(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 699 925**

(51) Int. CI.:

H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **07.12.2015 E 15198303 (8)**

(97) Fecha y número de publicación de la concesión europea: **29.08.2018 EP 3032799**

(54) Título: **Procedimiento de autenticación de un usuario, servidor, terminal de comunicaciones y programas correspondientes**

(30) Prioridad:

12.12.2014 FR 1462382

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
13.02.2019

(73) Titular/es:

INGENICO GROUP (100.0%)
28-32 Boulevard de Grenelle
75015 Paris, FR

(72) Inventor/es:

NACCACHE, DAVID

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Procedimiento de autenticación de un usuario, servidor, terminal de comunicaciones y programas correspondientes

1. Campo de la invención

La invención se refiere al campo de la autenticación de usuarios. Más particularmente, la invención se refiere al campo de la autenticación de usuarios con servicios tales como servicios de acceso a información confidencial o incluso servicios de pago.

2. Técnica anterior

La autenticación de usuarios con servicios y especialmente con servicios en línea es problemática. Como regla general, realizar una autenticación de un usuario requiere, por un lado, una entrada de un identificador (del tipo de inicio de sesión) que permita comunicar la identidad del usuario y una entrada de contraseña (o un código de identificación personal) que permita garantizar que la persona sea realmente la persona que dice ser. En realidad, dichos sistemas garantizan una sola cosa: que la persona que se identifica con un identificador (que no es necesariamente el suyo) también tiene la contraseña que corresponde a este identificador. En ningún momento, con estos sistemas, se garantiza que el usuario sea realmente el que dice ser.

Además, además de un identificador, el usuario a menudo debe recordar una contraseña, lo que plantea un problema. De hecho, para evitar tener demasiadas contraseñas, muchos usuarios usan la misma contraseña para todos los servicios (servicios de correo electrónico, servicios de almacenamiento de archivos en un espacio de almacenamiento común, acceso a cuentas bancarias, etc.). Otros usuarios, incluso menos cautelosos, usan contraseñas simples, tipo "azerty" o "password". En este segundo caso de figura, es evidente que dicha contraseña no sirve prácticamente para nada.

Paradójicamente, los usuarios exigen dispositivos de autenticación exitosos porque no quieren que su correo electrónico o sus cuentas bancarias se hackeen. Sin embargo, al ser refractario o desconocer las problemáticas de robo de identidad o piratería, el usuario suele ser el enlace débil en un sistema de autenticación.

Se han propuesto muchas técnicas para superar los problemas de autenticación y los problemas de usabilidad de la autenticación. Entre ellos, podemos mencionar el uso de tarjetas inteligentes, en algunos casos, o el uso de "tokens" (dispositivos físicos para generar contraseñas aleatorias). Sin embargo, aunque funcionan bien desde el punto de vista de la fuerza de la autenticación, estos sistemas son relativamente menos fáciles de usar: para el usuario, siempre es necesario introducir un identificador y/o una contraseña, la mayoría de las veces, es necesario introducir estas dos informaciones.

Existen sistemas que permiten introducir una sola contraseña: la entrada del identificador se realiza por otros medios. El sistema más conocido para hacer esto es la "cookie", este pequeño archivo de texto guardado por un navegador web cuando un servidor web lo solicita: en este sistema, el usuario solo introduce su identificador una vez (durante la primera conexión al servicio). Posteriormente, durante las conexiones posteriores al servicio, solo se debe introducir la contraseña. Existen otros sistemas (que permiten introducir una sola contraseña: se trata, por ejemplo, de sistemas basadosen el uso de tarjetas inteligentes o terminales de comunicación (incluidos los datos de identificación) que permiten pasar a introducir un identificador. Dichos sistemas, sin embargo, necesitan incluso introducir una contraseña. Esto también es preferente porque es incómodo permitir que un dispositivo, tan seguro como es, autentifique completamente un usuario. El documento US2010/058064, del 4 de marzo de 2010 (2010-03-04) describe un procedimiento que permite a un usuario que desee acceder a un servicio remoto desde un terminal de comunicaciones no seguro realizar el procedimiento de autenticación requerido por este servicio remoto desde un terminal de confianza en su poder. Esto no impide que la problemática general de la autenticación plantee un problema importante de facilidad de uso, que es perjudicial para la seguridad del sistema.

3. Sumario de la invención

La técnica propuesta no plantea estos problemas de la técnica anterior. Más particularmente, la divulgación se refiere a un procedimiento de autenticación de un terminal de comunicaciones que pertenece a un usuario después de un servidor de autenticación conectado a un terminal de pasarela a través de una red de comunicaciones. Dicho procedimiento comprende, dentro del servidor de autenticación:

- una etapa de obtención, desde dicho terminal de pasarela, un dato representativo de una identidad del usuario;

- una etapa de configuración, por dicho servidor de autenticación de un enlace de transmisión de datos entre dicho servidor de autenticación y dicho terminal de comunicaciones del usuario, a través de una interfaz de transmisión de datos predeterminada de dicho terminal de pasarela y en función de dicho dato representativo de una identidad del usuario;

- una etapa de transmisión, mediante el servidor de autenticación, al terminal de comunicaciones del usuario, de un dato de verificación de autenticación cifrado, a través del enlace de transmisión de datos;

- una etapa de recepción, por el servidor de autenticación, desde el terminal de comunicaciones del usuario, de un dato de contra-verificación de autenticación cifrado;

- una etapa de suministro de una aserción de autenticación de usuario cuando el dato de contra-verificación de autenticación coincide con dicho dato de verificación.

De acuerdo con una característica particular, la interfaz de transmisión de datos predeterminada de dicho terminal de pasarela es una interfaz Bluetooth y en que el enlace de transmisión de datos entre el servidor de autenticación y el terminal de comunicaciones del usuario es un enlace Bluetooth virtual.

De acuerdo con una característica particular, antes de la etapa de obtener un dato representativo de una identidad del usuario, dicho procedimiento comprende:

- una etapa de recepción, procedente de dicho terminal de pasarela o de un servidor conectado a dicho servidor de autenticación, de una solicitud de conexión; y

- una etapa de transmisión, a dicho terminal de pasarela, de una solicitud de identificación en función de dicha solicitud de conexión.

De acuerdo con una característica particular, la etapa de configuración, por dicho servidor de autenticación de un enlace de transmisión de datos entre dicho servidor de autenticación y dicho terminal de comunicaciones del usuario, comprende:

- una etapa de obtención, de al menos un dato representativo de al menos un parámetro de conexión al terminal de comunicaciones por medio de dicho dato representativo de dicha identidad del usuario;

- una etapa de transmisión de dicha al menos una parte de datos representativos de un parámetro de conexión a dicho terminal de pasarela;

De acuerdo con una característica particular, dicho al menos un parámetro de conexión comprende al menos un dato necesario para la construcción del enlace entre el terminal de comunicaciones del usuario y el terminal de pasarela.

De acuerdo con una característica particular, dicho al menos un parámetro de conexión comprende al menos un dato perteneciente al grupo que comprende:

- una dirección física del terminal de comunicaciones del usuario;

- un dato de tipo código de emparejamiento;

- un dato de tipo contraseña.

En otro modo de realización, la técnica también se refiere a un servidor de autenticación de un terminal de comunicaciones perteneciente a un usuario después de un servidor de autenticación conectado a un terminal de pasarela a través de una red de comunicaciones. Dicho servidor incluye:

- un módulo configurado para obtener, desde dicho terminal de pasarela, un dato representativo de una identidad del usuario;

- un módulo configurado para configurar un enlace de transmisión de datos entre dicho servidor de autenticación y dicho terminal de comunicaciones de usuario, a través de una interfaz de transmisión de datos predeterminada de dicho terminal de pasarela y de acuerdo con dicho elemento de datos representativo de una identidad del usuario;

- un módulo configurado para transmitir un dato de verificación de autenticación cifrado al terminal de comunicaciones del usuario a través del enlace de transmisión de datos;

- un módulo configurado para recibir, procedente del terminal de comunicaciones del usuario, un dato de contra-verificación de autenticación cifrado;

- un módulo configurado para suministrar una aserción de autenticación del usuario cuando el dato de contra-verificación de autenticación corresponde a dicho dato de verificación.

De acuerdo con otro aspecto, la técnica propuesta se refiere igualmente a un terminal intermedio y a un terminal de comunicaciones de usuario. Cada uno de estos dos terminales comprende medios para implementar las etapas del procedimiento que lo concierne y, en particular, medios para crear una conexión inalámbrica con el fin de montar un enlace seguro entre el terminal de comunicaciones y el servidor de autenticación. Los procesos implementados, que se describen a continuación, son complementarios al proceso de autenticación en el servidor de autenticación.

De acuerdo con una implementación preferida, las diversas etapas de los procedimientos de acuerdo con la invención se implementan mediante uno o más programas o programas informáticos, que comprenden instrucciones de software destinadas a ejecutarse por un procesador de datos de un módulo de relé de acuerdo con la invención y estando previsto para controlar la ejecución de las diferentes etapas de los procedimientos.

Por consiguiente, la invención también está dirigida a un programa, susceptible de ejecutarse por un ordenador o por un procesador de datos, comprendiendo este programa instrucciones para controlar la ejecución de las etapas de un procedimiento como se mencionó anteriormente.

Este programa puede usar cualquier lenguaje de programación, y puede ser en forma de código fuente, código objeto o código intermedio entre el código fuente y el código objeto, tal como en una forma parcialmente compilada, o en cualquier otra forma deseable.

La invención también se refiere a un soporte de datos legible por un procesador de datos, y que comprende instrucciones de un programa tal como se mencionó anteriormente.

El soporte de información puede ser cualquier entidad o dispositivo capaz de almacenar el programa. Por ejemplo, el medio puede comprender medios de almacenamiento, tales como una ROM, por ejemplo, un CD ROM o una ROM de circuito microelectrónico, o incluso un medio de grabación magnética, por ejemplo un disquete (disco flexible) o un disco duro.

Por otro lado, el soporte de información puede ser un soporte transmisible tal como una señal eléctrica u óptica, que puede transportarse a través de un cable eléctrico u óptico, por radio o por otros medios. El programa de acuerdo con la invención se puede descargar en particular en una red de tipo Internet.

Alternativamente, el soporte de información puede ser un circuito integrado en el que se incorpore el programa, estando el circuito adaptado para ejecutarse o para usarse en la ejecución del procedimiento en cuestión.

De acuerdo con un modo de realización, la invención se implementa por medio de componentes de software y/o hardware. En este contexto, el término "módulo" puede corresponder en este documento a un componente de software, un componente de hardware o un conjunto de componentes de hardware y software.

Un componente de software corresponde a uno o más programas informáticos, uno o más subprogramas de un programa, o más generalmente a cualquier elemento de un programa o software capaz de implementar una función o un conjunto de funciones, como se describe a continuación para el módulo en cuestión. Dicho componente de software se ejecuta por un procesador de datos de una entidad física (terminal, servidor, pasarela, enrutador, etc.) y es susceptible de acceder a los recursos de hardware de esta entidad física (memorias, medios de grabación, bus de comunicación, tarjetas de comunicación, tarjetas electrónicas de entrada/salida, interfaces de usuario, etc.).

De la misma manera, un componente de hardware corresponde a cualquier elemento de un conjunto de hardware (o hardware) capaz de implementar una función o un conjunto de funciones, como se describe a continuación para el módulo en cuestión. Puede tratarse de un componente de hardware programable o con un procesador integrado para ejecutar software, por ejemplo, un circuito integrado, una tarjeta inteligente, una tarjeta de memoria, una tarjeta electrónica para ejecutar un firmware, etc.

Cada componente del sistema descrito anteriormente implementa naturalmente sus propios módulos de software.

Los diversos modos de realización mencionados anteriormente se pueden combinar entre sí para la implementación de la invención.

4. Dibujos

Otras características y ventajas de la invención aparecerán más claramente al leer la siguiente descripción de un modo de realización preferido, dada como un ejemplo simple ilustrativo y no limitativo, y los dibujos adjuntos, entre los cuales:

- la Figura 1 muestra un sinóptico de la técnica propuesta, desde un punto de vista general, que involucra a los terminales y al servidor de autenticación;

- la Figura 2 muestra un servidor de autenticación de acuerdo con la técnica propuesta;

- la Figura 3 describe un terminal de comunicaciones de usuario capaz de implementar la técnica propuesta;

- la Figura 4 describe un terminal de pasarela capaz de implementar la técnica propuesta.

5. Descripción

5.1. Recordatorio del principio general

Como se expuso anteriormente, el principio general de la técnica propuesta reside en el uso de un terminal de comunicaciones, específico para el usuario, para realizar una operación de autenticación desde otro terminal. Más particularmente, el principio consiste en iniciar un emparejamiento entre un terminal de comunicaciones del usuario (por ejemplo, un teléfono) y un servidor de autenticación a *través de* otro terminal de comunicaciones del usuario (por ejemplo, un ordenador). De acuerdo con la técnica propuesta, este emparejamiento se realiza usando medios de comunicación específicos para un primer terminal de comunicaciones (por ejemplo, un ordenador personal o una tablet o una consola de juegos, etc.), llamado terminal de comunicaciones de pasarela, desde el cual se inicia la autenticación. En otras palabras, un segundo terminal de comunicaciones del usuario implementa parte del procedimiento de autenticación (el que consiste, por ejemplo, en introducir la contraseña para acceder a un servicio) usando medios de comunicación de terceros, que están disponibles desde un primer terminal de comunicaciones, dicho terminal de pasarela. El terminal de pasarela, como se prevé en el presente documento, no es un enrutador, un punto de acceso o una caja de operador: estos equipos no permiten que el usuario se conecte a un servicio (por ejemplo, para una página web de comercio electrónico, una página de acceso restringido) e introduzca los datos de inicio de sesión del nombre de usuario/contraseña. El terminal de pasarela es el terminal desde el cual se inicia el procedimiento de autenticación. El terminal de pasarela es el iniciador del procedimiento de autenticación.

Más particularmente, en al menos un modo de realización de la técnica propuesta, el segundo terminal de comunicaciones del usuario implementa una interfaz de comunicación inalámbrica (*Bluetooth,* WiFi) para conectarse con el servidor de autenticación usando el terminal de comunicaciones de pasarela. Se trata de algún modo de una especie de interfaz de interferencia. Además, combinada con este uso de una interfaz de terminal de comunicaciones de pasarela, la técnica propuesta comprende además el establecimiento de un enlace de transmisión de datos específico entre el servidor de autenticación y el segundo terminal de comunicaciones.

La técnica propuesta se describe en relación con la Figura 1.

Un usuario (UTI) desea conectarse a un servicio en línea, tal como un servicio bancario. Para hacer esto, desde un ordenador o tableta (TCP#1), dicho terminal de pasarela, abre (50) una aplicación (por ejemplo, un navegador) (esta etapa es opcional) y requiere (100) una conexión para la autenticación a un servidor de autenticación (ServA) (o al servidor del proveedor de servicios al que está conectado el usuario a través del terminal de pasarela [el servidor del proveedor de servicios luego transmite esta solicitud al servidor de autenticación]). La solicitud de conexión, transmitida por el terminal de pasarela o por un servidor al que está conectado el terminal de pasarela, permite al servidor de autenticación (ServA) iniciar la transacción y determinar a qué dispositivo debe responder.

El servidor de autenticación (ServA) transmite (110) al terminal de pasarela (TCP#1) una solicitud de identificación (ReqId). El contenido de esta solicitud de identificación se explicita más adelante. La solicitud de identificación es opcional. Sirve, por ejemplo, para redirigir el terminal de pasarela hacia una conexión segura.

El terminal de pasarela (TCP#1) usa (120) el contenido de esta solicitud de identificación (Reqld), para solicitar (121) al usuario una entrada de un identificador (Id_U) (tal como una dirección de correo electrónico). Cuando la entrada se realiza y valida por el usuario, este identificador (Id_U) se transmite (122) por el terminal de pasarela (TCP#1) al servidor de autenticación (ServA).

Al recibir este identificador (Id_U), el servidor de autenticación (ServA) busca (130), dentro de una base de datos (BddPm), al menos una parte de datos representativos de un parámetro de conexión (PmC) a un terminal de comunicaciones (TCP#2). Estos datos representativos de un parámetro de conexión (PmC) se obtienen al proporcionar el identificador (Id_U) del usuario. Estos datos luego se transmiten (140) al terminal de pasarela (TCP#1) posiblemente acompañados por una instrucción para construir una conexión virtual entre el servidor (ServA) y el terminal de comunicaciones (TCP#2).

El terminal de pasarela (TCP#1) recibe este parámetro de conexión (PmC) y gracias al que crea una instancia (150) de un enlace de transmisión/recepción de datos con el terminal de comunicaciones del usuario (TCP#2). Por ejemplo, cuando se usa una interfaz *Bluetooth*, el terminal de comunicaciones del usuario (TCP#2) recibe (160) del terminal de pasarela (TCP#1), una solicitud de emparejamiento (ReqAp) a dicho terminal de pasarela (TCP#1), dicha solicitud de emparejamiento (ReqAp) comprende datos que permiten un emparejamiento con el terminal de comunicaciones del usuario (TCP#2) a través de la interfaz *Bluetooth.* El contenido de la solicitud de emparejamiento se explicita más adelante. Por ejemplo, cuando se usa una interfaz WiFi, el terminal de comunicaciones del usuario (TCP#2) recibe (160), del terminal de pasarela (TCP#1), una solicitud de emparejamiento (ReqAp) a dicho terminal de pasarela (TCP#1), comprendiendo dicha solicitud de emparejamiento (ReqAp) datos que permiten un emparejamiento con el terminal de comunicaciones del usuario (TCP#2) a través de la interfaz WiFi. La interfaz de transmisión inalámbrica entre el terminal de comunicaciones del usuario (TCP#2) y el terminal de pasarela (TCP#1) es relativamente poco importante, aunque la interfaz *Bluetooth* es una solución preferida porque, en términos de implementación, la interfaz *Bluetooth* facilita la conexión de un terminal tipo teléfono inteligente con un terminal de pasarela de tipo PC o tableta: no es necesario montar una red ad-hoc con la interfaz *Bluetooth.*

Después de la recepción (160) de la solicitud de emparejamiento (ReqAp), y tras el establecimiento del emparejamiento con el terminal de pasarela (TCP#1), el terminal de comunicaciones del usuario (TCP#2), busca (180), dentro de una base de datos interna y/o un espacio de almacenamiento seguro del terminal, un dato de identificación (Id_S) del servidor de autenticación (ServA). Compara (190) estos datos de identificación (almacenados dentro del terminal) con los datos de identificación recibidos del servidor. El dato de identificación recibido del servidor están presentes dentro de la solicitud de emparejamiento (ReqAp) o se transmiten (170) por el servidor después del emparejamiento. Esto hace posible garantizar que el terminal de comunicaciones del usuario no sufra un intento de hackeo por parte de un servidor de terceros o del terminal de comunicaciones de pasarela fraudulentas.

Cuando el terminal de comunicaciones del usuario (TCP#2) ha verificado la identidad del servidor de autenticación (ServA), el terminal de comunicaciones del usuario (TCP#2) transmite (200) al servidor de autenticación (ServA) un dato de autenticación (DataAuth).

Se ofrecen dos posibilidades:

- o bien el terminal de comunicaciones del usuario (TCP#2) transmite estos datos a través de una conexión de datos complementaria disponible para el terminal de comunicaciones (por ejemplo, una conexión 3G o 4G) contactando directamente con el servidor de autenticación;

- o bien el terminal de comunicaciones del usuario (TCP#2) transmite estos datos a través de la conexión realizada con el terminal de pasarela (TCP#1). En este segundo caso de figura, al menos un mensaje se transmite "sobre" el protocolo usado para la conexión (por ejemplo, "sobre *Bluetooth* " o "sobre WiFi") al servidor de autenticación. De manera complementaria, este mensaje se transmite cifrado usando una clave privada del terminal de comunicaciones del usuario (TCP#2).

Al recibir este dato de identificación (DataAuth), el servidor de autenticación (ServA) asigna (210) una aserción de autenticación al usuario (y, por lo tanto, al terminal de pasarela (TCP#1)).

De este modo, el procedimiento descrito permite no tener que introducir una contraseña para poder autenticar a un usuario con un servicio. El único dato requerido para realizar la autenticación es un inicio de sesión. Por supuesto, como con cualquier procedimiento de autenticación, el procedimiento propuesto requiere un registro previo con el servidor de autenticación. Este registro previo se detalla más adelante.

El procedimiento descrito se basa en la transmisión de varias solicitudes. Sólo se mencionaron las solicitudes específicas de la técnica descrita.

La solicitud de identificación (ReqId) comprende, por ejemplo, una dirección (por ejemplo, del tipo de URL), a la que el terminal de pasarela (TCP#1) debe conectarse antes de proporcionar cualquier información. Los parámetros de conexión (PmC) comprenden, por ejemplo, los datos necesarios para la construcción del enlace físico entre el terminal de comunicaciones del usuario (TCP#2) y el terminal de pasarela (TCP#1). Entre estos datos, se encuentra en particular la dirección física (dirección MAC) del terminal de comunicaciones del usuario y posiblemente un tipo de dato de emparejamiento o contraseña WiFi. Este dato se transmite al terminal de comunicaciones del usuario para permitir una conexión directa entre el terminal de comunicaciones del usuario y el terminal de pasarela. En el caso de un código de emparejamiento *Bluetooth,* se trata del código de emparejamiento del servidor de autenticación.

La solicitud de emparejamiento (ReqAp) comprende al menos un dato de identificación del servidor de autenticación (ServA). Estos datos de identificación (DIdServA) permiten que el terminal de comunicaciones del usuario (TCP#2) verifique la identidad del dispositivo que intente transmitir una solicitud de autenticación. De acuerdo con un modo de realización particular, estos datos de identificación corresponden a una dirección (por ejemplo, una dirección MAC) del servidor de autenticación (ServA) cifrada usando una clave pública del terminal de comunicaciones del usuario (TCP#2). La manera en que esta información se pone a disposición del servidor de autenticación (ServA) se describe más adelante. De acuerdo con un modo de realización particular, estos datos de identificación corresponden a una dirección (por ejemplo, una dirección MAC) del servidor de autenticación (ServA) cifrada utilizando una clave privada del servidor de autenticación (ServA). Por cierto, también se incluyen otros datos de identificación, para aumentar la seguridad.

En otras palabras, en lugar de realizar un emparejamiento con el terminal de pasarela, la invención permite un emparejamiento directamente con el servidor de autenticación usando un enlace de datos "transportado" a través del terminal de pasarela. En el caso del *Bluetooth,* por ejemplo, el terminal de comunicaciones del usuario se empareja a través de *Bluetooth* con el servidor de autenticación (y no con el terminal de pasarela). Se establece una conexión *Bluetooth* no entre el terminal del usuario y el terminal de pasarela (desde el cual el usuario está tratando de conectarse), sino entre el servidor de autenticación y el terminal del usuario a través del terminal de pasarela. Por lo tanto, el servidor de autenticación puede retransmitir al terminal de pasarela, a través de un enlace TCP/IP, paquetes *Bluetooth*, paquetes que se envían (tal como están) por el terminal de pasarela (que no puede comprender su contenido) lo que hace posible crear un tipo de canal *Bluetooth* virtual de larga distancia entre el terminal del usuario y el servidor de autenticación.

En realidad, por lo tanto, hay un emparejamiento de *Bluetooth* emparejado con, por un lado, un enlace físico de Bluetooth que se establece entre el terminal de comunicaciones del usuario y el terminal de pasarela y un enlace funcional *Bluetooth* que se establece entre el terminal de comunicaciones del usuario y el servidor de autenticación.

Para que el sistema sea funcional, el terminal de pasarela simplemente implementa una traslación de direccionamiento Bluetooth para enrutar correctamente los datos que pasan entre el terminal de comunicaciones del usuario y el servidor de autenticación. Por lo tanto, técnicamente, el servidor de autenticación implementa una pila funcional correspondiente al protocolo usado (por ejemplo, una pila funcional *Bluetooth* o una pila funcional WiFi) mientras que el terminal de pasarela implementa naturalmente al menos una pila de hardware correspondiente al protocolo usado (por ejemplo: ejemplo, una pila de hardware *Bluetooth* o una pila funcional WiFi). Naturalmente, el terminal de pasarela también implementa una pila funcional correspondiente al protocolo usado, que está controlado por un módulo dedicado. Más específicamente, en el caso de una implementación a través de *Bluetooth,* se puede montar una red de tipo "scatternet" con el terminal de pasarela actuando como un "nodo esclavo" mientras que el terminal de comunicaciones del usuario y el servidor juegan ambos un rol de "nodo maestro".

Por supuesto, de esta presentación queda claro que la técnica propuesta tiene dos componentes distintos: por un lado, un procedimiento implementado en el lado del servidor de autenticación y, por otro lado, un procedimiento implementado por el cliente terminal del usuario, estos dos procedimientos tienen en común el uso de un terminal de pasarela para montar un enlace de transmisión de datos inalámbrico de larga distancia. Dado que solo una pequeña parte del enlace es verdaderamente inalámbrica, este enlace inalámbrico puede describirse como virtual.

5.2. Configuración de una conexión virtual

Para montar una conexión entre el terminal de comunicaciones del usuario y el servidor de autenticación, es ventajoso que el terminal de comunicaciones del usuario y el servidor de autenticación tengan equipos que permitan el reconocimiento mutuo seguro. Más particularmente, es deseable que el terminal de comunicaciones del usuario tenga al menos una clave pública del servidor de autenticación y que el servidor de autenticación tenga al menos una clave pública del terminal de comunicaciones del servidor de autenticación de usuario. La posesión de estos dos hardware permitirá a estas dos entidades intercambiar datos de forma segura. Además de estos dos elementos, también es deseable que el terminal de comunicaciones tenga datos que permitan la identificación del servidor de autenticación y que el servidor de autenticación tenga datos que permitan identificar el terminal de comunicaciones del usuario.

Para ello, se podrían implementar varios procedimientos. Sin embargo, los inventores tuvieron la idea de usar un procedimiento de conexión directa del terminal de comunicaciones del usuario con el servidor de autenticación. Esta conexión directa se implementa desde una aplicación específica, que el usuario se ha encargado de instalar de antemano en su terminal de comunicaciones, o mediante un servicio web accesible desde el terminal de comunicaciones del usuario. Independientemente del medio empleado para establecer esta conexión, incluye las etapas necesarias para el intercambio de los datos mencionados anteriormente (o los datos que permitan obtener los datos mencionados anteriormente), datos que se utilizan posteriormente en el contexto de solicitudes de identificación y emparejamientos.

Más particularmente, en al menos un modo de realización, las claves públicas que se ponen a disposición del terminal de comunicaciones del usuario, por una parte, y el servidor de autenticación, por otra parte, se utilizan para derivar las claves de sesión de la implementación de uno o más desafíos durante un procedimiento de intercambio mutuo de claves.

Este procedimiento de creación de claves de sesión se implementa posteriormente o concomitantemente con el establecimiento del enlace entre el terminal de comunicaciones del usuario y el servidor de autenticación. Para la implementación de este enlace, el terminal de pasarela se usa solo para la transmisión de datos en el canal físico (capa física de transmisión de datos).

De manera complementaria, durante el establecimiento del enlace entre el terminal de comunicaciones del usuario y el servidor de autenticación, es decir, subsiguiente a la transmisión por el terminal de pasarela de los datos de identificación del usuario (identificador, dirección de correo electrónico, etc.), el servidor de autenticación implementa una etapa preparatoria durante la cual garantiza que el terminal de pasarela sea compatible con el procedimiento de autenticación del servidor de autenticación de la técnica propuesta. Para ello, el servidor:

- verifica que el terminal de pasarela tenga las interfaces físicas necesarias para la implementación del enlace;
- verifica que puede solicitar, al terminal de pasarela, una implementación de estas interfaces;

Cuando el terminal de pasarela no permite que el servidor de autenticación realice estas verificaciones (por razones de seguridad, por ejemplo), el servidor de autenticación requiere que el terminal de pasarela instale una aplicación, que se denomina, por comodidad, aplicación de pasarela. Esta aplicación de pasarela puede, por ejemplo, tener la forma de un módulo de software instalado en el navegador web usado en el terminal de pasarela. Esta aplicación de pasarela también puede tener la forma de una aplicación ejecutable directamente por el sistema operativo del terminal de pasarela (por ejemplo, Windows™ o IOS™ o Android™). Cuando se instala esta aplicación de pasarela, es esta aplicación la que realiza las operaciones de verificación mencionadas en nombre del servidor de autenticación.

Además, cuando esta aplicación se instala dentro del terminal de pasarela, es esta aplicación la que se encarga de la función de retransmisión de la transmisión de datos entre el terminal de comunicaciones del usuario y el servidor de autenticación. Para hacer esto, la aplicación que se suministra por el propio servidor de autenticación comprende materiales criptográficos suficientes para garantizar la confidencialidad de los datos transmitidos.

5.3. Descripción de un caso de uso

En este caso de uso, el empleo de la técnica propuesta se presenta para llevar a cabo una transacción financiera en una página de comercio electrónico. En este caso de uso, el terminal de comunicaciones del usuario es un teléfono inteligente (en el que se instala una aplicación específica), el terminal de pasarela es un ordenador portátil tipo PC y el servidor de autenticación es un servidor bancario (se puede tratar de un servidor bancario físico o lógico destinado únicamente para la implementación de autenticaciones). Una cuarta entidad interviene en este caso de uso: es el servidor de la página de comercio electrónico que se usa para realizar las compras por parte del usuario.

Antes de la implementación de la técnica propuesta, se supone que el usuario ha seleccionado, en la página web en cuestión, al menos un artículo que ha colocado en un carrito de compras y que desea efectuar una transacción de pago para liquidar sus compras.

Cuando el usuario desea realizar el pago, se implementa el siguiente procedimiento, de acuerdo con las etapas descritas anteriormente:

- el usuario introduce, desde el terminal de pasarela, a un campo previsto para este propósito, desde la página web del comerciante al que está conectado, el identificador necesario para su autenticación en la página en cuestión;

- la página web transmite al servidor bancario el identificador introducido por el usuario y realiza una redirección (redireccionamiento HTTP, por ejemplo) a una página de pago del servidor bancario. A partir de este momento, el terminal de pasarela se conecta al servidor bancario.

- el servidor bancario, junto con el terminal de pasarela, monta una conexión Bluetooth con el teléfono inteligente del usuario, como se expuso anteriormente. Cuando el teléfono inteligente del usuario no está presente (es decir, no se encuentra en un área de transmisión/recepción de datos Bluetooth con respecto al terminal de pasarela, el procedimiento de autenticación no puede continuar y se cancela la transacción. Esto permite garantizar que el usuario esté presente. Es por esta razón que se prefiere la elección de la tecnología Bluetooth, debido a su rango de transmisión relativamente bajo (unos pocos metros). Si el teléfono inteligente está presente, entonces se implementa una aplicación específica de la técnica descrita en el teléfono inteligente para permitir que se autentique con el servidor bancario. Esta aplicación implementa las etapas del procedimiento que deben ejecutar el terminal de comunicaciones del usuario. Opcionalmente, para aumentar la seguridad, la aplicación requiere que el usuario introduzca un código de identificación personal (que puede ser por ejemplo, pero no necesariamente, un código de identificación personal idéntico al usado para la tarjeta bancaria del usuario). Cuando se implementa dicha opción, la transacción se cancela si este código de identificación personal no se introduce en un tiempo predeterminado después de la solicitud de entrada transmitida por la aplicación al usuario.

- cuando se realiza la autenticación del teléfono inteligente del usuario, el servidor bancario considera que el usuario es la persona que afirma ser e implementa la transacción financiera.

Accesoriamente, en la medida en que el servidor de autenticación tenga garantizada la autenticidad de la identidad del usuario, no requiere la introducción de información en la tarjeta de crédito: usa la tarjeta de crédito asociada a la cuenta del usuario por su banco, cuando esta información esté disponible, por supuesto. Opcionalmente, la página de comercio electrónico transmite la información relacionada con la tarjeta bancaria que se usará directamente en el servidor bancario, junto con la redirección al servidor bancario. Por lo tanto, el usuario no está obligado a introducir los datos de su tarjeta de crédito cada vez que quiera realizar un pago.

Por lo tanto, además del hecho de que ya no es necesario introducir una contraseña para acceder a un servicio, tampoco es necesario introducir información bancaria para acceder a este servicio.

5.4. Otras características y beneficios

En relación con la Figura 2, se describe un servidor de autenticación implementado para autenticar a un usuario desde un terminal de comunicaciones (TCP#2) diferente de un terminal de comunicaciones inicial, de acuerdo con el procedimiento descrito anteriormente.

Por ejemplo, el servidor de autenticación comprende una memoria 31 que consiste en una memoria intermedia, una unidad de procesamiento 32, equipada, por ejemplo, con un microprocesador y controlada por el programa informático 33, que implementa un procedimiento de autenticación de un terminal de comunicaciones. En la inicialización, las instrucciones de código del programa informático 33 se cargan, por ejemplo, en una memoria antes de ejecutarse por el procesador de la unidad de procesamiento 32. La unidad de procesamiento 32 recibe como entrada al menos una parte de datos representativos de un identificador de un identificador de usuario, desde el terminal de pasarela. El microprocesador de la unidad de procesamiento 32 implementa las etapas del procedimiento de autenticación, de

acuerdo con las instrucciones del programa informático 33 para obtener los datos necesarios para el establecimiento de un enlace virtual entre el terminal del usuario y el servidor de autenticación para intercambiar, con el terminal de comunicaciones del usuario, los datos necesarios para su autenticación.

Para esto, el servidor de autenticación comprende, además de la memoria intermedia 31, medios de comunicación, tales como módulos de comunicación de red, medios de transmisión de datos y posiblemente un procesador de cifrado.

Estos medios pueden tener la forma de un procesador particular implementado dentro del dispositivo, siendo dicho procesador un procesador seguro. De acuerdo con un modo de realización particular, este dispositivo implementa una aplicación o módulo particular que se encarga de realizar el procesamiento, esta aplicación o módulo se proporciona, por ejemplo, por el fabricante del procesador en cuestión para permitir el uso de dicho procesador. Para ello, el procesador comprende medios de identificación únicos. Estos medios de identificación únicos hacen posible garantizar la autenticidad del procesador y/o el servidor de autenticación.

Además, el servidor de autenticación comprende además medios para buscar, dentro de una base de datos, datos de conexión al terminal del usuario así como medios para obtener claves de cifrado, por ejemplo claves asimétricas (claves públicas/claves privadas) que sirven para generar datos de verificación y los datos de contra-verificación durante la autenticación. Estos medios también se presentan como interfaces de comunicación para el intercambio de datos en redes de comunicación, medios de interrogación y actualización de bases de datos,...

Con referencia a la Figura 3, se describe un terminal de comunicaciones de un usuario (TCP#2) implementado para autenticar un usuario que se ha identificado previamente a través de un terminal de pasarela (TPC#1), de acuerdo con el procedimiento descrito anteriormente.

Por ejemplo, el terminal de comunicaciones de un usuario comprende una memoria 41 constituida por una memoria intermedia, una unidad de procesamiento 42, equipada, por ejemplo, con un microprocesador, y controlada por el programa informático 43, que implementa una procedimiento de autenticación.

En la inicialización, las instrucciones de código del programa informático 43 se cargan, por ejemplo, en una memoria antes de ejecutarse por el procesador de la unidad de procesamiento 42. La unidad de procesamiento 42 recibe como entrada al menos un dato representativo de un comando de emparejamiento con el terminal de pasarela (TCP#1). El microprocesador de la unidad de procesamiento 42 implementa las etapas del procedimiento de autenticación, de acuerdo con las instrucciones del programa informático 43 para recibir una solicitud de emparejamiento desde el terminal de pasarela (TCP#1), buscar, dentro de una base de datos interna y/o un espacio de almacenamiento seguro, datos de identificación del servidor de autenticación (ServA); comparar estos datos de identificación con los datos de identificación recibidos del servidor (por ejemplo, dentro de la solicitud de emparejamiento); transmitir datos de autenticación (Authentication DataAuth) al servidor de autenticación (ServA).

Para esto, el terminal de comunicaciones de un usuario comprende, además de la memoria intermedia 41, medios de comunicación, tales como módulos de comunicación de red, medios de transmisión de datos y posiblemente un procesador de cifrado.

Estos medios pueden tener la forma de un procesador particular implementado dentro del dispositivo, siendo dicho procesador un procesador seguro. De acuerdo con un modo de realización particular, este terminal de comunicaciones de un usuario implementa una aplicación o módulo particular que está encargado de la realización de los intercambios, proporcionándose esta aplicación o módulo, por ejemplo, por el fabricante del procesador en cuestión (implementado dentro del terminal) para permitir el uso de dicho procesador. Para ello, el procesador comprende medios de identificación únicos. Estos medios de identificación únicos permiten garantizar la autenticidad del procesador y/o el terminal de comunicaciones.

Además, el terminal de comunicaciones de un usuario comprende además los medios para almacenar un dato de referencia de la identidad del servidor y medios para almacenar claves de cifrado. Estos medios también se presentan como interfaces de comunicación para el intercambio de datos en redes de comunicación, medios de interrogación y actualización de bases de datos, ...

En relación con la Figura 4, se describe un terminal de comunicaciones de pasarela (TCP#1) implementado para autenticar un usuario desde un terminal de comunicaciones (TPC # 1), de acuerdo con el procedimiento descrito anteriormente.

Por ejemplo, el terminal de comunicaciones de un usuario comprende una memoria 51 constituida por una memoria intermedia, una unidad de procesamiento 52, equipada, por ejemplo, con un microprocesador, y controlada por el programa informático 53, que implementa una procedimiento de autenticación.

En la inicialización, las instrucciones de código del programa informático 53 se cargan, por ejemplo, en una memoria antes de ejecutarse por el procesador de la unidad de procesamiento 52. La unidad de procesamiento 52 recibe como entrada al menos una parte de datos representativos de la identidad de un usuario (por ejemplo, un inicio de sesión). El microprocesador de la unidad de procesamiento 52 implementa las etapas del procedimiento de autenticación, de acuerdo con las instrucciones del programa informático 53 para transmitir esta identidad a un servidor de autenticación;

recibir de este servidor de autenticación un parámetro de conexión al terminal de comunicaciones del usuario (TCP#2), montar una conexión entre él y el terminal de comunicaciones del usuario (TCP#2) utilizando el parámetro recibido previamente transmitiendo una solicitud de emparejamiento al terminal y posiblemente una identidad del servidor de autenticación y recibir, en la parte del servidor de autenticación, una aserción de autenticación cuando la autenticación entre el terminal de comunicaciones (TCP#2) y el servidor de autenticación funcionó sin problemas.

Para esto, el terminal de comunicaciones de un usuario comprende, además de la memoria intermedia 51, medios de comunicación, tales como módulos de comunicación de red, medios de transmisión de datos y posiblemente un procesador de cifrado.

Estos medios pueden tener la forma de un procesador particular implementado dentro del dispositivo, siendo dicho procesador un procesador seguro. De acuerdo con un modo de realización particular, este terminal de comunicaciones de un usuario implementa un módulo particular que se encarga de realizar los intercambios (en particular los intercambios necesarios para la implementación de la conexión virtual entre el terminal de comunicaciones TCP#2 y el servidor de autenticación ServA), este módulo, por ejemplo, lo proporciona el fabricante del procesador en cuestión para permitir el uso de dicho procesador. Para ello, el procesador comprende medios de identificación únicos. Estos medios de identificación únicos permiten garantizar la autenticidad del procesador y/o del terminal de comunicaciones de la pasarela para fines de no falsificación.

Además, el terminal de comunicaciones de un usuario comprende además los medios para almacenar un dato de referencia de la identidad del servidor y medios para almacenar claves de cifrado. Estos medios también se presentan como interfaces de comunicación para el intercambio de datos en redes de comunicación, medios de interrogación y actualización de bases de datos, ...

REIVINDICACIONES

1. Procedimiento de autenticación de un terminal de comunicaciones (TCP#2) que pertenece a un usuario después de un servidor de autenticación (ServA) conectado a un terminal de pasarela (TCP#1) a través de una red de comunicaciones, **caracterizado por que** comprende, dentro del servidor de autenticación:

- una etapa de obtención, desde dicho terminal de pasarela (TCP#1), de un dato representativo de una identidad del usuario;

- una etapa de configuración, por dicho servidor de autenticación (ServA), de un enlace de transmisión de datos entre dicho servidor de autenticación (ServA) y dicho terminal de comunicaciones del usuario (TCP#2), a través de una interfaz de transmisión de datos predeterminada de dicho terminal de pasarela (TCP#1) y en función de dicho dato representativo de una identidad del usuario;

- una etapa de transmisión, por el servidor de autenticación (ServA), al terminal de comunicaciones del usuario (TCP#2) de los datos de verificación de autenticación cifrados, a través del enlace de transmisión de datos;

- una etapa de recepción, por el servidor de autenticación (ServA), desde el terminal de comunicaciones del usuario (TCP#2), de un dato de contra-verificación de autenticación cifrado;

- una etapa de suministro de una aserción de autenticación de usuario cuando los datos de contra-verificación de autenticación corresponde a dichos datos de verificación.

2. Procedimiento de autenticación de acuerdo con la reivindicación 1, **caracterizado por que** la interfaz de transmisión de datos predeterminada de dicho terminal de pasarela (TCP#1) es una interfaz Bluetooth y **por que** el enlace de transmisión de datos entre el servidor de autenticación (ServA) y el terminal de comunicaciones del usuario (TCP#2) es un enlace de Bluetooth virtual.

3. Procedimiento de acuerdo con la reivindicación 1, **caracterizado por que**, antes de la etapa de obtención de un dato representativo de una identidad del usuario, dicho procedimiento comprende:

- una etapa de recepción, desde dicho terminal de pasarela o desde un servidor conectado a dicho servidor de autenticación, una solicitud de conexión; y

- una etapa de transmisión, a dicho terminal de pasarela (TCP#1), una solicitud de identificación en función de dicha solicitud de conexión.

4. Procedimiento de acuerdo con la reivindicación 1, **caracterizado por** la etapa de configuración, por dicho servidor de autenticación (ServA) de un enlace de transmisión de datos entre dicho servidor de autenticación (ServA) y dicho terminal de comunicaciones de usuario (TCP#2) comprende:

- una etapa de obtención, de al menos un dato representativo de al menos un parámetro de conexión (PmC) desde el terminal de comunicaciones (TCP#2) utilizando dicho dato representativo de la identidad de dicho usuario;

una etapa de transmitir dicha al menos un dato representativo de un parámetro de conexión (PmC) a dicho terminal de pasarela (TCP#1);

5. Procedimiento de acuerdo con la reivindicación 4, **caracterizado por que** dicho al menos un parámetro de conexión (PmC) comprende al menos un dato necesario para la construcción del enlace entre el terminal de comunicaciones del usuario (TCP#2) y el terminal de pasarela (TCP#1).

6. Procedimiento de acuerdo con la reivindicación 4, **caracterizado por que** dicho al menos un parámetro de conexión (PmC) comprende al menos un dato que pertenece al grupo que comprende:

- una dirección física del terminal de comunicaciones del usuario (TCP#2);

- un dato de tipo de código de emparejamiento;

- un dato de tipo contraseña.

7. Servidor de autenticación de un terminal de comunicaciones (TCP#2) perteneciente a un usuario después de un servidor de autenticación (ServA) conectado a un terminal de pasarela (TCP#1) a través de una red de comunicaciones, servidor **caracterizado por que** comprende:

- un módulo configurado para obtener, desde dicho terminal de pasarela (TCP#1), datos representativos de una identidad del usuario;

- un módulo configurado para configurar un enlace de transmisión de datos entre dicho servidor de autenticación (ServA) y dicho terminal de comunicaciones de usuario (TCP#2), a través de una interfaz de transmisión de datos

predeterminada de dicho terminal de pasarela (TCP#1) y en función de dicho dato representativo de la identidad del usuario;

- un módulo configurado para transmitir un dato de verificación de autenticación cifrado al terminal de comunicaciones del usuario (TCP#2) a través del enlace de transmisión de datos;

- un módulo configurado para recibir, procedente del terminal de comunicaciones del usuario (TCP#2), un dato de contra-verificación de autenticación cifrado;

- un módulo configurado para suministrar una aserción de autenticación de usuario cuando el dato de contra-verificación de autenticación corresponde a dicho dato de verificación.

8. Producto de programa informático descargable desde una red de comunicaciones y/o almacenado en un medio legible por ordenador y/o ejecutable por un microprocesador, **caracterizado por que** comprende instrucciones de código de programa para ejecutar un procedimiento de autenticación de acuerdo con la reivindicación 1, cuando se ejecuta en un ordenador.

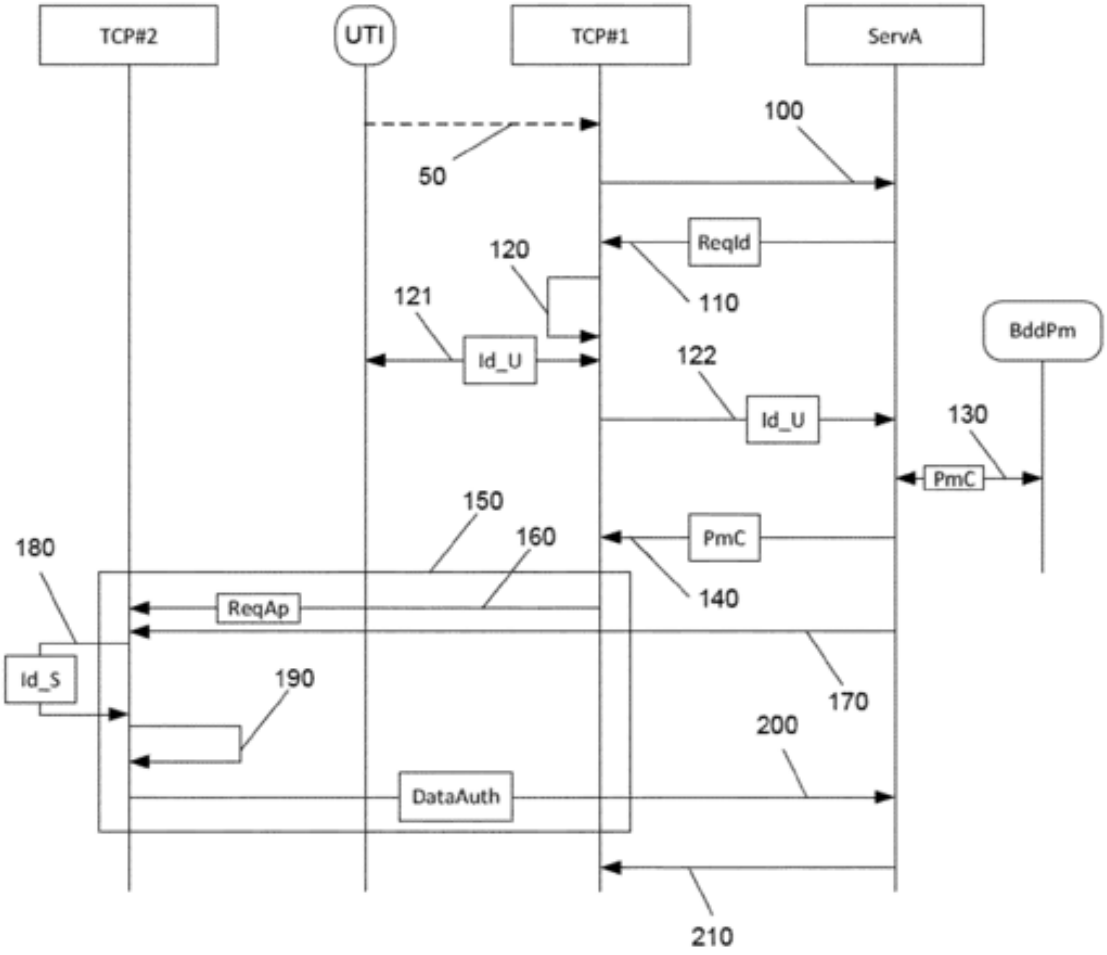
TCP#2
UTI
TCP#1
ServA
BddPm
100
50
ReqId
120
110
121
Id_U
122
Id_U
130
PmC
150
160
PmC
180
140
ReqAp
170
Id_S
190
200
DataAuth
210

Figura 1

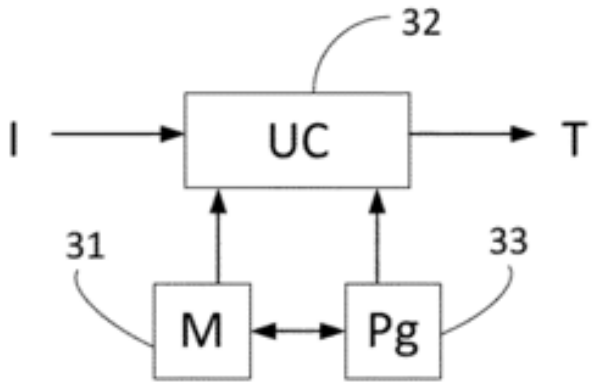

Figura 2

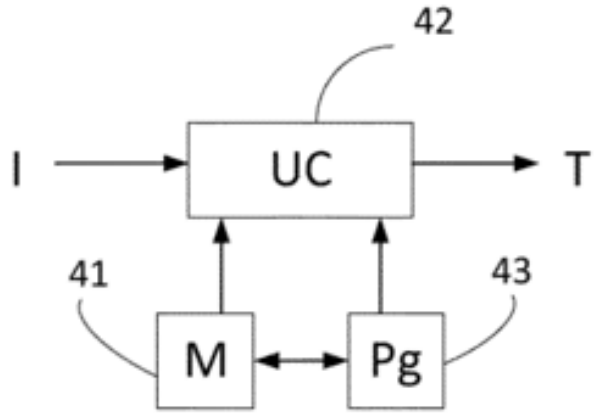

Figura 3

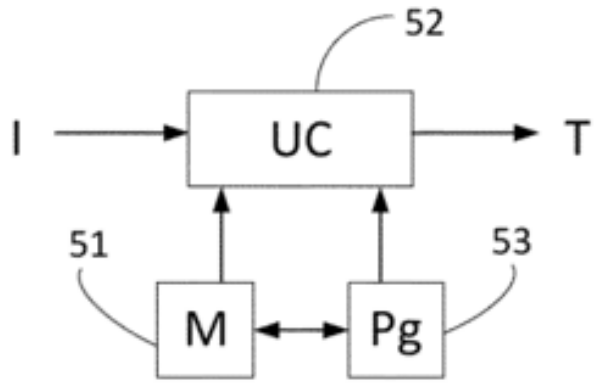

Figura 4