(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 989 067**

(51) Int. Cl.:

H04L 9/08 (2006.01)
H04L 9/32 (2006.01)
H04L 9/40 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **25.05.2022 E 22175341 (1)**

(97) Fecha y número de publicación de la concesión europea: **17.07.2024 EP 4283918**

(54) Título: **Procedimientos y disposiciones para habilitar comunicaciones digitales seguras dentro de un grupo**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
25.11.2024

(73) Titular/es:

GURULOGIC MICROSYSTEMS OY (100.0%)
Linnankatu 34
20100 Turku, FI

(72) Inventor/es:

KÄRKKÄINEN, TUOMAS

(74) Agente/Representante:

DURAN-CORRETJER, S.L.P

DESCRIPCIÓN

Procedimientos y disposiciones para habilitar comunicaciones digitales seguras dentro de un grupo.

SECTOR TÉCNICO DE LA INVENCIÓN

La invención se refiere, en general, al sector técnico de la seguridad necesaria al utilizar servicios digitales dentro de un grupo de dos o más partes. El particular, la invención se refiere a la tarea de establecer de manera central confianza entre partes que pueden, a continuación, depender de la confianza establecida de manera central en comunicaciones de grupo u otras clases de utilización de servicios digitales relacionada con grupos.

ESTADO DE LA TÉCNICA ANTERIOR

La seguridad en las comunicaciones digitales involucra múltiples aspectos, tales como confidencialidad (solamente las partes autorizadas pueden acceder a un fragmento de información), autenticación (una parte en comunicación tiene que asegurarse de con quién está comunicando), integridad (un fragmento de información no ha sido modificado de manera no permitida) y no repudio (una parte no puede negar con éxito haber enviado un determinado fragmento de información). Una subdivisión de las comunicaciones digitales son las comunicaciones de grupo, es decir, las comunicaciones digitales y/o el uso de otros servicios digitales entre los miembros de un grupo predefinido. Los miembros del grupo deben tener acceso a las comunicaciones específicas del grupo de la manera más fácil y fiable posible, garantizándose simultáneamente que las partes externas al grupo no pueden acceder a las comunicaciones o interferir de otro modo con estas. Debido a su dependencia inherente de las aplicaciones criptográficas, cualquier grupo de la clase a que se hace aquí referencia puede denominarse un grupo criptográfico digital.

Por lo menos, se conocen dos enfoques básicos para comunicaciones de grupo. En una solución centralizada, todas las comunicaciones entre los miembros del grupo son enrutadas a través de un servidor o un punto de servicios centralizados similar. En ese caso, el servidor puede tener una responsabilidad considerable en la autenticación de los participantes y la realización de las operaciones necesarias de cifrado y descifrado. El otro enfoque es una solución distribuida, en la que las comunicaciones pueden discurrir directamente entre los miembros. La solución distribuida requiere que los dispositivos de usuario tengan acceso a determinado o determinados secretos compartidos, para proporcionar la seguridad necesaria.

Las soluciones centralizadas tienen, por lo menos, el inconveniente de que dependen completamente del acceso continuo al servidor para todos los miembros activos del grupo. En las soluciones distribuidas, por otra parte, ha resultado ser problemático encontrar una manera económica y computacionalmente razonable de distribuir el secreto compartido. Por ejemplo, en el conocido procedimiento de Diffie-Hellman, las partes se tienen que poner de acuerdo sobre el orden en que las claves públicas se proporcionan para su procesamiento, con el fin de habilitar a cada parte para calcular el secreto compartido común al grupo. Asimismo, muchas soluciones distribuidas conocidas son ineficientes en la manera de establecer un nivel suficiente de confianza entre las partes, lo que puede hacer dichas soluciones vulnerables a ataques maliciosos. Otros inconvenientes de muchas soluciones distribuidas están relacionados con su dependencia de una tecnología particular para utilizar el grupo criptográfico digital establecido. Sería mejor que el grupo criptográfico digital fuera independiente de la tecnología, es decir, no dependiente de ninguna tecnología particular en relación con las maneras en que el propietario y los miembros del grupo planeen utilizarlo en el futuro.

El documento de Patente US 2011/320815 constituye técnica anterior relevante.

RESUMEN

Este resumen se da conocer para presentar de forma simplificada una selección de conceptos que se describen en mayor detalle a continuación en la descripción detallada. Este resumen no pretende identificar características clave o características esenciales de la materia objeto reivindicada, ni está destinado a ser utilizado para limitar el alcance de la materia objeto reivindicada.

Es un objetivo dar a conocer procedimientos y disposiciones para establecer, utilizar y habilitar la utilización de un grupo criptográfico digital sin los inconvenientes de la técnica anterior esbozada arriba.

Según un primer aspecto, se da conocer una disposición para establecer un grupo criptográfico digital. La disposición comprende un motor criptográfico configurado para producir productos criptográficos a partir de datos de entrada dados, y un extremo de recepción y un extremo de transmisión de un mecanismo de transporte seguro acoplado a dicho motor criptográfico. Dicho motor criptográfico está configurado para responder a la recepción de, a través de dicho mecanismo de transporte seguro, una primera solicitud que contiene una serie de identificadores de usuario, produciendo un producto criptográfico. Dicho motor

criptográfico está configurado para responder a la recepción de, a través de dicho mecanismo de transporte seguro, una subsiguiente segunda solicitud que contiene uno de dicha serie de identificadores de usuario, transmitiendo dicho producto criptográfico a través de dicho mecanismo de transporte seguro. Dicho producto criptográfico es un grupo criptográfico digital que contiene dicha serie de identificadores de usuario y una clave criptográfica común para utilizar en la criptografía simétrica entre usuarios identificados mediante dicha serie de identificadores de usuario, y/o claves públicas específicas por usuario y relacionadas con el identificador de usuario, para utilizar en criptografía asimétrica en comunicaciones entre usuarios identificados mediante dicha serie de identificadores de usuario.

Según una realización, la disposición está configurada para comprobar si dicha primera solicitud contiene una respectiva clave de cifrado específica por usuario para cada uno de dicha serie de identificadores de usuario. Entonces, la disposición puede estar configurada para responder al descubrimiento de que dicha primera solicitud no contiene una respectiva clave de cifrado específica por usuario para cada uno de dicha serie de identificadores de usuario, incrementando los datos recibidos en dicha primera solicitud para que contengan una respectiva clave de cifrado específica por usuario para cada uno de dicha serie de identificadores de usuario. Esto implica, por lo menos, la ventaja de que la disposición se puede adaptar flexiblemente a situaciones en las que no todas las claves de cifrado específicas por usuario están incluidas en la primera solicitud.

Según una realización, la disposición está configurada para realizar dicho incremento solicitando a fuentes externas a la disposición respectivas claves de cifrado específicas por usuario, y recibiéndolas. Esto involucra, por lo menos, la ventaja de que la disposición puede funcionar en, y adaptarse flexiblemente a situaciones en las que no posee por sí misma las claves de cifrado específicas por usuario faltantes.

Según una realización, la disposición está configurada para comprobar un fragmento de información relacionada con el usuario recibido en la primera solicitud, con un correspondiente fragmento de información relacionada con el usuario procedente de otra fuente, con el fin de averiguar si estos fragmentos de información relacionada con el usuario concuerdan entre sí. Esto involucra, por lo menos, la ventaja de que se puede detectar el uso fraudulento, u otro inapropiado, de información relacionada con el usuario y reaccionar al mismo.

Según una realización, la disposición está configurada para responder al descubrimiento de que dichos fragmentos de información relacionada con el usuario no concuerdan entre sí, adoptando una decisión sobre si se permite que continúe el establecimiento del grupo criptográfico digital. Esto involucra, por lo menos, la ventaja de que el funcionamiento de la disposición se puede adaptar flexiblemente a diferentes clases de necesidades en relación con cómo de preciso tiene que ser cada fragmento de información.

Según una realización, la disposición está configurada para utilizar una clave de firma con el fin de firmar digitalmente elementos de información que incluye en dicho grupo criptográfico. Esto involucra, por lo menos, la ventaja de que dichos elementos de información pueden transportar un valor especial como información de confianza cuando se utilizan posteriormente.

Según una realización, la disposición está configurada para comprobar a partir de dicha subsiguiente segunda solicitud si la solicitud está destinada a sí misma o a otro receptor, y para responder al descubrimiento de que la solicitud de está destinada a otro receptor reenviando dicha subsiguiente segunda solicitud hacia dicho otro receptor. Esto involucra, por lo menos, la ventaja de que se pueden cumplir los mismos principios funcionando en un entorno en el que diferentes usuarios pueden pertenecer a los dominios administrados de diferentes proveedores de confianza.

Según una realización, la disposición está configurada para, antes de dicho reenvío, sustituir una autenticación original de dicha subsiguiente segunda solicitud con una autenticación de la propia disposición. Esto involucra, por lo menos, la ventaja de que las relaciones de confianza entre las partes se pueden mantener y utilizar apropiadamente incluso cuando se vuelve a reenviar la información.

Según un segundo aspecto, se da conocer un procedimiento para establecer un grupo criptográfico digital. El procedimiento comprende recibir, a través de un mecanismo de transporte seguro, una primera solicitud que contiene una serie de identificadores de usuario, y producir como respuesta un producto criptográfico. El procedimiento comprende recibir, a través de dicho mecanismo de transporte seguro, una subsiguiente segunda solicitud que contiene uno de dicha serie de identificadores de usuario, y responder transmitiendo dicho producto criptográfico a través de dicho mecanismo de transporte seguro. Dicho producto criptográfico es un grupo criptográfico digital que contiene dicha serie de identificadores de usuario y una clave criptográfica común para utilizar en la criptografía simétrica entre usuarios identificados mediante dicha serie de identificadores de usuario, y/o claves públicas específicas por usuario y relacionadas con el identificador de usuario, para utilizar en criptografía asimétrica en comunicaciones entre usuarios identificados mediante dicha serie de identificadores de usuario.

Según una realización, el procedimiento comprende comprobar si dicha primera solicitud contiene una

respectiva clave de cifrado específica por usuario para cada uno de dicha serie de identificadores de usuario, y responder al descubrimiento de que dicha primera solicitud no contenía una respectiva clave de cifrado específica por usuario para cada uno de dicha serie de identificadores de usuario, incrementando los datos recibidos en dicha primera solicitud para que contengan una respectiva clave de cifrado específica por usuario para cada uno de dicha serie de identificadores de usuario. Esto involucra, por lo menos, la ventaja de que el procedimiento es adaptable flexiblemente a situaciones en las que no todas las claves de cifrado específicas por usuario están incluidas en la primera solicitud.

Según una realización, el procedimiento comprende, al producir dicho grupo criptográfico, utilizar una clave de firma para firmar digitalmente elementos de información incluidos en dicho grupo criptográfico. Esto involucra, por lo menos, la ventaja de que el procedimiento puede funcionar en, y adaptarse flexiblemente a situaciones en las que la disposición que ejecuta el procedimiento no posee por sí misma las claves de cifrado específicas por usuario faltantes.

Según una realización, el procedimiento comprende comprobar a partir de dicha subsiguiente segunda solicitud si la solicitud está destinada a la disposición que ejecuta el procedimiento o a otro receptor, y responder al descubrimiento de que la solicitud está destinada a otro receptor, reenviando dicha subsiguiente segunda solicitud hacia dicho otro receptor. Esto involucra, por lo menos, la ventaja de que se pueden cumplir los mismos principios funcionando en un entorno en el que diferentes usuarios pueden pertenecer a los dominios administrados de diferentes proveedores de confianza.

Según una realización, el procedimiento comprende, antes de dicho reenvío, sustituir una autenticación original de dicha subsiguiente segunda solicitud con una autenticación de la disposición que ejecuta el procedimiento. Esto involucra, por lo menos, la ventaja de que las relaciones de confianza entre las partes se pueden mantener y utilizar apropiadamente incluso cuando se vuelve a reenviar la información.

Según un tercer aspecto, se da conocer un producto de programa informático que comprende uno o varios conjuntos de una o varias instrucciones ejecutables por máquina que están configuradas para, cuando son ejecutadas por uno o varios procesadores, hacer que dicho uno o varios procesadores ejecuten un procedimiento de la clase descrita anteriormente.

El alcance de la invención se define mediante las reivindicaciones independientes. Se definen características opcionales en las reivindicaciones dependientes.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

En los dibujos:

la **figura 1** muestra el intercambio de información cuando se funciona según una realización, y
la **figura 2** muestra el intercambio de información cuando se funciona según una realización.

DESCRIPCIÓN DETALLADA

En la siguiente descripción se hace referencia a los dibujos adjuntos, que forman parte de la invención y que muestran, a modo de ilustración, aspectos específicos en los que se puede encontrar la presente invención. Se entiende que se pueden utilizar otros aspectos, y se pueden realizar cambios estructurales o lógicos sin apartarse del alcance de la presente invención. Por lo tanto, la siguiente descripción detallada no se debe tomar en sentido limitativo, dado que el alcance de la presente invención se define en las reivindicaciones adjuntas.

Por ejemplo, se entiende que una descripción en relación con el procedimiento descrito puede, asimismo, ser válida para un correspondiente dispositivo o sistema configurado para realizar el procedimiento, y viceversa. Por ejemplo, si se describe una etapa de procedimiento específica, un dispositivo correspondiente puede incluir una unidad para realizar la etapa de procedimiento descrita, incluso si dicha unidad no está descrita o mostrada explícitamente en las figuras. Por otra parte, por ejemplo, si se describe un aparato específico en base a unidades funcionales, un procedimiento correspondiente puede incluir una etapa que lleva a cabo la funcionalidad descrita, incluso si dicha etapa no se describe explícitamente o se muestra en las figuras. Además, se entiende que las características de los diversos aspectos de ejemplo descritos en el presente documento se pueden combinar entre sí, salvo que se indique específicamente lo contrario.

Un ejemplo de un grupo criptográfico digital es un grupo de, por lo menos, dos usuarios, por ejemplo (pero no necesariamente) personas individuales, que desean compartir entre ellos de manera segura información transmitida digitalmente, es decir, de manera que todos en el grupo puedan confiar en que los otros son quien parecen ser, y de manera que las partes que no son miembros del grupo no puedan acceder a la información compartida. Uno de dichos usuarios puede actuar como propietario o fundador del grupo.

Otro ejemplo de utilización de un grupo criptográfico digital es uno cuyo propósito es habilitar a un usuario individual para que posea de manera segura un atributo digital y lo presente para su comprobación cuando sea necesario. Por ejemplo, una autoridad nacional responsable de conceder permisos de conducir puede configurar y administrar dicho grupo por cada titular de un permiso de conducir válido. Un agente de policía puede ser considerado (preferentemente temporalmente) miembro de dicho grupo, en cuyo caso el agente tendría los medios para realizar comunicaciones digitales seguras con una cartera digital del usuario. El derecho del usuario a conducir una clase particular de vehículo puede haberse almacenado como un atributo, que la cartera digital del usuario puede entonces presentar al agente de policía para su inspección. Como otro ejemplo, el propietario del grupo puede ser una entidad comercial y los miembros pueden ser un usuario que posee una tarjeta de fidelidad y los miembros de su familia, que en los sistemas de la técnica anterior aparecían como propietarios de tarjetas subordinadas asociadas con la del usuario principal.

En la definición general utilizada en este texto, el propietario o fundador de un grupo criptográfico digital no es necesariamente un miembro del grupo, independientemente de que tenga dicho rol como propietario o fundador. La situación se puede visualizar con los conceptos de derecho de lectura y derecho de escritura. Los miembros del grupo criptográfico digital tienen siempre derecho de lectura; en otras palabras, tienen acceso continuo a atributos que han sido almacenados para el grupo, siempre que sigan siendo miembros. Aunque el propietario tiene derecho de escritura, es decir, derecho a decidir qué atributos se almacenarán para el grupo, después de configurar el grupo el propietario no tiene necesariamente acceso posterior a los atributos almacenados o a las comunicaciones entre los miembros. Sin embargo, en muchos casos, lo más práctico puede ser que el propietario se convierta asimismo en un miembro del grupo.

Los miembros de un grupo criptográfico digital pueden ser usuarios pero, por lo menos, en algunos casos, asimismo, organizaciones y/o dispositivos. En aquellos casos en que los miembros son usuarios, es habitual referirse a estos como miembros del grupo (y, asimismo, al propietario del grupo como tal) incluso si, en sentido estricto, las partes que actúan en las comunicaciones digitales reales son dispositivos electrónicos manejados por dichos usuarios y por el propietario del grupo. Dicho dispositivo electrónico puede ser, por ejemplo, un ordenador, un portátil, una tableta, un teléfono inteligente, un asistente digital portátil o algún otro dispositivo electrónico que comprenda los medios requeridos para procesamiento y comunicaciones. En algunos casos, un dispositivo electrónico programable e implantable de un usuario puede actuar como dicho dispositivo electrónico.

Se entiende que todas las referencias a un dispositivo en singular abarcan, asimismo, grupos de dos o más dispositivos que funcionan juntos bajo la supervisión del mismo usuario. Dicho grupo de dos o más dispositivos se puede describir como consistente en dispositivos que el usuario tiene conectados entre sí. Se adopta el concepto de identidad autosoberana (SSI, Self-Sovereign Identity) para implicar que un usuario tiene un control establecido criptográficamente sobre la información generada en el grupo, incluyendo derechos tales como derecho de administración, derecho de manipulación, y similares. El control establecido criptográficamente difiere de los derechos que se basarían simplemente en algunos derechos almacenados vinculados a un determinado ID de usuario: significa que el usuario posee los elementos criptográficos que son necesarios para leer y/o escribir la información apropiada. Establecer grupos criptográficos está dirigido a proporcionar a los miembros del grupo dicha posesión de los elementos criptográficos necesarios.

La figura 1 muestra algunas comunicaciones entre —y algunas operaciones realizadas por— un proveedor de confianza, un propietario del grupo y uno o varios miembros del grupo cuando ejecutan un procedimiento según una realización. El proveedor de confianza se puede denominar, asimismo, la cripta, recalcando la hipótesis de que representa una institución con un nivel de seguridad digital excepcionalmente alto. Asimismo, denominaciones similares que podrían utilizarse para el proveedor de confianza son proveedor de cartera y los acrónimos CA y/o VA (Certification Authority, Validation Authority; autoridad de certificación, autoridad de validación). El proveedor de confianza se puede manejar de manera privada, o puede pertenecer a una autoridad y/o funcionar bajo la supervisión de la misma.

Para comenzar a establecer un grupo, el propietario del grupo deberá poseer, por lo menos, algún medio para identificar digitalmente a cada miembro del grupo a formar. Se pueden posteriormente añadir más miembros a un grupo, pero se considerará primero aquí el caso de configurar un grupo para un número predefinido de usuarios conocidos. En relación con los nuevos miembros a añadir posteriormente, cabe señalar que añadir un nuevo miembro a un grupo previamente existente puede suponer que el nuevo miembro tenga acceso, asimismo, a información que ha sido procesada en el grupo antes de añadir el nuevo miembro. La información procesada previamente se puede mantener inaccesible a los nuevos miembros mediante cifrarla por separado dentro del grupo, o cifrarla con claves intercambiadas entre miembros antiguos del grupo, tal como con las denominadas claves PGP, cuyas claves públicas los miembros antiguos pueden haber distribuido entre sí, manteniendo al mismo tiempo para sí mismos las claves secretas. Otra posibilidad más es cifrar la información antigua solamente una vez con una clave conocida por los miembros antiguos, y cifrar por separado dicha clave para cada miembro antiguo. Esta última posibilidad puede ser la más rentable, dado que la cantidad de información compartida dentro del grupo no crece proporcionalmente al número de miembros; cada miembro antiguo necesita solamente almacenar de manera segura su propia

clave para la información cifrada dentro del grupo. Si un nuevo miembro no necesitara (o no debiera) categóricamente tener acceso a información procesada previamente, puede ser más sencillo configurar un nuevo grupo al que pertenezca, asimismo, el nuevo miembro. Asimismo, los miembros del grupo existentes pueden ser posteriormente eliminados de un grupo; habitualmente, esto requiere actualizar, por lo menos, algunas de las claves que se utilizan para la gestión segura de información relacionada con el grupo.

La figura 1 muestra esquemáticamente una etapa 101 en la que los usuarios comunican al propietario del grupo los identificadores mediante los que desean ser conocidos en el grupo. Sin embargo, se debe observar que para los propósitos de la siguiente descripción es irrelevante cómo y cuándo el propietario del grupo adquirió los ID de miembro u otros identificadores de los miembros del grupo. Si el propietario del grupo mantiene, por ejemplo, un catálogo de información de contacto, un registro oficial de información de población u otra base de datos de cliente, puede leer desde allí los identificadores de los miembros del grupo. Dado que puede haber i miembros en el grupo, donde i es un número entero positivo utilizado como índice, el identificador o los identificadores de usuario del miembro o de los miembros del grupo pueden denominarse, en general, UID_i.

En la etapa 101 (o en cualquier otra etapa, anterior), el propietario del grupo puede adquirir, asimismo, de cada miembro del grupo a configurar, una respectiva clave pública que constituye una mitad de un par de claves específicas por usuario de un sistema de criptografía asimétrica. Sin embargo, esto no es necesario dado que las claves públicas de los miembros del grupo pueden, asimismo, entrar en escena posteriormente, tal como se describirá en detalle en este texto. La clave pública del miembro i-ésimo en el grupo se puede denominar PK_{UIDi}.

En la etapa 102, el propietario del grupo compone una solicitud de AñadirGrupo, es decir, una solicitud para configurar el grupo criptográfico digital. La solicitud de AñadirGrupo se dirigirá al proveedor de confianza y deberá contener, por lo menos, los identificadores de los miembros del grupo, así como uno o varios atributos que están destinados a su futura utilización por los miembros del grupo. Como ejemplo de atributo, se considera aquí una clave precompartida (PSK, pre-shared key) denominada P_{G0}. Dicha PSK puede concebirse para su utilización como secreto compartido entre los miembros del grupo, por ejemplo, como una clave de cifrado y descifrado de un procedimiento de criptografía simétrica. La PSK y/u otros atributos se tratarán como parte de una estructura de datos denominada archivo de grupo de depósito de claves, conocida por su acrónimo KGA (Keystore Group Archive). Según una denominación formal, se tiene

$KGA(P_{G0},...)$

donde los puntos suspensivos muestran que el KGA puede contener, asimismo, otros atributos, como los identificadores UID_i de los miembros del grupo y/o claves públicas PK_{UIDi} de (por lo menos, parte de) los miembros del grupo. Si estos han de ser enumerados explícitamente, la denominación formal puede ser

$KGA\ (P_{G0}, UID_i, PK_{UIDi}, ...)$.

Ejemplos de otros posibles atributos en el KGA incluyen, de forma no limitativa: nombre y/u otro identificador del grupo criptográfico digital, marcas de tiempo para mostrar, por ejemplo, tiempos de creación y modificación del grupo criptográfico digital, datos de caducidad para mostrar durante cuánto tiempo debería seguir siendo válido el grupo criptográfico digital, identificador del proveedor de confianza al que se dirigirá la solicitud, y metadatos pertinentes para cualesquiera otro u otros aspectos del grupo criptográfico digital.

Por seguridad, la etapa 102 deberá comprender cifrar el KGA. Una manera ventajosa de generar una clave de cifrado K_{KGA} es

$$K_{KGA} = SHA2(X25519(SK_{UID}, PK_{VID}) \| PK_{VID} \| PK_{UID} \| n)$$

donde SHA2 () indica la ejecución del algoritmo de hash seguro 2 sobre el argumento en el paréntesis y X25519() indica la aplicación del procedimiento de Diffie-Hellman de curva elíptica Curve25519 sobre el argumento entre paréntesis. La letra n indica un nonce criptográfico, por ejemplo, un único nonce de 12 bits. La doble línea vertical ‖ significa una operación OR lógica bit a bit. Las claves PK_{VID} y PK_{UID} son las claves públicas del proveedor de confianza (PK_{VID}) y el propietario del grupo (PK_{UID}), respectivamente.

El cifrado del KGA se puede realizar, por ejemplo, utilizando el procedimiento AES256-GCM, que significa AES de 256 bits en modo Galois/Contador. Usando la notación hasta ahora introducida, el KGA cifrado se puede representar como

$$Enc(K_{KGA},\ KGA(P_{G0}, UID_1, PK_{UID1}, ...)) = AES256\text{-}GCM(SHA2(X25519(SK_{UID}, PK_{VID}) \| PK_{VID} \| PK_{UID} \| n), m, n,\ KGA(P_{G0}, UID_1, PK_{UID1}, ...))$$

donde la letra m indica un MAC o código de autenticación de mensaje para la etiqueta de autenticación de cifrado.

Además, es ventajoso que la etapa 102 comprenda la generación de un par de claves efímeras de un procedimiento de criptografía asimétrica. Estas claves efímeras se denominan aquí PK_{GRT} y SK_{GRT}, donde PK significa clave pública, SK significa clave secreta, y el subíndice GRT procede de las palabras Group Request Token (testigo de solicitud de grupo). El propietario del grupo mantendrá la clave secreta SK_{GRT} almacenada y proporcionará la clave pública PK_{GRT} al proveedor de confianza en la solicitud de AñadirGrupo. De este modo, el proveedor de confianza puede utilizar la clave pública PK_{GRT} para cifrar su respuesta final, garantizando que solamente el propietario del grupo podrá descifrarla. La naturaleza efímera de estas claves no es obligatoria, pero añade seguridad debido a que una parte maliciosa que se apropiara posteriormente de alguna de estas claves podría hacer poco uso de esta.

Transmitir la solicitud de AñadirGrupo completa desde el propietario del grupo al proveedor de confianza se muestra como etapa 103 en la figura 1. La denominación AñadirGrupo y todas las demás denominaciones específicas de la figura 1 son solamente a modo de ejemplo y no se deberán considerar limitativas en ningún sentido; naturalmente, se podría utilizar algún otro nombre para el mensaje. Asimismo, no es necesario transportar toda la información descrita aquí en un solo mensaje, sino que podrían utilizarse múltiples transmisiones a través de un canal común de comunicaciones o incluso de una serie de canales. Utilizando las notaciones presentadas arriba, la solicitud de AñadirGrupo en la etapa 103 puede contener, por lo menos, la clave pública efímera PK_{GRT} y el KGA cifrado.

Lo más ventajoso es utilizar un mecanismo de transporte seguro para transportar la solicitud de AñadirGrupo desde el propietario del grupo al proveedor de confianza, en la etapa 103. Un ejemplo no limitativo de dicho mecanismo de transporte seguro es un canal de comunicaciones digitales en el que se puede utilizar el protocolo de TLS (Transport Layer Security, seguridad de la capa de transporte). La disposición mencionada aquí anteriormente como proveedor de confianza comprende un extremo de recepción y un extremo de transmisión de dicho mecanismo de transporte seguro, acoplados al motor criptográfico capaz de realizar operaciones criptográficas. La recepción y transmisión a través del mecanismo de transporte seguro no necesariamente atraviesa el mismo canal o conexión, u otro similar, aunque no se excluyen ambas posibilidades.

La etapa 104 en la figura 1 se podría caracterizar, en general, como que el proveedor de confianza establece el grupo criptográfico digital solicitado y lo almacena en forma de una estructura de datos que puede comunicarse posteriormente a los miembros del grupo, a petición. La etapa 104 podría caracterizarse, asimismo, de manera que el motor criptográfico en la disposición del proveedor de confianza responde a recibir, a través de dicho mecanismo de transporte seguro, una primera solicitud (es decir, la solicitud de AñadirGrupo 103) que contiene una serie de identificadores de usuario (los UID_i) produciendo un producto criptográfico. Aquí, la expresión producto criptográfico se refiere al grupo criptográfico digital, que contiene, por lo menos, los identificadores de usuario de los miembros del grupo, así como una o varias claves para habilitar comunicaciones seguras entre los miembros del grupo. El grupo criptográfico digital puede contener, asimismo, otras informaciones diversas, como se describirá en mayor detalle posteriormente en este texto.

Dado que el KGA entró en la solicitud de AñadirGrupo 103 en forma cifrada, la disposición del proveedor de confianza deberá descifrarlo primero. Suponiendo que el propietario del grupo utilizó el procedimiento descrito anteriormente para generar la clave de cifrado para cifrar el KGA en la solicitud de AñadirGrupo 103, la disposición del proveedor de confianza puede regenerar la clave como

$$K_{KGA} = SHA2(X25519(SK_{VID}, PK_{UID}) || PK_{VID} || PK_{UID} || n)$$

y usar la clave regenerada para descifrar el KGA.

Ya se ha señalado anteriormente que, cuando construye la solicitud de AñadirGrupo 103, el propietario del grupo no está necesariamente en posesión de las claves de cifrado (públicas) específicas por usuario de todos (o incluso de alguno de) los miembros del grupo. Por esta razón, es ventajoso configurar la disposición del proveedor de confianza para que compruebe, como parte de la etapa 104, si la solicitud de AñadirGrupo 103 recibida contenía una respectiva clave de cifrado específica por usuario para cada identificador de usuario. Si no, la disposición del proveedor de confianza se puede configurar para incrementar los datos recibidos en dicha primera solicitud para que contengan una respectiva clave de cifrado específica por usuario para cada uno de dicha serie de identificadores de usuario.

Una posibilidad es que el proveedor de confianza conozca ya las respectivas claves de cifrado (públicas) específicas por usuario, por ejemplo, en base a algunas comunicaciones anteriores que ha tenido con dichos usuarios. Como otra posibilidad, la disposición del proveedor de confianza se puede configurar para realizar dicho incremento solicitando y recibiendo respectivas claves de cifrado específicas por usuario desde fuentes

externas a la disposición. Como un ejemplo, se puede considerar un caso en el que hay dos o más proveedores de confianza vinculados entre sí. Cada uno de dichos proveedores de confianza tiene una base de datos de usuarios que conoce previamente: los proveedores de confianza pueden ser, por ejemplo, diferentes autoridades con las que determinados usuarios se han comunicado anteriormente, y/o diferentes entidades comerciales que tienen, cada una, su propia base de datos de clientes. Las claves de cifrado específicas por usuario, en particular claves públicas, pueden aparecer almacenadas rutinariamente en dichas bases de datos, teniendo cada una de dichas claves de cifrado almacenadas una relación inequívoca con un respectivo identificador de usuario de clase similar a los utilizados en la solicitud de AñadirGrupo. La disposición del proveedor de confianza puede enviar solicitudes a uno o varios de dichos proveedores de confianza vinculados, y adquirir en respuesta las claves de cifrado específicas por usuario solicitadas.

Se puede aplicar un principio similar que concierne, asimismo, a otros datos a incluir en el grupo criptográfico: la disposición del proveedor de confianza puede incrementar los contenidos a incluir del grupo criptográfico generando cualesquiera elementos de información faltantes, ya sea por sí mismo o solicitándolos de otras fuentes vinculadas, o ambas cosas. La disposición del proveedor de confianza realiza cualquier incremento semejante, si es necesario, de acuerdo con las especificaciones predefinidas que rigen la creación y generación de grupos criptográficos.

La disposición del proveedor de confianza se puede configurar para comprobar cualquier fragmento de información, por ejemplo, información relacionada con el usuario, recibido en la solicitud de AñadirGrupo 103, con respecto a un correspondiente fragmento de información (relacionada con el usuario) procedente de otra fuente. Si se ejecuta, el propósito de dicha comprobación es averiguar si estos fragmentos de información relacionada con el usuario concuerdan entre sí. Por ejemplo, si la solicitud de AñadirGrupo 103 contenía una o varias claves de cifrado (públicas) específicas por usuario, la disposición del proveedor de confianza puede comparar estas con su propia base de datos o —si no las encuentra en su propia base de datos— puede realizar de nuevo solicitudes a otros proveedores de confianza posiblemente vinculados, parecido al caso anterior de solicitar la clave de cifrado específica por usuario.

Se puede suponer que cada usuario (u otra parte elegible como miembro en un grupo) "pertenece" a, o ha sido originalmente identificado de forma segura por algún proveedor de confianza. El proveedor de confianza cuya disposición recibió la solicitud de AñadirGrupo 103 puede no ser el que originariamente identificó de manera segura a todos aquellos usuarios que se van a incluir como miembros en el nuevo grupo. En otras palabras, la solicitud de AñadirGrupo 103 puede contener el UID de uno o varios miembros previstos del grupo que "pertenecen" a uno o varios proveedores de confianza diferentes de aquel cuya disposición recibió la solicitud de AñadirGrupo. En ese caso, una posibilidad es que la disposición del proveedor de confianza simplemente deje un espacio vacío donde utilizaría la clave de cifrado específica por usuario si uno de sus "propios" usuarios estuviera en cuestión. Dicha manera de funcionar, es decir, dejar vacía la clave de cifrado específica por usuario de un usuario "externo", puede tener determinadas consecuencias adicionales que se describen posteriormente en este texto.

Si dichos fragmentos de información relacionada con el usuario no concuerdan entre sí, la disposición del proveedor de confianza puede adoptar una decisión sobre si se permite que continúe el establecimiento del grupo criptográfico digital. Son posibles decisiones tanto positivas como negativas, en función de cómo ha sido programada la disposición del proveedor de confianza para funcionar y de qué clase de criterios de decisión aplica.

Anteriormente, se ha señalado ya que, además de los identificadores de usuario, el grupo criptográfico digital, cuando está completo, deberá contener una o varias claves para habilitar comunicaciones seguras entre los miembros del grupo. Las claves de cifrado (públicas) específicas por usuario pueden cumplir este requisito, porque se puede suponer que cada usuario tiene almacenada de manera segura la correspondiente clave secreta. Otro ejemplo de una clave de este tipo es una clave precompartida (PSK), denominada anteriormente P_{G0}, definida, en general, como una clave criptográfica común para utilizar en criptografía simétrica entre usuarios identificados por los identificadores de usuario. Si el propietario del grupo ha generado ya la P_{G0}, la disposición del proveedor de confianza puede simplemente leerla desde el KGA descifrado y almacenarla como parte del grupo criptográfico digital. Como otra alternativa, la disposición del proveedor de confianza puede generar dicha PSK y almacenarla como parte del grupo criptográfico digital.

La P_{G0} u otra PSK es un ejemplo de un atributo (o elemento de información) incluido en el grupo criptográfico en el que los miembros del grupo tienen que poder confiar completamente más adelante. Para proporcionar dicha seguridad, es ventajoso que la P_{G0} u otra PSK esté firmada digitalmente por el propietario del grupo (si el propietario del grupo ha generado ya la P_{G0}) y/o por la disposición del proveedor de confianza. De acuerdo con principios conocidos, la parte que firma utiliza su clave de firma secreta para la firma digital, de manera que otras partes pueden verificar posteriormente la integridad del elemento de información en cuestión utilizando una correspondiente clave de verificación pública de la parte que firma.

Para proporcionar seguridad adicional en subsiguientes fases del procedimiento, es ventajoso configurar la

disposición del proveedor de confianza para generar, como parte de la etapa 104, un par adicional de claves efímeras de un procedimiento de criptografía asimétrica. Se hará referencia aquí a este par de claves efímeras con el subíndice GAT, que significa Group Access Token (testigo de acceso de grupo). Como ejemplo no limitativo, la disposición del proveedor de confianza puede generar una clave GAT secreta, SK_{GAT}, como

$$SK_{GAT} = RNG(256)$$

donde el operador RNG() significa generar un número binario aleatorio con tantos bits como el número (en base decimal) en el paréntesis. A continuación, la correspondiente clave pública PK_{GAT} se puede generar, por ejemplo, como la clave pública a partir de scalarbasemult(SK_{GAT}). Aquí, scalarbase-mult() es una función que, en base a una curva elíptica, tal como la curva 25519, por ejemplo, devuelve de manera determinista una correspondiente clave pública cuando recibe como entrada una clave secreta. El nombre de la función puede cambiar dependiendo de la fuente utilizada pero, en el momento de escribir este texto, la documentación relativa a la función scalarmult() original se puede encontrar en https://doc.libsodium.org/. Siempre que sea necesario generar un par de claves secreta y pública, esto se puede realizar, asimismo, utilizando una única función adecuada que proporcione ambas claves como salidas.

La disposición del proveedor de confianza se puede configurar para cifrar el KGA creado o actualizado, de manera ligeramente diferente en función de si se trata del caso de crear este grupo criptográfico digital antes de transmitir una respuesta al propietario del grupo (o un caso de actualizar un grupo criptográfico digital creado previamente, pero antes de comunicar con ninguno de los otros miembros del grupo) en la etapa 104, o si el cifrado se realiza en asociación con la comunicación con un miembro del grupo distinto del propietario del grupo; ver la etapa 109 en la figura 1. En el caso mencionado primero, una posibilidad ventajosa es utilizar una clave obtenida previamente, específica para el propietario del grupo. Un procedimiento ventajoso de creación y manipulación de dicha clave se ha descrito en la solicitud de Patente codependiente EP22157019.5, que no está disponible para el público en la fecha de presentación de este texto. La clave en cuestión se denomina SK_{UAT} en dicho procedimiento, donde el subíndice UAT procede de User Access Token (testigo de acceso de usuario). El proceso de cifrar el KGA recién creado puede involucrar la generación de un secreto compartido SS_{GAK}, como

$$SS_{GAK} = scalarmult(SK_{GAT}, PK_{GRT})$$

donde el subíndice GAK procede de Group Archive Key (clave de archivo de grupo). La función scalarmult () es una función que, basándose en una curva elíptica, tal como la curva 25519, por ejemplo, devuelve el secreto compartido computacionalmente entre dos partes, haciendo innecesario transmitir una clave real, dependiendo al mismo tiempo de la seguridad establecida por pares de claves vinculadas matemáticamente. El KGA recién creado puede, a continuación, cifrarse como

Enc (SS_{GAK}, KGA (...))

donde nuevamente los puntos suspensivos representan, en general, toda la información que está incluida en el KGA. Si se tratara del caso de actualizar un KGA que ya se habría cifrado anteriormente con el SS_{GAK} como clave, pero antes de comunicar con ningún miembro del grupo distinto del propietario del grupo, la operación de actualización se puede describir como

Actualizar (Dec (SS_{GAK}, KGA(...)))

tras lo cual puede tener lugar el nuevo cifrado de manera similar a lo anterior.

Si el cifrado se realiza como parte de la etapa 109, en asociación con comunicar con un miembro del grupo diferente del propietario del grupo, se puede obtener seguridad añadida utilizando la clave GAT secreta, SK_{GAT}, presentada anteriormente en este texto. En ese caso, un secreto compartido SS_{GAK} se puede obtener como

$$SS_{GAK} = scalarmult(SK_{GAT}, PK_{GRT})$$

donde el subíndice GAK procede de Group Archive Key (clave de archivo del grupo). Entonces, el KGA se puede cifrar como

Enc (SS_{GAK}, KGA (...))

Almacenar de este modo el KGA en la disposición del proveedor de confianza, en forma cifrada con el SS_{GAK}, sirve al propósito de que siempre es necesaria una clave procedente de una fuente externa al proveedor de confianza para descifrar el KGA almacenado. Por lo tanto, incluso si se comprometió la seguridad en el proveedor de confianza y los KGA almacenados estuvieron expuestos, estos serían de poca utilidad para el

atacante debido a que ni siquiera el proveedor de confianza puede acceder a sus contenidos cifrados sin aquellos componentes clave que tienen que proceder del propietario del grupo o de uno de los otros miembros del grupo.

Como resultado de las etapas de procedimiento explicadas arriba, KGA (es decir, el producto criptográfico que produjo el motor criptográfico de la disposición del proveedor de confianza en la etapa 104) se puede describir, por ejemplo, como

KGA (P_{G0}, UID_i, PK_{UIDi}, PID, GID, GMD, ...)

donde P_{G0} es la PSK para el grupo, UID_i indica los miembros del grupo (incluyendo el propietario del grupo) listados por sus identificadores, PK_{UIDi} indica las claves de cifrado específicas por usuario (públicas) de los miembros del grupo, PID o ID de proveedor es un identificador público del proveedor de confianza, GID o ID de grupo es un identificador público del grupo, y GMD o metadatos del grupo (Group MetaData) indica todos los posibles metadatos asociados con el grupo. Se puede elegir un identificador y/o una clave pública del propietario del grupo para distinguirlo o distinguirlos del resto de UID_i y PK_{UIDi}.

Para mejorar la fiabilidad de los atributos en el grupo criptográfico, es ventajoso configurar la disposición del proveedor de confianza para que utilice una clave de firma en su posesión para firmar digitalmente elementos de información que incluye en el grupo criptográfico. Esto habilita a todos los miembros del grupo para garantizar posteriormente que los atributos leídos del grupo criptográfico son correctos, es decir, que su originalidad e integridad no han sido comprometidas.

La etapa en la que la disposición del proveedor de confianza transmite la respuesta de AñadirGrupo al propietario del grupo se muestra como etapa 105 en la figura 1. Comparable a la transmisión de AñadirGrupo anterior en la etapa 103, la disposición del proveedor de confianza cifra ventajosamente el KGA antes de transmitirlo al propietario del grupo en la respuesta de AñadirGrupo 105. Una forma ventajosa de dicho cifrado es

$$\begin{aligned} &Enc(K_{KGA},\ KGA(\ldots)) \\ &= AES256\text{-}GCM(SHA2(X25519(SK_{VID}, PK_{UID}) \\ &\quad \|PK_{VID}\|PK_{UID}\|n), m, n,\ KGA(\ldots)) \end{aligned}$$

Después de la etapa 105, el propietario del grupo tiene toda la información necesaria acerca del grupo, incluyendo la información incrementada que el proveedor de confianza proporcionó por sí mismo y/o solicitó a otros proveedores de confianza vinculados o a otras fuentes, durante la etapa 104. Adicionalmente, el propietario del grupo sabe que toda la información necesaria sobre el grupo está almacenada de manera segura en la disposición del proveedor de confianza, y preparada para ser distribuida de allí a los miembros del grupo.

La etapa 106 representa al propietario del grupo instruyendo a los miembros del grupo para que contacten con el proveedor de confianza y descarguen el KGA de la disposición del proveedor de confianza. Una manera ventajosa de habilitar a los miembros del grupo para ello es enviarles copias del testigo de solicitud de grupo, es decir, de la clave pública efímera PK_{GRT}. Adicional o alternativamente, el propietario del grupo puede enviar otra información sobre el grupo a los miembros del grupo, en la etapa 106.

El resto de las etapas mostradas en la figura 1 se muestran con respecto a solamente un miembro del grupo, para mantener claridad gráfica. Se ejecutarían etapas similares con respecto a todos los miembros del grupo para hacer el grupo totalmente operativo. Sin embargo, incluso si uno o varios miembros del grupo no hacen su parte, los miembros del grupo que han completado la ejecución de las etapas correspondientes pueden utilizar ya el grupo. Aquí, cabe señalar que se pueden conseguir ciertas ventajas al utilizar el proveedor de confianza como almacenamiento seguro de elementos de información relacionados con el grupo, incluso si solamente un miembro del grupo realizara de hecho estas etapas y utilizara el grupo criptográfico en el futuro.

La etapa 107 representa el miembro del grupo componiendo una solicitud para adquirir la información necesaria relativa al grupo, y la etapa 108 representa el miembro del grupo transmitiendo la solicitud, denominada aquí la solicitud de ObtenerGrupo, al proveedor de confianza. La transmisión en la etapa 108 es comparable a la transmisión en la etapa 103 anterior, en el sentido de que puede utilizar un mecanismo de transporte seguro, como un canal de comunicaciones digitales en el que se puede utilizar el protocolo TLS (seguridad de la capa de transporte).

La solicitud de ObtenerGrupo 108 debería permitir al proveedor de confianza garantizar que el emisor, es decir, el miembro del grupo, es uno de aquellos que tienen permitido recibir el KGA necesario para funcionar como miembro del grupo. Ventajosamente, la solicitud de ObtenerGrupo 108 contiene por lo tanto, como mínimo, un identificador de usuario UID , que el proveedor de confianza puede, a continuación, comparar con

la lista de identificadores de usuario UID_i que recibió anteriormente del propietario del grupo. Una manera ventajosa de hacer que la solicitud de ObtenerGrupo 108 contenga el identificador de usuario UID es hacer que contenga un certificado de la parte solicitante, certificado que contiene tanto el UID como una clave pública de la parte solicitante. En tal caso, el proveedor de confianza puede utilizar el UID para el propósito mencionado anteriormente, y la clave pública para proteger el KGA que se enviará como respuesta a la parte solicitante.

Adicionalmente, la solicitud de ObtenerGrupo 108 contiene ventajosamente el testigo de solicitud de grupo, es decir, la clave pública efímera PK_{GRT}. Otros posibles elementos de información que puede contener la solicitud de ObtenerGrupo, por lo menos, si el miembro del grupo solicitante los obtuvo anteriormente del propietario del grupo, incluyen, de forma no limitativa, el identificador de grupo GID, una referencia al identificador del propietario del grupo, diversos tipos de atributos firmados o no firmados, y/o cualesquiera metadatos relacionados con el grupo.

La etapa 109 en la figura 1 representa, en general, todas las comprobaciones que la disposición del proveedor de confianza está configurada para realizar en respuesta a recibir la solicitud de ObtenerGrupo 108. Básicamente, el motor criptográfico en la disposición del proveedor de confianza está configurada para responder a la recepción de, a través de dicho mecanismo de transporte seguro, la solicitud de ObtenerGrupo 108 (que contiene uno de la serie de identificadores de usuario recibidos anteriormente en la solicitud de AñadirGrupo 103) transmitiendo el producto criptográfico producido anteriormente, es decir, el grupo criptográfico digital, a través del mecanismo de transporte seguro.

Considerando que el KGA fue almacenado anteriormente en forma cifrada en la disposición del proveedor de confianza, la disposición puede generar primero la clave SS_{GAK} necesaria para el descifrado, como

$$SS_{GAK} = scalarmult(SK_{GAT}, PK_{GRT})$$

y, a continuación, realizar el descifrado
$Dec(SS_{GAK}, KGA (...))$.

La disposición puede proceder, a continuación, a cifrar de nuevo el KGA, esta vez para su transmisión al miembro del grupo solicitante, mediante disponer

$$n = RNG(96)$$

como un nonce y

$$K_{KGA} = SHA2(X25519(SK_{VID}, PK_{UID}) || PK_{VID} || PK_{UID} || n)$$

como una clave de cifrado (utilizando PK_{UID} de este usuario particular, leída del certificado si se recibió uno en la solicitud de ObtenerGrupo) y, a continuación, cifrando

$$Enc(K_{KGA}, KGA (...)) = AES256 - GCM (SHA2 (X25519 (SK_{VID}, PK_{UID}) || PK_{VID} || PK_{UID} || n), m, n, KGA (...))$$

Desde el punto de vista de la seguridad, es particularmente ventajoso requerir que el certificado mencionado anteriormente proceda siempre del solicitante, porque en la etapa 109 (y, posteriormente, en la etapa 210 en la figura 2), el archivo de grupo de depósito de claves está asegurado para el usuario frente a la clave pública del usuario particular PK_{UID}. El certificado puede venir en la solicitud de ObtenerGrupo, como se ha mencionado anteriormente, pero puede, asimismo, haber llegado al conocimiento de la disposición del proveedor de confianza por medio de alguna otra solución basada en PKI, por ejemplo, según un procedimiento descrito en la solicitud de Patente europea codependiente EP22157019.5, del mismo solicitante. Adicional o alternativamente, si está presente una tarjeta de identidad inteligente, pasaporte o documento correspondiente apropiado, la disposición del proveedor de confianza puede leer el certificado desde este, como un certificado RSA o ECC, según la especificación X.509.

Similarmente, desde el punto de vista de la seguridad, es muy ventajoso requerir que el certificado esté firmado por la disposición del proveedor de confianza o —en el caso de varios proveedores de confianza vinculados mutuamente— por una disposición de uno de dichos proveedores de confianza vinculados mutuamente. Cualquier parte que reciba a continuación un certificado puede comprobar la integridad y autenticidad del certificado y determinar que fue firmado por una parte fiable (es decir, por el proveedor de confianza o uno de los proveedores de confianza vinculados mutuamente). A su vez, esto demuestra que la clave pública contenida en el certificado se puede considerar fiable.

Del nonce n, se puede señalar que está relacionado con los requisitos del algoritmo AES-256 GCM aceptado por el IETF. Este proporciona 32 bits adicionales de seguridad mejorada a la clave de cifrado, en particular cuando está en uso durante un tiempo mayor, hasta un máximo de 350 GB.

La etapa 110 en la figura 1 representa la disposición del proveedor de confianza transmitiendo el KGA cifrado al miembro del grupo que lo solicitó. La transmisión se denomina respuesta de ObtenerGrupo en la figura 1, para enfatizar su asociación con la solicitud de ObtenerGrupo 108 anterior. De manera similar a la denominación AñadirGrupo anterior, la denominación ObtenerGrupo es naturalmente solo un ejemplo, y se podían utilizar otras denominaciones.

Como ejemplo de aplicar un procedimiento de la clase mostrada en la figura 1, se puede considerar una situación en la que un agente de policía en una patrulla rutinaria retiene a un ciudadano y desea comprobar que el ciudadano tiene derecho a conducir esa clase particular de vehículo. La autoridad nacional responsable de conceder permisos de conducir puede actuar como el propietario del grupo. Ya anteriormente, en el momento de conceder el permiso de conducir actualmente válido, la autoridad puede haber formado un grupo criptográfico digital en el que ella misma es propietaria del grupo y el ciudadano es un miembro. Al formar el grupo, la autoridad puede haber comunicado los tipos de vehículo permitidos, como atributos, al proveedor de confianza, y haber solicitado al proveedor de confianza que firme digitalmente estos atributos. Cuando el ciudadano se une, a continuación, al grupo al enviar una correspondiente solicitud de ObtenerGrupo, los atributos firmados digitalmente quedan almacenados en una "cartera digital", es decir, un emplazamiento de almacenamiento dedicado en el dispositivo de usuario del ciudadano. Estos atributos puede mantenerse válidos durante tanto tiempo como el documento básico (en este ejemplo: el permiso de conducir) siga siendo válido.

Habiendo conocido el identificador de usuario (público) por el ciudadano, el agente de policía puede enviar una solicitud a la autoridad, proporcionando su propio ID de usuario (y, posiblemente, la clave pública) y añadiendo, asimismo, a la solicitud el identificador de usuario del ciudadano como atributo. La autoridad puede, a continuación, enviar una solicitud de AñadirGrupo al proveedor de confianza, solicitando esencialmente que el agente de policía sea añadido temporalmente al grupo criptográfico digital formado anteriormente, con derecho a recibir del ciudadano un atributo de "tipos de vehículos permitidos". Como alternativa, se puede haber hecho (permanentemente o, como mínimo, a largo plazo) al agente de policía (o al cuerpo de policía como institución, con derechos derivados correspondientemente para agentes individuales cuando están de servicio) miembro del grupo ya con anterioridad, para permitirle inspeccionar el permiso de conducir del ciudadano también fuera de línea.

La disposición del proveedor de confianza puede realizar la adición solicitada al grupo criptográfico digital. Una indicación de esto llegará al dispositivo de usuario del agente de policía, conteniendo el testigo de solicitud de grupo. Cuando el dispositivo de usuario del agente de policía envíe, a continuación, una solicitud de ObtenerGrupo al proveedor de confianza, este recibirá finalmente una respuesta de ObtenerGrupo que contiene la información que necesita. Durante esta ronda de comunicaciones, pueden haber sido añadidos uno o varios atributos al grupo criptográfico digital: por ejemplo, información de validez de duración limitada que permite al dispositivo de usuario del agente de policía seguir siendo miembro del grupo solamente durante un periodo de tiempo.

Una vez el agente de policía pasa a ser un miembro del grupo criptográfico digital, los dispositivos de usuario del ciudadano y del agente de policía pueden entrar en comunicaciones locales, en las que el dispositivo de usuario del ciudadano presenta el atributo firmado digitalmente "tipos de vehículo permitidos", obtenido anteriormente, al dispositivo de usuario del agente de policía. Debido a la firma digital, el último es capaz de verificar que el atributo presentado es válido. Cuando se completan todas las verificaciones, el dispositivo de usuario del agente de policía puede ser eliminado del grupo criptográfico digital mediante una ronda de comunicaciones similar a cuando fue añadido, o se puede simplemente hacer depender de la información de tiempo mencionada anteriormente, para permitir que expire la membresía del agente de policía en el grupo criptográfico digital. Como una alternativa adicional, está la membresía permanente o, por lo menos, a largo plazo del policía en el grupo.

En un caso de ejemplo como el anterior, la autoridad puede desear actualizar regularmente los atributos del grupo criptográfico para garantizar que en los dispositivos de los usuarios no permanecen almacenados atributos caducados (o, por lo menos, atributos muy obsoletos). El dispositivo de usuario del ciudadano puede obtener el grupo criptográfico actualizado del proveedor de confianza, siguiendo la planificación conocida de actualizaciones y/o cuando así se lo requiera la autoridad.

La figura 2 muestra algunas comunicaciones entre —y algunas operaciones realizadas por— dos proveedores de confianza, un propietario del grupo y un miembro del grupo cuando ejecutan un procedimiento, según una realización. Como antecedente a esta realización, se puede recordar la hipótesis de que cada usuario puede "pertenecer" a su proveedor de confianza seleccionado. En este ejemplo, las dos líneas verticales centrales representan las disposiciones de los proveedores de confianza y las dos líneas verticales a la derecha y a la izquierda representan el propietario del grupo y el miembro del grupo, correspondientemente. Con fines ilustrativos, el ejemplo mostrado en la figura 2 se puede considerar en relación con un caso de uso práctico en el que el propietario del grupo desea establecer una llamada

telefónica protegida con el miembro del grupo.

La etapa 201 en la figura 2 es comparable a la etapa 101 en la figura 1, en el sentido de que el propietario del grupo debe haber adquirido de uno u otro modo un identificador de miembro del grupo. Esta etapa puede tener lugar incluso mucho tiempo antes, como es habitual, por ejemplo, para usuarios que almacenan unos los números telefónicos de los otros en sus dispositivos de usuario.

La etapa 202 es comparable, asimismo, a la correspondiente etapa 102 en la figura 1, en el sentido de que representa el dispositivo de usuario del propietario del grupo realizando etapas que están dirigidas al establecimiento de la llamada protegida, es decir, a la creación de un grupo criptográfico dentro del cual puede tener lugar la llamada protegida. La solicitud compuesta se muestra en la etapa 203 y se denomina una solicitud de AñadirGrupo, de manera similar a la etapa 103 de la figura 1. El propietario del grupo transmite la solicitud de AñadirGrupo 203 a su "propio" proveedor de confianza. Más ventajosamente, la solicitud de AñadirGrupo 203 contiene el KGA cifrado (archivo de grupo de depósito de claves) y el testigo de solicitud de grupo PK_{GRT}, cuyo KGA contiene, entre otras cosas, una clave precompartida (denominada PSK o, anteriormente, P_{G0} en este texto) y un identificador UID (y, posiblemente, una clave pública PK_{UID}) del miembro del grupo al que se debería realizar la llamada protegida.

La etapa 204 en la figura 4 es comparable a la etapa 104 en la figura 1, en el sentido de que representa el proveedor de confianza (aquel al que "pertenece" el propietario del grupo) estableciendo el grupo criptográfico solicitado y almacenándolo en forma de una estructura de datos que, posteriormente, se puede comunicar al miembro del grupo a petición. Un motor criptográfico en esta disposición del proveedor de confianza responde a la recepción, a través de un mecanismo de transporte seguro, de la solicitud de AñadirGrupo 203 que contiene una serie de identificadores de usuario (los UID del propietario del grupo y del miembro del grupo), produciendo un producto criptográfico, es decir, creando el grupo criptográfico solicitado. La etapa 205 es la respuesta de AñadirGrupo que la disposición del proveedor de confianza transmite de vuelta al propietario del grupo, de nuevo análogamente a la etapa 105 en la figura 5.

En la etapa 206, el dispositivo de usuario del propietario del grupo transmite al dispositivo de usuario del miembro del grupo, por lo menos, el testigo de solicitud de grupo PK_{GRT} y el identificador VID del proveedor de confianza del propietario del grupo. Aunque no se muestra explícitamente como una etapa separada en la figura 2, el dispositivo de usuario del miembro del grupo utiliza esta información para componer una solicitud para obtener el (KGA cifrado del) grupo criptográfico. Sin embargo, como el miembro del grupo pertenece a un proveedor de confianza diferente del propietario del grupo, la solicitud de ObtenerGrupo de la etapa 207 no se transmite al proveedor de confianza que contiene actualmente los datos almacenados del grupo criptográfico. En cambio, el dispositivo de usuario del miembro del grupo transmite la solicitud de ObtenerGrupo 207 a su propio proveedor de confianza.

Las relaciones preexistentes entre usuarios y sus proveedores de confianza significan que es particularmente fácil y sencillo para sus correspondientes dispositivos y disposiciones establecer y utilizar los mecanismos de transporte seguro que se utilizan para transmitir las solicitudes y respuestas mostradas en la figura 2. En alguna fase anterior, se pueden haber intercambiado suficientes claves y/u otra información secreta compartida entre cada usuario y su respectivo proveedor de confianza, para que estas conexiones de comunicación sean ambas rápidas y seguras de establecer cuando se requiera. Lo mismo aplica a las comunicaciones entre proveedores de confianza. Así, depender de secretos compartidos tal como se concibe aquí es independiente de la tecnología utilizada para establecerlos. Igual que con PKI (Public Key Infrastructure, infraestructura de clave pública), no es importante qué clase de cifrado (ECC, RSA u otros) y algoritmos se utilizan. Es razonable suponer que, por ejemplo, las autoridades pueden a menudo depender de tecnologías de cifrado más antiguas que las entidades privadas y los usuarios individuales más avanzados, de manera que, en el caso más ventajoso, el sistema y el procedimiento deberán permitir funcionar con cualquier tipo de claves PK.

La anterior referencia a secretos compartidos puede significar, ventajosamente, el secreto computacional entre pares de claves vinculadas matemáticamente, que procede del producto de la propia clave secreta (SK) de uno por la clave pública (PK) del otro, según, por ejemplo, los algoritmos ECC o RSA.

En la etapa 208, el proveedor de confianza del miembro del grupo recibe la solicitud de ObtenerGrupo 207 y constata que contiene, además del testigo de solicitud de grupo, un VID externo. En otras palabras, el VID en las solicitudes de ObtenerGrupo 207 no es el del proveedor de confianza del miembro del grupo, sino que identifica en cambio el proveedor de confianza del propietario del grupo. Basándose en una relación vinculada, establecida anteriormente, entre los proveedores de confianza, el proveedor de confianza del miembro del grupo es capaz de reenviar la solicitud de ObtenerGrupo al proveedor de confianza del propietario del grupo, tal como se muestra en la etapa 209 de la figura 2. Sin embargo, el proveedor de confianza del miembro del grupo utiliza sus propias credenciales (en lugar de las del miembro del grupo) para autenticar la solicitud de ObtenerGrupo 209 que reenvía al proveedor de confianza del propietario del grupo.

La etapa 210 en la figura 2 es comparable a la etapa 109 en la figura 1, en el sentido de que el motor criptográfico en la disposición del proveedor de confianza del propietario del grupo responde a recibir, a través de un mecanismo de transporte seguro (que se utilizó para comunicar entre proveedores de confianza), la solicitud de ObtenerGrupo 209. Dicha solicitud contiene uno de la serie de identificadores de usuario recibidos anteriormente en la solicitud de AñadirGrupo 203 —el del miembro del grupo. La disposición del proveedor de confianza del propietario del grupo responde transmitiendo el producto criptográfico producido anteriormente, es decir, el grupo criptográfico digital, a través del mecanismo de transporte seguro hacia el proveedor de confianza del miembro del grupo (ver la etapa 211 en la figura 2).

El proveedor de confianza del miembro del grupo no necesita estar al corriente de ninguno de los contenidos de la respuesta de ObtenerGrupo 211 que recibe. Por el contrario, es suficiente reemplazar los mecanismos de autenticación que se utilizaron entre los dos proveedores de confianza con los utilizados entre el proveedor de confianza del miembro del grupo y el miembro del grupo. La respuesta de ObtenerGrupo reenviada correspondientemente es tal como se muestra en la etapa 212 en la figura 2. Después de recibirla y descifrar su contenido, el dispositivo de usuario del miembro del grupo está preparado para participar en comunicaciones seguras con el dispositivo de usuario del propietario del grupo, tal como se muestra en la etapa 213 de la figura 2.

Una de las ventajas significativas asociadas con los procedimientos y disposiciones descritos anteriormente es la posibilidad de aplicar la práctica de identificadores descentralizados, denominados normalmente DID. Para establecer relaciones de confianza para comunicaciones digitales, el proveedor de confianza puede tener diferentes claves criptográficas (públicas) e información de inicio de sesión del usuario con diferentes propósitos. Una consecuencia ventajosa de esto es la posibilidad de aplicar control a diferentes niveles. Otra es la posibilidad de la apariencia como anónimos y/o seudónimos para los miembros del grupo. Dependiendo del caso de uso, los miembros del grupo pueden parecer anónimos, incluso entre sí, o funcionar como seudónimos, pero con plena confianza en la relación o las relaciones de confianza garantizadas por el proveedor de confianza. Es posible, asimismo, que los miembros del grupo se puedan identificar entre sí, mientras permanecen no identificados para los no miembros.

Cualquier valor de dispositivo o intervalo proporcionado en el presente documento se puede extender o variar sin perder el efecto buscado. Asimismo, cualquier realización se puede combinar con otra realización, salvo que se desautorice explícitamente.

Aunque la materia objeto se ha descrito en lenguaje específico para las acciones y/o características estructurales, debe entenderse que la materia objeto definida en las reivindicaciones adjuntas no está necesariamente limitada a las acciones o características específicas descritas anteriormente. Por el contrario, las acciones y características específicas descritas anteriormente se dan a conocer como ejemplos de implementación de las reivindicaciones, y se prevé que otras características y acciones equivalentes están dentro del alcance de las reivindicaciones.

Se comprenderá que los beneficios y ventajas descritos anteriormente se pueden referir a una realización, o se pueden referir a varias realizaciones. Las realizaciones no se limitan a las que resuelven alguno o la totalidad de los problemas indicados, ni a las que tienen alguno o la totalidad de los beneficios y ventajas indicados. Se comprenderá, además, que la referencia a 'un' elemento puede referirse a uno o varios de dichos elementos.

Las etapas de los procedimientos descritos en el presente documento se pueden llevar a cabo en cualquier orden adecuado, o simultáneamente cuando sea apropiado. Adicionalmente, se pueden eliminar bloques individuales de cualquiera de los procedimientos sin apartarse del alcance de la materia objeto descrita en el presente documento. Los aspectos de cualquiera de las realizaciones descritas anteriormente se pueden combinar con aspectos de cualquiera de las otras realizaciones descritas, para formar realizaciones adicionales sin perder el resultado perseguido.

La expresión "que comprende" o "comprendiendo", tal como se utiliza en el presente documento, pretende incluir el procedimiento, los bloques o los elementos identificados, pero que dichos bloques o elementos no comprenden una lista exclusiva, y un procedimiento o aparato puede contener bloques o elementos adicionales.

Se comprenderá que la descripción anterior se proporciona solamente a modo de ejemplo, y que los expertos en la materia pueden realizar diversas modificaciones. La anterior descripción, los ejemplos y los datos dan a conocer una descripción completa de la estructura y utilización de realizaciones a modo de ejemplo. Aunque se han descrito en lo anterior diversas realizaciones con un cierto grado de particularidad, o haciendo referencia a una o varias realizaciones individuales, los expertos en la materia podrían realizar numerosas modificaciones a las realizaciones dadas a conocer, sin apartarse del alcance de esta memoria descriptiva.

REIVINDICACIONES

1. Disposición para establecer un grupo criptográfico digital, comprendiendo la disposición:

- un motor criptográfico configurado para producir productos criptográficos a partir de datos de entrada dados, y
- un extremo de recepción y un extremo de transmisión de un mecanismo de transporte seguro acoplado a dicho motor criptográfico;

en la que dicho motor criptográfico está configurado para responder a la recepción de, a través de dicho mecanismo de transporte seguro, una primera solicitud que contiene una serie de identificadores de usuario, produciendo un producto criptográfico,
y en la que dicho motor criptográfico está configurado para responder a la recepción de, a través de dicho mecanismo de transporte seguro, una subsiguiente segunda solicitud que contiene uno de dicha serie de identificadores de usuario, transmitiendo dicho producto criptográfico a través de dicho mecanismo de transporte seguro;
en la que dicho producto criptográfico es un grupo criptográfico digital que contiene dicha serie de identificadores de usuario y, por lo menos, una de:

- una clave criptográfica común para utilizar en criptografía simétrica entre usuarios identificados por dicha serie de identificadores de usuario,
- claves públicas específicas por usuario y relacionadas con el identificador de usuario, para utilizar en criptografía asimétrica en comunicaciones entre usuarios identificados por dicha serie de identificadores de usuario.

2. Disposición, según la reivindicación 1, en la que:

- la disposición está configurada para comprobar si dicha primera solicitud contenía una respectiva clave de cifrado específica por usuario para cada uno de dicha serie de identificadores de usuario, y
- la disposición está configurada para responder al descubrimiento de que dicha primera solicitud no contenía una respectiva clave de cifrado específica por usuario para cada uno de dicha serie de identificadores de usuario, incrementando los datos recibidos en dicha primera solicitud para que contengan una respectiva clave de cifrado específica por usuario para cada uno de dicha serie de identificadores de usuario.

3. Disposición, según la reivindicación 2,
en la que la disposición está configurada para realizar dicho incremento solicitando y recibiendo respectivas claves de cifrado específicas por usuario desde fuentes externas a la disposición.

4. Disposición, según cualquiera de las reivindicaciones anteriores, en la que la disposición está configurada para comprobar un fragmento de información relacionada con el usuario recibida en la primera solicitud, frente a un correspondiente fragmento de información relacionada con el usuario procedente de otra fuente, para averiguar si estos fragmentos de información relacionada con el usuario concuerdan entre sí.

5. Disposición, según la reivindicación 4,
en la que la disposición está configurada para responder al descubrimiento de que dichos fragmentos de información relacionada con el usuario no concuerdan entre sí, adoptando una decisión acerca de si se permite que continúe el establecimiento del grupo criptográfico digital.

6. Disposición, según cualquiera de las reivindicaciones anteriores, en la que la disposición está configurada para utilizar una clave de firma para firmar digitalmente elementos de información que incluye en dicho grupo criptográfico.

7. Disposición, según cualquiera de las reivindicaciones anteriores, en la que la disposición está configurada para comprobar, a partir de dicha subsiguiente segunda solicitud, si la solicitud está destinada a la misma o a otro receptor, y para responder al descubrimiento de que la solicitud está destinada a otro receptor reenviando dicha subsiguiente segunda solicitud hacia dicho otro receptor.

8. Disposición, según la reivindicación 7,
en la que la disposición está configurada para, antes de dicho reenvío, reemplazar una autenticación original de dicha subsiguiente segunda solicitud con una autenticación de la propia disposición.

9. Procedimiento para establecer un grupo criptográfico digital, comprendiendo el procedimiento:

- recibir, a través de un mecanismo de transporte seguro, una primera solicitud que contiene una serie de identificadores de usuario,
- como respuesta a recibir dicha primera solicitud, producir un producto criptográfico,

- recibir, a través de dicho mecanismo de transporte seguro, una subsiguiente segunda solicitud que contiene uno de dicha serie de identificadores de usuario, y
- como respuesta a recibir dicha segunda solicitud, transmitir dicho producto criptográfico a través de dicho mecanismo de transporte seguro,

en el que dicho producto criptográfico es un grupo criptográfico digital que contiene dicha serie de identificadores de usuario y, por lo menos, una de:

- una clave criptográfica común para utilizar en criptografía simétrica entre usuarios identificados por dicha serie de identificadores de usuario,
- claves públicas específicas por usuario y relacionadas con el identificador de usuario, para utilizar en criptografía asimétrica en comunicaciones entre usuarios identificados por dicha serie de identificadores de usuario.

10. Procedimiento, según la reivindicación 9, que comprende:

- comprobar si dicha primera solicitud contenía una respectiva clave de cifrado específica por usuario para cada uno de dicha serie de identificadores de usuario, y
- responder al descubrimiento de que dicha primera solicitud no contenía una respectiva clave de cifrado específica por usuario para cada uno de dicha serie de identificadores de usuario, incrementando los datos recibidos en dicha primera solicitud para que contengan una respectiva clave de cifrado específica por usuario para cada uno de dicha serie de identificadores de usuario.

11. Procedimiento, según la reivindicación 9 o 10, que comprende:

- al producir dicho grupo criptográfico, utilizar una clave de firma para firmar digitalmente elementos de información incluidos en dicho grupo criptográfico.

12. Procedimiento, según cualquiera de las reivindicaciones 9 a 11, que comprende:

- comprobar, a partir de dicha subsiguiente segunda solicitud, si la solicitud está destinada a la disposición que ejecuta el procedimiento o a otro receptor, y
- responder, al descubrimiento de que la solicitud está destinada a otro receptor, reenviando dicha subsiguiente segunda solicitud hacia dicho otro receptor.

13. Procedimiento, según la reivindicación 12, que comprende:

- antes de dicho reenvío, reemplazar una autenticación original de dicha subsiguiente segunda solicitud con una autenticación de la disposición que ejecuta el procedimiento.

14. Producto de programa informático que comprende uno o varios conjuntos de una o varias instrucciones ejecutables por máquina que están configuradas para, cuando son ejecutadas por uno o varios procesadores, hacer que dicho uno o varios procesadores ejecuten un procedimiento, según cualquiera de las reivindicaciones 9 a 13.

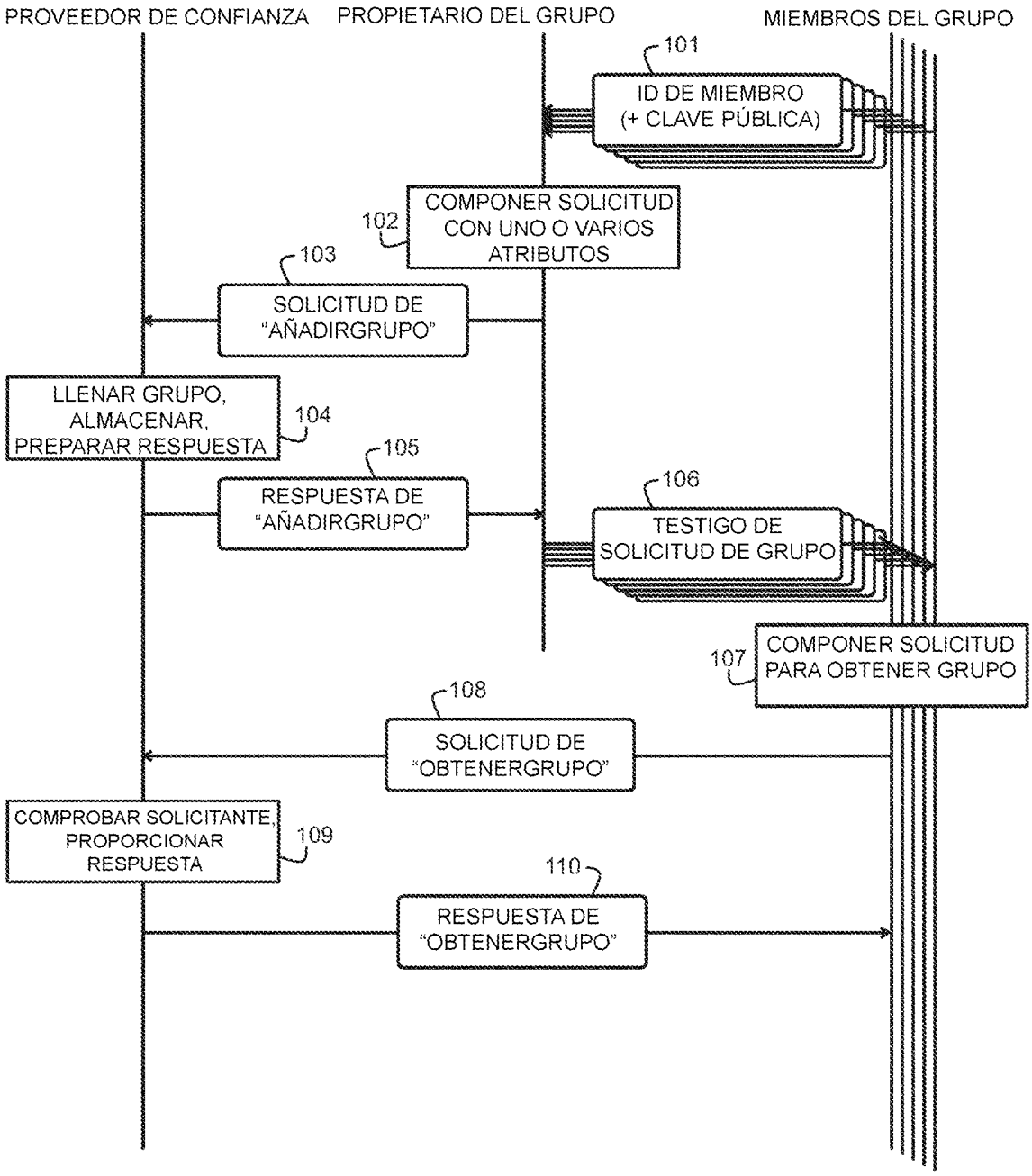
PROVEEDOR DE CONFIANZA
PROPIETARIO DEL GRUPO
MIEMBROS DEL GRUPO
101
ID DE MIEMBRO
(+ CLAVE PÚBLICA)
102
COMPONER SOLICITUD
CON UNO O VARIOS
ATRIBUTOS
103
SOLICITUD DE
"AÑADIRGRUPO"
LLENAR GRUPO,
ALMACENAR,
PREPARAR RESPUESTA
104
105
RESPUESTA DE
"AÑADIRGRUPO"
106
TESTIGO DE
SOLICITUD DE GRUPO
107
COMPONER SOLICITUD
PARA OBTENER GRUPO
108
SOLICITUD DE
"OBTENERGRUPO"
COMPROBAR SOLICITANTE,
PROPORCIONAR
RESPUESTA
109
110
RESPUESTA DE
"OBTENERGRUPO"

Fig. 1

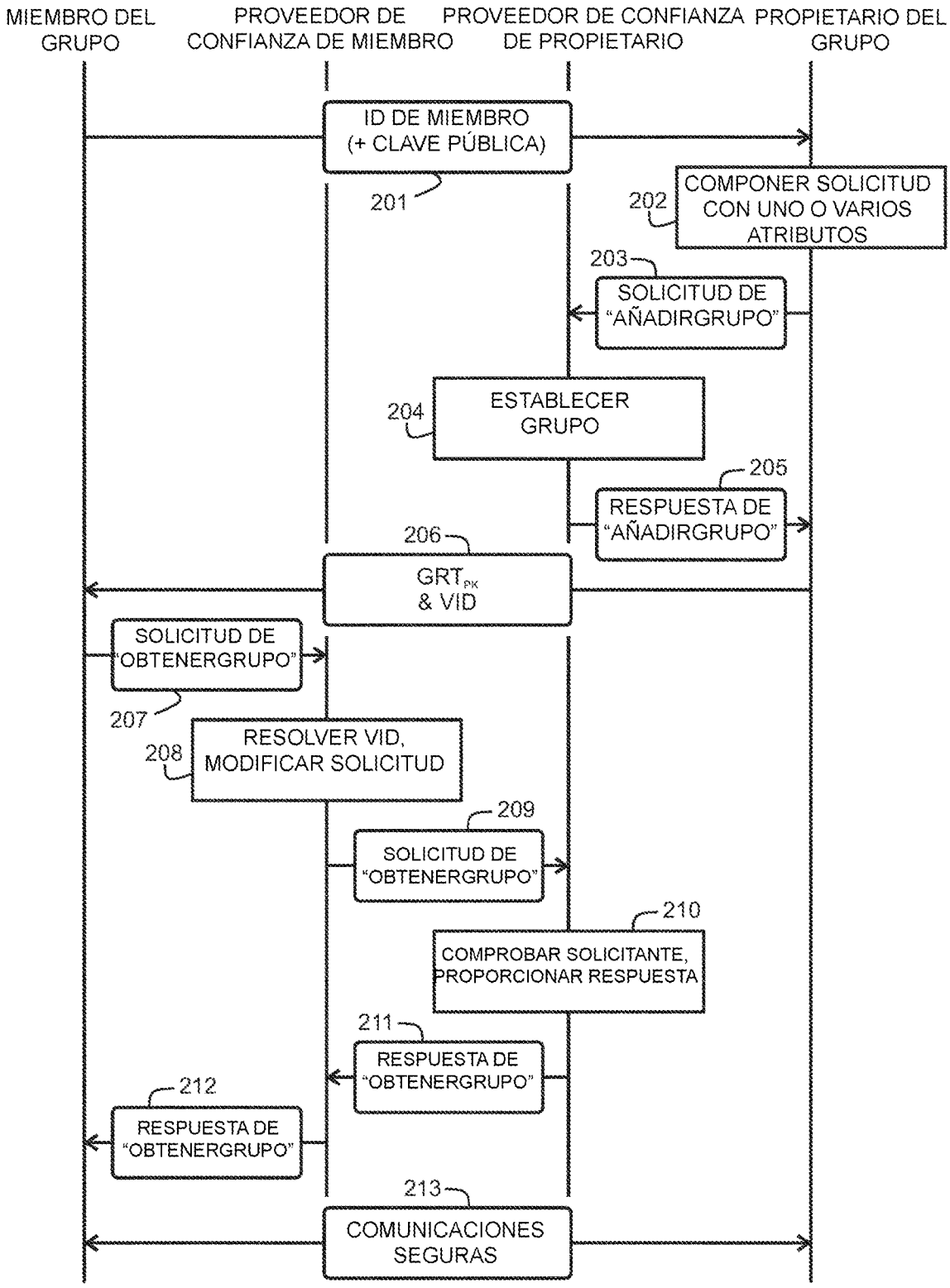
MIEMBRO DEL GRUPO
PROVEEDOR DE CONFIANZA DE MIEMBRO
PROVEEDOR DE CONFIANZA DE PROPIETARIO
PROPIETARIO DEL GRUPO
ID DE MIEMBRO (+ CLAVE PÚBLICA)
201
202
COMPONER SOLICITUD CON UNO O VARIOS ATRIBUTOS
203
SOLICITUD DE "AÑADIRGRUPO"
204
ESTABLECER GRUPO
205
RESPUESTA DE "AÑADIRGRUPO"
206
GRT PK & VID
SOLICITUD DE "OBTENERGRUPO"
207
208
RESOLVER VID, MODIFICAR SOLICITUD
209
SOLICITUD DE "OBTENERGRUPO"
210
COMPROBAR SOLICITANTE, PROPORCIONAR RESPUESTA
211
RESPUESTA DE "OBTENERGRUPO"
212
RESPUESTA DE "OBTENERGRUPO"
213
COMUNICACIONES SEGURAS

Fig. 2

REFERENCIAS CITADAS EN LA DESCRIPCIÓN

Esta lista de referencias citada por el solicitante es únicamente para mayor comodidad del lector. No forman parte del documento de la Patente Europea. Incluso teniendo en cuenta que la compilación de las referencias se ha efectuado con gran cuidado, los errores u omisiones no pueden descartarse; la EPO se exime de toda responsabilidad al respecto.

Documentos de patentes citados en la descripción

- US 2011320815 A
- EP 22157019