

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 551 942**

51 Int. Cl.:

G06K 19/073 (2006.01)

G06K 7/00 (2006.01)

G06K 7/10 (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Fecha de presentación y número de la solicitud europea: **13.03.2009 E 09719191 (0)**

97 Fecha y número de publicación de la concesión europea: **29.07.2015 EP 2255324**

54 Título: **Procesamiento optimizado de una instrucción en el ámbito de la comunicación con tarjetas de chip**

30 Prioridad:

14.03.2008 DE 102008014037

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

24.11.2015

73 Titular/es:

**GIESECKE & DEVRIENT GMBH (100.0%)
Prinzregentenstrasse 159
81677 München, DE**

72 Inventor/es:

**HOLLY, RALF y
LUTZ, KATRIN**

74 Agente/Representante:

DURÁN MOYA, Luis Alfonso

ES 2 551 942 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

Procesamiento optimizado de una instrucción en el ámbito de la comunicación con tarjetas de chip

5 La invención se refiere al sector de la tecnología de las tarjetas de chip, en especial, a la técnica de radio móvil y se refiere al procesamiento de las instrucciones que se intercambian entre una tarjeta de chip (tarjeta SIM) y un dispositivo de lectura de tarjetas (un aparato de usuario, tal como, por ejemplo, una estación móvil o similar). La invención se refiere, en especial a un procedimiento, a un soporte de datos móvil, a un sistema, a un medio de lectura por ordenador, a un producto de programa de ordenador/el procesamiento de una instrucción que se
10 transfiere mediante un protocolo estandarizado, en especial, según la norma ISO/IEC7816 desde un lector de tarjetas a un soporte móvil de datos.

Para el intercambio de datos entre la tarjeta de chip y un dispositivo de lectura de tarjetas se utiliza un esquema de comunicación fijo. Este esquema de comunicación, se basa en un llamado modelo maestro-esclavo, en el que el
15 terminal del maestro está definido para emitir instrucciones y, en el que la tarjeta actúa como esclavo, estando definida para el procesamiento de las instrucciones y para el reenvío de respuestas a dichas instrucciones. En esta situación, todas las acciones salen básicamente del terminal. La tarjeta reacciona solamente, como esclavo, ante las instrucciones del terminal y efectúa el procesamiento de estas.

20 Para la comunicación entre tarjetas de chip y un lector de tarjetas, existen varias normas. Así, por ejemplo, la norma ISO 7816-3 está destinada a las características eléctricas de los contactos y protocolo de comunicación, mientras que la norma ISO 7816-4 está destinada a cubrir los contenidos de la comunicación, estructura de datos de la tarjeta de chip, arquitectura de seguridad, mecanismos de acceso y similares. Además, se pueden utilizar diferentes protocolos de transmisión de datos. Los protocolos más habituales son en este caso, el protocolo T=0, el protocolo
25 T=1 (así como el protocolo T=14, que se utiliza especialmente en Alemania), de manera que los protocolos T=0 y T=1 están regulados por la norma ISO 7816-3. El protocolo, T=0 se trata de un protocolo asíncrono orientado a bytes, mientras que el protocolo T=1 es un protocolo orientado a bloques. En especial para el sector de la técnica de radio móvil y del intercambio de datos entre tarjetas SIM y aparatos móviles (ME, equipo móvil) sirve la norma GSM11.11 (que después de la nueva nomenclatura corresponde a ETS 300608) o bien la norma 3 GPP-TS 51.011,
30 que regula las interfaz y las estructuras lógicas.

La comunicación entre la tarjeta de chip y el terminal tiene lugar mediante unidades de instrucciones y unidades de respuesta. Estas unidades son paquetes de datos que están estructurados de acuerdo con un formato previamente definido. Según los casos, según la capa de un modelo de capas OSI/ISO involucrada, estas unidades son APDU
35 (Application Protocol Data Unit) o TPDU (Transmission Protocol Data Unit), cuando se involucra la capa de conducción. El formato y las normas para las APDU están definidas en la norma ISO (International Organization for Standardization) 7816-4.

El intercambio de datos entre las tarjetas de chip y el terminal comprende instrucciones y respuestas a estas
40 instrucciones, de manera que una instrucción es correspondida siempre por el terminal mediante la emisión de una comunicación de instrucción. Esta instrucción, o bien esta orden, es transferida del terminal a la tarjeta de chip en una llamada APDU de instrucción (Command APDU, C-APDU). La tarjeta de chip procesa la instrucción y envía una respuesta en forma de una APDU de respuesta (Response APDU, R-APDU) al terminal. Por lo tanto, una determinada APDU de respuesta se refiere siempre a una determinada APDU de instrucción. Esta referencia se
45 designa también como pareja, instrucción-respuesta. En una pareja de este tipo de instrucción-respuesta, la

comunicación de la instrucción y la comunicación de respuesta, pueden comprender datos.

5 Según la norma de base o bien el protocolo de transferencia, se prevé una clase de instrucciones que comprende instrucciones, en las que el terminal envía instrucciones (con o sin datos) a la tarjeta para permitir el procesamiento de la tarjeta, para preparar datos de contestación en la tarjeta, que más adelante, en un momento de tiempo determinado, puedan ser solicitados por el terminal, de manera explícita y mediante una instrucción de petición separada. En esta clase de instrucciones, están acopladas las instrucciones correspondientes, siempre con una instrucción de petición correspondiente (para recoger los datos de contestación en la instrucción correspondiente).

10 En esta clase de instrucciones, se pondrá en marcha mediante la instrucción, por ejemplo, mediante la orden SELECT, llevar a cabo procesamiento en la tarjeta. Las respuestas pueden ser recogidas con intermedio de una instrucción de petición especial, por ejemplo, mediante la orden GET RESPONSE.

15 No obstante, existen utilizaciones que requieren solamente la emisión de la instrucción correspondiente sin que sea necesario para ello recoger datos de respuesta. En estas utilizaciones, la instrucción de petición constituye una interrupción.

20 Como inconveniente esencial, se manifiesta en el estado de la técnica para el protocolo T=0, que el terminal no puede señalar que en una determinada instrucción no desea datos de respuesta, o bien que no se emite instrucción alguna de petición. Por lo tanto, la tarjeta pone a disposición los datos de respuesta en cada caso, aunque no sean necesarios para la utilización específica. El tiempo de procesamiento que es necesario para preparar además de la acción de instrucción propiamente dicha, los datos de la respuesta, se debe considerar en otras palabras como "tiempo perdido" y conduce a problemas sensibles de rendimiento.

25 Para superar el inconveniente de rendimiento explicado y para optimizar el procesamiento de la instrucción en la tarjeta de chip y para su estructuración variable, la presente invención se propone el objetivo de mejorar u optimizar el procesamiento de la instrucción, incluso en aquellos casos (con respecto al tiempo de procesamiento y potencia de cálculo), en los que el terminal no reclama o no pide datos de respuesta.

30 El documento US-A-5942738 da a conocer las características de la parte introductoria de las reivindicaciones 1 y 12.

35 Este objetivo se consigue mediante el objeto de las presentes reivindicaciones independientes, en especial, mediante un procedimiento, un soporte de datos móvil, un sistema y un producto de programa de ordenador para la preparación de instrucciones, que son transferidas dentro del ámbito de la comunicación entre un soporte de datos móvil y un lector de tarjetas.

40 Este objetivo se consigue, en particular, mediante un procedimiento para el procesamiento de una instrucción para un soporte de datos móvil, en especial para una tarjeta de chip, de manera que la instrucción es transmitida con intermedio de un protocolo normalizado, preferentemente, según la norma ISO-7816 desde un lector de tarjetas al soporte móvil de datos y, de manera que la instrucción prevé la generación de datos de respuesta y/o el envío de datos de respuesta al lector de tarjetas del soporte de datos móvil, de manera que los datos de respuesta serán solicitados en un momento de tiempo posterior del lector de tarjetas por una instrucción de petición emitida, presentando las siguientes etapas de procedimiento:

- captar la instrucción por parte del soporte de datos móvil;
 - generar y enviar una respuesta al lector de tarjetas, de manera que la respuesta consista solamente en un código de confirmación que muestra que los datos de la respuesta se pueden reclamar del soporte de datos móvil;
 - determinar si el lector de tarjetas pide los datos de respuesta con una instrucción de petición y en caso positivo:
- 5 - generar los datos de respuesta a la instrucción con respecto al soporte de datos y enviar los datos de respuesta al lector de tarjetas, de manera que la generación de los datos de respuesta empezará o será llevada a cabo solamente después de la emisión de la instrucción de petición por parte del lector de tarjetas o después de conseguir la instrucción de petición por parte del soporte móvil de datos.
- 10 Como aclaración, se puede indicar que dentro de la generación de datos de respuesta, también se debe comprender la necesaria realización de la instrucción captada por parte del soporte de datos.

A continuación, se explicarán de manera más detallada el alcance de las características de la solución que aporta la invención.

- 15
- En cuanto al soporte de datos móvil, se trata habitualmente de una tarjeta de chip. La tarjeta de chip puede estar constituida en forma de tarjeta inteligente, tarjeta SIM para utilizaciones GSM o también como tarjeta para utilizaciones no relacionadas con aparatos de radio móviles. Normalmente, la tarjeta chip comprende un circuito integrado (Integrated Circuit, IC) y elementos constitutivos de almacenamiento. También puede estar constituida en
- 20 forma de tarjeta de aplicaciones múltiples.

- El lector de tarjetas, o bien el dispositivo lector de tarjetas, se refiere a un aparato electrónico que está dispuesto para comunicar con la tarjeta de chip. Igualmente, se puede comprender bajo el concepto "lector de tarjetas" un terminal, de manera que la solución de acuerdo con la invención no está limitada a un determinado tipo de terminal,
- 25 comprendiendo una estación móvil (mobile station, MS; en especial teléfono móvil), un aparato móvil (equipo móvil, ME) un IFD (Interface Device), un CAD (Chip Accepting Device), un CCR (Chip Card Reader), un lector de tarjetas inteligentes y un adaptador de tarjetas inteligentes. Además, la presente invención puede ser utilizada sobre terminales portátiles y estacionarios.

- 30 En cuanto al protocolo, se trata en la forma de realización preferente del protocolo T=0, según la norma ISO 7816. Formas de realización alternativas de la invención prevén también otros protocolos que de manera correspondiente puede estar dispuestos según otras normas, tales como, por ejemplo, el protocolo T=1, el protocolo T=14, etc.

- La instrucción (o bien la orden) corresponde a una clase de instrucciones que pueden provocar el procesamiento de
- 35 datos en el soporte de datos móvil. En la preparación de la instrucción en un soporte de datos móvil se generan los datos de respuesta con referencia a la correspondiente instrucción que deben ser pedidos mediante una instrucción de petición siguiente separada del terminal. La clase de instrucciones se caracteriza por instrucciones que prevén que los datos de respuesta correspondientes a la instrucción deben ser solicitados con una instrucción de petición separada (para petición de los datos de respuesta) en un momento de tiempo posterior, en caso que el terminal requiera los datos de respuesta. En la forma de realización preferente, se trata en cuanto a la instrucción de una
- 40 instrucción de selección para archivos de datos, en especial, la instrucción SELECT y para la instrucción de petición de la instrucción GET RESPONSE. No obstante, son posibles otras parejas de instrucción-instrucción de petición, por ejemplo, instrucciones de búsqueda y/o lectura (por ejemplo, SEEK, SEARCH) u otras instrucciones de petición para recoger datos de respuesta. Otras instrucciones y/o instrucciones de petición dependen de la correspondiente

utilización y se deducen de la norma ISO/IEC 7816-4. Es esencial, que la instrucción pueda poner en marcha la preparación de datos de respuesta en la tarjeta de chip, que estos datos de respuesta deban ser recogidos o pedidos siempre con una instrucción de petición separada del terminal. No está previsto enviar inmediatamente al terminal los datos de respuesta después de recibir la instrucción.

5 En una forma de realización ventajosa, el procedimiento basado en ordenador, según la invención, se basa en la siguiente sucesión temporal de etapas de procedimiento:

- captar la instrucción;
- 10 - generar y enviar una respuesta al lector de tarjetas sin generar, o preparar datos de respuesta en la tarjeta;
- determinar si a la instrucción captada, ha facilitado una instrucción de petición y solamente en caso afirmativo:
- generar, preparar y/o enviar los datos de respuesta al lector de tarjetas.

15 De otro modo, en caso de que no se ha facilitado ninguna instrucción de petición (y, por lo tanto, no se han pedido datos de respuesta) no se preparan, disponen o generan datos de respuesta en la tarjeta de chip.

Como aclaración, se puede indicar que con el término generar una respuesta, se comprende también la necesaria realización de la instrucción captada por el lado del soporte de datos.

20 De esta manera, se puede conseguir, de acuerdo con la invención, un ahorro sensible de tiempo, dado que la preparación engorrosa de datos de respuesta, se lleva a cabo solamente en el caso de que ello sea necesario (es decir, cuando se han pedido del terminal datos de respuesta).

25 La captación de la instrucción tiene lugar mediante el proceso de la correspondiente unidad de mando APDU en el soporte de datos móvil. La generación y envío de una respuesta será llevada a cabo en la tarjeta, de manera que la respuesta es una señal de confirmación, de acuerdo con el formato previamente definido de la respuesta APDU (respuesta APDU) y, además del obligado "Trailer" (que comprende palabras de situación 1 y 2; SW1, SW2) capta adicionalmente la longitud de los datos de respuesta esperados. La respuesta no contiene datos de contestación o datos de respuesta, porque estos solamente se deben preparar o generar dependiendo de ciertos eventos (es decir, dependiendo de la existencia de una instrucción de petición) en un momento de tiempo posterior.

30 Para determinar si el lector de tarjetas pide datos de respuesta recuperables, se evaluarán de acuerdo con la invención, las otras instrucciones siguientes a la correspondiente instrucción, de manera directa o indirecta y se analizará si se trata en cuanto a la instrucción adicional de una instrucción de petición para la instrucción.

35 En una forma de realización alternativa ventajosa se analizarán otras instrucciones adicionales siguientes, por si contienen una instrucción de petición, con respecto a la correspondiente instrucción. Entre la instrucción y una instrucción de petición, se pueden intercambiar, por lo tanto, datos variados. La determinación se basa, por lo tanto, en una diferenciación de un caso.

40 La generación de datos de respuesta, comprende básicamente todos los tipos de preparación de datos y puede corresponder a una señal binaria (SI o No). Igualmente es posible que los datos de respuesta sean preparados o estén dispuestos. La forma de preparación depende de la correspondiente instrucción.

De acuerdo con otro aspecto de la invención se prevé que la generación de datos de respuesta es llevada a cabo cuando se ha conseguido o se ha captado la instrucción de petición del soporte de datos móvil. No obstante, es posible también llevar a cabo la generación de los datos de respuesta dependiendo de la disposición de la instrucción, desde el lado del terminal. En el primer caso, tiene lugar la determinación (de si el lector de tarjetas pide datos de respuesta) en el lado del soporte de datos, en el que se analizará la recepción de la instrucción de petición. En el segundo caso, la determinación tiene lugar en el lado del terminal, en el que se analizará si el terminal ha enviado o dispuesto la instrucción de petición.

En una forma preferente de realización, se prevé que la generación de los datos de respuesta solamente se lleva a cabo cuando se ha terminado satisfactoriamente la etapa de procedimiento de la determinación. En una forma de realización alternativa es también posible que se empiece la generación de los datos de respuesta solamente cuando se ha llevado a cabo de manera satisfactoria la determinación. El segundo caso se refiere también a un proceso claramente secuencial, mientras que el primer caso prevé también una preparación de datos parcial (generación de datos de respuesta) en la tarjeta de chip.

A continuación, se describirá la invención en base a la solución que se presenta por parte de la presente invención. En este caso, las características explicadas, formas de realización alternativas y/o ventajas se pueden aplicar igualmente a las otras soluciones del objetivo, en especial en soportes de datos móviles, sobre el producto, el medio y/o el sistema, e igualmente de forma inversa. Con otras palabras, el soporte de datos móvil, el producto, el medio y/o el sistema, pueden ser desarrollados adicionalmente con las características que se describen o reivindican en relación con el procedimiento. Para ello, las correspondientes características funcionales del procedimiento serán implementadas mediante correspondientes módulos de hardware y/o de software, que están destinados a llevar a cabo la correspondiente función.

De acuerdo con una forma de realización preferente la instrucción, la instrucción de petición, la respuesta y los datos de respuesta serán transferidos mediante una unidad de comunicación encapsulada separada. En una unidad de comunicación del modelo de capas ISO/OSI están comprendidas las unidades de comunicación APDU, las APDU de instrucciones y las APDU de respuesta. En una capa de potencia del modelo de capas ISO/OSI, son las unidades de comunicación TPDU.

El código de confirmación, que es enviado como respuesta a la instrucción de la tarjeta de chip al terminal, muestra que los datos de respuesta se pueden reclamar en el soporte de datos móvil. El código de confirmación no comprende datos de respuesta. El código de confirmación es, por el contrario, una señal con una información binaria (existe o no). En una forma de realización preferente, el código de confirmación comprende un código de retorno, que facilita la longitud de los datos de respuesta esperados. Relacionado con el protocolo T=0 se utilizará en este caso, una palabra especial de estado SW1SW2 (por ejemplo, 9FXX, en la que XX significa la longitud de los datos que se pueden reclamar).

Una realización adicional ventajosa del procedimiento de la invención consiste en cubrir también un caso de fallo y señalar este al terminal. Un caso de fallo puede consistir, por ejemplo, en que los datos de respuesta no se pueden reclamar en la instrucción, o que ha tenido lugar otro tipo de alteración de la comunicación entre el lector de tarjetas y la tarjeta de chip, de manera que, no se han transferido datos y/o instrucciones o no lo han sido de manera completa. A este respecto, la respuesta puede comprender un código de fallos que señala el caso de fallo al terminal, en caso de que los datos de respuesta no se pueden reclamar, o en el caso de que una instrucción anterior

no se puede o no se pudo llevar a cabo.

Un campo de utilización principal para el procedimiento de la invención son, la instrucción "SELECT" y la instrucción de petición "GET RESPONSE". De manera alternativa, se pueden prever también cualquier otra pareja de instrucción-instrucción de respuesta en las que una instrucción requiera una instrucción de petición que está definida para la recogida de datos de la instrucción.

De acuerdo con una forma de realización preferente, el procedimiento se utilizará para una tarjeta SIM en un terminal móvil, en especial, durante el funcionamiento del terminal móvil, puesto que, en este caso, de acuerdo con la invención se consigue un ahorro de tiempo máximo al evitar preparaciones e instrucciones innecesarias en la tarjeta.

Otra solución adicional del objetivo consiste en un soporte de datos móvil con una unidad de proceso y un código de programa, que está definido para la realización en el soporte de datos y/o en el lector de tarjetas y, en el que está implementado el procedimiento que actualmente se describe.

Otra solución adicional del objetivo, consiste en un sistema para el proceso de una instrucción que presenta:

- como mínimo, un soporte de datos móvil,
- como mínimo, un lector de tarjetas que envía una instrucción al soporte de datos móvil, de manera que la instrucción es transferida mediante un protocolo normalizado y, que prevé la generación de datos de respuesta desde el soporte de datos móvil, de manera que los datos de respuesta son pedidos por medio de una instrucción de petición separada del lector de tarjetas;
- como mínimo, una interfaz para comunicación entre el soporte de datos móvil y el lector de tarjetas, que está preparada para enviar una instrucción y opcionalmente una instrucción de respuesta separada del lector de tarjetas al soporte de datos móviles y que está preparada para enviar una respuesta y, opcionalmente datos de respuesta del soporte de datos móvil al lector de tarjetas, de manera que el soporte de datos móvil, comprende lo siguiente:
 - como mínimo, un módulo de captación que está definido para la captación de la instrucción del lado del soporte de datos móvil;
 - como mínimo, un generador de respuesta, que está previsto para la generación y envío de una respuesta al lector de tarjetas, de manera que la respuesta consiste solamente en un código de confirmación, que muestra que los datos de respuesta pueden ser reclamados en el soporte de datos móvil;
 - como mínimo, un módulo de determinación que está dispuesto para determinar si el lector de tarjetas pide los datos de respuesta que se pueden reclamar con una instrucción siguiente de petición;
 - como mínimo, un generador de respuesta que está preparado, además, para generar datos de respuesta a la instrucción en el soporte de datos móvil y enviar los datos de respuesta al lector de tarjetas, de manera que el generador de respuesta genera solamente los datos de respuesta, después de que el módulo de determinación ha determinado la existencia de una instrucción de petición.

Las formas de realización del procedimiento según la invención, que se han descrito, pueden estar constituidas también como producto de programa de ordenador, de manera que se implementará un ordenador o un aparato programable para la realización del procedimiento, según la invención, que se ha descrito y cuyo código de programa será realizado mediante un procesador cuando el código de programa es cargado en el ordenador o en el aparato programable.

Una solución alternativa al objetivo, prevé un medio de almacenamiento, que está determinado para el almacenamiento del procedimiento que se ha descrito, implementable por ordenador, y que puede ser leído por un ordenador o por un aparato programable por ordenador, en especial un lector de tarjetas o un soporte de datos móvil.

Otras formas de realización ventajosas resultan de las reivindicaciones dependientes.

En la descripción de figuras detallada siguiente, se explicarán de manera no limitativa ejemplos de realización que presentan las características y otras ventajas, según los dibujos que muestran:

- La figura 1a una representación esquemática de unidades de comunicación, que serán transferidas entre una tarjeta de chip y un lector de tarjetas;
- La figura 1b muestra una representación esquemática de unidades de comunicación, que se transfieren entre una tarjeta de chip y un lector de tarjetas, en caso de que no se pidan datos de respuesta desde el lado del lector de tarjetas y
- La figura 2 muestra una representación esquemática de unidades de comunicación transferidas entre la tarjeta de chip y un lector de tarjetas con módulos correspondientes.

Tal como muestra en la parte superior de la figura 1a, la solución según la invención se refiere a la preparación de instrucciones sobre una tarjeta de chip -C-, de manera que una instrucción -B- es enviada desde un lector de tarjetas o bien de un terminal -T- a la tarjeta de chip -C-. En este caso, se utilizará un protocolo normalizado, en especial, según la norma ISO7816. Básicamente, la instrucción -B- será enviada siempre del terminal -T- a la tarjeta de chip y, opcionalmente se procesará en la tarjeta de chip -C-. La tarjeta de chip -C- trabaja, por lo tanto, en la modalidad llamada esclavo, mientras que el terminal -T- funciona como maestro e inicia la correspondiente comunicación.

En la parte inferior de la figura 1a se ha mostrado el desarrollo temporal de un procedimiento, según la invención para el proceso de la instrucción -B-.

La instrucción -B-, en esta ocasión se trata de una instrucción "SELECT", será transferida del terminal -T- a la tarjeta de chip -C-. De acuerdo con la invención tiene lugar adicionalmente para la selección propiamente dicha del archivo, la generación y envío (lo cual está designado con las referencias -1-) de una respuesta -A-, es decir, una palabra de estado sin datos de respuesta al terminal -T-.

En una forma de realización preferente, en esta etapa solamente se determina la longitud de los datos de respuesta (XX). De manera ventajosa, no obstante, no se prepararán en este momento de tiempo, datos de respuesta -AD-. Se enviará por lo tanto solamente una respuesta -A- de la tarjeta de chip -C- al terminal -T- que determina que se disponga de los datos de respuesta -AD-. Esto tiene lugar preferentemente por el envío de las siguientes palabras de estado: "SW1 SW2 = 9FXX".

El desarrollo adicional del procedimiento según la invención depende ahora de eventos generados del lado del terminal -T-, o bien de otras instrucciones enviadas del terminal -T- a la tarjeta de chip -C-. En la figura 1a se ha mostrado el caso en el que el terminal -T- pide también datos de respuesta -AD- sobre la instrucción -B-. En la figura 1b, se ha mostrado por el contrario el caso en el que el terminal -T- después del envío de la instrucción -B- no

5 dispone ninguna otra instrucción de petición adicional -AB- y por lo tanto no necesita datos de respuesta -AD-. Tal como es visible en la figura 1b, se termina por lo tanto en este punto de tiempo el proceso de la invención sin que se hayan generado de manera explícita datos de respuesta -AD- del lado de la tarjeta de chip -C-. Tal como se ha mostrado en la figura 1b, se ha generado solamente una respuesta -A- en la etapa -1- y se ha enviado en retorno al terminal -T-.

10 De otro modo, en caso de que el terminal -T- solicite también los datos de respuesta -AD- se prevé que el terminal -T- envíe una instrucción de petición -AB- a la tarjeta de chip -C-. De manera habitual se trata en esta instrucción de petición de la orden "GET RESPONSE". De manera alternativa, son también posibles en este caso, otras ordenes de petición. Solamente después de este evento, es decir, después de que el terminal -T- ha enviado la instrucción de petición "GET RESPONSE" -AB- a la tarjeta de chip -C-, se enviarán en retorno los datos de contestación -AD- generados en la etapa -2- al terminal -T-.

15 A diferencia de ello, no tiene lugar la generación de los datos de respuesta -AD- en el caso de que el terminal -T- no pida dichos datos de respuesta -AD-. Este caso se ha mostrado, tal como ya se ha explicado, en la figura 1b. En este caso se apreciará que el tiempo de preparación se reduce sustancialmente en la tarjeta de chip -C-.

20 La zona de utilización principal de la solución facilitada por la presente invención se encuentra en la zona de los teléfonos móviles, de manera que el terminal -T- es un aparato de usuario (por ejemplo un teléfono móvil, designado a continuación un "móvil") que comunica con una tarjeta SIM -C- en especial en el funcionamiento del aparato de usuario, envía una instrucción -B- (XX XX FID) "SELECT" a la tarjeta SIM -C-, por ejemplo en forma:

Móvil → A0 A4 00 00 02 XX XX → Tarjeta

25 El archivo correspondiente se seleccionará en base a la instrucción -B-. Los datos de respuesta -AD- para la instrucción B-SELECT no se calcularán en este momento de tiempo. Se evaluará solamente la longitud de los datos de respuesta existentes -AD- y se enviarán en retorno como palabra de estado (longitud YY de los datos de respuesta disponibles):

30 Móvil ← 9F YY ← Tarjeta

Tal como se ha explicado anteriormente, se diferencia el procedimiento siguiente con dependencia de otra instrucción de petición adicional -AB- del lado del móvil. En el caso de que la siguiente orden sea una instrucción de petición "GET RESPONSE" los datos de respuesta -AD- serán calculados y enviados en retorno.

35 Móvil → A0 C0 00 00 YY → Tarjeta
Móvil ← [YY Bytes] 90 00 ← Tarjeta

40 Cuando la orden que sigue a la instrucción SELECT no es una instrucción -AB- de petición GET RESPONSE se desestimarà la posibilidad de pedir datos de respuesta.

Este desarrollo está de acuerdo, por lo tanto, con el desarrollo básico del estado de la técnica; se diferencia solamente en el momento de la autorización de los datos de respuesta. Hasta ahora estos datos de respuesta eran ya autorizados siempre a la recepción de una instrucción -B- (por ejemplo SELECT). En caso de que a continuación

no se envíe instrucción GET RESPONSE, esta autorización pasa a ser sobrante. De acuerdo con la invención, este tiempo de autorización innecesario se puede ahorrar de manera completa.

5 Para diferenciar si a partir de una instrucción de petición -AB- se pueden enviar datos de respuesta de la tarjeta, se almacenará, de acuerdo con la invención, un estado interno en la tarjeta que muestra que los datos de respuesta -AD- pueden ser solicitados o recuperados (datos de respuesta XX-Byte recuperables).

10 Este estado muestra que los datos de respuesta -AD- son recuperables. En otras palabras, no es necesario que una instrucción de petición -AB- sea facilitada directamente después del envío de una instrucción -B-. Es también posible que la instrucción de petición -AB- se envíe solamente en un punto de tiempo posterior después de otras instrucciones -B-. El estado "datos de respuesta recuperables" subsiste mientras se relaciona con una instrucción específica -B-. Cuando el terminal -T- en el desarrollo posterior pide los datos de respuesta -AD- mediante la instrucción de petición GET RESPONSE, estos -siempre que se encuentren en la tarjeta -C- en el estado específico correspondiente serán preparados "Just in Time" y serán enviados al terminal -T-. Por lo tanto, desaparece la
15 preparación innecesaria de datos de respuesta -AD-.

Si la solución técnica según la presente invención, se utiliza concretamente en la fase activa o de funcionamiento de la tarjeta SIM en la conexión del teléfono móvil, normalmente el teléfono móvil no tiene interés alguno en los datos FCI (File-Control-Information-Datos) preparados por la tarjeta SIM -C- de acuerdo con el estado de la técnica. De
20 acuerdo con la invención no se enviará por lo tanto en este caso ninguna instrucción de petición subsiguiente GET RESPONSE. Por lo tanto se puede ahorrar el tiempo para la preparación de los datos FCI. Estos ascienden de manera típica a 10-80 ms por archivo.

La forma especial de realización corresponde a la instrucción SELECT. La instrucción SELECT es una orden case-4
25 y comprende, además de datos de entrada, también datos de salida. Otras utilizaciones de la solución de acuerdo con la invención pueden referirse también a otras ordenes "case-4".

Otra solución adicional al objetivo consiste en un sistema para procesar la instrucción -B- en base al procedimiento que se describe. El sistema comprende el lector de tarjetas -T-, una interfaz para comunicación entre una tarjeta de
30 chip -C- y el lector de tarjetas -T- y un módulo de captación -10-, un generador de respuesta -12-, un módulo de determinación -14- y un generador de respuesta -16-, de manera que todos los módulos y generadores están incorporados dentro de la tarjeta de chip -C-. El sistema con el intercambio de datos de acuerdo con la invención se ha mostrado en la figura 2.

35 Otra solución del objetivo de acuerdo con la invención es un producto de programa de ordenador que está definido para la realización del procedimiento según la invención que se ha descrito anteriormente. En este caso, pueden ser incorporados de manera integrada módulos de software y/o módulos de hardware del producto como módulos separados y/o en el sistema operativo.

40 Finalmente se deberá tener en cuenta que la descripción de la invención y los ejemplos de realización no son básicamente limitativos con respecto a una realización física práctica de la invención. Para un técnico habitual es en especial evidente que la invención puede ser realizada de manera parcial o completa en software y/o hardware y/o a base de varios productos físicos en especial también como producto de programa de ordenador.

REIVINDICACIONES

1. Procedimiento para el proceso de una instrucción (B) para un soporte de datos móvil (C), siendo transferida la instrucción desde un lector de tarjetas (T) al soporte de datos móvil (C) a través de un protocolo normalizado y proporcionando la generación de datos de respuesta (AD) por parte del soporte de datos móvil (C), siendo solicitados los datos de respuesta (AD) por el lector de tarjetas (T) a través de una instrucción de petición separada (AB), presentando el procedimiento las siguientes etapas:
- captar la instrucción por parte del soporte de datos móvil (C);
 - generar y enviar una respuesta (A) al lector de tarjetas (T), comprendiendo la respuesta (A) un código de confirmación que indica que los datos de respuesta (AD) pueden ser recuperados en el soporte de datos móvil (C);
 - determinar si el lector de tarjetas (T) pide los datos de respuesta recuperables (AD) con una instrucción de petición (AB), y en caso afirmativo:
- caracterizado por**
- generar los datos de respuesta (AD) para la instrucción captada (B) en el soporte de datos móvil (C) y enviar los datos de respuesta (AD) al lector de tarjetas, siendo realizada la generación de los datos de respuesta (AD) solamente después de recibir la instrucción de petición (AB) por parte del soporte de datos móvil.
2. Procedimiento, según la reivindicación 1, **caracterizado porque** la respuesta (A) no contiene datos de respuesta (AD).
3. Procedimiento, según la reivindicación 1 ó 2, **caracterizado porque** la instrucción (B) requiere una instrucción separada, subsiguiente de petición (AB) y está acoplada a la misma en este respecto para pedir los datos de respuesta (AD) para la instrucción del soporte de datos móvil (C).
4. Procedimiento, según como mínimo una de las reivindicaciones anteriores, **caracterizado porque** la instrucción (B) es una instrucción de selección de archivos, en particular una instrucción SELECT, una instrucción de búsqueda o una instrucción de lectura.
5. Procedimiento, según como mínimo una de las reivindicaciones anteriores, **caracterizado porque** el soporte de datos móvil (C) genera los datos de respuesta (AD) solamente en el momento en el que el lector de tarjetas (T) ha emitido la instrucción de petición (AB) o después de que el soporte de datos móvil (C) ha detectado la instrucción de petición (AB) del lector de tarjetas (T).
6. Procedimiento, según como mínimo una de las reivindicaciones anteriores, **caracterizado porque** la instrucción (B), la instrucción de petición (AB), la respuesta (A) y/o los datos de respuesta (AD) son transferidos entre el lector de tarjetas (T) y el soporte de datos móvil (C) mediante una unidad de comunicación encapsulada.
7. Procedimiento, según como mínimo una de las reivindicaciones anteriores, **caracterizado porque** el protocolo es un protocolo T=0.
8. Procedimiento, según como mínimo una de las reivindicaciones anteriores, **caracterizado porque** el código de

confirmación comprende un código de retorno que indica la longitud de los datos de respuesta esperados (AD).

5 9. Procedimiento, según como mínimo una de las reivindicaciones anteriores, **caracterizado porque** la respuesta (A) comprende un código de error si los datos de respuesta (AD) no son recuperables o si la instrucción (B) no puede ser ejecutada.

10 10. Procedimiento, según como mínimo una de las reivindicaciones anteriores, **caracterizado porque** se detecta un estado de recuperación que indica que datos de respuesta (AD) para una instrucción (B) pueden ser recuperados en el soporte móvil de datos (C) y en el que el soporte de datos móvil (C) está situado después del envío de la instrucción (B) hasta que los datos de respuesta (AD) han sido enviados al lector de tarjetas (T) o hasta que se envía otra instrucción (B) al soporte móvil de datos (C).

15 11. Soporte móvil de datos (C), que tiene una unidad de proceso y una memoria para almacenar un código de programa, **caracterizado porque** el soporte de datos móvil (C) está configurado para llevar a cabo un procedimiento, de acuerdo como mínimo una de las reivindicaciones 1 a 10, entre el soporte de datos móvil (C) y un lector de tarjetas (T).

12. Sistema para el proceso de una instrucción, que presenta:

- 20 - como mínimo un soporte de datos móvil (C),
- como mínimo un lector de tarjetas (T) que envía una instrucción al soporte de datos móvil (C), siendo transferida la instrucción mediante un protocolo normalizado y proporcionando la generación de datos de respuesta (AD) por parte del soporte móvil de datos (C), siendo pedidos los datos de respuesta (AD) por el lector de tarjetas (T) a través de una instrucción de petición separada (AB);
- 25 - como mínimo una interfaz para comunicación entre el soporte móvil de datos (C) y el lector de tarjetas (T) que está diseñada para enviar una instrucción (B) y, en caso que sea aplicable, una instrucción de respuesta separada (AB) desde el lector de tarjetas (T) al soporte de datos móvil (C), y que está diseñada para enviar una respuesta (A) y, en caso que de sea aplicable, datos de respuesta (AD) del soporte de datos móvil (C) al lector de tarjetas (T), comprendiendo el soporte de datos móvil (C) los elementos siguientes:
- 30 - como mínimo un módulo detector (10) que está destinado para detectar la instrucción del soporte de datos móvil (C);
- como mínimo un generador de respuesta (12) destinado a generar y enviar una respuesta (A) al lector de tarjetas (T), comprendiendo la respuesta (A) un código de confirmación que indica que los datos de respuesta (AD) son recuperables en el soporte de datos móvil;
- 35 - como mínimo un módulo de determinación (14) que está diseñado para determinar si el lector de tarjetas (T) pide los datos de respuesta recuperables (AD) con una instrucción de petición subsiguiente (AB);

caracterizado por

- 40 - como mínimo un generador de datos de respuesta (16) que está destinado a generar datos de respuesta (AD) para la instrucción en el soporte de datos móvil (C) y para enviar los datos de respuesta (AD) al lector de tarjetas (T), generando el generador de datos de respuesta (16) los datos de respuesta (AD) solamente después de que el módulo de determinación (14) ha determinado la existencia de una instrucción de petición (AB).

13. Producto de programa de ordenador que puede ser cargado en una memoria de un dispositivo programable (T, C) y que comprende partes de código de programa de ordenador, **caracterizado porque** las partes de código de programa de ordenador están destinadas a la realización de las etapas de un procedimiento de acuerdo como mínimo con una de las reivindicaciones 1 a 10 cuando el producto de programa de ordenador es cargado en el dispositivo programable (T, C).
- 5

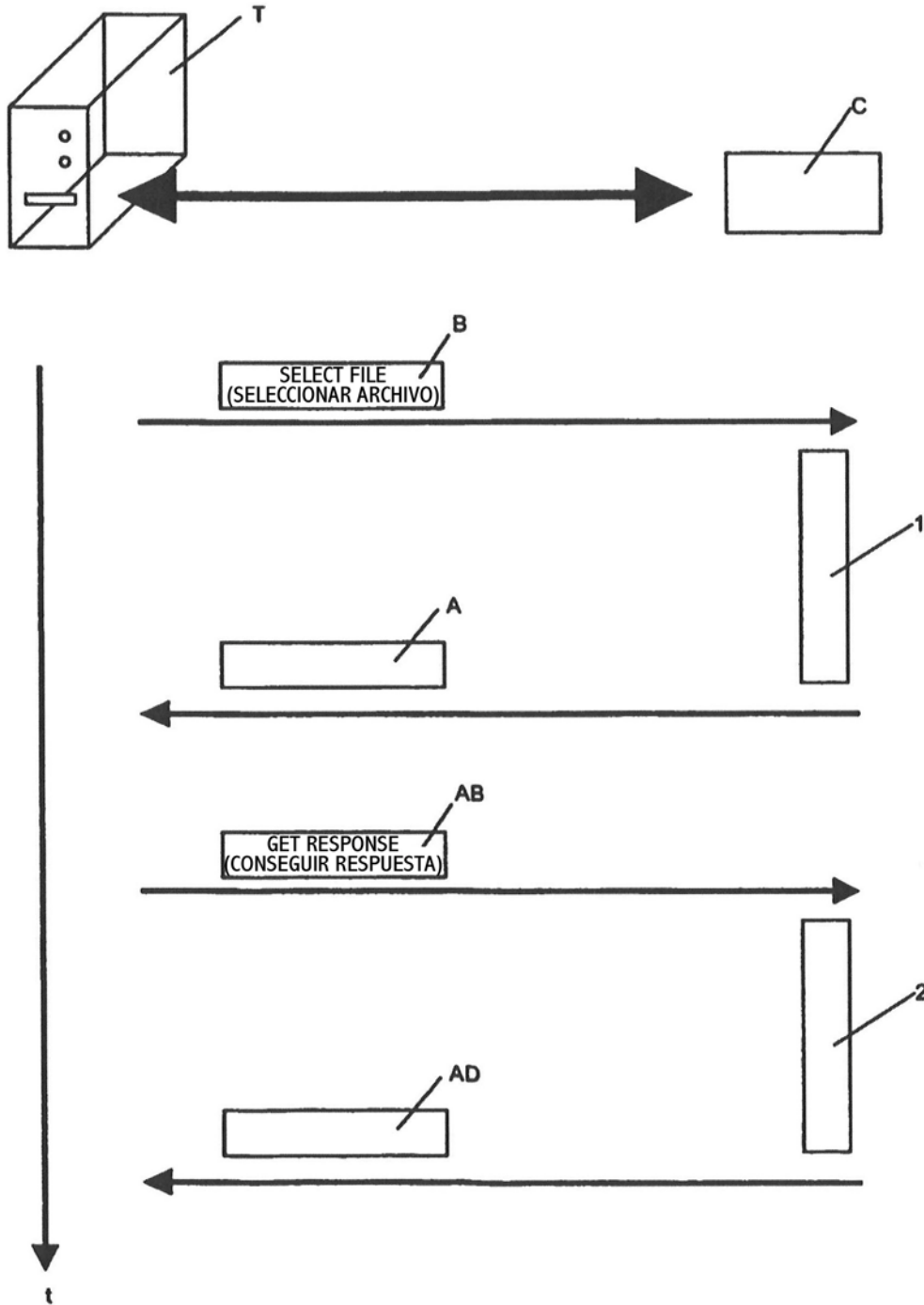


Fig. 1a

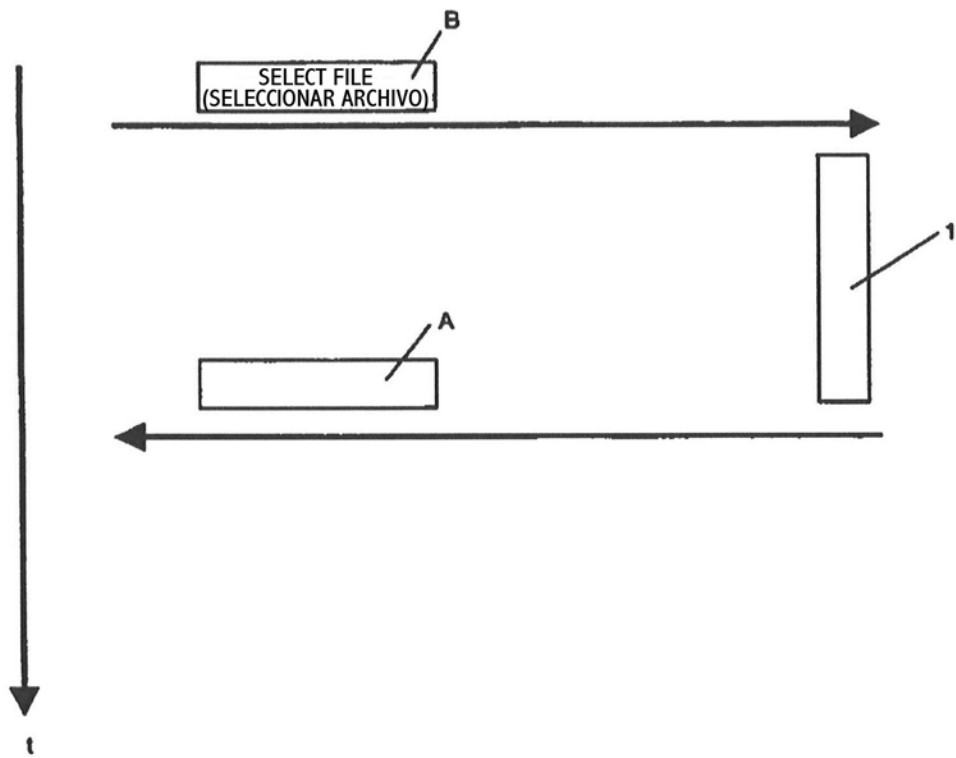


Fig. 1b

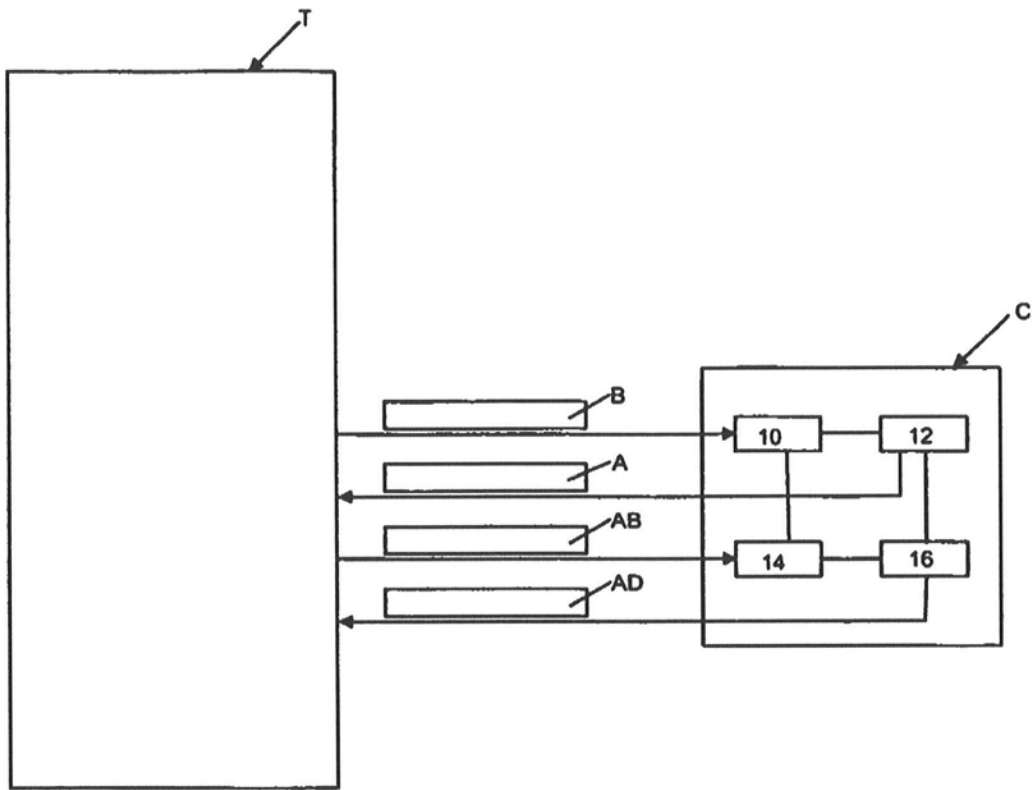


Fig. 2