemplo del primer campo 312 de firma de la figura 3. La ubicación de la licencia especificada en la línea 48 es un ejemplo de la referencia al campo 320A de credencial asociado a la figura 3.

El segundo elemento de firma es similar al primer elemento de firma excepto en que el segundo valor de firma está en la línea 69 y representa un ejemplo de segundo campo 313 de firma de la figura 3, mientras que la ubicación de la licencia se especifica en la línea 72 y representa un ejemplo de la referencia al campo 320B de credencial asociado de la figura 3.

Por consiguiente, los principios de la presente invención permiten la comunicación de múltiples credenciales en un único mensaje electrónico. Además, la referencia a una credencial asociada permite verificar la integridad de mensajes electrónicos.

En el ejemplo de código anterior, hay dos credenciales diferentes incluidos en el mensaje electrónico, una licencia binaria y una credencial binaria. Estos tipos de credencial pueden estructurarse de manera abstracta en un árbol de herencia. Un árbol de herencia semántica de credencial jerárquicamente estructurado que incluye estos tipos de credenciales se ilustra como el árbol 500 en la figura 5.

El árbol 500 incluye un tipo 501 de datos de credencial abstracto como su base. La credencial abstracta se estructura de acuerdo con un esquema 501A y tiene reglas 501B de manejo. El esquema 501A describe la estructura básica del tipo de datos de credencial abstracto. Las reglas 501B de manejo describen como manejar la credencial abstracta.

Una de las ramas de primer nivel del árbol 500 es un tipo 511 de datos de licencia abstracto, que incluye un esquema 511A extendido y reglas 511B de manejo extendido. El esquema y las reglas de manejo desde los nodos primarios en el árbol 500 pueden heredarse por los nodos secundarios. En otras palabras, el esquema 511A de la licencia abstracta puede reflejar el esquema 501A de la credencial abstracta con algunas extensiones especificadas. También, las reglas 511B de manejo pueden representar adicionalmente reglas de manejo además de las reglas 501B de manejo especificadas en el tipo de datos de credencial abstracto.

Otra de las ramas de primer nivel del árbol 500 es un tipo 512 de datos de credencial binario que incluye el esquema 512A y reglas 512B de manejo. Una segunda rama de niveles del árbol incluye la licencia 521 binaria que tiene un esquema 521A y reglas 521B de manejo. El árbol 500 puede expandirse adicionalmente definiendo un esquema que se extiende sobre el esquema de un nodo primario y/o definiendo adicionalmente reglas de manejo además de aquellas proporcionadas para un nodo primario.

Cuando se determina cómo estructurar una licencia binaria, por ejemplo, el sistema informático fuente usa el esquema 521A. Si el esquema 521A representó cambios estructurales incrementales en lugar de una definición estructural completa, el sistema informático fuente puede también consultar el esquema de los tipos 511 y 501 de datos ancestrales para determinar la forma estructural final de la licencia binaria. Al recibir una licencia binaria, el sistema informático receptor puede usar el esquema 521A para determinar cómo analizar la licencia binaria, junto con las reglas 521B de manejo para determinar cómo tratar la licencia binaria en términos de cómo procesar la licencia binaria y qué autoridades conceder en respuesta a la licencia binaria. Las reglas 521B de manejo pueden representar reglas de manejo incrementales en cuyo caso las reglas 511B y 501B de manejo ancestrales pueden también consultarse para determinar el manejo apropiado. El árbol 500 puede almacenarse tanto en el sistema informático fuente como en el sistema informático receptor para asegurar el tratamiento consistente de credenciales.

REIVINDICACIONES

1. En un entorno de red que incluye una pluralidad de sistemas informáticos capaces de comunicarse usando mensajería (300) electrónica, un procedimiento para un sistema informático fuente que construye un mensaje electrónico, comprendiendo el procedimiento lo siguiente:

un acto de incluir una o más firmas electrónicas en una parte de encabezado (310) de un mensaje electrónico, las firmas electrónicas generadas por un usuario;
un acto de generar (217) una referencia que indica dónde una credencial asociada con una firma electrónica puede encontrarse; en el que la referencia indica que la credencial asociada puede encontrarse en una ubicación que es externa al mensaje electrónico;
un acto de incluir (218) la referencia en la parte de encabezado del mensaje electrónico;
un acto de designar al menos una dirección de destino en el mensaje electrónico, la dirección de destino que corresponde a uno o más dispositivos informáticos receptores; un acto de transmitir el mensaje electrónico a uno o más dispositivos informáticos receptores.

2. El procedimiento de la reivindicación 1, en el que una primera firma (312) electrónica que se deriva al menos de una primera credencial (315) de un primer tipo (319A) de credencial y una segunda firma (313) electrónica que se deriva al menos desde una segunda credencial (316) de un segundo tipo (319B) de credencial, se incluyen en la parte de encabezado del mensaje electrónico.

3. El procedimiento de acuerdo con la reivindicación 2, que comprende además lo siguiente:

un acto de transmitir el mensaje electrónico con la primera firma y la segunda firma en la parte de encabezado a uno o más dispositivos informáticos receptores.

4. El procedimiento de acuerdo con la reivindicación 2, que comprende además lo siguiente:

un acto de incluir la primera credencial en el mensaje electrónico.

5. El procedimiento de acuerdo con la reivindicación 2, que comprende además lo siguiente:

un acto de incluir la segunda credencial en el mensaje electrónico.

6. El procedimiento de acuerdo con la reivindicación 2, que comprende, además:

un acto de designar una dirección intermediaria que corresponde a un dispositivo informático intermediario.

7. El procedimiento de acuerdo con la reivindicación 2, que comprende, además

un acto de codificar la primera credencial;
un acto de incluir, en la parte de encabezado, una identificación, de un formato de codificación de la primera credencial; y
un acto de incluir, en la parte de encabezado, una identificación de un tipo del token de seguridad.

8. El procedimiento de acuerdo con la reivindicación 1, que comprende además lo siguiente:

un acto de codificar una credencial, que identifica el dispositivo informático fuente;
un acto de incluir la credencial en una parte de encabezado de un mensaje electrónico;
un acto de incluir, en la parte de encabezado, una identificación de un formato de codificación de la credencial; y
un acto de incluir, en la parte de encabezado, una identificación de un tipo de la credencial.

9. Un procedimiento de acuerdo con la reivindicación 8, en el que la credencial es una licencia.

10. Un procedimiento de acuerdo con la reivindicación 9, en el que la credencial está en un formato binario, en el que el acto de incluir, en la parte de encabezado, una identificación de un tipo de la credencial comprende un acto de incluir, en la parte de encabezado, una identificación de que la credencial tiene el formato binario.

11. Unos procedimientos de acuerdo con la reivindicación 8, en los que la credencial está en un formato binario, en los que el acto de incluir, en la parte de encabezado, una identificación de un tipo de la credencial comprende un acto de incluir, en la parte de encabezado, una identificación de que la credencial tiene el formato binario.

12. Un medio legible por ordenador que almacena instrucciones ejecutables por ordenador que, cuando se llevan a cabo por un procesador, hacen que el procesador realice el procedimiento de una de las reivindicaciones 1 a 11.

13. Un sistema informático que comprende medios adaptados para realizar el procedimiento de una de las reivindicaciones 1 a 11.

14. En un entorno de red que incluye una pluralidad de sistemas informáticos capaces de comunicarse usando mensajería electrónica, un procedimiento para uno o más sistemas informáticos receptores para verificar la identidad

de un remitente de un mensaje electrónico, comprendiendo el procedimiento lo siguiente:

un acto de recibir (220) el mensaje electrónico;
un acto de leer (222) una firma electrónica desde una parte de encabezado del mensaje electrónico, la firma electrónica generada por un usuario;
un acto de leer una referencia desde la parte de encabezado; en el que la referencia indica que la credencial asociada puede encontrarse en una ubicación que es externa al mensaje electrónico;
un acto de usar (224) la referencia para encontrar la credencial; y
un acto de determinar (225) si la credencial corresponde a la firma electrónica.

15. El procedimiento de acuerdo con la reivindicación 14, en el que el mensaje electrónico contiene una primera credencial y una segunda credencial y se recibe por al menos un primer y un segundo sistema informático receptor.

16. El procedimiento de acuerdo con la reivindicación 15, que comprende además lo siguiente:

un acto en el que el primer sistema informático receptor usa la primera credencial para identificar el sistema informático fuente; y
un acto en el que el segundo sistema informático receptor usa la segunda credencial para identificar el sistema informático fuente.

17. El procedimiento de acuerdo con la reivindicación 14, en el que el mensaje electrónico contiene una primera credencial y una segunda credencial y se recibe por al menos un primer sistema informático receptor.

18. El procedimiento de acuerdo con la reivindicación 17, que comprende además lo siguiente:

un acto en el que el primer sistema informático receptor usa tanto la primera credencial como la segunda credencial para identificar el sistema informático fuente.

19. El procedimiento de acuerdo con la reivindicación 14, en el que el mensaje electrónico contiene una primera credencial y una segunda credencial y se recibe por al menos un primer sistema informático receptor, el mensaje también cruzando a través de un sistema informático intermediario.

20. El procedimiento de acuerdo con la reivindicación 19, que comprende además lo siguiente:

un acto en el que el primer sistema informático receptor usa la primera credencial para identificar el sistema informático fuente; y
un acto en el que el sistema informático intermediario usa la segunda credencial para identificar el sistema informático fuente.

21. Un medio legible por ordenador que almacena instrucciones ejecutables por ordenador que, cuando se llevan a cabo por un procesador, hacen que el procesador realice el procedimiento de una de las reivindicaciones 16 a 20.

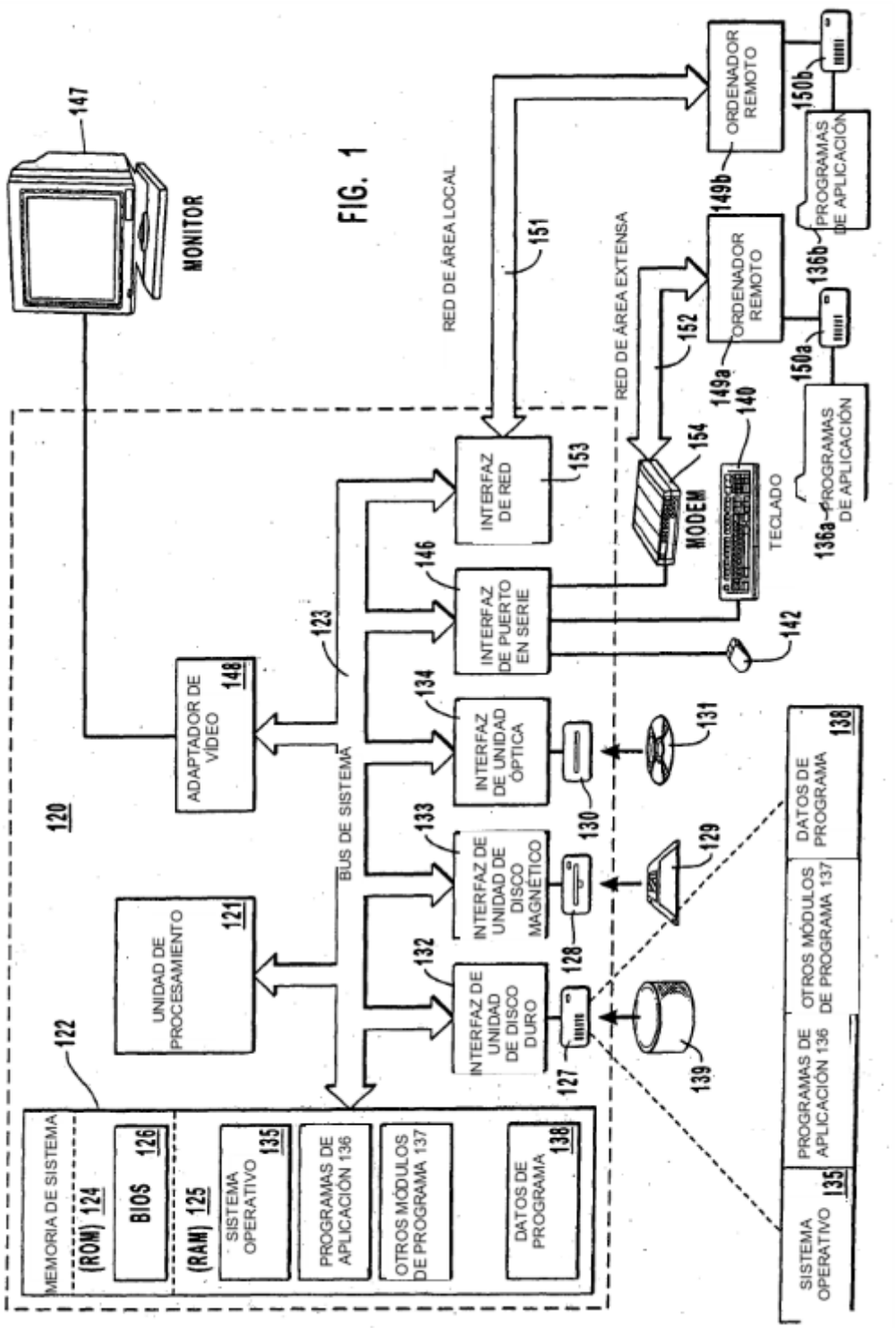
22. El medio legible por ordenador de acuerdo con la reivindicación 21, que comprende, además:

instrucciones ejecutables por ordenador para detectar el receptor de un mensaje electrónico;
instrucciones ejecutables por ordenador para leer una credencial desde el mensaje electrónico;
instrucciones ejecutables por ordenador para determinar cómo manejar la credencial y el mensaje electrónico basándose en una posición de la credencial dentro de un árbol jerárquico lógico de credenciales;
instrucciones legibles por ordenador para manejar la credencial y el mensaje electrónico como se determina.

23. El medio legible por ordenador de acuerdo con la reivindicación 21, que comprende, además:

instrucciones ejecutables por ordenador para consultar reglas de manejo de al menos una credencial ancestral en el árbol jerárquico lógico;
instrucciones ejecutables por ordenador para consultar reglas de manejo extendidas específicas a la credencial incluida en el mensaje electrónico; e
instrucciones ejecutables por ordenador para determinar reglas de manejo para la credencial incluida en el mensaje electrónico usando las reglas de manejo para la al menos una credencial ancestral, así como las reglas de manejo extendido específicas a la credencial incluida en el mensaje electrónico.

24. Un sistema informático que comprende medios adaptados para llevar a cabo el procedimiento de una de las reivindicaciones 16 a 20.


147
MONITOR
FIG. 1
RED DE ÁREA LOCAL
RED DE ÁREA EXTENSA
ORDENADOR REMOTO
150b
PROGRAMAS DE APLICACIÓN
149b
ORDENADOR REMOTO
136b
151
152
150a
149a
140
154
INTERFAZ DE RED
153
MODEM
TECLADO
136a
PROGRAMAS DE APLICACIÓN
146
INTERFAZ DE PUERTO EN SERIE
142
123
ADAPTADOR DE VÍDEO
148
134
INTERFAZ DE UNIDAD ÓPTICA
131
120
BUS DE SISTEMA
133
INTERFAZ DE UNIDAD DE DISCO MAGNÉTICO
130
129
UNIDAD DE PROCESAMIENTO
121
132
INTERFAZ DE UNIDAD DE DISCO DURO
128
DATOS DE PROGRAMA
138
OTROS MÓDULOS DE PROGRAMA 137
PROGRAMAS DE APLICACIÓN 136
SISTEMA OPERATIVO
135
127
139
122
MEMORIA DE SISTEMA
(ROM) 124
BIOS
126
(RAM) 125
SISTEMA OPERATIVO
135
PROGRAMAS DE APLICACIÓN 136
OTROS MÓDULOS DE PROGRAMA 137
DATOS DE PROGRAMA
138

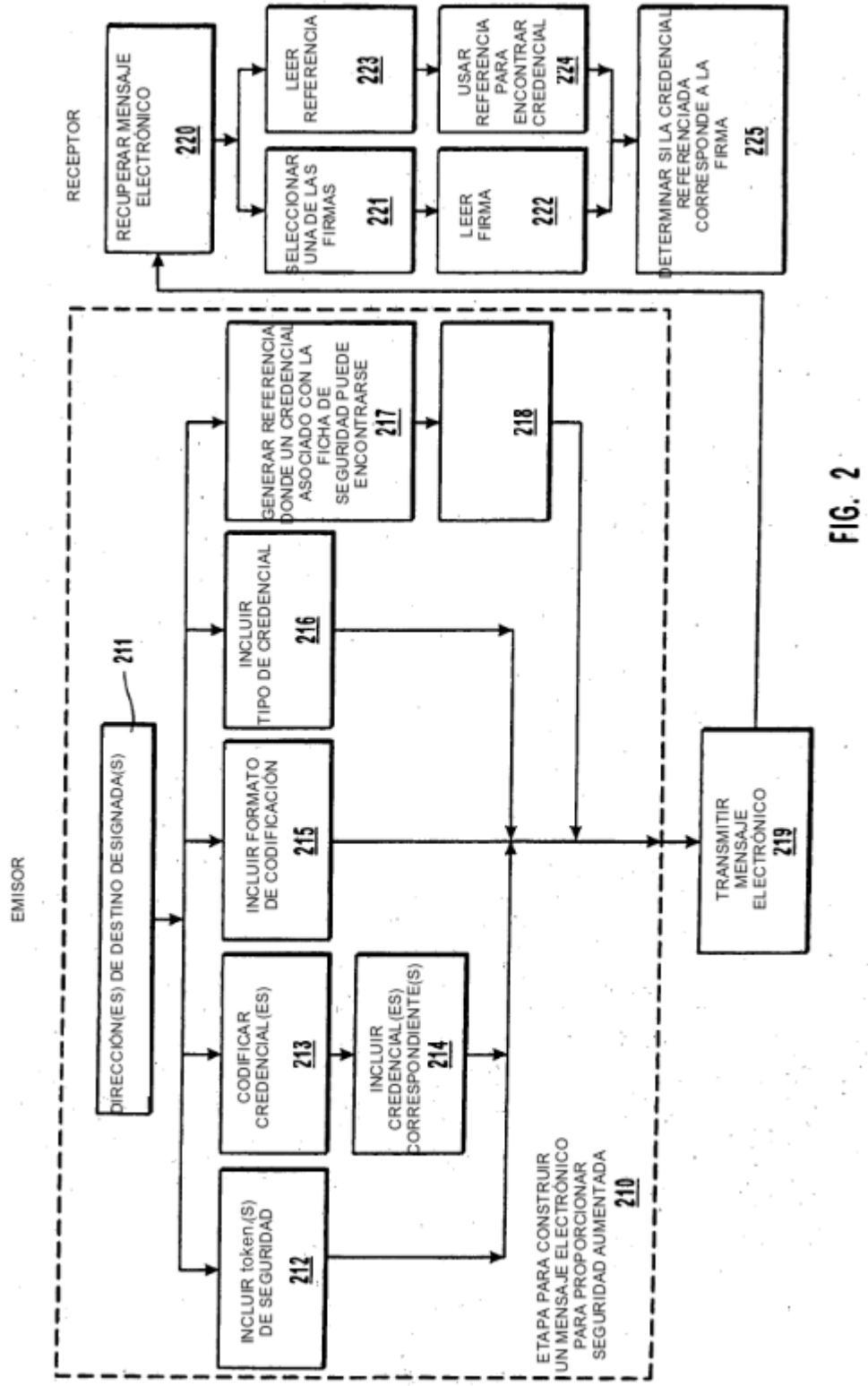

EMISOR
RECEPTOR
DIRECCIÓN(ES) DE DESTINO DESIGNADA(S)
211
INCLUIR token(S) DE SEGURIDAD
212
CODIFICAR CREDENCIAL(ES)
213
INCLUIR CREDENCIAL(ES) CORRESPONDIENTE(S)
214
INCLUIR FORMATO DE CODIFICACIÓN
215
INCLUIR TIPO DE CREDENCIAL
216
GENERAR REFERENCIA DONDE UN CREDENCIAL ASOCIADO CON LA FICHA DE SEGURIDAD PUEDE ENCONTRARSE
217
218
ETAPA PARA CONSTRUIR UN MENSAJE ELECTRÓNICO PARA PROPORCIONAR SEGURIDAD AUMENTADA
210
TRANSMITIR MENSAJE ELECTRÓNICO
219
RECUPERAR MENSAJE ELECTRÓNICO
220
SELECCIONAR UNA DE LAS FIRMAS
221
LEER FIRMA
222
LEER REFERENCIA
223
USAR REFERENCIA PARA ENCONTRAR CREDENCIAL
224
DETERMINAR SI LA CREDENCIAL REFERENCIADA CORRESPONDE A LA FIRMA
225

FIG. 2

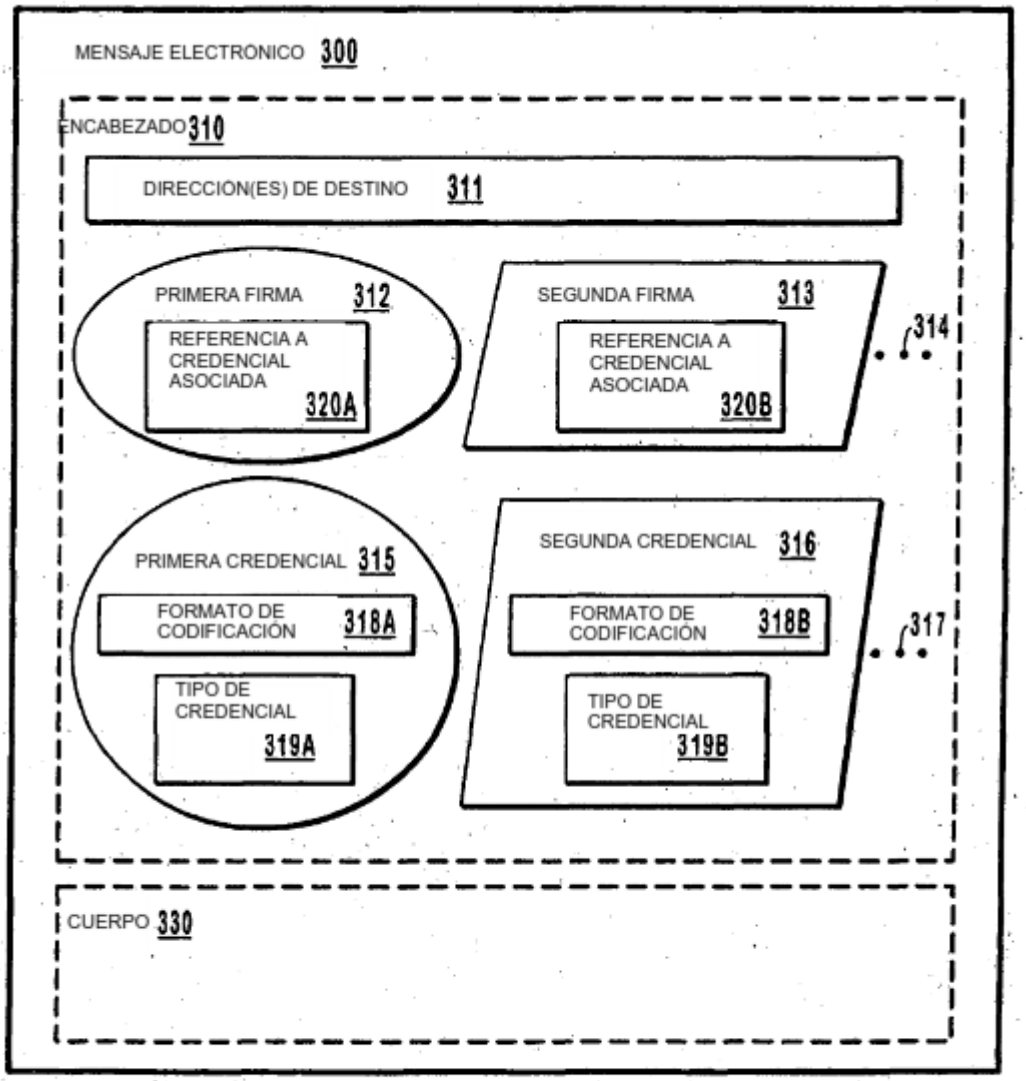

MENSAJE ELECTRONICO 300
ENCABEZADO 310
DIRECCION(ES) DE DESTINO 311
PRIMERA FIRMA 312
REFERENCIA A CREDENCIAL ASOCIADA 320A
SEGUNDA FIRMA 313
REFERENCIA A CREDENCIAL ASOCIADA 320B
314
PRIMERA CREDENCIAL 315
FORMATO DE CODIFICACIÓN 318A
TIPO DE CREDENCIAL 319A
SEGUNDA CREDENCIAL 316
FORMATO DE CODIFICACIÓN 318B
TIPO DE CREDENCIAL 319B
317
CUERPO 330

FIG. 3

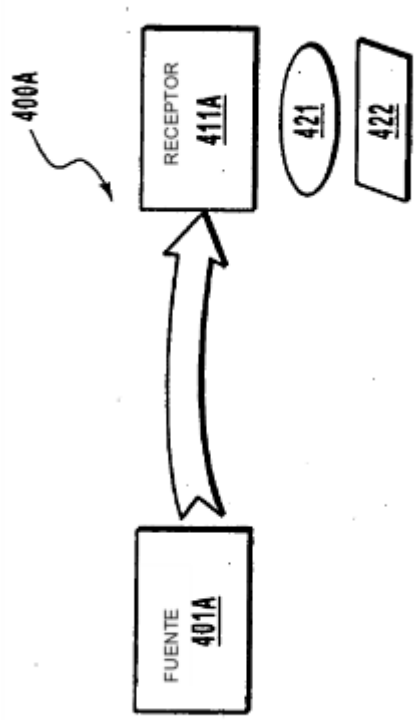

400A
RECEPTOR
411A
421
422
FUENTE
401A

FIG. 4A

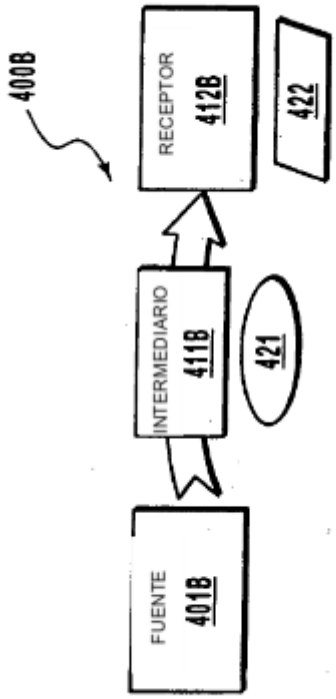

400B
RECEPTOR
412B
422
INTERMEDIARIO
411B
421
FUENTE
401B

FIG. 4B

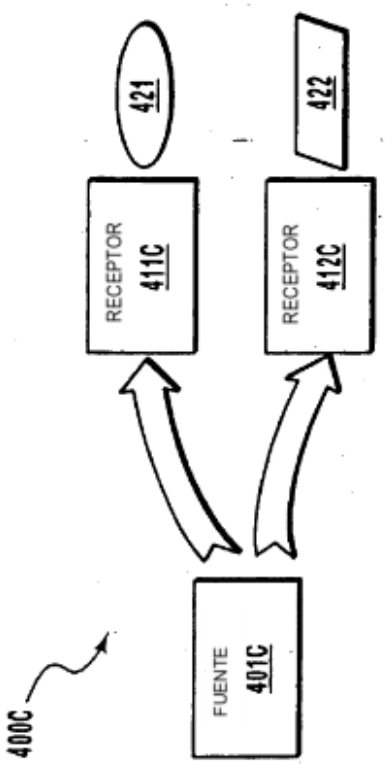

400C
FUENTE
401C
RECEPTOR
411C
RECEPTOR
412C
421
422

FIG. 4C

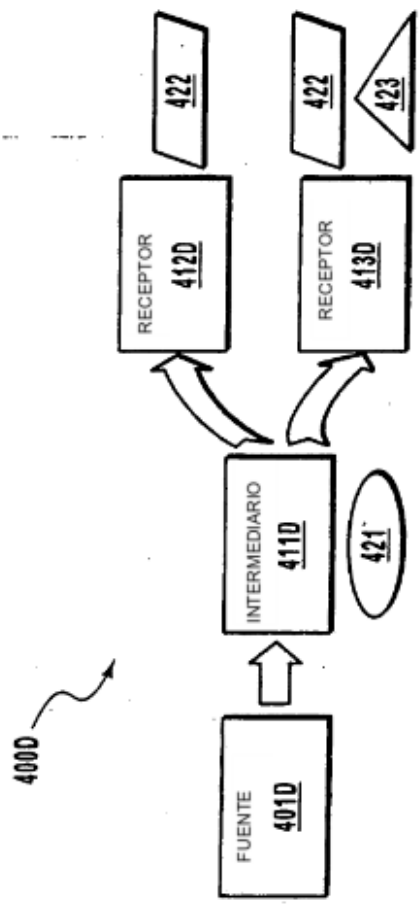

400D
FUENTE
401D
INTERMEDIARIO
411D
RECEPTOR
412D
RECEPTOR
413D
421
422
422
423

FIG. 4D

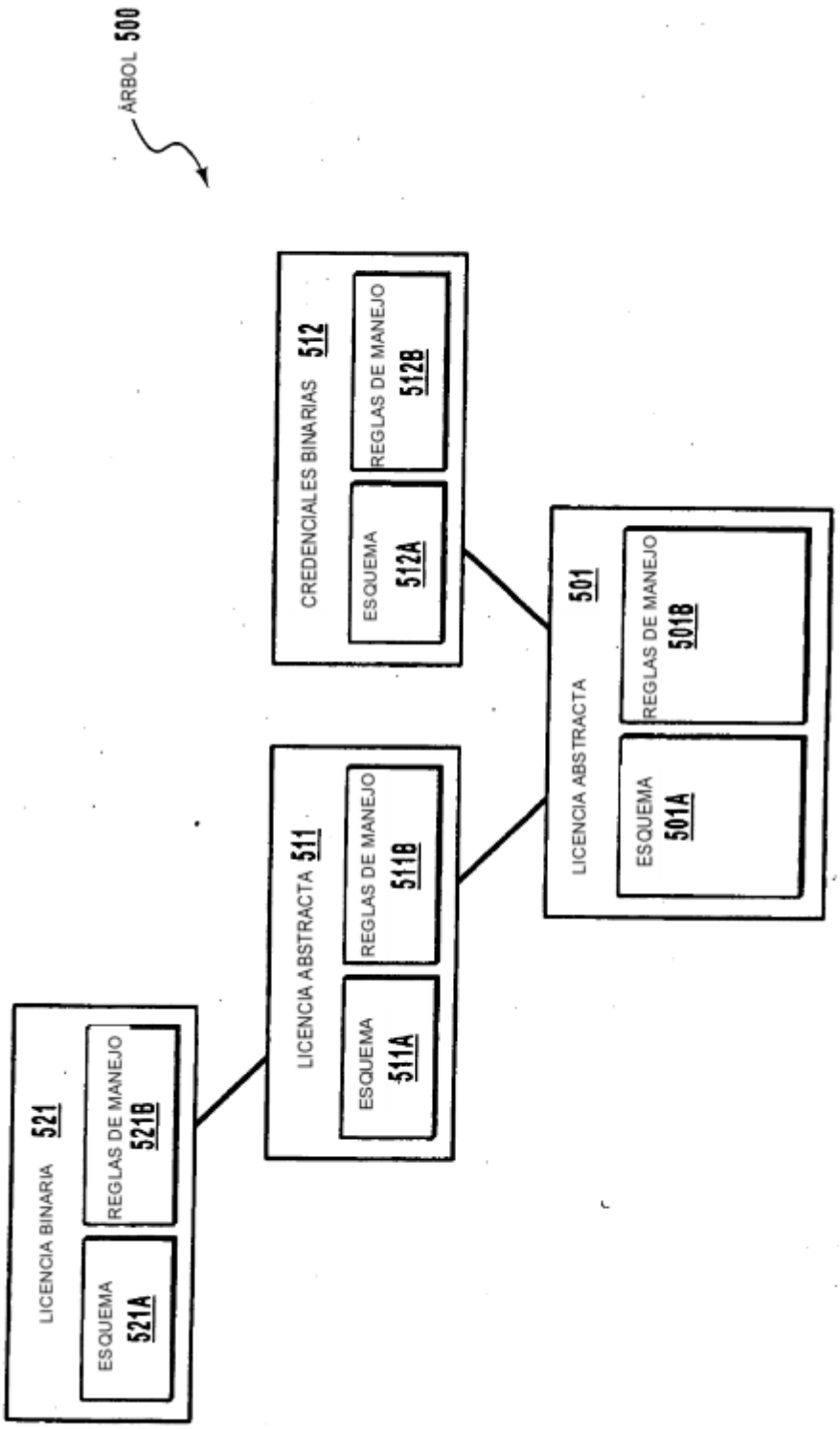

ÁRBOL 500
LICENCIA BINARIA 521
ESQUEMA 521A
REGLAS DE MANEJO 521B
LICENCIA ABSTRACTA 511
ESQUEMA 511A
REGLAS DE MANEJO 511B
CREDENCIALES BINARIAS 512
ESQUEMA 512A
REGLAS DE MANEJO 512B
LICENCIA ABSTRACTA 501
ESQUEMA 501A
REGLAS DE MANEJO 501B

FIG. 5