



19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA

11 Número de publicación: **2 353 062**

51 Int. Cl.:
G07F 7/10 (2006.01)
G07F 19/00 (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Número de solicitud europea: **04075996 .1**
96 Fecha de presentación : **26.04.1996**
97 Número de publicación de la solicitud: **1460594**
97 Fecha de publicación de la solicitud: **22.09.2004**

54 Título: **Un dispositivo para interacción transparente entre una tarjeta de CI y un terminal remoto.**

30 Prioridad: **28.04.1995 NL 1000254**
17.01.1996 NL 1002112

45 Fecha de publicación de la mención BOPI:
25.02.2011

45 Fecha de la publicación del folleto de la patente:
25.02.2011

73 Titular/es: **KONINKLIJKE KPN N.V.**
Maanplein 55
2516 CK The Hague, NL

72 Inventor/es: **Pieterse, Rob;**
Van Pomerén, Frank Pieter;
Van Tilburg, Johan;
Pors, Mark Albert y
De Lange, Martin Klaas

74 Agente: **Justo Bailey, Mario de**

ES 2 353 062 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).

DESCRIPCION

ANTECEDENTES DE LA INVENCION

La invención se refiere a un dispositivo para la interacción entre una tarjeta de CI y un terminal remoto.

5 Más en particular, la invención se refiere a un dispositivo que permite una interacción directa entre una tarjeta de CI y un terminal remoto, usando un sistema de comunicaciones.

En la actualidad, hay una demanda creciente de servicios remotos. Así, a través de la televisión se
10 ofrecen diversos productos y servicios que los consumidores pueden encargar a domicilio. Tales servicios incluyen "vídeo bajo demanda" (VOD), compras por teléfono y actividades de ocio por teléfono. Los consumidores quieren una entrega rápida de los productos encargados o un acceso
15 rápido a los servicios de ocio, tales como vídeo bajo demanda. Para impedir el mal uso de este tipo de servicios, o bien se debe efectuar un pago inmediato, o bien se debe verificar la identidad del usuario, antes de realizar el servicio.

20 Las tarjetas de CI o tarjetas inteligentes se usan ampliamente en la actualidad para efectuar pagos por ejemplo en teléfonos públicos (teléfonos de monedas). Una tarjeta de CI contiene un circuito integrado (CI) con una memoria y, en las tarjetas más avanzadas, también un
25 microprocesador. Las tarjetas de este tipo permiten realizar pagos deduciendo una cantidad que se va a pagar de un saldo en la tarjeta. En las tarjetas avanzadas, tales pagos se aseguran mediante protocolos que implican el procesamiento criptográfico de ciertos datos y el uso de
30 claves asociadas. Con respecto a esto, se hace referencia

por ejemplo a los documentos EP 0637004 y US 5247578.

Las tarjetas de CI avanzadas también permiten establecer la identidad de la tarjeta, por ejemplo transmitiendo un número de identidad de tarjeta (procesado
5 criptográficamente). Si el acceso a la tarjeta está protegido por medio de, por ejemplo, un número de identificación personal (PIN) secreto, la tarjeta se puede emplear para la verificación del usuario, es decir para establecer de forma segura la identidad del usuario. Una
10 verificación del usuario de este tipo, no sólo es necesaria cuando se desea un servicio rápido, sino también cuando se llevan a cabo transacciones de pago sin una entrega instantánea de un servicio o producto de una manera remota (por ejemplo telebanco).

15 Actualmente, existen sistemas de pago, tal como los sistemas con tarjeta de crédito, con los que se envía información del pago a una organización de pagos a través de un aparato telefónico. Para este tipo de transacciones, el aparato telefónico en cuestión está adaptado
20 especialmente con un lector de tarjetas y, opcionalmente, con un teclado. Los dispositivos de este tipo tienen la desventaja de que son relativamente caros. No es de esperar que un gran número de consumidores compren un dispositivo de este tipo en un futuro inmediato.

25 Además, se conoce en la práctica comunicar, a través de un aparato telefónico convencional, un número de tarjeta de crédito de una manera oral. Esto tiene la desventaja de que terceras partes (por ejemplo infiltrándose en la conexión telefónica) puedan hacer mal uso del número
30 fácilmente.

Se conocen de la técnica anterior varios dispositivos para comunicarse con una tarjeta de CI. El documento US 5189287, por ejemplo, da a conocer un sistema para transmitir datos. El sistema comprende unidades portátiles, dotadas cada una de una ranura de tarjeta para alojar una tarjeta de memoria de doble chip en la que se almacenan datos, y transceptores ópticos y acústicos para intercambiar información con terminales ópticos especiales y con sistemas remotos a través de una red telefónica, respectivamente. Las unidades comprenden medios de procesamiento, tales como un microprocesador, para procesar datos que se pueden introducir manualmente usando un teclado.

El documento WO 95/04328 también da a conocer un dispositivo para comunicarse con una tarjeta de CI. Este dispositivo de la técnica anterior comprende un microordenador y un sistema operativo asociado, dispuestos para ejecutar programas de aplicación. El dispositivo está dispuesto para el procesamiento y almacenamiento de datos financieros, comprendiendo el procesamiento el procesamiento criptográfico de los datos.

El documento WO 91/07042 da a conocer un cajero automático portátil. El dispositivo, que comprende un microprocesador, opera sin necesidad de conexión directa a una línea telefónica y por tanto, es básicamente una unidad independiente.

El documento EP 0451288 da a conocer un dispositivo portátil de recogida y transmisión de datos para su uso con una tarjeta de CI. El dispositivo, que comprende un acoplador acústico para comunicarse a través de una línea

telefónica, comprende además una memoria para almacenar datos. De esta manera se pueden transmitir datos almacenados.

5 El documento WO 94/28498 da a conocer un dispositivo para comunicarse con una tarjeta de CI. El dispositivo no tiene medios acústicos para comunicarse con un aparato telefónico, sino que necesita una conexión separada a una línea de abonado.

10 Estos dispositivos de la técnica anterior son básicamente unidades independientes, dotadas de un microprocesador o similar para procesar datos de manera independiente de un terminal o sistema remoto.

15 El documento WO 92/21110 da a conocer un dispositivo para su uso en un sistema para la verificación del usuario electrónica y/o transacciones de pago electrónicas. El sistema comprende una red de telecomunicaciones, un proveedor de servicios que está acoplado a la red, proveedor de servicios que está dispuesto para llevar a cabo servicios electrónicos y/u órdenes de pago
20 electrónico, un aparato de comunicaciones y una tarjeta de CI electrónica que está dispuesta para transacciones seguras. El dispositivo está dispuesto para intercambiar datos entre la tarjeta de CI y el proveedor de servicios. Comprende: medios de conexión para su conexión con la
25 tarjeta de CI y medios de control para controlar la transferencia de los datos dentro del dispositivo. El dispositivo está dispuesto para transferir los datos sin alterar el contenido de los mismos. El dispositivo está conectado en paralelo con un aparato telefónico a una
30 clavija de teléfono normal a través de un enchufe adaptador

convencional.

El documento WO 94/07217 da a conocer un dispositivo para realizar transacciones monetarias con tarjetas inteligentes tales como tarjetas bancarias que comprende, en un alojamiento un acoplador para tarjetas inteligentes, una ranura ubicada en el acoplador para la inserción parcial de una tarjeta inteligente, un teclado para introducir al menos un código confidencial asociado con una tarjeta insertada en el medio de acoplador para procesar y validar la transacción. Según la invención, la ranura es adyacente a un borde del teclado, y el acoplador y la ranura están colocados de modo que una parte (CAM2) de la tarjeta que permanece fuera del alojamiento tras la inserción parcial se extiende al menos parcialmente por encima del teclado, formando de esta manera una pantalla durante la introducción del código para proteger su confidencialidad.

SUMARIO DE LA INVENCION

Un objeto de la invención es eliminar las desventajas mencionadas anteriormente y otras de la técnica anterior y proporcionar un dispositivo que permita llevar a cabo un intercambio de información protegido de una manera sencilla y económica, especialmente para la identificación de usuario remoto.

Otro objeto de la invención es proporcionar un dispositivo para la verificación del usuario a través de un sistema de comunicaciones, particularmente a través de un sistema de telecomunicaciones no protegido tal como el sistema de telefonía pública.

Un objeto adicional de la invención es proporcionar

un dispositivo para llevar a cabo, de una manera remota a través de una conexión telefónica, una verificación segura del usuario para servicios electrónicos, tales como transacciones de pago electrónicas.

5 Todavía un objeto adicional de la invención es proporcionar un sistema sencillo y económico existente o que no esté al menos específicamente equipado para la verificación del usuario.

10 Aún un objeto adicional de la invención es proporcionar un dispositivo para su uso en combinación con un aparato telefónico y una tarjeta de CI, dispositivo que permita un intercambio más eficaz de mensajes seguros.

15 Para este fin, se proporcionan un sistema según la reivindicación 1 y un sistema según la reivindicación 6. En las reivindicaciones dependientes 2-5 se definen realizaciones favorables.

20 La presente invención se basa en la revelación de que, para una comunicación segura entre una tarjeta de CI y un sistema remoto, se puede hacer uso de manera eficaz de las características de las tarjetas actuales (tarjetas inteligentes). En efecto, utilizando la inteligencia de la tarjeta, se puede prescindir sustancialmente de la inteligencia del dispositivo. Al proporcionar una transferencia de datos transparente, el dispositivo puede
25 seguir siendo sencillo, mientras que el intercambio seguro de datos entre la tarjeta de CI y el terminal remoto sigue sustancialmente intacto. Al proporcionar un dispositivo de transferencia transparente, se posibilita una comunicación de extremo a extremo segura y fiable entre la tarjeta de CI
30 y el terminal remoto.

El dispositivo de la presente invención está dispuesto preferiblemente para comunicarse con el terminal remoto en un primer nivel y con la tarjeta de CI en un segundo nivel.

5 Preferiblemente, en el dispositivo según la invención una orden de primer nivel comprende una única orden de segundo nivel. Manteniendo una relación de uno a uno entre órdenes de los dos niveles, es posible pasar una orden de segundo nivel como una orden de primer nivel desde el
10 terminal remoto hasta el dispositivo de la invención. Sin embargo, de manera ventajosa, una orden de primer nivel representa una o más órdenes de segundo nivel. De esta forma, se puede reducir drásticamente el número de órdenes de segundo nivel que es necesario intercambiar entre el
15 dispositivo y el terminal remoto.

La invención se basa por tanto en la premisa de que sólo se ha de establecer un acoplamiento entre una tarjeta inteligente y un aparato de comunicaciones para permitir una verificación del usuario y/o tarjeta remota segura para
20 los servicios.

REALIZACIONES EJEMPLARES

En lo sucesivo, la invención se esclarecerá más en detalle con referencia a las figuras.

La figura 1 muestra una vista lateral y superior de
25 un primer ejemplo de un dispositivo;

la figura 2 muestra en una vista en perspectiva un segundo ejemplo de un dispositivo;

la figura 3 muestra el ejemplo de la figura 2 en una vista lateral;

30 la figura 4 muestra esquemáticamente la estructura

interna de un dispositivo;

la figura 5 muestra esquemáticamente una estructura interna alternativa de un dispositivo;

la figura 6 muestra esquemáticamente el intercambio
5 de mensajes entre las partes constituyentes de un sistema de pago remoto según la invención;

la figura 7 muestra esquemáticamente un ejemplo de un sistema de pago.

En la figura 1 se representa un ejemplo de un
10 dispositivo. Los dispositivos 1 mostrados en la figura 1 comprenden un alojamiento 2, un micrófono 3, un altavoz 4, una pantalla 5, un botón 7 de control y teclas 9. En el alojamiento 2, se ha practicado una ranura 8 para insertar una tarjeta 11 de CI. La vista lateral del dispositivo 1
15 muestra un conector 12 para el intercambio de datos (en serie) con, por ejemplo, un ordenador.

El micrófono 3 y el altavoz 4 constituyen transductores acústicos para convertir señales eléctricas en señales acústicas (por ejemplo, tonos DTMF) para
20 establecer un intercambio de información entre la tarjeta 11 de CI y un aparato de comunicaciones, tal como un aparato telefónico. Aunque se muestran como unidades separadas en la figura 1, el micrófono 3 y el altavoz 4 se pueden combinar en una única unidad.

25 El dispositivo 1 se puede activar mediante el botón 7 de control. Sin embargo, el dispositivo también se puede activar mediante un conmutador interno que actúa en presencia de una tarjeta 11, en cuyo caso se puede omitir el botón 7 de control. La pantalla 5, que preferiblemente
30 está constituida por una pantalla de visualización LCD,

sirve como indicador del estado del dispositivo para facilitar su uso. Alternativamente, se pueden usar LED (no mostrados) o un generador de tono y/o voz para este fin. En este último caso, el altavoz 4 se puede usar ventajosamente para indicar el estado. Las teclas 9 sirven para introducir datos, tal como un código de identificación personal (PIN) del usuario de la tarjeta 11 de CI.

El alojamiento 2 tiene preferiblemente una forma tal que, mientras se usa el dispositivo 1, se puede sujetar fácilmente en una mano. Este criterio se cumple con la forma mostrada en la figura 1, pero también se podría cumplir, por ejemplo, con una forma redonda u ovalada.

El ejemplo alternativo del dispositivo 1, mostrado en las figuras 2 y 3, comprende un alojamiento 2, un micrófono 3, un altavoz 4, un primer LED 5, un segundo LED 6 y un botón 7 de control. En el ejemplo mostrado, el alojamiento 2 está compuesto de dos partes 2a y 2b, que están interconectadas por medio de una bisagra 10. En el alojamiento 2 (parte 2a) hay una ranura 8 practicada para insertar una tarjeta 11 de CI. Además, el dispositivo 1 comprende teclas 9 para introducir, entre otros, datos numéricos. El alojamiento, que está compuesto de las dos partes 2a y 2b, está implementado preferiblemente de una manera tal que se puede cerrar y abrir. En el estado cerrado, entre otros, las teclas 9 y el micrófono 3 quedan protegidos; en el estado abierto, la distancia entre el micrófono 3 y el altavoz 4 es aproximadamente igual que la distancia entre el altavoz 14 y el micrófono 15 del receptor 13 de un aparato telefónico. Posiblemente, la bisagra 10 se puede realizar de una manera tal que, cuando

se abre el alojamiento, el dispositivo se activa automáticamente de modo que se puede omitir el botón 7 de control.

El receptor o auricular 13, mostrado en las figuras 2 y 3, está dotado de un altavoz 14 y un micrófono 15. Un cable 16 conecta el receptor 13 a un aparato de comunicaciones, tal como un aparato telefónico (no mostrado).

El modo de operación y el uso del dispositivo 1 se explicarán adicionalmente a continuación con referencia a las figuras 4-7.

En la figura 3, el dispositivo 1 y el receptor 13 de la figura 2 se muestran en una vista lateral. Tal como se muestra en la figura 3, cuando se usa el dispositivo 1, el altavoz 4 está situado en las proximidades del micrófono 15 del receptor 13. Además, el micrófono 3 del dispositivo 1 está situado entonces en las proximidades del altavoz 14 del receptor 13. Para proteger el micrófono 3, se ha dispuesto de una manera tal que se protege mediante la parte 2b en el estado cerrado del alojamiento 2. Esta colocación en el "interior" no ha demostrado en la práctica plantear ningún problema. Posiblemente, el micrófono 3 se puede disponer en el otro lado de la parte 2b. Se observa, que, por motivos de claridad, el micrófono se ha mostrado esférico en la figura 3; sin embargo, en la práctica también se puede usar un micrófono plano.

El dispositivo se puede realizar como un dispositivo que se puede sujetar en una mano, tal como se muestra en las figuras 1, 2 y 3; sin embargo, también se puede realizar como una "versión de mesa" en la que se puede

colocar un receptor de un aparato telefónico. Además, el dispositivo se puede implementar integrado en o/y acoplado a un aparato telefónico u otro dispositivo de comunicación, tal como un aparato de fax.

5 La composición interna del dispositivo (1 en las figuras 1, 2 y 3) y mostrada esquemáticamente a modo de ejemplo en la figura 4 comprende una unidad 20 de control, un circuito 21 de acoplamiento, un conector 22 de tarjetas, un altavoz 23, un micrófono 24, una unidad 25 de
10 señalización (opcional), un teclado 26 (opcional) y una fuente 27 de alimentación. Por motivos de claridad, no se muestra el alojamiento 2 en la figura 4. El altavoz 23 y el micrófono 24 pueden corresponder al micrófono 3 y al altavoz 4, respectivamente, de las figuras 1, 2 y 3. El
15 teclado 26 opcional puede estar constituido por las teclas 9 en las figuras 1, 2 y 3.

 En el alojamiento (2 en las figuras 1, 2 y 3) del dispositivo, se ha practicado un espacio en el que se puede insertar una tarjeta de CI a través de una ranura (8 en las
20 figuras 1 y 2). En este espacio, se ha dispuesto el conector 22 de tarjetas para proporcionar un contacto mecánico y eléctrico con la tarjeta de CI. Un conector de este tipo se puede implementar según la norma ISO 7816. En caso de que se usen las denominadas tarjetas sin contacto,
25 el conector se puede reemplazar ventajosamente por medios adecuados (electromagnéticos) para intercambiar información con la tarjeta, tal como un transceptor dotado de un medio de antena adecuado.

 El circuito 21 de acoplamiento, que proporciona el
30 acoplamiento entre, por una parte, el conector 22 y, por

otra parte, el altavoz 23 y el micrófono 24, por ejemplo comprende un transductor 28 de DTMF (*dual-tone multi-frequency*), un multiplexor o circuito 29 bifurcado y un adaptador 30 de tasa (opcional). Bajo la influencia de la

5 unidad 20 de control, se intercambia información entre el conector 22 (y la tarjeta de CI conectada al mismo) y un transductor 31 (acústico), que está constituido por el micrófono 24 y el altavoz 23. El transductor 31 acústico transforma señales eléctricas en señales acústicas y

10 viceversa. Posiblemente, el transductor 31 está implementado en la realización preferida de una manera tal que realiza una transducción entre señales eléctricas y ópticas, en cuyo caso el altavoz 23 se reemplazaría, por ejemplo, por un transmisor de infrarrojos y el micrófono

15 24, por ejemplo, por un receptor de infrarrojos. Otra posibilidad sería reemplazar el transductor 31 por una interfaz de línea que proporcione un acoplamiento (eléctrico) entre el dispositivo y una red de comunicación.

La unidad 25 de señalización se ocupa de la

20 señalización al usuario, por ejemplo indicando el estado del dispositivo por medio de, por ejemplo, los LED 5 y 6 mostrados en la figura 2. Ventajosamente, la unidad 25 de señalización puede estar dotada de un generador de voz para producir instrucciones habladas para el usuario.

25 La fuente 27 de alimentación está formada preferiblemente por una batería, pero también puede comprender un acoplamiento a la fuente de alimentación de un aparato telefónico. El dispositivo puede estar dotado de un teclado 26 (teclas 9 en la figura 2) para introducir un

30 código. Dicho código puede comprender un número de

identificación personal (PIN) o un número de teléfono o código de acceso, respectivamente, por ejemplo de una institución para efectuar pagos. Los números de teléfono y/o números de acceso también se pueden introducirse a través del teclado y almacenarse en el dispositivo y/o la tarjeta de CI. Cuando se usa RDSI (Red Digital de Servicios Integrados) (por ejemplo a través del denominado SBus), se puede usar el teclado 26 para introducir los números de acceso. Posiblemente, el teclado 26 también puede ser adecuado para introducir datos no numéricos (teclado alfanumérico).

El dispositivo se puede usar de la siguiente forma. El usuario pulsa el botón de control (7 en las figuras 1, 2 y 3), con lo que el dispositivo se activa. El primer LED (5 en la figura 2) parpadea para indicar que el dispositivo está activo. En todo momento el dispositivo, y por consiguiente la tarjeta de CI, se pueden bloquear o desactivar apretando de nuevo el botón de control.

El usuario coloca entonces el dispositivo 1 cerca del receptor (13 en las figuras 2, 3 y 7) del aparato de comunicaciones (por ejemplo, un aparato telefónico) e introduce su código de identificación (por ejemplo un PIN) en el teclado 26. Si el dispositivo 1 no está dotado de un teclado, el código se puede introducir en el aparato de comunicaciones. También se puede introducir un periodo de tiempo, por ejemplo un límite de tiempo máximo de la sesión de verificación o de uso del servicio en cuestión. Con el código de identificación, se activa la tarjeta de CI. Se debe entender que no es necesario transmitir el propio código de identificación al aparato de comunicaciones, sólo

a la tarjeta de CI. Esto mejora adicionalmente la seguridad del dispositivo.

Posteriormente, el usuario marca el número (por ejemplo, el número de teléfono) del servicio u organización deseado, introduciendo este número en el teclado del dispositivo 1 o del aparato telefónico (43 en las figuras 5 y 6). Si el número está almacenado en el dispositivo o en el medio de pago, este número puede aparecer automáticamente. Entonces, se inicia la sesión de verificación entre el proveedor de servicios (institución u organización de servicios) y la tarjeta de CI.

En la primera parte de la sesión, el usuario coloca el micrófono (3 en las figuras 1, 2 y 3) del dispositivo 1 cerca del altavoz (14 en las figuras 2 y 3) del auricular 13 telefónico para recibir información. Si esto ha ido bien, el primer LED (5 en la figura 2) comienza a iluminarse permanentemente y el segundo LED (6 en la figura 2) comienza a parpadear para indicar al usuario que puede comenzar la segunda parte de la sesión. Para este fin, el usuario coloca el altavoz (4 en las figuras 1, 2 y 3) en las proximidades del micrófono (15 en las figuras 2 y 3) del receptor (13 en las figuras 2 y 3). Si la transmisión de la información por el dispositivo 1 demuestra ser satisfactoria, el segundo LED (6 en la figura 2) comenzará a iluminarse permanentemente. Esto completa la transacción (por ejemplo, el pago o la verificación del usuario). Preferiblemente, el proveedor de servicios o la institución para efectuar pagos emitirá una señal de retorno al usuario a través del dispositivo 1. Cuando haya finalizado la sesión, se apagarán ambos LED.

El escenario anterior sólo se facilita a modo de ejemplo; se entenderá que son posibles muchos otros escenarios.

5 El dispositivo puede estar dotado de medios (en sí conocidos) para el reconocimiento de voz. En primer lugar, entonces es posible hacer que el dispositivo 1 esté controlado por voz, de modo que se puede omitir el pulsado de las teclas y el botón de control. Esto es especialmente, pero no exclusivamente, ventajoso para personas que no ven
10 bien o personas discapacitadas. En segundo lugar, es posible ofrecer una verificación adicional del usuario por medio de verificación de voz, es decir, identificar al hablante inequívocamente basándose en su voz. Posiblemente, se puede omitir entonces la introducción de un código PIN.

15 La información que se intercambia a través del dispositivo 1 entre el aparato telefónico y la tarjeta de CI, puede comprender al menos tres tipos de información. En primer lugar, información de identificación o verificación para verificar la identidad del usuario. Después de todo,
20 antes de que un pago se pueda cargar en una cuenta, se debe establecer la identidad del usuario. El intercambio de información puede comprender además información del pago. Es decir, en el caso de realizar un cargo en una tarjeta, información relacionada con el saldo que queda en la
25 tarjeta y el valor que posiblemente se debe descontar de la tarjeta. Además, se puede intercambiar información de marcación, o al menos se puede emitir al aparato telefónico mediante el dispositivo. Posiblemente, el aparato telefónico puede emitir información de marcación al
30 dispositivo para el uso posterior (solicitar un número de

acceso de una organización de pago). Dicha información de marcación se puede almacenar por ejemplo en la tarjeta de CI.

5 Tal como se indica anteriormente, el dispositivo 1 forma una interfaz entre el aparato telefónico y la tarjeta de CI, transfiriendo información en dos direcciones. Se pueden usar las posibilidades de la tarjeta de CI (procesador y memoria con algoritmo de verificación) para realizar una verificación del usuario y/o una verificación de la tarjeta (verificación que preferiblemente está protegida de una manera criptográfica). Puesto que se utilizan las posibilidades incorporadas de la tarjeta de CI y el dispositivo básicamente sólo pasa órdenes y/o datos de una manera transparente, el dispositivo 1 puede ser muy sencillo y por tanto económico. Además, el dispositivo es intercambiable, es decir, el dispositivo se puede usar por diferentes personas que tienen cada una su propia tarjeta de CI.

20 El dispositivo 1 puede estar compuesto de componentes comercialmente disponibles. La unidad 20 de control puede estar formada por un microprocesador y una memoria. Se puede proporcionar una memoria adicional (no mostrada en la figura 4) por ejemplo para almacenar códigos de acceso y/o códigos PIN. Preferiblemente, los diversos componentes electrónicos, tales como la unidad 20 de control, el 25 circuito 21 de acoplamiento y la unidad 25 de señalización se alojan en un único circuito integrado de aplicación específica (ASIC).

30 La figura 5 muestra una disposición interna alternativa del dispositivo. En la disposición mostrada, la

unidad 20 de control está constituida por un microcontrolador, es decir un microprocesador con una memoria incorporada y posiblemente circuitos adicionales. Puesto que el microcontrolador 20 comprende preferiblemente puertos de entrada y salida (UART) se pueden omitir el multiplexor 29 y el adaptador 30 de tasa. El transductor 28 de DTMF se ha reemplazado por un módem. Una pantalla 32 está conectada al microcontrolador 20. Una memoria 33 programable borrrable (EPROM), que puede estar constituida por una EEPROM o una denominada flash EPROM, sirve para almacenar el software adecuado del microcontrolador 20. Preferiblemente, el dispositivo permite que se actualice el software en la memoria 33, por ejemplo cargando un nuevo software de una tarjeta de CI insertada en el dispositivo.

Un conector 34 en serie (opcional) sirve para proporcionar una conexión eléctrica directa, por ejemplo según el protocolo RS232, con dispositivos externos, tales como ordenadores. Esto permite usar el dispositivo para aplicaciones en redes informáticas, por ejemplo realizando pagos a través de Internet. La unidad 25 de señalización (opcional) puede estar constituida por uno o más LED.

La unidad de control o el microcontrolador 20 sirve principalmente para pasar los datos de la tarjeta (es decir, órdenes y datos de la tarjeta apropiados) entre el conector 22 de tarjetas y el módem 28. Aunque el microcontrolador 20 (y por tanto, el dispositivo 1 de transferencia) es básicamente transparente porque los datos de la tarjeta (es decir, las órdenes de la tarjeta y los datos de la tarjeta apropiados) simplemente se hacen pasar a su través, el microcontrolador realiza preferiblemente

una adaptación de los datos de la tarjeta para aumentar la velocidad a la que se intercambian los datos de la tarjeta. Esto se explicará adicionalmente con referencia a la figura 6.

5 En la figura 6, se representa esquemáticamente el intercambio de los datos de la tarjeta (órdenes y datos enviados a la tarjeta de CI y sus respuestas) entre una tarjeta de CI por una parte y un módulo seguro de una unidad de transacción por otra. La tarjeta de CI se puede
10 corresponder con la tarjeta 11 de las figuras 1, 2, 3 y 7, el dispositivo de transferencia se puede corresponder con el dispositivo 1 de las figuras 1, 2 y 3, la unidad de transacción puede ser un ordenador o dispositivo similar incorporado en la unidad 42 de proveedor de servicios de la
15 figura 7, y el módulo seguro se puede corresponder con el módulo 44 seguro (SM) en la figura 7.

 Según un aspecto adicional de la presente invención, se hace una distinción entre dos niveles del intercambio de órdenes de la tarjeta. Entre la tarjeta de CI y el
20 dispositivo de transferencia tiene lugar un intercambio de bajo nivel: las órdenes de la tarjeta y los datos de la tarjeta reales se envían a y se reciben desde la tarjeta. Puesto que este intercambio se realiza usando señales eléctricas dentro del dispositivo 1 de transferencia, el
25 intercambio puede tener una alta tasa de datos. Entre el dispositivo de transferencia y la unidad de transacción, sin embargo, está presente una trayectoria acústica (entre el dispositivo 1 y el receptor 13). Esta sección de la conexión entre la tarjeta de CI y el módulo seguro tiene
30 habitualmente una velocidad de transmisión limitada. Por

este motivo, en esta sección tiene lugar un intercambio de alto nivel en el que varias órdenes de bajo nivel se agrupan entre sí y se reemplazan por una única orden de alto nivel. De esta forma, se puede reducir
5 significativamente el tiempo de transmisión requerido para una transacción.

Tal como se muestra en la figura 6, la unidad de transacción puede emitir una orden de alto nivel (indicada mediante H). En respuesta a la recepción de esta única
10 orden de alto nivel, el dispositivo de transferencia intercambia varias órdenes de bajo nivel (indicadas mediante L) con la tarjeta de CI. El resultado de este intercambio se envía por el dispositivo de transferencia a la unidad de transacción como una única orden de alto nivel
15 (H). Posteriormente, esta orden de alto nivel da como resultado el intercambio de varias órdenes de bajo nivel (L) entre la unidad de transacción y el módulo seguro. Cada orden de alto nivel (H) representa por tanto una rutina que comprende una pluralidad (por ejemplo cinco de diez)
20 órdenes de bajo nivel (L). Preferiblemente, las órdenes de alto nivel se optimizan por eficacia, por ejemplo representando cada rutina comúnmente usada mediante una única orden de alto nivel.

Preferiblemente, el dispositivo de transferencia
25 soporta dos modos diferentes de intercambio de datos. En un primer modo (indicado mediante Modo I en la figura 6), el dispositivo de transferencia opera tal como se describió anteriormente: una orden de alto nivel representa varias órdenes de bajo nivel. En un segundo modo (indicado
30 mediante Modo II en la figura 6) una única orden de bajo

nivel (L) se envía como una orden de alto nivel (H*) al dispositivo de transferencia, que pasa la orden como una orden de bajo nivel a la tarjeta de CI. La orden de bajo nivel (L) resultante producida por la tarjeta se envía de nuevo por el dispositivo de transferencia a la unidad de transacción como una orden de alto nivel (H*), que posteriormente convierte la orden de nuevo en una orden de bajo nivel (L). Se entenderá que las órdenes de alto nivel H* simplemente transfieren órdenes de bajo nivel (L). Es decir, las órdenes de alto nivel H* pueden consistir, por ejemplo, en una orden de bajo nivel más un encabezamiento apropiado. De esta forma, las órdenes de bajo nivel pueden pasar de manera transparente a la tarjeta de CI mientras se usa el protocolo de datos y/o estructura de las órdenes de alto nivel. Este paso transparente tiene la ventaja de que se pueden usar órdenes de bajo nivel para las que no se dispone de una orden de alto nivel, es decir que no se pueden agrupar en una orden de alto nivel existente. Esto es especialmente ventajoso ya que la introducción de una tarjeta de CI con una o más órdenes nuevas no necesita la actualización del software del dispositivo de transacción.

Preferiblemente, el dispositivo de transferencia, así como la unidad de transacción, se pueden desplazar entre el Modo I y el Modo II, de modo que las órdenes de alto nivel (H) que representan varias órdenes de bajo nivel se puedan intercalar con órdenes de alto nivel (H*) transfiriendo simplemente una única orden de bajo nivel.

El sistema 40 (de pago), mostrado en la figura 7, comprende un sistema 41 de telecomunicaciones, que puede comprender una red telefónica. Una organización 42 de

proporcionamiento de servicios está acoplada al sistema 41 de telecomunicaciones. Esta organización 42, por ejemplo, es una institución para efectuar pagos (tal como un banco) que está dispuesta para pagar de una manera electrónica y por tanto para ejecutar procedimientos de verificación. El proveedor 42 de servicios no sólo puede ser una organización de pagos, sino también una organización de proporcionamiento de servicios en general (videoclub; reparto de pizza a domicilio). La unidad de transacción del proveedor 42 de servicios comprende un módulo 44 seguro (SM) en el que se almacenan de manera segura los datos del pago y las claves criptográficas. Se entenderá que por motivos de claridad en la figura 7 sólo se muestra un único proveedor 42 de servicios, pero que en la práctica se pueden conectar a la red 41 una pluralidad de proveedores 42 de servicios.

Un aparato 43 telefónico, que también está acoplado al sistema 41 de telecomunicaciones, comprende un receptor 13. A través de un dispositivo 1 (que se corresponde con el dispositivo 1 de la figura 1), una tarjeta 11 de CI puede, cuando se pone en contacto con el dispositivo 1 de la figura 1, intercambiar información con el aparato 43 telefónico y por tanto con la organización 42. Mediante el intercambio de información de verificación se pueden comprobar la identidad y la autorización de acceso del usuario de la tarjeta 11 de CI (tarjeta de verificación). Además, se puede verificar de esta manera la autenticidad de la tarjeta 11.

Se entenderá que siempre que se mencionan "aparatos telefónicos" en este texto, éstos no sólo deben incluir

aparatos fijos, sino también aparatos de teléfono móvil y/o fax (en general: un aparato de comunicaciones). Un aparato de comunicaciones de este tipo también puede estar formado por un ordenador (tal como un PC) con un micrófono. Además, la expresión "transacciones de pago electrónicas" significará pago remoto, en otras palabras, pago a través de un dispositivo de (tele)comunicaciones. Dicho pago de manera remota se puede realizar por ejemplo por un cliente en su domicilio, o por un cliente en su oficina. La invención es especialmente adecuada en combinación con emisiones televisivas con la posibilidad de encargar y pagar inmediatamente los productos anunciados.

La tarjeta de CI mencionada en este texto será en general un medio electrónico para efectuar pagos, con un circuito electrónico, dispuesto sobre un sustrato de plástico tal como una denominada tarjeta inteligente o tarjeta con chip. Sin embargo, se entenderá que no es necesario que la tarjeta de CI tenga una forma similar a una tarjeta. Sólo es esencial que la tarjeta de CI se pueda usar para realizar un procedimiento de verificación, a saber, la determinación inequívoca de la autenticidad y posiblemente también la identidad de la tarjeta. Por tanto, se puede comprobar la autorización de acceso de la tarjeta y/o el usuario ("autenticación"). Por tanto, la expresión "medios para efectuar el pago" no sólo debe incluir una tarjeta de CI, sino por ejemplo también un módulo electrónico con un circuito electrónico adecuado para fines de verificación. El circuito integrado necesario para la verificación (por ejemplo un denominado ASIC) también se puede disponer posiblemente en el dispositivo, sin una

tarjeta o un sustrato de este tipo. Esto se puede realizar por ejemplo practicando una abertura en el alojamiento (compárese con la ranura 8 en la figura 1) en la que se puede insertar un circuito integrado de una manera no desmontable. Esto ofrece todavía la ventaja de que el propio dispositivo se puede realizar de una manera muy sencilla y por tanto económica.

Una transacción financiera, ejecutada con la ayuda del dispositivo comprende una transacción de pago, pero también una transacción de recargo (revalorización), en la que el saldo de la tarjeta de CI aumenta en lugar de disminuir.

Los expertos en la técnica entenderán que la invención no se limita a las realizaciones representadas y que son posibles diversas modificaciones y adiciones sin salir del alcance de la invención.

REIVINDICACIONES

1.- Sistema (40) para transacciones financieras electrónicas, que comprende una red (41) de telecomunicaciones, un proveedor (42) de servicios que está acoplado a la red (41), cuyo proveedor (42) de servicios está dispuesto para llevar a cabo órdenes de pago electrónico, un aparato (43) de comunicaciones que también está acoplado a la red (41), una tarjeta (11) de CI electrónica, teniendo la tarjeta un saldo en la tarjeta, que se dispone para transacciones seguras entre la tarjeta y el proveedor de servicios a través de un dispositivo (1) para intercambiar datos entre la tarjeta de CI y el aparato (43) de comunicaciones, comprendiendo el dispositivo:

- primeros medios (22) de conexión para su conexión con la tarjeta (11) de CI,

- segundos medios (31) de conexión para intercambiar datos con el aparato (43) de comunicaciones mediante medios ópticos, incluyendo por ejemplo medios infrarrojos, y

- medios (20) de control para controlar la transferencia de datos dentro del dispositivo;

cuyos medios (20, 22, 31) están acoplados entre sí para intercambiar datos entre el aparato (43) de comunicaciones y la tarjeta (11) de CI, estando dispuesto además el sistema (40) para el intercambio seguro de datos en dos direcciones entre la tarjeta de CI y el proveedor de servicios sin alterar el contenido de los mismos, y ejecutándose además las transacciones financieras electrónicas a modo de pago remoto mientras disminuye el saldo en la tarjeta de CI, estando dispuesto además el dispositivo para comunicarse con el proveedor de servicios

con órdenes en un primer nivel y con la tarjeta con órdenes en un segundo nivel, en el que varias órdenes de segundo nivel se agrupan entre sí y se reemplazan por una única orden de primer nivel.

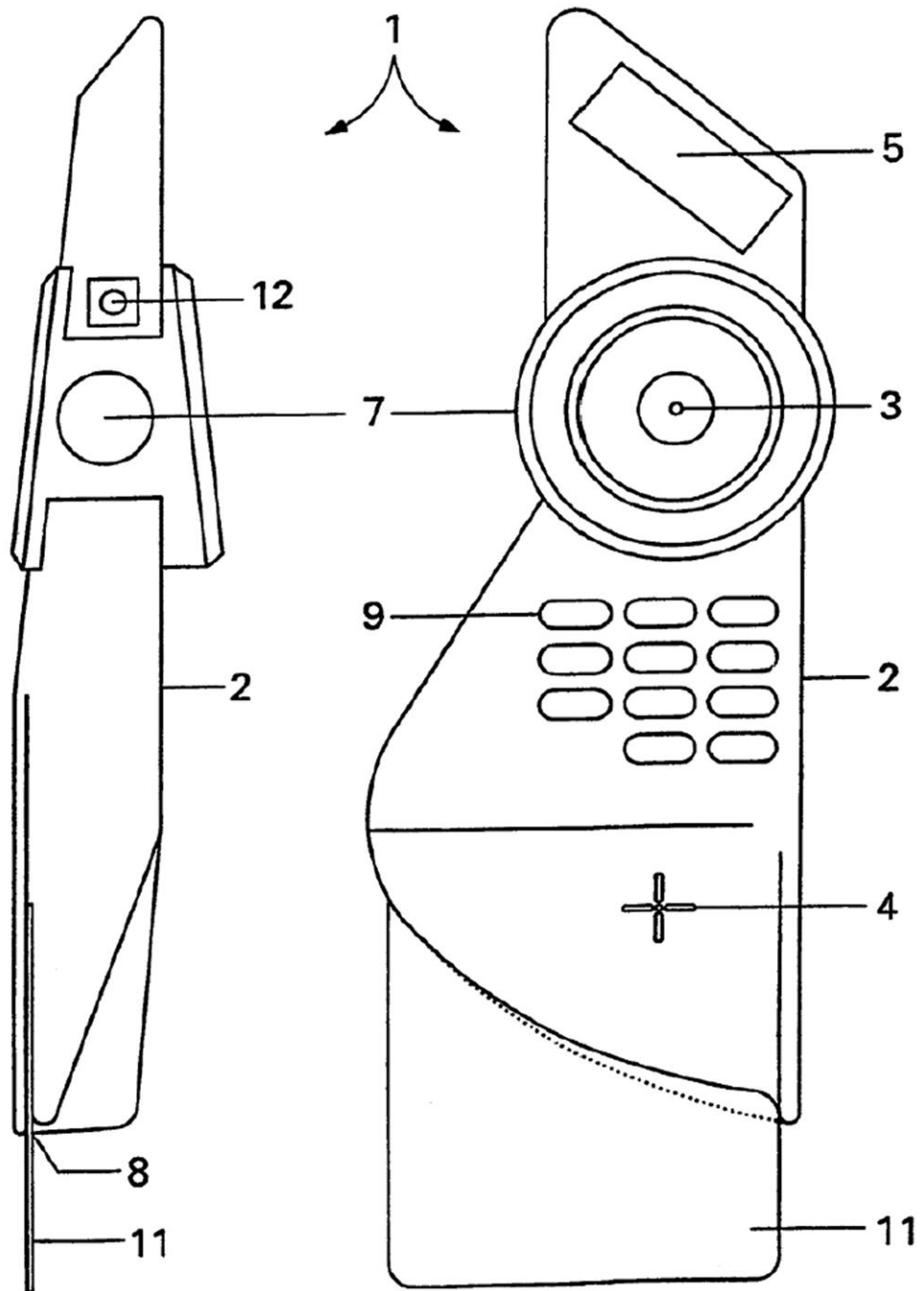


Fig. 1

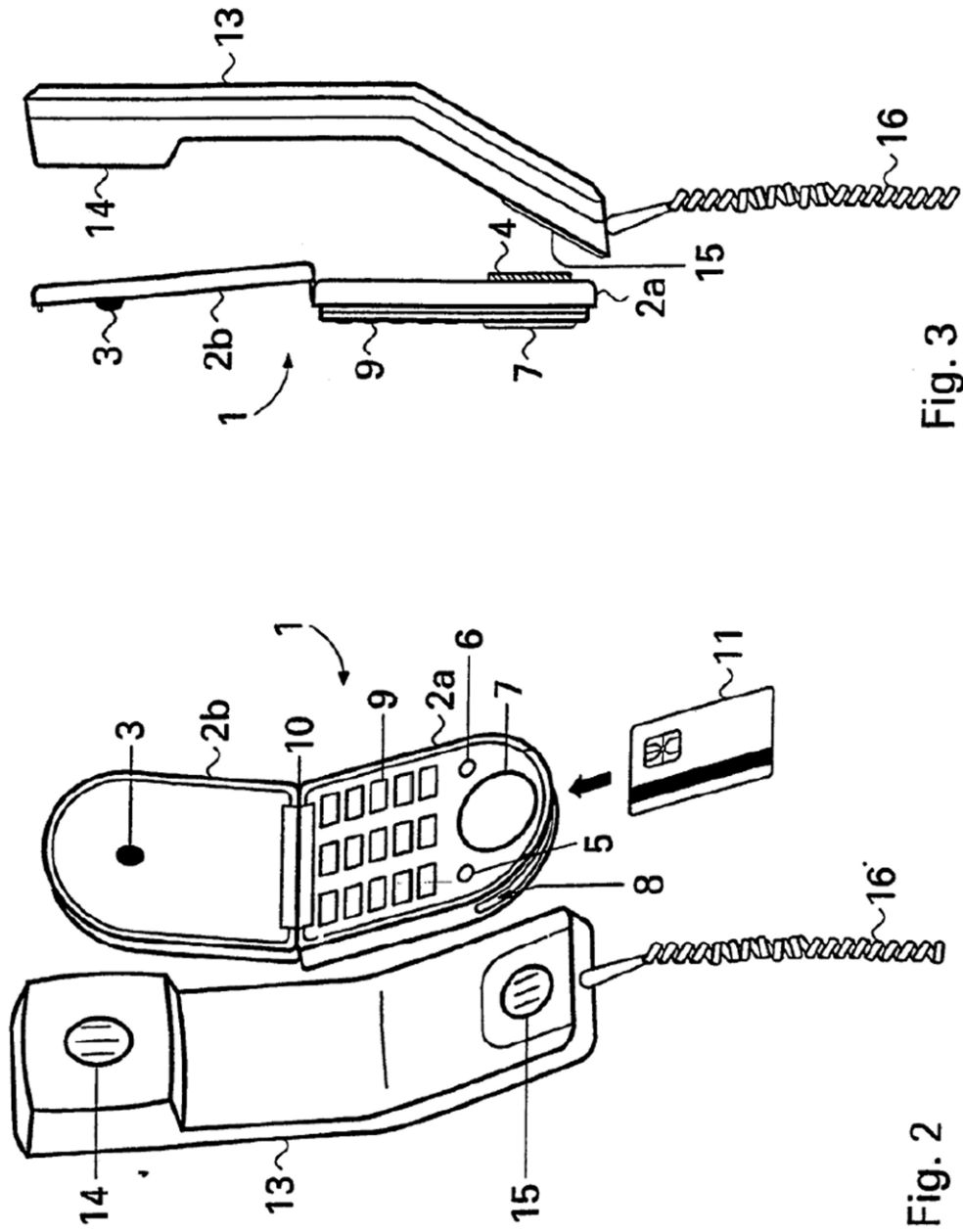


Fig. 3

Fig. 2

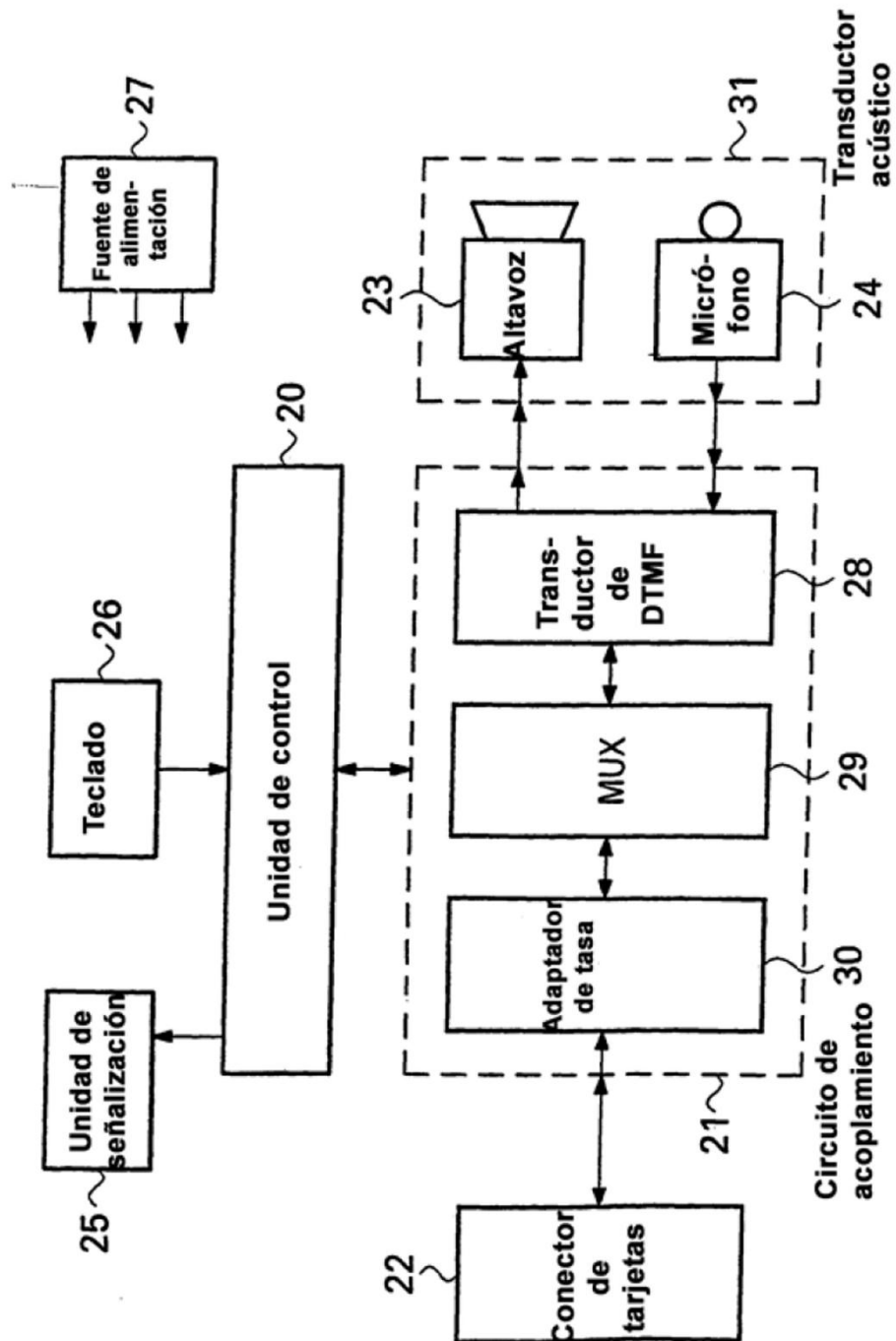


Fig. 4

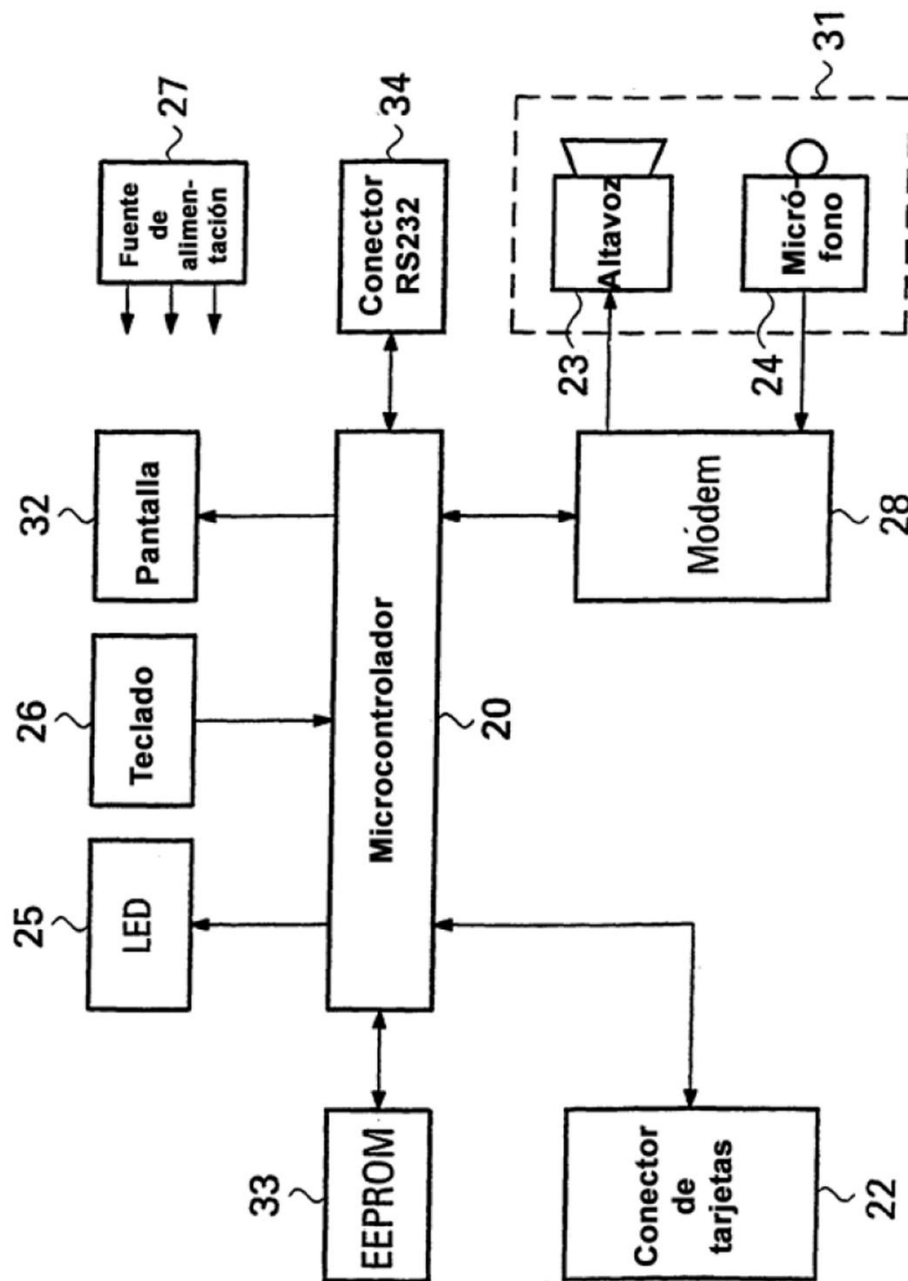


Fig. 5

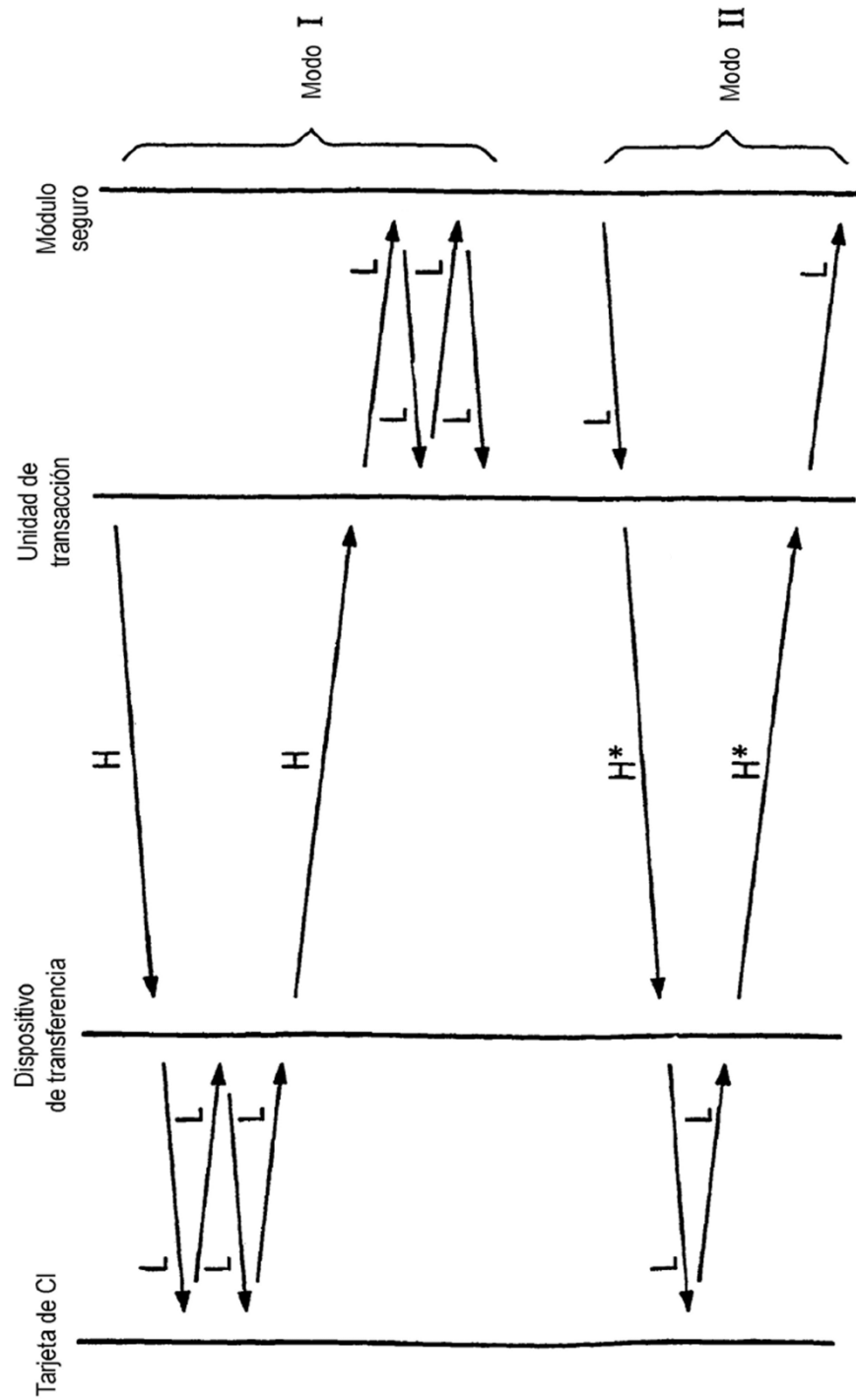


Fig. 6

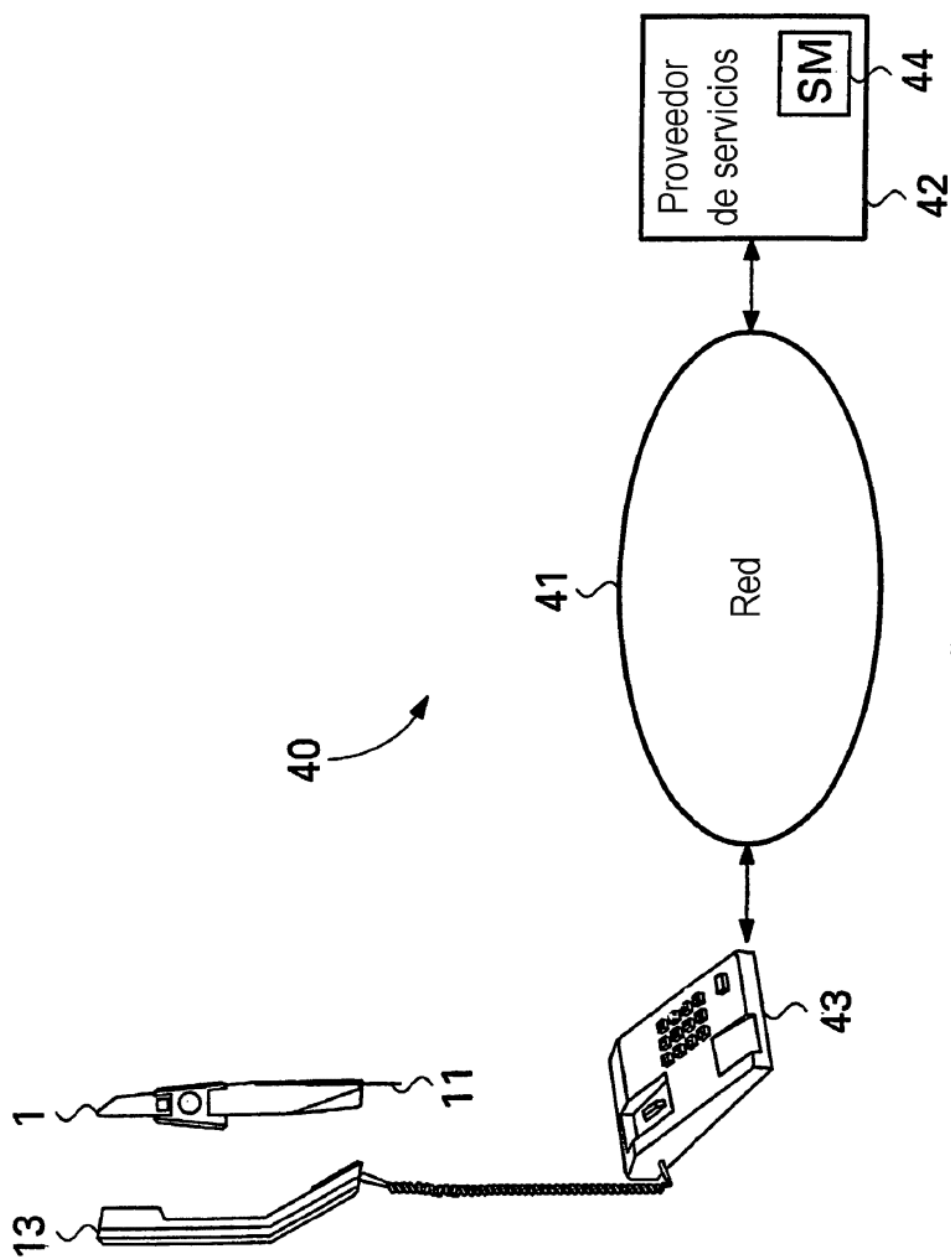


Fig. 7