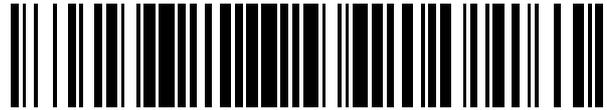


19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 391 982**

51 Int. Cl.:

G06K 19/07 (2006.01)

G07F 7/10 (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Número de solicitud europea: **06739852 .9**

96 Fecha de presentación: **28.03.2006**

97 Número de publicación de la solicitud: **1958127**

97 Fecha de publicación de la solicitud: **20.08.2008**

54 Título: **Tarjeta inteligente**

30 Prioridad:

08.12.2005 US 296309

45 Fecha de publicación de la mención BOPI:

03.12.2012

45 Fecha de la publicación del folleto de la patente:

03.12.2012

73 Titular/es:

**HO, CHUN-HSIN (100.0%)
8F-1 NO. 180, SEC. 2 DUEN HUA SOUTH ROAD
TAIPEI 106, TW**

72 Inventor/es:

HO, CHUN-HSIN

74 Agente/Representante:

DÍAZ DE BUSTAMANTE TERMINEL, Isidro

ES 2 391 982 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

Tarjeta inteligente.

CAMPO DE LA INVENCION

5 La presente invención se refiere a una tarjeta inteligente y, más particularmente, a una tarjeta inteligente en un sistema de tarjeta doble para su uso con un terminal tal como un cajero automático (ATM) o un lector de tarjetas de un punto de venta (POS) o con un terminal de comunicación, es decir, un teléfono móvil.

ANTECEDENTES DE LA INVENCION

10 En el pasado, se ha usado una tarjeta magnética tal como una tarjeta bancaria o tarjeta de crédito. En un sistema de tarjeta magnética, un dato de identificación personal para identificar a un propietario de la tarjeta magnética, que se conoce como contraseña, se almacena en la tarjeta magnética, y la coincidencia entre la contraseña leída de forma electromagnética desde la tarjeta magnética cargada en un lector de tarjetas y una contraseña introducida de forma manual por el propietario de la tarjeta es comprobada para determinar si el usuario de la tarjeta es un propietario de la tarjeta válido. Sin embargo, la tarjeta magnética plantea los siguientes problemas.

15 En primer lugar, la contraseña grabada en la tarjeta magnética puede ser leída por un hardware sencillo y, por lo tanto, el uso por una persona no autorizada puede conseguirse fácilmente.

En segundo lugar, la contraseña debe ser conocida solamente por el propietario. Sin embargo, es necesario el hardware para escribir la contraseña y una persona que prepara la tarjeta conoce la contraseña.

20 En tercer lugar, la protección de seguridad para un ATM o un lector de tarjetas de crédito no es perfecta y la prevención de la filtración de la contraseña no es perfecta. Sin embargo, el propietario no puede cambiar la contraseña y la tarjeta es usada incluso después de que otra persona conozca la contraseña.

25 Para superar los problemas anteriores, la Patente de Estados Unidos N° 4.758,718, titulada "High Security IC Card with an Updateable Password" de Fujisaki et al., describe una tarjeta con IC (circuito integrado) que tiene un microprocesador y una memoria. En la figura 1, el número 10 indica una tarjeta con IC usada como medio de identificación para identificar a una persona, el número 11 indica un microprocesador para controlar el registro y la actualización de un dato de contraseña, el número 12 indica una interfaz de comunicación para la conexión con un dispositivo terminal, el número 13 indica un teclado para introducir el dato de contraseña, el número 14 indica un dispositivo de visualización tal como una pantalla LCD para mostrar el dato de contraseña, el número 15 indica una memoria que tiene áreas para almacenar los datos necesarios para el registro y la actualización de la contraseña, el número 16 indica un área de memoria de la contraseña en la memoria 15, teniendo el área de la contraseña 16 bits, el número 17 indica un área para almacenar el número de veces de no coincidencia de la contraseña en la memoria 15, el número 18 indica un área para almacenar datos que representan un tipo y atributos de la tarjeta con IC 10, y el número 19 indica una batería. La memoria 15 tiene un área de registro de la contraseña en la que se registrará la contraseña y un área de actualización de la contraseña en la que se almacenan datos de actualización para actualizar la contraseña registrada en el área de registro. La contraseña se introduce mediante una operación de teclado y el microprocesador controla el registro de la contraseña y registra la contraseña introducida en el área de registro de la contraseña. Cuando se va a cambiar la contraseña registrada, el número de veces de error de introducción para la contraseña registrada en el microprocesador se comprueba en base a datos preestablecidos en el área de actualización de la contraseña. Si el número de veces de error es menor que un número predeterminado, el área de registro así como el área de actualización de la contraseña se borran y se permite que una contraseña recién introducida sea registrada en el área de registro.

35 Hoy en día, las tarjetas con IC o las llamadas "tarjetas inteligentes" se usan en numerosas aplicaciones tales como el pago en un punto de venta (conocidas como "tarjetas bancarias"), teléfonos públicos, pago por aparcamiento, pago para peajes de circulación, teléfonos móviles (por ejemplo, tarjetas SIM), servicios sanitarios, transporte público o monedero electrónico. Cada una de estas aplicaciones está asociada con una tarjeta específica: una tarjeta bancaria, una tarjeta telefónica, una tarjeta de aparcamiento, una tarjeta SIM para telefonía GSM, y demás.

45 Uno de los problemas que se plantean en el uso diario de dicha variedad de tarjetas se basa en que una de las tarjetas podría no estar disponible cuando debe usarse, sin importar si se dejó en casa, se terminó su saldo o si ha caducado. Además, la administración y el porte de diversas tarjetas son incómodos. Por lo tanto, existe una fuerte necesidad de las llamadas "tarjetas de aplicación múltiple".

50 Por ejemplo, la Patente de Estados Unidos N° 6.325.293, titulada "Method and System for Using a Microcircuit Card in a Plurality of Applications" de Moreno, describe una tarjeta con microcircuito que incluye un dispositivo que activa una aplicación por defecto a ejecutar, dispositivo que activa una aplicación diana a ejecutar, y dispositivo de conmutación que activa la tarjeta a configurar a voluntad como tarjeta de aplicación por defecto o como tarjeta de aplicación diana. La figura 2 muestra la organización y la secuencia de funcionamiento general del método de la misma.

Tal como se muestra en la figura 2, la suscripción extraída por un cliente 20 del operador de radioteléfono 21 que opera el radioteléfono del usuario 22 incluye no solamente servicio radiotelefónico general, sino también un servicio especial, por ejemplo pago por aparcamiento, en el que la cantidad estará incluida como un elemento específico en el listado mensual de consumo telefónico recibido del operador 21 (facturación representada mediante 23).

5 Después de aparcar un coche cerca de un parquímetro de aparcamiento de pago electrónico 24 programado para aceptar el pago de tarjetas prepago emitidas por el municipio 25, el conductor puede descubrir que no tiene ninguna tarjeta de aparcamiento utilizable disponible o que la tarjeta ha caducado o no es válida. Para realizar el pago requerido por la máquina, el usuario emite entonces una orden de “aparcamiento” en el radioteléfono, por ejemplo pulsando un botón 26 o seleccionando una opción en un menú que proporciona los servicios opcionales ofrecidos por el operador de telefonía. Esta orden hace que la tarjeta SIM 27 del radioteléfono se “reconfigure” como tarjeta de aparcamiento. El usuario saca entonces la tarjeta 27 del radioteléfono y la inserta (flecha 28) en la máquina 24, que percibe a la tarjeta como si fuera una tarjeta de aparcamiento, y la tarjeta funciona y es cargada como tal. El usuario reinserta a continuación la tarjeta 27 (flecha 29) en el radioteléfono 22 donde es leída por el radioteléfono que la reconfigura automáticamente para la función de GSM.

15 Aunque dichas tarjetas de aplicación múltiple son técnicamente factibles, en la práctica son muy difíciles de implementar, tal como se ha demostrado mediante numerosos intentos vanguardistas desde la invención de la propia la tarjeta con IC.

20 Con el ampliamente extendido uso de tarjetas inteligentes en la industria de la telefonía móvil tal como SIM para GSM, USIM para WCDMA, RUIM para CDMA2000 y PIM para red PHS, se han desarrollado una gran diversidad de aplicaciones utilizando tarjetas inteligentes ubicadas en el teléfono móvil (SIM/USIM/RUIM/PIM, denominadas en lo sucesivo en este documento como UICC, Tarjeta Universal con Circuito Integrado) para proporcionar servicios de seguridad. Los operadores de telefonía móvil garantizan la seguridad del uso de un servicio de telefonía móvil mediante la autenticación de las claves almacenadas en las tarjetas inteligentes que los operadores de telefonía móvil facilitaron a los abonados. Además, los operadores de telefonía móvil también proporcionan servicios *Premium* como operaciones bancarias a través del teléfono móvil, servicio de operaciones bursátiles a través del teléfono móvil almacenando claves proporcionadas por los bancos u otros proveedores de servicios en las tarjetas SIM. Las claves se manipulan mediante una interfaz de aplicación desarrollada por el Conjunto de Herramientas SIM (STK) que también está ubicado en la propia tarjeta SIM. Cuando aparecieron los teléfonos WAP (Protocolo de Aplicaciones Inalámbricas), los proveedores de la tarjeta SIM también desarrollaron el WIM (Módulo de Identificación Inalámbrica) para reforzar la seguridad WAP almacenando un certificado y algoritmo de PKI en la propia SIM (tarjeta SWIM) u otra tarjeta WIM independiente que puede insertarse en otra ranura para tarjetas en el teléfono móvil.

35 El teclado y la pantalla de visualización del teléfono móvil facilitan a la tarjeta inteligente insertada una gran interfaz del usuario y la naturaleza móvil del acceso a distancia a los proveedores de servicios consigue completamente el objetivo de movilidad del servicio. Para conseguir la movilidad de servicio, los proveedores de servicios como bancos, entidades emisoras de tarjetas de crédito, emisores de tarjetas de transporte, emisores de certificados y agentes de bolsa están deseosos de cooperar con el operador de telefonía móvil para emitir tarjetas SIM mejoradas para proporcionar servicios relacionados con sus actividades profesionales. Sin embargo, la provisión y gestión de la capacidad y funcionalidades de la SIM están bajo el control de los operadores de telefonía móvil y, por lo tanto, forma un sistema cerrado en el que solamente se permite participar a partes autorizadas. Además, la relación entre los proveedores de servicios y los operadores de telefonía móvil es de mutua desconfianza y ambos tienen planes similares relativos al control de la seguridad y los métodos de pago. Esto se convierte en el principal obstáculo para el desarrollo de servicios de seguridad para telefonía móvil.

45 En el mundo de las comunicaciones a través del teléfono móvil, otra demanda emergente basada en la tarjeta inteligente es la llamada “propiedad de múltiples SIM” que indica la tendencia de un único usuario de teléfono móvil a poseer más de una tarjeta SIM que pueden haber sido emitidas por diferentes operadores de telefonía móvil. La tendencia surge debido a las siguientes razones:

- tener cuentas diferentes para uso personal y de negocios
- tener diferentes SIM de operadores de telefonía móvil de diferentes países cuando se viaja para ahorrar en la tarifa por servicio itinerante
- 50 • mantener diferentes SIM para diferentes planes de servicio, tales como llamadas durante el día y llamadas con tarifa reducida
- mantener diferentes SIM para diferentes paquetes de tarifa promocionales para ahorrar costes

Se solía presentar un teléfono móvil especial con capacidad para chip doble o ranura doble para resolver los problemas anteriores, proporcionando una ranura para chip adicional en el teléfono móvil para que el proveedor del servicio u otro operador de telefonía móvil emita su propia tarjeta inteligente o SIM que almacene sus propias claves secretas. Sin embargo, los teléfonos especiales normalmente son costosos y no son bien aceptados por el usuario, formando de este modo un mercado fragmentado donde los proveedores de servicio pueden operar.

Por lo tanto, es necesario proporcionar una tarjeta inteligente que pueda rectificar estos inconvenientes de la técnica anterior y resolver los problemas anteriores.

5 Los lectores de tarjetas inteligentes pueden realizarse de diferentes maneras. Por ejemplo, La Patente Europea N° 0858046 describe un lector de tarjetas con circuito integrado portátil para la inserción de una tarjeta con circuito integrado, La Publicación Estadounidense N° 2004-089717 describe un adaptador de tarjetas de memoria para proporcionar una interfaz de conexión diferente a una tarjeta de memoria insertada en él, y la Patente WIPO N° 01/29762 describe un adaptador para tarjetas con circuito integrado para proporcionar múltiples interfaces de conexión a una tarjeta con circuito integrado insertada en su interior.

RESUMEN DE LA INVENCION

10 Este párrafo extrae y compila algunas características de la presente invención; otras características se describirán en los siguientes párrafos. Se pretende cubrir diversas modificaciones y disposiciones similares incluidas en el alcance de las reivindicaciones adjuntas.

15 De acuerdo con un aspecto de la presente invención, una tarjeta inteligente incluye un procesador y una primera interfaz para su uso en la comunicación con un terminal, incluyendo dicho procesador (310) medios de generación de ATR (319) para generar una señal de ATR caracterizados porque dicha tarjeta inteligente tiene una segunda interfaz para su uso en comunicación con otra tarjeta inteligente y medios de generación RST para generar una señal de reset (RST) para la otra tarjeta inteligente, permitiendo de este modo que la otra tarjeta inteligente sea controlada por la tarjeta inteligente.

20 Preferentemente, el procesador incluye además una memoria tampón para recibir y guardar una señal de ATR (Respuesta Al Reset) desde la otra tarjeta inteligente.

Preferentemente, el procesador incluye además medios de generación de una petición de PTS (Selección del Tipo de Protocolo) para generar una señal de petición de PTS para otra tarjeta inteligente.

Preferentemente, el procesador incluye además medios de generación de una respuesta de PTS para generar una señal de respuesta de PTS para el terminal.

25 Preferentemente, el procesador incluye además medios de determinación de PTS para determinar si la señal de petición de PTS es aceptable tanto por el terminal como por otra tarjeta inteligente.

Preferentemente, el procesador incluye además un regulador del reloj para proporcionar una frecuencia de reloj para otra tarjeta inteligente.

30 Más ventajosamente, el procesador incluye además medios de determinación de APDU (Unidad de Datos del Protocolo de Aplicación) de comando para determinar si una señal de APDU de comando emitida desde el terminal está asociada con la tarjeta inteligente u otra tarjeta inteligente.

Más ventajosamente, el procesador incluye además medios de generación de APDU de comando para generar una señal de APDU de comando para otra tarjeta inteligente.

35 Más ventajosamente, el procesador incluye además una memoria tampón para recibir y guardar una señal de APDU de respuesta de otra tarjeta inteligente.

Más ventajosamente, el procesador incluye además medios de generación de APDU de respuesta para generar una señal de APDU de respuesta para el terminal.

Más ventajosamente, la tarjeta inteligente está provista de una antena para comunicación con un terminal sin contacto.

40 Más ventajosamente, la tarjeta inteligente comprende una tarjeta SIM (Módulo de Identificación del Abonado), tarjeta USIM (Módulo de Identificación del Abonado Universal), tarjeta UIM (Módulo de Identificación del Usuario) y tarjeta RUIM (Módulo de Identificación del Usuario Extraíble).

Más ventajosamente, la tarjeta inteligente o la otra tarjeta inteligente comprende una tarjeta ATM.

BREVE DESCRIPCION DE LOS DIBUJOS

45 Los anteriores objetos y ventajas de la presente invención serán más evidentes para los expertos en la materia después de revisar la siguiente descripción detallada y dibujos adjuntos, en los que:

La figura 1 es un diagrama de bloques que muestra una tarjeta con IC convencional;

La figura 2 es un diagrama que muestra diversos dispositivos y reproductores de acuerdo con otro método convencional;

La figura 3 es un diagrama de bloques de una primera realización de una tarjeta inteligente en un sistema de tarjeta doble para su uso con un terminal de transacción de acuerdo con la presente invención;

La figura 4 es un diagrama de bloques de una tarjeta inteligente en un sistema de tarjeta doble para su uso con un terminal de comunicación que no pertenece a la presente invención; y

5 Las figuras 5A y 5B son diagramas de flujo que muestran un método de transacción mediante el uso de un sistema de tarjeta doble de acuerdo con la presente invención.

DESCRIPCIÓN DETALLADA DE LA REALIZACIÓN PREFERENTE

10 La presente invención describe una tarjeta inteligente en un sistema de tarjeta doble y un método para usarla, y los objetos y ventajas de la presente invención serán más evidentes para los expertos en la materia después de revisar la siguiente descripción detallada. No es necesario limitar la presente invención a las siguientes realizaciones.

Primera realización

15 Por favor, remítase a la figura 3. Ésta ilustra un diagrama de bloques de una primera realización de una tarjeta inteligente en un sistema de tarjeta doble para su uso con un terminal de transacción de acuerdo con la presente invención. Tal como se muestra en la figura 3, el sistema de tarjeta doble para su uso con el terminal de transacción 30 está constituido por una primera tarjeta 32 y una segunda tarjeta 31. La primera tarjeta 32 tiene una primera memoria 321 para almacenar una primera información de identificación para su uso en una transacción diana con un terminal de transacción 30. La segunda tarjeta 31 incluye un procesador 310, un dispositivo de generación de RST 314b, una segunda memoria 311, una tercera memoria 312, una cuarta memoria 313, y un regulador del reloj 34a. La segunda memoria 311 almacena segunda información de identificación para su uso en una transacción diana con el terminal de transacción 30. La tercera memoria 312 almacena información relacionada con la transacción. La cuarta memoria 313 almacena una primera información personal que no está protegida por la primera tarjeta 32. El regulador del reloj 34a recibe una señal de reloj del terminal de transacción 30 mediante el cable CLK 34 y proporciona otra señal de reloj a la primera tarjeta 32 mediante el cable CLK 37. La señal de reloj proporcionada por el regulador del reloj 34a puede ser la misma o diferente de la proporcionada por el terminal de transacción 30.

20 Mientras tanto, la primera tarjeta 32 se instala con un primer sistema operativo, y la segunda tarjeta 31 se instala con un segundo sistema operativo. La segunda tarjeta 31 puede desempeñar los papeles de una tarjeta inteligente y un lector de tarjetas simultáneamente para controlar a la primera tarjeta 32.

25 La segunda tarjeta 31 está acoplada al terminal de transacción 30 mediante tres cables: cable RST 33, cable CLK 34, y puerto I/O (entrada/salida) 35, cables que están naturalmente además de un cable de suministro de energía VCC y un cable de tierra GND. Además, el terminal de transacción 30 es un lector de tarjetas inteligentes de un dispositivo portátil o un terminal fijo como ATM o POS. Además, la primera tarjeta 32 está acoplada a la segunda tarjeta 31 mediante tres cables: cable RST 36, cable CLK 37 y puerto I/O 38, tal como se muestra. En realidad, la segunda tarjeta 31 está provista de dos puertos I/O, el puerto I/O 35 y el puerto I/O 38 para comunicar con el terminal de transacción 30 y la primera tarjeta 32, respectivamente. Ciertamente, la segunda tarjeta 31 es capaz de tratar con diferentes protocolos de comunicación del puerto I/O 35 y el puerto I/O 38. De acuerdo con la primera realización de la presente invención, la segunda tarjeta 31 también es capaz de emitir comandos de la Unidad de Datos del Protocolo de Aplicación (APDU) a través del puerto I/O 38 a la primera tarjeta 32, y la segunda tarjeta 31 proporciona señales de reloj a la primera tarjeta 32 a través del cable CLK 27. En otras palabras, la segunda tarjeta 31 actúa como una tarjeta inteligente y como un lector de tarjeta inteligente, controlando a la primera tarjeta 32.

30 Generalmente, una tarjeta inteligente envía una ATR (Respuesta Al Reset) mediante el puerto I/O a un lector de tarjetas después de que se hayan aplicado un voltaje de suministro VCC, un reloj CLK y una señal de reset RST. La cadena de datos y los elementos de datos de la ATR se definen y se describen en detalle en la norma ISO/IEC 7816-3. El formato de ATR básico se muestra en la Tabla 1.

Tabla 1 Los elementos de datos de la ATR y sus significados, de acuerdo con la ISO/IEC 7816-3

Elemento de datos	Descripción
TS	Carácter inicial
T0	Carácter de formato
TA1, TB1, TC 1, TD1,...	Caracteres de interfaz
T1, T2, ..., TK	Caracteres históricos
TCK	Carácter de comprobación

5 Los dos primeros bytes, denominados TS y T0, definen diversos parámetros de transferencia fundamentales y la presencia de bytes posteriores. Los caracteres de interfaz especifican parámetros de transferencia especiales para el protocolo, que son importantes para las siguientes transferencias de datos. Los caracteres históricos describen el alcance de las funciones básicas de la tarjeta inteligente. El carácter de comprobación, que es una suma de comprobación "checksum" de los bytes anteriores, puede ser enviado opcionalmente como el último byte de la ATR, dependiendo del protocolo de transmisión. Además, esta cadena de datos de ATR siempre es enviada como un valor divisor y contiene diversos datos relevantes para el protocolo de transmisión y la tarjeta. Tal como se conoce, la tarjeta inteligente muestra diversos parámetros de transferencia de datos en los caracteres de interfaz de ATR, tales como el protocolo de transmisión y el tiempo de espera del carácter.

Además, si un terminal quiere modificar uno o más de estos parámetros, debe realizarse una Selección del Tipo de Protocolo (PTS) antes de la ejecución real del protocolo. El terminal puede usar esto para modificar ciertos parámetros del protocolo, siempre que esto lo permita la tarjeta.

15 En la presente invención, en referencia a las figuras 3 y 5, el procesador 310 de la segunda tarjeta 31 incluye una memoria tampón 318, un dispositivo de generación de ATR 319, un dispositivo de determinación de PTS 315a, un dispositivo de generación de petición de PTS 315b, un dispositivo de generación de respuesta de PTS 315c, un dispositivo de determinación de APDU de comando 316a, un dispositivo de generación de APDU de comando 316b, y un dispositivo de generación de APDU de respuesta 317. En una transacción, un terminal de transacción 30 determina si una primera tarjeta 32 existe después de haber sido encendido (etapa S500 y S501). Si una primera tarjeta 32 no existe en un sistema de transacción, entonces el terminal de transacción 30 realizará una transacción por defecto con la segunda tarjeta 31 (etapa S502). Además, la transacción por defecto también puede ser una comunicación sin contacto con otro terminal mediante una antena provista en la segunda tarjeta 31. En este caso, la comunicación es a través de una comunicación por radio. Por otro lado, si una primera tarjeta 32 existe, entonces el terminal de transacción 30 funcionará en un sistema de tarjeta doble. En un sistema de tarjeta doble, las señales que van a ser enviadas a la primera tarjeta 32 van todas a través de la segunda tarjeta 31. En otras palabras, el terminal de transacción 30 no comunica directamente con la primera tarjeta 32. Es decir, la segunda tarjeta 31 es esclava del terminal de transacción 30, pero también maestra de la primera tarjeta 32. Por lo tanto, las señales de reset (RST2) emitidas desde el terminal de transacción 30 son enviadas directamente a la segunda tarjeta 31 solamente, no importa si la transacción está relacionada con la primera tarjeta 32 o la segunda tarjeta 31. Una vez que la segunda tarjeta recibe la RST2, entonces el dispositivo de generación de RST 314b generará una señal de reset (RST1) para la primera tarjeta 32 (etapa S503). Después de recibir la RST1, la primera tarjeta 32 responde con una señal de Respuesta a Reset (ATR1) para la memoria tampón 318 (por ejemplo memoria interna Primero en Entrar, Primero en Salir (FIFO)) de la segunda tarjeta 31 (etapa S504). Después de recibir la ATR1 de la primera tarjeta 32, el dispositivo de generación de ATR 319 de la segunda tarjeta 31 genera otra señal de Respuesta a Reset (ATR2') para el terminal de transacción 30 (etapa S505).

40 En términos generales, una señal de Respuesta a Reset debe producirse entre 400 y 40.000 ciclos de reloj después de que el terminal de transacción 30 emite una señal de reset. Con una frecuencia del reloj de 3,5712 MHz, esto corresponde a un intervalo de 112 μ s a 11,20 ms, mientras que a 4,9152 MHz el intervalo es de 81,38 μ s a 8,14 ms. Si el terminal de transacción 30 no recibe la ATR dentro de este intervalo, repite la secuencia de activación varias veces (habitualmente hasta tres veces) para intentar detectar una ATR. Si todos estos intentos fallan, el terminal supone que la tarjeta es defectuosa y responde de forma consecutiva. Sin embargo, si la ATR1 es enviada a la segunda tarjeta 31 después de que la segunda tarjeta 31 reciba la RST2 del terminal de transacción 30, tal como se ha mencionado anteriormente, entonces sería difícil para la ATR1 responder a tiempo. Por lo tanto, para superar este problema, el dispositivo de generación de RST 314b de la segunda tarjeta 31 está programado para generar de forma espontánea una señal de reset (RST1) para la primera tarjeta 32 una vez que la segunda tarjeta 31 es encendida independientemente de la recepción de RST2 desde el terminal de transacción 30. Es decir, el dispositivo de generación de RST 314b no espera necesariamente hasta que la RST2 sea enviada desde el terminal de transacción 30 antes de enviar la RST1 a la primera tarjeta 32 para evitar una respuesta retardada para el terminal de transacción 30. Por lo tanto, la segunda tarjeta 31 conserva la ATR1 enviada desde la primera tarjeta 32 en la

memoria tampón 318 hasta que la RST2 es recibida. De esta manera, la ATR1 puede ser enviada inmediatamente después de que la RST2 sea emitida.

Después de que el terminal de transacción 30 recibe una señal de ATR desde el dispositivo de generación de ATR 319, el terminal envía a continuación de forma continua una señal de petición de PTS (Selección del Tipo de Protocolo) (PTS1) a la segunda tarjeta 31 para realizar la negociación de PTS (etapa S506). A continuación, el dispositivo de generación de petición de PTS 315b de la segunda tarjeta 31 generará una señal de petición de PTS (PTS2) para la primera tarjeta 32. En respuesta a la PTS2, la primera tarjeta 32 envía una señal de respuesta de PTS (PTS3) de vuelta a la segunda tarjeta 31. Por consiguiente, el dispositivo de determinación de PTS 315a de la segunda tarjeta 31 determina si el protocolo indicado por la primera señal de petición de PTS emitida desde el terminal de transacción 30 es capaz de ser realizado tanto por la primera tarjeta 32 como por la segunda tarjeta 31 de acuerdo con la PTS3 enviada desde la primera tarjeta 31. A continuación, el dispositivo de generación de respuesta de PTS 315c de la segunda tarjeta 31 enviará otra señal de respuesta de PTS (PTS4) para el terminal de transacción 30. Esta secuencia continuará hasta que el protocolo indicado del terminal de transacción 30 sea aceptado entre el terminal de transacción 30 y la segunda tarjeta 31, y entre la segunda tarjeta 31 y la primera tarjeta 32.

Una vez que se ha encontrado un protocolo indicado, el terminal de transacción 30 enviará una señal de APDU de comando (c-APDU1) al dispositivo de determinación de APDU de comando 316a de la segunda tarjeta 31 (etapa S507) solicitando una transacción. Después de recibir la c-APDU1, el dispositivo de determinación de APDU de comando 316a determina si la c-APDU1 solicita una transacción por defecto o una transacción diana (etapa S508). Si la c-APDU1 emitida desde el terminal de transacción 30 solicita una transacción diana, el dispositivo de generación de APDU de comando 316b de la segunda tarjeta 31 generará una señal de APDU de comando (c-APDU2) para la primera tarjeta 32 (etapa S509), y a continuación realizará la transacción diana (etapa S510). La primera tarjeta 32 enviará una APDU de respuesta (r-APDU1) a la memoria tampón 318 de la segunda tarjeta 31 después de que la transacción diana se ha realizado (etapa S511). Después de recibir la r-APDU1 desde la primera tarjeta 32, el dispositivo de generación de APDU de respuesta 317 de la segunda tarjeta 32 genera a continuación otra señal de APDU de respuesta (r-APDU2) para el terminal de transacción 30 que indica que la transacción diana ha finalizado (etapa S512).

En esta realización de la presente invención, la información relacionada con la transacción es reescrita por el procesador 310 cuando una petición de transacción emitida desde la primera tarjeta es aprobada por el terminal de transacción 30 en base a la primera o segunda información de identificación. Por ejemplo, la información relacionada con la transacción puede ser un balance para un valor de tarjeta de débito, y el procesador 310 puede aumentar/reducir el balance cuando se realiza la transacción.

Además, la segunda tarjeta 31 puede detectar la existencia de la primera tarjeta 32 calculando el tiempo de respuesta de ATR1 desde la primera tarjeta 32 cuando el sistema de tarjeta doble es insertado en un terminal de transacción; como alternativa, la segunda tarjeta 31 puede proporcionar una interfaz del usuario tal como el Menú de conjunto de herramientas de aplicación SIM de la tarjeta SIM para que el usuario configure la presencia de la primera tarjeta si el sistema de tarjeta doble es insertado en un teléfono móvil.

Por ejemplo, una tarjeta POS (Punto de Venta), que almacena valores, se considera como la segunda tarjeta 31 de la presente invención, y una tarjeta ATM, que almacena una cuenta bancaria, se considera como la primera tarjeta 32. Ambas dos tienen funciones originales. En la presente invención, la tarjeta POS puede considerarse como una tarjeta maestra, que es también un lector de tarjetas y capaz de leer la tarjeta ATM en un terminal de transacción. Por lo tanto, un usuario puede enviar dinero desde la cuenta bancaria almacenada en la tarjeta ATM al monedero electrónico de la tarjeta POS mediante el terminal de transacción de acuerdo con la presente invención. En el caso del sistema de tarjeta doble en un teléfono móvil, la tarjeta SIM se considera como la segunda tarjeta, y una tarjeta POS se considera como la primera tarjeta de la presente invención, un usuario puede recargar dinero el monedero electrónico de la tarjeta POS mediante un mensaje corto terminado en el móvil desde el banco en respuesta a un mensaje corto originado desde el móvil del usuario, para recargar al máximo la tarjeta POS. En este caso, el teléfono celular se considera como el terminal. Por consiguiente, la presente invención proporciona un sistema de tarjeta doble para su uso con dos terminales de transacción diferentes para facilitar la transacción de información en la práctica.

Por favor remítase a la figura 4. Ésta ilustra un diagrama de bloques de una tarjeta inteligente en un sistema de tarjeta doble para su uso con un terminal de comunicación que no pertenece a la presente invención. Tal como se muestra en la figura 4, el sistema de tarjeta doble para su uso con el terminal de comunicación 40 está constituido por una primera tarjeta 42 y una segunda tarjeta 41. La primera tarjeta 42 tiene una primera memoria 421 para almacenar una primera información de identificación que incluye primera información personal, primeras claves secretas, y primera función de seguridad para su uso en comunicación con un terminal remoto 49 mediante el terminal de comunicación 40. La segunda tarjeta 41 incluye un procesador 410, una segunda memoria 411, una tercera memoria 412 y un dispositivo de selección 413. La segunda memoria 411 almacena segunda información de identificación que incluye segunda información personal, segundas claves secretas y segunda función de seguridad para su uso en comunicación con un terminal remoto 49 mediante el terminal de comunicación 40. La tercera

memoria 412 puede almacenar la primera información personal que no está protegida por la primera tarjeta 32. El dispositivo de selección 413 es para determinar una función de seguridad de la primera tarjeta y la segunda tarjeta que se va a realizar. El procesador 410 efectúa o no la primera tarjeta 42 en base a si la primera tarjeta o la segunda tarjeta es seleccionada por el dispositivo de selección 413.

5 En la figura 4, cualquiera de la primera tarjeta 42 y la segunda tarjeta 41 podría ser una tarjeta SIM (Módulo de Identificación del Abonado), tarjeta USIM (Módulo de Identificación del Abonado Universal), tarjeta UIM (Módulo de Identificación del Usuario) y tarjeta RUIM (Módulo de Identificación del Usuario Extraíble), que se usan para diferentes sistemas de comunicación por telefonía móvil. Cuando dos tarjetas SIM son consideradas como la primera tarjeta 42 y la segunda tarjeta 41, respectivamente, la segunda tarjeta SIM podría integrar ambas informaciones de dos tarjetas SIM, tales como dos agendas telefónicas. El dispositivo de selección es presentado normalmente por un menú de Conjunto de Herramientas SIM que proporciona la interfaz del usuario para seleccionar la SIM que se va a usar para registrarse a la red de telefonía móvil. En la práctica, el sistema de tarjeta doble es capaz de integrar dos tarjetas SIM en un terminal de comunicación, es decir, teléfono móvil. Una compañía de telecomunicaciones por telefonía móvil podría proporcionar el servicio a su usuario para integrar una vieja tarjeta SIM de otra compañía con una nueva tarjeta SIM. El usuario podría realizar una llamada telefónica con dos identificaciones diferentes seleccionando una de las dos tarjetas SIM a su propia elección.

10 Aunque la invención se ha descrito en términos de lo que actualmente se considera que son las realizaciones más prácticas y preferidas, debe entenderse que no es necesario limitar la invención a las realizaciones descritas. Por el contrario, se pretende abarcar diversas modificaciones y disposiciones similares incluidas dentro del alcance de las reivindicaciones adjuntas, que deben coincidir con la interpretación más amplia para abarcar todas de dichas modificaciones y estructuras similares.

REIVINDICACIONES

- 5 1. Una tarjeta inteligente (31) que comprende un procesador (310) y una primera interfaz para su uso en comunicación con un terminal (30), incluyendo dicho procesador (310) medios de generación de ATR (319) para generar una señal de ATR **caracterizada porque** dicha tarjeta inteligente (31) tiene una segunda interfaz para su uso en comunicación con otra tarjeta inteligente (32) y medios de generación de RST (314b) para generar una señal de reset (RST) para dicha otra tarjeta inteligente (32), permitiendo de este modo que dicha otra tarjeta inteligente (32) esté controlada por dicha tarjeta inteligente (31).
- 10 2. La tarjeta inteligente de acuerdo con la reivindicación 1, en la que dicho procesador (310) incluye, además, una memoria tampón (318) para recibir y guardar una señal de ATR, Respuesta Al Reset, desde dicha otra tarjeta inteligente (32).
3. La tarjeta inteligente de acuerdo con la reivindicación 1, en la que dicho procesador (310) incluye, además, medios de generación de una petición de PTS, Selección del Tipo de Protocolo, (315b) para generar una señal de petición de PTS para dicha otra tarjeta inteligente (32).
- 15 4. La tarjeta inteligente de acuerdo con la reivindicación 1, en la que dicho procesador (310) incluye, además, medios de generación de una respuesta de PTS (315c) para generar una señal de respuesta de PTS para dicho terminal (30).
5. La tarjeta inteligente de acuerdo con la reivindicación 4 3, en la que dicho procesador (310) incluye, además, medios de determinación de PTS (315a) para determinar si dicha señal de petición de PTS es aceptable tanto por dicho terminal (30) como por dicha otra tarjeta inteligente (32).
- 20 6. La tarjeta inteligente de acuerdo con la reivindicación 1, en la que dicho procesador (310) incluye, además, un regulador del reloj (34a) para proporcionar una frecuencia de reloj para dicha otra tarjeta inteligente (32).
7. La tarjeta inteligente de acuerdo con la reivindicación 1, en la que dicho procesador (310) incluye, además, medios de determinación de APDU, Unidad de Datos del Protocolo de Aplicación, de comando (316a) para determinar si una señal de APDU de comando emitida desde dicho terminal (30) está asociada con dicha tarjeta inteligente (31) o dicha otra tarjeta inteligente (32).
- 25 8. La tarjeta inteligente de acuerdo con la reivindicación 1, en la que dicho procesador (310) incluye, además, medios de generación de APDU de comando (316b) para generar una señal de APDU de comando para dicha otra tarjeta inteligente (32).
- 30 9. La tarjeta inteligente de acuerdo con la reivindicación 1, en la que dicho procesador (310) incluye, además, una memoria tampón (318) para recibir y guarda una señal de APDU de respuesta desde dicha otra tarjeta inteligente (32).
10. La tarjeta inteligente de acuerdo con la reivindicación 1, en la que dicho procesador (310) incluye, además, medios de generación de APDU de respuesta (317) para generar una señal de APDU de respuesta para dicho terminal (30).
- 35 11. La tarjeta inteligente de acuerdo con la reivindicación 1, en la que dicha tarjeta inteligente (31) está provista de una antena para comunicación con otro terminal (30).
- 40 12. La tarjeta inteligente de acuerdo con la reivindicación 1, en la que dicha tarjeta inteligente (31) comprende una tarjeta SIM, Módulo de Identificación del Abonado, tarjeta USIM, Módulo de Identificación del Abonado Universal, tarjeta UIM, Módulo de Identificación del Usuario y tarjeta RUIM, Módulo de Identificación del Usuario Extraíble.
13. La tarjeta inteligente de acuerdo con la reivindicación 1, en la que dicha tarjeta inteligente (31) o dicha otra tarjeta inteligente (32) comprende una tarjeta ATM.

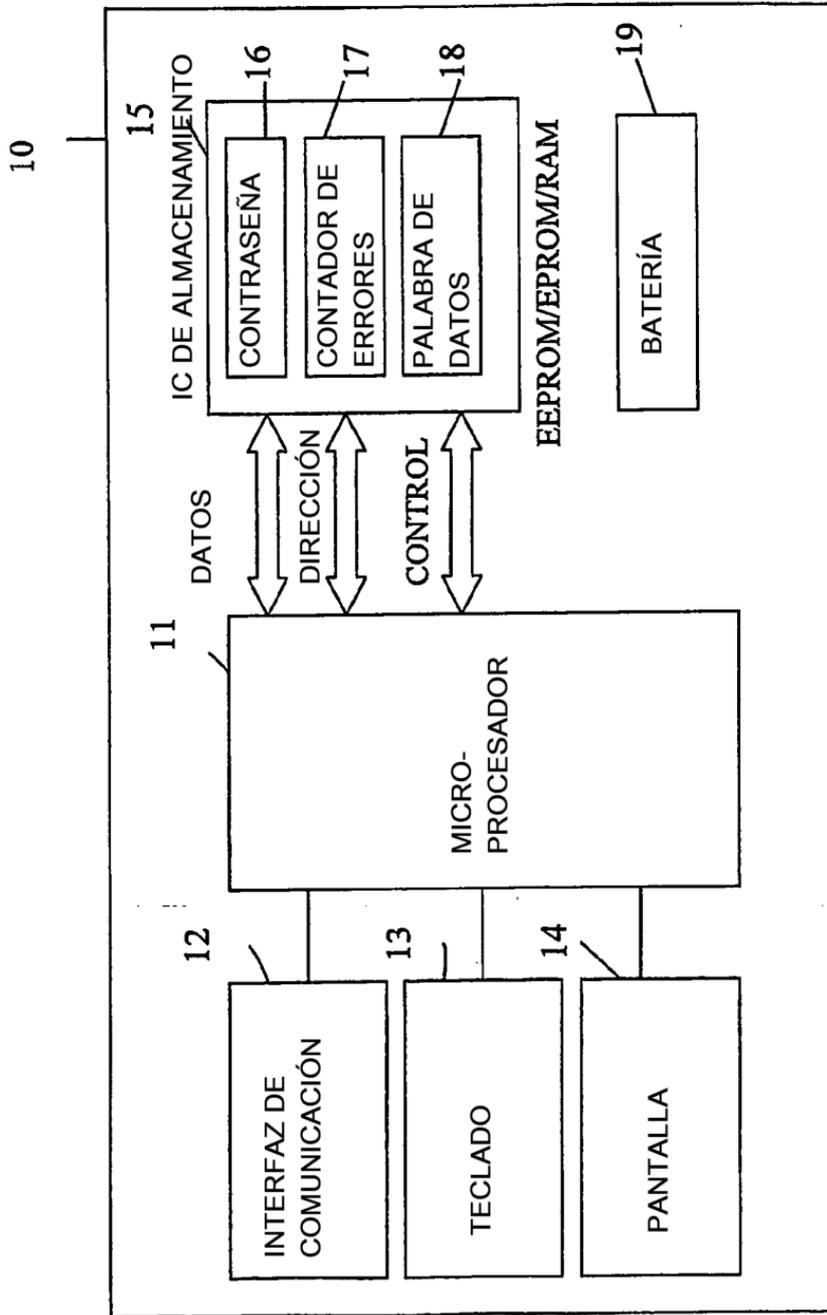


Fig. 1

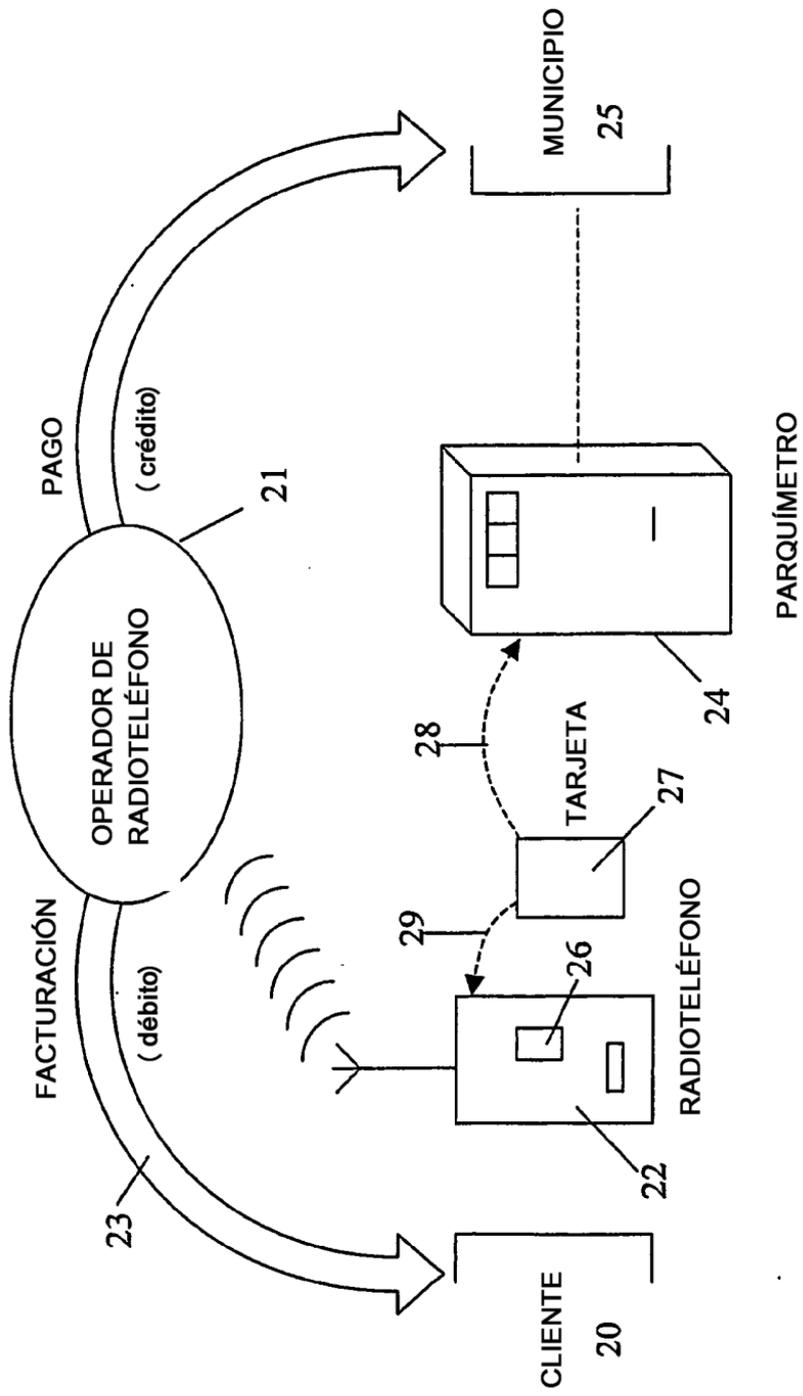


Fig. 2

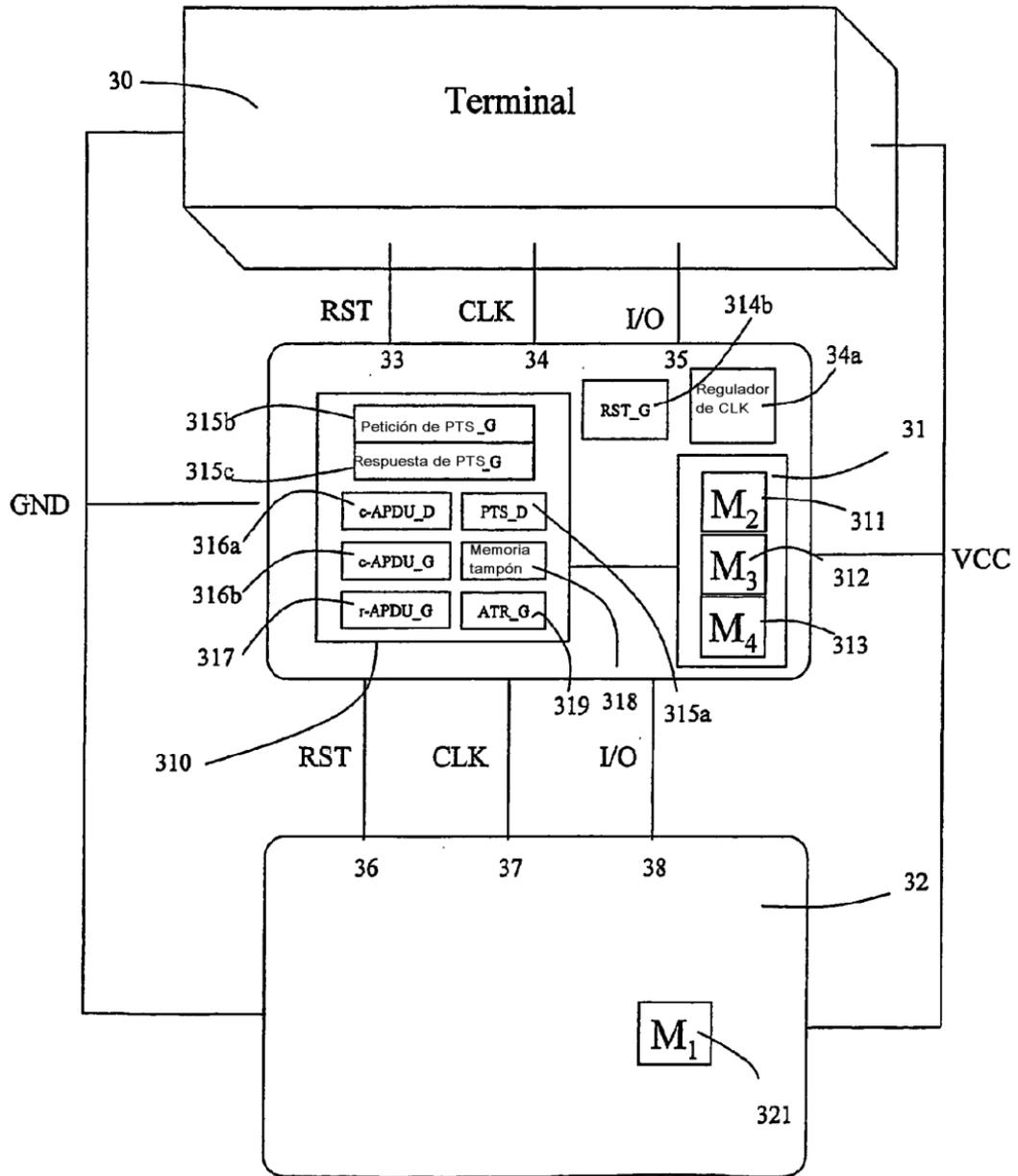


Fig. 3

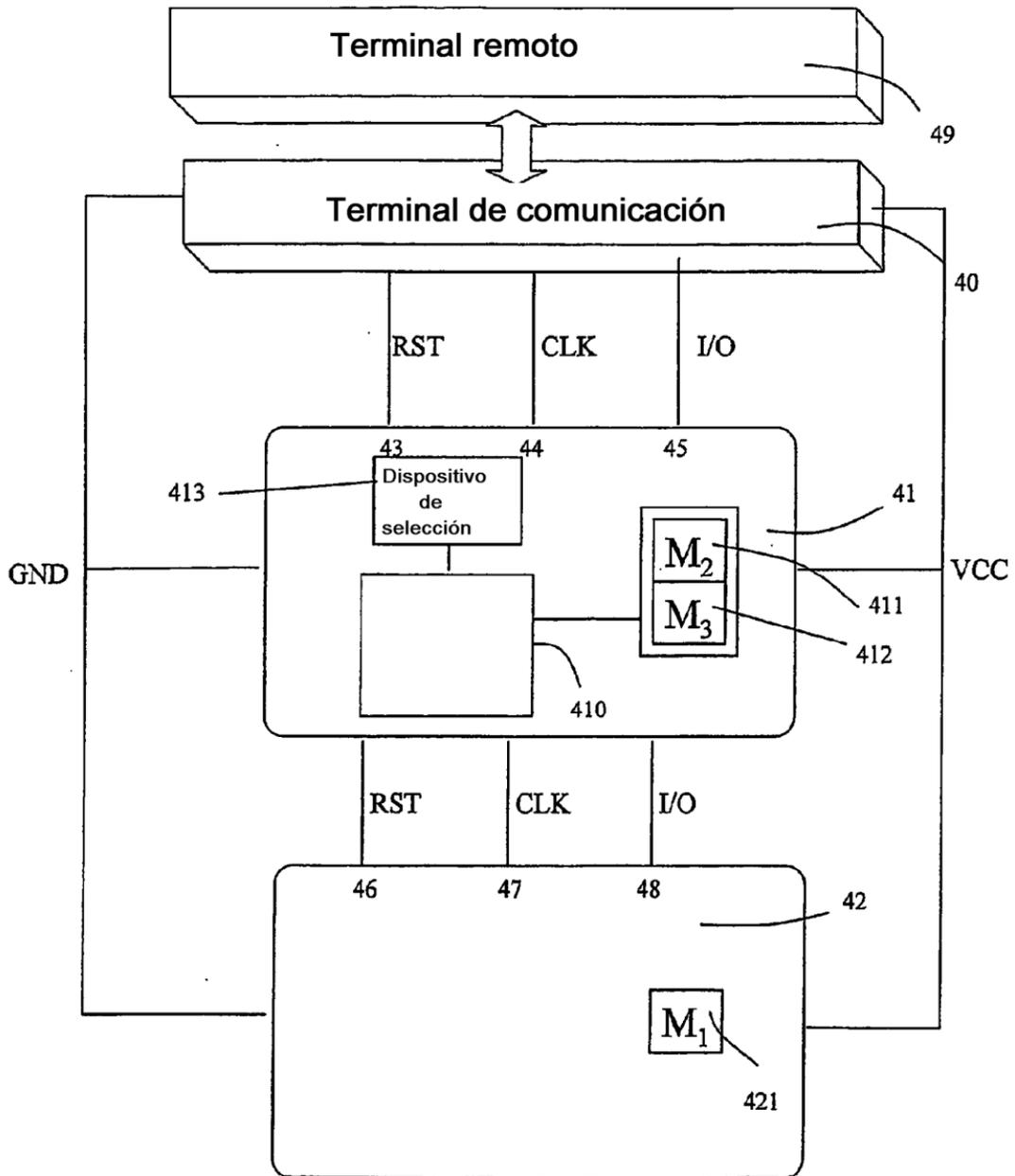


Fig. 4

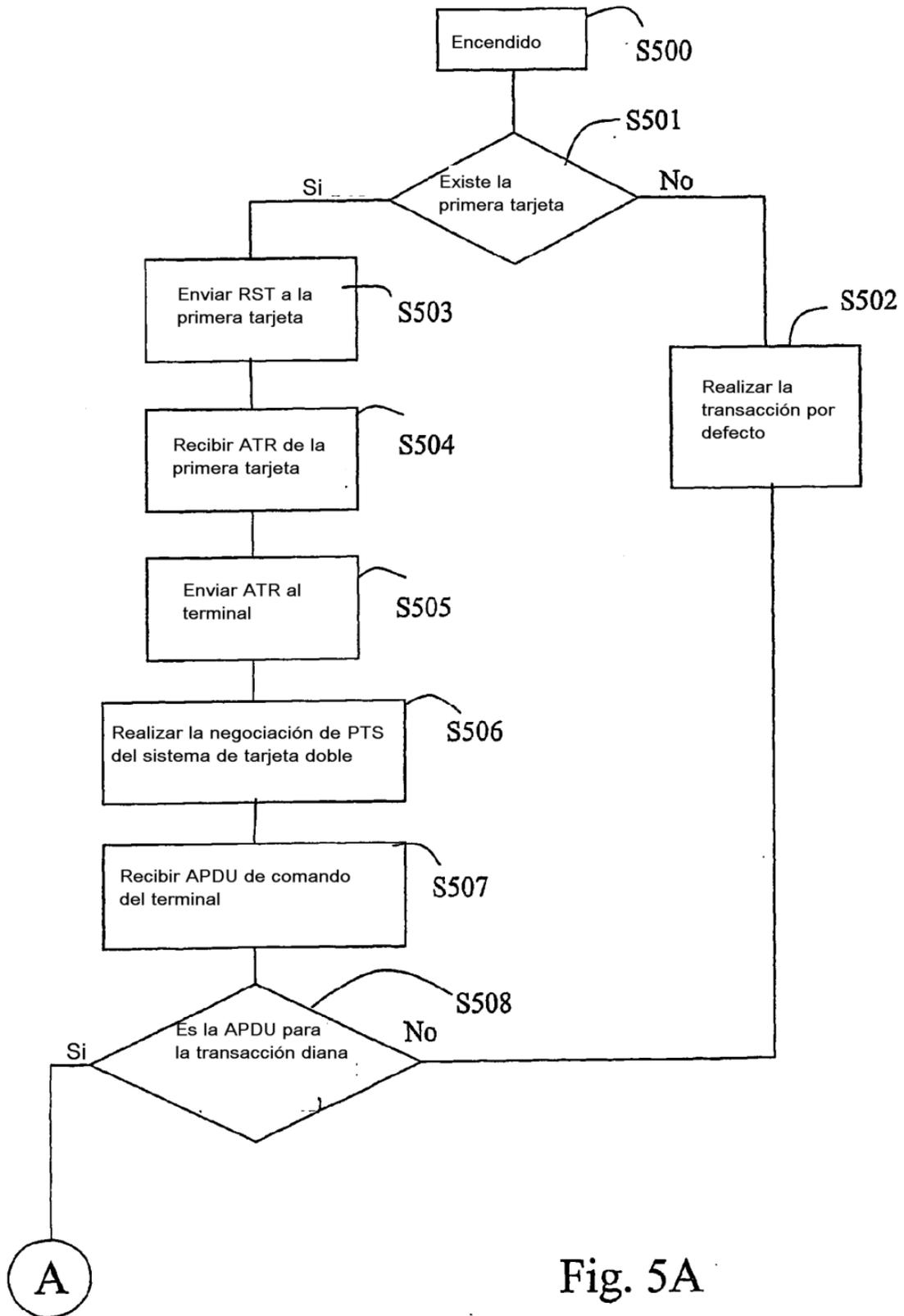


Fig. 5A

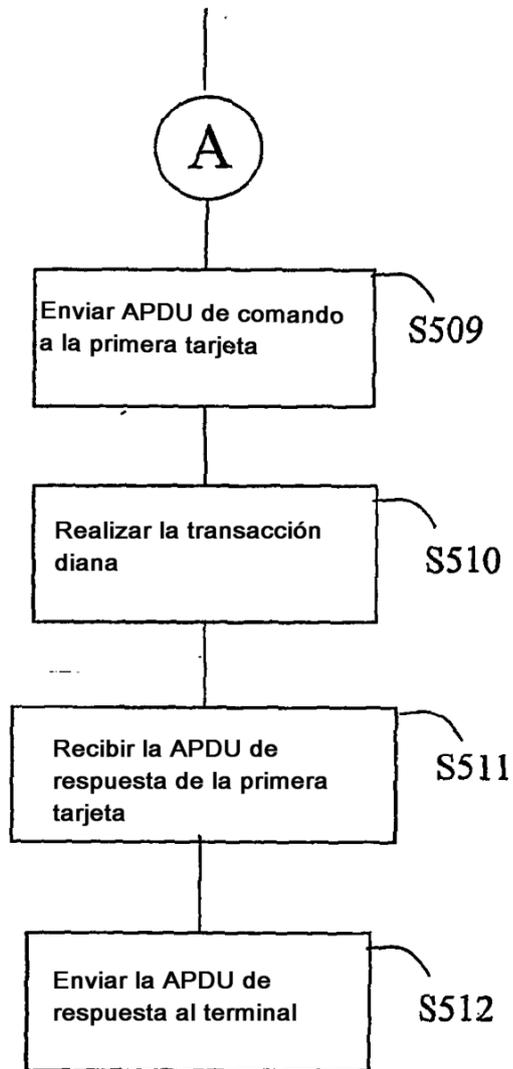


Fig. 5B