(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 792 974**

(51) Int. CI.:

***G06F 21/57*** (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **19.12.2014 PCT/EP2014/078731**

(87) Fecha y número de publicación internacional: **09.07.2015 WO15101522**

(96) Fecha de presentación y número de la solicitud europea: **19.12.2014 E 14815743 (1)**

(97) Fecha y número de publicación de la concesión europea: **04.03.2020 EP 3090376**

(54) Título: **Procedimiento para acceder a un servicio y un servidor correspondiente**

(30) Prioridad:

**30.12.2013 EP 13306888**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
**12.11.2020**

(73) Titular/es:

**THALES DIS FRANCE SA (100.0%)**
**6, rue de la Verrerie**
**92190 Meudon, FR**

(72) Inventor/es:

**EL MAROUANI, ABDELLAH y**
**FRANCHI, CHRISTOPHE**

(74) Agente/Representante:

**ELZABURU, S.L.P**

## DESCRIPCIÓN

Procedimiento para acceder a un servicio y un servidor correspondiente

**Campo de la invención:**

La invención se refiere, en general, a un procedimiento para acceder a un servicio que proporciona al menos un nivel de confianza de dispositivo de usuario.

Además, la invención también se refiere a un servidor para acceder a un servicio que proporciona al menos un nivel de confianza de dispositivo de usuario.

**Estado de la técnica:**

Los documentos US 2010/100939 A1 y WO 2013/147891 A1 divulgan ambos una técnica anterior.

El documento WO 2009/105540 A1 se refiere a una solución de asignar una función a un usuario en un entorno distribuido en base a un nivel actual de confianza. El nivel actual de confianza se determina en base al contexto y los atributos de la entidad.

Hoy en día, cada vez hay más dispositivos de comunicación, tales como teléfonos móviles, tabletas, ordenadores personales (o PC), PC portátiles, asistentes digitales personales (o PDA) u otros terminales de usuario que están conectados a una red de radiocomunicación móvil o a una red de tipo Internet. Por tanto, dichas personas conectadas están llevando a cabo comunicaciones más sencillas entre sí a través de llamadas de voz, llamadas visuales y de audio, mensajes de texto intercambiados, por medio de correos electrónicos o mensajes de tipo Servicio de mensajes cortos (SMS), o similares.

Sin embargo, cuando un usuario de un teléfono móvil, como un dispositivo, desea comunicarse o llevar a cabo una transacción con otro usuario de dispositivo, el usuario de dispositivo desea saber si puede confiar o no en el otro usuario de dispositivo antes del intercambio con este último.

De este modo, el usuario de dispositivo no se convierte en víctima de un robo, como el otro usuario de dispositivo e interlocutor.

Existe una necesidad de proporcionar una solución que permita saber si un posible usuario de dispositivo interlocutor puede ser confiable o no.

**Sumario de la invención:**

La invención propone una solución para resolver la necesidad especificada anteriormente en el presente documento proporcionando un procedimiento para acceder a un servicio que proporciona al menos un nivel de confianza de dispositivo de usuario, definiéndose el procedimiento en la reivindicación 1 y proporcionando un servidor correspondiente como se define en la reivindicación 10.

El principio de la invención consiste en que un servidor remoto recopila información relacionada con cada aplicación de primer dispositivo de usuario que se comunica con una aplicación de segundo dispositivo de usuario y determina, utilizando la información recopilada, como un informe de primer dispositivo de usuario, un nivel de confianza de primer dispositivo de usuario. A continuación, el servidor remoto transmite el nivel de confianza de primer dispositivo de usuario después de una solicitud que se origina en un tercer dispositivo.

Por tanto, el servidor remoto realiza un seguimiento de una actividad relacionada con una o varias aplicaciones de comunicación ejecutadas en un lado del primer dispositivo.

Se debe observar que, en la presente descripción, una aplicación de transacción es una aplicación de comunicación particular.

La solución de la invención permite a un usuario de tercer dispositivo que desea comunicarse con un primer dispositivo saber más, como solicitante de un nivel de confianza relacionado con el primer dispositivo, sobre un usuario de primer dispositivo, como su interlocutor potencial.

Por tanto, el usuario de tercer dispositivo puede formar una opinión positiva sobre el usuario de primer dispositivo que es confiable si el nivel de confianza de primer dispositivo es mayor que un umbral predefinido.

Cabe señalar que el tercer dispositivo puede ser el segundo dispositivo. En otras palabras, el tercer dispositivo puede haberse comunicado con el primer dispositivo y puede haberse enviado un informe de primer dispositivo correspondiente y/o un informe de tercer dispositivo correspondiente desde el primer dispositivo y/o el tercer dispositivo, respectivamente.

**Breve descripción de los dibujos:**

Las características y ventajas adicionales de la invención se comprenderán más claramente después de leer una descripción detallada de un modo de realización preferente de la invención, dado como un ejemplo indicativo y no limitativo, junto con los siguientes dibujos:

- la Figura 1 ilustra un diagrama simplificado de un servidor remoto que está conectado a un terminal y un teléfono móvil que incluye un chip, estando dispuesto el servidor remoto para recibir información relacionada con una actividad de comunicación del teléfono, para determinar un nivel de confianza relacionado con el teléfono y para enviar, cuando se solicite, al terminal el nivel de confianza del teléfono, de acuerdo con la invención; y

- la Figura 2 representa un ejemplo de un flujo de mensajes entre el servidor remoto, el chip y el terminal de la Figura 1, de modo que el usuario del terminal decida si inicia (o no) un intercambio con el usuario del teléfono, gracias a nivel de confianza del teléfono recibido del servidor remoto.

**Descripción detallada:**

A continuación en el presente documento, se considera un caso en el que el procedimiento de la invención para acceder a un servicio se implementa mediante un servidor remoto y un teléfono móvil, como un primer dispositivo, que incluye un chip incrustado.

De acuerdo con otro modo de realización, el procedimiento de la invención para acceder a un servicio se implementa mediante un servidor remoto y un teléfono móvil, como primer dispositivo y entidad independiente. En otras palabras, el teléfono móvil, como un terminal de usuario (y, más exactamente, el microprocesador del teléfono) no coopera con ningún chip, para enviar al servidor remoto información relacionada con cualquier actividad de comunicación del teléfono. De acuerdo con dicho modo de realización (no representado), el primer dispositivo está adaptado para llevar a cabo las funciones que llevan a cabo el chip y el primer dispositivo y que se describen a continuación.

Naturalmente, el modo de realización descrito a continuación en el presente documento es solo para fines ilustrativos y no se considera que reduzca el alcance de la invención.

La Figura 1 muestra esquemáticamente un equipo móvil 10, como un terminal de un usuario, y un terminal 114, como un terminal de otro usuario, que están conectados a un servidor remoto 110.

El equipo móvil 10 incluye un teléfono móvil 12, como un terminal de usuario, y una tarjeta de circuito integrado universal incrustada (o eUICC) 14, como un chip incrustado acoplado al teléfono móvil 12.

En lugar de estar incrustado, el chip puede estar incluido dentro de una tarjeta inteligente denominada tarjeta de tipo Módulo de identidad de abonado (o SIM) o similar, como un elemento seguro (Secure Element, o SE).

La invención no impone ninguna restricción en cuanto a una clase del tipo de SE. Como un SE extraíble, puede ser una tarjeta de tipo SIM, un Módulo extraíble seguro (Secure Removable Module, o SRM), un dongle inteligente del tipo USB (acrónimo de "Universal Serial Bus"), una tarjeta de tipo (micro-) Secure Digital (o SD) o una tarjeta de tipo multimedia (Multi-Media Card, o MMC) o una tarjeta de cualquier formato que se acople a un dispositivo huésped, como primer dispositivo.

En la presente descripción, un elemento seguro (o SE) es un objeto inteligente que, por un lado, protege el acceso a los datos que almacena el objeto inteligente y, por otro lado, está concebido para comunicarse con el mundo exterior.

Por razones de simplicidad, el teléfono móvil 12, la eUICC 14, el otro terminal de usuario 114 y el servidor remoto 110 se denominan a continuación en el presente documento el teléfono 12, el chip 14, el PC 114 y el servidor 110, respectivamente.

Solo se representan un teléfono 12 y un PC 114 que están conectados al servidor 110 por razones de claridad. Sin embargo, se puede acceder al servidor 110 y acceder, por el aire (Over-The-Air, u OTA), a través de Internet (Over-The-Internet, u OTI) o a través de la nube (Over The Cloud, u OTC), a una flota de terminales conectados.

En lugar de un teléfono, puede ser cualquier otro dispositivo que incluya medios para procesar datos, que comprenda o esté conectado a medios de comunicación inalámbrica para intercambiar datos con el exterior, y que comprenda o esté conectado a medios para almacenar datos.

En la presente descripción, el adjetivo "inalámbrico" denota notablemente que los medios de comunicación se comunican por medio de uno o varios enlaces de radiofrecuencia (o RF) de largo alcance (o LR).

La RF de LF se puede fijar a varios cientos de MHz, por ejemplo, alrededor de 850, 900, 1800, 1900 y/o 2100 MHz.

El teléfono 12 se usa para acceder a una o varias redes de radiocomunicación móvil.

La una o varias redes de radiocomunicación móvil pueden estar constituidas por un Servicio Global para Móviles (Global Service for Mobiles, o GSM), un Servicio General de Radio por Paquetes (General Packet Radio Service, o GPRS), un Sistema Universal de Telecomunicaciones Móviles (Universal Mobile Telecommunications System, o UMTS), una UTRAN (acrónimo de "UMTS Terrestrial Radio Access Network", "Red de acceso por radio terrestre del UMTS"), un EDGE (acrónimo de "Enhanced Data Rates for GSM Evolution", "Velocidades de datos mejoradas para la evolución de GSM"), un Acceso múltiple por división de código (Code Division Multiple Access, o CDMA), una WLAN (acrónimo de "Wide Local Area Network", "Red de área local amplia") y/o redes de tipo Evolución a largo plazo (Long Term Evolution, o LTE).

Dicho conjunto de redes de radiocomunicación móvil no es exhaustivo, sino que solo tiene fines ilustrativos.

La(s) red(es) de radiocomunicación móvil (no representada(s)) se incluye(n) dentro de una red 18 que está conectada al servidor 110.

La red 18 comprende o está conectada a una red de tipo Internet (no representada).

El teléfono 12 está habilitado para la comunicación de campo cercano (Near Field Communication, o NFC) y, como tal, puede comunicarse con un dispositivo sin contacto (Contact-Less, o CL) 16.

La tecnología de comunicación NFC se incluye dentro de una tecnología de comunicación CL, como tecnología de comunicación de proximidad.

El dispositivo CL 16 puede ser una etiqueta de identificación por radiofrecuencia (Radio Frequency IDentification, o RFID) a leer, un lector CL o similar.

El dispositivo CL 16 puede estar conectado a una red de comunicación, como un sistema de salida (no representado) y a una infraestructura de NFC.

El dispositivo CL 16 incluye una antena 162 para comunicarse, a través de un enlace de RF de corto alcance (o SR) 15, con un dispositivo externo, como el teléfono 12, como terminal de usuario.

La antena 162 puede recibir datos y enviar datos al exterior, a través del enlace de RF de SR 15.

El dispositivo CL 16 está presente en una localización geográfica en la que se puede acceder a una o varias aplicaciones o servicios CL.

En cuanto al teléfono 12, puede ser cualquier dispositivo que incluya medios para procesar datos, que comprenda o esté conectado a una primera antena 122 para enviar y/o recibir datos del exterior, que comprenda o esté conectado a medios para interactuar con un usuario, como interfaz hombre máquina (Man Machine Interface, o MMI), como un teclado 124, un altavoz (no representado) y/o una pantalla de visualización 126, que comprenda o esté conectado a medios para almacenar datos, y que comprenda o esté conectado a una segunda antena 128 para enviar a y/o recibir datos del exterior.

El teléfono 12 incluye una batería (no representada), uno o varios microprocesadores (no representados), como medios de procesamiento de datos, una o varias memorias (no representadas), como medios de almacenamiento de datos y dos o más interfaces de E/S.

La primera antena 122 permite el intercambio, por medio de un chip NFC (no representado), a través del enlace de RF de SR 15, con una(s) entidad(es) CL externa(s) de datos transportados por una señal de RF de SR.

El enlace de RF de SR 15 también se denomina enlace CL y permite comunicar datos de manera cercana, por ejemplo, hasta 20 cm.

La frecuencia del enlace de RF de SR 15 se puede fijar, por ejemplo, a 13,56 MHz.

La RF de SR está relacionada con una tecnología de comunicación sin contacto, como tecnología de comunicación de proximidad.

El chip NFC incluye, en particular, un(os) microprocesador(es) (no representado(s)), como medios para procesar datos, una(s) memoria(s) (no representada(s)), como medios para almacenar datos y al menos una interfaz de Entrada/Salida (o E/S) (no representada) para intercambiar datos con el mundo exterior, que están unidos internamente a través de un bus de datos y control (no representado).

El chip NFC, o denominado chip de entrada sin contacto (Contact-Less Front End, o CLF), está incorporado dentro del teléfono 12.

De acuerdo con un modo de realización alternativo (no representado), el chip NFC se incorpora dentro de un SE separado que está acoplado al teléfono e interactúa con el teléfono.

El chip NFC está soldado en una placa de circuito impreso (o PCB) del teléfono 12. El chip NFC está conectado al microprocesador del teléfono y a la primera antena 122 configurada para intercambiar datos, a través de una señal de RF de SR, con un dispositivo de comunicación CL externo.

El chip NFC se conecta directamente o a través de una interfaz de E/S del teléfono al chip 14.

El chip NFC desempeña un papel de modulador-demodulador (o módem) para el chip 14, es decir, un dispositivo que:

- demodula una señal portadora analógica recibida para descodificar información digital codificada que se recibe, a través de la primera antena 122, desde una entidad CL externa y se transmite al chip 14, y

- modula una señal portadora analógica para codificar la información digital recibida del chip 14 y para transmitirse, a través de la primera antena 122, a una entidad CL externa.

En un modo lector, es decir, cuando la batería del teléfono 12 alimenta un dispositivo CL externo 16, el chip NFC recibe energía de la batería del teléfono 12 y alimenta el dispositivo CL difundiendo una señal de RF de SR. La batería del teléfono 12 alimenta el chip 14 y los componentes electrónicos del teléfono 12.

En un modo de emulación de tarjeta (o modo de transpondedor), es decir, si el chip 14 se alimenta, al menos en parte, mediante un dispositivo CL externo 16, el chip NFC recibe energía del dispositivo CL 16 y proporciona energía al chip 14 y a los componentes del teléfono 12. El chip 14 se alimenta así incluso si la batería del teléfono está apagada.

En el modo lector y en el modo de emulación de tarjeta, el chip NFC se comunica con el chip 14, como su interlocutor.

El chip NFC y el chip 14 pueden intercambiar datos implementando un protocolo del tipo Protocolo de cable único (Single Wire Protocol, o SWP), como protocolo de bajo nivel.

El chip NFC puede intercambiar con el chip 14 implementando un protocolo del tipo Interfaz de controlador de huésped (Host Controller Interface, o HCI), como protocolo de alto nivel, es decir, un protocolo utilizado para el intercambio desde una aplicación ejecutada por el microprocesador del chip NFC a una aplicación ejecutada por un microprocesador del chip 142.

El microprocesador del teléfono procesa datos que se originan en la memoria del teléfono o en una entidad externa. El microprocesador del teléfono ejecuta una o varias aplicaciones, para interactuar con una aplicación que es soportada por el chip 14 y se ofrece al usuario del teléfono.

La(s) memoria(s) del teléfono puede(n) comprender una o varias memorias volátiles y una y/o varias memorias no volátiles.

La memoria del teléfono almacena datos, como datos de usuario.

La memoria del teléfono almacena un sistema operativo (u OS) y una o varias aplicaciones para que el microprocesador del teléfono las ejecute.

Como aplicaciones, existe al menos una aplicación de comunicación para comunicarse con un dispositivo de usuario externo, como una aplicación de llamadas telefónicas, una aplicación de comunicación de mensajes de tipo SMS, una aplicación de comunicación de mensajes de tipo correo electrónico, una aplicación de pago por Internet y/o similares.

Cada una de las aplicaciones de comunicación soportadas por el teléfono 12 se mide mediante una aplicación soportada por el teléfono 12, como una aplicación complementaria de una aplicación de la invención para medir una actividad de comunicación de usuario que es soportada por el chip 14 y se describe más adelante.

Para medir cada una de las aplicaciones de comunicación que soporta el teléfono 12, la aplicación complementaria se activa cada vez que se produce un evento entrante o saliente mientras se obtienen datos relacionados con la ejecución de la aplicación de comunicación en cuestión. Más exactamente, la aplicación complementaria se activa cada vez que:

- hay una llamada telefónica entrante o saliente para la aplicación de llamadas telefónicas;

- se recibe o envía un mensaje de tipo SMS para la aplicación de comunicación de mensajes de tipo SMS;

- se recibe o envía un mensaje de tipo correo electrónico para la aplicación de comunicación de mensajes de tipo correo electrónico;

- se recibe o se envía un pago por Internet para la aplicación de pago por Internet.

La aplicación complementaria está adaptada para transmitir a la aplicación de la invención soportada por el chip 14, cada vez que se produce un evento entrante o un evento saliente, datos relacionados con una aplicación de comunicación en cuestión que se ejecuta mediante el teléfono 12 y se recupera de la aplicación de comunicación en cuestión.

Como aplicaciones soportadas por el teléfono 12, también hay preferentemente al menos un menú o un navegador web, como interfaz de usuario para acceder a una o varias aplicaciones soportadas por el chip 14, como una o varias aplicaciones de comunicación que usan una tecnología de comunicación CL. Una aplicación del chip 14 permite comunicar o intercambiar datos, a través de un enlace CL, a través de la primera antena 122, de una manera cercana, entre, por ejemplo, el dispositivo CL proximal 16, el chip 14 y un usuario de teléfono.

El teléfono 12 se puede usar para permitir la comunicación, a través del chip NFC, de manera cercana, al chip 14 y al dispositivo CL proximal 16.

La MMI del teléfono permite que un usuario de teléfono interactúe con el teléfono 12 o el chip 14.

La segunda antena 128 permite comunicar datos, a través de un enlace de RF de LR 17, con una o varias redes de radiocomunicación móvil que están conectadas al servidor 110 y a cualquier otra entidad, como el PC 114.

El teléfono 12 desempeña, de manera preferente, un papel de modulador-demodulador (o módem) especialmente para el chip 14.

El teléfono 12 lleva a cabo las siguientes operaciones:

- una modulación de una señal portadora analógica para codificar información digital a transmitir, a través de la segunda antena 128, al servidor 110 y/u a otra entidad, como el PC 114, y

- una demodulación de una señal portadora analógica recibida para descodificar la información digital codificada que se recibe, a través de la segunda antena 128, desde el servidor 110 y/u otra entidad, como el PC 114.

Por tanto, el teléfono 12 puede intercambiar datos, de manera distante, con el servidor 110 o una entidad, como otro teléfono móvil o el PC 114, que esté conectada a una red de radiocomunicación móvil y/o a la red 18.

El teléfono 12, como dispositivo huésped del chip 14, está preferentemente acoplado o conectado al chip 14.

Las interfaces de E/S del teléfono incluyen una o varias interfaces de E/S para intercambiar datos con el chip 14.

El chip 14 está bajo el control del microprocesador del teléfono.

Alternativamente, en lugar de estar acopladas al chip 14, la(s) memoria(s) del teléfono almacena(n) datos almacenados dentro del chip 14, como se describe más adelante.

De acuerdo con un modo de realización particular, el chip 14 está soldado a una placa de circuito impreso (o PCB) del teléfono 12.

De acuerdo con otro modo de realización, la interfaz de E/S del teléfono con el chip 14 es una interfaz 7816 de la Organización Internacional de Normalización (o ISO), como interfaz de contacto, cuando el chip 14 se inserta, de manera extraíble, dentro del teléfono 12.

Alternativamente, en lugar de una interfaz de contacto, la interfaz de E/S del teléfono con el chip 14 está conectada a o incluye una interfaz CL. El teléfono 12 está conectado a o incluye medios para comunicar datos mientras se usa preferentemente un enlace de RF de SR. El enlace de RF de SR puede estar relacionado con cualquier tecnología que permita que el teléfono 12 intercambie datos, a través de un enlace CL, con el chip 14. La RF de SR puede estar relacionada con una tecnología de comunicación de tipo NFC.

El chip 14 pertenece a un usuario, como abonado de uno o más servicios inalámbricos y preferentemente usuario de uno o más servicios CL.

El chip 14 está conectado, a través de un enlace bidireccional 13, al teléfono 12.

El chip 14 incluye un(os) microprocesador(es) 142, como medios de procesamiento de datos, una(s) memoria(s) 144, como medios de almacenamiento de datos, y una o varias interfaces de E/S 146 que están todos conectados entre sí internamente, a través de un bus de datos bidireccional interno 143.

La(s) interfaz(interfaces) de E/S 146 permite(n) la comunicación de datos desde los componentes internos del chip al exterior del chip y viceversa.

El microprocesador 142 procesa, controla y comunica internamente datos con el resto de componentes incorporados dentro del chip y, a través de la(s) interfaz(interfaces) de E/S 146, con el exterior del chip.

El microprocesador 142 ejecuta una o varias aplicaciones.

Como aplicaciones, hay al menos una aplicación de comunicación para comunicarse con un dispositivo de usuario externo, tal como una o varias aplicaciones de tipo de administración electrónica NFC, una o varias aplicaciones de tipo de banca/finanzas NFC, una o varias aplicaciones de tipo de comunicación móvil NFC, una o varias aplicaciones de tipo de fidelidad NFC, una o varias aplicaciones de tipo de venta de entradas NFC, una o varias aplicaciones de tipo de transporte NFC, una o varias aplicaciones de tipo de pago NFC y/o una o varias aplicaciones de tipo de información NFC y/u otras aplicaciones de comunicación CL.

Entre las aplicaciones soportadas por el chip 14, hay una aplicación de la invención para medir una actividad de comunicación de usuario, es decir, cualquier evento entrante o cualquier evento saliente que se origine en el teléfono 12 si la aplicación de comunicación en cuestión se ejecuta mediante el teléfono 12 o en el chip 14 si la aplicación de comunicación en cuestión se ejecuta mediante el chip 14.

La aplicación de la invención para medir una actividad de comunicación de usuario permite que la aplicación recopile datos relacionados con la ejecución de cualquier aplicación medida, como primera ejecución de aplicación. La aplicación medida se utiliza para comunicarse con otro dispositivo externo, independientemente de si la aplicación de comunicación medida se ejecuta mediante el teléfono 12 o el chip 14.

Cada una de las aplicaciones de comunicación soportadas por el chip 14 se mide mediante una aplicación de la invención soportada por el chip 14.

Para medir cada una de las aplicaciones de comunicación soportadas por el teléfono 12 o el chip 14, la aplicación de la invención se activa cada vez que se produce un evento entrante o un evento saliente mientras se obtienen datos relacionados con la ejecución de la aplicación de comunicación en cuestión.

Para medir un evento entrante o un evento saliente en el lado del teléfono 12, la aplicación complementaria soportada por el teléfono 12 notifica a la aplicación de la invención soportada por el chip 14 cuándo la aplicación de comunicación en cuestión que ejecuta el teléfono 12 recibe un comando correspondiente.

Por ejemplo, la aplicación complementaria que se ejecuta mediante el teléfono 12 notifica a la aplicación de la invención soportada por el chip 14 cada vez que la aplicación de llamadas telefónicas recibe una solicitud de establecimiento de llamada cuando la aplicación de la invención soportada por el chip 14 se registra en el evento "EVENT_EVENT_DOWNLOAD_MT_CALL" en el que MT se usa para "Terminado por el móvil".

Por ejemplo, la aplicación complementaria ejecutada por el teléfono 12 notifica a la aplicación de la invención soportada por el chip 14 cada vez que un mensaje de tipo SMS se va a actualizar en el archivo de mensajes cortos del chip 14 mediante la aplicación de comunicación de mensajes de tipo SMS cuando la aplicación de la invención soportada por el chip 14 se registra en el evento "EVENT_UNFORMATTED_SMS_PP_UPD" en el que PP se usa para "Punto a punto" y UPD se usa para "Actualizado".

Para medir un evento entrante o un evento saliente en el lado del chip 14, se notifica directamente a la aplicación de la invención soportada por el chip 14, es decir, sin ninguna aplicación intermediaria como una aplicación complementaria, cada vez que la aplicación de comunicación en cuestión recibe un comando correspondiente que se ejecuta mediante el chip 14.

Si el chip 14 soporta la aplicación de comunicación, la aplicación de la invención se activa cada vez que se produce un evento entrante o saliente mientras se obtienen datos relacionados con la ejecución de la aplicación de comunicación en cuestión.

Por ejemplo, para una aplicación de tipo de pago NFC soportada por el chip 14, la aplicación de la invención se activa cuando se produce un pago NFC mientras se obtienen datos relacionados con la ejecución del pago NFC en cuestión.

La aplicación medida, como primera aplicación, independientemente de si la aplicación de comunicación en cuestión se ejecuta mediante el teléfono 12 o el chip 14, transmite directa o indirectamente, es decir, a través de la aplicación complementaria intermediaria, a la aplicación de la invención datos relacionados con la ejecución de aplicación (o aplicación de comunicación) medida.

Como datos relacionados con una ejecución de aplicación de comunicación, hay al menos un atributo.

Como atributo(s) relacionado(s) con una ejecución de aplicación de comunicación, se pueden incluir un tipo de tecnología de comunicación de datos, un tipo de aplicación de comunicación, un tipo de función de usuario, una fecha y hora de ejecución de aplicación de comunicación de teléfono, una localización relacionada con el teléfono 12 cuando el teléfono 12 ejecuta la aplicación de comunicación de teléfono, un identificador relacionado con el teléfono 12 y/o un identificador relacionado con el chip 14.

Como tipo de tecnología de comunicación de datos, se puede incluir una tecnología de comunicación CL, una tecnología de comunicación inalámbrica y/o una tecnología de comunicación de tipo Internet con o sin autenticación de usuario.

Como tipo de aplicación de comunicación, la aplicación de comunicación (o primera aplicación) puede ser una aplicación segura o una aplicación no segura. La aplicación segura, cuando se ejecuta, autentica correctamente al usuario de la primera aplicación.

Como tipo de función de usuario (teléfono 12 o chip 14), se puede incluir una función que está vinculada a la aplicación de usuario en la que el usuario, como deudor, da dinero a su interlocutor, en la que el usuario, como acreedor, recibe dinero de su interlocutor, en la que el usuario, como transmisor de datos, transmite datos a su interlocutor, en la que el usuario, como persona que comparte datos mutuamente, comparte datos con su interlocutor o en la que el usuario, como receptor de datos, recibe datos de su interlocutor.

La aplicación de la invención para medir una actividad de comunicación de usuario permite, por tanto, medir o escuchar un conjunto de aplicaciones de comunicación mientras solicita, a cada una de ellas, cuando se produce un evento entrante o saliente correspondiente, ser informada de una ocurrencia del evento en cuestión, preferentemente junto con uno o varios atributos relacionados con la aplicación de comunicación en cuestión, cuando se ejecuta.

La aplicación de la invención para medir una actividad de comunicación de usuario también permite enviar al servidor 110 datos relacionados con la ejecución de aplicación de comunicación que se recopilan desde la aplicación de comunicación en cuestión.

El microprocesador 142 es preferentemente capaz de iniciar acciones, para interactuar directamente con el mundo exterior, de manera independiente del teléfono 12, como un dispositivo huésped del chip. Dicha capacidad de interacción por iniciativa del chip 14 también se conoce como capacidad proactiva. De acuerdo con un modo de realización preferente, el chip 14 puede usar comandos de tipo SIM ToolKit (o STK), como comandos proactivos.

Por tanto, el chip 14 puede enviar, por iniciativa propia, a través del teléfono 12, a cualquier dispositivo conectado al teléfono 12 un comando proactivo para enviar un mensaje al servidor 110, como un mensaje de tipo Protocolo de transferencia de hipertexto (o HTTP), que incluye una solicitud para cargar datos relacionados con cualquier aplicación soportada.

El microprocesador 142 ejecuta, de manera preferente, una o varias funciones de seguridad.

Las funciones de seguridad incluyen preferentemente un proceso de autenticación de usuario que se utilizará antes de continuar la ejecución de una aplicación de comunicación que se puede ejecutar mediante el teléfono 12 o el chip 14. Para autenticar al usuario, el usuario debe proporcionar un Número de identidad personal (o PIN) o datos biométricos, como datos de referencia de usuario, que se almacenan en la memoria 144. Como datos biométricos, se pueden incluir una o varias huellas digitales, una o varias huellas de iris, una o varias huellas de voz relacionadas con uno o varios usuarios autorizados.

La memoria 144 almacena datos relacionados con una o varias suscripciones a varias redes de radiocomunicación móvil, como servicios inalámbricos.

Los datos relacionados con una suscripción a una red de radiocomunicación móvil incluyen:

- una identidad internacional de abonado móvil (o IMSI), como identificador de suscripción de abonado y servicio para acceder a una red de radiocomunicación móvil;

- una clave Ki, como clave de autenticación de red, que permite autenticar al abonado en cuestión en la red de radiocomunicación móvil en cuestión;

- Milenage, como algoritmo de autenticación, que permite autenticar al abonado en cuestión en la red de radiocomunicación móvil en cuestión;

- una o varias contraseñas, como un PIN, y/o uno o varios algoritmos criptográficos, como datos relacionados con un(os) secreto(s), que se almacena(n) de forma segura en el chip 14;

- un sistema de archivos que incluye uno o varios archivos elementales (Elementary Files, o EF);

- una o varias claves de seguridad, como una(s) clave(s) para cifrar/descifrar datos y/o una(s) clave(s) para firmar datos;

- una o varias claves de aplicación, como una clave para acceder a una cuenta bancaria de usuario a través de la red de radiocomunicación móvil; y/o

- una o varias credenciales, como un nombre de usuario y/o un identificador (o ID) del abonado, como datos relacionados con el usuario.

La memoria 144 almacena un OS.

La memoria 144 almacena preferentemente una o varias aplicaciones de tipo Módulo de identidad de abonado (o SIM).

La(s) aplicación(es) de tipo SIM incluye(n), entre otras, una aplicación SIM para una red de tipo Servicio Global para Móviles (o GSM), una aplicación de Módulo de Identidad de Abonado Universal (o USIM) para una red de tipo Sistema Universal de Telecomunicaciones Móviles (o UMTS), una aplicación de Módulo de Identidad de Abonado (o CSIM) de Acceso Múltiple por División de Código (o CDMA) y/o una aplicación de Módulo de Identidad de Abonado (o ISIM) de Subsistema Multimedia de protocolo de Internet (o IMS).

La(s) aplicación(es) de tipo SIM permiten que el teléfono 12 se identifique y se autentique en una o varias redes de radiocomunicación móvil 16.

La memoria 144 almacena una o varias aplicaciones que ejecuta el microprocesador 142. Entre las aplicaciones soportadas, la memoria 144 almacena la aplicación de la invención para medir una actividad de comunicación de usuario. La memoria 144 almacena preferentemente una o varias aplicaciones de comunicación, como una aplicación de pago NFC.

La memoria 144 almacena preferentemente datos relacionados con un Identificador Uniforme de Recursos (Uniform Resource Identifier, o URI), un Localizador Uniforme de Recursos (Uniform Resource Locator, o URL) y/o una dirección de Protocolo de Internet (o IP) de una entidad externa a direccionar, como el servidor 110 o un PC 114, como un dispositivo interlocutor.

El servidor 110 se conecta, a través de un enlace bidireccional 19, a la red 18.

El servidor 110 se identifica mediante un URI, como un URL, una dirección IP o similar, como identificador del servidor.

El identificador del servidor se puede almacenar en la memoria del chip 144 o en la memoria del teléfono.

El servidor 110 se puede hacer funcionar por un operador de red de radiocomunicación móvil, como un MNO o un Operador de red virtual móvil (Mobile Virtual Network Operator, o MVNO), un proveedor de servicios o en su nombre.

El servidor 110 está alojado por un ordenador.

El servidor 110 incluye un(os) microprocesador(es) (no representado(s)), como medios de procesamiento de datos, comprende y/o está conectado a una(s) memoria(s), como medios de almacenamiento de datos, y una o varias interfaces de E/S (no representadas).

El servidor 110 está dedicado a ejecutar una aplicación para gestionar una base de datos y comunicar datos de la base de datos al exterior.

Alternativamente, otro servidor (no representado) que está conectado al servidor 110 gestiona la base de datos.

El servidor 110 se conecta, a través de un enlace bidireccional 111, a una memoria 112 que almacena la base de datos.

En lugar de una memoria externa, el servidor 110 incluye una memoria interna (no representada) que almacena la base de datos.

La base de datos incluye un conjunto de uno o varios identificadores relacionados, cada uno de ellos, con un dispositivo de cliente individual que está, cada uno de ellos, asociado con un nivel de confianza que se determina como se especifica a continuación.

El servidor 110 está adaptado para recibir de cualquier dispositivo de usuario, como dispositivo de cliente, datos relacionados con una ejecución de aplicación de comunicación, como un informe de dispositivo de usuario. El dispositivo de cliente es utilizado por un usuario que pretende ser reconocido preferentemente como una persona confiable.

De acuerdo con una característica esencial de la invención, el servidor 110 está adaptado para determinar, en base a uno o varios informes de dispositivos de usuario, un nivel de confianza relacionado con un dispositivo de usuario.

Para determinar el nivel de confianza relacionado con un dispositivo de usuario, el servidor 110 asigna un factor de ponderación predeterminado a uno o varios atributos relacionados con cada ejecución de aplicación de comunicación.

El servidor 110 está adaptado preferentemente para priorizar al menos un atributo de seguridad relacionado con una o varias ejecuciones de aplicaciones de comunicación.

Como atributo(s) relacionado(s) con una ejecución de aplicación de comunicación, se puede incluir un tipo de tecnología de comunicación de datos, un tipo de aplicación de comunicación, un tipo de función de usuario, una fecha y hora de ejecución de aplicación de comunicación de teléfono, una localización relacionada con el teléfono 12 si el teléfono 12 ejecuta la aplicación de comunicación de teléfono, un identificador relacionado con el teléfono 12 y/o un identificador relacionado con el chip 14.

Por ejemplo, el servidor 110 da un nivel de prioridad en un orden descendente de la lista de atributos indicada anteriormente en el presente documento, es decir, una prioridad más alta en el primero y una prioridad más baja en el último mientras establece un valor de ponderación más alto correspondiente al tipo de tecnología de comunicación de datos y un valor de peso más bajo correspondiente al tipo de dispositivo.

Como tipo de tecnología de comunicación de datos, se puede incluir una tecnología de comunicación CL, una tecnología de comunicación inalámbrica y/o una tecnología de comunicación de tipo Internet con o sin autenticación de usuario.

Por ejemplo, el servidor 110 da un nivel de prioridad en un orden descendente de la lista de tecnología de comunicación de datos indicada anteriormente, es decir, una prioridad más alta en el primero y una prioridad más baja en el último mientras establece un valor de ponderación más alto correspondiente para la tecnología de comunicación CL, como una tecnología de proximidad segura, y un valor de ponderación más bajo correspondiente a la tecnología de comunicación de tipo Internet sin autenticación de usuario, como una tecnología sin proximidad y no segura.

Como un tipo de aplicación de comunicación, la aplicación de comunicación puede ser una aplicación segura o una aplicación no segura. La aplicación segura, cuando se ejecuta, autentica correctamente al usuario de la primera aplicación.

Por ejemplo, el servidor 110 da un nivel de prioridad en un orden descendente de la lista de aplicaciones de comunicación indicadas anteriormente, es decir, una prioridad más alta en la primera y una prioridad más baja en la última mientras establece un valor de ponderación más alto correspondiente para la aplicación segura y un valor de ponderación más bajo correspondiente para la aplicación no segura.

Como tipo de función de usuario, se puede incluir una función en la que el usuario, como deudor, entrega dinero a su interlocutor, en la que el usuario, como acreedor, recibe dinero de su interlocutor, en la que el usuario, como un transmisor de datos, transmite datos a su interlocutor, en la que el usuario, como persona que intercambia datos mutuamente, comparte datos con su interlocutor o en la que el usuario, como receptor de datos, recibe datos de su/su interlocutor.

Por ejemplo, el servidor 110 da un nivel de prioridad en un orden descendente de la lista de funciones de usuario indicada anteriormente, es decir, una prioridad más alta en el primero y una prioridad más baja en el último mientras establece un valor de ponderación más alto correspondiente para el deudor y un valor de ponderación más bajo correspondiente para el receptor de datos.

El servidor 110 determina un nivel de confianza relacionado con un dispositivo de usuario utilizando todos los datos relacionados con una o varias ejecuciones de una o varias aplicaciones de comunicación soportadas en un lado del dispositivo.

El servidor 110 establece preferentemente un nivel de confianza escalonado, como una puntuación de 100, como el valor de nivel de confianza más alto. Si el nivel de confianza relacionado con un dispositivo supera un umbral predeterminado, por ejemplo, 50/100, entonces al menos un dispositivo de usuario puede considerarse confiable.

El servidor 110 realiza un seguimiento así de una actividad relacionada con una o varias aplicaciones de comunicación soportadas en un lado del dispositivo.

El servidor 110 está adaptado para recibir (desde un dispositivo) una solicitud para obtener un nivel de confianza relacionado con un dispositivo de usuario identificado.

El servidor 110 también está adaptado para enviar (al dispositivo solicitante) el nivel de confianza relacionado con el dispositivo de usuario identificado, como respuesta a la solicitud.

Si el dispositivo de usuario identificado ha enviado previamente al servidor 110, al menos una vez, datos relacionados con una ejecución de aplicación de comunicación, entonces el servidor 110 envía al dispositivo de usuario solicitante el nivel de confianza relacionado con el dispositivo de usuario identificado.

Si el dispositivo de usuario identificado no ha enviado previamente al servidor 110 datos relacionados con una ejecución de aplicación de comunicación, entonces el servidor 110 puede enviar al dispositivo de usuario solicitante

un mensaje del tipo "el dispositivo de usuario identificado no está registrado" o "el nivel de confianza es cero", como un valor por defecto predeterminado.

El PC 114, como terminal de usuario, se conecta, a través de un enlace bidireccional, a la red 18.

En lugar de un PC, el terminal de usuario puede ser cualquier otro dispositivo de usuario que incluya medios para procesar datos, que comprenda o esté conectado a medios de comunicación para intercambiar datos con el exterior, y que comprenda o esté conectado a medios para almacenar datos.

El PC 114 es un ordenador.

El PC 114 se puede comunicar con el servidor 110.

El PC 114 también se puede comunicar con otro dispositivo, como un terminal de usuario, como el teléfono 12.

La Figura 2 representa un modo de realización ejemplar de un flujo de mensajes 20 que implica al teléfono 12, el chip 14, el servidor 110 y el PC 114.

En el ejemplo explicado, se supone que el usuario del teléfono 12 ha recibido un SMS utilizando su teléfono 12 y una aplicación de comunicación de mensajes SMS ejecutada por el teléfono 12, como primer dispositivo de usuario.

El teléfono 12 envía al chip 14 un mensaje 22 que incluye un comando para invocar la aplicación para medir una actividad de comunicación de usuario acompañado de datos relacionados con una ejecución de la aplicación de comunicación de mensajes SMS. Dicho comando permite lanzar una ejecución de la aplicación para medir una actividad de comunicación de usuario. Los datos relacionados con una ejecución de la aplicación de comunicación de mensajes SMS incluyen un identificador, tal como un número de teléfono, relacionado con un dispositivo de envío de mensajes SMS, como segundo dispositivo de usuario.

El chip 14 ejecuta la aplicación para medir una actividad de comunicación de usuario.

El chip 14 recopila los datos relacionados con una ejecución de la aplicación de comunicación de mensajes SMS que el teléfono 12 ha ejecutado.

A continuación, el chip 14 envía al servidor 110 un mensaje 24 que incluye, además de un identificador relacionado con el chip 14, los datos, como un informe del teléfono, relacionados con una ejecución de la aplicación de comunicación de mensajes SMS que el teléfono 12 ha ejecutado.

El servidor 110 determina, en base al informe del teléfono, un nivel de confianza relacionado con el teléfono 12.

El usuario del PC 114 desea comunicarse con el usuario del teléfono 12.

El PC 114, como tercer dispositivo de usuario, envía al servidor 110 una solicitud 26 para obtener un nivel de confianza relacionado con el teléfono 12.

El servidor 110 recupera el nivel de confianza relacionado con el teléfono 12 que se ha determinado y almacenado previamente en el lado del servidor.

El servidor 110 envía al PC 114 un mensaje 28 que incluye, como respuesta a la solicitud, el nivel de confianza relacionado con el teléfono 12.

Una vez que el PC 114 recibe el nivel de confianza relacionado con el teléfono 12, el usuario del PC verifica si una comunicación con el usuario del teléfono es confiable utilizando al menos el nivel de confianza relacionado con el teléfono 12.

Si el nivel de confianza relacionado con el teléfono 12 no supera un umbral predeterminado, entonces el usuario del PC puede cancelar su intención de comunicarse con el usuario del teléfono 12 o definir una tecnología de comunicación de datos que el usuario del PC deberá usar o priorizar, con el fin de comunicarse con el teléfono 12.

De lo contrario, es decir, si el nivel de confianza relacionado con el teléfono 12 supera un umbral predeterminado, el usuario del PC inicia una comunicación con el teléfono 12. A continuación, el PC 114 envía al teléfono 12 un mensaje 210, como un mensaje de tipo de correo electrónico, que incluye, además de un identificador relacionado con el PC 114, un texto.

La invención permite a un usuario de dispositivo que desea comunicarse con otro usuario de dispositivo saber si su potencial interlocutor es (o no) confiable.

Por lo tanto, la invención es conveniente para un usuario de dispositivo, como solicitante de nivel de confianza.

El modo de realización que se acaba de describir no pretende limitar el alcance de la invención en cuestión. Se pueden dar otros modos de realización. Como otro ejemplo de modo de realización, en lugar de intercambiar con un

servidor remoto, los dispositivos de usuario intercambian, a través de un enlace CL, con una entidad local, como un servidor local.

**REIVINDICACIONES**

1. Un procedimiento (20) para acceder a un servicio que proporciona al menos un nivel de confianza de dispositivo de usuario, comprendiendo el procedimiento:

- ejecutar mediante al menos un primer dispositivo de usuario una primera aplicación que se comunica con una segunda aplicación de dispositivo de usuario;

- el primer dispositivo de usuario envía a un servidor remoto (110) datos de actividad de comunicación de usuario (24) relacionados con la ejecución de la primera aplicación, como un informe de primer dispositivo de usuario, incluyendo los datos de actividad de comunicación de usuario relacionados con la ejecución de la primera aplicación información relacionada con un evento entrante o un evento saliente y al menos un atributo relacionado con la ejecución de la primera aplicación, incluyendo el al menos un atributo relacionado con la ejecución de la primera aplicación un tipo de tecnología de comunicación de datos, realizando el servidor remoto un seguimiento de una actividad relacionada con al menos la primera aplicación ejecutada por al menos un primer dispositivo de usuario;

- el servidor remoto determina, en base a al menos el informe de primer dispositivo de usuario, un nivel de confianza relacionado con el primer dispositivo de usuario;

- un tercer dispositivo de usuario (114) envía al servidor remoto una solicitud (26) para obtener un nivel de confianza relacionado con el primer dispositivo de usuario; y

- el servidor remoto envía al tercer dispositivo de usuario, como respuesta a la solicitud, el nivel de confianza (28) relacionado con el primer dispositivo de usuario.

2. Procedimiento, de acuerdo con la reivindicación 1, en el que, para determinar el nivel de confianza relacionado con el primer dispositivo de usuario, el servidor remoto asigna un factor de ponderación predeterminado relacionado con el al menos un atributo relacionado con la ejecución de la primera aplicación.

3. Procedimiento, de acuerdo con la reivindicación 2, en el que el al menos un atributo relacionado con la ejecución de la primera aplicación incluye, además, al menos un elemento del siguiente grupo:

- un tipo de la primera aplicación;

- un tipo de función de usuario del primer dispositivo de usuario;

- una frecuencia de ejecución de la primera aplicación;

- una localización relacionada con el primer dispositivo de usuario cuando el primer dispositivo de usuario ejecuta la primera aplicación; y

- un tipo de primer dispositivo de usuario.

4. Procedimiento, de acuerdo con la reivindicación 1, en el que el tipo de tecnología de comunicación de datos incluye al menos un elemento del siguiente grupo:

- una tecnología de comunicación sin contacto, como una tecnología de comunicación de proximidad;

- una tecnología de comunicación inalámbrica; y

- una tecnología de comunicación de tipo Internet con o sin autenticación de usuario.

5. Procedimiento, de acuerdo con la reivindicación 3, en el que el tipo de la primera aplicación incluye al menos un elemento del siguiente grupo:

- una aplicación segura, autenticando correctamente la aplicación segura al primer usuario de la aplicación; y

- una aplicación no segura.

6. Procedimiento, de acuerdo con la reivindicación 3, en el que el tipo de función de usuario del primer dispositivo de usuario incluye al menos un elemento del siguiente grupo:

- un deudor;

- un acreedor;

- un transmisor de datos;

- una persona que intercambia datos mutuamente; y

- un receptor de datos.

7. Procedimiento, de acuerdo con cualquier reivindicación anterior, en el que, antes de posiblemente enviar datos al primer dispositivo de usuario, el usuario del tercer dispositivo de usuario verifica si una comunicación con el usuario del primer dispositivo de usuario es confiable utilizando al menos el nivel de confianza relacionado con el primer dispositivo de usuario.

8. Procedimiento, de acuerdo con la reivindicación 7, en el que el procedimiento comprende, además, una etapa mediante la cual el usuario del tercer dispositivo inicia, si el nivel de confianza relacionado con el primer dispositivo supera un umbral predeterminado, una comunicación con el primer dispositivo.

9. Procedimiento, de acuerdo con cualquier reivindicación anterior, en el que el primer dispositivo de usuario coopera con un elemento seguro, siendo el elemento seguro un objeto inteligente que protege los datos almacenados.

10. Un servidor (110) para acceder a un servicio que proporciona al menos un nivel de confianza de dispositivo de usuario,

estando configurado el servidor para:

- recibir datos de actividad de comunicación de usuario relacionados con una ejecución de la primera aplicación, como un informe de primer dispositivo de usuario, incluyendo los datos de actividad de comunicación de usuario relacionados con la ejecución de la primera aplicación información relacionada con un evento entrante o un evento saliente y al menos un atributo relacionado con la ejecución de la primera aplicación, incluyendo el al menos un atributo relacionado con la ejecución de la primera aplicación un tipo de tecnología de comunicación de datos, realizando el servidor un seguimiento de una actividad relacionada con al menos la primera aplicación ejecutada por al menos un primer dispositivo de usuario;

- determinar, en base a al menos el informe de primer dispositivo del usuario, un nivel de confianza relacionado con un primer dispositivo del usuario;

- recibir una solicitud (26) para obtener un nivel de confianza relacionado con el primer dispositivo de usuario; y

- enviar, como respuesta a la solicitud, el nivel de confianza (28) relacionado con el primer dispositivo de usuario.

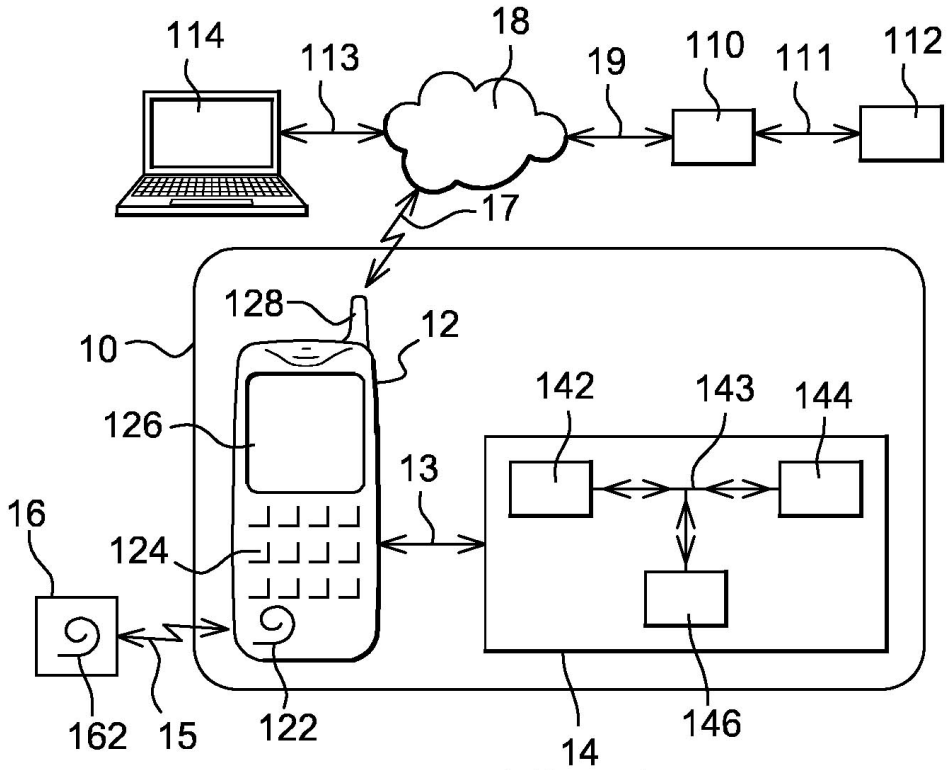
114
113
18
19
110
111
112
17
128
12
10
126
142
143
144
13
16
124
162
15
122
14
146

Fig. 1

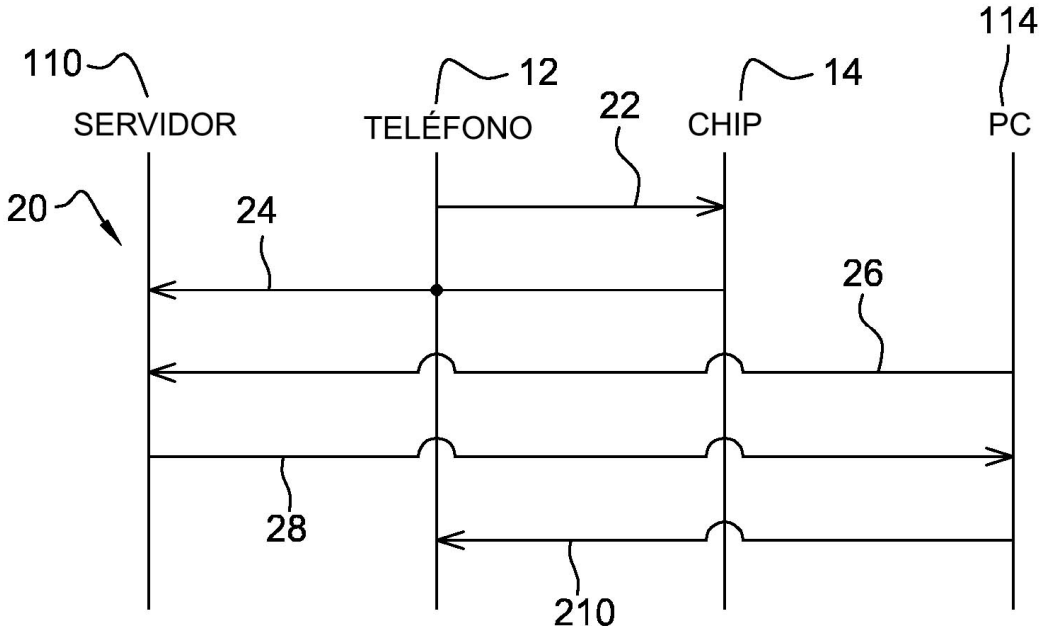
110
SERVIDOR
12
TELÉFONO
22
14
CHIP
114
PC
20
24
26
28
210

Fig. 2