(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 741 398**

(51) Int. CI.:

G06F 21/64 (2013.01)
G06F 21/73 (2013.01)
H04L 29/06 (2006.01)
H04L 9/32 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **20.10.2015 PCT/GB2015/053132**

(87) Fecha y número de publicación internacional: **28.04.2016 WO16063044**

(96) Fecha de presentación y número de la solicitud europea: **20.10.2015 E 15793886 (1)**

(97) Fecha y número de publicación de la concesión europea: **08.05.2019 EP 3210158**

(54) Título: **Transmisión segura**

(30) Prioridad:

23.10.2014 US 201414521929

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
10.02.2020

(73) Titular/es:

Y R FREE LABS LIMITED (100.0%)
3rd Floor, 80 Mosley Street
Manchester M2 3FX, GB

(72) Inventor/es:

DAVIES, PHIL

(74) Agente/Representante:

VALLEJO LÓPEZ, Juan Pedro

DESCRIPCIÓN

Transmisión segura

Antecedentes

Los dispositivos de computación móviles, tales como teléfonos móviles, teléfonos inteligentes, ordenadores de tableta, etc. comprenden a menudo, o tienen acceso a, una serie de sensores tales como sensores de imagen y sensores de sonido. Aunque comúnmente se utilizan para registrar eventos para el consumo personal, tales grabaciones por lo general no son adecuadas para su uso como prueba en un proceso en el que la autenticidad, exactitud y/o la procedencia de esas grabaciones pueden requerir la verificación.

La rápida proliferación de dispositivos móviles es tal, sin embargo, que los dispositivos móviles están a menudo presentes en circunstancias en las que dichos datos probatorios se pueden obtener de manera útil. Por tanto, sería beneficioso si tales dispositivos móviles fueron capaces de obtener y proporcionar grabaciones de calidad probatorias de transacciones o eventos. Tales grabaciones de calidad probatoria pueden tener usos, por ejemplo, en procesos judiciales, reclamaciones de seguros, etc.

Un objetivo de la presente invención es obviar o mitigar al menos uno de los problemas de la técnica anterior si se identifica en el presente documento o en otro lugar.

Sumario

La presente invención se define por las reivindicaciones adjuntas. De acuerdo con un primer aspecto descrito en el presente documento, se proporciona un método para proporcionar datos probatorios, que comprende en un dispositivo móvil: establecer uno o más primeros testigos secretos con un servidor; obtener uno o más elementos de datos de uno o más sensores; modificar uno o más elementos de datos con al menos uno del uno o más primeros testigos secretos para proporcionar uno o más elementos de datos modificados; generar un primer valor hash respectivo para cada uno del uno o más elementos de datos modificados; generar un segundo valor hash para un conjunto de datos que comprende cada uno del uno o más elementos de datos; y transmitir el uno o más elementos de datos, el uno o más primeros valores hash y el segundo valor hash al servidor.

El conjunto de datos puede comprender los primeros valores hash.

El método puede comprender además obtener uno o más identificadores de transacción, siendo cada identificador de transacción adecuado para la identificación de una propiedad del dispositivo móvil; y transmitir una indicación de dichos identificadores de transacción al servidor.

El conjunto de datos puede comprender uno o más de los identificadores de transacción.

El uno o más identificadores de transacción puede comprender uno o más identificadores estáticos, en el que cada identificador estático es adecuado para identificar una propiedad estática del dispositivo móvil.

La transmisión de una indicación de los identificadores estáticos al servidor puede comprender la generación de un tercer valor hash respectivo para cada uno del uno o más identificadores estáticos, en el que la indicación comprende los terceros valores hash.

El conjunto de datos puede comprender los terceros valores hash.

El cálculo de cada tercer valor hash respectivo puede comprender la modificación de cada uno de la pluralidad de identificadores estáticos con al menos uno del uno o más primeros testigos secretos y el cálculo de cada uno de dichos terceros valores hash basándose en los identificadores estáticos modificados.

Los identificadores de transacción pueden comprender uno o más identificadores variables y cada identificador variable puede ser adecuado para identificar una propiedad variable del dispositivo móvil. Transmitir una indicación de los identificadores variables al servidor puede comprender la transmisión del identificador variable al servidor.

El conjunto de datos puede comprender los identificadores variables.

El método puede comprender, además, un procedimiento de inicialización. El procedimiento de inicialización puede comprender la transmisión de una pluralidad de identificadores de inicialización al servidor.

Los identificadores de inicialización pueden comprender uno o más identificadores estáticos y/o uno o más identificadores variables.

La transmisión de una pluralidad de identificadores de inicialización puede comprender la obtención de la pluralidad

de identificadores de inicialización, el cifrado de los identificadores de inicialización obtenidos y la transmisión de los identificadores de inicialización cifrados al servidor.

Los identificadores de transacción se pueden basar en los identificadores de inicialización para permitir la comparación en el servidor entre los valores de los identificadores de inicialización y los identificadores de transacción.

El uno o más sensores pueden comprender al menos un sensor de entre el grupo que comprende una cámara del dispositivo móvil y un micrófono del dispositivo móvil.

El uno o más elementos de datos pueden comprender una o más imágenes fijas.

El uno o más elementos de datos pueden comprender uno o más vídeos.

El uno o más elementos de datos pueden comprender una o más grabaciones de sonido.

El uno o más identificadores estáticos pueden comprender al menos un identificador del grupo que comprende un número de identificación de una batería del dispositivo móvil, un número IMEI del dispositivo móvil, número de teléfono del dispositivo móvil.

El uno o más identificadores variables pueden comprender al menos un identificador del grupo que comprende una ubicación geográfica del dispositivo móvil, una fecha y hora reportados por el dispositivo móvil, una duración de tiempo desde que el dispositivo móvil se enciende, una indicación de otros dispositivos detectados por el dispositivo móvil y una estructura de archivos del dispositivo móvil.

El método puede comprender además el establecimiento de uno o más segundos testigos secretos con el servidor después de la transmisión del uno o más elementos de datos y dicho primer y segundo valores hash.

De acuerdo con un segundo aspecto, se proporciona un método para recibir datos probatorios que comprende, en un servidor: establecer uno o más primeros testigos secretos con un dispositivo móvil; recibir uno o más elementos de datos, uno o más primeros valores hash y un segundo valor hash desde el dispositivo móvil; en el que cada uno del uno o más primeros valores hash son valores hash generados basándose en uno respectivo del uno o más elementos de datos modificados con al menos uno del uno o más primeros testigos secretos; en el que el segundo valor hash es un valor hash generado basándose en un conjunto de datos que comprende cada uno del uno o más elementos de datos.

El método puede comprender además modificar cada uno del uno o más elementos de datos recibidos con al menos uno del uno o más primeros testigos secretos; generar un primer valor hash de comparación respectivo para cada uno del uno o más elementos de datos modificados recibidos; comparar cada primer valor hash de comparación respectivo con uno correspondiente de los primeros valores hash; y proporcionar una indicación para cada primer valor hash de comparación respectivo que no coincida con uno correspondiente de los primeros valores hash.

Proporcionar una indicación puede comprender la emisión de una indicación a un dispositivo de visualización, o guardar una indicación junto con los datos.

El método puede comprender además recibir una pluralidad de identificadores de inicialización desde el dispositivo móvil; recibir uno o más identificadores de transacción, siendo cada uno del uno o más identificadores de transacción adecuados para identificar una propiedad del dispositivo móvil; y comparar al menos uno de los identificadores de inicialización con al menos uno de los identificadores de transacción.

El método puede comprender además transmitir una solicitud de los identificadores de transacción basándose en los identificadores de inicialización recibidos.

Los identificadores de inicialización pueden comprender un primer identificador estático adecuado para identificar una propiedad estática del dispositivo móvil. El uno o más identificadores de transacción pueden comprender una indicación de un identificador estático correspondiente. La comparación de al menos uno del identificador de inicialización puede comprender la comparación del primer identificador estático con el identificador estático correspondiente.

La indicación del identificador estático puede comprender un tercer valor hash basándose en el identificador estático correspondiente. Comparar el primer identificador estático con el identificador estático correspondiente puede comprender la generación de un cuarto valor hash basándose en el primer identificador estático y comparar el cuarto valor hash con el tercer valor hash.

El tercer valor hash puede haberse generado por el dispositivo móvil que realiza las etapas de modificar el identificador estático correspondiente con al menos uno del uno o más primeros testigos secretos y calcular cada uno de los terceros valores hash basándose en el identificador estático correspondiente modificado. Generar el cuarto valor hash

puede comprender la modificación del primer identificador estático con al menos uno del uno o más primeros testigos secretos y calcular el cuarto valor hash basándose en el primer identificador estático modificado.

Los identificadores de inicialización pueden comprender un primer identificador variable adecuado para indicar las propiedades variables del dispositivo móvil. Los identificadores de transacción recibidos pueden comprender un identificador variable correspondiente. Comparar el primer identificador variable con el identificador variable correspondiente puede comprender la determinación de si una diferencia entre el primer identificador variable y el segundo identificador variable está dentro de los límites predeterminados.

Los identificadores de inicialización pueden comprender al menos uno de un número de una batería del dispositivo móvil, un número IMEI del dispositivo móvil, número de teléfono del dispositivo móvil.

El uno o más identificadores variables pueden comprender al menos un identificador del grupo que comprende una ubicación geográfica del dispositivo móvil, una fecha y hora reportados por el dispositivo móvil, una duración de tiempo desde que el dispositivo móvil se enciende, una indicación de otros dispositivos detectados por el dispositivo móvil y una estructura de archivos del dispositivo móvil.

El método puede comprender además el establecimiento de uno o más segundos testigos secretos con el dispositivo móvil después de la recepción del uno o más elementos de datos y dicho primeros y segundo valores hash.

De acuerdo con un tercer aspecto, se proporciona un aparato para proporcionar datos probatorios, que comprende: una memoria que almacena instrucciones legibles por ordenador configurada para hacer que un ordenador realice un método de acuerdo con una cualquiera de las reivindicaciones 1 a 24; y un procesador configurado para ejecutar las instrucciones legibles por ordenador.

Se ha de entender que las características descritas con referencia a un aspecto anterior pueden combinarse con otros aspectos.

Breve descripción de las figuras

A continuación se describirán las realizaciones de la invención, solamente a modo de ejemplo, con referencia a los dibujos adjuntos, en los que:

la Figura 1 ilustra esquemáticamente una red a modo de ejemplo de los componentes que pueden usarse para implementar una realización;
la Figura 2 ilustra esquemáticamente una configuración a modo de ejemplo de los componentes que pueden usarse para implementar el servidor de la Figura 1;
la Figura 3 ilustra esquemáticamente una configuración a modo de ejemplo de los componentes que pueden usarse para implementar un dispositivo móvil de la Figura 1;
la Figura 4 es un diagrama de flujo que muestra el procedimiento iniciación realizado por el servidor y el dispositivo móvil de la Figura 1;
la Figura 5 es un diagrama de flujo que muestra el procedimiento realizado por el dispositivo móvil de la Figura 1 para transmitir datos probatorios; y
la Figura 6 es un diagrama de flujo que muestra el procedimiento realizado por el servidor para recibir datos probatorios desde el dispositivo móvil.

Descripción detallada

La Figura 1 ilustra una red de dispositivos informáticos que se pueden utilizar para implementar las realizaciones de la presente invención. Un dispositivo móvil 1 se conecta a un servidor 2 a través de una red 3. La red 3 puede ser cualquier red pública o privada adecuada y puede, por ejemplo, ser Internet. El dispositivo móvil 1 puede adoptar cualquier forma adecuada para su conexión a la red 2. Por ejemplo, el dispositivo móvil 1 puede ser un teléfono móvil, un teléfono inteligente, una tableta, etc.

Las conexiones entre el servidor 2, el dispositivo móvil 1, y la red 3 pueden adoptar cualquier forma adecuada y pueden ser conexiones inalámbricas o cableadas. Se apreciará que si bien un dispositivo móvil individual 1 se ilustra en la Figura 1, esto es meramente a modo de ejemplo y cualquier número de dispositivo móvil puede conectarse con el servidor 2.

El dispositivo móvil 1 se configura para proporcionar datos al servidor 2 a través de la red 3. En particular, el dispositivo móvil 1 se configura para proporcionar datos relativos a los incidentes que ocurren en la proximidad del dispositivo móvil 1, como accidentes, crímenes, etc., con la finalidad de tener pruebas. Por ejemplo, el dispositivo móvil 1 puede estar equipado con medios de grabación tales como una o más cámaras para el registro de imágenes o vídeo, micrófonos para la grabación de sonidos, y receptores para la grabación de señales de radio recibidas. Se apreciará que el dispositivo móvil 1 puede usarse para obtener cualquier forma de datos probatorios según se requiera.

El dispositivo móvil 1 puede comunicarse con el servidor 2 desde una aplicación de ordenador local que opera en el dispositivo móvil 1 (o "aplicación") o por medio de una aplicación remota proporcionada por el servidor 2 y con acceso desde el dispositivo móvil 1 a través de, por ejemplo, un navegador web. Referencias futuras a una aplicación informática con la que el dispositivo móvil 1 puede comunicarse con el servidor 2 pueden por tanto ser o bien una aplicación informática local o una aplicación remota.

Tras la obtención de los datos probatorios, el dispositivo móvil 1 transmite los datos probatorios al servidor 2 a través de la red 3. En particular, el dispositivo móvil 1 transmite los datos probatorios junto con más datos para permitir que el servidor 2 y/o terceros (como la policía o autoridades judiciales) determinen que los datos probatorios se originan desde el dispositivo móvil 1 y no ha sido modificados o alterados de otra manera, con posterioridad a su creación y/o transmisión al servidor 2.

El servidor 2 se conecta a un almacén de datos públicos 4 y un almacén de datos privado 5. El almacén de datos privados 5 puede estar aislado de la red 3 para impedir el acceso a los archivos almacenados en su interior, por ejemplo, el dispositivo móvil 1, y cualquier otro dispositivo. Un servidor de seguridad 6 se puede conectar entre el almacén de datos privado 5 y el servidor 2.

El dispositivo móvil 1 puede funcionar en las proximidades de uno o más dispositivos de indicación de ubicación. Como se usa en el presente documento, la expresión dispositivo de indicación de ubicación significa cualquier dispositivo que se puede usar para proporcionar indicaciones de la ubicación geográfica actual del dispositivo móvil 1 o indicaciones de ubicaciones geográficas por las que ha pasado el dispositivo móvil 1. Por ejemplo, el dispositivo móvil 1 puede pasar dentro y fuera de un rango de uno o más puntos de acceso inalámbrico o estaciones de base 7, 8 (por ejemplo, puntos de acceso WiFi y/o estaciones de base WiMAX, por ejemplo), uno o más satélites de posicionamiento global (GPS) 9 y una o más antenas de la red celular 10.

La Figura 2 muestra una ilustración esquemática a modo de ejemplo de los componentes que pueden usarse para proporcionar el dispositivo móvil 1 de acuerdo con algunas realizaciones de la presente invención. Se puede observar que el dispositivo móvil 1 comprende una CPU 1a que se configura para leer y ejecutar instrucciones almacenadas en una memoria de acceso aleatorio (RAM) 1b que, en este ejemplo, toma la forma de memoria volátil 1b. Se apreciará que la memoria RAM no volátil puede usarse igualmente en una realización de este tipo. La RAM 1b almacena las instrucciones para su ejecución por la CPU 1a y los datos utilizados por dichas instrucciones. Por ejemplo, las instrucciones cargadas en la RAM 1b pueden proporcionar uno o más programas informáticos que son operables para obtener datos probatorios y para transmitir los datos probatorios al servidor 2.

El dispositivo móvil 1 comprende, además, almacenamiento no volátil 1c, que puede adoptar cualquier forma adecuada, tal como, por ejemplo, una unidad de disco duro (HDD) o unidad de estado sólido (SSD). Instrucciones legibles por ordenador para facilitar la captura, almacenamiento y transmisión de datos probatorios al servidor 2 se pueden almacenar en el almacenamiento no volátil 1c.

El dispositivo móvil 1 comprende además una interfaz E/S 1d a la que se conectan los dispositivos periféricos utilizados en conexión con el dispositivo móvil 1. Más particularmente, una pantalla 1e se configura para mostrar la salida desde el dispositivo móvil 1. La pantalla 1e puede ser una pantalla táctil, permitiendo a un usuario proporcionar entrada al dispositivo móvil 1e. Otros dispositivos de entrada están también conectados a la interfaz E/S 1d. Tales dispositivos de entrada incluyen una cámara 1f y un micrófono 1g, lo que permite a un usuario del dispositivo móvil 1 obtener imágenes (incluyendo de vídeo y estáticas) y sonido. Se apreciará que otros dispositivos de entrada pueden ser proporcionados por igual. Por ejemplo, medios de barrido biométricos dedicados, tales como escáneres de huellas dactilares, se pueden proporcionar.

Una interfaz de red 1h permite que el dispositivo móvil 1 se conecte a redes de ordenadores apropiados, tales como la red 3, a fin de recibir y transmitir datos desde y hacia otros dispositivos informáticos tales como el servidor 2. La interfaz de red 1h puede permitir también la conexión con, o la detección de señales desde, los dispositivos de indicación de ubicación tales como los dispositivos de indicación de ubicación de 7 a 10.

La CPU 1a, la memoria volátil 1b, la RAM 1c, la interfaz E/S 1d, y la interfaz de red 1h, están conectadas entre sí por un bus 1i.

Se apreciará que la disposición de los componentes ilustrados en la Figura 2 es meramente a modo de ejemplo, y que el dispositivo móvil 1 puede comprender componentes adicionales o menos que los ilustrados en la Figura 2.

La Figura 3 muestra una ilustración esquemática de los componentes que pueden usarse para proporcionar el servidor 2 de acuerdo con algunas realizaciones de la presente invención. Se puede observar que, a un nivel esquemático, el servidor 2 puede implementarse de manera similar al dispositivo móvil 1. En particular, el servidor 2 puede comprender una CPU 2a que se configura para leer y ejecutar instrucciones almacenadas en una memoria de acceso aleatorio (RAM) 2b. La RAM 2b almacena las instrucciones para su ejecución por la CPU 2a y los datos utilizados por dichas instrucciones. Por ejemplo, las instrucciones cargadas en la RAM 2b pueden proporcionar uno o más programas informáticos que son operables para facilitar la recepción de los datos probatorios desde el dispositivo móvil 1 y para

confirmar que los datos probatorios recibidos son adecuados para su uso como prueba.

El servidor 2 comprende, además, un almacenamiento no volátil 2c, que puede adoptar cualquier forma adecuada, tal como, por ejemplo, una unidad de disco duro (HDD) o unidad de estado sólido (SSD). El almacenamiento no volátil 2 puede comprender los almacenes de datos 4, 5. De forma alternativa, los almacenes de datos 4, 5 pueden estar conectados al servidor 2 a través de una red de almacenamiento (no mostrada).

El servidor 2 comprende además una interfaz E/S 2d a la que están conectados los dispositivos periféricos utilizados en conexión con el servidor 2. Más particularmente, una pantalla 2e se configura para mostrar la salida desde el servidor 2. La pantalla 2e puede ser una pantalla táctil, permitiendo a un usuario proporcionar entrada al servidor 2. Otros dispositivos de entrada pueden también conectarse a la interfaz E/S 2d, tal como un teclado 2f. Se apreciará que otros dispositivos de entrada pueden proporcionarse por igual.

Una interfaz de red 2h permite al servidor 2 conectarse a redes de ordenadores apropiados, tales como la red 3, a fin de recibir y transmitir datos desde y hacia otros dispositivos informáticos tales como el dispositivo móvil 1.

La CPU 2a, la memoria volátil 2b, la RAM2c, la interfaz E/S 2d, y la interfaz de red 2h, están conectadas entre sí por un bus 2i.

Se apreciará que la disposición de los componentes ilustrados en la Figura 3 es meramente a modo de ejemplo, y que el servidor 2 puede comprender componentes adicionales o menos que los ilustrados en la Figura 3. De hecho se ilustra esquemáticamente, el dispositivo móvil 1 que puede comprender una pluralidad de los ordenadores dispuestos de forma similar a, o diferente del dispositivo móvil 1. Por ejemplo, el servidor 2 puede comprender una pluralidad de ordenadores adaptados respectivamente para proporcionar, entre otras cosas, un servidor web, un servidor de aplicaciones, un servidor de pasarela y un servidor de base de datos, etc., para proporcionar aplicaciones adecuadas al dispositivo móvil 1 a través de la red 3. Es decir, se debe entender que, como el dispositivo móvil 1, el servidor 2 puede implementarse utilizando cualquier configuración adecuada como será fácilmente apreciado por los expertos en la materia.

La Figura 3 es un diagrama de flujo que ilustra un proceso de inicialización que se realiza por el dispositivo móvil 1 y el servidor 2 realizado antes de las transacciones para la transmisión de los datos probatorios entre el dispositivo móvil 1 con el servidor 2. La Figura 4 ilustra esquemáticamente los datos que se generan e intercambian por el dispositivo móvil 1 y el servidor 2 durante el procedimiento de la Figura 3. Se supone que antes de la transformación de la Figura 3, un usuario del dispositivo móvil 1 se ha registrado como un cliente o usuario de un servicio que recibe datos probatorios. Por ejemplo, el usuario del dispositivo móvil 1 puede obtener un producto de seguro, como el seguro del vehículo, de una entidad que opera el servidor 2 o en cuyo nombre el servidor 2 es operado. En este ejemplo, el usuario 1 puede usar las realizaciones descritas en el presente documento para proporcionar datos probatorios relacionados con accidentes, daños, etc. de un vehículo que está asegurado.

Antes del procedimiento de la Figura 3, la entidad con la que el usuario se está registrado puede proporcionar datos de acceso adecuados para el uso de la aplicación. Como alternativa, el usuario puede establecer datos de acceso a través de un proceso de registro realizado a través de la aplicación, como será fácilmente apreciado por la persona experta.

En la etapa S1 el usuario del dispositivo móvil 1 entra sus datos de acceso en una interfaz adecuada proporcionada por la aplicación. En la etapa S2 el servidor 2 recibe los datos de acceso del usuario y valida que los datos de acceso pertenecen a una cuenta registrada. Tras la validación de los datos de acceso, de la etapa S1, el procedimiento en el dispositivo móvil 1 pasa a la etapa S3, mientras que el procedimiento en el servidor 2 pasa a la etapa S4. En las etapas S3 y S4 el dispositivo 1 y el servidor 2 intercambian claves públicas móviles para su uso con la criptografía asimétrica. Con referencia a la Figura 4, el dispositivo móvil 1 transmite su clave pública 15 al servidor 2, mientras que el servidor 2 transmite su clave pública 16 al dispositivo móvil 1. En la Figura 4, el servidor 2 se muestra como recibiendo la clave pública 15 y el dispositivo móvil se muestra como recibiendo la clave pública 16. Se apreciará que esto es meramente esquemático, y que el servidor 2 mantendrá una copia de la clave pública 15, mientras que el dispositivo móvil 1 mantendrá una copia de la clave pública 16. El dispositivo móvil 1 almacena además una clave privada 17 (correspondiente a su clave pública 15), mientras que el servidor 2 almacena una clave privada 18 (correspondiente a su clave pública 16).

Las claves 15, 16, 17, 18 se pueden generar antes del procedimiento de la Figura 3 o se pueden generar como parte del procedimiento de las etapas S3 y S4. Las claves pública y privada pueden generarse usando cualquier medio apropiado como será fácilmente evidente para la persona experta. A modo de ejemplo solamente, las claves públicas y privadas se pueden generar utilizando el algoritmo RSA.

Tras la recepción de la clave pública 15 desde el dispositivo móvil 1, el procedimiento en el servidor 2 pasa a la etapa S5 en la que el servidor 2 genera un único testigo, generado al azar 21. El testigo 21 se cifra utilizando la clave pública 15 recibida del dispositivo móvil 1 para generar un testigo cifrado 22 que solo puede descifrarse utilizando la clave privada 17 del dispositivo móvil 1. El testigo 21 (o los datos a enviar en combinación con el testigo 21) puede

adicionalmente firmarse (no se muestra en la Figura 4) por el servidor 2 utilizando la clave privada 18. Por ejemplo, el testigo 21, o un hash del testigo 21, puede adicionalmente cifrarse usando la clave privada 18 de tal manera que el testigo 21 solo puede descifrarse por el dispositivo móvil 1 utilizando la clave pública 16 recibida desde el servidor 2. De esta manera, el dispositivo móvil 1 puede tener mayor certeza de que el testigo 21 se ha recibido desde el servidor 2, y no desde un tercero.

El testigo cifrado 22 se transmite al dispositivo móvil 1 y se recibe por el dispositivo móvil 1 en la etapa S7. El dispositivo móvil 1 descifra el testigo cifrado 22 utilizando su clave privada 19 para obtener el testigo 21.

Después del procedimiento de las etapas S3 a S7, cada uno del dispositivo móvil 1 y el servidor 2 posee información, en la forma del testigo 21, conocido solo entre sí. Se apreciará, sin embargo, que el procedimiento de las etapas S3 a S7 son meramente a modo de ejemplo y que en la práctica cualquier medio adecuado puede usarse para que el dispositivo móvil 1 y el servidor 2 intercambien de forma segura un testigo adecuado. En otras realizaciones, por ejemplo, una pluralidad de testigos secretos pueden intercambiarse.

El procedimiento pasa de la etapa S7 a la etapa S8 en la que el dispositivo móvil 1 genera u obtiene una pluralidad de elementos de datos de identificación de inicialización 25. Los elementos de datos de identificación adecuados incluyen, por ejemplo, un número de Identidad del Equipo de Estación Móvil Internacional (IMEI) del dispositivo móvil 1 (o identificadores similares, tales como ESN, MEID, etc.), un número de Identidad de Abonado móvil Internacional (IMSI), datos históricos del identificador de paquetes de servicio (SSID) (es decir, con cuales SSID el dispositivo móvil 1 ha entrado en contacto), datos GPS, una indicación de una corriente de datos de la celda móvil, fecha y hora actual locales, tiempo de actividad registrada por el dispositivo móvil 1, una última vez de reinicio del dispositivo móvil 1, velocidad de bits entre el dispositivo móvil 1 y el servidor 2, estructura de directorios de archivos del dispositivo móvil 1, etc. es decir, se apreciará que los datos de identificación pueden comprender cualquier datos de identificación adecuado que pueda usarse por el servidor 2 para determinar la autenticidad de un dispositivo que afirma ser el dispositivo móvil 1 en futuras transacciones.

Los datos de identificación pueden comprender ambos identificadores "estáticos" e identificadores "variables". Los identificadores estáticos pueden ser identificadores que no se espera que cambie con el tiempo o que se espera que cambien con muy poca frecuencia. Por ejemplo, puede esperarse que los números de identificación de la batería, números IMEI, datos de la estructura de archivos, etc., varíen con poca frecuencia. Los identificadores variables pueden ser aquellos identificadores que se espera que cambien con el tiempo. Por ejemplo, identificadores de tiempo y datos, identificadores de ubicación, datos de historial de SSID, etc. pueden esperarse que varíen entre una inicialización y una primera transacción, y entre las transacciones respectivas.

Como se describe a continuación con más detalle con referencia a las Figuras 5 y 6, los identificadores pueden transmitirse al servidor 2 desde el dispositivo móvil 1 durante cada transacción (es decir, las transacciones para transmitir datos probatorios). Debido a que no se espera que los identificadores estáticos varíen con frecuencia, puede que no sea necesario volver a transmitir (después de la transmisión inicial durante el procedimiento de la Figura 3) cada identificador estático. Más bien, como se describe a continuación, en algunas realizaciones, solo se transmite un valor hash basándose en cada identificador estático.

El conjunto particular de elementos de datos de identificación 25 obtenidos o generados por el dispositivo móvil 1 puede seleccionarse al azar por el dispositivo móvil 1 o por un usuario del dispositivo móvil 1. Como alternativa, el conjunto de elementos de datos de identificación puede seleccionarse por el servidor 2 y enviarse como una solicitud para el dispositivo móvil 1. Como alternativa, el conjunto de elementos de datos de identificación puede ser acordado entre el servidor 2 y el dispositivo móvil 1 en una operación acordada en la que se determina que los elementos de datos pueden ser proporcionados. Por ejemplo, se apreciará que los diferentes dispositivos (por ejemplo, tabletas y teléfonos móviles) pueden tener diferentes características que limitan o facilitan la generación de uno o más elementos de datos de identificación.

Después de haber generado los elementos de datos de identificación 25, el procedimiento pasa de la etapa S8 a la etapa S9 en la que los elementos de datos de identificación 25 se cifran para proporcionar elementos de datos de identificación cifrados 26. En el ejemplo de realización mostrado en la Figura 4, los elementos de datos de identificación 25 se cifran cada uno usando la clave pública del servidor 2. Se ha de apreciar, sin embargo, que los elementos de datos de identificación pueden cifrarse usando cualquier esquema de cifrado apropiado, o transmitirse de cualquier manera apropiada segura. Por ejemplo, el testigo pre-compartido se puede usar como una clave de cifrado simétrica, y los elementos de datos de identificación pueden cifrarse utilizando el testigo pre-compartido. En otras realizaciones, los elementos de datos de identificación 25 no pueden cifrarse antes de su transmisión al servidor 2.

Los elementos de datos de identificación cifrados 26 se transmiten desde el dispositivo móvil 1 al servidor 2. En la etapa S10, el servidor 2 recibe los elementos de datos de identificación cifrados 26 y, junto con la clave privada 18, el servidor 2 descifra los elementos de datos de identificación cifrados 26 para obtener los elementos de datos 25.

Con referencia a las figuras 5 y 6, se describe a continuación el procedimiento realizado en el dispositivo móvil 1 para la obtención y transmisión de datos probatorios al servidor 2.

En la etapa S15, el dispositivo móvil 1 obtiene datos 35 que se van a utilizar con la finalidad de presentar pruebas. Los datos 35 pueden comprender una pluralidad de elementos de datos. Por ejemplo, los datos 35 pueden comprender una o más imágenes fijas obtenidas usando la cámara 1f del dispositivo móvil 1, uno o más vídeos capturados utilizando la cámara 1f, uno o más registros de sonido obtenidos con el micrófono 1g, etc. Cuando los datos 35 comprenden una o más grabaciones de vídeo, la una o más de las grabaciones de vídeo pueden separarse en las respectivas tramas.

El procedimiento pasa a la etapa S16 en la que se selecciona un primer elemento de datos a partir de los datos 35. En la etapa S17 el elemento de datos se combina con el testigo 21 con el fin de generar un elemento de datos modificado 36. El testigo 21 se puede combinar con el elemento de datos de cualquier forma apropiada, tal como, por ejemplo, anteponiendo, añadiendo o distribuyendo el testigo a través de todo el elemento de datos de acuerdo con un esquema predeterminado conocido tanto para el dispositivo móvil 1 como para el servidor 2. El procedimiento pasa de la etapa S17 a la etapa S18 en el que un valor hash 37 se genera basándose en el elemento de datos modificado 36. El valor hash 37 se puede generar usando cualquier algoritmo hash apropiado. Como ejemplos solamente, el algoritmo hash SHA1 o SHA2 ampliamente utilizado, o el algoritmo SHA3 más reciente, se pueden utilizar.

El procedimiento pasa de la etapa S18 a la etapa S19 en la que se determina si hay algún elemento de datos adicionales en los datos 35. Si se determina que hay más elementos de datos, el procedimiento pasa de la etapa S19 a la etapa S20 en el que la se selecciona el próximo elemento de datos. El procedimiento pasa de la etapa S20 a la etapa S17. Por lo tanto, El procedimiento genera un bucle entre las etapas S17 a S20 hasta que cada uno de los elementos de datos en los datos 35 se ha tratado con el fin de generar una pluralidad de respectivos elementos de datos modificados 36 y una pluralidad correspondiente de valores hash 37.

Cuando se determina en la etapa S19 que todos los elementos de datos en los datos 35 se han procesado, el procedimiento pasa a la etapa S21, en la que se genera un único valor hash 38 partir de un paquete que comprende cada elemento de datos en los datos 35. Los paquetes de datos pueden comprender, además, los valores hash 37. El valor hash 38 puede generarse adicional o alternativamente a partir de los datos 35 combinados de alguna forma conocida con el testigo 21.

En la etapa S22, los datos 35, junto con los valores hash 37 y el valor hash 38 se transmiten al servidor 2. Mediante la transmisión de cada uno de los valores hash 37, junto con el valor hash 38, el servidor 2 es capaz de realizar una comprobación inicial (basándose en el valor hash 38) de que los datos 35 no se han modificado. En particular, tras la recepción de los datos 35, el servidor 2 es capaz de calcular un valor hash que debe, tener el mismo valor que el valor hash 38. Si se descubre que los datos se han modificado o dañado, (porque el valor hash calculado por el servidor 2 no coincide con el valor hash 38), debido a que cada uno de los valores hash 37 se transmite también, es posible que el servidor 2 identifique posteriormente con exactitud cuál de los elementos de datos en los datos 35 se ha modificado, dañado, o no transmitido por el dispositivo móvil 1.

Adicionalmente, uno o más identificadores 25' se pueden transmitir junto con los datos probatorios en la etapa S22. Los identificadores 25' pueden denominarse identificadores de transacción (puesto que se transmiten durante una transacción) para distinguirlos de los identificadores 25 que pueden referenciarse como identificadores de inicialización (puesto que se transmiten durante un procedimiento de inicialización).

Los identificadores 25' pueden comprender uno o más de los mismos identificadores 25 que se transmiten al servidor 2 en la etapa S10 de la Figura 3. Por ejemplo, el servidor 2 puede solicitar, durante una transacción, uno o identificadores más específicos (tales como el número IMEI del dispositivo móvil 1), o puede solicitar que los identificadores correspondientes a cada uno de los identificadores 25 se incluyan en los identificadores 25'. Como se ha descrito anteriormente, si bien los identificadores 25' pueden incluir uno o más del mismo tipo de identificador incluido en los identificadores 25 (por ejemplo, identificadores de tipo 'fecha'), es de esperar que el valor de uno o más de los identificadores pueda diferir entre los identificadores 25 y los identificadores 25'. Como se ha descrito anteriormente, los identificadores que se espera que difieran pueden referirse como identificadores variables.

Al igual que los elementos de datos en los datos 35, cada uno de los identificadores 25' puede, además, combinarse con el testigo 21 y los valores hash calculados a partir del mismo con el fin de crear un paquete de valores hash d 39 del identificador, que puede transmitirse al servidor 2. En algunas realizaciones uno o más de los valores hash 39 se transmiten en lugar del identificador 25' correspondiente. Por ejemplo, cuando el identificador 25' es un identificador estático (tal como un número IMEI, que puede esperarse que sea el mismo que era cuando se envió el identificador correspondiente 25), un hash 39 del identificador estático puede transmitirse al servidor 2, en lugar de volver a enviar el identificador. Cuando el identificador estático se modificar primero utilizando el testigo 21. De esta manera, el servidor 2 puede realizar otras comprobaciones para mejorar la confianza de que el dispositivo que transmite los identificadores 25' es el dispositivo móvil 1.

El procedimiento de la Figura 5 es tal que cuando los datos 35 se utilizan como prueba, que puede ser después de un período de almacenamiento en el servidor 2, el servidor 2 puede determinar que los datos 35 no se han manipulado o de otro modo dañado (es decir, que los datos 35 son adecuados para usos probatorios). En particular, como describe

a continuación con referencia a la Figura 7, solo el servidor 2 es capaz de volver a crear los valores hash 37, 38 basándose en los datos recibidos. Es decir, puesto que solo el servidor 2 conoce el valor del testigo 21 (y el esquema utilizado para combinar el testigo 21 con los elementos de datos de los datos 35), solo el servidor es capaz de recrear los valores hash. Como tal, el éxito de la re-creación de los valores hash 37, 38 en el servidor 2 es prueba de que los elementos de datos son auténticos y están sin modificar. Además, los identificadores 25' y/o los valores hash del identificador 39 se pueden usar para confirmar aún más la identidad del dispositivo móvil 1.

Además de, o como alternativa a, que se transmiten al servidor 2, los valores hash 37, 38, 39 pueden transmitirse a un tercero independiente para su almacenamiento seguro hasta un tiempo tal en que se requiera la verificación de los datos 35. Cuando tanto el servidor 2 como un tercero reciben los valores hash 37, 38, 39, la verificación de los datos 35 se puede realizar tanto por el servidor 2 como por el tercero de forma independiente. En una realización, algunos o todos los valores hash 37, 38, 39 solo se envían al tercero. En algunas realizaciones, el servidor transmite el testigo 21 a un tercero que puede ser el mismo o un tercero distinto del que recibe los valores hash 37, 38, 39. Se puede ver por lo tanto, que la verificación independiente de los datos 35 puede proporcionarse mediante el uso de terceros no relacionados con el usuario del dispositivo móvil 1 o la entidad asociada con el servidor 2.

La Figura 7 ilustra el procedimiento que puede realizarse en el servidor 2 después de la recepción de los datos probatorios desde el dispositivo móvil 1 a través del procedimiento de la Figura 6. Se apreciará que el procedimiento de la Figura 7, o un procedimiento similar pueden realizarse en cualquier etapa después de la recepción de los datos desde el dispositivo móvil 1. Por ejemplo, el procedimiento de la Figura 7 (o similar) puede aplazarse hasta que los datos se vayan a utilizar de una manera probatoria. Por ejemplo, en el ejemplo anterior del seguro de vehículo, el procedimiento para determinar la veracidad, autenticidad y fiabilidad de los datos recibidos desde el dispositivo móvil 1 pueden diferirse hasta que una reclamación particular se procese por un agente de la aseguradora, por ejemplo.

Haciendo referencia a la Figura 7, en la etapa S30, los datos enviados por el dispositivo móvil 1 se reciben en el servidor 2. Como se ha descrito anteriormente, los datos transmitidos por el dispositivo móvil 1 comprenden los datos que se va a utilizar como prueba, junto con una pluralidad de valores hash 37 (un valor hash respectivo para cada elemento de datos) y un único valor hash 38 que representa los datos como un paquete (que puede o no puede combinarse con el testigo 21). El procedimiento pasa desde la etapa S30 a la etapa S31 en la que el servidor 2 calcula al menos un valor hash basándose en los datos recibidos y el testigo 21 almacenado en el servidor 2.

En particular, el servidor 2 puede calcular primero solo el valor hash 38. Los valores hash respectivos para cada uno de los elementos de datos recibidos pueden calcularse solo en el caso de que el valor hash 38 no pueda recrearse por el servidor 2 con el fin de determinar qué datos son sospechosos. En otras realizaciones, el servidor 2 puede calcular todos los valores hash desde el principio.

Después de calcular los valores hash, el procedimiento pasa a la etapa S32 en la que los valores hash calculados por el servidor 2 se comparan con los valores hash recibidos desde el dispositivo móvil 1. Si se determina en la etapa S32 que los valores hash calculados por el servidor 2 no coinciden con los valores hash recibidos desde el dispositivo móvil 1, esto indica que los datos recibidos pueden, por ejemplo, haberse modificado, corrompido durante su transmisión, u originados a partir de un dispositivo que no era el dispositivo móvil 1 (de manera que el otro dispositivo no conocía el valor del testigo pre-compartido 21). Cuando los valores hash no coinciden, esto puede indicar que los datos recibidos en el servidor 2 no son adecuado para su uso como prueba. El procedimiento pasa de la etapa S32 a la etapa S33.

En la etapa S33, se proporciona una indicación (por ejemplo, una indicación puede representarse en la pantalla 2e del servidor 2, representarse en la pantalla 1e del dispositivo móvil 1, y/o guardarse junto con los datos recibidos en el servidor 2) de que los valores hash calculados no coinciden con los valores hash recibidos. Se apreciará que el procedimiento adicional puede realizarse después de la determinación en la etapa S32 de que los valores hash no coinciden. Por ejemplo, los datos recibidos pueden ser rechazados, y un mensaje puede enviarse del servidor 2 al dispositivo móvil 1 solicitando que se retransmitan los datos. Otros procedimientos que pueden realizarse serán fácilmente evidentes para el experto.

Si, por otro lado, se determina en la etapa S32 que los valores hash calculados por el servidor 2 sí coinciden con los valores hash recibidos desde el dispositivo móvil 1, el procedimiento pasa de la etapa S32 a la etapa S34 en la que se determina si el uno o más de los identificadores 25' coincide con los identificadores 25 que fueron enviados desde el dispositivo móvil 1 al servidor 2 durante el procedimiento de la Figura 3 y/o si los valores hash 39 del identificador coinciden con los valores hash correspondientes calculados por el servidor 2 basándose en los identificadores 25 recibidos durante el procedimiento de la Figura 3. Se ha de entender que no todos los identificadores se comprueban necesariamente en la etapa S34.

Si se determina en la etapa S34 que el uno o más identificadores examinados 25' no coinciden con los identificadores correspondientes 25 y/o que los valores hash 39 del identificador no coinciden con los valores hash calculados por el servidor 2 basándose en los identificadores 25 correspondientes, el procedimiento pasa de la etapa S34 a la etapa S35, en la que se proporciona la indicación (por ejemplo, una indicación puede emitirse en el servidor 2, emitirse en el dispositivo móvil 1, o guardarse junto con los datos recibidos) de que los identificadores 25 no coinciden con el identificadores 25' y/o de que los valores hash calculados no coinciden con los valores hash recibidos 39. Se apreciará

que el procedimiento adicional puede realizarse en la etapa S35. Por ejemplo, los datos pueden ser rechazados, y un mensaje puede enviarse desde el servidor 2 al dispositivo móvil 1 solicitando que se retransmitan los datos.

Si, por otro lado, se determina en la etapa S34 que los identificadores recibidos 25' coinciden con los identificadores almacenados 25, y/o que los valores hash 39 del identificador coinciden con los valores hash calculados, el procedimiento pasa a la etapa S36, en la que los datos recibidos se almacenan para su uso posterior. El almacenamiento de los datos puede ser, por ejemplo, tanto en el dispositivo de almacenamiento 4 como en el dispositivo de almacenamiento 5. Los datos almacenados en el dispositivo de almacenamiento 4 pueden ser accesibles (por ejemplo para su visualización, anotación, modificación, etc.) para el dispositivo móvil 1, mientras que los datos almacenados en el dispositivo de almacenamiento 5 pueden ser inaccesibles para el dispositivo móvil 1. De esta manera, los datos almacenados en el dispositivo de almacenamiento 5 se pueden usar para confirmar que los datos almacenados en el dispositivo móvil 4 no se han modificado de tal manera que ya no se pueden utilizar con fines probatorios.

Después de cada recepción de datos, un nuevo testigo puede intercambiarse entre el servidor 2 y el dispositivo móvil 1 en una etapa S35. Como se ha descrito anteriormente con referencia al procedimiento de la Figura 3, un nuevo testigo puede generarse e intercambiarse en cualquier forma apropiada. Por ejemplo, un nuevo testigo puede seleccionarse al azar por uno del servidor 2 o el dispositivo móvil 1 y transmitirse al otro dispositivo usando criptografía de clave pública. Como alternativa, el servidor 2 puede emitir un nuevo testigo al dispositivo móvil 1, en el que el dispositivo móvil 1 introduce la información conocida solo por el dispositivo móvil 1 y el servidor 2 (tal como uno de los identificadores 25, 25', un número de transacción, etc.).

Un registro ordenado se puede mantener en el servidor 2 de todos los testigos que se han emitido en el dispositivo móvil 1. Por ejemplo, un registro de cada testigo se puede almacenar junto con el tiempo en el que esa señal fue emitida al dispositivo móvil 1. El registro puede almacenar una indicación de la una o más transacciones particulares para las que el testigo es válido. De esta manera, si la comunicación entre el dispositivo móvil 1 y el servidor 2 se intercepta de tal manera que un tercero es capaz de reutilizar un testigo interceptado en más comunicaciones, por comparación con el registro almacenado de testigos emitidos en el dispositivo móvil 1, el servidor 2 es capaz de determinar que el testigo usado por el tercero está demasiado cargado y/o se utiliza fuera de orden.

Se apreciará, que incluso en el caso de que los datos 35 se identifiquen como originándose desde el dispositivo móvil 1, y como que no han sido modificados o dañados antes de su recepción en el servidor 2, se puede desear además determinar que los datos 35 son dignos de confianza (es decir, que el usuario del dispositivo móvil 1 no ha fabricado los datos 35). Como se describirá en más detalle a continuación, los identificadores 25' pueden, además, usarse para proporcionar indicaciones en cuanto a si los datos 35 son de confianza.

Después de la recepción de datos desde el dispositivo móvil 1 durante una transacción, el servidor 2 puede realizar el procedimiento de fondo para comparar los identificadores 25 con los identificadores 25' para determinar si los identificadores 25' son válidos o plausibles en vista de los identificadores 25. Por ejemplo, cuando los identificadores 25 y 25' incluyen, cada uno, uno o más identificadores basados en el tiempo (como una hora o fecha actual), se puede determinar si los identificadores basados en el tiempo en los identificadores 25 preceden a los identificadores basados en el tiempo en los identificadores 25'. Como un ejemplo adicional, cuando los identificadores 25, 25' incluyen cada uno un identificador basado en la ubicación (tal como una ubicación de GPS, una ubicación de celda actual, etc.) se puede determinar si es factible que el dispositivo móvil 1 podría haber alcanzado la ubicación indicada en los identificadores 25' dada la ubicación indicada en los identificadores 25. Determinar si una ubicación es factible puede comprender la comparación de una distancia entre las ubicaciones identificadas en cada uno de los identificadores 25, 25' con respecto a una indicación de tiempo. Como otro ejemplo, cuando los identificadores 25, 25' incluyen identificadores de hardware del dispositivo móvil 1 (por ejemplo, número de serie de la batería, el tiempo de actividad, el número IMEI del teléfono, el último reinicio, hora de inicio, etc.), se pueden hacer comparaciones para identificar las inconsistencias.

Se apreciará que una pluralidad de comprobaciones de coherencia puede realizarse basándose en los identificadores 25, 25'. Se apreciará además que en muchos casos, los datos recibidos en el servidor 2 pueden aceptarse para su almacenamiento incluso en el caso de inconsistencias en los identificadores 25, 25', cuando las inconsistencias se observan meramente junto con los datos recibidos de modo que las inconsistencias identificadas pueden ser tomadas en cuenta al evaluar si los datos recibidos son adecuados para su uso como prueba. En otras realizaciones, sin embargo, las inconsistencias determinadas se pueden usar para rechazar automáticamente los datos recibidos y/o activar otro procedimiento tal como solicitudes de información adicional.

Se ha descrito anteriormente que el proceso de inicialización comprende el intercambio de identificadores que se utilizan para la comparación en otras transacciones. En otras realizaciones, la inicialización no comprende la transmisión de dichos identificadores. En algunas realizaciones los identificadores se pueden transferir durante cada transacción y se comparan a través de diferentes transacciones.

En algunas realizaciones, los identificadores son transferidos fuera de transacciones o procedimientos de inicialización, de manera que el servidor 2 mantiene una copia regularmente actualizada de los identificadores

correspondientes. Por ejemplo, una aplicación que opera en el dispositivo móvil 1 se puede disponer para transferir uno o más identificadores en el servidor 2 en las operaciones de procedimiento de fondo. Como alternativa, la aplicación puede solicitar a un usuario del dispositivo móvil 1 autorizar la transmisión de identificadores fuera de las transacciones iniciadas por el usuario. Tales instrucciones u operaciones de procedimiento de fondo pueden estar a intervalos regulares o aleatorios.

Se apreciará que los aspectos pueden implementarse en cualquier forma conveniente incluyéndose a modo de hardware y/o software adecuado. Por ejemplo, los dispositivos dispuestos para implementar las realizaciones pueden crearse usando componentes de hardware apropiados. Como alternativa, un dispositivo programable, tal como un ASIC, se puede programar para implementar las realizaciones.

La invención proporciona, por tanto, también programas informáticos adecuados para implementación de aspectos. Tales programas informáticos pueden llevarse en medios portadores adecuados incluyendo medios portadores tangibles (por ejemplo, discos duros, CD-ROM, etc.) y medios portadores intangibles tales como señales de comunicaciones.

Se apreciará además que si bien las realizaciones a modo de ejemplo se han descrito anteriormente, se pueden hacer modificaciones a esos ejemplos sin apartarse del alcance de las reivindicaciones adjuntas.

REIVINDICACIONES

1. Un método para proporcionar datos probatorios, que comprende en un dispositivo móvil:

establecer uno o más primeros testigos secretos con un servidor;
obtener uno o más elementos de datos de uno o más sensores;
combinar el uno o más elementos de datos con al menos uno del uno o más primeros testigos secretos para proporcionar uno o más elementos de datos modificados;
generar un primer valor hash respectivo para cada uno del uno o más elementos de datos modificados;
generar un segundo valor hash para un conjunto de datos que comprende cada uno del uno o más elementos de datos; y
transmitir al servidor un primer mensaje que comprende el uno o más elementos de datos, el uno o más primeros valores hash y el segundo valor hash;
establecer uno o más segundos testigos secretos con el servidor después de la transmisión del primer mensaje, el uno o más segundos testigos secretos para combinarse con uno o más segundos elementos de datos obtenidos a partir del uno o más sensores para generar un segundo mensaje;
obtener uno o más identificadores de transacción, incluyendo el uno o más identificadores de transacción uno o más identificadores estáticos, en donde cada identificador estático es adecuado para identificar una propiedad estática del dispositivo móvil; y
transmitir una indicación de los identificadores estáticos al servidor, incluyendo la generación de un tercer valor hash respectivo para cada uno del uno o más identificadores estáticos, en donde la indicación incluye los terceros valores hash,
en donde los uno o más primeros testigos secretos se establecen antes de transmitir el primer mensaje que comprende el uno o más elementos de datos.

2. El método de la reivindicación 1, en el que el cálculo de cada tercer valor hash respectivo comprende modificar cada uno de la pluralidad de identificadores estáticos con al menos uno del uno o más primeros testigos secretos y calcular cada uno de dichos terceros valores hash basándose en los identificadores estáticos modificados.

3. El método de cualquier reivindicación anterior, en el que los identificadores de transacción comprenden uno o más identificadores variables y en el que cada identificador variable es adecuado para identificar una propiedad variable del dispositivo móvil; y
en donde la transmisión de una indicación de los identificadores variables al servidor comprende la transmisión del identificador variable al servidor.

4. El método de cualquier reivindicación anterior, que comprende además un procedimiento de inicialización, comprendiendo el procedimiento de inicialización transmitir una pluralidad de identificadores de inicialización al servidor.

5. El método de la reivindicación 4, en el que los identificadores de inicialización presentan uno o más identificadores estáticos y/o uno o más identificadores variables.

6. El método de cualquier reivindicación anterior, en el que el uno o más sensores comprenden al menos un sensor de entre el grupo que comprende una cámara del dispositivo móvil y un micrófono del dispositivo móvil.

7. El método de cualquier reivindicación anterior, en el que el uno o más elementos de datos comprenden al menos uno de: una o más imágenes fijas, uno o más vídeos y una o más grabaciones de sonidos.

8. El método de cualquier reivindicación anterior, en el que el uno o más identificadores estáticos comprenden al menos un identificador del grupo que comprende un número de identificación de una batería del dispositivo móvil, un número IMEI del dispositivo móvil, número de teléfono del dispositivo móvil.

9. El método de la reivindicación 3 o de cualquier reivindicación dependiente de la misma, en el que el uno o más identificadores variables comprenden al menos un identificador del grupo que comprende una ubicación geográfica del dispositivo móvil, una fecha y hora reportados por el dispositivo móvil, una duración desde el momento en donde dispositivo móvil se enciende, una indicación de otros dispositivos detectados por el dispositivo móvil y una estructura de archivos del dispositivo móvil.

10. Un método para recibir datos probatorios que comprende, en un servidor:

establecer uno o más primeros testigos secretos con un dispositivo móvil;
recibir uno o más primeros elementos de datos, uno o más primeros valores hash y un segundo valor hash desde el dispositivo móvil en un primer mensaje utilizable por el servidor para autenticar el uno o más elementos de datos, el uno o más primeros elementos de datos obtenidos a partir de uno o más sensores;
en donde cada uno del uno o más primeros valores hash son valores hash generados basándose en uno respectivo del uno o más elementos de datos modificados con al menos uno del uno o más primeros testigos secretos; y

en donde el segundo valor hash es un valor hash generado basándose en un conjunto de datos que comprende cada uno del uno o más elementos de datos;
establecer uno o más segundos testigos secretos con el dispositivo móvil después de la transmisión del primer mensaje, el uno o más segundos testigos secretos para ser combinados por el dispositivo móvil con uno o más segundos elementos de datos obtenidos a partir del uno o más sensores para generar un segundo mensaje;
recibir desde el dispositivo móvil una pluralidad de identificadores de inicialización que incluyen un primer identificador estático adecuado para identificar una propiedad estática del dispositivo móvil;
recibir uno o más identificadores de transacción desde el dispositivo móvil, incluyendo los identificadores de transacción una indicación de un identificador estático correspondiente que incluye un tercer valor hash basándose en el identificador estático correspondiente; y
comparar el primer identificador estático con el identificador estático correspondiente, incluyendo la generación de un cuarto valor hash basándose en el primer identificador estático y comparar el cuarto valor hash con el tercer valor hash;
en donde el uno o más primeros testigos secretos se establecen antes de transmitir el primer mensaje que comprende el uno o más elementos de datos.

11. El método de la reivindicación 10, que comprende además:

modificar cada uno del uno o más elementos de datos recibidos con al menos uno del uno o más primeros testigos secretos;
generar un primer valor hash de comparación respectivo para cada uno del uno o más elementos de datos modificados recibidos;
comparar cada primer valor hash de comparación respectivo con uno correspondiente de los primeros valores hash; y
proporcionar una indicación para cada primer valor hash de comparación respectivo que no coincida con uno correspondiente de los primeros valores hash.

12. El método de la reivindicación 10, en el que el tercer valor hash fue generado por el dispositivo móvil mediante la modificación del identificador estático correspondiente con al menos uno del uno o más primeros testigos secretos y el cálculo de cada uno de los terceros valores hash basándose en el identificador estático correspondiente modificado; y
en el que generar el cuarto valor hash comprende modificar el primer identificador estático con al menos uno del uno o más primeros testigos secretos y calcular el cuarto valor hash basándose en el primer identificador estático modificado.

13. El método de una cualquiera de las reivindicaciones 10 a 12, en el que los identificadores de inicialización comprenden un primer identificador variable adecuado para indicar propiedades variables del dispositivo móvil;
en donde los identificadores de transacción recibidos comprenden un identificador variable correspondiente; y
en donde la comparación del primer identificador variable con el identificador variable correspondiente comprende determinar si una diferencia entre el primer identificador variable y el segundo identificador variable está dentro de límites predeterminados.

14. El método de una cualquiera de las reivindicaciones 10 a 13, que comprende además el establecimiento de uno o más segundos testigos secretos con el dispositivo móvil después de la recepción del uno o más elementos de datos y dicho primer y segundo valores hash.

15. Aparato para el procesamiento de datos probatorios, que comprende:

una memoria que almacena instrucciones legibles por ordenador configurada para hacer que un ordenador realice un método de acuerdo con cualquier reivindicación anterior; y
un procesador configurado para ejecutar las instrucciones legibles por ordenador.

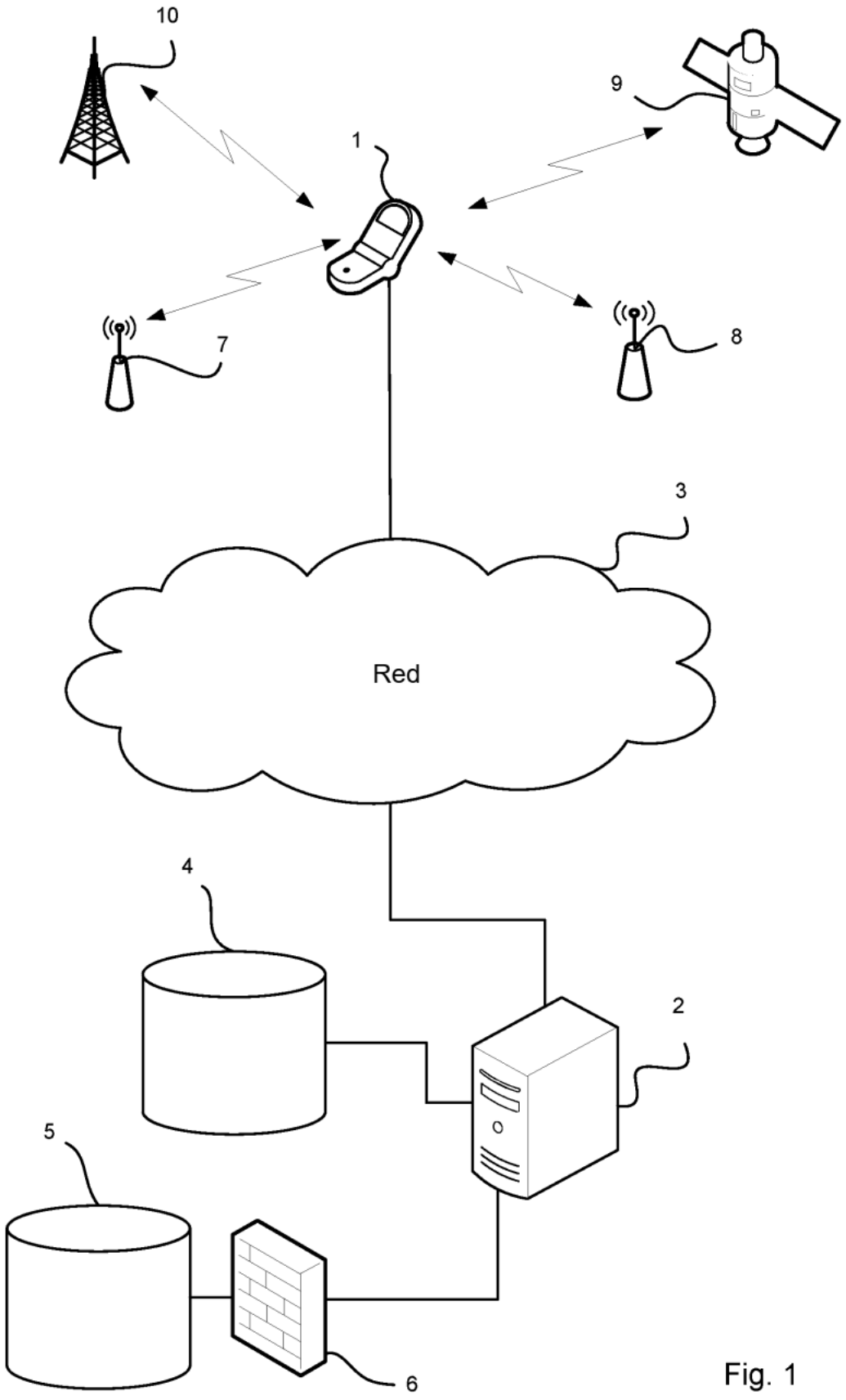

Fig. 1

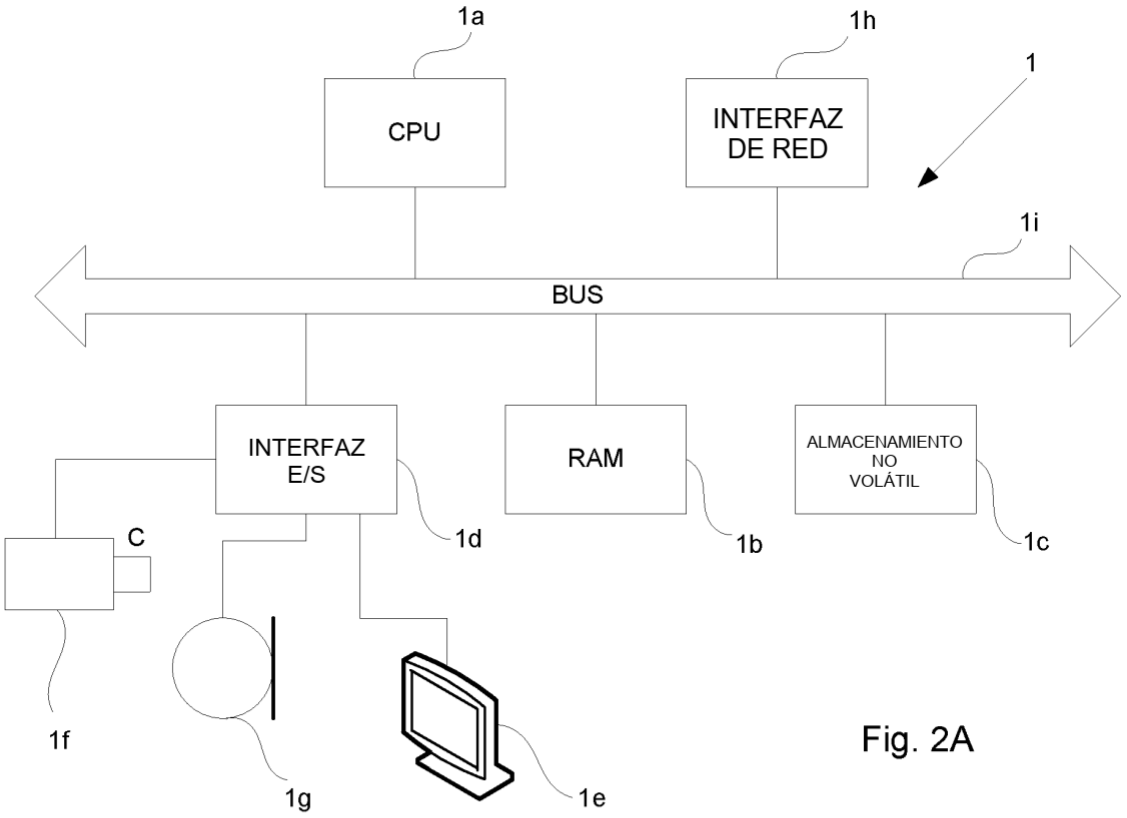
1a
1h
1
CPU
INTERFAZ DE RED
1i
BUS
INTERFAZ E/S
RAM
ALMACENAMIENTO NO VOLÁTIL
C
1d
1b
1c
1f
1g
1e

Fig. 2A

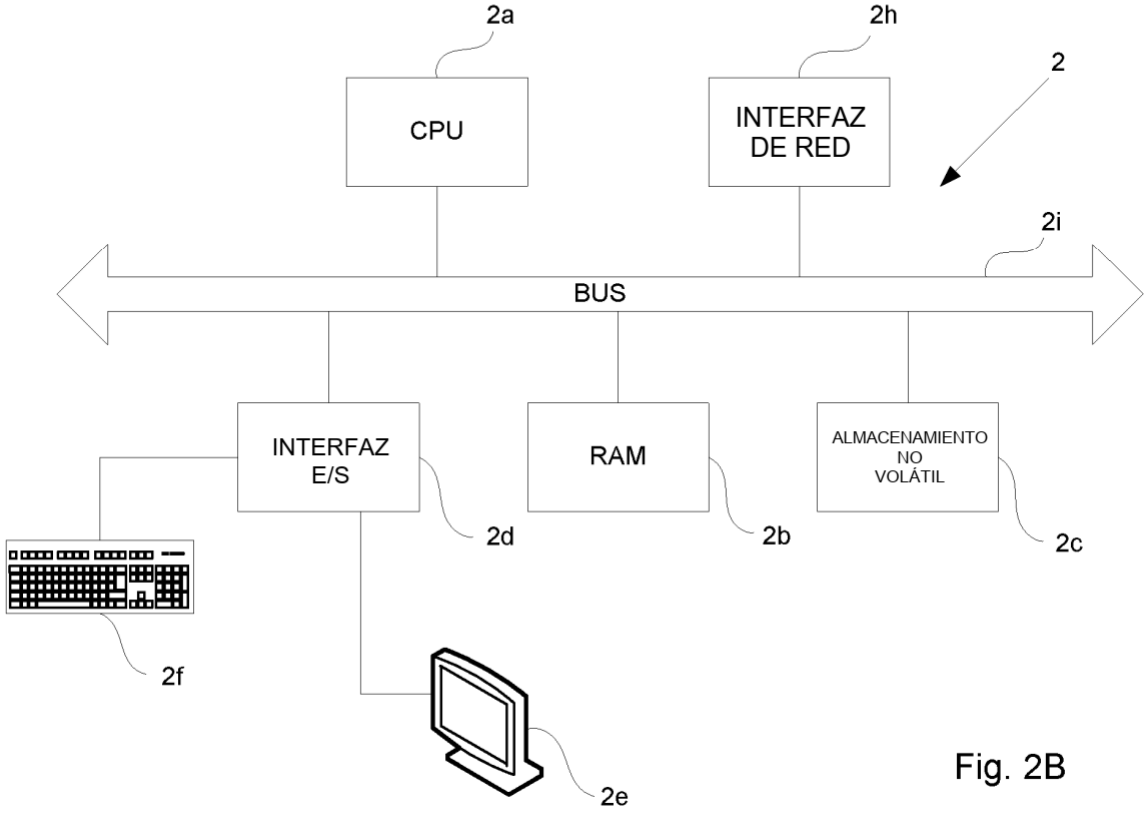
2a
2h
2
CPU
INTERFAZ DE RED
2i
BUS
INTERFAZ E/S
RAM
ALMACENAMIENTO NO VOLÁTIL
2d
2b
2c
2f
2e

Fig. 2B

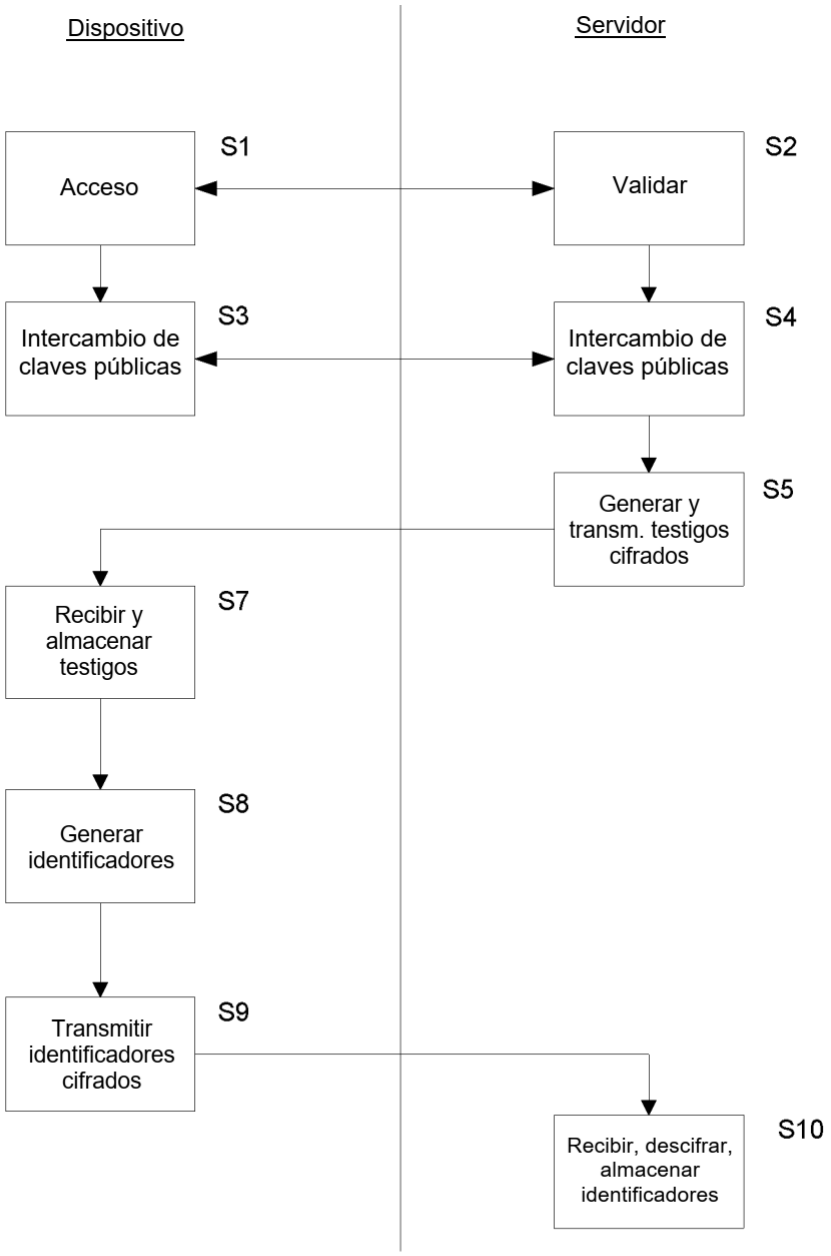
Dispositivo
Servidor
Acceso
S1
Validar
S2
Intercambio de claves públicas
S3
Intercambio de claves públicas
S4
Generar y transm. testigos cifrados
S5
Recibir y almacenar testigos
S7
Generar identificadores
S8
Transmitir identificadores cifrados
S9
Recibir, descifrar, almacenar identificadores
S10

Fig. 3

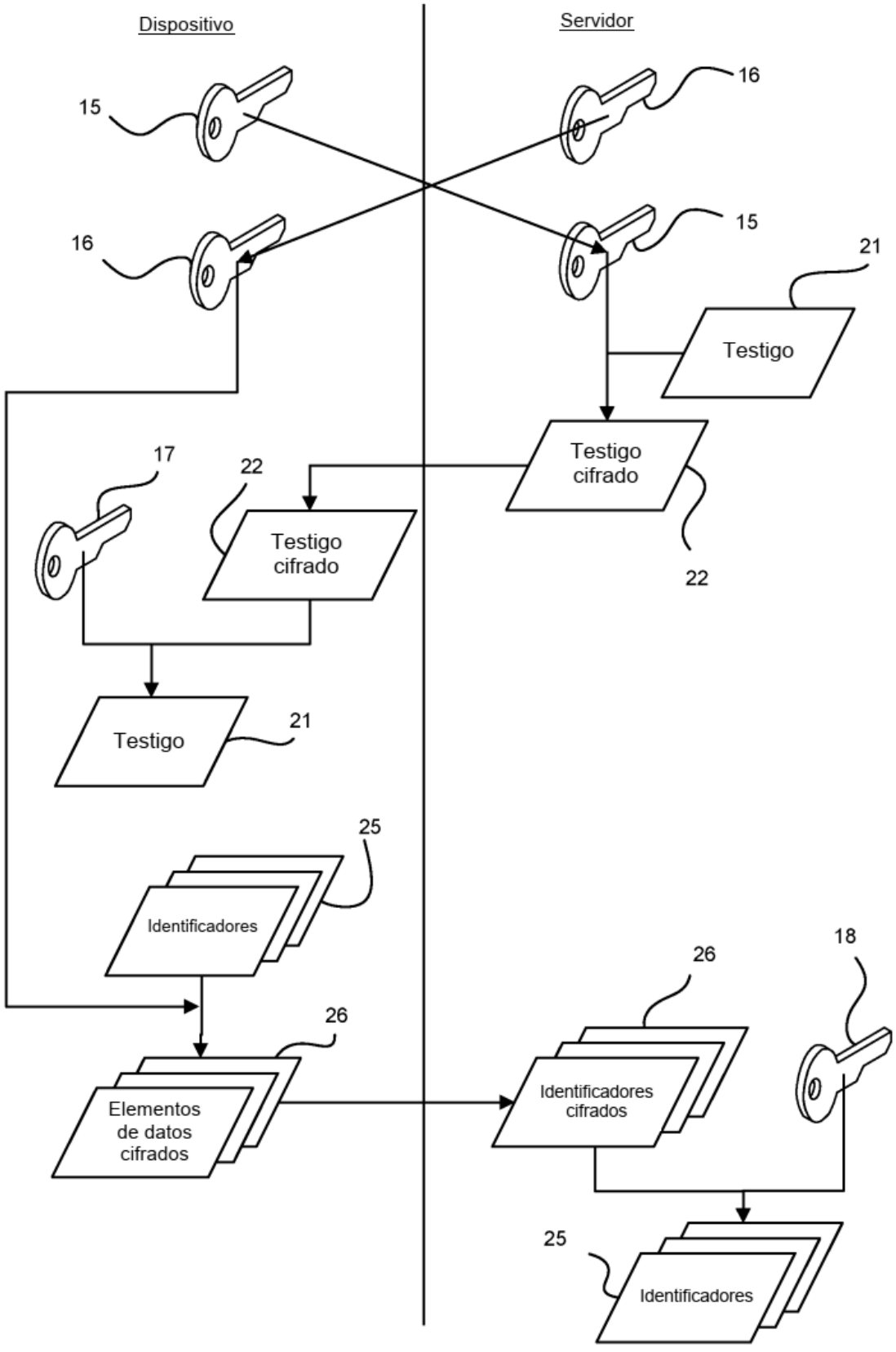
Dispositivo
Servidor
15
16
16
15
21
Testigo
Testigo cifrado
22
17
22
Testigo cifrado
Testigo
21
25
Identificadores
26
Elementos de datos cifrados
26
18
Identificadores cifrados
25
Identificadores

Fig. 4

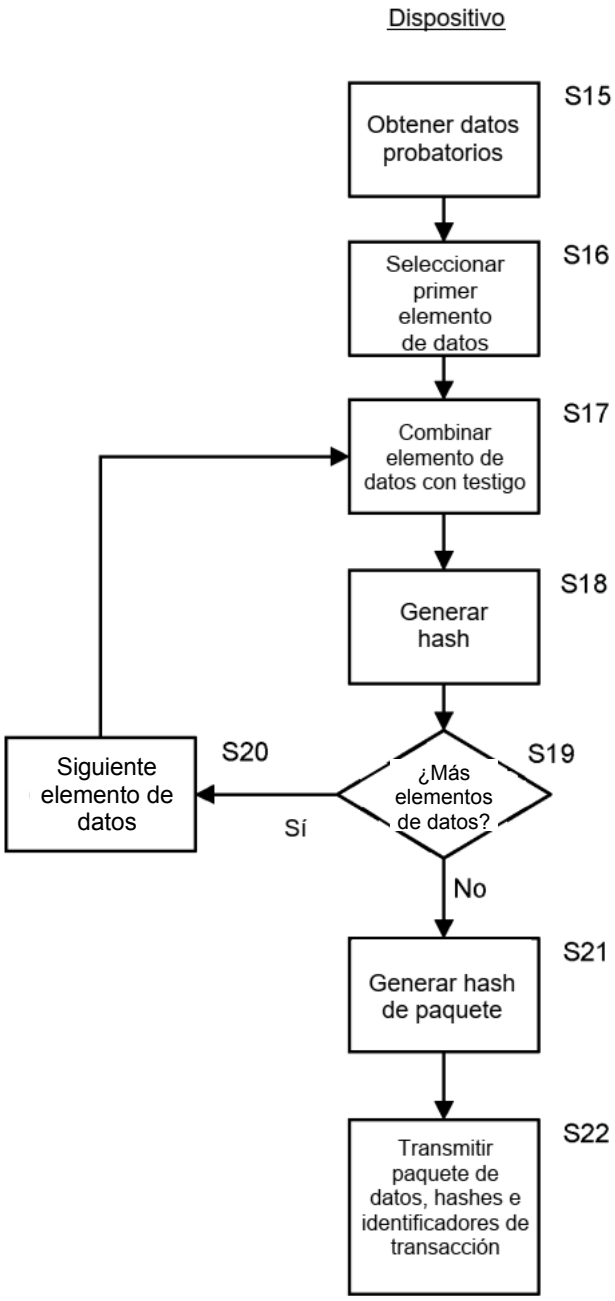
Dispositivo
Obtener datos probatorios
S15
Seleccionar primer elemento de datos
S16
Combinar elemento de datos con testigo
S17
Generar hash
S18
¿Más elementos de datos?
S19
Sí
Siguiente elemento de datos
S20
No
Generar hash de paquete
S21
Transmitir paquete de datos, hashes e identificadores de transacción
S22

Fig. 5

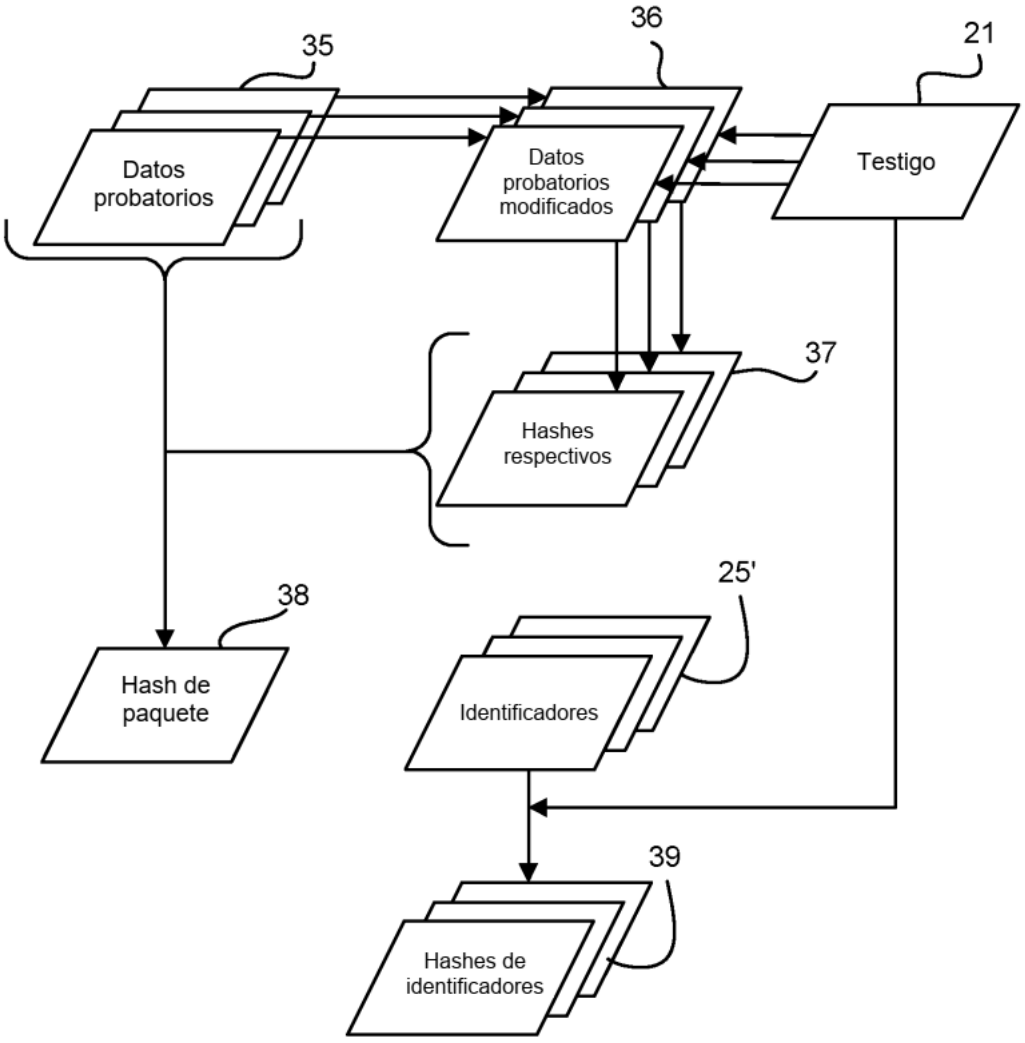
35
36
21
Datos probatorios
Datos probatorios modificados
Testigo
37
Hashes respectivos
38
25'
Hash de paquete
Identificadores
39
Hashes de identificadores

Fig. 6

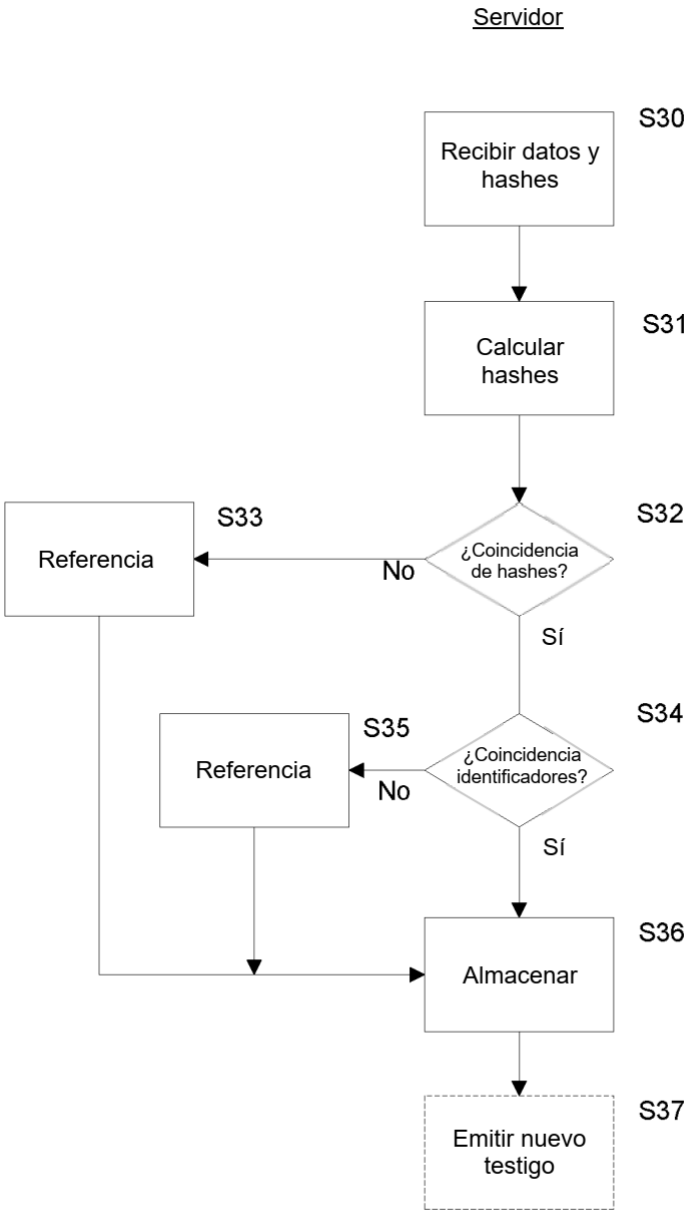
Servidor
S30
Recibir datos y hashes
S31
Calcular hashes
S32
¿Coincidencia de hashes?
No
S33
Referencia
Sí
S34
¿Coincidencia identificadores?
No
S35
Referencia
Sí
S36
Almacenar
S37
Emitir nuevo testigo

Fig. 7