(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 578 003**

(51) Int. CI.:

H04M 3/42 (2006.01)
H04M 1/57 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **28.03.2014 E 14162376 (9)**

(97) Fecha y número de publicación de la concesión europea: **23.03.2016 EP 2785029**

(54) Título: **Procedimiento y dispositivo de transmisión de una llamada con número oculto, procedimiento y dispositivo de recepción de una llamada con número oculto, señal de transmisión de una llamada con número oculto y programa de ordenador correspondiente**

(30) Prioridad:

29.03.2013 FR 1352893

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
20.07.2016

(73) Titular/es:

ORANGE (100.0%)
78, rue Olivier de Serres
75015 Paris, FR

(72) Inventor/es:

TAMAGNAN, PHILIPPE

(74) Agente/Representante:

ISERN JARA, Jorge

DESCRIPCIÓN

Procedimiento y dispositivo de transmisión de una llamada con número oculto, procedimiento y dispositivo de recepción de una llamada con número oculto, señal de transmisión de una llamada con número oculto y programa de ordenador correspondiente

1. Campo de la invención

El campo de la invención es el de las comunicaciones entre diferentes terminales de comunicación.

De manera más precisa, la invención se refiere a la gestión de las llamas “ocultas”, en las que la identidad del emisor de una llamada no se comunica al destinatario de la llamada.

De manera aun más precisa, la invención propone una solución que permite que el receptor de una llamada “identifique” al emisor de la llamada que emite una llamada con número oculto, con una cierta probabilidad.

La invención encuentra aplicaciones en cualquier sistema de comunicación que implementa terminales de comunicación (de tipo teléfono, ordenador, tableta táctil, etc.), y en particular en el campo de la telefonía y de las telecomunicaciones.

2. Técnica anterior

Por un lado, un primer usuario A puede desear disponer de un servicio de tipo “no identificación del solicitante en fase de llamada” (en inglés “CLIR” por “Calling Line Identification Restriction”) con el fin de no dar a conocer su identidad. Un caso de uso es evitar comunicar su identidad telefónica (por ejemplo, su número de teléfono) a empresas comerciales. Este servicio se puede activar a petición, pero la mayoría de las veces se configura de manera permanente en la red telefónica. Este último caso (“modo permanente”) por lo general no puede modificarlo el usuario. Por otra parte, los controles de activación o de modificación de servicio no los conocen bien los usuarios, los cuales establecen en general las llamadas basándose en la configuración por defecto del terminal y de la red.

Por otro lado, un segundo usuario B puede elegir, en particular para proteger su vida privada, no aceptar nunca llamadas procedentes de identidades ocultas utilizando el anterior servicio.

Ahora bien, puede suceder que los usuarios A y B se conozcan, pero que no lleguen a establecer una comunicación telefónica, pudiendo el usuario A entrar en comunicación con el usuario B solo al desactivar el servicio de tipo CLIR temporalmente, o al llamar con otra línea.

Otra solución la proporciona el documento WO 2011/154221 en la que el número del emisor de la llamada está encriptado y se envía al usuario llamado en una primera llamada. El receptor de la llamada registra el número encriptado del emisor de la llamada en su directorio. En la siguiente llamada, se encuentra el número encriptado del emisor de la llamada y se muestra el número del emisor de la llamada al receptor de la llamada.

Una solución habitual a este problema, proporcionada por los operadores telefónicos, es para el usuario B suscribirse a un servicio de terminación que activa un diálogo vocal previo con el emisor de la llamada A, invitando a este último a identificarse verbalmente. La respuesta vocal del emisor de la llamada A se registra entonces, y a continuación se presenta al receptor de la llamada B, el cual elige o no aceptar la llamada.

Un inconveniente de esta solución es que se basa en una suscripción voluntaria a este servicio, lo que puede presentar un obstáculo para los usuarios. En particular, la suscripción a este servicio es de pago.

Además, dicha solución puede ser complicada de utilizar, en particular para aquellas personas que no están en pleno uso de sus facultades (por ejemplo las personas de edad avanzada), que pueden no entender el mensaje que les invita a identificarse, en particular cuando estas tienen serias dificultades.

Existe, por lo tanto, la necesidad de una nueva solución que permita a un receptor de llamada identificar al menos con una cierta probabilidad, a un emisor de llamada que emite una llamada con número oculto, pero sin que se violen las disposiciones legales relativas al secreto de llamada.

3. Descripción de la invención

La invención propone una nueva solución que no presenta el conjunto de los inconvenientes de la técnica anterior, en forma de un procedimiento de transmisión de una llamada de un emisor hacia un destinatario, en el que la identidad del emisor está oculta para el destinatario, denominada llamada con número oculto.

De acuerdo con la invención, dicho procedimiento implementa las siguientes etapas:

- generación de un testigo no invertible de identificación del emisor, a partir de un identificador del emisor; y
- transmisión al destinatario de la llamada con número oculto y del testigo de identificación.

De este modo la invención propone una nueva solución para la transmisión de una llamada con número oculto, que se basa en la transmisión de un testigo de identificación no invertible, de forma conjunta con la llamada con número oculto. En el lado del destinatario, dicho testigo de identificación se podrá utilizar para determinar, con una cierta probabilidad, si el destinatario conoce al emisor, basándose en una lista de contactos contenida en un directorio del terminal destinatario.

Dicho de otro modo, dicha solución permite que un emisor llame a un destinatario manteniendo su enmascaramiento de identidad, siendo al mismo tiempo reconocido por el destinatario. Dicho identificador del emisor podrá, por ejemplo, ser el número de teléfono (en abierto) del emisor, o una parte de este número suprimiendo por ejemplo algunas cifras en el centro o en un extremo del número de teléfono completo; la utilización de una parte del número de teléfono del emisor permite, si se desea, garantizar el respeto del anonimato del emisor. Dicho identificador del emisor podrá, en otro ejemplo, ser una cadena de caracteres, que corresponden por ejemplo al nombre del emisor.

Esta solución presenta, en particular, la ventaja de no necesitar ningún diálogo previo entre el emisor y el destinatario. Además, no necesita la suscripción a un servicio, o el registro de un identificador del emisor en una lista blanca o una lista negra. Por último, permite que el emisor conserve su anonimato cuando llama por teléfono a empresas comerciales por ejemplo, que no pueden *a priori* localizar su identidad, y “levantar su anonimato” cuando llama por teléfono a los amigos, que pueden *a priori* identificarlo.

En particular, dicho testigo de identificación se genera utilizando una función denominada “unidireccional”, que toma en la entrada el identificador del emisor. Por ello, dicho testigo de identificación es fácil de calcular en el lado del emisor, pero no es posible (o es difícil) encontrar exactamente la identidad del emisor en el lado del destinatario, aplicando una función inversa. Por lo tanto no es invertible.

Además de no ser invertible, el algoritmo elegido para calcular el testigo de identificación debe tener, de preferencia, una probabilidad absoluta de colisión entre dos identidades distintas lo suficientemente alta para impedir violar el principio del anonimato del emisor. De este modo, la identidad del emisor no se da a conocer, sino que simplemente se presume.

De acuerdo con una forma particular de realización, la etapa de generación de un testigo de identificación tiene también en cuenta una simiente.

Dicha simiente (en inglés “seed”) permite en particular añadir diversidad al testigo de identificación. Por ello, dicho testigo de identificación es difícil de repetir. Dicho de otro modo, la utilización de una simiente permite reducir el riesgo de una reutilización fraudulenta del testigo de identificación en el caso de que los testigos de identificación se almacenen en una memoria del terminal del destinatario, aunque un testigo de identificación sea interceptado por un intruso.

De acuerdo con una característica particular, el procedimiento de transmisión comprende una etapa previa de construcción de la simiente, a partir de una información temporal y/o de un número aleatorio. Por ejemplo, la información temporal es de tipo fecha y hora.

De esta forma se evita cualquier previsibilidad de la simiente, y por lo tanto del testigo de identificación, lo que permite garantizar la seguridad de la transmisión.

De acuerdo con otra característica particular, se genera una nueva simiente con cada nueva llamada que hay que transmitir.

Se garantiza de esta forma que el testigo de identificación, generado a partir de un identificador del emisor y de la simiente, es único.

En particular, el procedimiento de transmisión de acuerdo con la invención comprende una etapa de transmisión de la simiente. Por lo tanto, el destinatario recibe directamente la simiente y no tiene necesidad de generarla por su parte.

De acuerdo con una variante, la simiente se genera también en el destinatario.

De acuerdo con una forma de realización de la invención, la etapa de generación implementa una función *hash*, que emite un condensado representativo de un identificador del emisor.

Dicha función *hash* se puede aplicar por ejemplo al número de teléfono completo del emisor, o a una parte de este número de teléfono (por ejemplo suprimiendo algunas cifras, en el centro o en un extremo del número de teléfono completo).

Por ejemplo, dicha función *hash* es una función *hash* criptográfica segura de tipo SHA1, SHA2, SHA3, SHA2556 (en inglés “Secure Hash Algorithm”). Esta se puede aplicar directamente al identificador del emisor, o a una concatenación de la simiente y del identificador del emisor.

De acuerdo con otro ejemplo, dicha función *hash* es de tipo HMAC (en inglés “Keyed-Hash Message Authentication Code”, en español “código de autentificación de una huella criptográfica de mensaje con clave”). En este caso, la simiente puede desempeñar la función de clave, y el identificador del emisor desempeñar la función del mensaje que hay que codificar.

De acuerdo con una característica particular, el testigo de identificación se obtiene suprimiendo al menos un elemento del condensado. Dicha supresión se puede llevar a cabo al inicio o al final del condensado, e implementarse de forma fija o aleatoria.

De nuevo, esta operación permite garantizar el anonimato del emisor.

De acuerdo con otro aspecto, la invención se refiere a un dispositivo de transmisión de una llamada de un emisor hacia un destinatario, en el que la identidad del emisor está oculta para el destinatario, denominada llamada con número oculto.

De acuerdo con la invención, dicho dispositivo comprende:

- un módulo de generación de un testigo no invertible de identificación del emisor, a partir de un identificador del emisor; y
- al menos un módulo de transmisión al destinatario de la llamada con número oculto y del testigo de identificación.

Dicho dispositivo de transmisión está en particular adaptado para implementar el procedimiento de transmisión descrito con anterioridad.

Dicho dispositivo se puede integrar en un terminal de tipo teléfono (móvil o fijo), ordenador (portátil o fijo), tableta, etc. También puede integrarse en un equipo de terceros de la red de transmisión.

Por supuesto, este dispositivo podrá constar de las diferentes características relativas al procedimiento de transmisión de acuerdo con la invención, que se pueden combinar o considerar de forma aislada. De este modo, las características y ventajas de este dispositivo son las mismas que las del procedimiento de transmisión. Por consiguiente, no se detallan de manera más amplia.

Por otra parte, la invención se refiere a una señal de transmisión de una llamada de un emisor hacia un destinatario, en la que la identidad del emisor está oculta para el destinatario, denominada llamada con número oculto.

De acuerdo con la invención, dicha señal comprende un campo específico que lleva al menos un testigo no invertible de identificación de dicho emisor, generado a partir de un identificador de dicho emisor, y que también lleva la llamada con número oculto.

Dicha señal se puede generar y transmitir utilizando el procedimiento de transmisión descrito con anterioridad. En particular, dicha señal también puede presentar otro campo que lleva la simiente, si esta se transmite al destinatario.

Por supuesto, esta señal podrá constar de las diferentes características relativas al procedimiento de transmisión de acuerdo con la invención.

En particular, si el testigo de identificación no lo genera el terminal del emisor, la señal lleva al menos un indicador implícito o explícito que permite el cálculo de un testigo de identificación mediante un equipo de terceros de la red de transmisión.

Por otra parte, la invención se refiere a un procedimiento de recepción de una llamada emitida por un emisor hacia un destinatario, en el que la identidad del emisor está oculta para el destinatario, denominada llamada con número oculto.

De acuerdo con la invención, dicho procedimiento implementa las siguientes etapas:

- recepción de una llamada con número oculto y de un testigo no invertible de identificación del emisor, generado a partir de un identificador del emisor;
- generación de al menos un testigo de control, a partir de al menos un identificador presente en un directorio del destinatario;
- comparación del testigo de identificación y del o de los testigos de control; y

- en caso de detección de al menos una porción idéntica entre el testigo de identificación y uno de los testigos de control, restitución al destinatario bien de una información que representa el identificador del emisor, bien de una mención que indica la presencia del identificador del emisor en dicho directorio del destinatario.

Dicho procedimiento está en particular adaptado para recibir una llamada emitida de acuerdo con el procedimiento de transmisión descrito con anterioridad.

De este modo, la invención propone comparar un testigo de identificación del emisor, con al menos un testigo de control construido a partir de un identificador presente en el directorio del destinatario, con el fin de determinar, con una cierta probabilidad, si un identificador del emisor está presente en este directorio. Dicho identificador del emisor podrá, por ejemplo, ser el número de teléfono (en abierto) del emisor, o una parte de este número. De acuerdo con otro ejemplo, el identificador del emisor podrá ser una cadena de caracteres.

Si este es el caso, se puede informar al destinatario de que “el emisor de la llamada con número oculto está presente en el directorio”, o que el emisor es “mamá” por ejemplo.

Hay que señalar que se puede calcular un testigo de control a partir de la integridad de un identificador del directorio (por ejemplo número de teléfono). En efecto, no se busca en este caso conservar el anonimato del identificador, puesto que el testigo de control no está destinado a transmitirse en la red.

Además, se realiza una protección de la identidad del emisor por el hecho de que su número está presente en el directorio, por lo tanto esta ha sido objeto en algún momento de una transmisión voluntaria de datos personales del emisor al destinatario.

En particular, dicho procedimiento puede implementar una etapa de recepción de una simiente transmitida con el testigo de identificación. En este caso, la generación del o de los testigos de control tiene también en cuenta la simiente.

De acuerdo con otra variante, la simiente no se transmite con el testigo de identificación, sino que se genera también en el lado del destinatario. Esto es en particular posible cuando la simiente está compuesta por una información variable pero universalmente accesible (por ejemplo la hora UTC (del inglés “Universal Time Coordinate“, hora universal coordinada) limitada al minuto).

De acuerdo con otra variante más, la simiente la genera el destinatario y la transmite hacia aguas arriba. Se calcula entonces el testigo aguas arriba y se transmite al receptor de la llamada.

De acuerdo con otra característica particular, las etapas de generación y de comparación tienen en cuenta una frecuencia de llamadas recibidas por parte de al menos un emisor del cual está presente un identificador en el directorio del destinatario.

De esta forma, se puede “jerarquizar” el cálculo del o de los testigos de control, calculando en primer lugar el testigo de control que corresponde al identificador que llama más a menudo, y a continuación comparando este testigo de control con el testigo de identificación, y procediendo así sucesivamente mientras ningún testigo se considere similar al testigo de identificación.

En particular, la etapa de generación de al menos un testigo de control implementa una función *hash*, idéntica a una función *hash* utilizada para la generación del testigo de identificación.

De acuerdo con otro aspecto, la invención se refiere a un dispositivo de recepción de una llamada emitida por un emisor hacia un destinatario, en el que la identidad del emisor está oculta para el destinatario, denominada llamada con número oculto.

De acuerdo con la invención, dicho dispositivo comprende:

- al menos un módulo de recepción de la llamada con número oculto y de un testigo no invertible de identificación del emisor, generado a partir de un identificador del emisor;
- un módulo de generación de al menos un testigo de control, a partir de al menos un identificador presente en un directorio del destinatario;
- un módulo de comparación del testigo de identificación y del o de los testigos de control; y
- un módulo de restitución al destinatario bien de una información que representa el identificador del emisor, bien de una mención que indica la presencia del identificador del emisor en dicho directorio del destinatario, activado en caso de detección de al menos una porción idéntica entre el testigo de identificación y uno de los testigos de control.

Dicho dispositivo de recepción está en particular adaptado para implementar el procedimiento de recepción descrito con anterioridad.

Dicho dispositivo puede integrarse en un terminal de tipo teléfono (móvil o fijo), ordenador (portátil o fijo), tableta, etc.

En particular, está adaptado para recibir una llamada con número oculto y un testigo de identificación procedentes del dispositivo de transmisión descrito con anterioridad.

Por supuesto, este dispositivo podrá constar de las diferentes características relativas al dispositivo de recepción de acuerdo con la invención, que se pueden combinar o considerar de forma aislada. De este modo, las características y ventajas de este dispositivo son las mismas que las del procedimiento de recepción. Por consiguiente, no se detallan de manera más amplia.

En otra forma de realización, la invención se refiere a uno o varios programas de ordenador que constan de unas instrucciones para la implementación de un procedimiento de transmisión y/o de las instrucciones para la implementación de un procedimiento de recepción tal como se han descrito con anterioridad, cuando este o estos programas los ejecuta un procesador.

En otra forma más de realización, la invención se refiere a un soporte de información, fijo, o parcialmente o totalmente extraíble, legible mediante un ordenador, y que consta de las instrucciones de un programa de ordenador para la ejecución de las etapas del procedimiento de transmisión o del procedimiento de recepción tal como se han descrito con anterioridad.

4. Lista de las figuras

Se mostrarán de manera más clara otras características y ventajas de la invención con la lectura de la siguiente descripción de una forma particular de realización, dada a título de simple ejemplo ilustrativo y no limitativo, y de los dibujos adjuntos, en los que:

- la figura 1 ilustra dos terminales que desean entrar en comunicación;
- la figura 2 presenta las principales etapas de un procedimiento de transmisión de acuerdo con una forma particular de realización de la invención;
- la figura 3 presenta las principales etapas de un procedimiento de recepción de acuerdo con una forma particular de realización de la invención;
- las figuras 4 y 5 presentan respectivamente la estructura simplificada de un dispositivo de transmisión que implementa una técnica de transmisión y la estructura simplificada de un dispositivo de recepción que implementa una técnica de recepción de acuerdo con una forma particular de realización de la invención.

5. Descripción de una forma de realización de la invención

5.1 Principio general

Nos situamos en el contexto de la generación de una llamada con número oculto por un emisor, es decir una llamada en la que la identidad del emisor está oculta para el destinatario.

El principio general de la invención se basa en la transmisión, a un destinatario, de un testigo de identificación del emisor, que permite que el destinatario identifique al emisor con una cierta probabilidad si el destinatario lo conoce (por ejemplo si el emisor está presente en la agenda de direcciones / directorio del destinatario), manteniendo al mismo tiempo el enmascaramiento de identidad del emisor.

Por ejemplo, como se ilustra en la figura 1, un emisor de tipo teléfono 11 emite una llamada, ocultando su identidad, destinada a un destinatario de tipo teléfono 12.

El destinatario 12, que recibe una llamada con número oculto, es reacio a descolgar.

De acuerdo con la invención, además de la llamada con número oculto, el emisor 11 transmite al destinatario 12 un testigo de identificación. Al recibir este testigo de identificación, el destinatario 12 puede determinar si conoce al emisor 11, y aceptar o rechazar la comunicación.

Se considera, de acuerdo con la invención, que el emisor y el destinatario son unos equipos con una o varias redes, adaptadas para comunicarse entre sí. Se trata, por ejemplo, de teléfonos, tabletas táctiles, ordenadores, etc. Además, se entiende por “llamada” cualquier tipo de comunicación entre estos equipos (comunicaciones de voz, de texto, multimedia (por ejemplo Skype - marca registrada)…). En particular, estas comunicaciones pueden utilizar las redes IMS (en inglés “IP Multimedia System”), que se basan en la utilización del protocolo IP. En particular, las redes IMS recurren al protocolo de señalización SIP (“Session Initiation Protocol”), estandarizado por la IETF (“Internet Engineering Task Force”, órgano de normalización técnica de Internet).

De este modo, la invención propone una nueva solución para la transmisión de una llamada con número oculto a un destinatario, que se puede proponer en forma de un nuevo servicio denominado de “Control de Identidad de Línea

Llamante" (en inglés "Calling Line Identity Check"). Dicha solución no necesita un diálogo de voz, ni suscripción, ni registro de lista blanca, con el fin de permitir que un emisor llame a un destinatario manteniendo el enmascaramiento de identidad, pero siendo sin embargo reconocido por este.

El principio se basa en la transmisión al destinatario de un testigo no invertible que representa al emisor con una cierta probabilidad, y en la comparación de este testigo de identificación con unos testigos de control obtenidos para todos los contactos presentes en el directorio del destinatario, o eventualmente solo para los contactos presentes en el directorio del destinatario abonados a este servicio.

De este modo, la solución propuesta permite que dos personas se comuniquen cumpliendo con las exigencias de seguridad de cada una.

Además, se puede transponer a todos los tipos de redes que disponen de facilidad de presentación o de no presentación de identidad. Del mismo modo, la invención depende del soporte de los fabricantes de terminales pero no provoca ninguna modificación de los terminales existentes, que pueden funcionar de manera clásica, sin tener en cuenta el testigo de identificación de acuerdo con la invención.

Por otra parte, hay que señalar que la invención se puede desplegar como propietaria en una red de operador. En particular, la invención no provoca restricciones en los demás servicios del operador.

Se presentan, a continuación, en relación con la figura 2, las principales etapas implementadas mediante el procedimiento de transmisión de una llamada del emisor 11 hacia el destinatario 12 de acuerdo con la invención.

A lo largo de una primera etapa 21, se genera un testigo no invertible de identificación del emisor, a partir de un identificador del emisor, con la referencia NA. Para ello, se utiliza una función unidireccional, con el fin de que el destinatario no pueda encontrar directamente la identidad del emisor aplicando una función inversa al testigo de identificación. Hay que señalar que la generación del testigo de identificación se puede llevar a cabo directamente al nivel del terminal emisor 11, o bien al nivel de un equipo de terceros de la red.

A lo largo de una segunda etapa 22, se transmite al destinatario la llamada con número oculto y el testigo de identificación. Este testigo de identificación lo puede utilizar el destinatario 12 para determinar si conoce al emisor 11.

De manera más precisa, la figura 3 ilustra las principales etapas implementadas mediante el procedimiento de recepción de una llamada del emisor 11 hacia el destinatario 12 de acuerdo con la invención.

A lo largo de una primera etapa 31, el destinatario 12 recibe el testigo de identificación y la llamada con número oculto.

A lo largo de una segunda etapa 32, se genera al menos un testigo de control a partir de al menos un identificador presente en un directorio del destinatario 12, con la referencia Ni.

A lo largo de una tercera etapa 33, se compara el testigo de identificación y el o los testigos de control.

En caso de comparación positiva, p. ej. si se detecta al menos una porción idéntica entre el testigo de identificación y uno de los testigos de control, se restituye al destinatario 12 bien una información que representa al identificador del emisor 11 (por ejemplo número de teléfono o nombre de contacto), bien una mención que indica la presencia del identificador del emisor 11 en el directorio del destinatario, a lo largo de una cuarta etapa 34.

5.2 Descripción de una forma particular de realización

A continuación se describe un ejemplo de realización, en el que se construye el testigo digital no invertible de identificación KA (por el emisor o por una entidad de la red), a partir de un identificador NA de un emisor 11 y de una simiente S. Se recuerda que la utilización de una simiente S permite limitar las posibilidades de reutilización del testigo de identificación, en particular mediante el almacenamiento en el destinatario de una lista de los últimos valores recibidos.

5.2.1 Generación del testigo de identificación

Para garantizar las propiedades de no invertibilidad y de colisión, el testigo de identificación KA(NA, S) debe construirse con ciertas precauciones, por ejemplo utilizando solo una parte de un número de teléfono del emisor, o incluso truncando el resultado de la función unidireccional.

De acuerdo con este ejemplo particular, el testigo de identificación del emisor KA se construye, por una parte, aplicando una función *hash* al par (NA, S), por otra parte truncando el resultado obtenido:

KA = truncamiento (h), siendo h = H(NA, S).

Se recuerda que se puede, por ejemplo, para obtener el identificador NA, extraer de forma previa una subcadena de una cadena de caracteres asociados al emisor (por ejemplo su número de teléfono), retirando P últimos caracteres (por ejemplo P = 2), antes de inyectarla en la función H. Esto garantiza el respeto del anonimato, pero puede provocar colisiones no deseadas, por ejemplo en el caso de un tramo de números consecutivos asignados a una empresa o a una zona de residencia o un número corto de red privada virtual. Un método más refinado es retirar o sobrescribir caracteres en el centro de dicha cadena de caracteres (por ejemplo la cifra de las decenas de millar).

La función H se puede construir a partir de una función *hash*. Por ejemplo:

a. H(NA, S) = HASH(S | NA), donde HASH designa por ejemplo el algoritmo SHA1, SHA2, SHA3 o SHA256; o
b. H(NA, S) = HMAC(S | NA), con S desempeñando la función de las claves y NA desempeñando la función del mensaje, donde HMAC designa el código de identificación de una huella criptográfica de mensaje con clave. Por ejemplo: H(NA, S) = HAHS[(S ⊕opad) | HASH((S ⊕ipad) ⊕NA)], donde el símbolo "|" designa la concatenación, el símbolo ⊕ designa la adición bit a bit, y donde los símbolos "opad" e "ipad" son unas contantes predeterminadas.

La función truncamiento (h) extrae una subcadena de su argumento h. Se pueden suprimir unos caracteres al inicio y/o al final de la cadena, de manera fija o eventualmente aleatoria (por ejemplo retirando P caracteres al inicio de la cadena, Q caracteres al final de la cadena), según la llamada. El hecho de proceder a este truncamiento garantiza el respeto del anonimato, puesto que una colisión es en teoría posible. Al final solo queda un número R reducido de caracteres consecutivos, por ejemplo R = 5.

Con el fin de evitar cualquier previsibilidad, la simiente S se puede construir a partir del tiempo *t* (por ejemplo fecha y hora actual), y de un número aleatorio *r* eventualmente extraído de un registro aleatorio): *S* = *S*(*t*,*r*). Esta se puede expresar en forma de cadena explícita imprimible (por ejemplo 1234 12 de octubre de 2013 16:55:28) o en un formato más compacto hexadecimal (123412102013165528 que se convierte en 1B672A7257A9FD8).

5.2.2 Ejemplo completo de realización de servicio

Nos situamos aquí en un contexto de red (o de un conjunto de redes) de telefonía IMS basada en el protocolo SIP.

De acuerdo con este ejemplo, se añade a la señalización un encabezado propietario con la referencia "x-qualif-id", para el mensaje INVITE. Su valor es "no", "sí", o bien la sucesión de las cadenas KA y S.

Se considera que el valor del testigo de identificación KA se deriva del algoritmo SHA1 y que la simiente S es aleatoria. Es, por ejemplo, una cadena de algunos caracteres.

La autorización de control de identidad de línea emisora de llamada puede llevarse a cabo llamada por llamada, si el emisor transmite un encabezado x-qualif-id que vale "sí" o "no". La autorización también se puede configurar implícitamente en la red de manera global o incluso en el perfil del emisor. El valor eventualmente recibido en el mensaje INVITE sobrecarga el valor configurado para contribuir a la regla de decisión que se da a continuación.

Autorización configurada en la red (global o, si la red en la que se origina la comunicación es distinta de la red donde acaba, eventualmente específica para el perfil del emisor)	Autorización recibida de x-qualif-id	Decisión final
"Sí"	"sí"	x-qualif-id= <testigo KA> <simiente S>
"Sí"	"no"	Sin transmisión de x-qualif-id
"Sí"	ninguna	x-qualif-id id= <testigo KA> <simiente S>
"No"	"sí"	x-qualif-id id = <testigo KA> <simiente S>
"No"	"no"	Sin transmisión de x-qualif-id
"No"	ninguna	Sin transmisión de x-qualif-id (o nada, a elección del operador)

De ese modo, el servicio propuesto se puede implementar bien a petición mediante una acción voluntaria del emisor, bien de manera permanente configurada previamente en la red a petición expresa del destinatario mediante suscripción. De este modo, el emisor guarda por defecto la posibilidad de ocultar totalmente su identidad si este lo desea.

En particular, cuando el servicio se implementa a petición, el emisor debe enviar en la señalización un indicador adecuado que permite el cálculo del testigo de identificación por la red y su transmisión a un destinatario (tradicionalmente reservado a terminales antiguos).

En ambos casos (permanente o a petición), el indicador y el par (S, KA) se transmiten en la señalización, y puede hacerse en particular en la interconexión entre dos redes. Si no se proporciona aguas arriba, el valor del testigo de identificación se puede calcular por la o las redes, si los acuerdos entre los operadores lo permiten, por ejemplo lo más cerca posible del destinatario.

El servicio es, por construcción, compatible con los demás servicios de la red. En el caso de un procedimiento de llamada que implementaría un cambio de la identidad del emisor de llamada en tránsito, el servicio que opera esta modificación puede o no suprimir la señalización adicional de acuerdo con la invención.

En particular, hay que señalar que debe poderse inhibir en un terminal la implementación del servicio, tanto en la salida como en la llegada.

La construcción del testigo de identificación KA se lleva a cabo aquí más bien en la red en la que se origina la comunicación. En efecto, de acuerdo con la política de seguridad del operador, el secreto de llamada se gestiona en las redes IMS ocultando (mediante la sustitución de una cadena fija) o no la identidad privada desde la red en la que se origina la comunicación. Si este es el caso, esto no permite garantizar el servicio en la red en la que se acaba la comunicación, puesto que esta última red ya no dispone de la identidad del emisor de la llamada.

Se considera, por ejemplo, que el emisor es Alicia, con número E164 +33296106155, y que el destinatario es Bernardo, con número E164 +33950131054.

El terminal de Alicia solicita explícitamente, por ejemplo, el servicio añadiendo el encabezado “x-qualif-id= sí” al mismo tiempo que el servicio de enmascaramiento de identidad (“header SIP Privacy”), en un mensaje INVITE. Hay que señalar que el resultado sería similar si el terminal de Alicia no hubiera indicado nada (p. ej. ningún encabezado x-qualif-id), pero la red permitiera por defecto el servicio.

De acuerdo con este ejemplo, la generación del testigo de identificación del emisor se lleva a cabo al nivel de una entidad de la red en la que se origina la comunicación.

Para ello, la entidad de la red recupera el número de emisor de llamada expresado, aquí con el formato E.164. Este número se extrae, por ejemplo, de la identidad privada, disponible en el campo “From” (“de”): From: <sip:+330296106155@172.20.74.194>.

De este modo, se obtiene un identificador del emisor NA= “+330296106155”.

Hay que señalar que este identificador también se puede obtener mediante otros medios (relación hecha por la red entre identidad pública certificada con la identidad privada).

En este ejemplo simplificado, se elige no truncar el número de identificador obtenido de este modo.

La entidad de la red genera también una simiente S. En este ejemplo simplificado, S se construye a partir del par (fecha, hora). Por ejemplo, S= “12 de octubre de 2013 16:55:28”.

La entidad de la red aplica entonces una función *hash* al par (NA, S), y a continuación una función de truncamiento al condensado obtenido. De acuerdo con este ejemplo, para garantizar las colisiones, se concatena S | NA, se aplica SHA1 y se retiran 17 caracteres al inicio y otros 16 caracteres al final de la cadena de caracteres obtenida. Se trata aquí de una elección arbitraria y aleatoria, que depende de la llamada.

De este modo, si se considera el siguiente texto de entrada, formado por la concatenación de la simiente S y del identificador NA:

Texto de entrada: 12 de octubre de 2013 16:55:28+33296106155,

se obtiene en la salida de la función *hash*:

Resultado SHA1: 68e2d03501daba37a25720e9cb77e84af05a0a96

y a continuación en la señal de la función de truncamiento:

Resultado SHA1 truncado: KA= 25720e9 (truncado de 17+16= 33 caracteres).

El resultado obtenido corresponde al testigo de identificación del emisor. Este se puede inyectar en el encabezado “x-qualif-id”, con la simiente, para su transmisión a Bernardo: x-qualif-id: “25720e9” “12 de octubre de 2013 16:55:28”.

De manera más precisa, el mensaje SIP se retransmite hacia Bernardo (destinatario), volviendo anónima la identidad privada:

From: “Anonymous” <sip:anonymous@anonymous.invalid>
x-qualif-id: “25720e9” “12 de octubre de 2013 16:55:28”

El terminal de Bernardo recibe la llamada con número oculto, así como el testigo de identificación y la simiente presentes en el encabezado x-qualif-id.

Al recibir la llamada, el terminal de Bernardo lleva a cabo una serie de cálculos a partir de los identificadores Ni presentes en su directorio. De manera más precisa, el terminal receptor de la llamada determina unos testigos de control asociados a los diferentes identificadores presentes en su agenda de direcciones, aplicando la función *hash* H= SHA1(S | Ni) para cada uno de los números Ni de la agenda de direcciones del terminal de Bernardo.

Quién	Agenda de direcciones	SHA1(S | NA) resultante (testigo de control)
Daniel	+33145295750	80939d5b3115c68b6442d8f7acc75638628cf727
Ludovico	+33169284275	0bae4d53ddc85f615f8488ef1579a7cef8f1614d
Alicia	+33296106155	68e2d03501daba37a**25720e9**cb77e84af05a0a96
Marión	+33296106153	540be3f89456278aad8b5a2adb78cadf56f4f892
Guido	+33169284274	f41219e7c1faf157b21ff2347362c9524bef6c31
etc.		

El terminal de Bernardo compara entonces los testigos de control obtenidos con el testigo de identificación, y constata que el valor de K= 25720e9 presente en el encabezado “x-qualif-id” es una subcadena de la tercera línea (Alicia). Puede, por tanto, suponer que el emisor de la llamada es Alicia, pero sin poder probarlo. La identidad supuesta (nombre o número) se muestra entonces en el terminal de Bernardo, con opcionalmente una mención que indica su carácter no seguro (por ejemplo nombre o sucesión de cifras seguido/a de un símbolo de interrogación). También se puede mostrar el simple hecho de que se detecta la identidad en el directorio, por ejemplo por medio de un mensaje de tipo “número oculto (presente en su directorio)”.

Se puede ver que en un directorio de tamaño pequeño como el de un particular (que contiene en general menos de doscientos números), la probabilidad relativa de colisión en el directorio debe ser insignificante con el fin de no ocasionar confusión en el usuario. Esta lo será en la práctica en la medida en que una proporción poco importante de usuarios se presenta con un número oculto, y en que el terminal puede proceder mediante auto-aprendizaje, examinando de forma sucesiva.

- las identidades de naturaleza de presentación no determinable (servicio de identificación del solicitante en fase de llamada posible o no -en inglés CLIP por “calling line identification presentation”);
- las identidades que sabe que se han presentado de forma explícita (CLIP) recientemente, por ejemplo utilizando el diario de llamadas.

Hay que señalar que son posibles otras implementaciones distintas de un encabezado específico, como por ejemplo un parámetro específico en un campo de identidad existente.

Además, se puede expresar la simiente en un formato más compacto, como el formato hexadecimal.

Por último, el caso de interfuncionamiento con otras redes basadas, por ejemplo, en señalizaciones de circuito no se describe en detalle, pero se puede imaginar en función de las extensiones de protocolo disponibles, o de elementos específicos del operador.

En la entrada de la red IMS, si no se proporciona el encabezado x-qualif-id (o su equivalente en el protocolo de la red interconectada), pero la identidad del emisor aun está disponible (acompañada de una indicación de no divulgación), entonces se puede generar el encabezado x-qualif-id.

5.3 Descripción de los dispositivos de transmisión y de recepción de acuerdo con la invención

Se presenta finalmente, en relación con las figuras 4 y 5 respectivamente, la estructura simplificada de un dispositivo de transmisión que implementa una técnica de transmisión de una llamada con número oculto y la estructura de un

dispositivo de recepción que implementa una técnica de recepción de una llamada con número oculto de acuerdo con una forma particular de realización de la invención.

Como se ilustra en la figura 4, dicho dispositivo de transmisión comprende una memoria 41 que comprende una memoria temporal, una unidad de tratamiento 42, equipada por ejemplo con un microprocesador µP y controlada por el programa de ordenador 43, que implementa el procedimiento de transmisión de acuerdo con la invención.

En la inicialización, se cargan las instrucciones de código del programa de ordenador, por ejemplo, en una memoria RAM antes de que las ejecute el procesador de la unidad de tratamiento 42. La unidad de tratamiento 42 recibe en la entrada una llamada Ap que hay que transmitir. El microprocesador de la unidad de tratamiento 42 implementa las etapas del procedimiento de transmisión descrito con anterioridad, de acuerdo con las instrucciones del programa de ordenador 43, para generar el testigo de identificación, y transmitir la llamada con número oculto ApM y el testigo de identificación K (y eventualmente la simiente) a un destinatario. Para ello, el dispositivo de transmisión comprende, además de la memoria temporal 41, un módulo de generación de un testigo no invertible de identificación del emisor, a partir de un identificador del emisor, y al menos un módulo de transmisión al destinatario de la llamada con número oculto y del testigo de identificación. A estos módulos los controla el microprocesador de la unidad de tratamiento 42.

Como se ilustra en la figura 5, dicho dispositivo de recepción de una llamada con número oculto comprende por su parte una memoria 51 que comprende una memoria temporal, una unidad de tratamiento 52, equipada por ejemplo con un microprocesador µPm y controlada por el programa de ordenador 53, que implementa el procedimiento de recepción de una llamada con número oculto de acuerdo con la invención.

En la inicialización, se cargan las instrucciones de código del programa de ordenador 53, por ejemplo, en una memoria RAM antes de que las ejecute el procesador de la unidad de tratamiento 52. La unidad de tratamiento 52 recibe la entrada una llamada con número oculto ApM, así como un testigo de identificación K. El microprocesador de la unidad de tratamiento 52 implementa las etapas del procedimiento de recepción descrito con anterioridad, de acuerdo con las instrucciones del programa de ordenador 53, para determinar unos testigos de control asociados a los identificadores de un directorio del destinatario, comparar estos testigos de control con el testigo de identificación y detectar si uno de los testigos de control corresponde al testigo de identificación.

Para ello, el dispositivo de recepción comprende, además de la memoria temporal 51, al menos un módulo de recepción de la llamada con número oculto y de un testigo no invertible de identificación del emisor, generado a partir de un identificador del emisor, un módulo de generación de al menos un testigo de control, a partir de al menos un identificador presente en un directorio del destinatario, un módulo de comparación del testigo de identificación y del o de los testigos de control, y un módulo de restitución al destinatario bien de una información que representa el identificador del emisor, bien de una mención indicando la presencia del identificador del emisor en el directorio del destinatario, activado en caso de detección de al menos una porción idéntica entre el testigo de identificación y uno de los testigos de control. A estos módulos los controla el microprocesador de la unidad de tratamiento 52.

REIVINDICACIONES

1. Procedimiento de transmisión de una llamada de un emisor (A) hacia un destinatario (B), en el que la identidad de dicho emisor está oculta para dicho destinatario, denominada llamada con número oculto, caracterizado por que implementa las siguientes etapas:

- generación (21) de un testigo no invertible de identificación de dicho emisor, a partir de un identificador de dicho emisor; y
- transmisión (22) a dicho destinatario de dicha llamada con número oculto y de dicho testigo de identificación.

2. Procedimiento de transmisión de acuerdo con la reivindicación 1, caracterizado por que dicho identificador del emisor es el número de teléfono del emisor o una parte de este número.

3. Procedimiento de transmisión de acuerdo con una cualquiera de las reivindicaciones 1 y 2, caracterizado por que dicha etapa de generación (21) de un testigo de identificación también tiene en cuenta una simiente.

4. Procedimiento de transmisión de acuerdo con la reivindicación 3, caracterizado por que se genera una nueva simiente en cada nueva llamada que hay que transmitir.

5. Procedimiento de transmisión de acuerdo con una cualquiera de las reivindicaciones 1 a 4, caracterizado por que dicha etapa de generación implementa una función *hash*, que emite un condensado representativo de un identificador de dicho emisor.

6. Dispositivo de transmisión de una llamada de un emisor (A) hacia un destinatario (B), en el que la identidad de dicho emisor está oculto para dicho destinatario, denominada llamada con número oculto, caracterizado por que comprende:

- un módulo de generación de un testigo no invertible de identificación de dicho emisor, a partir de un identificador de dicho emisor; y
- al menos un módulo de transmisión a dicho destinatario de dicha llamada con número oculto y de dicho testigo de identificación.

7. Terminal caracterizado por que comprende un dispositivo de transmisión de acuerdo con la reivindicación 6.

8. Señal de transmisión de una llamada de un emisor (A) hacia un destinatario (B), en el que la identidad de dicho emisor está oculta para dicho destinatario, denominada llamada con número oculto, caracterizada por que comprende un campo específico que lleva al menos un testigo no invertible de identificación de dicho emisor, generado a partir de un identificador de dicho emisor y que también lleva dicha llamada con número oculto.

9. Procedimiento de recepción de una llamada emitida por un emisor (A) hacia un destinatario (B), en el que la identidad de dicho emisor está oculta para dicho destinatario, denominada llamada con número oculto, caracterizado por que implementa las siguientes etapas:

- recepción (31) de dicha llamada con número oculto y de un testigo no invertible de identificación de dicho emisor, generado a partir de un identificador de dicho emisor;
- generación (32) de al menos un testigo de control, a partir de al menos un identificador presente en un directorio de dicho destinatario;
- comparación (33) de dicho testigo de identificación y de dicho al menos un testigo de control; y
- en caso de detección de al menos una porción idéntica entre dicho testigo de identificación y uno de dichos testigos de control, restitución (34) a dicho destinatario bien de una información que representa dicho identificador del emisor, bien de una mención que indica la presencia de dicho identificador del emisor en dicho directorio del destinatario.

10. Procedimiento de recepción de acuerdo con la reivindicación 9, caracterizado por que dicha etapa de generación también tiene en cuenta una simiente.

11. Procedimiento de recepción de acuerdo con una cualquiera de las reivindicaciones 9 y 10, caracterizado por que dicha etapa de generación de al menos un testigo de control implementa una función *hash*, idéntica a una función *hash* utilizada para la generación de dicho testigo de identificación.

12. Dispositivo de recepción de una llamada emitida por un emisor (A) hacia un destinatario (B), en el que la identidad de dicho emisor está oculta para dicho destinatario, denominada llamada con número oculto, caracterizado por que comprende:

- al menos un módulo de recepción de dicha llamada con número oculto y de un testigo no invertible de identificación de dicho emisor, generado a partir de un identificador de dicho emisor;
- un módulo de generación de al menos un testigo de control, a partir de al menos un identificador presente en un directorio de dicho destinatario;
- un módulo de comparación de dicho testigo de identificación y de dicho al menos un testigo de control; y
- un módulo de restitución a dicho destinatario bien de una información que representa dicho identificador del emisor, bien de una mención que indica la presencia de dicho identificador del emisor en dicho directorio del destinatario, activado en caso de detección de al menos una porción idéntica entre dicho testigo de identificación y uno de dichos testigos de control.

13. Terminal caracterizado por que comprende un dispositivo de recepción de acuerdo con la reivindicación 12.

14. Programa de ordenador que consta de unas instrucciones para la implementación de un procedimiento de transmisión de acuerdo con la reivindicación 1 o de un procedimiento de recepción de acuerdo con la reivindicación 9 cuando este programa lo ejecuta un procesador.

15. Soporte de información, inamovible, o parcial o totalmente extraíble, legible mediante un ordenador y que consta de instrucciones de un programa de ordenador para la ejecución de las etapas de un procedimiento de transmisión de acuerdo con la reivindicación 1 o de un procedimiento de recepción de acuerdo con la reivindicación 9.

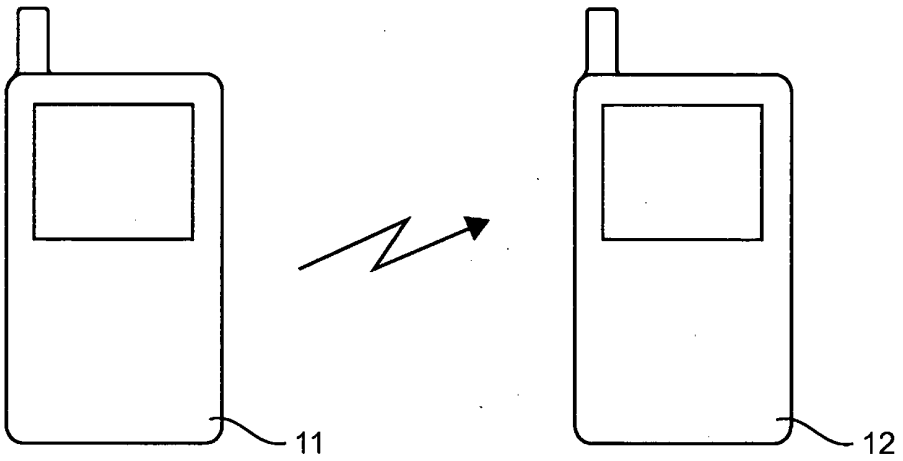

Fig. 1

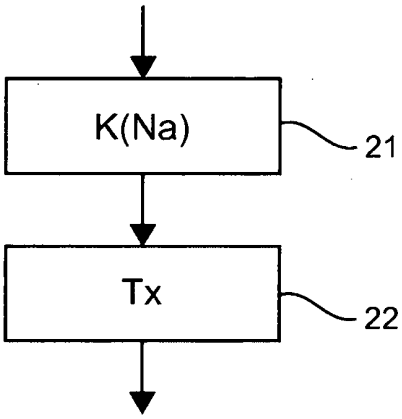

Fig. 2

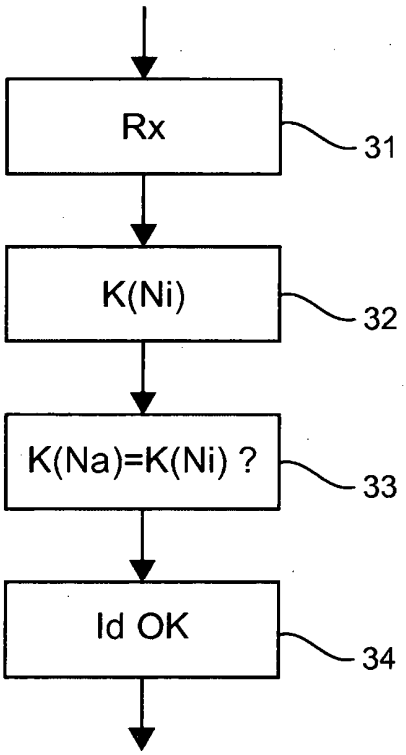

Fig. 3

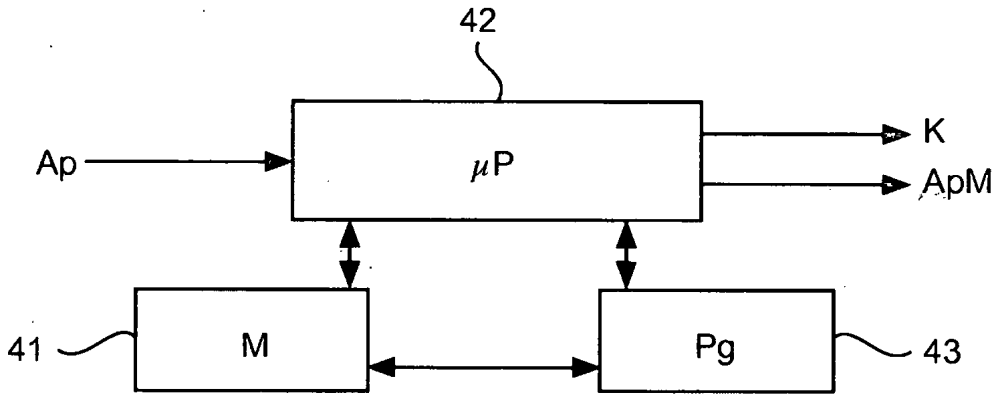

Fig. 4

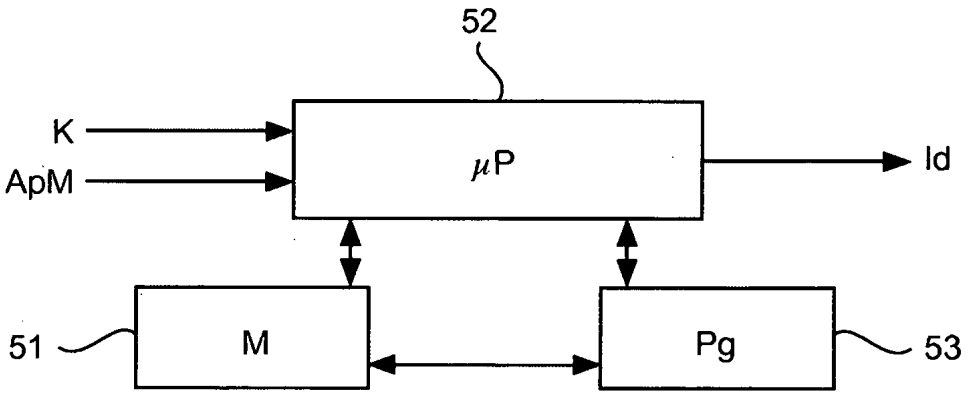

Fig. 5