(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 662 071**

(51) Int. CI.:

***H04L 9/32*** (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **05.10.2007 PCT/US2007/080525**

(87) Fecha y número de publicación internacional: **17.04.2008 WO08045773**

(96) Fecha de presentación y número de la solicitud europea: **05.10.2007 E 07853787 (5)**

(97) Fecha y número de publicación de la concesión europea: **24.01.2018 EP 2082525**

(54) Título: **Procedimiento y aparato para la autenticación mutua**

(30) Prioridad:

**10.10.2006 US 850882 P**
**03.10.2007 US 866946**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
**05.04.2018**

(73) Titular/es:

**QUALCOMM INCORPORATED (100.0%)**
**ATTN: INTERNATIONAL IP ADMINISTRATION,**
**5775 MOREHOUSE DRIVE**
**SAN DIEGO, CA 92121, US**

(72) Inventor/es:

**PEREZ, ARAM y**
**DONDETI, LAKSHMINATH REDDY**

(74) Agente/Representante:

**FORTEA LAGUNA, Juan José**

## DESCRIPCIÓN

Procedimiento y aparato para la autenticación mutua

**[0001]** La presente solicitud de patente reivindica prioridad a: Solicitud Provisional No. 60/850.882, titulada "PROCEDIMIENTO Y APARATO PARA LA AUTENTICACIÓN MUTUA" presentada el 10 de octubre de 2006. Esta solicitud provisional se asigna al cesionario de este documento.

### ANTECEDENTES

Campo

**[0002]** La presente invención se refiere, en general, a las comunicaciones inalámbricas y, más específicamente, a la autenticación mutua.

### Antecedentes

**[0003]** Un abonado móvil puede querer acceder a contenido protegido por un sistema que requeriría la autenticación con otra entidad o agente. Un protocolo de autenticación popular es el protocolo de intercambio de claves de Internet (IKE), descrito en RFC 4306. Sin embargo, el protocolo IKE supone que las entidades del proceso de autenticación tienen suficiente potencia de procesamiento o cálculo de modo que la velocidad de la autenticación no es una preocupación.

**[0004]** Por lo tanto, existe una necesidad en la técnica de una técnica de autenticación mutua eficaz con un dispositivo que tenga una potencia de procesamiento limitada.

**[0005]** Menezes y otros, "Manual of Criptografía aplicada", CRC Press, EUA, 1997, ISBN: o-8493-8523-7, páginas 403-405,506, divulga un protocolo de Needham-Schroeder PK modificado para la identificación que proporciona transporte de claves para claves distintas k1, k2 de A a B y de B a A, respectivamente, así como autenticación mutua.

**[0006]** US 6769060 B1 divulga un procedimiento para la autenticación bilateral de la identidad sobre un canal de comunicación que proporciona un procedimiento seguro para la autenticación de la identidad de las partes que se comunican y el establecimiento de una clave secreta. Cada parte calcula un desafío de autenticación basado en un valor intercambiado utilizado en un procedimiento de generación de clave. El desafío de autenticación se cifra a la clave pública de la otra parte. Después de recibir un canal de autenticación cifrado de la otra parte, cada parte descifra el desafío de autenticación y genera una respuesta de autenticación basada en el desafío de autenticación. La respuesta de autenticación incluye bits que la parte desafiante no puede predecir con antelación para evitar el uso fraudulento de la respuesta de autenticación por la parte desafiante o alguna otra tercera parte. Después de recibir una respuesta de autenticación de la otra parte, cada parte verifica que se recibió la respuesta de autenticación esperada.

**[0007]** El documento US 7024690 B1 divulga un proceso para la autenticación mutua de usuarios y redes a través de un canal de comunicación inalámbrico no seguro. La información confidencial (por ejemplo, contraseñas) no se comunica a través del canal no seguro. Más bien, las representaciones hash de identificadores de usuario, contraseñas, etc. y números generados aleatoriamente se comunican entre el cliente y la red durante el proceso de inicio de sesión. Las representaciones se pueden cifrar con una función hash unidireccional de manera tal que no sea computacionalmente factible que las descifre una persona no autorizada. La representación se puede generar basándose en el identificador de usuario, la contraseña y/o la dirección MAC de una tarjeta LAN inalámbrica.

**[0008]** El documento WO 2005/091551 A1 divulga un procedimiento para realizar la autenticación entre un dispositivo y un almacenamiento portátil, que es realizada por el dispositivo, que incluye transmitir una primera clave al almacenamiento portátil, recibir una tercera clave y un primer número aleatorio cifrado obtenido cifrando un primer número aleatorio utilizando la primera clave del almacenamiento portátil y descifrando el primer número aleatorio cifrado utilizando una segunda clave relacionada con la primera clave, generar un segundo número aleatorio cifrado mediante el cifrado de un segundo número aleatorio utilizando la tercera clave y transmitir el segundo número aleatorio cifrado al almacenamiento portátil, y generar una clave de sesión utilizando el primer número aleatorio y el segundo número aleatorio. La técnica garantiza una autenticación segura entre el dispositivo y el almacenamiento portátil para la DRM.

### SUMARIO

**[0009]** La invención se define en las reivindicaciones independientes. Un aspecto de la presente invención puede residir en un procedimiento para la autenticación mutua entre una primera entidad y una segunda entidad. En el procedimiento, la primera entidad inicia la autenticación mutua enviando un mensaje a la segunda entidad. La segunda entidad verifica una primera clave pública asociada con la primera entidad, genera un primer número

aleatorio, cifra el primer número aleatorio utilizando la primera clave pública y envía el primer número aleatorio cifrado en un mensaje a la primera entidad. La primera entidad verifica una segunda clave pública asociada con la segunda entidad, descifra el primer número aleatorio cifrado utilizando una primera clave privada correspondiente a la primera clave pública, genera un segundo número aleatorio, genera una primera hash basada en al menos el primer número aleatorio, cifra el segundo número aleatorio y la primera hash utilizando la segunda clave pública, y envía el segundo número aleatorio cifrado y la primera hash en un mensaje a la segunda entidad. La segunda entidad descifra el segundo número aleatorio cifrado y la primera hash utilizando una segunda clave privada correspondiente a la segunda clave pública, verifica la primera hash para autenticar la primera entidad, genera una segunda hash basada en al menos el segundo número aleatorio y envía la segunda hash a la primera entidad. La primera entidad verifica la segunda hash para autenticar la segunda entidad.

**[0010]** En aspectos más detallados de la invención, la primera entidad y la segunda entidad obtiene cada una una clave de cifrado de sesión y la clave de código de autenticación de mensaje (MAC) utilizando el primer número aleatorio y el segundo número aleatorio basándose en una función de derivación de claves, para su uso en comunicaciones entre la primera entidad y la segunda entidad.

**[0011]** Además, el mensaje que inicia la autenticación mutua puede incluir una hash de al menos una clave raíz de confianza y una cadena de certificados correspondiente para la primera entidad. La cadena de certificados para la primera entidad puede incluir la clave pública asociada con la primera entidad. Además, el mensaje de la segunda entidad a la primera entidad que tiene el primer número aleatorio cifrado puede incluir adicionalmente una cadena de certificados para la segunda entidad. La cadena de certificados para la segunda entidad puede incluir la clave pública asociada con la segunda entidad.

**[0012]** En otros aspectos más detallados de la invención, la primera entidad puede ser un agente de derechos digitales de una estación móvil, y la segunda entidad puede ser un dispositivo seguro de medios extraíbles. La segunda entidad puede tener una potencia de procesamiento limitada. Además, la primera hash puede estar basada adicionalmente en el segundo número aleatorio, de manera que la primera hash se genera en base al primer número aleatorio concatenado con el segundo número aleatorio. La segunda hash puede basarse, además, en el primer número aleatorio, o basarse, además, en la primera hash, de modo que la segunda hash puede basarse en el segundo número aleatorio concatenado con la primera hash.

**[0013]** Otro aspecto de la invención puede residir en un aparato para la autenticación mutua que incluye medios para iniciar la autenticación mutua, medios para la verificación de una primera clave pública, la generación de un primer número aleatorio, y el cifrado del primer número aleatorio utilizando la primera clave pública, medios para verificar una segunda clave pública, descifrar el primer número aleatorio cifrado utilizando una primera clave privada correspondiente a la primera clave pública, generar un segundo número aleatorio, generar una primera hash basada en al menos el primer número aleatorio y cifrar el segundo número aleatorio y la primera hash utilizando la segunda clave pública, medios para descifrar el segundo número aleatorio cifrado y la primera hash utilizando una segunda clave privada correspondiente a la segunda clave pública, verificar la primera hash para la autenticación y generar una segunda hash basada en al menos el segundo número aleatorio y medios para verificar la segunda hash para la autenticación.

**[0014]** Otro aspecto de la invención puede residir en una estación móvil que tiene autenticación mutua con un dispositivo seguro de medios extraíbles, y que incluye un agente de derechos digitales. El agente de derechos digitales inicia la autenticación mutua enviando un mensaje a un dispositivo seguro de medios extraíbles, en la que el dispositivo seguro de medios extraíbles verifica una primera clave pública asociada con el agente de derechos digitales, genera un primer número aleatorio y cifra el primer número aleatorio utilizando la primera clave pública, y envía el primer número aleatorio cifrado en un mensaje al agente de derechos digitales. El agente de derechos digitales verifica una segunda clave pública asociada con el dispositivo seguro de medios extraíbles, descifra el primer número aleatorio cifrado utilizando una primera clave privada correspondiente a la primera clave pública, genera un segundo número aleatorio, genera una primera hash basada en al menos el primer número aleatorio, cifra el segundo número aleatorio y la primera hash utilizando la segunda clave pública, y envía el segundo número aleatorio cifrado y la primera hash en un mensaje al dispositivo seguro de medios extraíbles, en el que el dispositivo seguro de medios extraíbles descifra el segundo número aleatorio cifrado y la primera hash utilizando una segunda clave privada correspondiente a la segunda clave pública, verifica la primera hash para autenticar al agente de derechos digitales, genera una segunda hash basada en al menos el segundo número aleatorio y envía la segunda hash al agente de derechos digitales. El agente de derechos digitales verifica la segunda hash para autenticar el dispositivo seguro de medios extraíbles.

**[0015]** Otro aspecto más de la invención puede residir en un producto de programa informático que comprende un medio legible por ordenador que comprende código para hacer que un ordenador de una estación que tiene un agente de derechos digitales inicie la autenticación mutua mediante el envío de un mensaje a un dispositivo seguro de medios extraíbles, en el que el dispositivo seguro de medios extraíbles verifica una primera clave pública asociada con el agente de derechos digitales, genera un primer número aleatorio, cifra el primer número aleatorio utilizando la primera clave pública y envía el primer número aleatorio cifrado en un mensaje al agente de derechos digitales, código para hacer que un ordenador haga que el agente de derechos digitales verifique una segunda clave

pública asociada con el dispositivo seguro de medios extraíbles, descifre el primer número aleatorio cifrado utilizando una primera clave privada correspondiente a la primera clave pública, genere un segundo número aleatorio, genere una primera hash basada en al menos el primer número aleatorio, cifre el segundo número aleatorio y la primera hash utilizando la segunda clave pública, y envíe el segundo número aleatorio cifrado y la primera hash en un mensaje al dispositivo seguro de medios extraíbles, en el que el dispositivo seguro de medios extraíbles descifra el segundo número aleatorio cifrado y la primera hash utilizando una segunda clave privada correspondiente a la segunda clave pública, verifica la primera hash para autenticar al agente de derechos digitales, genera una segunda hash basada en al menos el segundo número aleatorio y envía la segunda hash al agente de derechos digitales y código para hacer que un ordenador haga que el agente de derechos digitales verifique una segunda hash para autenticar el dispositivo seguro de medios extraíbles.

**[0016]** Otro aspecto de la invención puede residir en un producto de programa informático, que comprende un medio legible por ordenador que comprende código para hacer que un ordenador haga que un dispositivo seguro de medios extraíble verifique una primera clave pública asociada con un agente de derechos digitales, genere un primer número aleatorio, cifre el primer número aleatorio utilizando la primera clave pública, y envíe el primer número aleatorio cifrado en un mensaje al agente de derechos digitales, en el que el agente de derechos digitales verifica una segunda clave pública asociada con el dispositivo seguro de medios extraíbles, descifra el primer número aleatorio cifrado utilizando una primera clave privada correspondiente a la primera clave pública, genera un segundo número aleatorio, genera una primera hash basada en al menos el primer número aleatorio, cifra el segundo número aleatorio y la primera hash utilizando la segunda clave pública, y envía el segundo número aleatorio cifrado y la primera hash en un mensaje al dispositivo seguro de medios extraíbles, y código para hacer que un ordenador provoque que un dispositivo seguro de medios extraíbles descifre el segundo número aleatorio cifrado y la primera hash utilizando una segunda clave privada correspondiente a la segunda clave pública, verifique la primera hash para autenticar el agente de derechos digitales, genere una segunda hash basada en al menos el segundo número aleatorio y envíe la segunda hash al agente de derechos digitales, en el que el agente de derechos digitales verifica la segunda hash para autenticar el dispositivo seguro de medios extraíbles.

## BREVE DESCRIPCIÓN DE LOS DIBUJOS

**[0017]**

La Figura 1 es un ejemplo de un sistema de comunicación inalámbrica;

La Figura 2 es un diagrama de bloques de una estación móvil y un dispositivo seguro de medios extraíbles que tiene autenticación mutua;

La Figura 3 es un diagrama de flujo de un procedimiento para la autenticación mutua entre una estación móvil y un dispositivo seguro de medios extraíbles.

## DESCRIPCIÓN DETALLADA

**[0018]** El término "a modo de ejemplo" se utiliza en el presente documento para significar "que sirve de ejemplo, caso particular o ilustración". No debe considerarse necesariamente que cualquier modo de realización descrito en el presente documento como "a modo de ejemplo" sea preferido o ventajoso con respecto a otros modos de realización.

**[0019]** Una estación remota, también conocida como una estación móvil (MS), un terminal de acceso (AT), equipo de usuario o unidad de abonado, puede ser móvil o estacionaria, y puede comunicarse con una o más estaciones base, también conocidas como estaciones transceptoras base (BTS) o nodos B. Una estación remota transmite y recibe paquetes de datos a través de una o más estaciones base a un controlador de estación base, también conocido como controladores de red de radio (RNC). Las estaciones base y los controladores de estación base son partes de una red, llamada red de acceso. Una red de acceso transporta paquetes de datos entre múltiples estaciones remotas. La red de acceso puede conectarse, además, a redes adicionales externas a la red de acceso, tal como una intranet corporativa o a Internet, y puede transportar paquetes de datos entre cada estación remota y tales redes externas. Una estación remota que ha establecido una conexión activa de canal de tráfico con una o más estaciones base se denomina estación remota activa y se dice que está en un estado de tráfico. Se dice que una estación remota que está en el proceso de establecer una conexión activa de canal de tráfico con una o más estaciones base está en un estado de establecimiento de conexión. Una estación remota puede ser cualquier dispositivo de datos que se comunique a través de un canal inalámbrico. Una estación remota puede ser, además, cualquiera de una pluralidad de tipos de dispositivos incluyendo, pero de forma no limitativa, una tarjeta de PC, una memoria flash compacta, un módem externo o interno, o un teléfono inalámbrico. El enlace de comunicación a través del cual la estación remota envía señales a la estación base se denomina enlace ascendente, también conocido como enlace inverso. El enlace de comunicación a través del cual una estación base envía señales a una estación remota se denomina enlace descendente, también conocido como enlace directo.

**[0020]** Con referencia a la Figura 2, un sistema de comunicación inalámbrica 100 incluye una o más estaciones

inalámbricas móviles (MS) 102, una o más estaciones base (BS) 104, uno o más controladores de estación base (BSC) 106, y una red central 108. La red central puede estar conectada a Internet 110 y a una Red telefónica pública conmutada (PSTN) 112 a través de redes de retorno adecuadas. Una estación móvil inalámbrica típica puede incluir un teléfono portátil o un ordenador portátil. El sistema de comunicación inalámbrica 100 puede emplear cualquiera de varias técnicas de acceso múltiple tales como acceso múltiple por división de código (CDMA), acceso múltiple por división de tiempo (TDMA), acceso múltiple por división de frecuencia (FDMA), acceso múltiple por división de espacio (SDMA), acceso múltiple por división de polarización (PDMA), u otras técnicas de modulación conocidas en la técnica.

**[0021]** Muchos dispositivos de bajo coste con potencia de cálculo limitada se están introduciendo en el mercado, tales como tarjetas inteligentes y memorias flash (en muchos factores de forma diferentes). Tales dispositivos pueden requerir autenticación. Por ejemplo, existe el deseo de que estos dispositivos tengan derechos de uso con los sistemas de Gestión de Derechos Digitales (DRM). Antes de intercambiar derechos con estos dispositivos, debe haber una autenticación mutua de ambas entidades involucradas en el intercambio para limitar el intercambio a las entidades autorizadas. Estos modos de realización proporcionan un procedimiento eficiente para lograr la autenticación mutua, y también proporcionan un intercambio confirmado de un secreto que se puede utilizar en comunicaciones adicionales entre las entidades involucradas. La eficiencia es tanto en términos de potencia de cálculo como de velocidad.

**[0022]** Como es evidente para un experto en la técnica, los esquemas de autenticación mutua se pueden utilizar siempre que se requiera la autenticación mutua entre dos entidades. Los esquemas de autenticación mutua no están limitados a las aplicaciones específicas (como gestión de derechos digitales), sistemas y dispositivos utilizados aquí para describir los modos de realización.

**[0023]** Un modo de realización de la invención realiza una autenticación mutua con un intercambio de claves confirmado mediante el intercambio de 4 mensajes. Requiere 2 verificaciones de firma de clave pública (+ 1 por cada certificado intermedio), 2 cifrados de clave pública, 2 descifrados de clave pública, 2 generaciones de hash y 2 verificaciones de hash. El número específico de intercambios de mensajes, verificaciones de clave pública, descifrados de clave pública, generaciones de hash y verificaciones de hash se puede dividir o modificar para lograr las cantidades requeridas de seguridad y eficiencia.

**[0024]** La eficacia del protocolo se ve reforzada al minimizar el número de operaciones criptográficas de clave pública y utilizar las funciones hash para proporcionar una prueba de posesión del material de la clave intercambiada.

**[0025]** Una autenticación mutua eficiente y un protocolo de intercambio de claves confirmado se describe para su uso con dispositivos con límite de cálculo. La eficiencia se logra al minimizar el número de operaciones de clave pública y el uso de hashes criptográficas para proporcionar una prueba de posesión.

**[0026]** El protocolo se ilustra con respecto a las figuras 2 y 3 que muestran un procedimiento 300 (Figura 3) para la autenticación mutua. Los siguientes pasos corresponden a las flechas numeradas de la Figura 3.

**[0027]** En el procedimiento 300, la Entidad A, por ejemplo, un agente DRM 202 de la MS 102, envía el mensaje HelloA (etapa 302) a la entidad B, por ejemplo, un dispositivo seguro de medios extraíbles (SRM) 204 que tiene un agente SRM 206. El agente SRM administra el acceso al almacenamiento seguro 208 en el dispositivo SRM. (Un sistema operativo 210 de la MS puede acceder directamente al almacenamiento general 212 del dispositivo SRM). HelloA consiste en las hash de las claves raíz de confianza (o las propias claves raíz) y las cadenas de certificados correspondientes. Al recibir este mensaje, la entidad B encuentra una clave raíz en la que confía del mensaje y encuentra una cadena de certificados bajo la clave raíz seleccionada. Verifica la cadena de certificados de la entidad A bajo la clave raíz seleccionada.

**[0028]** La entidad B genera un número aleatorio RanB (etapa 304).

**[0029]** La entidad B envía el mensaje HelloB a la entidad A (etapa 306). HelloB consiste en la cadena de certificados de B bajo la clave raíz seleccionada y junto con RanB cifrada con la clave pública de la entidad A de la cadena de certificados seleccionada después de la etapa 302. Al recibir este mensaje, la entidad A verifica la cadena de certificados de la entidad B. Si es válida, descifra RanB con su clave privada (correspondiente a la clave raíz seleccionada).

**[0030]** Se debe tener en cuenta que una vez se ha producido la selección de la clave raíz y el intercambio de la cadena de certificados, la entidad A y la entidad B tendrán cada uno la cadena de certificados del otro. Por lo tanto, puede no ser necesario enviar estos parámetros entre la entidad A y la entidad B en futuros mensajes HelloA y HelloB para una futura autenticación mutua. En ese caso, el intercambio de la cadena de certificados en las etapas 302 y 306 puede ser opcional.

**[0031]** La entidad A genera RanA (etapa 308).

**[0032]** La entidad A envía el mensaje ConfirmClaveA a la entidad B (etapa 310). ConfirmClaveA consiste en RanA concatenado con la hash de RanB concatenado con RanA (H[RanA | RanB]) y todo esto cifrado con la clave pública de B. Al recibir este mensaje, la entidad B lo descifra. Utilizando el RanA descifrado, verifica la hash de RanB concatenada con RanA. Nota: en esta etapa, la entidad B ha autenticado la entidad A y se garantiza que la entidad A conoce RanB.

**[0033]** La entidad B envía el mensaje ConfirmClaveB a la entidad A (etapa 312). ConfirmClaveB consiste en la hash de la parte descifrada del mensaje ConfirmClaveA. Al recibir este mensaje, la entidad A verifica la hash. Nota: en esta etapa, la entidad A ha autenticado la entidad B y se garantiza que la entidad B conoce RanA.

**[0034]** En este punto, ambas entidades se han autenticado mutuamente y han confirmado que cada uno de ellos comparten los mismos RanA y RanB. RanA y RanB ahora se pueden utilizar para derivar una clave de cifrado de sesión (SK) y una clave MAC (MK) basándose en una Función de derivación de claves (KDF) para su utilización con otras comunicaciones entre las partes (etapa 314).

**[0035]** Los detalles del mensaje se dan a continuación. El mensaje HelloA se envía para iniciar la autenticación mutua con el protocolo de confirmación de clave. El Hello A tiene un parámetro "versión" y un parámetro "raízYCadenas[]". El parámetro versión puede ser un valor de 8 bits que contiene la versión de protocolo de este mensaje. Está correlacionado con los 5 MSB para la versión mayor y los 3 LSB para la versión menor. El parámetro raízYCadenas[] puede ser una matriz de las hashes raíz y las cadenas de certificados para la entidad A bajo todos los modelos de confianza admitidos por A. La estructura para el parámetro RaízHashYCadenaCert es un parámetro raízHash, que es la hash SHA-1 de la clave pública raíz del modelo de confianza, y un parámetro cadenaCert, la cadena de certificados de la entidad bajo la clave pública raíz. El certificado de la entidad viene primero seguido de cualquier certificado CA (en orden de firma) hasta, pero sin incluir, el certificado raíz.

**[0036]** El mensaje HelloB continúa la autenticación mutua con el protocolo de confirmación de clave por la entidad B. En la siguiente tabla se describen los parámetros. El HelloB tiene los parámetros: "versión", "estado", "cadenaCert" y "cifRanB". El parámetro versión puede ser un valor de 8 bits que contiene la versión del protocolo de este mensaje. Está correlacionado con los 5 MSB para la versión mayor y los 3 LSB para la versión menor. El parámetro de estado puede ser un valor de 8 bits que contiene el estado de la entidad B que procesa el mensaje HelloA. Los valores para el parámetro de estado pueden ser 0 para el éxito -no se encontraron errores con el mensaje anterior, y 1 para claveRaíz-noCompartida -la entidad B no encontró una clave raíz que comparta con la entidad A. Los valores 2-255 pueden reservarse para un uso futuro. El parámetro cadenaCert es la cadena de certificados de la entidad B bajo una clave raíz seleccionada del mensaje HelloA. Si el valor del parámetro de estado no es exitoso, el parámetro cadenaCert no está presente. El parámetro cifRanB es un ranB cifrado RSA-OAEP, que utiliza la clave pública de la entidad A (de la cadena de certificados seleccionada). ranB puede ser un número aleatorio de 20 bytes generado por la entidad B. Si el valor del estado no es exitoso, el parámetro cifRanB no está presente.

**[0037]** El mensaje ConfirmClaveA continúa la autenticación mutua con el protocolo de confirmación de claves por la entidad A. El mensaje ConfirmClaveA tiene un parámetro de "versión" y un parámetro de "cifRanB". El parámetro versión puede ser un valor de 8 bits que contiene la versión de protocolo de este mensaje. Se puede correlacionar con los 5 MSB para la versión mayor y los 3 LSB para la versión menor. El parámetro cifRanB puede ser una estructura DatosConfirmClave cifrada RSA-OAEP que tiene un parámetro "ranA" y un parámetro "hashBA". El parámetro ranA puede ser un número aleatorio de 20 bytes generado por la entidad A, y el parámetro hash BA puede ser el algoritmo hash SHA-1 de ranB concatenado con ranA.

**[0038]** El mensaje ConfirmClaveB finaliza la autenticación mutua con el protocolo de confirmación de clave por parte de la entidad B. El mensaje ConfirmClaveB tiene un parámetro de "versión", un parámetro de estado, y un parámetro "hashConfirmClave". El parámetro versión puede ser un valor de 8 bits que contiene la versión de protocolo de este mensaje. Se puede correlacionar con los 5 MSB para la versión mayor y los 3 LSB para la versión menor. El parámetro de estado puede ser un valor de 8 bits que contiene el estado de la entidad B que procesa el mensaje. El parámetro hashConfirmClave puede ser el hash SHA-1 de la estructura DatosConfirmClave que fue descifrada por la entidad B. Si el valor del parámetro de estado no es exitoso, este parámetro no está presente.

**[0039]** Otro aspecto de la invención puede residir en una estación móvil 102 que incluye un procesador de control 216 y el sistema operativo 210 para hacer que el agente DRM 202 implemente el procedimiento 300. Todavía otro aspecto de la invención puede residir en un producto de programa informático que comprende un medio legible por ordenador (tal como un dispositivo de memoria 218) que comprende un código para hacer que un ordenador haga que el agente DRM realice las etapas del procedimiento 300.

**[0040]** Los expertos en la técnica entenderán que la información y las señales pueden representarse utilizando cualquiera de entre varias tecnologías y técnicas diferentes. Por ejemplo, los datos, las instrucciones, los comandos, la información, las señales, los bits, los símbolos y los chips que puedan haber sido mencionados a lo largo de la descripción anterior pueden representarse mediante voltajes, corrientes, ondas electromagnéticas, campos o partículas magnéticos, campos o partículas ópticos, o cualquier combinación de los mismos.

**[0041]** Los expertos en la técnica apreciarán, además, que los diversos bloques lógicos, módulos, circuitos y etapas de algoritmo ilustrativos descritos en relación con los modos de realización divulgados en el presente documento pueden implementarse como hardware electrónico, software informático o combinaciones de ambos. Para ilustrar claramente esta intercambiabilidad de hardware y software, se han descrito anteriormente, en general, diversos componentes, bloques, módulos, circuitos y etapas ilustrativos en lo que respecta a su funcionalidad. Que dicha funcionalidad se implemente como hardware o software depende de la aplicación particular y de las restricciones de diseño impuestas al sistema global. Los expertos en la materia pueden implementar la funcionalidad descrita de formas distintas para cada aplicación particular, pero no debe interpretarse que tales decisiones de implementación suponen una desviación del alcance de la presente invención.

**[0042]** Los diversos bloques lógicos, módulos y circuitos ilustrativos descritos en relación con los modos de realización divulgados en el presente documento pueden implementarse o realizarse con un procesador de uso general, con un procesador de señales digitales (DSP), con un circuito integrado específico de la aplicación (ASIC), con una matriz de puertas programables in situ (FPGA) o con otro dispositivo de lógica programable, lógica de transistores o puertas discretas, componentes de hardware discretos, o con cualquier combinación de los mismos diseñada para realizar las funciones descritas en el presente documento. Un procesador de uso general puede ser un microprocesador pero, como alternativa, el procesador puede ser cualquier procesador, controlador, microcontrolador o máquina de estados convencional. Un procesador también puede implementarse como una combinación de dispositivos informáticos, por ejemplo, una combinación de un DSP y un microprocesador, una pluralidad de microprocesadores, uno o más microprocesadores junto con un núcleo de DSP o cualquier otra configuración de este tipo.

**[0043]** Las etapas de un procedimiento o algoritmo descrito en relación con los modos de realización divulgados en el presente documento pueden realizarse directamente en hardware, en un módulo de software ejecutado por un procesador o en una combinación de los dos. Un módulo de software puede residir en una memoria RAM, memoria flash, memoria ROM, memoria EPROM, memoria EEPROM, registros, un disco duro, un disco extraíble, un CDROM o en cualquier otra forma de medio de almacenamiento conocida en la técnica. Un medio de almacenamiento a modo de ejemplo está acoplado al procesador de manera que el procesador pueda leer información de, y escribir información en, el medio de almacenamiento. De forma alternativa, el medio de almacenamiento puede estar integrado en el procesador. El procesador y el medio de almacenamiento pueden residir en un ASIC. El ASIC puede residir en un terminal de usuario. Como alternativa, el procesador y el medio de almacenamiento pueden residir como componentes discretos en un terminal de usuario.

**[0044]** En uno o más modos de realización a modo de ejemplo, las funciones descritas pueden implementarse en hardware, software, firmware o en cualquier combinación de estos. Si se implementan en software como producto de programa informático, las funciones pueden almacenarse o transmitirse como una o varias instrucciones o código en un medio legible por ordenador. Los medios legibles por ordenador incluyen tanto medios de almacenamiento informáticos como medios de comunicación, incluyendo cualquier medio que facilite la transferencia de un programa informático de un lugar a otro. Un medio de almacenamiento puede ser cualquier medio disponible al que pueda accederse mediante un ordenador. A modo de ejemplo, y no de manera limitativa, tales medios legibles por ordenador pueden comprender RAM, ROM, EEPROM, CDROM u otro almacenamiento de disco óptico, almacenamiento de disco magnético u otros dispositivos de almacenamiento magnético, o cualquier otro medio que pueda utilizarse para transportar o almacenar código de programa deseado en forma de instrucciones o estructuras de datos y al que pueda accederse mediante un ordenador. Además, cualquier conexión recibe adecuadamente la denominación de medio legible por ordenador. Por ejemplo, si el software se transmite desde una página web, un servidor u otra fuente remota, utilizando un cable coaxial, un cable de fibra óptica, un par trenzado, una línea de abonado digital (DSL) o tecnologías inalámbricas tales como infrarrojos, radio y microondas, entonces el cable coaxial, el cable de fibra óptica, el par trenzado, la DSL o las tecnologías inalámbricas, tales como infrarrojos, radio y microondas, se incluyen en la definición de medio. Los discos, tal como se utilizan en el presente documento, incluyen un disco compacto (CD), un disco láser, un disco óptico, un disco versátil digital (DVD), un disco flexible y un disco Blu-ray, donde algunos discos habitualmente reproducen los datos magnéticamente, mientras que otros discos reproducen los datos ópticamente con láseres. Las combinaciones de lo anterior deberían incluirse también dentro del alcance de los medios legibles por ordenador.

**[0045]** La anterior descripción de los modos de realización divulgados se proporciona para permitir que cualquier experto en la materia realice o utilice la presente invención. Diversas modificaciones de estos modos de realización resultarán fácilmente evidentes a los expertos en la materia y los principios genéricos definidos en el presente documento pueden aplicarse a otros modos de realización sin apartarse de la presente invención. Por tanto, la presente invención no pretende limitarse a los modos de realización mostrados en el presente documento, sino que se le concede el alcance más amplio compatible con los principios y características novedosas divulgados en el presente documento.

**[0046]** Otros modos de realización preferidos de la invención incluyen:

Un procedimiento para la autenticación mutua entre la primera entidad y una segunda entidad; que comprende:

la primera entidad inicia la autenticación mutua enviando un mensaje a la segunda entidad; la segunda entidad verifica una primera clave pública asociada con la primera entidad, genera un primer número aleatorio, cifra el primer número aleatorio utilizando la primera clave pública, y envía el primer número aleatorio cifrado en un mensaje a la primera entidad; la primera entidad verifica una segunda clave pública asociada con la segunda entidad, descifra el primer número aleatorio cifrado utilizando una primera clave privada correspondiente a la primera clave pública, genera un segundo número aleatorio, genera una primera hash basada en al menos el primer número aleatorio, cifra el segundo número aleatorio y la primera hash utilizando la segunda clave pública, y envía el segundo número aleatorio cifrado y la primera hash en un mensaje a la segunda entidad; la segunda entidad descifra el segundo número aleatorio cifrado y la primera hash utilizando una segunda clave privada correspondiente a la segunda clave pública, verifica la primera hash para autenticar la primera entidad, genera una segunda hash basada en al menos el segundo número aleatorio y envía la segunda hash a la primera entidad; y la primera entidad verifica la segunda hash para autenticar la segunda entidad.

**[0047]** En el procedimiento para la autenticación mutua de la primera entidad y la segunda entidad pueden cada uno derivar una clave de cifrado de sesión y la clave de código de autenticación de mensaje (MAC), utilizando el primer número aleatorio y el segundo número aleatorio basado en una función de derivación de claves, para su uso en las comunicaciones entre la primera entidad y la segunda entidad.

**[0048]** En el procedimiento para la autenticación mutua el mensaje que inicia la autenticación mutua puede incluir una hash de al menos una clave raíz de confianza y una cadena de certificados correspondiente para la primera entidad.

**[0049]** En el procedimiento para la autenticación mutua el mensaje desde la segunda entidad a la primera entidad que tiene el primer número aleatorio cifrado puede incluir, además, una cadena de certificados para la segunda entidad.

**[0050]** En el procedimiento para la autenticación mutua la primera entidad puede ser un agente de derechos digitales y la segunda entidad es un dispositivo seguro de medios extraíbles.

**[0051]** En el procedimiento para la autenticación mutua la primera entidad puede ser una estación móvil.

**[0052]** En el procedimiento para la autenticación mutua la segunda entidad puede tener potencia de procesamiento limitada.

**[0053]** En el procedimiento para la autenticación mutua la primera hash puede basarse, además, en al menos el segundo número aleatorio tal que la primera hash se genera en base a al menos el primer número aleatorio concatenado con el segundo número aleatorio.

**[0054]** En el procedimiento para la autenticación mutua la segunda hash puede basarse adicionalmente en al menos el primer número aleatorio.

**[0055]** En el procedimiento para la autenticación mutua la segunda hash puede basarse, además, en al menos la primera hash de tal manera que se genera la segunda hash basada en al menos el segundo número aleatorio concatenado con la primera hash.

**[0056]** Aún otros modos de realización preferidos de la invención incluyen:

Aparato para la autenticación mutua que comprende: medios para iniciar la autenticación mutua; medios para verificar una primera clave pública, generar un primer número aleatorio y cifrar el primer número aleatorio utilizando la primera clave pública; medios para verificar una segunda clave pública, descifrar el primer número aleatorio cifrado utilizando una primera clave privada correspondiente a la primera clave pública, generar un segundo número aleatorio, generar una primera hash basada en al menos el primer número aleatorio y cifrar el segundo número aleatorio y la primera hash utilizando la segunda clave pública; medios para descifrar el segundo número aleatorio cifrado y la primera hash utilizando una segunda clave privada correspondiente a la segunda clave pública, verificar la primera hash para la autenticación, y generar una segunda hash basada en al menos el segundo número aleatorio; y medios para verificar la segunda hash para la autenticación.

**[0057]** En el aparato para la autenticación mutua se puede comprender, además: medios para derivar una clave de cifrado de sesión y una clave de código de autenticación de mensaje (MAC) utilizando el primer número aleatorio y el segundo número aleatorio basándose en una función de derivación de claves, para su uso en las comunicaciones entre la primera entidad y la segunda entidad.

**[0058]** En el aparato para la autenticación mutua, la primera hash puede basarse, además, en al menos el segundo número aleatorio de tal manera que se genera la primera hash basada en al menos el primer número aleatorio concatenado con el segundo número aleatorio.

**[0059]** En el aparato para la autenticación mutua, la segunda hash puede basarse adicionalmente en al menos el primer número aleatorio.

**[0060]** En el aparato para la autenticación mutua, la segunda hash puede basarse, además, en la primera hash de modo que la segunda hash se genera en base al segundo número aleatorio concatenado con la primera hash.

**[0061]** Aún otros modos de realización preferidos de la invención incluyen:

Una estación que tiene autenticación mutua con un dispositivo seguro de medios extraíbles, que comprende: un agente de derechos digitales, en donde: el agente de derechos digitales inicia la autenticación mutua enviando un mensaje al dispositivo seguro de medios extraíbles, en el que el dispositivo seguro de medios extraíbles verifica una primera clave pública asociada con el agente de derechos digitales, genera un primer número aleatorio, cifra el primer número aleatorio utilizando la primera clave pública, y envía el primer número aleatorio cifrado en un mensaje al agente de derechos digitales; el agente de derechos digitales verifica una segunda clave pública asociada con el dispositivo seguro de medios extraíbles, descifra el primer número aleatorio cifrado utilizando una primera clave privada correspondiente a la primera clave pública, genera un segundo número aleatorio, genera una primera hash basada en al menos el primer número aleatorio, cifra el segundo número aleatorio y la primera hash utilizando la segunda clave pública, y envía el segundo número aleatorio cifrado y la primera hash en un mensaje al dispositivo seguro de medios extraíbles, en el que el dispositivo seguro de medios extraíbles descifra el segundo número aleatorio cifrado y la primera hash utilizando una segunda clave privada correspondiente a la segunda clave pública, verifica la primera hash para autenticar al agente de derechos digitales, genera una segunda hash basada en al menos el segundo número aleatorio y envía la segunda hash al agente de derechos digitales; y el agente de derechos digitales verifica la segunda hash para autenticar el dispositivo seguro de medios extraíbles.

**[0062]** En la estación que tiene la autenticación mutua, el agente de derechos digitales y el dispositivo seguro de medios extraíble derivan cada uno una clave de cifrado de sesión y la clave de código de autenticación de mensaje (MAC) utilizando el primer número aleatorio y el segundo número aleatorio basado en una función de derivación de claves, para uso en comunicaciones entre el agente de derechos digitales y el dispositivo seguro de medios extraíbles.

**[0063]** En la estación que tiene la autenticación mutua, el mensaje enviado por el agente de derechos digitales para iniciar la autenticación mutua puede incluir una hash de al menos una clave raíz de confianza y una cadena de certificados correspondiente para el agente de derechos digitales.

**[0064]** En la estación que tiene la autenticación mutua la cadena de certificados para el agente de derechos digitales puede incluir la clave pública asociada con el agente de derechos digitales.

**[0065]** En la estación que tiene la autenticación mutua, el mensaje enviado por el dispositivo seguro de medios extraíbles al agente de derechos digitales que tiene el primer número aleatorio cifrado puede incluir, además, una cadena de certificados para el dispositivo seguro de medios extraíbles.

**[0066]** En la estación que tiene la autenticación mutua, la cadena de certificados para el dispositivo seguro de medios extraíbles puede incluir la clave pública asociada con el dispositivo seguro de medios extraíbles.

**[0067]** En la estación que tiene la autenticación mutua, la estación puede ser una estación móvil.

**[0068]** En la estación que tiene la autenticación mutua, la primera hash puede basarse, además, en al menos el segundo número aleatorio de modo que el agente de derechos digitales genera la primera hash basada en al menos el primer número aleatorio concatenado con el segundo número aleatorio.

**[0069]** Aún otro modo de realización preferido de la invención incluye:

Un producto de programa informático que comprende: un medio legible por ordenador que comprende: código para hacer que un ordenador haga que un agente de derechos digitales de una estación inicie la autenticación mutua enviando un mensaje a un dispositivo seguro de medios extraíbles, en el que el dispositivo seguro de medios extraíbles verifica una primera clave pública asociada con el agente de derechos digitales, genera un primer número aleatorio, cifra el primer número aleatorio utilizando la primera clave pública, y envía el primer número aleatorio cifrado en un mensaje al agente de derechos digitales; código para hacer que un ordenador haga que el agente de derechos digitales verifique una segunda clave pública asociada con el dispositivo seguro de medios extraíbles, descifre el primer número aleatorio cifrado utilizando una primera clave privada correspondiente a la primera clave pública, genere un segundo número aleatorio, genere una primera hash basada en al menos el primer número aleatorio, cifre el segundo número aleatorio y la primera hash utilizando la segunda clave pública, y envíe el segundo número aleatorio cifrado y la primera hash en un mensaje al dispositivo seguro de medios extraíbles, en el que el dispositivo seguro de medios extraíbles descifra el segundo número aleatorio cifrado y la primera hash utilizando una segunda clave privada correspondiente a la segunda

clave pública, verifica la primera hash para autenticar al agente de derechos digitales, genera una segunda hash basada en al menos el segundo número aleatorio y envía la segunda hash al agente de derechos digitales; y código para hacer que un ordenador haga que el agente de derechos digitales verifique la segunda hash para autenticar el dispositivo seguro de medios extraíbles.

**[0070]** Aún otro modo de realización preferido de la invención incluye:

Un producto de programa informático, que comprende: un medio legible por ordenador que comprende: código para hacer que un ordenador haga que un dispositivo seguro de medios extraíbles verifique una primera clave pública asociada con un agente de derechos digitales, genere un primer número aleatorio, cifre el primer número aleatorio utilizando la primera clave pública, y envíe el primer número aleatorio cifrado en un mensaje al agente de derechos digitales, en el que el agente de derechos digitales verifica una segunda clave pública asociada con el dispositivo seguro de medios extraíbles, descifra el primer número aleatorio cifrado utilizando una primera clave privada correspondiente a la primera clave pública, genera un segundo número aleatorio, genera una primera hash basada en al menos el primer número aleatorio, cifra el segundo número aleatorio y la primera hash utilizando la segunda clave pública, y envía el segundo número aleatorio cifrado y la primera hash en un mensaje al dispositivo seguro de medios extraíbles; código para hacer que un ordenador haga que el dispositivo seguro de medios extraíbles descifre el segundo número aleatorio cifrado y la primera hash utilizando una segunda clave privada correspondiente a la segunda clave pública, verifique la primera hash para autenticar al agente de derechos digitales, genere una segunda hash basada en al menos el segundo número aleatorio, y envíe la segunda hash al agente de derechos digitales, en el que el agente de derechos digitales verifica la segunda hash para autenticar el dispositivo seguro de medios extraíbles.

**REIVINDICACIONES**

**1.** Un procedimiento (300) para la autenticación mutua entre la primera entidad (202) y una segunda entidad (204); que comprende:

la primera entidad (202) que inicia (302) la autenticación mutua enviando un mensaje a la segunda entidad (204);

la segunda entidad (204) que verifica una primera clave pública asociada con la primera entidad (202), que genera (304) un primer número aleatorio, que cifra el primer número aleatorio utilizando la primera clave pública y que envía (306) el primer número aleatorio cifrado en un mensaje a la primera entidad (202);

la primera entidad (202) que verifica una segunda clave pública asociada con la segunda entidad, que descifra el primer número aleatorio cifrado utilizando una primera clave privada correspondiente a la primera clave pública, que genera (308) un segundo número aleatorio, que genera una primera hash basada en al menos el primer número aleatorio, que cifra el segundo número aleatorio y la primera hash utilizando la segunda clave pública, y que envía (310) el segundo número aleatorio cifrado y la primera hash en un mensaje a la segunda entidad (204);

la segunda entidad (204) que descifra el segundo número aleatorio cifrado y la primera hash utilizando una segunda clave privada correspondiente a la segunda clave pública, que verifica la primera hash para autenticar la primera entidad (202), que genera una segunda hash basada en el segundo número aleatorio, en el que la segunda hash se basa, además, en el primer número aleatorio, y que envía (312) la segunda hash a la primera entidad (202); y

la primera entidad (202) que verifica la segunda hash para autenticar la segunda entidad (204).

**2.** Un procedimiento (300) para la autenticación mutua según se define en la reivindicación 1, en el que la primera entidad (202) y la segunda entidad (204) obtienen cada una una clave de cifrado de sesión y una clave de código de autenticación de mensaje, MAC utilizando el primer número aleatorio y el segundo número aleatorio basándose en una función de derivación de claves, para uso en comunicaciones entre la primera entidad (202) y la segunda entidad (204).

**3.** Un procedimiento (300) para la autenticación mutua según se define en la reivindicación 1, en el que el mensaje que inicia la autenticación mutua incluye una hash de al menos una clave raíz de confianza y una cadena de certificados correspondiente para la primera entidad (202).

**4.** Un procedimiento (300) para la autenticación mutua según se define en la reivindicación 1, en el que el mensaje de la segunda entidad (204) a la primera entidad (202) que tiene el primer número aleatorio cifrado incluye, además, una cadena de certificados para la segunda entidad (204).

**5.** Un procedimiento (300) para la autenticación mutua según se define en la reivindicación 1, en el que la primera entidad (202) es un agente de derechos digitales y la segunda entidad (204) es un dispositivo seguro de medios extraíbles.

**6.** Un procedimiento (300) para la autenticación mutua según se define en la reivindicación 1, en el que la primera entidad (202) es una estación móvil.

**7.** Un procedimiento (300) para la autenticación mutua según se define en la reivindicación 1, en el que la segunda entidad (204) tiene una potencia de procesamiento limitada.

**8.** Un procedimiento (300) para la autenticación mutua según se define en la reivindicación 1, en el que la primera hash se basa, además, en al menos el segundo número aleatorio de modo que la primera hash se genera basándose en al menos el primer número aleatorio concatenado con el segundo número aleatorio.

**9.** Un procedimiento (300) para la autenticación mutua según se define en la reivindicación 1, en el que la segunda hash se basa, además, en al menos la primera hash de tal manera que la segunda hash se genera basándose en al menos el segundo número aleatorio concatenado con la primera hash.

**10.** Aparato para la autenticación mutua que comprende:

medios para iniciar la autenticación mutua;

medios para verificar una primera clave pública, generar (304) un primer número aleatorio y cifrar el primer número aleatorio utilizando la primera clave pública;

medios para verificar una segunda clave pública, descifrar el primer número aleatorio cifrado utilizando una primera clave privada correspondiente a la primera clave pública, generar (308) un segundo número aleatorio, generar una primera hash basada en al menos el primer número aleatorio y cifrar el segundo número aleatorio y la primera hash utilizando la segunda clave pública;

medios para descifrar el segundo número aleatorio cifrado y la primera hash utilizando una segunda clave privada correspondiente a la segunda clave pública, verificar la primera hash para la autenticación y generar una segunda hash basada en el segundo número aleatorio, en el que la segunda hash se basa adicionalmente en el primer número aleatorio; y

medios para verificar la segunda hash para la autenticación.

**11.** Aparato para la autenticación mutua según la reivindicación 10, que comprende, además, medios para derivar una clave de cifrado de sesión y una clave de código de autenticación de mensaje, MAC utilizando el primer número aleatorio y el segundo número aleatorio basado en una función de derivación de claves para uso en comunicaciones entre la primera entidad (202) y la segunda entidad (204).

**12.** Una estación (102) que tiene autenticación mutua con un dispositivo seguro de medios extraíbles (204), que comprende:

un agente de derechos digitales (202), en el que:

el agente de derechos digitales (202) está configurado para iniciar la autenticación mutua enviando (302) un mensaje a un dispositivo seguro de medios extraíbles (204), en el que el dispositivo seguro de medios extraíbles (204) verifica una primera clave pública asociada con el agente de derechos digitales (202), genera (304) un primer número aleatorio, cifra el primer número aleatorio utilizando la primera clave pública y envía (306) el primer número aleatorio cifrado en un mensaje al agente de derechos digitales (202);

el agente de derechos digitales (202) está configurado, además, para verificar una segunda clave pública asociada con el dispositivo seguro de medios extraíbles (204), descifra el primer número aleatorio cifrado utilizando una primera clave privada correspondiente a la primera clave pública, genera un segundo número aleatorio, genera una primera hash basada en al menos el primer número aleatorio, cifra el segundo número aleatorio y la primera hash utilizando la segunda clave pública, y envía (310) el segundo número aleatorio cifrado y la primera hash en un mensaje al dispositivo seguros de medios extraíbles (204), en el que el dispositivo seguro de medios extraíbles (204) descifra el segundo número aleatorio cifrado y la primera hash utilizando una segunda clave privada correspondiente a la segunda clave pública, verifica la primera hash para autenticar el agente de derechos digitales, genera una segunda hash basada en el segundo número aleatorio, en el que la segunda hash se basa, además, en el primer número aleatorio, y envía (312) la segunda hash al agente de derechos digitales; y

el agente de derechos digitales (202) está configurado para verificar la segunda hash para autenticar el dispositivo de medios extraíbles seguros (204).

**13.** Un dispositivo seguro de medios extraíbles (204) para realizar la autenticación mutua con un agente de derechos digitales (202), en el que:

el dispositivo seguro de medios extraíbles (204) está configurado para verificar una primera clave pública asociada con el agente de derechos digitales (202), generar (304) un primer número aleatorio, cifrar el primer número aleatorio utilizando la primera clave pública y enviar (306) el primer número aleatorio cifrado en un mensaje al agente de derechos digitales (202), en el que el agente de derechos digitales (202) verifica una segunda clave pública asociada con el dispositivo seguro de medios extraíbles (204), descifra el primer número aleatorio cifrado utilizando un primera clave privada correspondiente a la primera clave pública, genera un segundo número aleatorio, genera una primera hash basada en al menos el primer número aleatorio, cifra el segundo número aleatorio y la primera hash utilizando la segunda clave pública, y envía (310) el segundo número aleatorio cifrado y la primera hash en un mensaje al dispositivo seguro de medios extraíbles (204); y

el dispositivo seguro de medios extraíbles (204) está configurado para descifrar el segundo número aleatorio cifrado y la primera hash utilizando una segunda clave privada correspondiente a la segunda clave pública, verifica la primera hash para autenticar al agente de derechos digitales, genera una segunda hash basada en el segundo número aleatorio, en el que la segunda hash se basa, además, en el primer número aleatorio, y envía (312) la segunda hash al agente de derechos digitales (202), en el que el agente de derechos digitales (202) verifica la segunda hash para autenticar el dispositivo seguro de

medios extraíbles (204).

**14.** Un producto de programa informático, que comprende:

un medio legible por ordenador, que comprende:

código para hacer que un ordenador haga que un agente de derechos digitales (202) de una estación (102) inicie la autenticación mutua enviando (302) un mensaje a un dispositivo seguro de medios extraíbles (204), en el que el dispositivo seguro de medios extraíbles (204) verifica una primera clave pública asociada con el agente de derechos digitales (202), genera un primer número aleatorio, cifra el primer número aleatorio utilizando la primera clave pública y envía (306) el primer número aleatorio cifrado en un mensaje al agente de derechos digitales (202);

código para hacer que un ordenador haga que el agente de derechos digitales (202) verifique una segunda clave pública asociada con el dispositivo seguro de medios extraíbles (204), descifre el primer número aleatorio cifrado utilizando una primera clave privada correspondiente a la primera clave pública, genere un segundo número aleatorio, genere una primera hash basada en al menos el primer número aleatorio, cifre el segundo número aleatorio y la primera hash utilizando la segunda clave pública, y envíe (310) el segundo número aleatorio cifrado y la primera hash en un mensaje al dispositivo seguro de medios extraíbles (204), en el que el dispositivo seguro de medios extraíbles (204) descifra el segundo número aleatorio cifrado y la primera hash utilizando una segunda clave privada correspondiente a la segunda clave pública, verifica la primera hash para autenticar al agente de derechos digitales, genera una segunda hash basada en el segundo número aleatorio, en el que la segunda hash se basa, además, en el primer número aleatorio, y envía (312) la segunda hash al agente de derechos digitales (202); y

código para hacer que un ordenador haga que el agente de derechos digitales (202) verifique la segunda hash para autenticar el dispositivo seguro de medios extraíbles (204).

**15.** Un producto de programa informático, que comprende:

un medio legible por ordenador, que comprende:

código para hacer que un ordenador haga que un dispositivo seguro de medios extraíbles (204) verifique una primera clave pública asociada con un agente de derechos digitales (202), genere (304) un primer número aleatorio, cifre el primer número aleatorio utilizando la primera clave pública y envíe (306) el primer número aleatorio cifrado en un mensaje al agente de derechos digitales (202), en el que el agente de derechos digitales (202) verifica una segunda clave pública asociada con el dispositivo seguro de medios extraíbles, descifra el primer número aleatorio cifrado utilizando una primera clave privada correspondiente a la primera clave pública, genera (308) un segundo número aleatorio, genera una primera hash basada en al menos el primer número aleatorio, cifra el segundo número aleatorio y la primera hash utilizando la segunda clave pública, y envía (310) el segundo número aleatorio cifrado y la primera hash en un mensaje al dispositivo seguro de medios extraíbles (204); y

código para hacer que el dispositivo seguro de medios extraíbles (204) descifre el segundo número aleatorio cifrado y la primera hash utilizando una segunda clave privada correspondiente a la segunda clave pública, verifique la primera hash para autenticar el agente de derechos digitales (202), genere una segunda hash basada en el segundo número aleatorio, en el que la segunda hash se basa, además, en el primer número aleatorio, y envíe (312) la segunda hash al agente de derechos digitales (202), en el que el agente de derechos digitales (202) verifica la segunda hash para autenticar el dispositivo seguro de medios extraíbles.

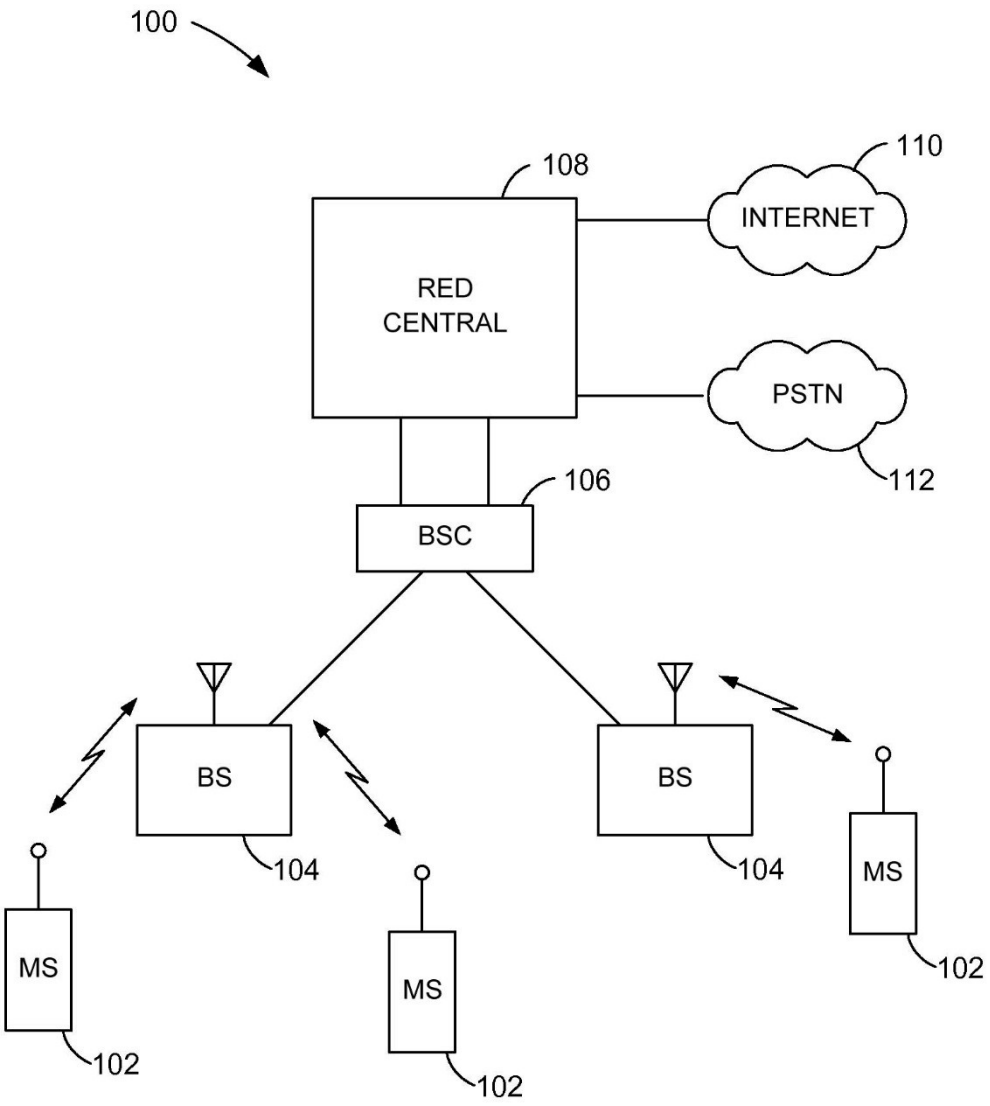
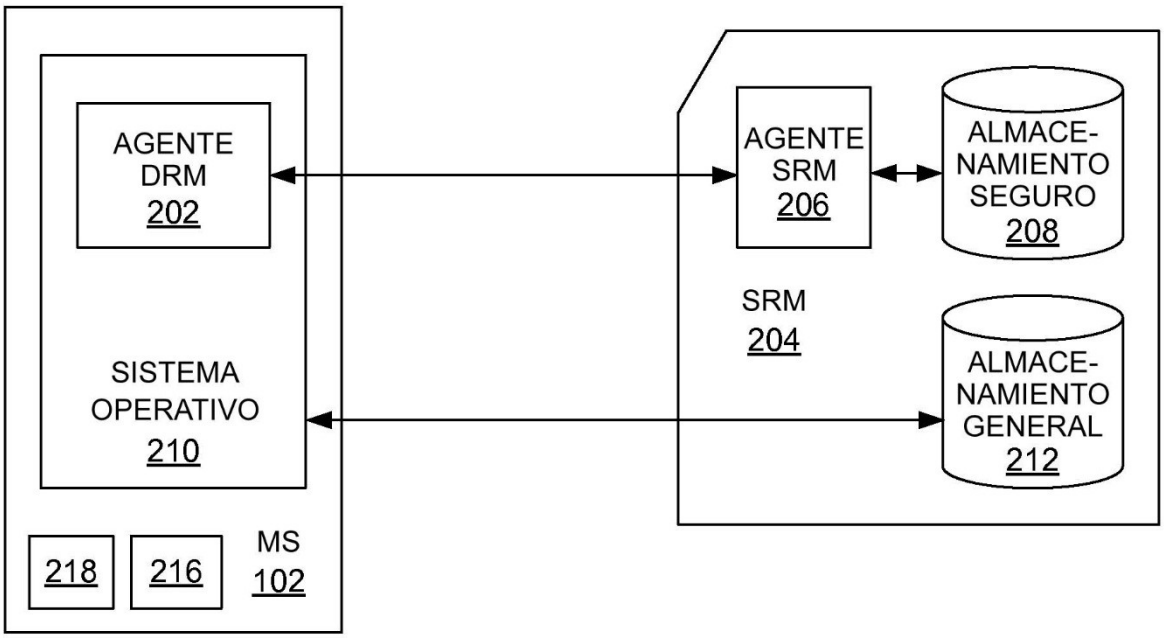

100
108
110
INTERNET
RED
CENTRAL
PSTN
112
106
BSC
BS
BS
104
104
MS
MS
MS
102
102
102

FIG. 1

FIG. 2


AGENTE DRM 202
SISTEMA OPERATIVO 210
218
216
MS 102
AGENTE SRM 206
ALMACE-NAMIENTO SEGURO 208
SRM 204
ALMACE-NAMIENTO GENERAL 212

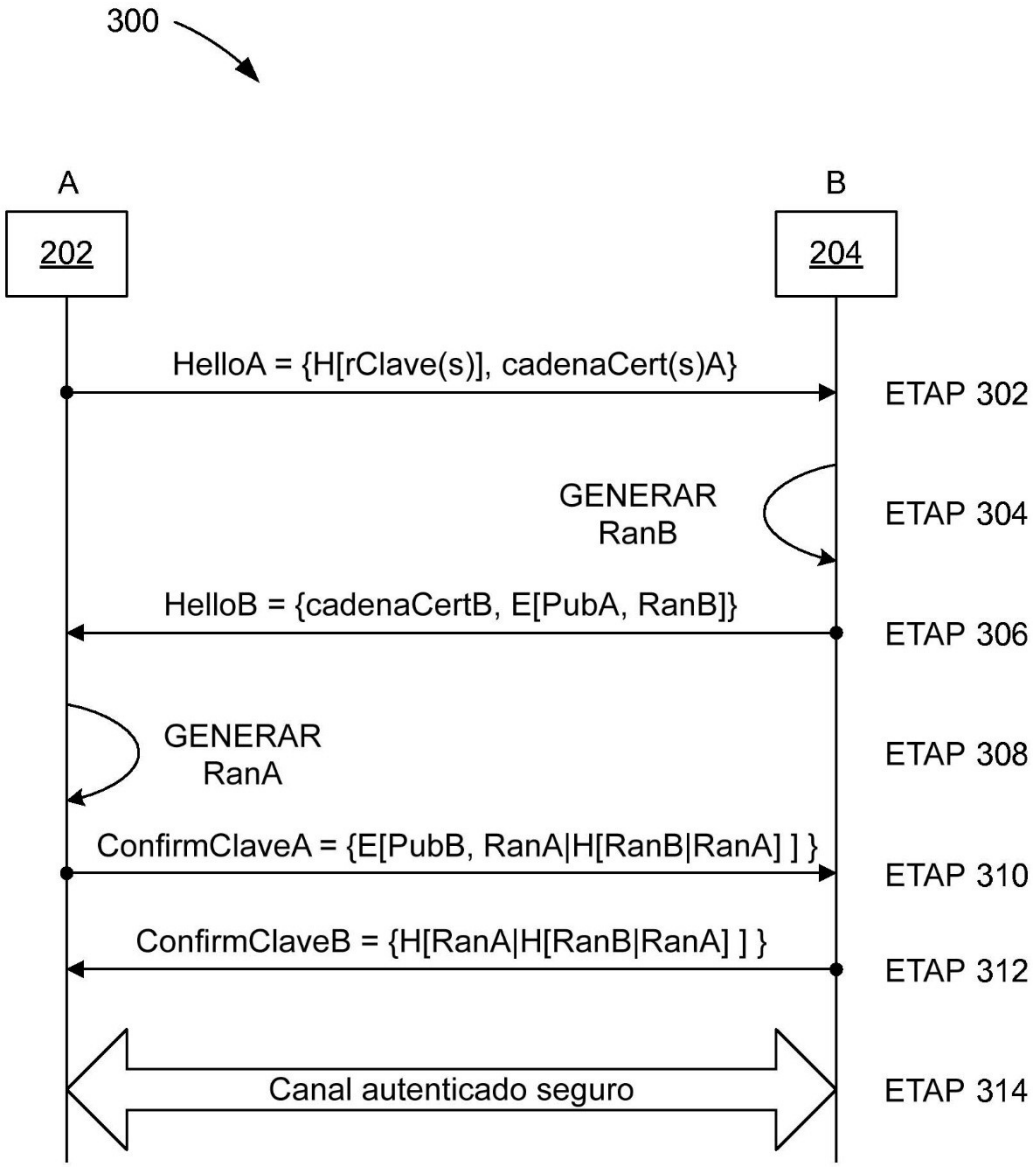

300
A
202
B
204
HelloA = {H[rClave(s)], cadenaCert(s)A}
ETAP 302
GENERAR
RanB
ETAP 304
HelloB = {cadenaCertB, E[PubA, RanB]}
ETAP 306
GENERAR
RanA
ETAP 308
ConfirmClaveA = {E[PubB, RanA|H[RanB|RanA] ] }
ETAP 310
ConfirmClaveB = {H[RanA|H[RanB|RanA] ] }
ETAP 312
Canal autenticado seguro
ETAP 314

FIG. 3