(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 906 174**

(51) Int. CI.:

H04B 5/00 (2006.01)
H04W 12/06 (2011.01)
H04W 12/08 (2011.01)
H04W 4/80 (2008.01)
G06Q 20/32 (2012.01)
G06Q 20/34 (2012.01)
H04K 1/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **19.07.2017 E 17182194 (5)**

(97) Fecha y número de publicación de la concesión europea: **15.12.2021 EP 3273398**

(54) Título: **Método de tratamiento de datos mediante un dispositivo electrónico de adquisición de datos, dispositivo y programa correspondiente**

(30) Prioridad:

21.07.2016 FR 1656960

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
13.04.2022

(73) Titular/es:

BANKS AND ACQUIRERS INTERNATIONAL HOLDING (100.0%)
28-32 boulevard de Grenelle
75015 Paris, FR

(72) Inventor/es:

BEUNARDEAU, MARC

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Método de tratamiento de datos mediante un dispositivo electrónico de adquisición de datos, dispositivo y programa correspondiente

1. Campo

La presente técnica hace referencia al campo de la protección de los datos intercambiados a través de un protocolo de transmisión de datos sin contacto. Más particularmente, la técnica hace referencia a la transmisión de datos de tipo NFC, en la que se efectúa una transmisión entre un primer dispositivo y un segundo dispositivo separados por una distancia del orden de una decena de centímetros como máximo. La técnica no se aplica y no tiene por objetivo aplicarse en el ámbito de las técnicas de transmisión de datos de tipo WiFi, WiMax, LTE, cuyas tecnologías de transmisión son diferentes.

2. Técnica anterior

Muchos dispositivos de la vida cotidiana son capaces de comunicarse e intercambiar datos entre ellos. Una parte cada vez mayor de dispositivos utilizan protocolos de intercambio de datos denominados "de campo cercano" o incluso NFC para este fin. A veces, estas técnicas de transmisión de datos también se denominan RFID. Esta denominación no es correcta, ya que NFC significa comunicación de campo cercano, mientras que RFID hace referencia a medios de identificación por radiofrecuencia. Ambas utilizan señales de radio para todo tipo de fines de identificación y seguimiento, y a veces sustituyen a los códigos de barras. Ambas utilizan medios de transmisión de datos de corto alcance.

Sin embargo, la utilización de este tipo de tecnología sigue suscitando temores y dudas por parte de los usuarios. Muchas personas tienen poca o ninguna confianza en estas tecnologías, más particularmente cuando se trata de utilizarlas con fines de tratamiento de datos personales y/o confidenciales. Este es el caso, por ejemplo, del pago. Hace relativamente poco tiempo que han aparecido los dispositivos de pago sin contacto. Se trata, por ejemplo, de las tarjetas de pago sin contacto, que permiten efectuar un pago (cuyo importe normalmente está limitado) oponiendo (o acercando) la tarjeta a un terminal de pago compatible. También se trata de terminales de comunicación, que también incorporan "chips" sin contacto: estos chips (también denominados "chips sin contacto") proporcionan capacidades de intercambio de datos a los terminales de comunicación, capacidades que se pueden utilizar para efectuar pagos, aproximadamente como si el terminal de comunicación imitara el comportamiento de una tarjeta de pago sin contacto.

Muchos rumores, a menudo infundados, sugieren que una comunicación o un pago sin contacto son poco seguros. También se suele decir que los propios dispositivos son poco seguros y que es posible recuperar datos contenidos en estos dispositivos sin que el usuario se entere. Aunque estos rumores a menudo son infundados, existen sin embargo riesgos durante la transmisión de datos entre los dispositivos implicados (tarjetas, terminal de comunicación, terminal de pago) y especialmente durante la transmisión de datos de pago. Los riesgos, sin embargo, no provienen de la tecnología utilizada, per se, sino generalmente del propio usuario. De este modo, por ejemplo, en el caso de un terminal de comunicación que utilice la interfaz NFC para efectuar un pago, es posible que el usuario haya instalado una aplicación poco segura, o incluso una aplicación maliciosa, cuyo objetivo sea utilizar los datos de pago con fines fraudulentos. La situación es la misma del lado del terminal del comerciante.

Por ejemplo, en el caso de una tarjeta inteligente que comunica sus credenciales bancarias a un teléfono inteligente a través de NFC, se plantea el siguiente problema. Los datos (transmitidos por la tarjeta) no están cifrados (debido a la falta de capacidad de cálculo por parte de la tarjeta). De este modo, la seguridad en el caso de un pago sin contacto convencional (tarjeta sin contacto-terminal de pago) se basa en el hecho de que sólo el terminal de pago "escucha" los datos transmitidos (en el campo cercano) por la tarjeta; se supone que el terminal se comporta de manera honesta (está protegido y certificado): en estos escenarios convencionales, el terminal de pago que trata la transacción de pago es un dispositivo protegido. Ha sido diseñado para evitar las intrusiones, tanto de hardware como de software.

En el caso de un teléfono inteligente es difícil evitar que se instale una aplicación maliciosa. Por ejemplo, cualquiera puede ofrecer una aplicación en una tienda de aplicaciones, y aunque el código de las aplicaciones esté verificado, se ha demostrado que es posible ofrecer aplicaciones maliciosas. Una vez disponible en la tienda de aplicaciones, la aplicación maliciosa puede ser descargada por todos los usuarios de teléfonos inteligentes compatibles con dicha aplicación.

La aplicación maliciosa tiene entonces acceso a los comandos propuestos por parte del sistema operativo del terminal de comunicación. Sin embargo, el sistema operativo de los terminales de comunicación proporciona una interfaz de aplicación (API) que permite tener acceso a los datos de la aplicación transmitidos a través de la interfaz NFC del terminal de comunicación. La aplicación maliciosa puede entonces detectar el inicio de una transmisión de datos por vía NFC y obtener fácilmente los datos procedentes de una tarjeta de pago sin contacto (por ejemplo, el PAN de la tarjeta, el nombre del titular, etc.).

Este también puede ser el caso del terminal de comunicación que transmite los datos de pago sin contacto a un terminal de pago: el caso en concreto es el mismo que el anterior, excepto que la aplicación maliciosa intercepta los datos durante su transmisión (del terminal de comunicación al terminal de pago) y no durante la recepción de estos datos por parte del terminal de comunicación. Para este propósito, la aplicación maliciosa se aprovecha del hecho de que sólo hay un chip NFC en el terminal de comunicación y de que los datos "sensibles" procedentes de, por ejemplo, un entorno de confianza (protegido) del terminal de comunicación siguen pasando por la interfaz NFC y a través de la interfaz "estándar" de la aplicación.

El documento WO 2004/012352 A1 hace referencia a un teléfono móvil 550, equipado con un módulo de lectura/escritura de tarjetas inteligentes sin contacto 500 conectado al teléfono 550 por medio de un alojamiento para tarjetas 552 para un módulo de identificación de abonado (universal) (SIM/USIM).

Por lo tanto, es necesario proporcionar una solución a este problema que ofrezca una protección para los datos transmitidos al terminal de pago (o terminal de comunicación), incluso en el caso de un intercambio de datos no protegido.

3. Resumen de la invención

La técnica propuesta no plantea estos problemas de la técnica anterior. Más concretamente, proporciona una solución sencilla al problema identificado anteriormente. Esta solución es totalmente compatible con los dispositivos y protocolos existentes. La solución, a diferencia de las soluciones que se podrían proponer, no se basa en el cifrado de datos, sino en una modificación más sutil de la transmisión/recepción de datos entre el medio de pago (tarjeta de pago sin contacto, terminal de comunicación) y el dispositivo de pago (terminal de comunicación, terminal de pago).

Más concretamente, se propone modificar la frecuencia con la que se solicita al medio de pago que efectue la transmisión de los datos de pago, al mismo tiempo que se lleva a cabo un mecanismo de tratamiento particular para la señal recibida de los medios de pago, como una interfaz de aplicación protegida.

De este modo, el método llevado a cabo permite que una aplicación legítima que disponga de los derechos para efectuar un pago obtenga los datos del mismo de manera transparente. El método llevado a cabo también permite evitar que las aplicaciones maliciosas espíen los datos transmitidos a la aplicación legítima.

De forma más general, la invención hace referencia a un método de tratamiento de datos por parte de un dispositivo electrónico de adquisición de datos que se comunica con un dispositivo electrónico de aprovisionamiento de datos utilizando una tecnología de comunicación inalámbrica de corto alcance NFC que define una frecuencia de transmisión/recepción de referencia, comprendiendo el dispositivo electrónico de adquisición de datos: una interfaz de aplicación pública (PuAPI) accesible por una capa de aplicación (AppLyr), que utiliza la interfaz de aplicación pública (PuAPI) para transmitir y recibir datos por parte de un módulo NFC (ModNFC) conectado a una antena de transmisión/recepción (Ant); y una interfaz de aplicación privada (PrAPI) accesible por un componente de determinación de la frecuencia (CMF) y por una capa de aplicación protegida (SecApL), comprendiendo el método las siguientes etapas llevadas a cabo por parte del componente de determinación de la frecuencia (CMF):

- modificación de la frecuencia de transmisión/recepción de datos del módulo NFC (ModNFC) aplicando un parámetro de modificación (PMF) a la frecuencia de transmisión/recepción de referencia,

- recuperación de una señal procedente del módulo NFC y transformación de esta señal para obtener datos decodificados con la frecuencia de transmisión modificada, y

- transmisión de los datos descodificados a la capa de aplicación protegida (SecApL) a través de la interfaz de aplicación privada (PrAPI).

De este modo, una aplicación maliciosa no tiene la capacidad de obtener información mediante la monitorización de la frecuencia de referencia, puesto que no se utiliza para transmitir y recibir datos.

De acuerdo con una característica particular, dicho componente de determinación de la frecuencia está bajo el control exclusivo de un entorno de ejecución protegido de dicho dispositivo electrónico.

De este modo, una aplicación maliciosa no puede tener acceso al componente y, por lo tanto, no puede conocer la señal de respuesta a través de este componente.

De acuerdo con una característica particular, dicho método comprende:

- una etapa de recepción, por parte del componente de determinación de la frecuencia del dispositivo electrónico de adquisición de datos, de una solicitud de obtención de datos;

- una etapa de obtención, por parte del componente de determinación de la frecuencia, del parámetro de determinación de la frecuencia;

- la etapa de modificación, por parte del componente de determinación de la frecuencia, de la frecuencia de una señal de interrogación con destino al dispositivo de aprovisionamiento de datos, en función del parámetro de determinación de la frecuencia, proporcionando la frecuencia de interrogación;

- una etapa de transmisión, por parte del módulo NFC, de la señal de interrogación al dispositivo electrónico de aprovisionamiento de datos con dicha frecuencia de interrogación.

De este modo, la frecuencia modificada no está precodificada, sino que depende de un parámetro de determinación de la frecuencia cuyo valor puede, por ejemplo, evolucionar con el tiempo o depender de un índice determinado.

De acuerdo con una característica particular, la etapa de recuperación de la señal procedente del módulo NFC y de transformación de esta señal para obtener datos decodificados con la frecuencia de transmisión modificada comprende:

- una etapa de recepción, procedente del dispositivo electrónico de aprovisionamiento de datos, de una señal de respuesta, muestreada con dicha frecuencia de interrogación;

- una etapa de obtención, a partir de dicha señal de respuesta, en función de dicha frecuencia de interrogación, de una secuencia de bits;

- una etapa de transformación de dicha secuencia de bits en un conjunto de datos;

- una etapa de transmisión de dicho conjunto de datos.

De este modo, como la transmisión de datos, en el ámbito de la tecnología de campo cercano, da lugar (en el modo de respuesta pasiva) a una retransmisión en la misma frecuencia que la de transmisión, la señal recibida también se muestrea con la frecuencia de interrogación. Por lo tanto, una aplicación maliciosa que espíe los datos transmitidos a la "frecuencia normal" (normalmente 13,56 MHz) no puede percibir esta respuesta, que se realiza a una frecuencia diferente de la de referencia.

De acuerdo con una característica particular, la etapa de recepción, por parte del componente de determinación de la frecuencia del dispositivo electrónico de adquisición de datos, de la solicitud de obtención de datos, se lleva a cabo, al menos en parte, por parte de la interfaz de aplicación privada y comprende una etapa de emisión de una autorización de aplicación.

De este modo, el acceso al componente de determinación de la frecuencia está controlado: en consecuencia, una aplicación maliciosa, que por definición no tiene permiso para llamar a esta interfaz de aplicación privada, no puede tener acceso a los mensajes (transmitidos o recibidos) a través del componente de determinación de la frecuencia.

De acuerdo con una característica particular, la etapa de emisión de una autorización de aplicación comprende:

- una etapa de obtención de un dato representativo de un identificador de aplicación de la aplicación llamante, denominado identificador de aplicación;

- una etapa opcional de obtención de un dato representativo de una capa de aplicación llamante, denominado identificador de capa de aplicación;

- una etapa de determinación de una autorización de ejecución del componente de determinación en función de dicho identificador de aplicación y/o dicho identificador de capa de aplicación.

De este modo, en función de los datos predefinidos, por ejemplo, por parte del fabricante del dispositivo de interrogación, se define una lista de aplicaciones y/o una lista particular de capas de aplicación que tiene acceso al módulo de determinación de la frecuencia.

De acuerdo con una característica particular, el parámetro de determinación de la frecuencia es un factor multiplicativo.

De acuerdo con una característica particular, dicho factor multiplicativo tiene un valor comprendido entre 1,1 y 1,8.

Este rango de valores funciona con la mayoría de los dispositivos electrónicos de aprovisionamiento de datos.

De acuerdo con una característica particular, el valor del factor multiplicativo se determina de forma aleatoria en un rango de valores comprendido entre 1,1 y 1,8.

De este modo, una aplicación maliciosa no puede predecir el valor del factor multiplicativo.

De acuerdo con una característica particular, el valor del factor multiplicativo se determina por parte del componente de determinación de la frecuencia durante la recepción de una solicitud de obtención de datos sin contacto.

De este modo, el valor del factor multiplicativo no se puede deducir por una aplicación maliciosa sobre la base de la observación anterior, ya que este valor, decidido en el momento de la recepción de la solicitud, es capaz de evolucionar con cada transacción.

De acuerdo con otro aspecto, la invención también hace referencia a un dispositivo electrónico de adquisición de datos, que se comunica con un dispositivo electrónico de aprovisionamiento de datos utilizando una tecnología de comunicación inalámbrica de corto alcance NFC que define una frecuencia de transmisión/recepción de referencia, comprendiendo el dispositivo electrónico de adquisición de datos:

- una interfaz de aplicación pública (PuAPI) accesible por una capa de aplicación (AppLyr), que hace uso de la interfaz de aplicación pública (PuAPI) para transmitir y recibir datos por parte de un módulo NFC (ModNFC) conectado a una antena de transmisión/recepción (Ant); y

- una interfaz de aplicación privada (PrAPI) accesible a través de un componente de determinación de la frecuencia (CMF) y una capa de aplicación protegida (SecApL)

estando configurado el componente de determinación de la frecuencia (CMF) para:

- modificar la frecuencia de transmisión/recepción de datos del módulo NFC (ModNFC) aplicando un parámetro de modificación (PMF) a la frecuencia de transmisión/recepción de referencia,

- recuperar una señal procedente del módulo NFC y transformar esta señal para obtener datos decodificados con la frecuencia de transmisión modificada, y

- acceder a la interfaz de aplicación privada (PrAPI) para transmitir los datos descodificados a la capa de aplicación protegida (SecApL).

De manera más general, un dispositivo de este tipo comprende medios para llevar a cabo las etapas de los métodos descritos anteriormente.

De acuerdo con una implementación preferida, las diferentes etapas de los métodos de acuerdo con la invención se llevan a cabo mediante uno o más programas de software o programas informáticos, que comprenden instrucciones de software que tienen por objetivo ser ejecutadas por un procesador de datos de un módulo de relés de acuerdo con la invención y que se diseñan para controlar la ejecución de las diferentes etapas de los métodos.

En consecuencia, la invención también tiene por objetivo un programa, que se puede ejecutar mediante un ordenador o procesador de datos, teniendo este programa instrucciones para controlar la ejecución de las etapas de un método tal como el mencionado anteriormente.

Este programa puede utilizar cualquier lenguaje de programación, y estar 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 tiene por objetivo un soporte de datos legible por un procesador de datos, y que tiene instrucciones de un programa tal como el mencionado anteriormente.

El soporte de la información puede ser cualquier entidad o dispositivo capaz de almacenar el programa. Por ejemplo, el medio puede tener un medio de almacenamiento, tal como una ROM, por ejemplo, un CD ROM o una ROM de circuito microelectrónico, o incluso un medio de grabación magnético, por ejemplo, un disquete (floppy disc) o un disco duro.

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

Como alternativa, el soporte de la información puede ser un circuito integrado en el que se incorpore el programa, estando el circuito adaptado para ejecutar o ser utilizado en la ejecución del método en cuestión.

De acuerdo con una forma de realización, la invención se lleva a cabo por medio de componentes de software y/o hardware. En esta óptica, el término "módulo" se puede utilizar en este documento para hacer referencia tanto a un componente de software, un componente de hardware como un conjunto de componentes de hardware y software.

Un componente de software se corresponde con uno o más programas informáticos, uno o más subprogramas de un programa o, de manera más general, cualquier elemento de un programa o software capaz de llevar a cabo una función o un conjunto de funciones, de acuerdo con lo que se describe a continuación para el módulo en cuestión. Un componente de software de este tipo es ejecutado por un procesador de datos de una entidad física (terminal, servidor, pasarela, router, etc.) y puede acceder a los recursos de hardware de esta entidad física (memorias, soportes de grabación, buses de comunicación, tarjetas electrónicas de entrada/salida, interfaces de usuario, etc.).

De la misma manera, un componente de hardware se corresponde con cualquier elemento de un conjunto de hardware que puede llevar a cabo una función o un conjunto de funciones, de acuerdo con lo que se describe a continuación para el módulo en cuestión. Puede ser un componente de hardware programable o uno con un procesador integrado para la ejecución del software, por ejemplo, un circuito integrado, una tarjeta inteligente, una tarjeta de memoria, una tarjeta electrónica para la ejecución de un microsoftware (firmware), etc.

Cada componente del sistema descrito anteriormente lleva a cabo por supuesto sus propios módulos de software.

4. Dibujos

Otras características y ventajas de la invención quedarán más claras con la lectura de la siguiente descripción de una forma de realización preferida, dada meramente a modo de ejemplo ilustrativo y no restrictivo, y de los dibujos adjuntos, entre los cuales:

- la figura 1 muestra un sinóptico de la técnica propuesta;

- la figura 2 muestra una forma de realización aplicada a un terminal de comunicación que desea obtener datos procedentes de una tarjeta de pago;

- la figura 3 describe una implementación del método de tratamiento de datos en la forma de realización de la figura 2.

- la figura 4 describe un terminal de comunicación modificado para la implementación de la técnica propuesta.

5. DESCRIPCIÓN

5.1. Principio general

Como se indicó anteriormente, la técnica propuesta permite resolver los problemas de la técnica anterior. Más concretamente, la técnica propuesta puede contrarrestar el espionaje fraudulento realizado por una aplicación maliciosa.

La técnica propuesta presenta una solución para comunicar datos secretos, utilizando una antena NFC, en un entorno no protegido. La figura 1 presenta el principio general de la técnica propuesta;

Más concretamente, se propone modificar la frecuencia a la que un dispositivo electrónico de adquisición de datos (DEAD), solicita la obtención de datos a un dispositivo electrónico de aprovisionamiento de datos (DEFD), comunicándose el dispositivo electrónico de adquisición de datos (DEAD) y el dispositivo electrónico de aprovisionamiento de datos (DEFD) uno con el otro utilizando una tecnología de comunicación inalámbrica de corto alcance (NFC) que define una frecuencia de transmisión/recepción de referencia (por ejemplo, 13,56 MHz). La determinación de la frecuencia de interrogación se realiza a partir de un parámetro de determinación de la frecuencia (PMF) y de la frecuencia de referencia (FR) por un componente de determinación (CMF). La frecuencia a la que el módulo NFC (ModNFC) transmite la señal NFC puede ser modificada por el componente (CMF). En función de las formas de realización, la etapa de determinación de la frecuencia (de interrogación) consiste en aplicar una modificación de la frecuencia para efectuar la interrogación a una frecuencia inferior o superior a la frecuencia de referencia. Por lo tanto, la frecuencia de interrogación no es la frecuencia de referencia, sino una frecuencia diferente

de la frecuencia de referencia y el parámetro de determinación de la frecuencia (PMF) se utiliza para determinar cuál es esta frecuencia.

En función de las formas de realización y de las limitaciones de funcionamiento, el componente de determinación de la frecuencia (CMF) puede estar bajo el control exclusivo de un entorno de ejecución protegido de dicho dispositivo electrónico (TEE). Por lo tanto, sólo este entorno protegido (que puede ser un módulo protegido del dispositivo electrónico), tiene la capacidad de utilizar el componente de determinación de la frecuencia.

Además, para garantizar un acceso protegido al componente de determinación de la frecuencia, se lleva a cabo un mecanismo de control de autorización. En este mecanismo, sólo algunas aplicaciones (que se ejecutan dentro del dispositivo electrónico de adquisición de datos) o algunas capas de aplicación tienen la capacidad de acceder al componente de determinación de la frecuencia. La decisión de acceso se lleva a cabo, por ejemplo, por parte del entorno protegido, sobre la base de una lista de identificadores de aplicación autorizados y/o capas de aplicación autorizadas. Las aplicaciones y/o capas de aplicación autorizadas se determinan, por ejemplo, en el momento de la configuración del dispositivo electrónico, en forma de una base de datos interna (del tipo de archivo plano o XML, por ejemplo). El acceso y/o la transmisión de una solicitud de obtención de datos al componente de determinación de la frecuencia se lleva a cabo a través de una interfaz de aplicación privada, que permite solicitar los datos. El componente de determinación de la frecuencia actúa como intermediario (de determinación de la frecuencia de interrogación) entre la interfaz de la aplicación privada y el módulo NFC (convencional) que realmente va a construir y transmitir la señal (a partir de la frecuencia). Por lo tanto, el componente de determinación de la frecuencia no sólo se utiliza para modificar la frecuencia de transmisión de la señal, sino que también se utiliza para decodificar la señal de respuesta recibida y transformarla en una secuencia de bits: se trata, por lo tanto, de un componente pasarela. Este mecanismo comprende:

- una etapa de obtención de datos representativos de un identificador de aplicación de la aplicación llamante, denominado identificador de aplicación; y/o

- una etapa de obtención de un dato representativo de una capa de aplicación llamante, denominado identificador de capa de aplicación;

- una etapa de determinación de una autorización de ejecución del componente de determinación en función de dicho identificador de aplicación y/o dicho identificador de capa de aplicación.

Con esta técnica, una aplicación maliciosa (BadAPP) instalada en el dispositivo electrónico de adquisición de datos (DEAD) no puede acceder a los datos realmente recibidos por parte del componente de determinación de la frecuencia (CMF). En el mejor de los casos, esta aplicación maliciosa (BadAPP) puede acceder, a través de una interfaz de aplicación pública (PuAPI), a los datos decodificados a partir del módulo NFC (ModNFC). Sin embargo, como este módulo se configura para tratar la señal que recibe con una frecuencia de referencia, tiene la capacidad de tratar una señal con una frecuencia superior.

A continuación, se describe una forma de realización relacionada con la obtención de datos de pago a través de un terminal de comunicación del usuario. Se entiende que la siguiente forma de realización se da a título ilustrativo y que las técnicas descritas en esta forma de realización se pueden combinar entre sí o individualmente con el fin de adaptarse a condiciones de funcionamiento que pueden ser diferentes a las del pago, como por ejemplo la transferencia de archivos entre dos terminales, o la obtención de datos distintos de los datos bancarios.

5.2. Descripción de una forma de realización

En esta forma de realización, es posible aplicar la técnica propuesta, por ejemplo, para una comunicación de teléfono inteligente (o tableta u otro) a teléfono inteligente, teléfono inteligente a terminal de pago, tarjeta inteligente a teléfono inteligente, etc. Permite comunicar, por ejemplo, las credenciales bancarias de una tarjeta (de pago) al teléfono inteligente utilizando el hardware NFC, incluso en el caso de que una aplicación maliciosa instalada en el teléfono inteligente pueda llamar a las interfaces de aplicación proporcionadas por el sistema operativo que permiten escuchar la comunicación NFC. También permite prescindir del cifrado criptográfico por parte del transmisor (por ejemplo, la tarjeta de pago).

Para conseguir estos resultados, el principio general consiste en aplicar una modulación de frecuencia. Más concretamente, en lugar de utilizar una frecuencia de interrogación normalizada (por ejemplo, 13,56 Mhz), el dispositivo de pago interroga al medio de pago con una frecuencia superior (por ejemplo, 15,60 Mhz). Esta frecuencia de interrogación es la frecuencia con la que el dispositivo de pago transmite la solicitud de obtención de datos bancarios a los medios de pago. Los inventores han comprobado de hecho que un incremento controlado de la frecuencia de interrogación de los medios de pago no repercute necesariamente en la capacidad de los medios de pago para responder a la solicitud transmitida.

Para comprender el fundamento de la técnica propuesta por los inventores, es necesario hacer referencia al funcionamiento de un medio de pago NFC, como una tarjeta de pago, por ejemplo. Una tarjeta de pago NFC comprende un circuito impreso, siendo utilizado este circuito impreso para realizar un tratamiento de datos. Por regla general, el tratamiento de datos consiste en responder, según una norma de intercambio de datos particular, a una o más órdenes recibidas por parte del terminal de pago. Para recibir estas órdenes, la placa de circuito impreso se conecta a una antena. Esta antena (que generalmente es invisible y se dispone en el sustrato de la tarjeta) tiene dos funciones: la primera es transmitir un dato (una orden) al procesador para que éste sea tratado. La segunda función es alimentar el circuito impreso para que pueda realizar los tratamientos solicitados. De este modo, una tarjeta de pago NFC incluye una antena y un convertidor de señal asociados al circuito impreso. La antena capta la señal (alterna) transmitida a distancia por el dispositivo de pago, y el convertidor transforma esta señal en primer lugar en una corriente continua que alimenta el chip, y en segundo lugar en una corriente alterna denominada reloj que se utiliza para sincronizar los intercambios del chip y del dispositivo de pago en el tiempo.

Para resolver los problemas de seguridad planteados por la técnica anterior, los inventores tuvieron la ingeniosa idea de aumentar la frecuencia de la señal alterna transmitida (en proporciones que dependen del hardware) por el dispositivo de pago (y recibida por el medio de pago), conservando al mismo tiempo las funcionalidades de recepción, tratamiento y transmisión de datos del medio de pago.

Para asegurar el proceso, los inventores definen un nuevo componente de software y/o hardware de modulación, componente que se implanta dentro del dispositivo de pago. Ingeniosamente, este componente de software y/o hardware de modulación permite, por un lado, modular la frecuencia del reloj del módulo de transmisión/recepción de datos NFC (módulo NFC) y, por otro lado, tratar y descodificar los datos recibidos (es decir, los datos recibidos a través del módulo NFC). Normalmente, el factor multiplicativo de la frecuencia está comprendido entre 1,1 y 1,8. Se pueden utilizar otros valores, dependiendo de las necesidades y de la arquitectura del hardware. Por lo tanto, el componente de determinación utiliza una frecuencia comprendida entre 1,1 y 1,8 veces la frecuencia estándar de transmisión de campo cercano de 13,56 MHz, es decir, una frecuencia comprendida entre 14,916 MHz y 24,408 MHz. Además, de manera complementaria, también es posible disminuir la frecuencia de transmisión: en este caso el factor multiplicativo es inferior a 1. Normalmente, se podría aplicar un factor multiplicativo comprendido entre 0,7 y 0,9.

En relación con la Figura 2 se muestra una forma de forma de realización.

Un medio de pago NFC (10) (por ejemplo, una tarjeta) comprende una antena NFC (11) que está conectada a una placa de circuito impreso (12). Un dispositivo de pago (CTerm) (por ejemplo, un teléfono inteligente) comprende un módulo NFC (ModNFC) y se conecta a una antena de transmisión/recepción (Ant) y a una denominada capa de aplicación (AppLyr).

En funcionamiento normal (por ejemplo, un funcionamiento de intercambio de archivos), la capa de aplicación (AppLyr) hace uso de una interfaz de aplicación pública (PuAPI) para transmitir y recibir datos por parte del módulo NFC (ModNFC).

Una capa de aplicación se define como un conjunto de hardware y/o software que puede tener acceso a los datos procedentes de una o más capas "inferiores", es decir, capas (apiladas o no) que tratan directa o indirectamente las señales físicas que pasan por los componentes de hardware del dispositivo (en este caso, se trata de un dispositivo de pago). El acceso a los datos por una capa de aplicación se efectua a través de una interfaz de aplicación, que actúa como una especie de puerta de acceso a los datos procedentes de una capa inferior. Se pueden apilar varias capas de aplicación unas sobre otras, según se define, por ejemplo, en el modelo OSI para los protocolos de red.

En un funcionamiento alternativo, de acuerdo con la presente técnica, (por ejemplo, el funcionamiento para llevar a cabo un pago mediante una aplicación de pago AppP), un componente de determinación (CMF), modifica la frecuencia de transmisión/recepción de datos del módulo NFC (ModNFC). Para este propósito, el componente de determinación (CMF) aplica un parámetro de modificación predeterminado (PMF) al módulo NFC (ModNFC), causando la aplicación de este parámetro un incremento (o disminución) de la frecuencia de transmisión, según se explicó anteriormente. Durante la recepción de datos, el componente de determinación (CMF) recupera la señal procedente del módulo NFC y transforma esta señal para obtener datos descodificados con la frecuencia de transmisión establecida. El componente de determinación (CMF) tiene acceso a una interfaz de aplicación privada (PrAPI) que se utiliza para transmitir los datos del componente de determinación (CMF) a la capa de aplicación (AppLyr) o a una capa de aplicación protegida (SecApL).

La interfaz de aplicación privada (PrAPI) es accesible, de acuerdo con esta forma de realización general, únicamente para el componente de determinación (CMF) y, de forma alternativa o acumulativa, para la capa de aplicación protegida (SecApL) o para algunas aplicaciones de la capa de aplicación (AppLyr).

En relación con la Figura 3, se describe una forma de realización que ilustra el tratamiento de una transacción de pago que utiliza la técnica y los componentes descritos anteriormente.

Un usuario (USR) desea efectuar una transación de pago con su terminal de comunicación (CTerm) equipado con una interfaz NFC. Para efectuar el pago, el usuario colocará su tarjeta de pago (SCNFC) en el terminal de comunicación (CTerm). Sin embargo, previamente, se lleva a cabo el siguiente método:

- se abre una aplicación de pago (AppP) (10-1) (bien por el propio usuario USR o bien por una aplicación de un comerciante, previamente instalada en el terminal de comunicación y en la que el usuario desea efectuar una compra);

- la aplicación de pago (AppP), por ejemplo, después de haber mostrado el logotipo de pago sin contacto en la pantalla del terminal de comunicación (Cterm), transmite (10-2), a través de la interfaz de aplicación privada (PrAPI), una solicitud de obtención de datos sin contacto; esta solicitud se transmite (10-3) al componente de determinación (CMF);

- el componente de determinación (CMF) obtiene (10-4) un parámetro de determinación (PMF) que utiliza acto seguido para determinar la frecuencia de interrogación y para transmitir (10-5) al módulo NFC (ModNFC), una solicitud de obtención de datos sin contacto, de acuerdo con un protocolo predeterminado y con una frecuencia de interrogación a partir del parámetro de determinación (PMF);

Cuando el usuario constata que aparece el logotipo de pago sin contacto, coloca (10-6) su tarjeta de pago en el terminal de comunicación. La tarjeta recibe la señal procedente del terminal de comunicación y los datos de la tarjeta se transmiten (10-7), después de un posible tratamiento, en forma de señal de respuesta al módulo NFC (ModNFC) del terminal de comunicación.

- el componente de determinación (CMF) obtiene (10-8) la señal recibida por parte del módulo NFC (ModNFC) y la descodifica con la frecuencia de interrogación;

- el componente de determinación (CMF) transmite (10-9), a través de la interfaz de aplicación privada (PrAPI) (10-10), los datos descodificados a la aplicación de pago (AppP), que los puede utilizar para efectuar o finalizar la transacción de pago.

Esta utilización tiene varias ventajas. En primer lugar, la frecuencia de interrogación modifica la señal recibida. Por lo tanto, ésta dificilmente se puede interpretar por parte de los posibles dispositivos de espionaje (es decir, dispositivos adicionales de los alrededores que podrían intentar interceptar los datos). Además, como la frecuencia depende de un parámetro de modulación (que puede ser variable para un dispositivo determinado), el hecho de conocer una frecuencia no permite eludir la presente técnica. Se señala además que este parámetro se puede obtener de forma aleatoria o pseudoaleatoria, dentro de un rango de configuración determinado: por ejemplo, un valor aleatorio dentro de un rango de 1kHz, 10kHz o 100kHz.

Además, la arquitectura y el método propuestos ofrecen una ventaja desde el punto de vista de la aplicación maliciosa (posiblemente instalada en el terminal de comunicación). De hecho, la técnica propuesta permite engañar a esta posible aplicación: la aplicación maliciosa, que al llamar a la interfaz de la aplicación pública, obtiene datos erróneos procedentes del módulo NFC. De hecho, la interfaz de aplicación pública, al no estar informada de la determinación de la frecuencia de interrogación, intenta transformar la señal de acuerdo con una frecuencia estándar. Sin embargo, un intento de este tipo está destinado a fracasar y da lugar a la transmisión bien de datos erróneos o bien de errores a la aplicación maliciosa.

5.3. Otras características y ventajas

En relación con la figura 4, se describe un terminal de comunicación que se utiliza para realizar una transmisión de datos en el ámbito de un proceso de pago de acuerdo con el método anteriormente descrito.

Por ejemplo, el terminal de comunicación comprende una memoria 41 constituida por una memoria intermedia, un procesador de procesamiento general 42, por ejemplo un microprocesador, y accionado por un programa informático 43, y una memoria protegida, un procesador de procesamiento protegido 44 (por ejemplo TEE), accionado por un programa informático 45, estos procesadores de procesamiento llevan a cabo los métodos de tratamiento y de transmisión/recepción de datos tal como se han descrito anteriormente para efectuar el tratamiento de datos con destino y procedentes de una interfaz sin contacto.

En la inicialización, las instrucciones de código del programa informático 45 se cargan, por ejemplo, en una memoria antes de ser ejecutadas por el procesador de procesamiento protegido 44.

El procesador de procesamiento protegido 44 recibe (a través de una interfaz de software o hardware) como entrada al menos una solicitud de obtención de datos sin contacto procedente, por ejemplo, del procesador de procesamiento general 42. El procesador de procesamiento protegido 44 lleva a cabo las etapas del método de transmisión de datos, de acuerdo con las instrucciones del programa informático 45 para obtener (con una frecuencia predefinida), una o

más señales procedentes de un medio de pago sin contacto, señales que se transforman en datos que se transmiten al procesador de procesamiento general 42. El procesador de procesamiento general 42 efectúa un tratamiento de estos datos para, por ejemplo, efectuar una transacción de pago.

Para ello, el terminal de comunicación comprende, además de la memoria intermedia 41, medios de comunicación, tales como módulos de comunicación en red, medios de transmisión de datos y circuitos de transmisión de datos entre los distintos componentes del terminal de comunicación.

Estos medios se pueden presentar en forma de un procesador particular implementado dentro del terminal de comunicación. De acuerdo con una forma de realización particular, este dispositivo lleva a cabo una aplicación particular que se encarga de la realización de transacciones, siendo esta aplicación, por ejemplo, proporcionada por parte del fabricante del procesador en cuestión con el fin de permitir la utilización de dicho procesador o por parte de un proveedor de soluciones de pago para terminales "abiertos". Para este propósito, el procesador comprende medios de identificación únicos. Estos medios de identificación únicos permiten garantizar la autenticidad del procesador.

Como se indicó, el terminal de comunicación comprende medios de comunicación de campo cercano, denominados NFC (ModNFC) y medios de transmisión y de recepción de datos procedentes de las redes de comunicaciones. Estos medios también se presentan como interfaces de comunicación que permiten intercambiar datos a través de redes de comunicación, medios de interrogación y de actualización de bases de datos. Más concretamente, los medios de comunicación de campo cercano se pueden configurar para transmitir y recibir datos en función de una frecuencia de transmisión/recepción, pudiendo modularse esta frecuencia (de una transmisión a otra) en función de un parámetro de modulación, siendo este parámetro de modulación definido bien por parte del procesador de procesamiento protegido (cuando existe), bien a través de un entorno protegido (TEE) dependiendo del sistema operativo del terminal de comunicación y accesible a través de un componente de determinación (CMF).

REIVINDICACIONES

1. Método de tratamiento de datos por un dispositivo electrónico de adquisición de datos (DEAD, CTerm) que se comunica con un dispositivo electrónico de aprovisionamiento de datos (DEFD, 10, SCNFC) utilizando una tecnología de comunicación inalámbrica de corto alcance NFC que define una frecuencia de transmisión/recepción de referencia (FR), comprendiendo el dispositivo electrónico de adquisición de datos (DEAD, CTerm):

- una interfaz de aplicación pública (PuAPI) accesible por una capa de aplicación (AppLyr), que hace uso de la interfaz de aplicación pública (PuAPI) para transmitir y recibir datos por parte de un módulo NFC (ModNFC) conectado a una antena de transmisión/recepción (Ant); y

- una interfaz de aplicación privada (PrAPI) accesible por un componente de determinación de la frecuencia (CMF) y una capa de aplicación protegida (SecApL),

comprendiendo el método las siguientes etapas, llevadas a cabo por parte del componente de determinación de la frecuencia (CMF):

- modificación (10-4, 10-5, 10-7) de la frecuencia de transmisión/recepción de datos del módulo NFC (ModNFC) aplicando un parámetro de modificación (PMF) a la frecuencia de transmisión/recepción de referencia (FR),

- recuperación (10-8) de una señal procedente del módulo NFC y transformación de esta señal para obtener datos decodificados con la frecuencia de transmisión modificada, y

- transmisión (10-9, 10-10) de los datos descodificados a la capa de aplicación protegida (SecApL) a través de la interfaz de aplicación privada (PrAPI).

2. Método de tratamiento de datos, de acuerdo con la reivindicación 1, caracterizado por que dicho componente de determinación de la frecuencia (CMF) está bajo el control exclusivo de un entorno de ejecución protegido (TEE) de dicho dispositivo electrónico.

3. Método de tratamiento de datos de acuerdo con la reivindicación 1, caracterizado por que comprende:

- una etapa de recepción (10-1, 10-2, 10-3), por parte del componente de determinación de la frecuencia (CMF) del dispositivo electrónico de adquisición de datos (DEAD, CTerm), de una solicitud de obtención de datos;

- una etapa de obtención (10-4), por parte del componente de determinación de la frecuencia (CMF), del parámetro de determinación de la frecuencia (PMF);

- una etapa de modificación (10-4, 10-5), por parte del componente de determinación de la frecuencia (CMF), de la frecuencia de una señal de interrogación con destino del dispositivo de aprovisionamiento de datos (DEFD, 10, SCNFC), en función del parámetro de determinación de la frecuencia (PMF) que proporciona la frecuencia de interrogación;

- una etapa de transmisión (10-7), por parte del módulo NFC (ModNFC), de la señal de interrogación al dispositivo electrónico de aprovisionamiento de datos (DEFD, 10, SCNFC) con dicha frecuencia de interrogación.

4. Método de tratamiento de datos de acuerdo con la reivindicación 3, caracterizado por que la etapa de recuperación (10-8) de la señal procedente del módulo NFC (ModNFC) y de transformación de esta señal para obtener datos decodificados con la frecuencia de transmisión modificada comprende:

- una etapa de recepción (10-7, 10-8), procedente del dispositivo electrónico de aprovisionamiento de datos (DEFD, 10, SCNFC), de una señal de respuesta, muestreada con dicha frecuencia de interrogación;

- una etapa de obtención, a partir de dicha señal de respuesta, en función de dicha frecuencia de interrogación, de una secuencia de bits;

- una etapa de transformación de dicha secuencia de bits en un conjunto de datos;

- una etapa de transmisión (10-9, 10-10) de dicho conjunto de datos.

5. Método de tratamiento de datos de acuerdo con la reivindicación 3, caracterizado por que dicha etapa de recepción (10-1, 10-2), por parte del componente de determinación de la frecuencia (CMF) del dispositivo electrónico de

adquisición de datos (DEFD, 10, SCNFC), de la solicitud de obtención de datos se lleva a cabo, al menos en parte, por la interfaz de aplicación privada (PrAPI) y comprende una etapa de emisión de una autorización de aplicación.

6. Método de tratamiento de datos de acuerdo con la reivindicación 5, caracterizado por que la etapa de emisión de una autorización de aplicación comprende:

- una etapa de obtención de un dato representativo de un identificador de aplicación de la aplicación llamante (AppP), denominado identificador de aplicación; y/o

- una etapa de obtención de un dato representativo de una capa de aplicación llamante (AppLyr), denominado identificador de capa de aplicación;

- una etapa de determinación de una autorización de ejecución del componente de determinación (CMF) en función de dicho identificador de aplicación y/o dicho identificador de capa de aplicación.

7. Método de tratamiento de datos de acuerdo con la reivindicación 1, caracterizado por que el parámetro de determinación de la frecuencia (PMF) es un factor multiplicativo.

8. Método de tratamiento de datos de acuerdo con la reivindicación 7, caracterizado por que dicho factor multiplicativo tiene un valor comprendido entre 1,1 y 1,8.

9. Método de tratamiento de datos de acuerdo con la reivindicación 7, caracterizado por que el valor del factor multiplicativo se determina aleatoriamente en un rango de valores comprendido entre 1,1 y 1,8.

10. Método de tratamiento de datos de acuerdo con la reivindicación 7, caracterizado por que el valor del factor multiplicativo se determina por el componente de determinación de la frecuencia (CMF) durante la recepción (10-1, 10-2, 10-3) de una solicitud de obtención de datos sin contacto.

11. Dispositivo electrónico de adquisición de datos (DEAD, CTerm) que se comunica con un dispositivo electrónico de aprovisionamiento de datos (DEFD, 10, SCNFC) utilizando una tecnología de comunicación inalámbrica de corto alcance NFC que define una frecuencia de transmisión/recepción de referencia (FR), comprendiendo el dispositivo electrónico de adquisición de datos (DEAD, CTerm):

- una interfaz de aplicación pública (PuAPI) accesible por una capa de aplicación (AppLyr), que hace uso de la interfaz de aplicación pública (PuAPI) para transmitir y recibir datos por parte de un módulo NFC (ModNFC) conectado a una antena de transmisión/recepción (Ant); y

- una interfaz de aplicación privada (PrAPI) accesible por un componente de determinación de la frecuencia (CMF) y una capa de aplicación protegida (SecApL)

estando configurado el componente de determinación de la frecuencia (CMF) para:

- modificar (10-4, 10-5, 10-7) la frecuencia de transmisión/recepción de datos del módulo NFC (ModNFC) aplicando un parámetro de modificación (PMF) a la frecuencia de transmisión/recepción de referencia (FR),

- recuperar (10-7, 10-8) una señal procedente del módulo NFC y transformar esta señal para obtener datos decodificados con la frecuencia de transmisión modificada, y

- acceder (10-9, 10-10) a la interfaz de aplicación privada (PrAPI) para transmitir los datos decodificados a la capa de aplicación protegida (SecApL).

12. Un producto de programa informático que se puede descargar 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 la ejecución de un método de tratamiento de datos de acuerdo con la reivindicación 1, cuando se ejecuta en un procesador.

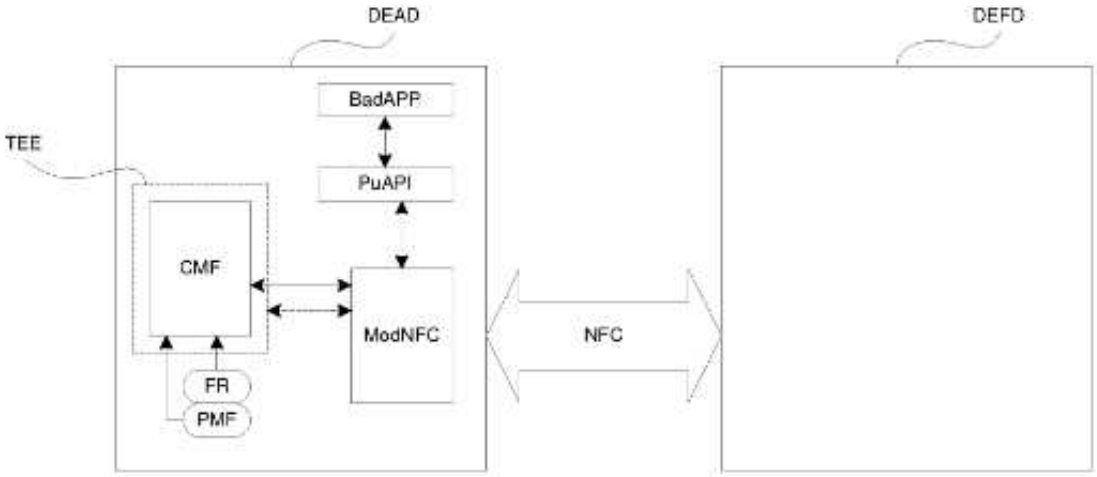

Figura 1

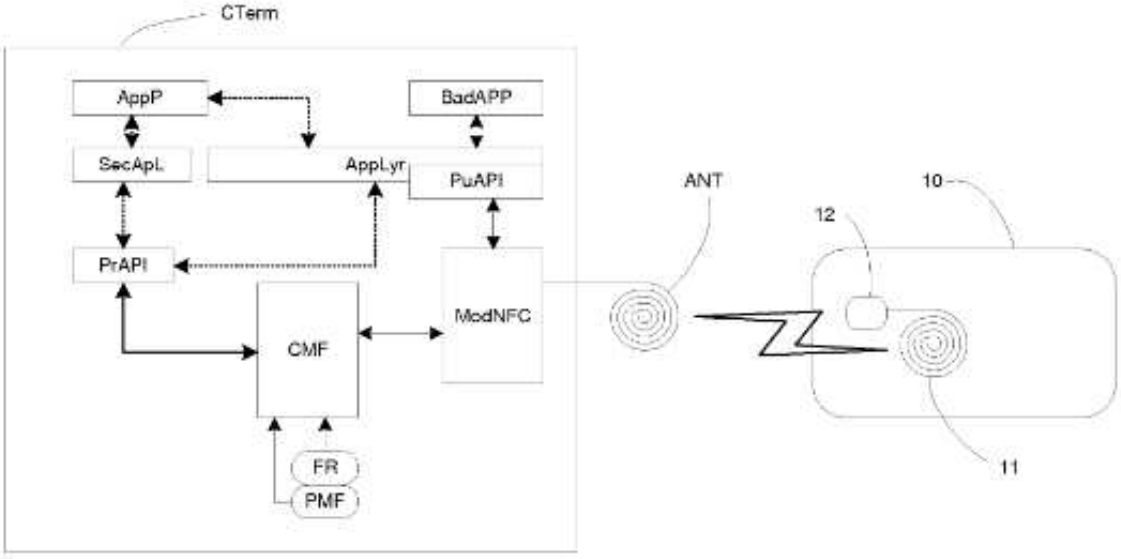

Figura 2

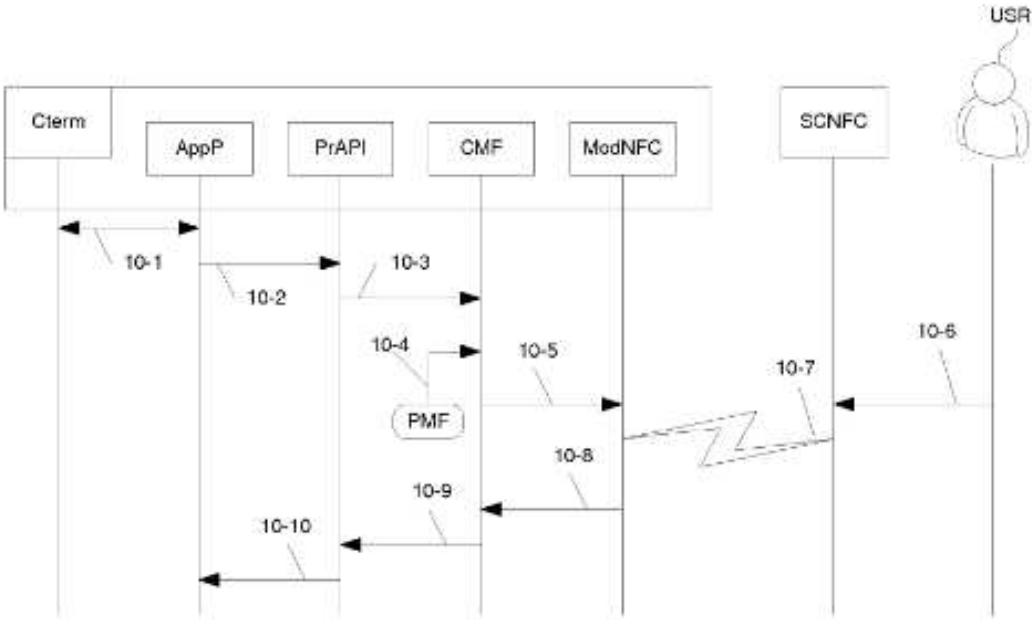

Figura 3

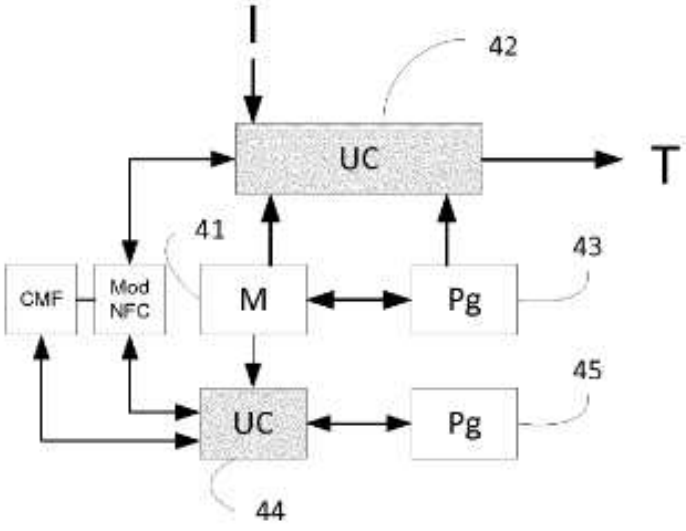

Figura 4