(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 559 617**

(51) Int. CI.:

H04W 12/08 (2009.01)
H04W 8/20 (2009.01)
H04W 88/08 (2009.01)
H04W 84/04 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **30.08.2010 E 10785000 (0)**

(97) Fecha y número de publicación de la concesión europea: **12.08.2015 EP 2474178**

(54) Título: **Procedimiento para la comunicación de datos entre un elemento seguro y un punto de acceso a la red y el elemento seguro correspondiente**

(30) Prioridad:

31.08.2009 EP 09305804

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
15.02.2016

(73) Titular/es:

GEMALTO SA (100.0%)
6, rue de la Verrerie
92190 Meudon, FR

(72) Inventor/es:

PAULIAC, MIREILLE

(74) Agente/Representante:

ISERN CUYAS, María Luisa

DESCRIPCIÓN

Procedimiento para la comunicación de datos entre un elemento seguro y un punto de acceso a la red y el elemento seguro correspondiente.

La invención se refiere, de manera general, a un método para comunicar datos entre un elemento seguro y un punto de acceso a la red.

Por otra parte, la invención también se refiere a un elemento seguro para comunicar datos con un punto de acceso a la red.

En la presente descripción, un elemento seguro es un objeto inteligente con intención de comunicarse con el mundo exterior.

En particular, el elemento seguro puede cooperar con un punto de acceso de red que está o tiene que estar conectado a una red de comunicación.

La presente invención es especialmente, pero no exclusivamente, aplicable a una red de comunicación, como Internet, con la que una Femtocelda, como punto de acceso de red, esta o tiene que estar acoplado. Por otra parte, una tarjeta inteligente o similar, como un Módulo de Alojamiento de Parte (o HPM), como elemento seguro, se acopla o tiene que ser acoplada a la Femtocelda.

Estado de la técnica

Tal como se conoce *per se*, cuando se acoplan entre si, un HPM y una Femtocelda intercambian notablemente datos relativos a sus propias identidades, a saber, una identidad de un HPM y una identidad de una Femtocelda.

Dado que la identidad del HPM y la identidad de la Femtocelda son ambas únicas y especificas a la entidad que identifica, impide que cada una de las dos entidades sea sustituida por otra entidad del mismo tipo, por ejemplo por razones de mantenimiento.

El libro blanco "Implementación de Femtocelda: Libro Blanco de aspectos de Seguridad" publicado en 2008 por la Asociación GSM y la especificación técnica ETSI TS 102 484 v7.4.0 (junio 2009) discuten el uso de mecanismos para conectar de manera segura un token, como por ejemplo una UICC, ana Femtocelda. El informe técnico 3GPP TR 33.820 v8.1.0 (Junio 2009) describe el uso de un módulo seguro para asegurar una estación base doméstica. La estación base registra con un servidor en la red la unión entre su identidad y la identidad del módulo seguro.

Existe la necesidad de proporcionar una solución que permita ser más flexible que la solución conocida mencionada anteriormente mientras la seguridad se siga manteniendo.

Resumen de la invención

La invención propone una solución para satisfacer la necesidad especificada anteriormente en este documento proporcionando un método para comunicar datos entre un elemento seguro y un punto de acceso a la red. El elemento de seguridad, dicho primer elemento seguro, es acoplado con un punto de acceso a la red. El punto de acceso de red esta incluido dentro de una red de comunicación.

Según la invención, al menos un primer elemento seguro y el punto de acceso de red envían, a otro punto de acceso de red y al primer elemento de seguro respectivamente, datos relativos a la identidad de un enlace de comunicación entre el primer elemento seguro y el punto de acceso de red.

El principio de la invención consiste en que el primer elemento de seguro y el punto de acceso de red intercambian datos que identifican un enlace lógico que une el elemento seguro y el punto de acceso a la red, a fin de comunicar.

Por consiguiente, el uso de los datos de identificación de un enlace de comunicación entre el primer elemento seguro y el punto de acceso a la red permite servir de enlace a una de las dos entidades, a saber, ya sea el primer elemento seguro o el punto de acceso a la red, como uno interlocutor, con un representante de la otra entidad, como otro interlocutor.

Por lo tanto, la solución de la invención permite, entre otros, un punto de acceso a la red, para intercambiar con un elemento seguro que sustituye el lugar de un elemento de seguridad anterior, como primer elemento seguro (que ya ha sido acoplado con el punto de acceso de red), mediante el uso de datos relativos a la identidad del enlace de comunicación entre el punto de acceso a la red y el primer elemento seguro.

Naturalmente, la solución de la invención permite, entre otros, un elemento seguro, para intercambiar con un punto de acceso a la red que sustituye el lugar de un punto de acceso a la red anterior (que ya ha sido acoplado con el elemento de seguridad), mediante el uso de datos relativos a la identidad del enlace de comunicación entre el punto de acceso a la red y el elemento seguro.

La solución de la invención es mas flexible que la solución conocida descrita anteriormente en este documento. De hecho, por ejemplo, un elemento de seguro, que toma el lugar de un elemento seguro anterior, es capaz de utilizar los datos relativos a la identidad del enlace de comunicación entre el punto de acceso a la red y el elemento seguro anterior, para comunicarse con el punto de acceso de red mientras sea reconocido como un interlocutor identificado del punto de acceso de red.

La solución de la invención permite que una de las entidades, a saber, o un punto de acceso de red o un elemento seguro, a intercambiar con un representante de la otra entidad que representa a la otra entidad, es decir, el primer elemento seguro o el punto de acceso de red respectivamente, mediante el uso de datos relativos a la identidad del enlace de comunicación entre la entidad y la entidad representada que han sido previamente acoplados entre sí.

Ventajosamente, el primer elemento seguro y el punto de acceso a la red intercambian datos en relación a la identidad del punto de acceso a la red y/o datos relativos a la identidad del primer elemento seguro, de modo que los datos relativos a la identidad del enlace de comunicación entre el punto de acceso a la red y el primer elemento seguro se asocian con los datos relativos a la identidad del punto de acceso a la red y/o los datos relativos a la identidad del primer elemento seguro.

En otras palabras, los datos de identificación del enlace lógico entre el primer elemento seguro y el punto de acceso de red son por lo tanto emparejados con datos relativos a la identidad del punto de acceso de red y/o los datos relativos a la identidad del primer

elemento seguro. Los datos que permiten identificar el enlace logico entre el primer elemento seguro y el punto de acceso a la red y los datos relativos a la identidad del punto de acceso a la red y/o los datos relativos a la identidad del primer elemento seguro son los que se utilizaran para la comunicación entre los dos interlocutores, a saber, un elemento seguro y el punto de acceso a la red.

Una realización de esta invención permite emparejar los datos relativos a una identidad de al menos uno de los interlocutores, a saber, el punto de acceso a la red y/o el primer elemento seguro, y los datos relativos a la identidad de un enlace de comunicación entre los dos interlocutores.

Más exactamente, la solución de la invención permite a un punto de acceso a la red, intercambiar con un elemento seguro que reemplaza a un elemento seguro anterior (que ya se ha unido a un mismo punto de acceso a la red), mediante el uso de pares coincidentes, a saber, datos relativos a la identidad del primer elemento de seguro y los datos relativos a la identidad del enlace de comunicación entre el punto de acceso a la red y el primer elemento seguro.

De acuerdo con un aspecto adicional, la invención es un elemento seguro para comunicar datos con un punto de acceso a la red. El elemento seguro, dicho primer elemento de seguridad, es capaz de ser acoplado con un punto de acceso a la red. El punto de acceso de red esta comprendido dentro de una red de comunicación.

Según la invención, el primer elemento seguro comprende medios para enviar al punto de acceso a la red datos relativos a la identidad de un enlace de comunicación entre el primer elemento seguro y el punto de acceso a la red.

Como elemento seguro, puede ser cualquier dispositivo electrónico que comprenda al menos un microprocesador, como medios de procesamiento de datos, al menos una memoria (o estar conectado a al menos una memoria), y al menos una interfaz/ces de comunicación de entrada/salida. El elemento seguro puede estar constituido por cualquier medio electrónico, como un Módulo Seguro Extraíble (o SRM). Por ejemplo, el elemento seguro se puede incluir dentro de una tarjeta inteligente o un dongle de tipo Bus de Serie Universal (o USB), una Tarjeta Digital Segura (o tarjeta SD), una Tarjeta MultiMedia (o MMC) o un chip para ser fijado a un huésped, como un punto de acceso a la red, preferiblemente de manera desmontable. El elemento seguro puede ser cualquier medio electrónico que puede tener diferentes factores de forma.

Breve descripción de los dibujos

Las características y ventajas adicionales de la invención serán mas claramente comprensibles tras la lectura de la descripción detallada de una realización preferida de la invención, dada a modo de ejemplo indicativo y no limitativo, en conjunción con las siguientes figuras:

La Figura 1 ilustra un diagrama simplificado de una realización de un elemento seguro unido a una estación base domestica, como punto de acceso a la red, para dar un acceso a una red de comunicación de un terminal de usuario, estando dispuesto el elemento de seguro de manera que se permite a otro elemento seguro reemplazar al elemento seguro acoplado, de acuerdo con la invención; y

La Figura 2 representa un ejemplo de un flujo de mensajes particularmente entre el elemento seguro a ser reemplazado de la Figura 1, el punto de acceso a la red, un servidor remoto conectado a la red de comunicación, y el elemento seguro sustituidor.

Descripción detallada

A continuación se considera un caso en el que el método de la invención para la comunicación de datos entre un elemento seguro y un punto de acceso a la red es implementado mediante una Femtocelda, como punto de acceso a la red, y un módulo de identidad del abonado (o SIM) tipo tarjeta inteligente, como HPM, como elemento seguro, acoplado a la Femtocelda.

Naturalmente, la forma de realización descrita a continuación tiene solo fines de ejemplificación y no se considera para reducir el alcance de la presente invención.

Por ejemplo, en lugar de estar constituido por una tarjeta inteligente tipo SIM, el elemento de seguridad puede estar constituido por un dongle (que no necesita ningún lector especifico dentro de un punto de acceso a la red, como equipo anfitrión), una tarjeta inteligente USB, y/o cualquier otro medio electrónico que puede tener diferentes factores de forma. De acuerdo con aun otros ejemplos, el elemento seguro también puede ser un chip fijado, posiblemente de manera extraíble, al punto de acceso de red, o conectado mecánicamente al punto de acceso a la red.

Asimismo, en lugar de estar constituido por una Femtocelda, el punto de acceso a la red puede estar constituida por una picooelda, un Hogar (e) Nodo B, una estación base domestica, y/o una puerta de enlace.

La Figura 1 muestra esquemáticamente una red de comunicación 10, como Internet, a la que un ordenador personal (o PC) 12, como equipo de usuario, se conecta a través de una Femtocelda 14, como punto de acceso de red.

La Femtocelda 14 se acopla con una de tarjeta inteligente tipo SIM 16, como elemento seguro.

Como equipo de usuario, también puede ser cualquier ordenador de mano, como un teléfono móvil, un asistente personal digital (o PDA), un teléfono con protocolo de voz por internet, un netbook, y/o un ordenador portátil móvil. El equipo de usuario también puede incluir un decodificador, un ordenador de sobremesa, un reproductor multimedia, una consola de juegos, y/o un televisor portátil (o TV).

Un usuario accede al PC 12 a través de una interfaz hombre maquina, con el fin de poder explotar, al menos en parte, uno o varios servicios (es decir, la ejecución de una o varias aplicaciones) accesibles a través de la red de comunicación 10. El usuario interactúa con la interfaz hombre maquina y opera el PC 12.

El interfaz hombre maquina puede comprender un teclado 122 para introducir información escrita, una pantalla de visualización 124 para ver información, un altavoz para reproducir una señal de audio y un micrófono para capturar una señal de audio, y/o un puntero para señalar y/o seleccionar la información, como un ratón.

El PC 12 está equipado con un módem y una antena 126 para comunicar datos, a través de un enlace bidireccional 13, a través de la Femtocelda 14, con la red de comunicación 10.

Los datos comunicados se transportan, a través del enlace bidireccional 13, sobre un enlace de radiofrecuencia de corto alcance, como Bluetooth o Wi-Fi, o por medio de un cable.

El PC 12 se usa por un usuario para comunicarse, por ejemplo, o con otro equipo de usuario conectado a la red de comunicación 10 o con una entidad, como una entidad remota 18 incluida en o conectada a la red de comunicación 10.

El usuario del PC puede así beneficiarse de uno o varios servicios ofrecidos por o a través de la red de comunicación 10 a través de la Femtocelda 14.

La Femtocelda 14 puede estar situada dentro de una casa, de un sujeto o de los locales de una empresa.

La Femtocelda 14 puede ser portátil y por lo tanto móvil.

El Femtocell 14 incluye todos los componentes electrónicos (no mostrados), como medios de procesamiento de datos, memorias volátiles y no volátiles, y varias interfaces de comunicación.

Las memorias de la Femtocelda almacenan preferentemente una clave(s), denominada una clave(s) de sesión, que se utiliza para transferir datos de forma confidencial con la tarjeta inteligente tipo SIM 16. La clave(s) de sesión puede incluir una clave de integridad utilizada para verificar que los datos no se han modificado y/o una clave de confidencialidad utilizada para cifrar los datos que se intercambian entre la Femtocelda 14 y la tarjeta inteligente tipo SIM 16.

Las memorias de la Femtocelda pueden almacenar los datos relativos a la identidad de la Femtocelda 14.

Las memorias de la Femtocelda pueden almacenar una clave privada y una clave pública correspondiente.

Como interfaces de comunicación, la Femtocelda 14 incluye una interfaz de comunicación con el PC 12 y otra interfaz de comunicación con la red de comunicación 10.

La Femtocelda 14 puede ser un elemento de comunicación intermediario transmitiendo información enviada desde o el PC 12 o la red de comunicación 10 y destinada o a la red de comunicaciones 10 o al PC 12, respectivamente.

La Femtocelda 14 esta conectada, a través de un enlace bidireccional 15, a la red de comunicación 10, a fin de intercambiar información con la red de comunicación 10 a través de o una línea de alambre o una línea inalámbrica, como una línea de radio-comunicación.

La Femtocelda 14, como una pequeña estación base celular, cuando se acopla con el PC 12 a través de un enlace de radiofrecuencia de corto alcance, tiene una cobertura de radio que permite que al PC 12 acceder a la red de comunicación 10.

La Femtocelda 14 esta conectada, por un lado, al PC 12, y por otro lado, a la red de comunicación 10, y por todavía otro lado, a la tarjeta inteligente tipo SIM de 16, como un elemento seguro separado y destinado asociado con la Femtocelda 14.

Para una mayor simplicidad, la tarjeta inteligente tipo SIM 16 se denominará en adelante tarjeta 16.

La tarjeta 16 esta acoplada, a través de un enlace bidireccional 19, a la Femtocelda 14 permitiendo a la tarjeta 16 y la Femtocelda 14 intercambiar información.

Un enlace de contacto físico constituye el enlace bidireccional 19 entre la tarjeta 16 y la Femtocelda 14.

Según otra forma de realización, la tarjeta 16 y la Femtocelda 14 están conectadas a través de un enlace de radiofrecuencia, tal como un enlace de radiofrecuencia de corto alcance, como un enlace Bluetooth o Wifi.

De acuerdo con aun otra realización, la tarjeta 16 y la Femtocelda 14 están conectadas a través de, por una parte, un enlace de radiofrecuencia, y, por otra parte, un enlace de contacto físico. De acuerdo con esta realización, por ejemplo, la tarjeta 16 recibe datos de la Femtocelda 14 asociada a través del enlace de radiofrecuencia y la tarjeta 16 envía datos a la Femtocelda 14 asociada a través del enlace de contacto físico. Naturalmente, la otra implementación también es posible, a saber, la tarjeta 16 envía datos a la Femtocelda 14 asociada a través del enlace de radiofrecuencia y la tarjeta 16 recibe datos de la Femtocelda 14 asociada a través del enlace de contacto físico.

La tarjeta 16 está acoplada eléctricamente con su Femtocelda 14 asociada para cooperar con ella.

La tarjeta 16 esta o bien fijada o desmontable de la Femtocelda 14 con la que la tarjeta 16 esta asociada.

La tarjeta 16 está, por ejemplo, conectada mecánicamente o directamente a la Femtocelda 14 misma o a una antena o a cualquier otro elemento físico conectado a la Femtocelda 14.

La tarjeta 16 recibe datos del mundo exterior, o desde la Femtocelda 14 o a través de la Femtocelda 14.

En cambio, la tarjeta 16 envía datos al resto del mundo, o a la Femtocelda 14 o a través de la Femtocelda 14.

La tarjeta 16 pertenece a un usuario. El usuario de la tarjeta utiliza la tarjeta 16 para uno o varios servicios. El servicio puede ser proporcionado o por una entidad remota 18 o por otra entidad conectada a la red de comunicación 10, como proveedora de servicios.

La tarjeta 16 se utiliza preferentemente para configurar a la Femtocelda 14 para operar. La tarjeta 16 incorpora al menos un chip.

El chip incluye al menos un microprocesador 162, al menos una memoria 164, y al menos una interfaz entrada/salida (ó I/O) 166 que se comunica con el exterior del chip.

El microprocesador 162 esta unido, a través de un bus de datos bidireccional interno 163, a la memoria 164 y a la interfaz I/O 166.

El microprocesador 162 procesa, controla y comunica datos internamente, a través del bus de datos bidireccional interno 163, con todos los otros diferentes componentes electrónicos incorporados dentro del chip.

El microprocesador 162 puede leer datos de, escribir datos en, y/o ejecutar datos almacenados en la memoria 164. Además, el microprocesador 162 controla el acceso a los datos almacenados dentro de la memoria 164 y comunica los datos, a través de la interfaz I/O 166, con el mundo exterior.

El microprocesador 162 ejecuta el Sistema Operativo (u OS) y al menos una aplicación almacenada en la memoria 164.

Preferiblemente, la memoria 164 almacena una clave(s), denominada clave(s) de sesión, para ser utilizada para comunicar los datos de manera confidencial con la Femtocelda 14.

Se ha de notar que la clave(s) sesión es(son) una clave/s simétrica definitiva y permanente que esta(n) compartida con la Femtocelda 14 (es decir, también almacenada por la Femtocelda 14).

La memoria 164 puede almacenar de forma segura datos relativos a la tarjeta 16 en si, como una clave privada y una clave pública correspondiente. La memoria 164 también puede almacenar de forma segura datos relativos a la Femtocelda 14, tal como un conjunto particular de parámetros y/o variables de acceso, para permitir operar a la Femtocelda 14.

La memoria 164 preferiblemente almacena un certificado raíz proporcionado por una autoridad de certificación, como un operador de red de comunicación o en su nombre, y un algoritmo para verificar que un certificado de Femtocelda ha sido derivado del certificado raíz, con el fin de certificar que su interlocutor, como la Femtocelda 14, es una Femtocelda genuina bajo control de una autoridad de confianza.

La memoria 164 preferiblemente almacena los datos relativos a la Femtocelda 14 a la cual está emparejada, como por ejemplo datos relativos a la identidad de la Femtocelda.

La memoria 164 puede almacenar la clave pública de la Femtocelda 14, como los datos proporcionados por el fabricante de la tarjeta durante su proceso de personalización, la Femtocelda 14, y/o el servidor remoto 18.

La memoria 164 preferiblemente almacena los datos relativos a una dirección del Localizador Uniforme de Recursos (o URL) del servidor remoto 18.

Según una característica importante de la invención, la memoria 164 almacena los datos relativos a la identidad de un enlace de comunicación, como enlace lógico, entre la Femtocelda 14 y la tarjeta 16.

Para una mayor simplicidad, los datos relativos a la identidad de un enlace de comunicación entre la tarjeta 16 y la Femtocelda 14 se denominaran en lo sucesivo identidad del enlace de tarjeta.

La identidad del enlace de tarjeta puede almacenarse en un archivo específico, como un Archivo Elemental para los datos relativos a un enlace con una Femtocelda asociada.

La identidad del enlace de tarjeta puede tener un formato de datos que tiene una longitud de cuatro bytes, como un formato de Identidad de Abonado Móvil temporal.

Según una forma de realización preferida de la invención, la tarjeta 16 esta dispuesta para enviar a la Femtocelda 14 la identidad del enlace de tarjeta.

La identidad del enlace de tarjeta se utiliza, a fin de vincular la tarjeta 16 a la Femtocelda 14.

Tan pronto como la tarjeta 16 esta acoplada físicamente a la Femtocelda 14, la Femtocelda 14 intercambia datos con la tarjeta 16 solo cuando, de antemano, la tarjeta 16 identifica a la Femtocelda 14 enviándole en particular la identidad del enlace de tarjeta En otras palabras, si la identidad del enlace de tarjeta no esta incluida en los datos presentados a la Femtocelda 14, entonces la Femtocelda 14 no reconoce al originador de los datos presentados como la tarjeta 16 permitido y por lo tanto prohíbe comunicar los datos al originador en cuestión.

Por ejemplo, la tarjeta 16 es probable que envíe a la Femtocelda 14 la identidad del enlace de tarjeta, justo después de que la tarjeta 16 ha sido acoplada físicamente a la Femtocelda 14 durante una primera sesión de comunicación. Para realizar dicho envío de la identidad del enlace de tarjeta, la tarjeta de 16 almacena dentro de sus memorias 164 y ejecuta, gracias a su microprocesador 162, una solicitud relativa a una unían a una Femtocelda.

La ejecución de dicha aplicación de unión puede ser activada una vez que un canal seguro haya sido previamente establecido entre la tarjeta 16 y la Femtocelda 14, es decir, la tarjeta 16 y la Femtocelda 14 comparten al menos una clave común que se utilizara para el intercambio de datos de manera segura, a saber, una clave de integridad y/o una clave de confidencialidad, usada como clave(s) de sesión.

La identidad del enlace de tarjeta puede ser generada al azar por un operador de red de comunicación. El operador de red de comunicación puede proporcionar la identidad del enlace de tarjeta al fabricante de la tarjeta, a fin de configurar el enlace lógico entre la tarjeta y la Femtocelda.

La tarjeta 16 es así cargada, durante su fabricación en un proceso de personalización, con la Identidad del enlace de tarjeta.

Según otra forma de realización, la tarjeta 16 ha generado previamente la identidad del enlace de tarjeta mediante el uso de un algoritmo predeterminado almacenado y/o algunos datos predefinidos almacenados.

Preferiblemente, cada vez que la identidad del enlace de tarjeta es intercambiada, la identidad del enlace de tarjeta se cifra con una clave de cifrado y un algoritmo de cifrado almacenado por el emisor y descifrada por el receptor con la correspondiente clave de descifrado y el algoritmo de descifrado almacenado.

Por ejemplo, la tarjeta 16 cifra la identidad del enlace de tarjeta con una clave de sesión compartida con la Femtocelda 14 proporcionada previamente por o generado por la tarjeta 16. Sólo la Femtocelda 14 es capaz de descifrar la identidad del enlace de tarjeta cifrada, ya que la Femtocelda 14 tiene la clave de sesión que es simétrica.

Para una mayor simplicidad, los datos relativos a la identidad de la Femtocelda 14 y los datos relativos a la identidad de la tarjeta se denominaran en lo sucesivo, identidad de la Femtocelda e identidad de la tarjeta respectivamente.

Preferiblemente, la memoria 164 almacena la identidad del enlace de tarjeta asociada a la identidad de la Femtocelda, a fin de ser utilizada como datos para la identificación de la tarjeta 16 como interlocutor de la Femtocelda 14, para definir mejor un enlace de la tarjeta 16 y de la Femtocelda 14.

Dicha asociación o emparejamiento de la identidad del enlace de tarjeta y la identidad de la tarjeta permite caracterizar una relación de la tarjeta 16 con el mundo exterior. El emparejamiento de la identidad del enlace de tarjeta y la identidad de la tarjeta permite identificar la tarjeta y el enlace con la Femtocelda 14.

La identidad del enlace de tarjeta puede ser utilizada para generar al menos una clave, tal como una clave de cifrado (o denominada tecla de confidencialidad) y/o una clave de integridad. En tal caso, la tarjeta 16 genera la clave(s) en base a la identidad del enlace de tarjeta y envía la clave(s) generada a la Femtocelda 14, como una clave(s) secreta para ser compartida.

La tarjeta chip esta preferiblemente adaptada para llevar a cabo procedimientos de acceso, como una autenticación de la Femtocelda 14 asociada y/o cualquier entidad externa, como la entidad remota 18, antes de la comunicación de datos con ella.

La tarjeta 16 es capaz de comunicar datos, a través de la Femtocelda 14 y una o varias entidades (no representadas) como una o varias puertas domésticas, con la entidad remota 18.

En una forma preferida, la tarjeta de memoria 164 tiendas almacena una clave simétrica ya almacenada por la entidad remota 18, que se utiliza para proteger la integridad y cifrar los datos que se enviaran a la entidad remota 18. La clave simétrica puede ser cargada en la tarjeta de memoria 164 durante un proceso de fabricación en una fase de personalización o descargado desde la entidad remota 18.

La entidad remota 18 se incluye dentro de una plataforma OTI (acrónimo de "Over The Internet" (por internet)) almacenada dentro de un elemento de red que esta comprendido dentro de la red de comunicación 10.

Según otra forma de realización, la entidad remota 18 se incluye dentro de una plataforma OTA (acrónimo de "Over The Air" (por el aire)) almacenada dentro de un elemento de red, como el comprendido dentro de la red de comunicación 10.

La entidad remota 18 es un servidor. El servidor remoto 18 gestiona a través de la tarjeta de 16, como un administrador de red remota, una base de datos 110.

El servidor remoto 18 accede a la base de datos de 110.

El servidor remoto 18 incluye un programa de ordenador. Dicho programa informático ofrece especialmente servicios de bases de datos a otros programas de ordenador u ordenadores, entre los cuales hay la tarjeta 16 asociada con la Femtocelda 14. El servidor remoto 18 puede intercambiar datos con la tarjeta 16 a través de la red de comunicación 10.

El papel del servidor remoto 18 es administrar de forma remota la información del usuario en la tarjeta 16 y, a través de la tarjeta 16, la Femtocelda 14 que trasmite la información transportada al equipo de usuario vinculado a la red de comunicación 10.

La base de datos 110 incluye preferiblemente datos relativos a al menos una Femtocelda de la red de comunicación 10 que esta unido a una tarjeta, como un token. Como datos relativos a al menos una Femtocelda de la red de comunicación 10, la base de datos 110 incluye la identidad del enlace de tarjeta preferiblemente asociada con la identidad de la Femtocelda y/o la identidad de la tarjeta relacionada con el par constituido por la tarjeta 16 y la Femtocelda 14.

La base de datos 110 preferiblemente registra la clave simétrica compartida que se utiliza para ser utilizada para comunicarse con la tarjeta 16 y los datos relativos al usuario de la tarjeta.

La Femtocelda 14 puede ser administrada por tanto desde el servidor remoto 18, de una manera interoperable, remota y segura, mediante la interposición de la tarjeta 16 asociada entre la Femtocelda 14 y el servidor remoto 18, la tarjeta 16 puede almacenar datos relativos a la operación de la Femtocelda 14, para evitar que cualquier atacante lea y/o cambie las características del comportamiento de la Femtocelda 14 cuando se comunica con la red de comunicaciones 10 y/o con uno o varios equipos de usuario.

La Figura 2 representa, de acuerdo con una realización particular, especialmente los mensajes 20 que se intercambian entre la tarjeta 16, la Femtocelda 14, el servidor remoto 18 y otra tarjeta 22, como otro token.

La otra tarjeta 22 esta destinada a reemplazar la tarjeta 16, como la entidad en sustitución de la tarjeta 16, como interlocutor único de la Femtocelda 14, como un token.

Según otra realización, en lugar de otra tarjeta 22, la entidad en sustitución de la tarjeta 16 es otro tipo de token y pueden estar constituidos por cualquier otro medio electrónico que pueden tener diferentes factores de forma, mientras incorpora al menos un chip, tal como un dongle USB.

Se supone que, en primer lugar, la tarjeta 16 se ha acoplado físicamente a la Femtocelda 14, y, en segundo lugar, la tarjeta 16 y la Femtocelda 14 han establecido un canal seguro entre ellos.

El canal seguro consiste en utilizar una clave{s), como clave(s) de sesión, compartida entre la tarjeta 16 y la Femtocelda 14, a fin de intercambiar información de manera segura.

De acuerdo con una realización preferida, la clave(s) de sesión resulta de una sesión de protocolo (no representada) entre la tarjeta 16 y la Femtocelda 14. Durante la sesión de protocolo, la tarjeta 16 juega el papel de un cliente, mientras la Femtocelda 14 desempeña el papel de un servidor, la tarjeta 16 autentica preferiblemente la Femtocelda 14, la Femtocelda 14 también puede autenticar la tarjeta 16.

Por ejemplo, como sesión de protocolo, una sesión de Seguridad en la Capa de Transporte (o TLS) tiene lugar tan pronto como la tarjeta 16 se inserta físicamente dentro de la Femtocelda 14, la tarjeta 16 envía los datos aleatorios de tarjeta a la Femtocelda 14 mediante el uso del protocolo TLS como es definido por el Grupo de Trabajo de Ingeniería de Internet (o IETF) Petición de Comentarios (o RFC) 4346.

Entonces, la Femtocelda 14 envía de vuelta a la tarjeta 16 los datos aleatorios de la Femtocelda y preferentemente un certificado relativo a la Femtocelda 14.

Cuando se obtiene el certificado de la Femtocelda, la tarjeta 16 verifica, gracias al certificado raíz, y el algoritmo de verificación de que el certificado de la Femtocelda ha sido derivado del certificado raíz.

La tarjeta 16 determina una clave pre-master mediante el uso de los datos aleatorios de tarjetas, los datos aleatorios de la Femtocelda y un algoritmo predeterminado.

Una vez que la tarjeta 16 ha generado la clave pre-master, la tarjeta 16 envía la clave pre-master a la Femtocelda 14, preferiblemente después de haber sido cifrada con una clave pública relacionada con la Femtocelda 14 (proporcionada previamente a la tarjeta 16).

La Femtocelda 14 computa o determina, mediante el uso de la clave pre-master y los algoritmos predefinidos como TLS_RSA_WITH_AES_128_CBC_SHA (acrónimos de "Transport Layer Security, Rivest Shamir Adleman, Cipher Block Chaining y Secure Hash Algorithm"), una llave maestra y al menos una clave de sesión, a saber, una clave de integridad y/o una clave de confidencialidad.

Asimismo, la tarjeta 16 determina una llave maestra y al menos una clave de sesión, a saber, una clave de integridad y/o una clave de confidencialidad (o denominada clave de cifrado), mediante el uso de la clave de pre-master y los mismos algoritmos predefinidos que los utilizados por la Femtocelda 14.

Una vez que ha tenido lugar la sesión de protocolo, la clave(s) de sesión, utilizada como clave(s) secreta compartida, puede no ser sustituida por otra clave(s) que la(s) establecida a continuación de la sesión de protocolo La clave(s) compartida es(son) para ser utilizada entre la tarjeta 16 y la Femtocelda 14 para cualquier intercambio de información complementaria en un canal seguro.

Durante una sesión de unión de la tarjeta 16 a la Femtocelda 14, la tarjeta 16 envía a la Femtocelda 14 un primer mensaje 24 con la identidad del enlace de tarjeta preferiblemente cifrado mediante el uso de al menos una clave de sesión. La Femtocelda 14 ha, de manera preferente, solicitado previamente a la tarjeta de 16 la identidad del enlace de tarjeta mediante el envío a la tarjeta 16 un comando (no representado) para recuperar la identidad del enlace de tarjeta almacenado en la tarjeta 16.

Si la Femtocelda 14 recibe la identidad del enlace de tarjeta de manera cifrada, entonces la Femtocelda 14 utiliza el correspondiente algoritmo de descifrado y la clave de descifrado para descifrar la identidad del enlace de tarjeta cifrado.

La Femtocelda 14 obtiene la identidad del enlace de tarjeta transparente (es decir, de manera no cifrada). La Femtocelda 14 puede guardar la identidad del enlace de tarjeta de manera cifrada.

La tarjeta 16 y la Femtocelda 14 están así emparejadas.

La tarjeta 16 y la Femtocelda 14 pueden generar una clave (secreta) basada en al menos la identidad del enlace de tarjeta y un algoritmo compartido predeterminado, para ser utilizado por ejemplo como otra clave de sesión.

De acuerdo con una alternativa, solo la tarjeta 16 genera una clave (secreta) basada en al menos la identidad del enlace de tarjeta y un algoritmo predeterminado. Entonces, la tarjeta 16 envía a la Femtocelda 14, dentro del primer mensaje 24 o un mensaje separado, la clave generada que puede ser utilizada entre la tarjeta 16 y la Femtocelda 14, por ejemplo como otra clave de sesión.

La Femtocelda 14 reconoce, como su interlocutor autorizado, solamente una entidad capaz de suministrarle la identidad del enlace de tarjeta.

Preferiblemente, la tarjeta 16 envía a la Femtocelda 14, dentro del primer mensaje 24 o un mensaje separado, la identidad de la tarjeta que esta ligada con la identidad del enlace de tarjeta, preferiblemente de manera cifrada mediante el uso de al menos una clave de sesión.

Para mejorar la seguridad entre la tarjeta 16 y la Femtocelda 14, la tarjeta 16 puede también enviar, dentro del primer mensaje 24 o un mensaje separado, a la Femtocelda 14 otros datos, tales como la identidad de la Femtocelda, preferiblemente de manera cifrada mediante el uso de al menos una clave de sesión, a fin de estar autorizado para comunicarse con la Femtocelda 14, como su tarjeta emparejada.

A continuación, la tarjeta 16 y la Femtocelda 14 registran y comparten los mismos datos relativos a la identidad del enlace que las une y posiblemente, al menos una de sus propias identidades, concretamente la identidad de la tarjeta y/o la identidad de la Femtocelda, para reconocerse una a otra, como un interlocutor de las dos partes acopladas.

La Femtocelda 14 esta adaptada a fin de permitir a su interlocutor, como el token al cual la Femtocelda 14 esta acoplado, para identificar a su interlocutor como la tarjeta 16 o un token que sustituye a la tarjeta 16.

Asimismo, la tarjeta 16 puede ser adaptada a fin de permitir a su interlocutor, como el punto de acceso a la red a la que la tarjeta 16 esta acoplado, para identificar a su interlocutor como la Femtocelda 14 o un punto de acceso a la red que sustituya a la Femtocelda 14.

Más exactamente, si un interlocutor envía a la Femtocelda 14 (o la tarjeta 16), datos de identificación diferentes de la identidad del enlace de tarjeta, entonces la Femtocelda 14 (o la tarjeta 16) prohíbe procesar los datos originados por su interlocutor, como la tarjeta 16 (o como la Femtocelda 14), y envía datos a su interlocutor, como la tarjeta 16. De lo contrario, es decir, si un interlocutor envía a la Femtocelda 14 (o la tarjeta 16), datos de identificación que coincide con la identidad del enlace de tarjeta, entonces la Femtocelda 14 (o la tarjeta 16) es capaz de reconocer a su interlocutor como la tarjeta 16 (o la Femtocelda 14) o un representante de la tarjeta de 16 (o un representante de la Femtocelda 14).

Además, preferiblemente, si un interlocutor envía a la Femtocelda 14 (o la tarjeta 16), datos de autenticación no protegidos por medio de la clave de sesión compartida (es decir, mediante el descifrado con la clave de sesión compartida), entonces la Femtocelda 14 (o la tarjeta 16) prohíbe procesar los datos procedentes de su interlocutor, como la tarjeta 16 (o como la Femtocelda 14), y envía datos a su interlocutor, como la tarjeta 16. De lo contrario, es decir, si un interlocutor envía a la Femtocelda 14 (o la tarjeta 16), la autenticación de datos que están protegidos por medio de la clave de sesión compartida, entonces la Femtocelda 14 (o la tarjeta 16) es capaz de autenticar a su interlocutor como la tarjeta 16 (o la Femtocelda 14) o un representante de la tarjeta 16 (o un representante de la Femtocelda 14).

Una vez que la sesión de unión se ha llevado a cabo, tiene lugar una sesión de actualización del perfil de abonado a la red después de una sesión de comunicación que involucra a la tarjeta 16 y al servidor remoto 18.

Según una característica interesante de la invención, se permite al menos a una entidad remota, como el servidor remoto 18, por la tarjeta 16 acceder a los datos almacenados dentro de la tarjeta 16 y relativos a la Femtocelda 14 a la que la tarjeta 16 está unida.

Una sesión de comunicación entre la tarjeta 16 y el servidor remoto autorizado 18 puede ser abierta desde la tarjeta 16 o el servidor remoto 18.

Para iniciar un acceso remoto a la tarjeta 16, para una administración a distancia (desde la plataforma OTI) de la Femtocelda 14 a través de la tarjeta 16, la plataforma OTI puede enviar a la tarjeta 16, a través de la red de comunicación 10, y vía la Femtocelda 14, un mensaje predeterminado (no representado).

Una vez que el servidor remoto 18, como interlocutor de la tarjeta 16, que es identificado gracias a la dirección URL almacenada en la tarjeta 16, es autenticado preferentemente por la tarjeta 16.

La tarjeta 16 puede abrir una conexión mediante un Protocolo de Control de Transmisión/Protocolo de Internet (o TCP/IP), un Protocolo Independiente Portador (o BIP), o un canal de Servicio de Mensajes Cortos (o SMS) con el servidor remoto 18.

Para abrir la conexión, la tarjeta 16 envía, a través de la Femtocelda 14, al servidor remoto 18, un segundo mensaje 26 incluyendo la identidad del enlace de tarjeta preferiblemente en forma cifrada, por ejemplo mediante el uso de la clave simétrica compartida relacionada con el servidor remoto 18.

Una vez que el servidor remoto 18 ha recibido de la tarjeta 16 la identidad del enlace de tarjeta (preferiblemente después de haber descifrado los correspondiente datos cifrados, por ejemplo mediante el uso de la clave simétrica compartida relacionada con el servidor remoto), el servidor remoto 18 guarda la identidad del enlace de tarjeta dentro de la base de datos 110 o en una memoria externa, como datos relativos a un perfil de abonado a la red, para la referida Femtocelda 14.

Preferiblemente, la tarjeta 16 envía al servidor remoto 18, dentro del segundo mensaje 26 o un mensaje separado, la identidad de la tarjeta que esta ligada con la identidad del enlace de tarjeta y preferentemente cifrada, por ejemplo mediante el uso de la clave simétrica compartida relacionada con el servidor remoto 18.

La tarjeta de 16 puede enviar al servidor remoto 18, en el segundo mensaje 26 o un mensaje separado, la identidad de la Femtocelda que está ligada con la identidad del enlace de tarjeta y preferentemente cifrada, por ejemplo mediante el uso de la clave simétrica compartida relacionada con el servidor remoto 18.

Preferiblemente, la tarjeta 16 envía al servidor remoto 18, dentro del segundo mensaje 26 o un mensaje separado, la clave(s) de sesión que está(n) compartida con la Femtocelda 14 y preferentemente cifrada, por ejemplo mediante el uso de la clave simétrica compartida relacionada con el servidor remoto 18.

La tarjeta de 16 pueden enviar al servidor remoto 18, en el segundo mensaje 26 o un mensaje separado, la clave(s) de sesión que está(n) basada en la identidad del enlace de tarjeta, y que es(son) compartida con la Femtocelda 14 y preferentemente cifrada, por ejemplo mediante el uso de la clave simétrica compartida relacionada con el servidor remoto 18.

El servidor remoto 18 actualiza su base de datos 110 mediante el guardado dentro de la base de datos 110, como el perfil de abonado a la red relacionado con la Femtocelda 14, la identidad del enlace de tarjeta acompañada preferiblemente con la identidad de la Femtocelda, la clave(s) de sesión, y posiblemente la identidad de la tarjeta, y/o la clave(s) de sesión basada en la identidad del enlace de tarjeta.

La tarjeta 16 puede ser reemplazada, de manera temporal o definitiva, por un token de sustitución. El token de sustitución puede ser otra tarjeta 22, otro medio con un chip o un chip diferente del de la tarjeta 16. El token de reemplazo incluye al menos un chip que tiene que almacenar los mismos datos específicos, a saber, al menos la identidad del enlace de tarjeta preferentemente asociado con la identidad de la tarjeta, así como la clave(s) de sesión compartida.

El operador de la red de comunicaciones (o en su nombre) que administra el servidor remoto 18 informa al servidor remoto 18 mediante la introducción de la identidad de una tarjeta de reemplazo 22 en la base de datos 110 dentro del perfil del abonado a la red preferiblemente acompañado con la clave(s) de sesión compartida de la tarjeta reemplazada 16.

La tarjeta de sustitución 22 se carga preferentemente, durante su proceso de fabricación, en una fase de personalización, con, por un lado, datos relativos al perfil del abonado a la red de la referida Femtocelda 14, a saber, la identidad del enlace de tarjeta preferentemente acompañada de la identidad de la tarjeta y/o la identidad de la Femtocelda, la clave(s) de sesión compartida con la Femtocelda 14, y, por otra parte, los datos relativos a una clave(s) simétrica compartida con el servidor remoto 18 que se utiliza para proteger la integridad de los datos a ser intercambiados y/o para cifrar los datos a ser intercambiados de manera confidencial.

De acuerdo con una alternativa, el servidor remoto 18 puede descargar, a través de otro mensaje (no representado), en la tarjeta de reemplazo de 22 identificado dentro de la base de datos 110, preferiblemente de manera cifrada, por ejemplo mediante el uso de la clave simétrica compartida (que se ha cargado, durante su proceso de fabricación, en una fase de personalización), los datos relativos a la referida Femtocelda 14, a saber, la información relativa al perfil de abonado a la red de la referida Femtocelda 14, incluyendo la clave(s) de sesión compartida con la Femtocelda 14.

La tarjeta de sustitución 22 tiene que ser acoplada a la Femtocelda 14 mientras se mantiene la identidad del enlace de tarjeta, como identificador de enlace lógico, que ha sido utilizado por la tarjeta 16 con Femtocelda 14 asociada, durante un acoplamiento anterior de la Femtocelda 14 con la tarjeta 16.

Asimismo, la tarjeta de sustitución 22 tiene que ser acoplada a la Femtocelda 14 mientras se mantiene la clave(s) de sesión compartida que ha(n) sido utilizada por la tarjeta 16 con Femtocelda 14 asociada, durante un acoplamiento anterior de la Femtocelda 14 con la tarjeta 16.

La tarjeta de reemplazo 22 entonces se acopla físicamente a la Femtocelda 14.

La tarjeta de reemplazo de 22 no tiene que establecer ninguna nueva credencial para asegurar el canal con la Femtocelda 14, ya que la tarjeta de reemplazo 22 tiene la clave(s) de sesión compartida originada en el canal seguro establecido entre la tarjeta de reemplazo 16 y la Femtocelda 14.

La tarjeta de sustitución de 22 utiliza así el canal seguro previamente establecido mediante el envío a la Femtocelda 14, a través de un tercer mensaje 28, de la identidad del enlace de tarjeta, que es preferiblemente cifrado usando una clave(s) de sesión compartida que ha(n) sido establecida por la tarjeta reemplazado 16.

Una vez que la tarjeta de reemplazo de 22 ha sido identificada por la Femtocelda 14, ya que la Femtocelda 14 ha recibido los mismos datos específicos esperados, es decir, al menos la identidad del enlace de tarjeta, entonces la Femtocelda 14 autoriza a la tarjeta de reemplazo 22 para jugar el papel de la tarjeta de 16, como el token reemplazado, como su interlocutor privilegiado.

Por lo tanto, la Femtocelda 14 no percibe ninguna diferencia entre la tarjeta de sustitución 22 y la tarjeta de sustitución 16, ya que se utiliza los mismos los datos de identificación procedentes de la tarjeta de sustitución 22, excepto cuando la identidad de la tarjeta es utilizada también por la tarjeta de sustitución 22.

El ejemplo que se acaba de describir no pretende limitar el alcance de la invención en cuestión. Se pueden dar otros ejemplos. Otro ejemplo es en el que una Femtocelda es el interlocutor a reemplazar. De acuerdo con ese otro ejemplo, los datos relativos a una identidad en relación con un enlace de comunicación entre una tarjeta y el enlace de identidad de la denominada Femtocelda (Femtocelda) y, preferentemente, la identidad de la tarjeta se pueden utilizar en lugar de la identidad del enlace de tarjeta y, preferentemente, la identidad de la Femtocelda respectivamente, como datos de identificación que deben tenerse en cuenta, como datos compartidos.

REIVINDICACIONES

1. Un procedimiento (20) para comunicar datos entre un primer elemento seguro (16), estando acoplado dicho primer elemento seguro a un punto de acceso a la red (14), y el punto de acceso a la red, estando el punto de acceso a la red comprendido dentro de una red de comunicación (10),

en el que al menos uno del primer elemento de seguro y el punto de acceso a la red envía (24), al otro del punto de acceso a la red y el primer elemento seguro respectivamente, los datos relativos a la identidad de un enlace de comunicación, como enlace lógico, entre el primer elemento seguro y el punto de acceso de red; y

caracterizado porque el primer elemento seguro envía (26) a un servidor remoto (18) conectado al punto de acceso a la red, datos relativos a al menos una clave de sesión compartida entre el primer elemento seguro y el punto de acceso a la red.

2. Procedimiento de acuerdo con la reivindicación 1, en el que el primer elemento de seguro y el punto de acceso a la red también intercambian datos relativos a una identidad del punto de acceso a la red y/o datos relativos a una identidad del primer elemento seguro, de modo que los datos relativos a la identidad del enlace de comunicación entre el punto de acceso a la red y el primer elemento seguro se asocian con los datos relativos a la identidad del punto de acceso a la red y/o los datos relativos a la identidad del primer elemento seguro.

3. Procedimiento de acuerdo con la reivindicación 1 o 2, en el que el primer elemento seguro envía al servidor remoto los datos relativos a la identidad del enlace de comunicación entre el primer elemento seguro y el punto de acceso a la red.

4. Procedimiento de acuerdo con la reivindicación 3, en el que el servidor remoto almacena y envía (28) a un segundo elemento seguro (22) los datos relativos a la identidad del enlace de comunicación entre el primer elemento seguro y el punto de acceso a la red.

5. Procedimiento de acuerdo con las reivindicación 3 o 4, en el que el servidor remoto almacena y envía a un segundo elemento seguro los datos relativos a:

- una identidad del primer elemento seguro con el que ha sido acoplado el punto de acceso a la red;

- una identidad del punto de acceso a la red con el que ha sido acoplado el primer elemento de seguro; y/o

- al menos una clave de entre una clave de confidencialidad y una clave de integridad almacenada por el primer elemento seguro y el punto de acceso a la red.

6. Procedimiento de acuerdo con cualquiera de las reivindicaciones 3 a 5, en el que el servidor remoto almacena datos relativos a la identidad de un segundo elemento seguro.

7. Procedimiento de acuerdo con cualquiera de las reivindicaciones 4 a 6, en el que el segundo elemento seguro envía (210) al punto de acceso a la red, los datos relativos a la

identidad del enlace de comunicación entre el primer elemento seguro y el punto de acceso a la red.

8. Un primer elemento seguro (16) para la comunicación de datos, siendo capaz dicho primer elemento seguro de ser acoplado a un punto de acceso a la red (14), estando comprendido el citado punto de acceso a la red dentro de una red de comunicaciones (10),

En el que el primer elemento seguro es capaz de:

- enviar (24) al punto de acceso a la red datos relativos a la identidad de un enlace de comunicación, como enlace lógico, entre el primer elemento seguro y el punto de acceso a la red, estando conectado un servidor remoto al punto de acceso a la red;

caracterizado porque el primer elemento seguro está adaptado para:

- enviar (26) al servidor remoto (18) los datos relativos a al menos una clave de sesión compartida entre el primer elemento seguro y el punto de acceso a la red.

9. Un elemento seguro de acuerdo con la reivindicación 8, en el que el primer elemento seguro comprende medios para enviar a un servidor remoto los datos relativos a la identidad de un enlace de comunicación entre el primer elemento seguro y el punto de acceso a la red.

10. Un elemento seguro de acuerdo con la reivindicación 8 o 9, en el que el primer elemento seguro comprende medios para enviar al punto de acceso a la red os datos relativos a la identidad del primer elemento seguro.

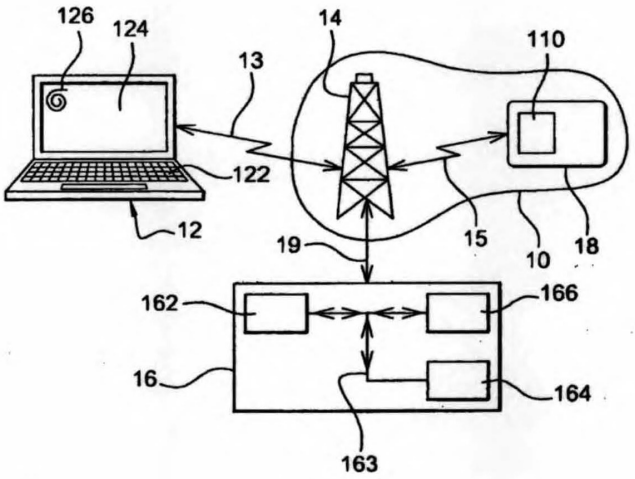
126
124
14
110
13
122
12
19
15
10
18
162
166
16
164
163

Fig. 1

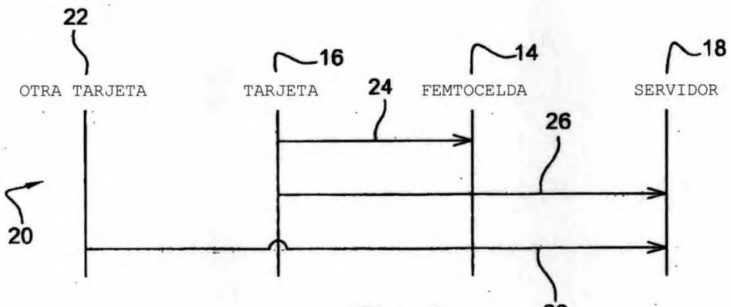
22
16
14
18
OTRA TARJETA
TARJETA
24
FEMTOCELDA
SERVIDOR
26
20
28

Fig. 2