(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 267 569**

(51) Int. Cl.:
H04Q 7/32 (2006.01)
H04L 29/06 (2006.01)
H04Q 7/38 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Número de solicitud europea: **00966632 .2**
(86) Fecha de presentación : **19.09.2000**
(87) Número de publicación de la solicitud: **1224822**
(87) Fecha de publicación de la solicitud: **24.07.2002**

(54) Título: **Un aparato de comunicación portátil que tiene una interfaz hombre-máquina y un método para su funcionamiento.**

(30) Prioridad: **01.10.1999 SE 9903560**
26.05.2000 SE 0001996

(45) Fecha de publicación de la mención BOPI:
16.03.2007

(45) Fecha de la publicación del folleto de la patente:
16.03.2007

(73) Titular/es:
TELEFONAKTIEBOLAGET LM ERICSSON (publ)
164 83 Stockholm, SE

(72) Inventor/es: **Kiessling, Johan;**
Arwald, Jan;
Nilsson, Bernt y
Saxen, Benny

(74) Agente: **Elzaburu Márquez, Alberto**

DESCRIPCIÓN

Una aparato de comunicación portátil que tiene una interfaz hombre-máquina y un método para su funcionamiento.

Campo técnico

Hablando en general, la presente invención se refiere a un aparato de comunicación portátil para proporcionar servicios de comunicación a un usuario a través de una interfaz hombre-máquina del aparato. Más específicamente, la invención se refiere a un aparato de comunicación portátil del tipo que tiene un controlador, un sistema operativo, un dispositivo local de almacenamiento para almacenar una primera aplicación, un recurso seguro que sólo es accesible desde el sistema operativo y una interfaz inalámbrica para conectar el aparato de comunicación portátil a un dispositivo remoto.

Descripción de la técnica anterior

Ejemplos de un aparato de comunicación portátil según lo establecido arriba son un teléfono móvil, un teléfono inalámbrico, un asistente portátil digital, un comunicador, un dispositivo buscapersonas, un dispositivo de pago electrónico, o un dispositivo de navegación portátil. En el resto de este documento, se hará referencia a un teléfono móvil para cualquier red de comunicaciones móviles como GSM, EDGE o UMTS. Sin embargo, la invención no se limita meramente a un teléfono móvil. Por el contrario, la invención se define mejor por medio de las reivindicaciones independientes adjuntas.

Tradicionalmente, los teléfonos móviles antiguos sólo eran capaces de proporcionar comunicación de voz entre dos usuarios humanos a través de una red de comunicaciones móviles y, en muchas situaciones, una red telefónica pública conmutada. Más recientemente, los teléfonos móviles han sido dotados de funcionalidades adicionales, como la capacidad para proporcionar comunicación de datos o facsímil entre el aparato de comunicación portátil y otro dispositivo electrónico. Además, dichos teléfonos frecuentemente contienen aplicaciones de servicio simples, como una agenda de teléfonos, una calculadora, una función de alarma o un videojuego.

Incluso más recientemente, se han introducido para teléfonos móviles numerosas aplicaciones de servicio adicionales avanzadas. Tales aplicaciones de servicio avanzadas incluyen comunicación de datos suplementaria de corto alcance entre el teléfono móvil y, por ejemplo, un ordenador portátil, una impresora, un accesorio inalámbrico para auriculares, etc. Un ejemplo de dicha comunicación de datos suplementaria de corto alcance es denominado comúnmente Bluetooth y funciona en la banda de frecuencias de 2,4 GHz, a la que se hace frecuentemente referencia como ISM ("Instrumental, Científica y Médica").

Otros ejemplos de aplicaciones de servicio avanzadas son el pago electrónico inalámbrico ("monedero electrónico"), aplicaciones de tarjetas inteligentes (como las aplicaciones de juego de herramientas SIM), el acceso inalámbrico a redes globales (como el WAP-"Protocolo de Aplicaciones Inalámbricas" para acceder a recursos en Internet), etc.

Consecuentemente, un teléfono móvil de hoy en día, y por supuesto en el futuro, podrá realizar múltiples aplicaciones, que comparten recursos comunes del teléfono móvil. Los recursos comúnmente compartidos incluirán la interfaz hombre-máquina, particularmente una pantalla del teléfono móvil, pero también recursos seguros o privados, como información almacenada en una tarjeta SIM ("Módulo de Identificación del Suscriptor") u otra memoria del teléfono móvil. Estas aplicaciones se ejecutarán en diferentes entornos dentro del teléfono móvil, por ejemplo en un navegador WAP/Java/HTML ("Lenguaje de Marcas de Hipertexto"), un procesador en la tarjeta SIM u otro tipo de tarjeta inteligente, directamente en el sistema operativo del teléfono móvil, etc. Además, algunas aplicaciones pueden ejecutarse fuera del teléfono móvil en un dispositivo externo conectado al teléfono. Además, se pueden descargar aplicaciones en el teléfono móvil después de la fabricación del mismo.

Muchas de estas aplicaciones pueden ser activadas o lanzadas por eventos que se producen sin que el usuario tenga alcance a su control o atención inmediatos. En la mayoría de los casos, las aplicaciones se comunicarán con el usuario a través de la interfaz hombre-máquina del teléfono móvil, particularmente su pantalla. Debido al tamaño limitado de la pantalla, una aplicación activa frecuentemente tendrá control completo de toda la pantalla. Cuando se activa otra aplicación, ésta puede entonces puede tomar el control de la pantalla y otras partes de la interfaz hombre-máquina, como el teclado del teléfono móvil. Será difícil que el usuario note, entienda y maneje correctamente cambios repentinos entre dichas aplicaciones que se ejecutan en diferentes entornos dentro del teléfono móvil o en un dispositivo externo. Consecuentemente, será difícil para el usuario darse cuenta de que una aplicación de un origen diferente, de un tipo diferente, o en un entorno diferente tiene repentinamente el control de la interfaz hombre-máquina.

Además, una aplicación que se ejecuta en un entorno de baja seguridad podría imitar una aplicación que se ejecuta en un entorno de alta seguridad. Por ejemplo, una aplicación WAP podría fingir ser una aplicación basada en la SIM/tarjeta inteligente. Similarmente, una aplicación externa podría fingir ser una aplicación dentro del teléfono móvil.

Lo mencionado arriba constituye una preocupación particular si el usuario utiliza el teléfono móvil para efectuar algún tipo de transacción segura en nombre de él/ella basándose en los recursos seguros del teléfono móvil. Por ejemplo, si el teléfono móvil es utilizado como un dispositivo de pago electrónico inalámbrico, es extremadamente importante para el usuario saber, sin ninguna duda, con qué tipo de aplicación él/ella se está comunicando actualmente a través de la interfaz hombre-máquina, que la aplicación activa es fiable, y que la aplicación se está comunicando con seguridad y directamente con los recursos seguros del teléfono móvil y la interfaz hombre-máquina del mismo sin ningún riesgo de que otra aplicación interfiera, modifique o capte cualquier dato seguro implicado en la comunicación.

Desafortunadamente, en la mayoría de los entornos de aplicaciones de servicio para teléfonos móviles, las cuestiones de seguridad son sólo opcionales pero no obligatorias. Por ejemplo, características de seguridad como WTLS ("Seguridad de Capas de Transporte Inalámbricas") son sólo opcionales en WAP 1.1 y 1.2 y también WIM ("Módulo de Identidad Inalámbrico").

Además, las aplicaciones de datos suplementarias de corto alcance (como Bluetooth) se pueden activar a través de enlaces que se establecen repentinamente, si

el usuario lleva el teléfono móvil en las proximidades de un dispositivo remoto capaz de dicha comunicación.

En vista de lo mencionado arriba, cuando se trata de aplicaciones de servicio avanzadas, la única alternativa segura existente para un usuario de un teléfono móvil de acuerdo con lo dicho arriba es verificar el propio teléfono móvil así como su implementación de partes opcionales de los estándares de comunicación implicados, la tarjeta SIM/tarjeta inteligente proporcionada por el operador telefónico y, finalmente, la seguridad de cada nodo individual en el enlace de comunicación entre el teléfono móvil y un dispositivo remoto.

El artículo "Detección y gestión del fraude en redes de telecomunicaciones móviles" de P. Burge *et al* en la Conferencia Europea de Seguridad y Detección, 28-30 de Abril de 1997, Conf. Pub. Nº 437, páginas 91-96, describe varios métodos que pueden ser utilizados por operadores de redes para la detección del uso fraudulento de un teléfono móvil basándose en el análisis de los patrones de uso del teléfono móvil.

US 5,461,372 describe un sistema y un método para modificar los niveles de seguridad dentro de un sistema de seguridad. Se permiten modificaciones externas sólo si se aumenta la seguridad de un punto.

Compendio de la invención

Es un objetivo de la presente invención proporcionar una mejora sustancial de la situación descrita arriba, con énfasis particular en mantener al usuario informado de la situación de seguridad momentánea en el entorno de la aplicación del teléfono móvil.

El objetivo de arriba se ha conseguido, de acuerdo con la invención, proporcionando un indicador de seguridad, que sólo el sistema operativo del teléfono móvil es capaz de indicar al usuario a través de la interfaz hombre-máquina del teléfono. El indicador de seguridad, que se proporciona preferiblemente de forma visual en la pantalla del teléfono, pero que alternativamente se puede proporcionar como una señal audible o táctil, dota al usuario de cierta información acerca de la seguridad de la conexión entre un recurso seguro del teléfono móvil y una aplicación activa, que, o bien se ejecuta internamente en el teléfono, o bien se ejecuta en un dispositivo remoto conectado al teléfono. En ambos casos, la aplicación activa utilizará la interfaz hombre-máquina del teléfono móvil. El indicador de seguridad también puede indicar un tipo, origen o certificado de la aplicación activa. Además, puede indicar la localización de la ejecución para la aplicación activa.

La solución al objetivo de arriba se define por medio de las reivindicaciones independientes de la patente que se adjuntan. Otros objetivos, características y ventajas serán evidentes a partir de la siguiente descripción detallada, de las sub reivindicaciones así como de los dibujos adjuntos.

Descripciones breves de los dibujos

Ahora se describirán con mayor detalle realizaciones preferidas y alternativas de la invención, haciéndose referencia a los dibujos adjuntos, en los que:

La Fig. 1 es un diagrama de bloques esquemático de un aparato de comunicación portátil y un entorno de aplicaciones de servicio en el que puede funcionar,

La Fig. 2 es un diagrama de bloques del aparato de comunicación portátil mostrado en la Fig. 1, y

Las Figs. 3, 4a-4b, 5a-5c, 6 y 7 ilustran una parte de una interfaz hombre-máquina del aparato de comunicación portátil de acuerdo con diferentes realizaciones.

Descripción detallada de las realizaciones

En primer lugar se hace referencia a la Fig. 1, que ilustra un aparato de comunicación portátil en la forma de un teléfono 1 móvil, así como el entorno en el que éste funciona. Normalmente, el teléfono 1 móvil comprende una pantalla 2, un teclado 3, un altavoz 4, y un micrófono 5. Los componentes 2-5 juntos forman una interfaz hombre-máquina, a través de la cual el usuario del teléfono 1 móvil puede interaccionar con y manejar el teléfono móvil. Además, el teléfono 1 móvil comprende una primera antena 6 para establecer una conexión 9 inalámbrica con una red 11 de telecomunicaciones móviles a través de una estación 10 base. La red 11 de telecomunicaciones móviles puede ser una red GSM ("Sistema Global de comunicaciones Móviles"), EDGE ("Tasas de Datos Mejoradas para la evolución de GSM") o UMTS ("Sistema de Telecomunicaciones Móviles Universales"). El teléfono 1 móvil también se puede utilizar para acceder a una red 13 de información global, a través de una pasarela 12, a través del enlace 9 inalámbrico. La red 13 de información global puede ser preferiblemente Internet, y la pasarela 12 puede ser un servidor WAP.

El teléfono 1 móvil también comprende una segunda antena 7, que se puede utilizar para establecer una conexión 14 de datos suplementaria de corto alcance con un dispositivo 15 remoto. El enlace 14 puede ser preferiblemente un enlace Bluetooth, según se describe en las secciones previas de este documento. El dispositivo 15 remoto puede ser, por ejemplo, una impresora, un dispositivo facsímil, un accesorio (como unos cascos) de teléfono inalámbrico, un ordenador (por ejemplo, un ordenador de mesa estacionario o un ordenador portátil), pero también son posibles muchos otros dispositivos.

La segunda antena 7 también puede ser utilizada para establecer una conexión 16 de datos suplementaria de corto alcance con un sistema 18 de pago electrónico a través de la pasarela 17.

Además de lo mencionado arriba, el teléfono 1 móvil comprende además una interfaz 8 IR (infrarrojos), por medio de la cual el teléfono 1 móvil puede establecer un enlace 19 IR con un dispositivo 20 remoto. El dispositivo 20 remoto puede ser, por ejemplo, un ordenador (estacionario, portátil o de bolsillo), un módem, una impresora, etc.

En la Fig. 2, se muestra el teléfono 1 móvil de la Fig. 1 con mayor detalle. Como se ha mencionado previamente, el teléfono 1 comprende una interfaz hombre-máquina 21, que incluye la pantalla 2, el teclado 3, el altavoz 4 y el micrófono 5. Una unidad (CPU) 23 central de procesamiento es responsable del control global del teléfono 1 móvil junto con una memoria 24 y un sistema 25 operativo. La unidad 23 central de procesamiento puede ser implementada mediante cualquier microprocesador comercialmente disponible u otro tipo de circuitería electrónica programable. La memoria 24 puede ser implementada como una memoria (RAM) de acceso aleatorio, una memoria (ROM) de sólo lectura, una memoria (EPROM, EEPROM) programable de sólo lectura que se puede borrar eléctricamente, una memoria flash, o cualquier combinación de dichas memorias. Preferiblemente, el sistema 25 operativo se almacena en una parte de la memoria 24.

El teléfono 1 móvil también tiene un módulo 33

SIM, preferiblemente en la forma de una tarjeta inteligente en la que se almacenan datos privados acerca de una suscripción a telefonía móvil para la red 11 de comunicaciones móviles. La tarjeta 33 SIM también puede comprender una o una pluralidad de aplicaciones de juego de herramientas SIM.

El teléfono 1 móvil también tiene circuitería 30 de radio, que se utilizará en combinación con la primera antena 6 para establecer el enlace 9 inalámbrico de la Fig. 1. Similarmente, el teléfono 1 móvil comprende circuitería 31 para una conectividad de datos suplementaria de corto alcance, que se utilizará para establecer los enlaces 14 ó 16 a través de la segunda antena 7 de la Fig. 1. La circuitería 31 puede, por ejemplo, estar adaptada para la comunicación Bluetooth. Adicionalmente, el teléfono móvil comprende circuitería 32 IR, que se utilizará para establecer un enlace 19 de infrarrojos con el dispositivo 20 remoto mostrado en la Fig. 1. La circuitería 32 IR puede preferiblemente estar adaptada para la comunicación IrDA. La circuitería 30 de radio, la circuitería 31 de datos suplementaria de corto alcance y la circuitería 32 IR son ya comercialmente disponibles, no forman parte central de la presente invención y por tanto no se describen con detalle en el presente documento.

También se indica en la Fig. 2 un módulo 29 de confianza, que puede implicar claves privadas, datos secretos, etc., para utilizar junto con un módulo WIM ("Módulo de Identidad Inalámbrico"), que se utiliza en aplicaciones WAP. El módulo 29 de confianza también puede estar relacionado con un módulo SWIM, por ejemplo, un módulo WIM implementado en la tarjeta 33 SIM. En algunas realizaciones, el módulo 29 de confianza puede estar almacenado en la memoria 24.

La Fig. 2 también contiene una indicación de una estructura de protocolo que se utiliza para los diferentes enlaces 9, 14, 16 y 19 inalámbricos de la Fig. 1. La estructura de protocolo esencialmente sigue la bien conocida estructura OSI de siete capas. En la base de la estructura de protocolo se proporciona una primera y una segunda capas 34 de banda base para el enlace 9 inalámbrico con la red 11 de telecomunicaciones móviles y la red 13 global (Internet). Además, se proporciona una primera y una segunda capas 35 de banda base correspondientes para la circuitería 31 Bluetooth y la circuitería 31 IR.

A continuación, en un tercer nivel, se proporciona una capa de red, como IP mediante PPP ("Protocolo de Internet", "Protocolo de Igual a Igual"). Se proporciona una capa 37 de transporte en el nivel 4. La capa de transporte puede ser, por ejemplo, TCP ("Protocolo de Control de Transporte"), UDP ("Protocolo de Datagramas de Usuario") o WDP ("Protocolo de Datagramas Inalámbrico").

En la capa 5 se proporciona una capa 38 de sesión WAP, que comprende, por ejemplo, WSP ("Protocolo de Sesión Inalámbrica"), o WAE ("Entorno de Aplicaciones Inalámbricas"). Se supone que todos los protocolos, que se han mencionado con respecto de las capas 34, 35, 36, 37 y 38 de arriba son bien conocidos en el campo técnico y no se describen con detalle en el presente documento.

En un sexto nivel se proporciona un protocolo 39 de seguridad, por ejemplo, SMT ("Transacción Móvil Segura"). SMT es un protocolo de seguridad a un nivel de aplicación, que está dirigido a las limitaciones en la comunicación con un dispositivo móvil personal. Actualmente, SMT está en desarrollo y por tanto todavía no es un estándar.

La estructura de protocolo descrita arriba es capaz de dar servicio a una pluralidad de aplicaciones, que se ejecutan en diferentes entornos dentro y fuera del teléfono 1 móvil. Consecuentemente, una primera aplicación 26 se puede comunicar directamente con la capa 37 de transporte y la interfaz 21 hombre-máquina. La aplicación 26 se almacena preferiblemente en la memoria 24 y es ejecutada por la unidad 23 central de procesamiento bajo el sistema 25 operativo. Adicionalmente, una segunda aplicación 27 se puede comunicar con la capa 38 WAP o la capa 39 de seguridad y la interfaz 21 hombre-máquina. Correspondientemente, la aplicación 27 puede ser almacenada en la memoria 24 y ser ejecutada por la unidad 23 central de procesamiento bajo el sistema 25 operativo. Alternativamente, las aplicaciones 26 y/o 27 se pueden almacenar en la tarjeta 33 SIM o en el módulo 29 de confianza.

El teléfono 1 móvil también puede dar servicio a una aplicación 28 externa, que está situada en un dispositivo remoto. Un dispositivo remoto como este puede ser, por ejemplo, cualquiera de los dispositivos 11, 12, 13, 15, 17, 18 ó 20 indicados en la Fig. 1. Una aplicación 28 externa como esta se comunicará con el teléfono 1 móvil a través de cualquiera de los enlaces 9, 14, 16 ó 19 inalámbricos (es decir, radio, de datos suplementario de corto alcance o infrarrojos). El usuario interaccionará con la aplicación 28 externa a través de la interfaz 21 hombre-máquina del teléfono 21 móvil.

Para resolver el objetivo arriba mencionado de la invención, el teléfono móvil está dotado de un indicador 22 de seguridad, que es parte de la interfaz 1 hombre-máquina y que sólo es controlable desde el sistema 25 operativo. Más particularmente, una aplicación 26, 27, 28 sólo puede afectar al indicador 22 de seguridad a través de ciertas llamadas de sistema operativo al sistema 25 operativo. Por tanto, ninguna aplicación puede modificar el indicador 22 de seguridad sin la cooperación y consentimiento del sistema 25 operativo. De acuerdo con diferentes realizaciones de la invención, el indicador 22 de seguridad comprende uno o más de un icono (22a en la Fig. 3) gráfico especial, que preferiblemente reside en una porción diferente de la pantalla 2 y que sólo puede ser actualizado por el sistema 25 operativo a través de las antes mencionadas llamadas de sistema operativo. Alternativamente, se puede proporcionar el indicador de seguridad como un carácter alfanumérico especial o como un mensaje (22b en la Fig. 4a) de texto especial, con un color o tamaño de fuente (22c en la Fig. 4b) especiales diferentes de los mensajes (42 y 43 en la Fig. 3) de texto normales presentados en la pantalla 2. Los iconos 40 y 41 de la Fig. 3 son indicadores convencionales de la potencia de la señal y la capacidad de la batería, respectivamente.

Como una alternativa a los tipos de indicador de seguridad de arriba, se puede proporcionar el indicador 22 de seguridad como una señal audible a través del altavoz 4 del teléfono 1 móvil. Como una alternativa más, el indicador de seguridad se puede proporcionar como una señal táctil (preferiblemente una señal vibratoria) generado por otros medios del teléfono 1 móvil.

El objetivo del indicador 22 de seguridad es proporcionar información al usuario acerca de un nivel

actual de seguridad en lo que respecta a una aplicación activa que se está comunicando actualmente con el usuario a través de la interfaz 21 hombre-máquina. Como el indicador 22 de seguridad sólo puede ser controlado desde el sistema 25 operativo, el usuario puede confiar en la información proporcionada por el indicador de seguridad. De acuerdo con una realización, el indicador de seguridad puede indicar un tipo, nivel de seguridad, u origen de una aplicación activa, con la que el usuario se está comunicando actualmente a través de la interfaz 21 hombre-máquina. Por ejemplo, como se muestra en la Fig. 5a, el indicador 22d de seguridad puede indicar que la aplicación activa es local (almacenada y ejecutada dentro del teléfono 1 móvil). Correspondientemente, una aplicación externa almacenada y/o ejecutada en un dispositivo remoto fuera del teléfono 1 puede ser indicada a través del indicador 22e de seguridad (Fig. 5b). Como se muestra en la Fig. 5c, el indicador 22f de seguridad puede indicar un tipo más detallado de la aplicación activa, por ejemplo, que es una aplicación de un juego de herramientas SIM. El indicador de seguridad también puede indicar que la aplicación activa se ejecuta en un navegador WAP/Java/HTML.

Alternativamente, el indicador 22g de seguridad puede indicar que la aplicación activa está certificada de algún modo (Fig. 6). El indicador de seguridad también puede indicar una conmutación desde una aplicación previamente activa a una aplicación actualmente activa.

De acuerdo con algunas realizaciones, el indicador de seguridad puede indicar si la aplicación activa fue proporcionada al teléfono 1 móvil ya en la fabricación del mismo, o si la aplicación activa se ha descargado en el teléfono 1 en un momento posterior.

Si la aplicación actualmente activa es una aplicación externa, el indicador 22 de seguridad puede representar el nivel de seguridad del enlace entre el teléfono 1 móvil y el dispositivo remoto, donde reside la aplicación externa. El nivel de seguridad se puede entonces indicar ventajosamente de un modo gráfico, como se indica mediante el icono 22a de la Fig. 3. Tres símbolos de llave en el icono 22a representa un alto nivel de seguridad, mientras que dos símbolos de llave representa una seguridad de nivel medio, sólo un símbolo de llave representa una seguridad de bajo nivel y, finalmente, ningún símbolo de llave representa una seguridad nula.

El indicador de seguridad (22h en la Fig. 7) también puede proporcionar una indicación acerca del tipo de enlace entre el teléfono 1 móvil y un dispositivo remoto, como un enlace (14, 16) Bluetooth, un enlace (19) de infrarrojos o un enlace (9) de radio. Además, el indicador 22 de seguridad puede indicar que una transacción que está siendo actualmente efectuada por la aplicación activa es atómica en el sentido de que la transacción no puede ser interrumpida, manipulada o interpretada por ninguna otra aplicación que no sea la aplicación activa. El indicador 22 de seguridad también podría indicar parámetros importantes de dicha transacción segura, como la longitud de la clave para un método de encriptado, etc.

Además de lo mencionado arriba, el indicador 22 de seguridad puede indicar si cualquiera de los enlaces 9, 14, 16 o 19 inalámbricos está establecido actualmente, un estado del mismo, o una calidad (potencia de la señal, etc) física de dicho enlace establecido.

Para resumir lo mencionado arriba, en su forma general, la presente invención proporciona un indicador de seguridad a través de la interfaz hombre-máquina de un aparato de comunicación portátil, donde el indicador de seguridad representa una seguridad de una conexión entre un recurso seguro del aparato de comunicación portátil y una aplicación activa, que está actualmente utilizando la interfaz hombre-máquina. El término recurso seguro se debe interpretar con amplitud y cubre, entre otras cosas, una cierta parte del teléfono 1 móvil (por ejemplo, su interfaz 21 hombre-máquina), claves privadas u otros datos seguros almacenados en el teléfono móvil, por ejemplo, en el módulo 29 de confianza, la memoria 24 o la tarjeta 33 SIM.

La presente invención se ha descrito arriba haciendo referencia a algunas realizaciones. Sin embargo, son igualmente posibles otras realizaciones diferentes de las referidas arriba dentro del alcance de la invención, que está definido por las reivindicaciones independientes adjuntas.

REIVINDICACIONES

1. Un aparato (1) de comunicación portátil que tiene una interfaz (2-5, 21) hombre-máquina, un controlador (23), un sistema (25) operativo, un dispositivo (24) de almacenamiento local para almacenar una primera aplicación (26, 27), un recurso (29, 33) seguro que sólo es accesible desde el sistema operativo, y una interfaz (6, 7, 30-32) inalámbrica para conectar el aparato de comunicación portátil a un dispositivo (10, 12, 15, 17, 20) remoto, donde la interfaz hombre-máquina está adaptada para proporcionar una interacción entre un usuario del aparato de comunicación portátil y la primera aplicación cuando es ejecutada por el controlador y el sistema operativo, y donde la interfaz hombre-máquina también está adaptada para proporcionar una interacción entre el usuario y una segunda aplicación (28) almacenada y/o ejecutada en el dispositivo remoto, **caracterizado** porque

el sistema (25) operativo y sólo el sistema operativo está adaptado para proporcionar un indicador (22) de seguridad a través de la interfaz (2-5, 21) hombre-máquina, donde el indicador de seguridad indica un nivel actual de seguridad de una aplicación activa de entre dichas primera y segunda aplicaciones (26-28) que están actualmente utilizando la interfaz hombre-máquina.

2. Un aparato de comunicación portátil de acuerdo con la reivindicación 1, donde el indicador (22) de seguridad indica un tipo, origen o certificado de dicha aplicación activa de entre dichas primera y segunda aplicaciones (26-28) que están actualmente utilizando la interfaz hombre-máquina.

3. Un aparato de comunicación portátil de acuerdo con la reivindicación 1 ó 2, donde el aparato de comunicación portátil incluye una pantalla (2) adaptada para presentar el indicador (22) de seguridad.

4. Un aparato de comunicación portátil de acuerdo con la reivindicación 3, donde el indicador (22) de seguridad comprende al menos un icono (22a) predeterminado.

5. Un aparato de comunicación portátil de acuerdo con la reivindicación 3, donde el indicador (22) de seguridad comprende un mensaje (22b) de texto predeterminado.

6. Un aparato de comunicación portátil de acuerdo con la reivindicación 5, donde dicho mensaje (22c) de texto predeterminado tiene un tipo de fuente, tamaño o color que es diferente de los otros mensajes de texto presentados en la pantalla (2).

7. Un aparato de comunicación portátil de acuerdo con cualquiera de las reivindicaciones 3-6, donde el indicador (22d, 22e) de seguridad indica si dicha aplicación activa de entre dichas primera y segunda aplicaciones (26-28) que está actualmente utilizando la interfaz (2-5, 21) hombre-máquina, es ejecutada localmente en el aparato de comunicación portátil o es ejecutada externamente al aparato de comunicación portátil.

8. Un aparato de comunicación portátil de acuerdo con cualquiera de las reivindicaciones 3-7, donde el indicador (22d, 22e) de seguridad indica si dicha aplicación activa de entre dichas primera y segunda aplicaciones (26-28) que está actualmente utilizando la interfaz (2-5, 21) hombre-máquina, estaba originalmente almacenada en dicho dispositivo (24) de almacenamiento local cuando el aparato de comunicación portátil fue fabricado, o se origina desde dicho dispositivo (12) remoto.

9. Un aparato de comunicación portátil de acuerdo con cualquier reivindicación precedente, donde el indicador (22h) de seguridad comprende una indicación de un tipo de una conexión (9, 14, 16, 19) entre el aparato de comunicación portátil y el dispositivo (10, 12, 15, 17, 20) remoto.

10. Un aparato de comunicación portátil de acuerdo con la reivindicación 9, donde dicha conexión (14, 16) es una conexión de datos suplementaria de corto alcance, como Bluetooth.

11. Un aparato de comunicación portátil de acuerdo con cualquier reivindicación precedente, donde el indicador (22) de seguridad comprende una señal audible a través de la interfaz (4, 21) hombre-máquina.

12. Un aparato de comunicación portátil de acuerdo con cualquier reivindicación precedente, donde el indicador (22) de seguridad comprende una señal táctil a través de la interfaz (21) hombre-máquina.

13. Un aparato de comunicación portátil de acuerdo con cualquier reivindicación precedente, **caracterizado** porque el aparato está capacitado para la telecomunicación móvil.

14. Un aparato de comunicación portátil de acuerdo con cualquier reivindicación precedente, donde el indicador (22) de seguridad comprende una indicación de si existe actualmente un enlace entre el aparato de comunicación portátil y un dispositivo (10, 12, 15, 17, 20) remoto.

15. Un aparato de comunicación portátil de acuerdo con cualquier reivindicación precedente, donde el indicador (22) de seguridad comprende una indicación de la calidad física de un enlace de dicha conexión segura.

16. Un aparato de comunicación portátil de acuerdo con cualquier reivindicación precedente, donde el indicador (22) de seguridad comprende una indicación acerca de que una transacción que está siendo actualmente efectuada por dicha aplicación activa de entre dichas primera y segunda aplicaciones no puede ser interrumpida, manipulada o interpretada por ninguna otra aplicación diferente de dicha aplicación activa de entre dichas primera y segunda aplicaciones (26-28) que están actualmente utilizando la interfaz (2-5, 21) hombre-máquina.

17. Un método para manejar una interfaz (2-5, 21) hombre máquina de un aparato (1) de comunicación portátil de acuerdo con la reivindicación 1, **caracterizado** por las operaciones de:

proporcionar el indicador (22) de seguridad en la interfaz (2-5, 21) hombre-máquina,

proporcionar una llamada de sistema operativo para llamar al indicador (22) de seguridad de, al menos, una aplicación de entre dichas primera y segunda aplicaciones (26-28),

proporcionar información acerca de un nivel actual de seguridad de una aplicación activa de entre dichas primera y segunda aplicaciones (26-28) que está actualmente utilizando la interfaz (2-5, 21) hombre-máquina, al recibir dicha llamada del sistema operativo, y

incluir dicha información en dicho indicador (22) de seguridad.

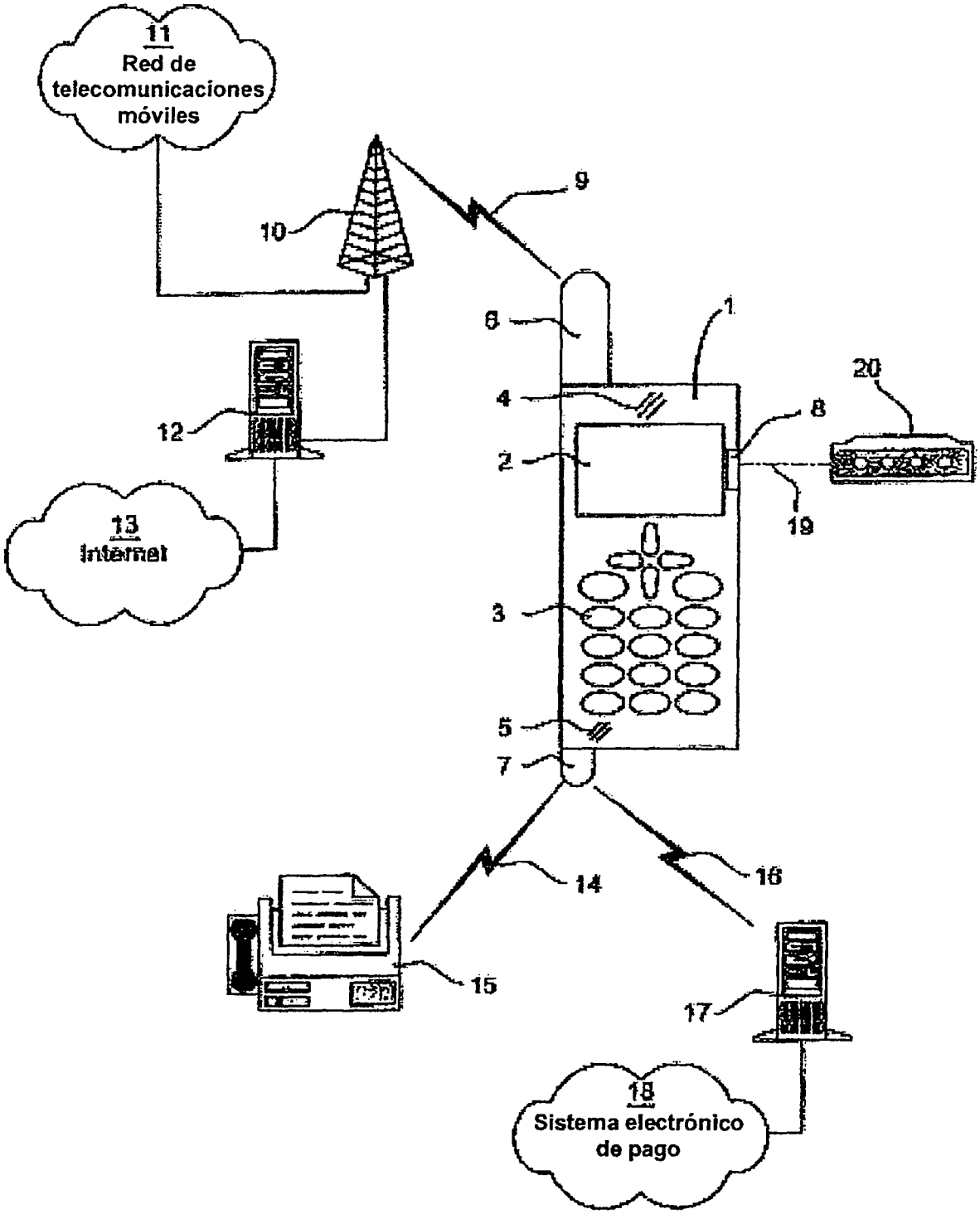
11
Red de telecomunicaciones móviles
10
9
6
1
20
4
8
12
2
19
13
Internet
3
5
7
14
16
15
17
18
Sistema electrónico de pago

Fig 1

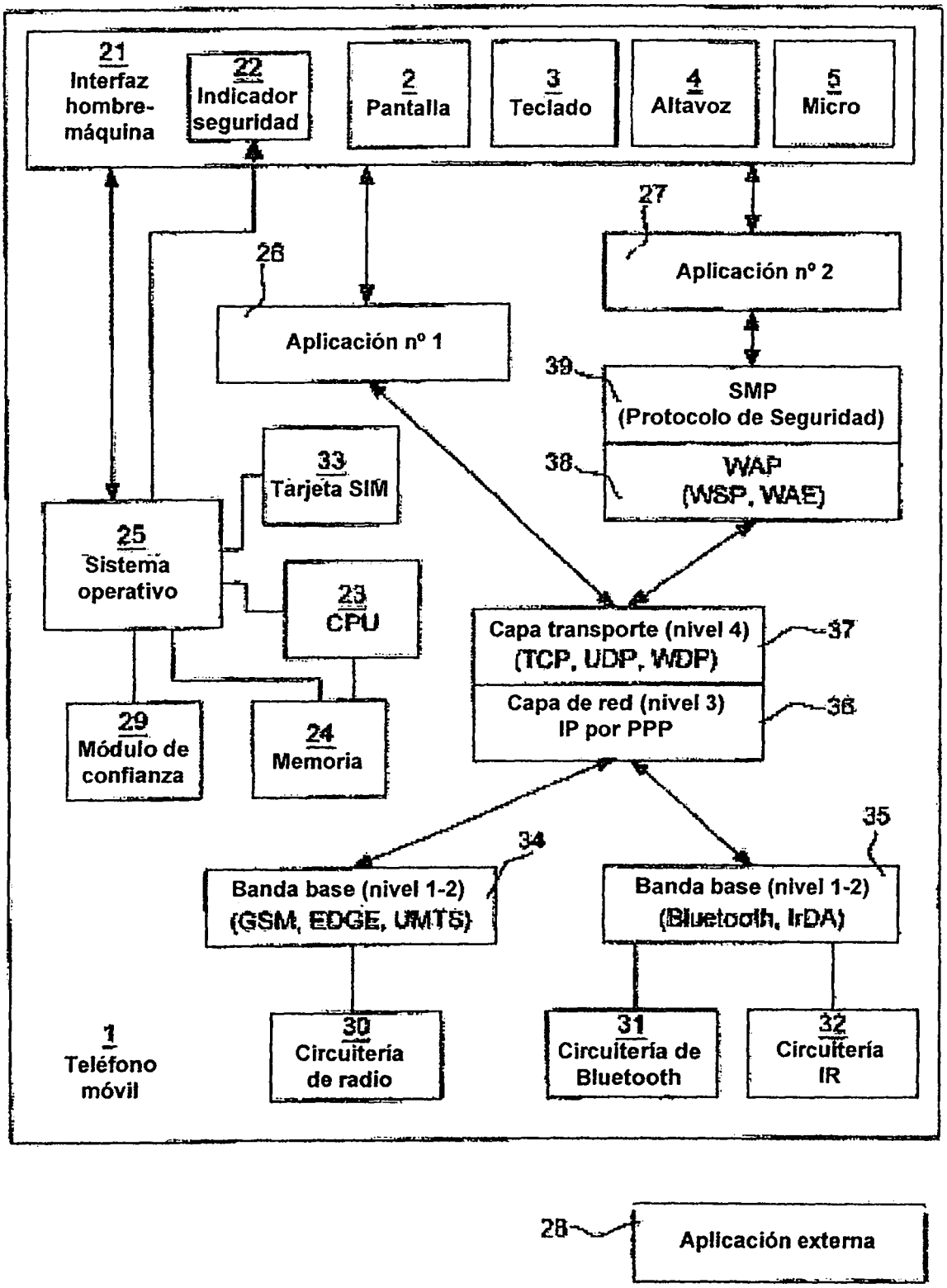
21
Interfaz hombre-máquina
22
Indicador seguridad
2
Pantalla
3
Teclado
4
Altavoz
5
Micro
27
Aplicación nº 2
26
Aplicación nº 1
39
SMP
(Protocolo de Seguridad)
38
WAP
(WSP, WAE)
33
Tarjeta SIM
25
Sistema operativo
23
CPU
Capa transporte (nivel 4)
(TCP, UDP, WDP)
37
Capa de red (nivel 3)
IP por PPP
36
29
Módulo de confianza
24
Memoria
35
34
Banda base (nivel 1-2)
(GSM, EDGE, UMTS)
Banda base (nivel 1-2)
(Bluetooth, IrDA)
1
Teléfono móvil
30
Circuitería de radio
31
Circuitería de Bluetooth
32
Circuitería IR
28
Aplicación externa

Fig 2

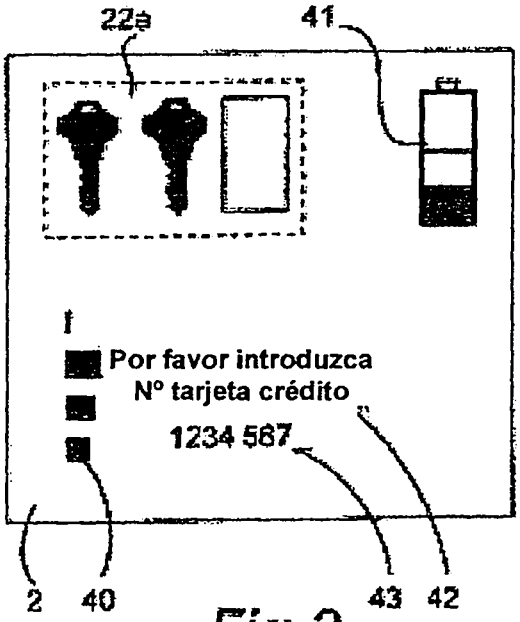

Fig 3

Fig 4a

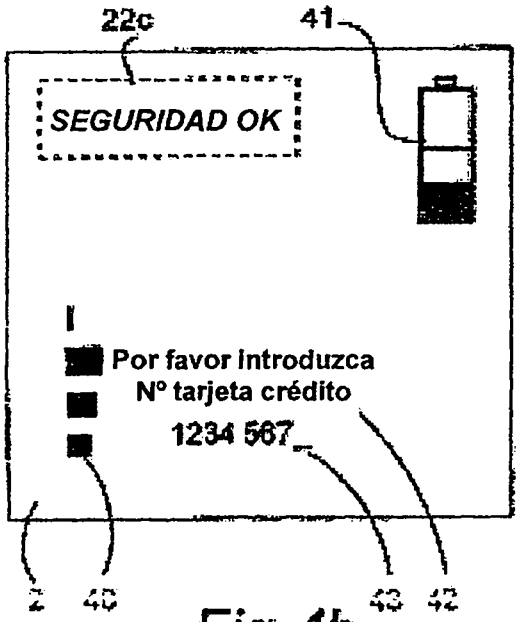

Fig 4b

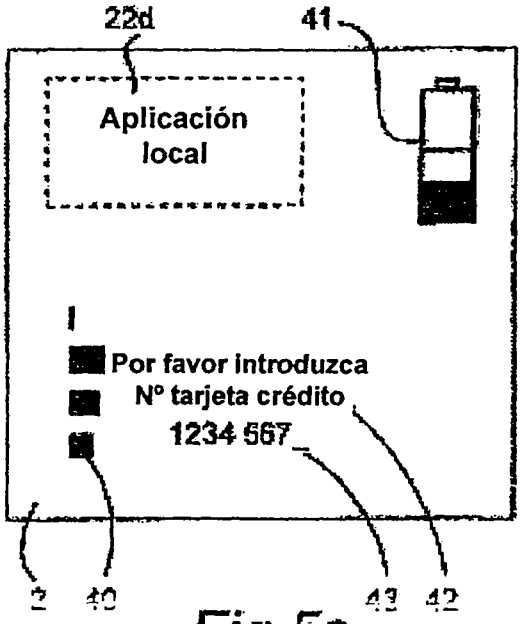

Fig 5a

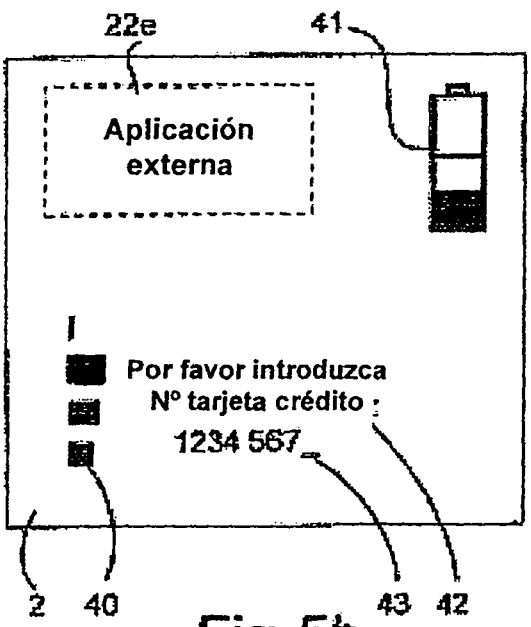

Fig 5b

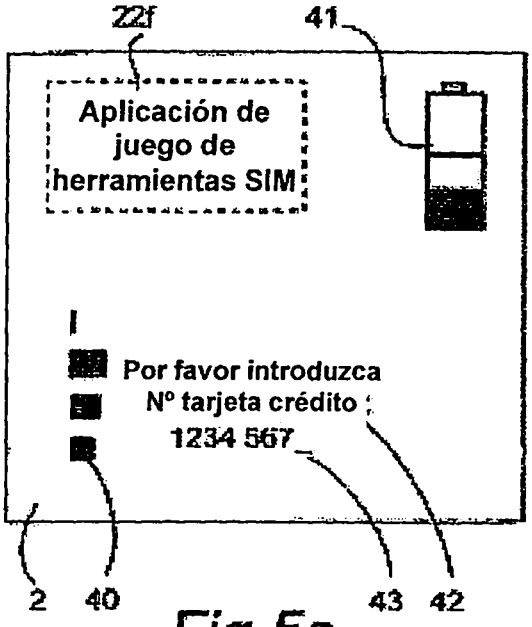

Fig 5c

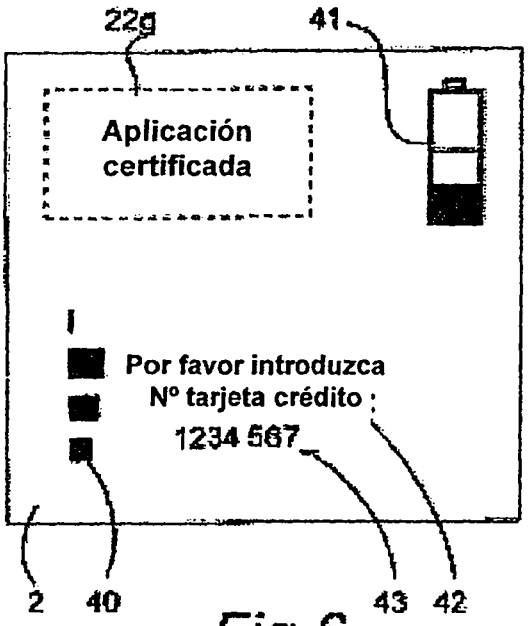

Fig 6

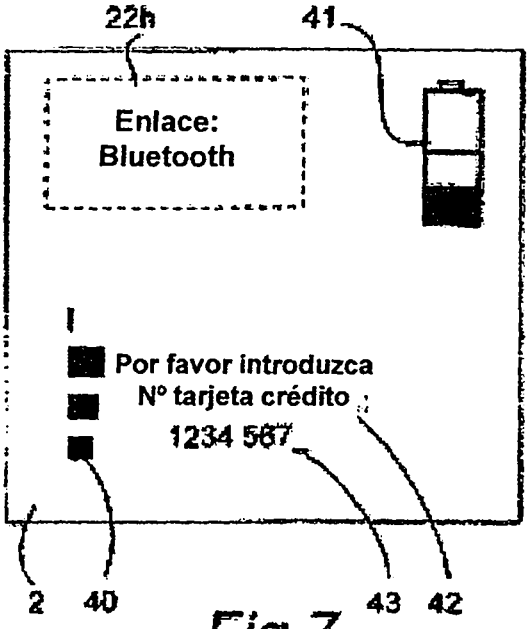

Fig 7