(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 741 176**

(51) Int. CI.:

H04N 7/16 (2011.01)
H04L 29/12 (2006.01)
H04L 29/06 (2006.01)
H04W 4/08 (2009.01)
H04W 84/08 (2009.01)
H04L 9/32 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **29.12.2011 PCT/US2011/067700**

(87) Fecha y número de publicación internacional: **05.07.2012 WO12092410**

(96) Fecha de presentación y número de la solicitud europea: **29.12.2011 E 11852249 (9)**

(97) Fecha y número de publicación de la concesión europea: **08.05.2019 EP 2659667**

(54) Título: **Método de establecimiento de grupos seguros de contactos de confianza con derechos de acceso en un sistema de comunicación segura**

(30) Prioridad:

30.12.2010 US 201061428586 P

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

(73) Titular/es:

CELLCRYPT INC. (100.0%)
8300 Boone Boulevard, Suite 500
Vienna, VA 22182-2681, US

(72) Inventor/es:

GALWAS, PAUL, ANTHONY

(74) Agente/Representante:

INGENIAS CREACIONES, SIGNOS E INVENCIONES, SLP

DESCRIPCIÓN

Método de establecimiento de grupos seguros de contactos de confianza con derechos de acceso en un sistema de comunicación segura

Campo de la invención

La presente divulgación se refiere a la provisión de comunicaciones de voz y otras comunicaciones de datos digitales en tiempo real a través de redes. En particular, la presente divulgación se refiere al establecimiento de grupos seguros de contactos de confianza entre puntos de extremo en un sistema de comunicación segura.

Antecedentes de la invención

En los sistemas de red, tales como la telefonía móvil, es importante llevar a cabo unos protocolos que establezcan una comunicación segura de datos en tiempo real a través de una red. Hay un campo establecido de comunicaciones en tiempo real a través de redes de Protocolo de Internet (IP, por sus siglas en inglés), que apuntala unas aplicaciones ampliamente generalizadas tales como Voz a través de IP (VoIP, por sus siglas en inglés). Hay protocolos convencionales tales como Protocolo de Inicio de Sesión (SIP, por sus siglas en inglés) y Protocolo de Transporte en Tiempo Real (RTP, por sus siglas en inglés) que soportan un tráfico en tiempo real no cifrado. El protocolo RTP Seguro (SRTP, por sus siglas en inglés) se ha ampliado para cifrar el tráfico en tiempo real. No obstante, ninguno de estos protocolos considera el establecimiento de una comunidad de grupos seguros de contactos de confianza para proporcionar adicionalmente unas comunicaciones seguras.

La presente divulgación se dirige hacia, pero no se limita a, la mejora de los problemas que se han hecho notar en lo que antecede mediante el establecimiento de grupos seguros de contactos de confianza en un sistema de comunicación segura.

Sumario de la invención

Algunas formas de realización a modo de ejemplo que se divulgan en el presente documento proporcionan un método de establecimiento de grupos seguros de contactos de confianza con derechos de acceso en un sistema de comunicación segura. El método, por ejemplo, incluye establecer, por un punto de extremo, grupos seguros de contactos de confianza en el sistema de comunicación segura; almacenar una información, por un gestor de bases de datos, que se corresponde con contactos de confianza de un grupo seguro, como un grupo seguro en una base de datos; y determinar unos derechos de acceso, por el punto de extremo, del grupo seguro y almacenar los derechos de acceso en la base de datos con la información almacenada que se corresponde con el grupo seguro.

Algunas formas de realización a modo de ejemplo también proporcionan un método de comunicación en un sistema de comunicación segura con grupos seguros de contactos de confianza y derechos de acceso, el método incluye, por ejemplo, iniciar una operación deseada para otro punto de extremo en el sistema de comunicación; verificar una base de datos de grupos seguros para verificar si el nombre que está asociado con el otro punto de extremo está enumerado en la base de datos; verificar los derechos de acceso que están asociados con el grupo seguro del otro punto de extremo si el nombre del punto de extremo está enumerado en la base de datos; determinar si se concede un permiso para llevar a cabo la operación deseada a partir de los derechos de acceso asociados; y llevar a cabo la operación deseada si se concede un permiso para llevar a cabo la operación deseada.

Breve descripción de los dibujos

La figura 1 es un diagrama de bloques que ilustra una forma de realización a modo de ejemplo de un sistema de comunicación tal como se divulga en el presente documento.
La figura 2 es un diagrama de bloques que ilustra una forma de realización a modo de ejemplo de una base de datos de grupos seguros.
La figura 3 es un diagrama de flujo que ilustra una representación a modo de ejemplo de uso de derechos de acceso en la base de datos de grupos seguros para controlar unas comunicaciones de datos.

Descripción detallada

La presente divulgación describe un protocolo de comunicación para proporcionar unas comunicaciones seguras en tiempo real en un sistema de red. El protocolo es eficiente en cuanto al ancho de banda y usa unos datos y mensajes mínimos para efectuar unas comunicaciones en tiempo real seguras en la red. El protocolo lleva a cabo una autenticación mutua y genera múltiples secretos compartidos para unas comunicaciones cifradas.

La figura 1 es un diagrama que ilustra una forma de realización a modo de ejemplo de un sistema de comunicación. El sistema incluye el punto de extremo 1010 que se comunica a través de la red inalámbrica 1000 con el sistema de red 1100 y el punto de extremo 1020 que se comunica con el sistema de red a través de la red inalámbrica 1200. El

sistema de red interconecta dos puntos de extremo en el sistema de comunicación, y el sistema de comunicación puede incluir dos o más puntos de extremo.

El punto de extremo 1010 puede ser, por ejemplo, un punto de extremo móvil, que incluye un equipo móvil (por ejemplo, un teléfono móvil) que está equipado con unos módulos de cifrado. Los módulos de cifrado proporcionan unas funciones de cifrado y de descifrado para datos de voz en tiempo real y establecen un enlace de comunicación segura con otro punto de extremo en el sistema de comunicación. Los módulos de cifrado pueden ser procesadores en los que hay insertadas unas instrucciones legibles por ordenador que, cuando se ejecutan, llevan a cabo unas funciones de cifrado y de descifrado.

El punto de extremo 1010 incluye la base de datos de contactos de confianza 1015, que almacena una lista de contactos de confianza (1 a n) (es decir, los puntos de extremo de confianza en el sistema de comunicación), unas bases de datos de grupos seguros 1075a y 1075b, que almacena una lista de grupos seguros y una información asociada y un gestor de bases de datos 1045. Los contactos de confianza se describen en la solicitud en trámite junto con la presente, "*A Method of Establishing Trusted Contacts With Access Rights in a Secure Communication System*", solicitud de patente de EE. UU. con número de publicación US20140150074A1 (número de solicitud 13/977068).

Un grupo seguro es un conjunto heterogéneo de contactos de confianza que están almacenados en la base de datos de grupos seguros 1075a, tal como se ilustra en la figura 2A. Cada grupo seguro contiene una lista de contactos de confianza. Cada contacto de confianza contiene, para un punto de extremo dado: nombre, ID de parte que llama, ID de elemento del mismo nivel, Credencial N y, de forma opcional, Credencial (que no se muestra) y derechos de acceso. El nombre es una cadena definida por el usuario para identificar el contacto. La ID de parte que llama se puede usar como una ID de parte que llama o una ID de parte llamada, y Credencial Z es AAZpub, o Cert-AAZ, y Z se corresponde con el punto de extremo 1010, el punto de extremo 1020, una pasarela 1030, o unos terminales o servicios específicos en la red de PBX a la que se conecta la pasarela 1030.

Para cada contacto de confianza, se almacenan unos derechos de acceso que definen un conjunto de permisos que están asociados con el contacto de confianza correspondiente. Para cada grupo seguro, se almacenan un certificado de grupo y unos derechos de acceso en la base de datos de grupos seguros 1075b. Los derechos de acceso de grupo seguro definen un conjunto de permisos que están asociados con la totalidad de los contactos de confianza dentro de un grupo seguro correspondiente, tal como se ilustra en la figura 2B.

La ID de elemento del mismo nivel identifica el dispositivo para el servidor de medios y se genera usando un generador de números aleatorios. En otra forma de realización a modo de ejemplo, la ID de elemento del mismo nivel se deriva de una clave pública de un par de claves criptográficas asimétrico que son generadas por un punto de extremo cuando se crea la misma. La ID de elemento del mismo nivel de un punto de extremo es independiente de la dirección de IP y se usa para identificar mensajes de medios a partir de un punto de extremo correspondiente en el sistema de comunicación.

La ID de parte que llama es el número de teléfono seguro por medio del cual el punto de extremo o la pasarela que inicia una llamada se direcciona en la red que porta llamadas cifradas. La ID de parte llamada es el número de teléfono seguro por medio del cual el punto de extremo o la pasarela que recibe la llamada se direcciona en la red que porta llamadas cifradas.

En otra forma de realización a modo de ejemplo, la ID de parte que llama y la ID de parte llamada se identifican por medio de un intervalo de confianza, que es un conjunto heterogéneo de elementos que pueden especificar todos los números de teléfono seguros que comienzan con un prefijo especificado y / o todos los números de teléfono seguros en un intervalo especificado.

AAZpub es el valor de clave pública del dispositivo Z. Cert-AAZ es el certificado digital que está asociado con el dispositivo Z y Z se corresponde con el punto de extremo 1010, el punto de extremo 1020 o la pasarela 1030. El certificado digital puede identificar un dispositivo, una persona, un atributo de uno u otra (por ejemplo, una ID de parte que llama, una dirección de correo electrónico, una ID de elemento del mismo nivel) o la combinación.

Los derechos de acceso son un conjunto de permisos. Los permisos de contacto de confianza podrían incluir el derecho de realizar o de recibir un mensaje de llamada segura, tal como un correo electrónico, un SMS o un IM, de ver un número de teléfono u otro identificador, de acceder a un buzón de voz o puente de conferencia y de transferir una llamada. Por ejemplo, el punto de extremo 1010 puede tener un permiso para enviar llamadas a una organización O que está acoplada con la pasarela 1030. Los derechos de acceso pueden ser de aplicación solo durante un intervalo de tiempo especificado, tal como la hora del día o la semana, y los derechos de acceso pueden tener un nivel de confianza asociado, que es un número entero positivo.

Los permisos de grupo seguro podrían incluir el derecho, para cualquier miembro de grupo, de realizar o recibir llamadas, mensajes, correos electrónicos, SMS o IM. Por ejemplo, cada uno del punto de extremo 1010 y el punto de extremo 1030 pueden tener, como un contacto de confianza, un permiso para enviar llamadas a la organización

O y, como un grupo seguro (es decir, un grupo seguro que comprende el punto de extremo 1010 y 1020), los puntos de extremo 1010 y 1020 pueden tener un permiso para enviar llamadas a un departamento D dentro de la organización O.

Los derechos de acceso de contacto de confianza y los derechos de acceso de grupo seguro pueden incluir el mismo tipo de derechos, pero el valor de esos derechos puede ser diferente. Un derecho que es de aplicación de modo uniforme a un conjunto de puntos de extremo (es decir, un derecho de acceso de grupo seguro) es más rápido de verificar y de mantener que los derechos equivalentes que están asociados directamente con cada punto de extremo en el conjunto. Así mismo, los derechos de grupo seguro requieren menos datos en el almacenamiento y la transmisión.

Cada punto de extremo tiene un nivel de confianza de punto de extremo asociado, que es un número entero positivo. Se supone que un punto de extremo con un nivel de confianza más alto es de más confianza que uno con un nivel de confianza más bajo. El nivel de confianza se almacena de forma opcional en la entrada de base de datos de contactos de confianza que está asociada con el punto de extremo. El nivel de confianza se puede establecer cuando se define el contacto de confianza, o bien por el usuario en el punto de extremo, o bien en un directorio central.

Los derechos de acceso pueden incluir de forma opcional un nivel de confianza. En particular, para diferentes niveles de confianza pueden ser de aplicación diferentes derechos de acceso. Por ejemplo, un punto de extremo puede tener el derecho de llamar a un punto de extremo con el mismo nivel de confianza, pero no de llamar a un punto de extremo con un nivel de confianza más alto.

Antes de llevar a cabo una función que involucra otro punto de extremo, un punto de extremo confirma que el nivel de confianza del derecho de acceso que está asociado con el otro punto de extremo es más grande que o igual al del nivel de confianza de punto de extremo. De lo contrario, este deniega la función. Cuando se define un nivel de confianza para el contacto de confianza y sus derechos de acceso, el nivel del derecho de acceso tiene prioridad.

El gestor de bases de datos 1045 incluye uno o más microprocesadores, una memoria legible por ordenador (por ejemplo, una memoria de solo lectura (ROM, por sus siglas en inglés) y una memoria de acceso aleatorio (RAM, por sus siglas en inglés)), unos mecanismos y estructuras para llevar a cabo operaciones de E / S. El gestor de bases de datos puede ejecutar un sistema operativo para la ejecución de órdenes en los uno o más microprocesadores y un programa de aplicación para controlar las operaciones de la base de datos de contactos de confianza 1015. El programa de aplicación se puede desarrollar usando cualquier lenguaje de programación informática adecuado, tal como, por ejemplo, programación en Java.

El punto de extremo 1010 incluye un dispositivo de almacenamiento (que no se muestra), que se puede poner en práctica con una diversidad de componentes o subsistemas que incluyen, por ejemplo, una unidad de disco magnético, una unidad de disco óptico, una memoria flash, o cualquier otro dispositivo capaz de almacenar de forma persistente una información. El dispositivo de almacenamiento almacena la base de datos de contactos de confianza.

El punto de extremo 1020 puede ser, por ejemplo, otro punto de extremo móvil, tal como el punto de extremo 1010, o un dispositivo de pasarela, tal como la pasarela 1030. El punto de extremo 1020 incluye una base de datos de contactos de confianza 1025, unas bases de datos de grupos seguros 1085a y 1085b y el gestor de bases de datos 10055 tal como se ha descrito en lo que antecede. La pasarela 1030 conecta un sistema telefónico tradicional, tal como, por ejemplo, Red Telefónica Pública Conmutada (PSTN, por sus siglas en inglés) y una central de conmutación (PBX, por sus siglas en inglés) con el sistema de red 1100. La pasarela convierte el tráfico telefónico de PSTN o de PBX a un formato de IP para la transmisión a través de una red de IP.

La pasarela 1030 está equipada con un módulo de cifrado para facilitar unas funciones de cifrado y de descifrado. Se proporciona un cifrado de punto a punto transparente entre el punto de extremo 1010 y el punto de extremo 1020, y entre el punto de extremo 1010 y la pasarela 1030. La pasarela 1030 incluye una base de datos de contactos de confianza 1035, unas bases de datos de grupos seguros 1095a y 1095b y el gestor de bases de datos 1045 tal como se ha descrito en lo que antecede.

Los módulos de cifrado pueden usar esquemas redundantes de cifrado para la sesión, la autenticación, el resumen y / o el intercambio de claves. Algunas formas de realización preferidas usan dos algoritmos fuertes en serie al mismo tiempo. El cifrado de los datos se puede llevar a cabo usando cualquier algoritmo de criptografía conocido, tal como, por ejemplo, Diffie-Hellman de Curva Elíptica (ECDH, por sus siglas en inglés), Rivest, Shamir y Adleman (RSA), Norma de Cifrado Avanzado (AES, por sus siglas en inglés), Algoritmo de Firma Digital (DSA, por sus siglas en inglés), etc.

En una forma de realización a modo de ejemplo, los contactos de confianza y los grupos seguros se almacenan en un directorio central (por ejemplo, Protocolo Ligero de Acceso a Directorios (LDAP, por sus siglas en inglés) o Directorio Activo de Microsoft). Los datos se procesan ahí y se distribuyen usando unos medios convencionales a los

puntos de extremo. Los datos se pueden asociar con otros elementos de datos que están asociados con el punto de extremo y / o el usuario de punto de extremo.

Las redes 1000 y 1200 son sistemas de red inalámbricos, tales como, por ejemplo, Sistemas Globales para las Comunicaciones Móviles (GSM, por sus siglas en inglés), Tasas de Datos Potenciadas para la Evolución de las GSM (EDGE, por sus siglas en inglés), Servicio General de Radio por Paquetes (GPRS, por sus siglas en inglés), GSM de 3G, HSPA, UMTS, CDMA y Wi-Fi.

El sistema de red 1100 es un sistema de red cableado, tal como, por ejemplo, un sistema de Protocolo de Internet (IP, por sus siglas en inglés). El sistema de red puede incluir uno o más servidores de señalización y uno o más servidores de medios. Un punto de extremo envía una solicitud al servidor de señalización para realizar una llamada o enviar un mensaje a otro punto de extremo. El servidor de señalización establece la llamada, indicando a cada punto de extremo que entre en contacto con el mismo servidor de medios. Los puntos de extremo envían los datos en tiempo real uno a otro a través del servidor de medios. El servidor de medios usa unos protocolos de medios para recibir datos de voz y enviar los mismos a través de la red.

El dispositivo de almacenamiento 1140 se puede poner en práctica con una diversidad de componentes o subsistemas que incluyen, por ejemplo, una unidad de disco magnético, una unidad de disco óptico, una memoria flash, o cualquier otro dispositivo capaz de almacenar de forma persistente una información. El dispositivo de almacenamiento 1140 incluye la base de datos de dispositivos 1125, que contiene una lista de la totalidad de las ID de Dispositivo que son conocidas por el sistema.

La arquitectura que se muestra en la figura 1 prevé una comunicación (por ejemplo, transmisión de datos, llamada de teléfono y vídeo) entre dos puntos de extremo o entre un punto de extremo y una pasarela en el sistema. Las comunicaciones en tiempo real entre dos puntos de extremo o entre un punto de extremo y una pasarela se cifran usando una o más claves de sesión que se derivan de un secreto compartido que es conocido solo por los puntos de extremo.

No obstante, antes de que se lleve a cabo comunicación segura alguna entre los puntos de extremo o un punto de extremo y una pasarela, el sistema determina si la parte solicitante es un contacto de confianza o un miembro de un grupo seguro, y los derechos de acceso asociados se verifican para determinar si se puede permitir el acceso que se ha solicitado.

Los grupos seguros son establecidos por un usuario en un punto de extremo o usando un servicio de grupo. El usuario de un punto de extremo puede compilar una base de datos de grupos seguros al llevar a cabo lo siguiente: Para cada grupo seguro,

1) Preguntar al usuario para que introduzca los nombres de los contactos que están asociados con el grupo seguro;
2) El punto de extremo verifica si cada contacto está enumerado en la base de datos de contactos de confianza;
3) De ser así, se verifica el certificado de cada contacto de confianza, y el contacto se añade al grupo seguro.
4) Si todos los certificados se verifican con éxito, se establece el grupo seguro. De forma opcional, el punto de extremo puede firmar el grupo seguro con su clave privada, creando de ese modo un certificado de grupo asociado para que el grupo muestre una autenticidad de origen. No obstante, puede que esto no sea necesario si el grupo seguro nunca abandona el punto de extremo. La información de grupo seguro se almacena en las bases de datos de grupos seguros.

En otra forma de realización a modo de ejemplo, después de la verificación de un certificado de un contacto de confianza, el punto de extremo sustituye el certificado que está almacenado en el contacto de confianza con la Clave Pública correspondiente a partir del contacto de confianza, por ejemplo, Nombre, ID de parte que llama, ID de elemento del mismo nivel, Certificado 1, Certificado 2 se sustituye con Nombre, ID de parte que llama, ID de elemento del mismo nivel, Clave Pública 1, Clave Pública 2. Por medio de este proceso, no es necesario que los usuarios del grupo seguro verifiquen, a continuación de lo anterior, el certificado asociado para cada contacto de confianza.

Una vez que se ha definido el grupo seguro y se ha recibido una solicitud de añadir un contacto nuevo al grupo seguro definido, el punto de extremo verifica que el contacto es un contacto de confianza y valida el certificado del contacto de confianza. Cuando un contacto no tiene un certificado asociado, la confianza se establece usando 'confianza en el primer uso' (TOFU, por sus siglas en inglés). Con TOFU, después de la primera llamada a, o a partir de, un punto de extremo que previamente no era de confianza, el punto de extremo del usuario pregunta al usuario si este desea confiar en el contacto nuevo. En general, el usuario decidirá si confiar en este contacto nuevo a través de un proceso fuera de banda, que puede incluir el uso del código de autenticación. Si el usuario decide confiar en el punto de extremo, el punto de extremo del usuario crea un contacto de confianza, que contiene la clave pública (pero no tiene certificado alguno). Un contacto de confianza de este tipo puede entonces ser un miembro legítimo de un grupo seguro.

Cuando se define un grupo seguro, o en cualquier instante durante su tiempo de vida, se pueden definir los derechos de acceso asociados:

a. A partir de un conjunto por defecto de derechos de acceso que se almacenan en el punto de extremo o se procesan en el directorio central;
b. Al preguntar al usuario de un punto de extremo para que especifique qué derechos pueden ser de aplicación cuando se define o se edita el grupo seguro; o
c. Por medio de un servicio de grupo que define y gestiona los grupos seguros en una base de datos central.

Como alternativa, se puede usar un servicio de grupo para establecer los grupos seguros. Un servicio de grupo es un administrador central, (es decir, una entidad que está separada del punto de extremo y que está compuesta de soporte físico y soporte lógico), que define y gestiona los grupos seguros en una base de datos central. El servicio de grupo distribuye los grupos seguros establecidos a uno o más puntos de extremo en el sistema de comunicación, usando cualquier mecanismo convencional tal como, por ejemplo, Directorio Activo o Protocolo Ligero de Acceso a Directorios (LDAP, por sus siglas en inglés).

En una forma de realización a modo de ejemplo de la presente divulgación, el sistema de comunicación incluye uno o más servicios de grupo, cada uno de los cuales opera de forma independiente para definir y gestionar los grupos seguros en el sistema de comunicaciones.

Los grupos seguros se establecen cuando el servicio de grupo compila una lista de grupos seguros en un directorio central, que se distribuyen más adelante a un conjunto de puntos de extremo.

Para cada grupo seguro,

1. El servicio de grupo enumera los nombres de los contactos
2. El servicio de grupo verifica si los contactos están enumerados en la base de datos de contactos de confianza central.
3. El servicio de grupo valida los certificados de los contactos de confianza.
4. El servicio de grupo define y añade los derechos de acceso para el grupo.
5. El servicio de grupo almacena el grupo seguro en las bases de datos de grupos seguros centrales.

El servicio de grupo valida los certificados de cada contacto de confianza en un grupo seguro usando mecanismos convencionales, tales como, por ejemplo, recorriendo la cadena de certificados y / o el protocolo de estado de certificado en línea (OCSP, por sus siglas en inglés).

El servicio de grupo puede cambiar un derecho de acceso que está asociado con un grupo seguro en las bases de datos de grupos seguros centrales.

En otra forma de realización a modo de ejemplo, el servicio de grupo puede evitar que un usuario cambie los derechos de acceso que están asociados con un grupo seguro.

En otra forma de realización a modo de ejemplo, un usuario puede cambiar un derecho de acceso que está asociado con un grupo seguro.

Una vez que se han definido los grupos seguros, los contactos nuevos se añaden a un grupo seguro al llevar a cabo lo siguiente,

1. El servicio de grupo verifica si los contactos están enumerados en la base de datos de contactos de confianza central;
2. El servicio de grupo valida los certificados de los contactos de confianza;
3. El servicio de grupo añade el contacto de confianza al grupo seguro (de forma opcional, cambiando el certificado del contacto a la clave pública);
4. El servicio de grupo firma el grupo seguro con su Clave Privada de Grupo.

En otra forma de realización a modo de ejemplo, el grupo seguro contiene una firma bajo una Clave Privada de Grupo, que tiene un certificado de grupo y está asociada con el servicio de grupo. El certificado de grupo puede ser, por ejemplo, un certificado digital de X.509 convencional. Durante el proceso de firma, el servicio de grupo verifica todos los certificados en el grupo seguro, y un contacto de confianza solo se añade al grupo seguro si se validan todos los certificados asociados. Cuando se crea o se cambia un grupo seguro, el servicio de grupo firma el grupo seguro con su Clave Privada de Grupo (es decir, el proceso de firma), para permitir que las partes dependientes validen la integridad de origen del grupo seguro. Esta firma también indica de forma implícita que el servicio de grupo ha validado los contactos seguros en el grupo seguro.

En otra forma de realización a modo de ejemplo, después de la verificación de un certificado de un contacto de confianza, el servicio de grupo sustituye el certificado en la base de datos de grupos seguros con la Clave Pública

correspondiente, por ejemplo, Nombre, ID de parte que llama, ID de elemento del mismo nivel, Certificado 1, Certificado 2, se sustituye con Nombre, ID de parte que llama, ID de elemento del mismo nivel, Clave Pública 1, Clave Pública 2. Por medio de este proceso, no es necesario que los usuarios del grupo seguro verifiquen, a continuación de lo anterior, el certificado asociado para cada contacto de confianza. Por lo tanto, los puntos de extremo que usan el contacto seguro (en el grupo seguro) pueden confiar en el contacto seguro gracias a la confianza en el grupo seguro, en lugar de a través de tener que validar cada contacto seguro de forma separada (a través de su cadena de certificados), potencialmente cada vez que se usa un contacto seguro, por ejemplo, para realizar o recibir una llamada. Esto da como resultado una reducción muy significativa de la carga de procesamiento y de comunicación en el sistema.

El servicio de grupo es capaz de distribuir los grupos seguros de forma frecuente a un punto de extremo y tiene un certificado de grupo asociado que tiene un tiempo de vida corto al menos durante tanto tiempo como lleve redistribuir todos los contactos de confianza a los puntos de extremo. En particular, no es necesario que haya relación alguna entre el tiempo de vida de los certificados originales y el de un grupo seguro. Por lo tanto, no es necesario que el punto de extremo verifique una lista de tipo Lista de Revocación de Certificados (CRL, por sus siglas en inglés) o que usan un Protocolo de Estado de Certificado en Línea (OCSP, por sus siglas en inglés) cuando se carga un grupo seguro a partir del servicio de grupo.

Una CRL contiene un registro para cada certificado revocado que es emitido por la autoridad de certificación asociada. La autoridad de certificación vuelve a emitir una CRL de forma periódica para mantener la misma actualizada. Una parte que confía (por ejemplo, un punto de extremo) ha de verificar la totalidad de la CRL actual al tiempo que se valida cada certificado. Cuando se valida cada certificado, una parte que confía ha de validar la cadena de certificados de vuelta a la autoridad de certificación (CA, por sus siglas en inglés), y verificar la 'vitalidad' (por ejemplo, si se ha revocado el certificado) del certificado o bien usando OSCP o bien verificando las CRL de las CA asociadas.

Cuando el tiempo de vida de un certificado es larga en comparación con la frecuencia de renovación de entidades a las que hace referencia el certificado, la CRL tiende a crecer de forma significativa, debido a que, por lo general el número de certificados emitidos supera, en un factor significativo, el número de certificados emitidos y que siguen siendo válidos. El esfuerzo de la verificación, por parte de la parte que confía, de todas las entradas en una CRL domina entonces el proceso de validación de certificados.

La CRL podría hacer referencia al certificado en un grupo seguro, reduciendo de ese modo el número de CRL que sería necesario que se verificaran si la CRL fuera a hacer referencia a la totalidad de los miembros del grupo. Una CRL podría estar asociada con un grupo seguro, por lo que es necesario que esta considere solo un subconjunto de los certificados emitidos, haciendo el mismo, en general, más pequeño.

El protocolo OCSP permite que un punto de extremo de parte que confía verifique la validez de un certificado que está asociado directamente con un punto de extremo y que está asociado con una Clave de Firma de Grupo, con un servicio de terceros cada vez que la misma busque la validación de un certificado. Esto impone una carga de cómputo y de comunicaciones adicional sobre el punto de extremo, en comparación con no usar el protocolo OCSP.

El punto de extremo que confía podría verificar de forma periódica el certificado de grupo seguro usando el servicio de grupo de OCSP, lo que validaría que la totalidad de las entradas en el grupo seguro siguen siendo válidas, aminorando de ese modo la carga de OCSP.

Cuando un punto de extremo carga un grupo seguro a partir del servicio de grupo, este verifica el certificado de grupo frente a su cadena de certificados, comenzando con el certificado de servicio de grupo y con raíz en una clave pública que está contenida en el punto de extremo. El punto de extremo verifica el certificado de grupo por medio de mecanismos convencionales, tales como, por ejemplo, OCSP y cadena de confianza / CRL. El punto de extremo solo carga el grupo seguro si se verifica el certificado. Este proceso asegura que el grupo seguro tiene una integridad de origen a partir del servicio de grupo.

Cuando se carga el grupo seguro verificado, el punto de extremo extrae cada contacto de confianza a partir del conjunto en el grupo seguro y lo añade a la base de datos de contactos de confianza. El punto de extremo sobrescribe un contacto de confianza existente con esa misma ID de parte que llama e ID de elemento del mismo nivel. El punto de extremo preguntará al usuario si se ha de sobrescribir un contacto de confianza existente con la misma ID de parte que llama (ID de elemento del mismo nivel) pero una ID de elemento del mismo nivel (ID de parte que llama) diferente.

El servicio de grupo, por ejemplo, un servicio de grupo A, puede cargar un grupo seguro verificado a partir de otro servicio de grupo, por ejemplo, un servicio de grupo B. Por ejemplo, si un grupo seguro es recibido por el servicio de grupo A desde el servicio de grupo B, el servicio de grupo A ha de verificar el grupo seguro para confirmar la integridad de origen desde el servicio de grupo B (es decir, frente a la Clave de Firma de Grupo y el certificado asociado de B). Entonces, el servicio de grupo A volverá a firmar (y, de forma opcional, volverá a validar los contactos seguros en el grupo seguro) el grupo seguro de tal modo que los puntos de extremo en la organización del

servicio de grupo A (que, en general, no tendrá una relación de confianza directa con la CA del servicio de grupo B) pueden confiar en sus contenidos. Cuando se carga el grupo seguro verificado, el servicio de grupo extrae cada contacto de confianza a partir del conjunto en el grupo seguro y usa los datos para construir otros grupos seguros. De esta forma, un servicio de grupo puede actuar como un agente de confianza para otros servicios de grupo.

En particular, un punto de extremo que confía en un servicio de grupo no necesita confiar en otros. Un punto de extremo que está asociado con un servicio de grupo, tendrá acceso al certificado del servicio de grupo, a través del cual este puede confiar en las firmas que son realizadas por ese servicio de grupo. Por ejemplo, un servicio de grupo de confianza podría estar asociado con una organización, y otro servicio de grupo de confianza con otra organización. Cada servicio de grupo de confianza puede establecer de forma independiente la confianza en los grupos seguros que administra este.

Los contactos de confianza que están asociados con una PKI pueden ser usados por los puntos de extremo que confían en otro servicio de grupo. Así mismo, se pueden construir los contactos de confianza que no confían en una PKI pero que confían en su servicio de grupo.

Una vez que se han establecido las bases de datos de grupos seguros, las comunicaciones entre puntos de extremo o entre un punto de extremo y una pasarela se llevan a cabo tal como se ilustra en la figura 3. En la etapa 3000, un punto de extremo / pasarela (por ejemplo, el punto de extremo 1010) inicia una operación deseada (por ejemplo, una llamada) para otro punto de extremo (por ejemplo, el punto de extremo 1020). El punto de extremo 1010 inicia la operación deseada mediante el envío del nombre que está asociado con el punto de extremo / pasarela y la operación deseada al gestor de bases de datos (por ejemplo, el gestor de bases de datos 1045).

En la etapa 3001, el gestor de bases de datos verifica la base de datos (por ejemplo, la base de datos 1075a) para verificar si el nombre que está asociado con el punto de extremo / pasarela se encuentra en un grupo seguro. Debido a que solo están enumerados los grupos seguros en la base de datos de grupos seguros 1075a, el gestor de bases de datos determina si el nombre está enumerado en la base de datos y, si no lo está, entonces el punto de extremo / pasarela asociado no se encuentra en un grupo seguro y no se permite la comunicación.

Si el punto de extremo se encuentra en un grupo seguro, el gestor de bases de datos confirma si se concede un permiso para llevar a cabo la operación deseada, en la etapa 3002. El gestor de bases de datos verifica los derechos de acceso que están asociados con el grupo seguro para determinar si es admisible la operación deseada, y si no se permite la operación deseada, se evita la comunicación del tiempo que se desea. Cuando hay un conflicto entre un derecho de acceso de contacto de confianza y un derecho de acceso de grupo seguro, el derecho de acceso de contacto de confianza tiene prioridad.

Si se permite la operación deseada, la operación se lleva a cabo en la etapa 3003.

Tal como se divulga en el presente documento, algunas formas de realización y características de la invención se pueden poner en práctica a través de soporte físico y / o soporte lógico informático. Tales formas de realización se pueden poner en práctica en diversos entornos, tales como entornos basados en informática y en red. La presente invención no se limita a tales ejemplos, y algunas formas de realización de la invención se pueden poner en práctica con otras plataformas y en otros entornos.

Además, a pesar de que en el presente documento se han descrito algunas formas de realización ilustrativas de la invención, algunas formas de realización adicionales pueden incluir elementos, modificaciones, omisiones, combinaciones (por ejemplo, de aspectos por diversas formas de realización), adaptaciones y / o alteraciones equivalentes, tal como sería apreciado por los expertos en la materia sobre la base de la presente divulgación.

REIVINDICACIONES

1. Un método de establecimiento de grupos seguros de contactos de confianza con derechos de acceso en un sistema de comunicación segura, que comprende las etapas de:

establecer, por un punto de extremo (1010), grupos seguros de contactos de confianza en el sistema de comunicación segura;
almacenar una información, por un gestor de bases de datos (1045) del punto de extremo (1010), que se corresponde con contactos de confianza de un grupo seguro, como un grupo seguro en una base de datos (1015, 1075a, 1075b) del punto de extremo (1010); y
en donde la información identifica los contactos de confianza y sus derechos de acceso individuales respectivos dentro del grupo seguro;
determinar unos derechos de acceso de grupo, por el punto de extremo (1010), del grupo seguro y almacenar los derechos de acceso de grupo en la base de datos (1015, 1075a, 1075b) del punto de extremo (1010) con la información almacenada que se corresponde con el grupo seguro,
caracterizado por que
la base de datos (1015, 1075a, 1075b) y el gestor de bases de datos (1045) están incluidos en el punto de extremo (1010), en donde la base de datos (1015, 1075a, 1075b) incluye:

a) una información de contacto de confianza que incluye un nombre, una ID de parte que llama, una ID de elemento del mismo nivel, una credencial y unos derechos de acceso de cada uno de los contactos de confianza, comprendiendo la credencial un certificado criptográfico del contacto de confianza respectivo, y
b) una información de grupo seguro que incluye una ID de grupo, un certificado de grupo y unos derechos de acceso de grupo de cada uno de los grupos seguros,

comprendiendo adicionalmente el método sustituir los certificados de los contactos de confianza con unas claves públicas correspondientes del grupo seguro tras la verificación de los certificados de los contactos de confianza.

2. El método de la reivindicación 1, en donde los grupos seguros son establecidos, como alternativa, por un servicio de grupo.

3. El método de la reivindicación 2, en donde el servicio de grupo distribuye la lista de grupos seguros a los puntos de extremo (1010) en el sistema de comunicación.

4. El método de la reivindicación 1, en donde cada punto de extremo (1010) y cada pasarela (1030) en el sistema de comunicación segura incluye una base de datos (1015, 1075a, 1075b) de grupos seguros.

5. Un método de comunicación en un sistema de comunicación segura con grupos seguros de contactos de confianza y derechos de acceso, que comprende las etapas de:

iniciar, por un punto de extremo (1010), una operación deseada para otro punto de extremo (1020) en el sistema de comunicación;
verificar, por un gestor de bases de datos (1045) del punto de extremo (1010), una base de datos (1015, 1075a, 1075b) que incluye una información que se corresponde con contactos de confianza de grupos seguros para verificar si el nombre que está asociado con el otro punto de extremo (1020) está enumerado en la base de datos (1015, 1075a, 1075b) como un contacto de confianza; en donde la información identifica los contactos de confianza y sus derechos de acceso dentro del grupo seguro;
verificar, por el gestor de bases de datos (1045) del punto de extremo (1010), los derechos de acceso en la base de datos (1015, 1075a, 1075b) que está asociada con el grupo seguro que está asociado con el otro punto de extremo (1020), si el nombre del punto de extremo está enumerado en la base de datos (1015, 1075a, 1075b) como un contacto de confianza;
determinar, por el gestor de bases de datos (1045), si se concede el permiso para llevar a cabo la operación deseada a partir de los derechos de acceso asociados; y
llevar a cabo la operación deseada si se concede un permiso para llevar a cabo la operación deseada,
caracterizado por que
la base de datos (1015, 1075a, 1075b) y el gestor de bases de datos (1045) están incluidos en el punto de extremo (1010), en donde la base de datos (1015, 1075a, 1075b) incluye:

a) una información de contacto de confianza que incluye un nombre, una ID de parte que llama, una ID de elemento del mismo nivel, una credencial y unos derechos de acceso de cada uno de los contactos de confianza, comprendiendo la credencial un certificado criptográfico del contacto de confianza respectivo, y
b) una información de grupo seguro que incluye una ID de grupo, un certificado de grupo y unos derechos de acceso de grupo de cada uno de los grupos seguros,

en donde los certificados de los contactos de confianza se sustituyen con unas claves públicas correspondientes del grupo seguro tras la verificación de los certificados de los contactos de confianza.

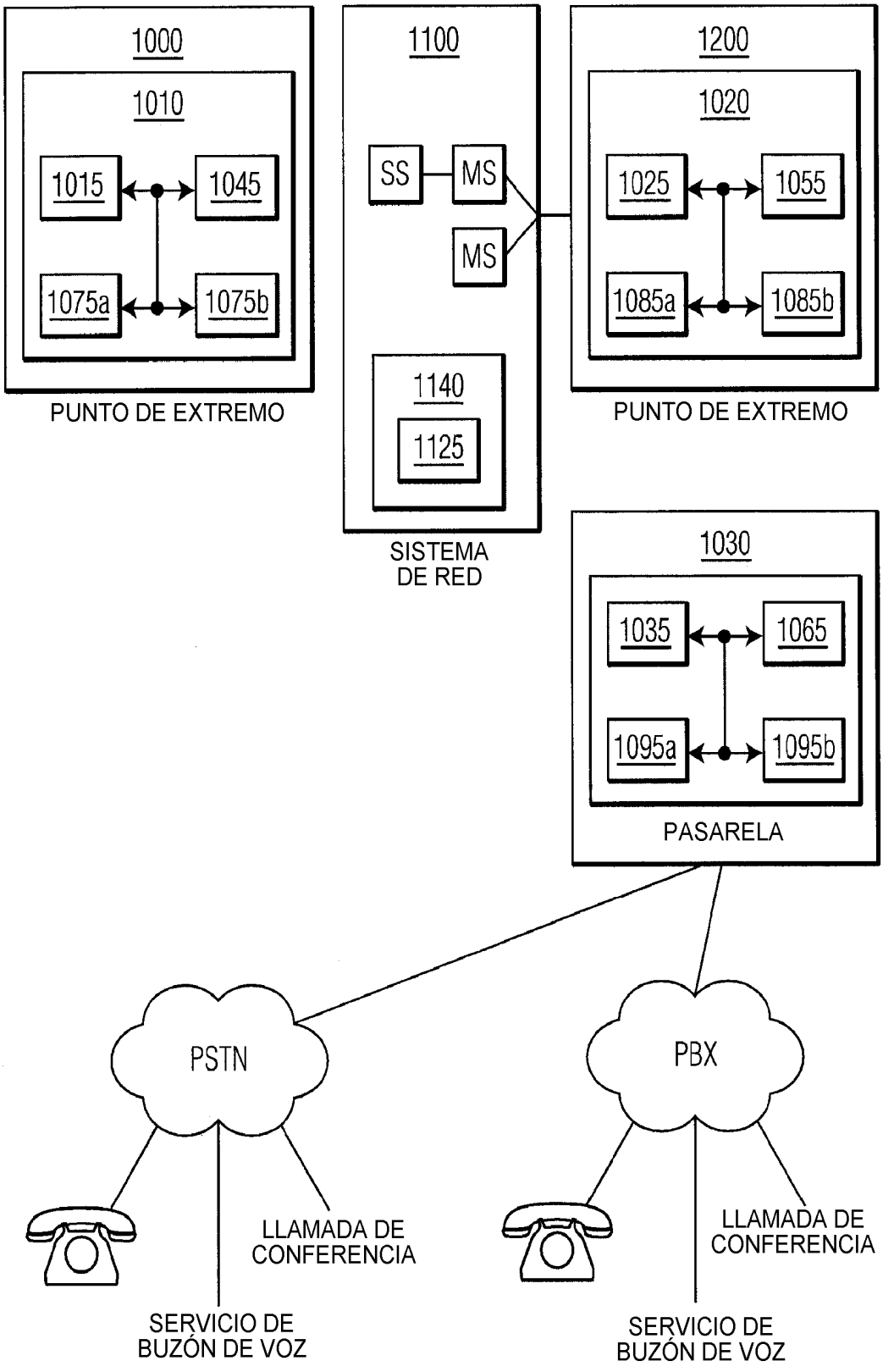
1000
1010
1015
1045
1075a
1075b
PUNTO DE EXTREMO
1100
SS
MS
MS
1140
1125
SISTEMA DE RED
1200
1020
1025
1055
1085a
1085b
PUNTO DE EXTREMO
1030
1035
1065
1095a
1095b
PASARELA
PSTN
PBX
LLAMADA DE CONFERENCIA
SERVICIO DE BUZÓN DE VOZ
LLAMADA DE CONFERENCIA
SERVICIO DE BUZÓN DE VOZ

FIG. 1

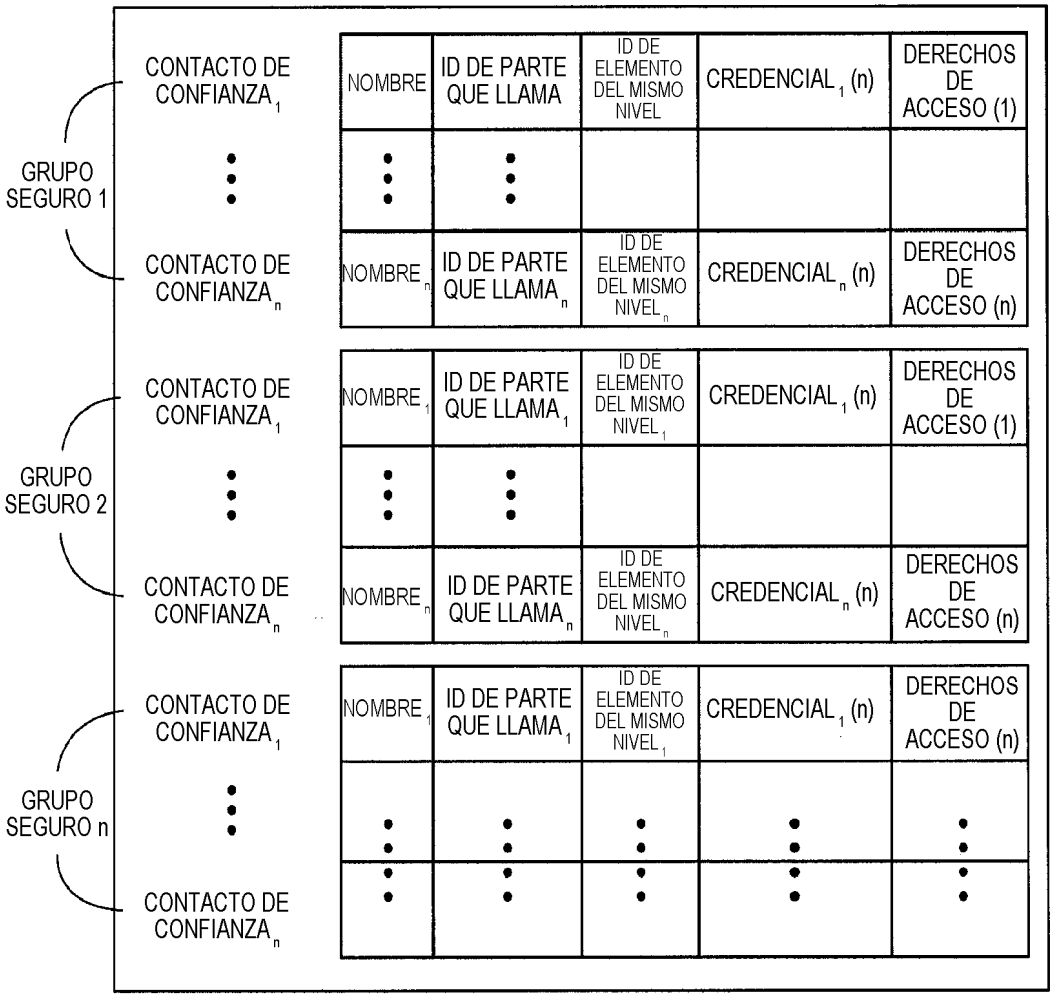

FIG. 2A

ID DE GRUPO SEGURO (1)	CERTIFICADO DE GRUPO (1)	DERECHOS DE ACCESO (1)
⋮	⋮	⋮
⋮	⋮	⋮
ID DE GRUPO SEGURO (n)	CERTIFICADO DE GRUPO (n)	DERECHOS DE ACCESO (n)

FIG. 2B

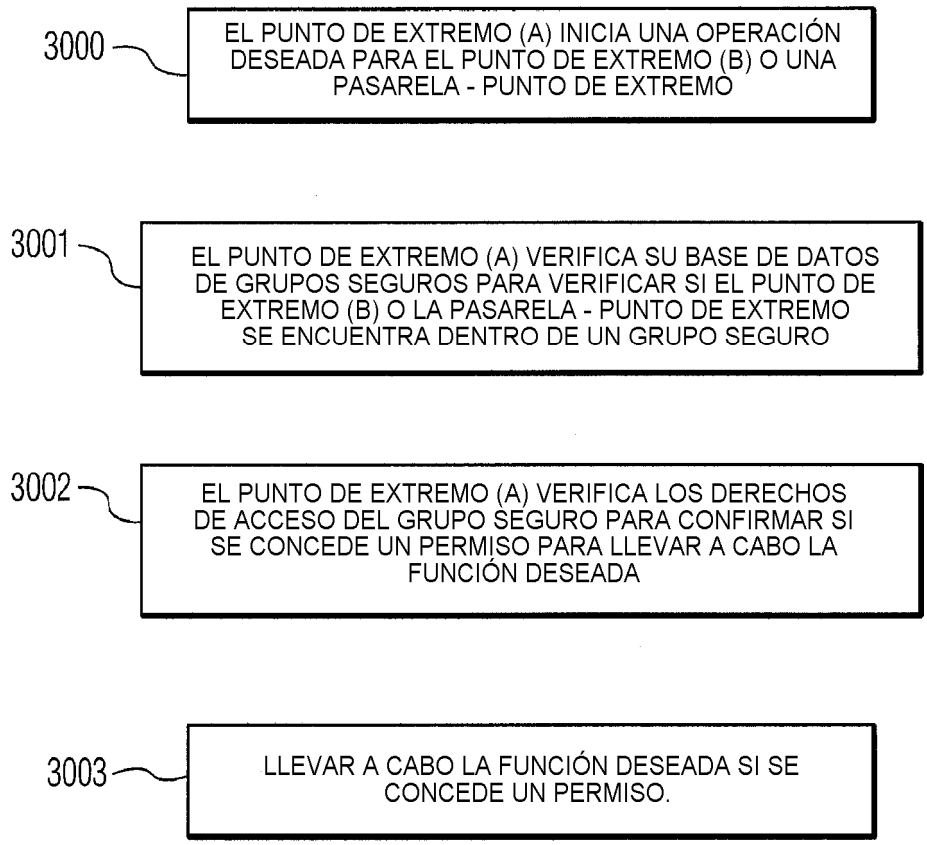
3000
EL PUNTO DE EXTREMO (A) INICIA UNA OPERACIÓN DESEADA PARA EL PUNTO DE EXTREMO (B) O UNA PASARELA - PUNTO DE EXTREMO
3001
EL PUNTO DE EXTREMO (A) VERIFICA SU BASE DE DATOS DE GRUPOS SEGUROS PARA VERIFICAR SI EL PUNTO DE EXTREMO (B) O LA PASARELA - PUNTO DE EXTREMO SE ENCUENTRA DENTRO DE UN GRUPO SEGURO
3002
EL PUNTO DE EXTREMO (A) VERIFICA LOS DERECHOS DE ACCESO DEL GRUPO SEGURO PARA CONFIRMAR SI SE CONCEDE UN PERMISO PARA LLEVAR A CABO LA FUNCIÓN DESEADA
3003
LLEVAR A CABO LA FUNCIÓN DESEADA SI SE CONCEDE UN PERMISO.

FIG. 3