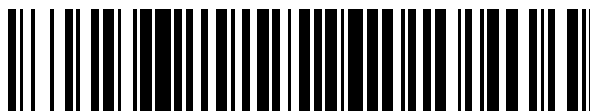


19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 427 239**

51 Int. Cl.:

G06Q 20/00 (2012.01)

G06Q 20/12 (2012.01)

G06Q 20/32 (2012.01)

G06Q 20/04 (2012.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Fecha de presentación y número de la solicitud europea: **28.03.2008 E 08799906 (6)**

97 Fecha y número de publicación de la concesión europea: **05.06.2013 EP 2143053**

54 Título: **Procedimiento de comunicación y de transmisión de un mensaje relativo a una transacción de una aplicación sin contacto, terminal, módulo seguro y sistema asociados**

30 Prioridad:

30.03.2007 FR 0754194

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

29.10.2013

73 Titular/es:

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

72 Inventor/es:

**PICQUENOT, DAVID y
FOURREAU, LAURENT**

74 Agente/Representante:

LINAGE GONZÁLEZ, Rafael

ES 2 427 239 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín europeo de patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre concesión de Patentes Europeas).

DESCRIPCIÓN

Procedimiento de comunicación y de transmisión de un mensaje relativo a una transacción de una aplicación sin contacto, terminal, módulo seguro y sistema asociados

5 La presente invención se refiere al campo de las telecomunicaciones y, de manera más particular, al de la gestión de las aplicaciones de un terminal móvil.

10 La mayoría de los terminales móviles existentes permiten, no solo establecer comunicaciones telefónicas, sino también ejecutar un determinado número de aplicaciones descargadas de Internet en un módulo seguro del terminal. Este módulo seguro puede ser un módulo de memoria del terminal o un soporte extraíble (por ejemplo una tarjeta de abonado UICC por "Universal Integrated Circuit Card") insertada en el terminal. Algunos de estos terminales están, además, equipados con un módulo específico, denominado "módulo sin contacto", que permite que el terminal móvil dialogue y/o realice transacciones sin contacto con unos bornes denominados "bornes sin contacto". De manera más precisa, este módulo permite la transferencia bidireccional de datos entre un borne sin contacto y una aplicación descargada de Internet. Una aplicación de este tipo es, por ejemplo, una aplicación en el ámbito de los transportes en la que el paso del terminal móvil por delante de un borne permite validar el acceso del usuario al medio de transporte.

20 Al ser la aplicación descargada de Internet una aplicación esclava, controlada por el borne sin contacto, el fin de la transacción no es fácilmente identificable por el terminal móvil y, por ello, este terminal difícilmente puede informar al portador del terminal del resultado de la transacción. El método que se utiliza en la actualidad consiste en configurar el terminal móvil para que consulte a intervalos regulares las diferentes aplicaciones instaladas; transmitiendo de retorno estas aplicaciones unas informaciones, si ha tenido lugar una transacción. Al ser la consulta del terminal móvil y la transacción dos procesos descorrelacionados, no se controla el plazo para una visualización tras una transacción y la visualización no se realiza en tiempo real. Este plazo para la visualización se puede reducir aumentando el número de consultas, pero esto plantea problemas de consumo eléctrico cuando las aplicaciones están instaladas en un módulo seguro extraíble insertado en el terminal ya que este módulo se debe alimentar eléctricamente en cada consulta.

30 La presente invención permite resolver este problema ofreciendo una solución que permite informar al portador del terminal móvil, en tiempo real, del resultado de una transacción sin contacto.

35 Para ello, la presente invención ofrece un procedimiento de comunicación de un mensaje relativo a una transacción de una aplicación sin contacto realizada entre un terminal móvil, equipado con un módulo sin contacto y con un módulo seguro, y un equipo, inicializándose dicha transacción mediante dicho equipo, comprendiendo el procedimiento las etapas que se establecen en la reivindicación 1.

40 De este modo, el procedimiento de acuerdo con la invención permite que al portador del terminal móvil se le informe mediante el terminal móvil del resultado de una transacción desde el momento en que esta se termina. Además el mensaje de información le permite saber qué aplicación ha realizado la transacción. Esta información resulta especialmente útil cuando se instalan varias aplicaciones en el terminal móvil.

45 En un modo de realización de acuerdo con la invención, la aplicación se memoriza en un módulo seguro del terminal móvil y la etapa de obtención comprende una etapa de envío al módulo seguro de una información de detección de fin de transacción y una etapa de recepción de dicho mensaje y de una instrucción de interfaz hombre máquina. De este modo, las informaciones relativas a una aplicación las gestiona una única entidad, el módulo seguro. Esto permite garantizar una mayor seguridad de la aplicación.

50 En un modo de realización, la información de detección de fin de transacción contiene un identificador correspondiente a la aplicación asociada a la transacción. Este identificador o bien se almacena durante la transacción, o bien se transmite mediante la aplicación al módulo sin contacto al final de transacción. Este identificador permite, al final de la transacción, identificar la aplicación vinculada a la transacción que se acaba de realizar entre el conjunto de las aplicaciones almacenadas en el terminal móvil.

55 En un modo de realización, el módulo seguro es una tarjeta de abonado insertada en el terminal móvil.

60 En un modo de realización de la invención, la información de fin de transacción comprende unos datos de la aplicación actualizados tras la ejecución de la transacción. El usuario del terminal móvil está de este modo informado de las modificaciones llevadas a cabo en la transacción.

65 Al final de la transacción, el mensaje que se obtiene mediante el procedimiento de la invención se transmite al portador del terminal móvil a través de una interfaz hombre máquina presente en el terminal. En un modo de realización, la etapa de comunicación es una etapa de visualización de dicho mensaje en una pantalla del terminal móvil y/o una etapa de difusión de un mensaje de voz que contiene dicho mensaje por el altavoz del terminal móvil.

La invención también se refiere a un procedimiento de acuerdo con la reivindicación 1, comprendiendo el procedimiento las siguientes etapas:

- identificación de la aplicación (AP1).

5 En un modo de realización, la etapa de identificación comprende una etapa de lectura de un identificador memorizado durante la transacción. En un modo de realización, el identificador se almacena en una memoria del módulo seguro durante la transacción y la etapa de identificación comprende una etapa de lectura de este
10 identificador en la memoria. En otro modo de realización, el identificador se almacena en una memoria del módulo sin contacto durante la transacción y se inserta en la información de detección de fin de detección transmitida desde el módulo sin contacto al módulo seguro. Estos modos de realización presentan la ventaja de no necesitar ninguna modificación de la aplicación.

15 En otro modo más de realización, la información de detección de fin de transacción también contiene una dirección de un programa vinculado a la aplicación, suministrándose mediante la aplicación la dirección al módulo sin contacto al final de la transacción. De este modo, no es necesario almacenar un identificador durante la transacción. Las transacciones "sin contacto" se realizan siempre en un tiempo muy limitado y la inserción de una orden adicional de memorización durante la transacción puede ser perjudicial para el buen adecuado desarrollo de la transacción. Este modo de realización permite evitar este tipo de problema.

20 La invención también se refiere a un terminal móvil de acuerdo con la reivindicación 11.

La invención también se refiere a un sistema de acuerdo con la reivindicación 12.

25 Se mostrarán otras particularidades y ventajas de la presente invención en la siguiente descripción de un modo de realización que se da a título de ejemplo no excluyente, en referencia los dibujos adjuntos, en los que:

- la figura 1 es un esquema general que presenta el contexto de la invención;

30 - la figura 2 es un esquema que ilustra los diferentes intercambios durante una transacción sin contacto;

- la figura 3 es un esquema que ilustra las diferentes etapas del procedimiento de la invención;

35 - la figura 4 es un esquema que ilustra las diferentes etapas del procedimiento de acuerdo con un primer modo de realización de la invención;

- la figura 5 es un esquema que ilustra las diferentes etapas del procedimiento de acuerdo con un segundo modo de realización de la invención;

40 - la figura 6 es un diagrama de bloques que representa un sistema de acuerdo con un modo de realización de la invención.

A continuación se va a describir en referencia a la figura 1 un modo de realización de la invención en el cual un usuario dispone de un terminal móvil 100 en el cual se han instalado varias aplicaciones. Este terminal móvil es, por
45 ejemplo, un teléfono móvil o una PDA (por "Personal Digital Assistant"). Este terminal móvil 100 comprende un módulo de comunicación sin contacto 10 que permite un diálogo entre el terminal 100 y un equipo 200 llamado de aquí en adelante "borne sin contacto". El módulo sin contacto es, por ejemplo un módulo compatible NFC (por "Near Field Communication").

50 El terminal móvil 100 también comprende un módulo seguro 20 que es una tarjeta de abonado de tipo UICC (por "Universal Integrated Circuit Card"). Como alternativa, este módulo puede ser una área de memoria segura del terminal móvil o un soporte extraíble de otro tipo (por ejemplo una tarjeta de abonado de tipo SIM o una tarjeta de memoria (*SD card*, *Embebed Secure controler...*)).

55 Se han almacenado una o varias aplicaciones (AP1, AP2...) en la memoria de la tarjeta de abonado. Entre estas aplicaciones, una o varias son aplicaciones sin contacto y funcionan utilizando el módulo sin contacto 10. Una aplicación de este tipo es, por ejemplo, una aplicación de control de acceso a un transporte público. Esta aplicación se utilizará entonces cada vez que el portador del móvil quiera acceder a este transporte. En cada uso, un diálogo entre la aplicación almacenada en la tarjeta de abonado 20 y un borne sin contacto 200 instalado en la entrada del
60 medio de transporte permite que el borne verifique que el portador del móvil está autorizado para coger este medio de transporte. Este diálogo permite, por ejemplo, verificar que el portador del móvil posee un abono válido para este medio de transporte o descontar un número de viajes almacenados en la tarjeta de abonado. Este diálogo entre la tarjeta de abonado 20 y el borne sin contacto 200 se realiza a través del módulo sin contacto 10.

65 De manera conocida, el borne sin contacto 200 emite un campo magnético. Cuando el usuario del móvil se presenta en la entrada del medio de transporte, su terminal móvil entra en el campo magnético que emite el borne 200. Se

realiza entonces una transacción entre la aplicación seleccionada presente en la tarjeta de abonado del terminal móvil y el borne 200. De manera más precisa, tal y como se describe en la figura 2, al entrar el terminal móvil en el campo magnético del borne sin contacto, el módulo sin contacto recibe del borne sin contacto un mensaje MS de selección (*select AID*) que contiene el identificador AID1 de una aplicación AP1 y lo transmite a la tarjeta de abonado. Con la recepción de este mensaje MS, la tarjeta de abonado ordena la ejecución de la aplicación AP1 seleccionada. El intercambio de los mensaje entre el módulo sin contacto y la tarjeta de abonado se realiza de forma clásica, por ejemplo utilizando el protocolo SWP por “Single Wire protocol” o la interfaz S²C por “SigIn-SigOut-Connection”. En función de la aplicación seleccionada, un determinado número de mensajes (M1, M2,... Mn) se van a intercambiar a continuación entre la aplicación y el borne sin contacto.

En el modo de realización descrito, tras haber recibido el mensaje de selección y antes de ordenar la ejecución de la aplicación, la tarjeta de abonado, durante una etapa E0, graba en una memoria temporal T de la tarjeta de abonado 20, el identificador AID1 de la aplicación seleccionada AP1. Como alternativa, este registro del identificador se puede realizar después de enviar la orden de ejecución de la aplicación o durante la transacción.

A continuación vamos a describir las principales etapas del procedimiento de acuerdo con la invención, en referencia a la figura 3. Estas etapas siguen al intercambio de los mensajes (M1, M2,... Mn). Durante una etapa E1, el módulo sin contacto detecta el fin de la transacción. El fin de la transacción se produce por una ruptura del campo magnético entre el borne y el terminal, no estando ya el terminal presente en el campo que emite el borne o eventualmente porque el borne ya no emite este campo. De manera más precisa, esta ruptura se detecta mediante un disparador (o “trigger” en inglés) añadido o integrado en el módulo sin contacto.

Como alternativa, el campo magnético que emite el borne se mantiene y el fin de la transacción se detecta mediante la recepción por el módulo sin contacto de un mensaje de fin de transacción que emite el borne (por ejemplo un mensaje *Disconnect* o *Deselect* ISO 14443-3).

A la etapa E1 le sigue una etapa E2 de obtención de un mensaje que contiene al menos una información que identifica la aplicación seleccionada y una información de fin de transacción.

El mensaje que se obtiene se comunica a continuación al portador del móvil, a través de la pantalla del terminal móvil, en una etapa E3. Como alternativa, la comunicación se puede realizar a través del altavoz del terminal.

A continuación vamos a describir de manera más precisa la etapa E2 de acuerdo con un primer modo de realización, en referencia a la figura 4.

En este modo de realización, el terminal móvil está provisto de un navegador WEB 110. Este navegador permite acceder a las páginas Web almacenadas en la tarjeta de abonado. Se alberga un servidor HTTP en la tarjeta de abonado. La tecnología que se utiliza es, por ejemplo, SCWS (por “SmartCard WEB Server”) en proceso de normalización en el OMA (Open Mobile Alliance) del grupo OMA SEC-Smart Card Technology subworking group (SEC-SCT). Esta tecnología permite que el terminal móvil inicie una aplicación almacenada en la tarjeta de abonado, a partir de un navegador WEB.

En una primera subetapa E210, tras la detección del fin de la transacción, el módulo de comunicación sin contacto 10 envía al navegador Web del terminal móvil una información de detección de fin de transacción. Esta información es una orden que permite iniciar el navegador Web del terminal móvil. Esta contiene, como parámetro, la dirección de un programa PG de la tarjeta de abonado. Esta orden y esta dirección se han almacenado previamente en el módulo sin contacto 10. En la etapa siguiente E212, con la recepción de esta información, el navegador, a través del SCWS, redirige la orden hacia la tarjeta de abonado que permite de este modo el inicio del programa PG. De manera más precisa, la dirección del programa PG es una url correspondiente a un programa PG de la tarjeta de abonado común a todas las aplicaciones. En una subetapa E214, la tarjeta de abonado procede a la lectura del identificador AID1 grabado, durante la transacción, en la memoria temporal T. Por ejemplo, se puede grabar en un EF (*Elementary File*). En una subetapa E216, la dirección de un segundo programa PAP1, vinculado a la aplicación AP1, se determina mediante la lectura en una tabla de correspondencias TAB que pone en correspondencia cada identificador de aplicación con una dirección de un subprograma. Esta dirección también es una url. En una subetapa E218, el empleo de una orden de redirección permite la ejecución del programa almacenado a partir de la dirección PAP1. Este programa es específico de la aplicación seleccionada.

En una etapa E220, este programa determina el mensaje destinado al portador del terminal. Este mensaje contiene una información que permite que el portador identifique la aplicación que se acaba de utilizar. Esta información almacenada en el programa PAP1 es una información en forma de texto, por ejemplo “bus Caen”. El mensaje también contiene una información de fin de transacción. Esta información de fin de transacción es, por ejemplo, una información almacenada en el programa en forma de texto, por ejemplo, “transacción terminada”. En otro modo de realización, el mensaje de fin de transacción puede contener una información de actualización de la aplicación. Para obtener esta información, el programa PAP1 consulta a la aplicación AP1 vinculada a este programa que, de retorno, le proporciona la información solicitada. Por ejemplo, el programa PAP1 obtiene de este modo el número de viajes de autobús comprados por el portador y aun no utilizados. La información que se obtiene se inserta a continuación

en un mensaje de texto mediante el programa PAP1. Por ejemplo, la información de fin de transacción es “transacción terminada - Le quedan 9 viajes”. Como alternativa, la información de fin de transacción puede implicar de forma implícita que la transacción ha terminado; por ejemplo, la información de fin de transacción puede ser: “le quedan 9 viajes”. La información que identifica la aplicación y la información de fin de transacción se insertan a continuación en un mismo mensaje.

En una etapa E224, el mensaje se transmite con una orden de visualización al navegador Web 110 del terminal móvil. En el modo de realización que se describe aquí, la orden de visualización y el mensaje que se va a visualizar se transmiten en una página XHTML.

En la etapa E3 siguiente, el navegador Web se dirige, de forma clásica, a la interfaz hombre máquina 120 del terminal móvil para ordenar la visualización del mensaje en la pantalla del terminal móvil.

Como alternativa, el identificador de la aplicación memorizado en la etapa E0 no se graba en la tarjeta de abonado, sino en una memoria del módulo sin contacto. Se transmite entonces como parámetro con la dirección del programa PG en las etapas E210 y E212, y la etapa E214 de lectura de identificador en la memoria se sustituye por una etapa de recepción de este identificador por la tarjeta de abonado.

A continuación vamos a describir un segundo modo de realización, en referencia a la figura 5. En este modo de realización, el identificador AID1 de la aplicación AP1 no se memoriza durante la transacción y las etapas E1 y E3 son idénticas a las del primer modo de realización descrito.

En la etapa E2, tras la detección del fin de la transacción, el módulo sin contacto envía al navegador Web 110 del terminal móvil, en una etapa E310, una información de detección de fin de transacción. Esta información es una orden que permite iniciar el navegador Web del terminal móvil. Esta contiene, como parámetro, la dirección de un programa PAP1 de la tarjeta de abonado. La orden que permite iniciar el navegador o bien se almacena en el módulo sin contacto, o bien se transmite a este mediante la aplicación AP1 con la dirección del programa PAP1. La dirección PAP1, que es la dirección de una aplicación vinculada a la aplicación AP1 seleccionada, se suministra mediante la aplicación AP1 al módulo sin contacto al final de la transacción tras la recepción por la tarjeta de abonado de una orden transmitida por el módulo sin contacto. De manera más precisa y a título de ejemplo, tras la detección del fin de transacción, el módulo sin contacto transmite una orden “Deselect Event” al módulo de recepción de la tarjeta de abonado (*SWP Handler*) que reenvía una orden “Deselect APDU” a la aplicación AP1. Tras la recepción de esta orden, la aplicación AP1 reenvía al módulo sin contacto la dirección PAP1.

Con la recepción de la información de detección de fin de transacción, en una etapa E312, el navegador, a través del SCWS, se dirige a la tarjeta y el programa PAP1 se ejecuta. De manera más precisa, la dirección del programa PAP1 es una url correspondiente a un programa de la tarjeta de abonado específica de la aplicación seleccionada.

A esta etapa le siguen unas etapas E320 y E324, similares a las etapas E220 y E224 del primer modo de realización.

En los dos modos de realización que se han descrito anteriormente, el módulo seguro es una tarjeta de abonado 20 y el diálogo entre el terminal móvil y la tarjeta de abonado utiliza un navegador Web. Como alternativa, y en particular en el caso en el que el módulo seguro es un área de memoria del terminal móvil, el diálogo se realiza, de manera conocida, mediante la interfaz entre el módulo sin contacto y el módulo principal del terminal móvil (*interface NFC chip-Digital Base Band*). De este modo, al final de la transacción, una orden de tipo *Launch* permite iniciar el programa (PG, PAP1). En el caso concreto en el que las aplicaciones son unas aplicaciones Java, se utiliza, por ejemplo, la API JRS 251 y la función “PushRegistry” definida en las especificaciones MIDP (por “Mobile Information Device Profile”) se utiliza para activar/iniciar la aplicación PAP1.

De acuerdo con un modo de realización seleccionado y representado en la figura 6, un sistema que aplica la invención se compone, por ejemplo, de un terminal móvil 100 y de una tarjeta de abonado 20.

El terminal móvil 100 comprende, de manera conocida, en particular una unidad de tratamiento 150 equipada con un microprocesador, una memoria de solo lectura de tipo ROM 170, una memoria viva de tipo RAM 190. El terminal móvil 100 comprende un módulo sin contacto 10 y puede comprender de manera clásica y no exhaustiva los siguientes elementos: un teclado, una pantalla, un micrófono, un altavoz, una interfaz de comunicación, un medio de almacenamiento. La memoria de solo lectura 170 comprende unos registros que memorizan un programa de ordenar que comprende unas instrucciones de programa adaptadas, por una parte, para recibir unas órdenes de control procedentes del módulo sin contacto y para retransmitirlas a la tarjeta de abonado 20 y, por otra parte, para recibir de la tarjeta de abonado unas instrucciones de interfaz hombre máquina y para ejecutarlas.

El módulo de comunicación sin contacto 10 comprende de manera conocida un microprocesador 11, un módulo de emisión recepción 12 para la comunicación con el borne sin contacto 200, un módulo de emisión recepción 14 para la comunicación con la aplicación situada en el módulo seguro, un módulo de emisión recepción 16 para la comunicación con el terminal móvil, una memoria 15. Este comprende, además, un disparador 18. Cuando el

disparador 18 detecta un corte de campo magnético o cuando el módulo 16 recibe un mensaje de desconexión emitido por el borne 200, el microprocesador 11 provoca el envío de la información de detección de fin de transacción al terminal móvil.

- 5 El sistema también comprende un módulo seguro 20. Este módulo seguro 20 es, por ejemplo, una tarjeta de abonado que comprende, de manera conocida, en particular una unidad de tratamiento 21 equipada con un microprocesador, una memoria de solo lectura de tipo ROM 22, una memoria viva de tipo RAM 23, un módulo de emisión recepción 25 para comunicar con el terminal móvil 100 y el módulo sin contacto 10. La memoria de solo lectura 22 comprende unos registros que memorizan uno o varios programas de ordenador que comprende unas instrucciones de programa adaptadas para ejecutar una o varias aplicaciones (AP1, AP2,...). Esta también
- 10 comprende unos registros que memorizan un programa de ordenador que comprende unas instrucciones de programa adaptadas para aplicar un procedimiento de transmisión de un mensaje de acuerdo con la invención tal y como se ha descrito en referencia a las figuras 3 a 5. Este programa está de este modo adaptado para recibir una información de detección de fin de transacción de una aplicación, para determinar un mensaje que contiene una
- 15 información que identifica la aplicación y una información de fin de transacción, y para transmitir el mensaje determinado al terminal móvil.

- En la detección del fin de una transacción por el módulo sin contacto, el terminal móvil transmite una información de fin de transacción a la tarjeta de abonado y el programa (PG, PAP1) almacenado en la memoria de solo lectura 21 se transfiere a la memoria viva que contendría entonces el código ejecutable de la invención así como unos registros para memorizar las variables necesarias para la aplicación de la invención.
- 20

REIVINDICACIONES

1. Procedimiento de comunicación de un mensaje relativo a una transacción de una aplicación sin contacto (AP1) realizada entre un equipo (200) y un terminal móvil (100) equipado con un módulo sin contacto (10) y con un módulo seguro (20), encontrándose dicha aplicación almacenada en dicho módulo seguro, inicializándose dicha transacción mediante dicho equipo, comprendiendo dicho procedimiento las siguientes etapas:
- 5 - entrada del terminal móvil en un campo magnético emitido por el equipo;
- 10 - recepción por el módulo sin contacto, procedente del equipo, de un mensaje (MS) de selección que contiene un identificador (AID1) de la aplicación (AP1);
- transmisión del mensaje (MS) del módulo sin contacto (10) al módulo seguro (20);
- 15 - inicio de la aplicación (AP1) por el módulo seguro (20);
- intercambio de mensajes (M1, M2,..., Mn) entre la aplicación y el equipo;
- detección (E1) de fin de transacción entre le terminal y el equipo;
- 20 - tras la detección de fin de transacción, obtención (E2) mediante una interfaz hombre máquina (120) del terminal móvil (10) de un mensaje que contiene al menos una información que identifica dicha aplicación y una información de fin de transacción;
- 25 - comunicación (E3) de dicho mensaje en la interfaz hombre máquina del terminal móvil;
- caracterizado porque:
- 30 - la detección de fin de transacción se realiza mediante el módulo sin contacto; y
- la etapa de obtención (E2) comprende las siguientes etapas:
- 35 ■ envío (E210-E212, E-310-E312) del módulo sin contacto (10) al módulo seguro (20) de una información de detección de fin de transacción, permitiendo dicha información el inicio de un programa (PAP1) del módulo seguro;
- inicio de dicho programa (PAP1);
- 40 ■ determinación mediante dicho programa (PAP1) de dicho mensaje y transmisión (E-224, E-324) mediante el programa de dicho mensaje y de una instrucción de comunicación de dicho mensaje en la interfaz hombre máquina del terminal móvil.
2. Procedimiento de acuerdo con la reivindicación 1, en el cual el fin de transacción lo detecta el módulo sin contacto mediante un disparador integrado en dicho módulo sin contacto, produciéndose el fin de transacción por una ruptura del campo magnético.
- 45 3. Procedimiento de acuerdo con la reivindicación 1, en el cual el fin de transacción se detecta mediante la recepción por el módulo sin contacto de un mensaje de fin de transacción emitido por el equipo, manteniendo dicho equipo el campo magnético.
- 50 4. Procedimiento de acuerdo con la reivindicación 1, en el cual la información de detección de fin de transacción contiene el identificador (AID1) correspondiente a dicha aplicación (AP1) asociada a la transacción.
- 55 5. Procedimiento de acuerdo con una de las reivindicaciones 1 o 4, en el cual el módulo seguro es una tarjeta de abonado insertada en dicho terminal.
6. Procedimiento de acuerdo con una de las reivindicaciones anteriores, en el cual la información de fin de transacción comprende unos datos de la aplicación actualizados tras la ejecución de la transacción.
- 60 7. Procedimiento de acuerdo con una cualquiera de las reivindicaciones anteriores, en el cual la etapa de comunicación es una etapa de visualización de dicho mensaje en una pantalla del terminal móvil y/o una etapa de difusión de un mensaje de voz que contiene dicho mensaje por un altavoz del terminal móvil.
8. Procedimiento de acuerdo con la reivindicación 1, que comprende, además, la siguiente etapa, que lleva a cabo el módulo seguro:
- 65 - identificación (E214) de la aplicación (AP1).

9. Procedimiento de acuerdo con la reivindicación 8, en el cual la etapa de identificación comprende una etapa de lectura de un identificador memorizado durante dicha transacción.
- 5 10. Procedimiento de acuerdo con la reivindicación 8 o 9, en el cual la información de fin de transacción comprende unos datos de la aplicación actualizados tras la ejecución de la transacción.
11. Terminal móvil equipado con un módulo seguro y con un módulo sin contacto preparado para aplicar el procedimiento de comunicación de un mensaje de acuerdo con una de las reivindicaciones 1 a 10.
- 10 12. Sistema que comprende un terminal móvil de acuerdo con la reivindicación 11 y un equipo preparados para aplicar el procedimiento de las reivindicaciones 1 a 10.

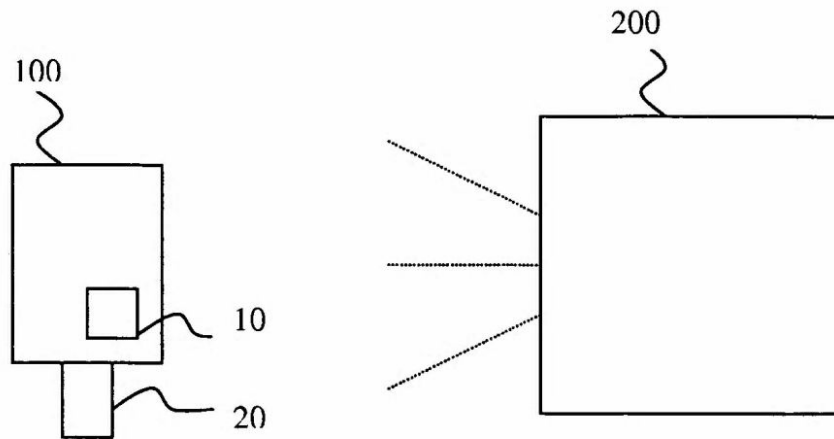


Figura 1

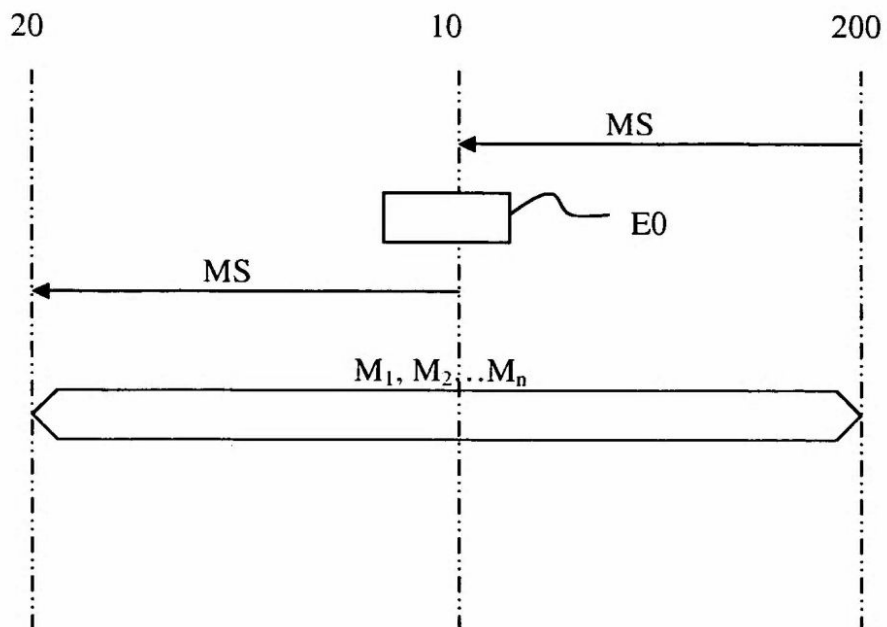


Figura 2

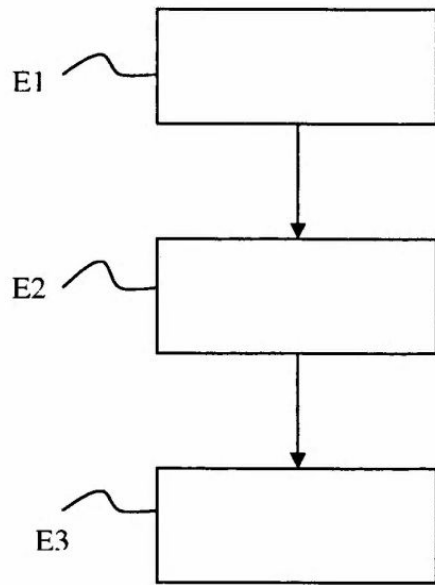


Figura 3

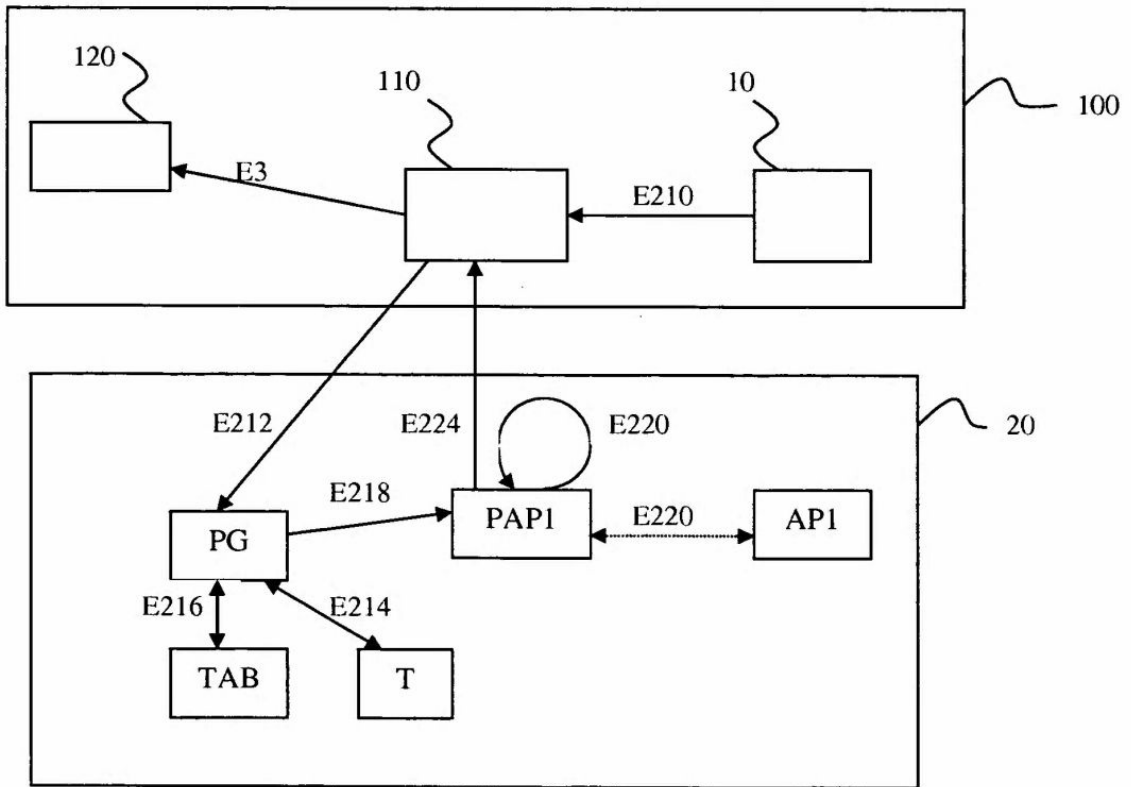


Figura 4

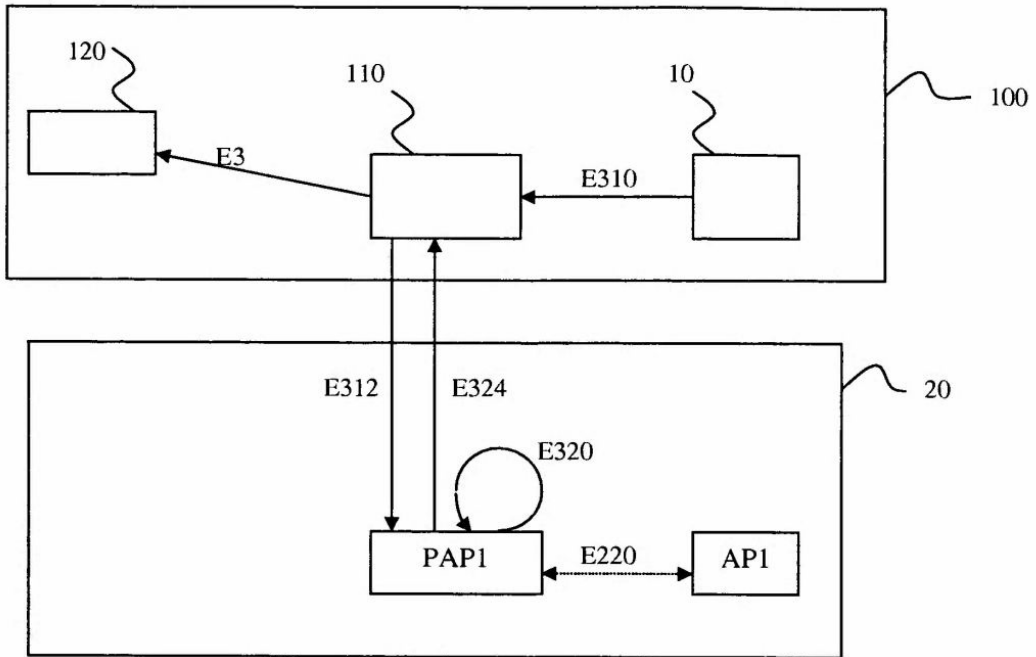


Figura 5

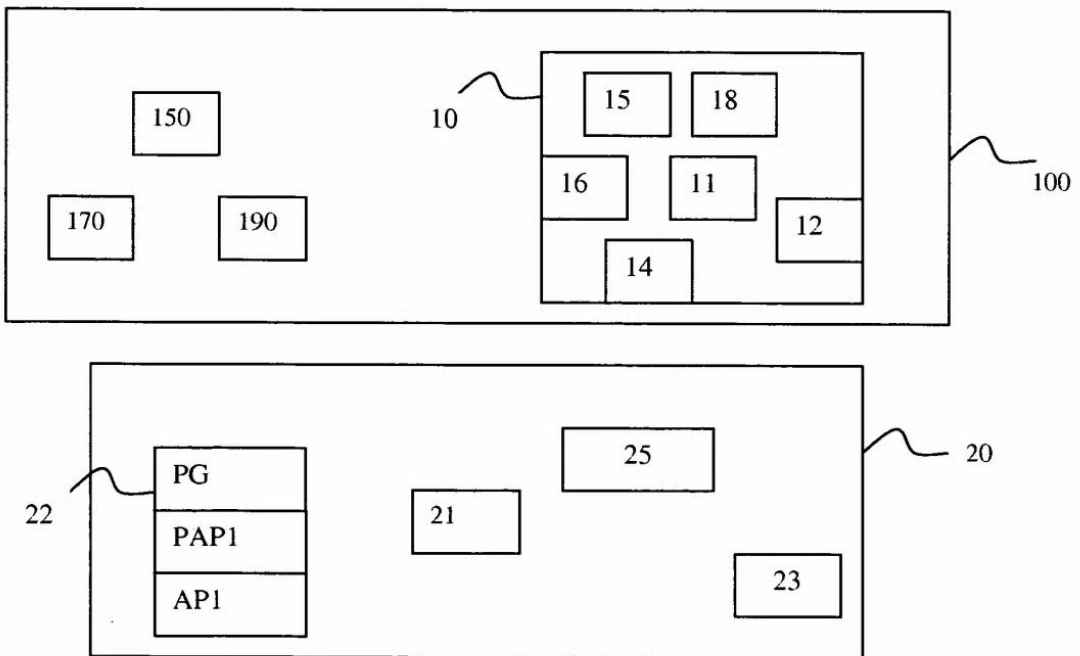


Figura 6