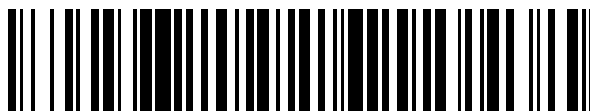


19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 626 296**

51 Int. Cl.:

G06Q 20/38 (2012.01)

G06Q 20/40 (2012.01)

H04L 12/24 (2006.01)

H04L 29/08 (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

86 Fecha de presentación y número de la solicitud internacional: **05.04.2012 PCT/EP2012/056317**

87 Fecha y número de publicación internacional: **18.10.2012 WO12139976**

96 Fecha de presentación y número de la solicitud europea: **05.04.2012 E 12713965 (7)**

97 Fecha y número de publicación de la concesión europea: **08.03.2017 EP 2697952**

54 Título: **Procedimiento de multiplexación de mensajes, dispositivo y programa correspondiente**

30 Prioridad:

13.04.2011 FR 1101142

45 Fecha de publicación y mención en BOPI de la traducción de la patente:
24.07.2017

73 Titular/es:

**INGENICO GROUP (100.0%)
28-32 Boulevard de Grenelle
75015 Paris, FR**

72 Inventor/es:

**POLIGNY, JEAN-ROCH;
GOMES, VINCENT;
JAMES, SÉBASTIEN;
ROYER, JESSICA;
POMMARET, JEAN-CHRISTOPHE y
GRANDEMENGÉ, JÉRÔME**

74 Agente/Representante:

CARPINTERO LÓPEZ, Mario

ES 2 626 296 T3

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

DESCRIPCIÓN

Procedimiento de multiplexación de mensajes, dispositivo y programa correspondiente

Campo de la invención

- 5 La presente invención se refiere al campo de los dispositivos de pago electrónicos. Más particularmente, la presente invención se refiere a un nuevo tipo de dispositivo de pago electrónico que puede emparejarse. La invención se refiere aún más particularmente a la transmisión de datos entre dos terminales que componen el dispositivo de pago electrónico.

Soluciones del estado de la técnica

- 10 En la actualidad, los terminales de pago se utilizan principalmente para permitir el ajuste de las compras de bienes y de servicios en el seno de los puntos de venta. Estos terminales comprenden generalmente un lector de tarjeta inteligente y un lector de tarjeta magnética. Comprenden igualmente una pantalla, que permite en particular visualizar informaciones, tales como las sumas de las transacciones, y un teclado de introducción de estos mismos importes, así como de códigos confidenciales introducidos por los clientes, o bien una pantalla táctil.

- 15 Los terminales más recientes se conectan a cajas registradoras y/o a ordenadores por medio de una red de comunicación. Tales conexiones pueden por cable, por ejemplo, de tipo Ethernet, o inalámbricas. Estas conexiones permiten, por ejemplo, conectarse a un servidor de autenticación o a un servidor bancario en vistas de la obtención de una autorización del débito.

- 20 Para poder comunicarse con el exterior, y en particular, con servidores bancarios, el terminal de pago utiliza uno o varios medios de conexión. Uno de estos medios consiste en utilizar una red de comunicación inalámbrica, por ejemplo, GPRS (del inglés "General Pocket Radio Service"). En este caso, el terminal de pago actúa de manera autónoma. El terminal de pago se provee entonces de una tarjeta SIM (del inglés "Subscriber Identity Dispositivo de multiplexación"). Se trata de un chip que contiene un microcontrolador y memoria. Esta tarjeta SIM se asocia generalmente a una suscripción telefónica (de tipo transmisión de datos) que debe suscribirse por el vendedor.
- 25 Además del hecho de que este tipo de suscripción es relativamente cara, la implementación de las funcionalidades de comunicación se atribuye al terminal. De este modo, además de las funciones de pago, el terminal manejar las funciones de comunicación, que no son naturalmente las funciones que esperamos de un terminal de pago.

- 30 Para superar el problema de coste de la suscripción asociada a la comunicación GPRS en particular, los nuevos tipos de terminales se comunican mediante una red de tipo "WiFi" (del inglés para "Wireless Fidelity"), por ejemplo. El vendedor ya no está obligado a una suscribir una suscripción particular. El terminal de pago puede conectarse a la red WiFi del vendedor y acceder, como en una conexión con cable, a servicios bancarios. Sin embargo, el uso del terminal se limita entonces a la zona de cobertura de la red WiFi, lo que no conviene a una utilización nómada (por ejemplo, para un médico de visita en casa de sus pacientes o para un chófer de taxi).

El estado de la técnica anterior se conoce a partir de los documentos US2004/0042450 A1 y US2008/0114699 A1.

- 35 Se presenta, en relación con la figura 1, la arquitectura de hardware general en la que el terminal de pago interviene para poder realizar una transacción bancaria, cuando este terminal no es autónomo (CAS 1) y cuando es autónomo (CAS 2).

- 40 De este modo, existe una necesidad para proponer un terminal de pago que pueda utilizarse para aplicaciones nómadas, por lo tanto, utilizando una red de comunicación inalámbrica, minimizando los costes de implementación de un tal terminal de pago. Para ello, se propone, de esta manera, emparejar el terminal de pago con un terminal de comunicación existente (por ejemplo, un iPhone™ o un iPod™). El terminal emparejado naturalmente incluye numerosas funcionalidades que están ausentes del terminal de pago cuando no se empareja.

El problema es que cualquier terminal de pago nuevo debe sufrir una serie de pruebas de certificación. Estas pruebas de certificación se llaman pruebas "PCI/PED". Son extremadamente caros. De este modo, los constructores de los terminales de pago cuidan de efectuar estas pruebas con criterio.

- 45 De este modo, existe pues una necesidad de proponer un terminal de pago que sea a la vez emparejable con un terminal de comunicación para formar un terminal emparejado, sin que sea necesario implementar nuevas pruebas de certificación cada vez que se desee emparejar una nueva versión o un nuevo tipo de terminal de comunicación (por ejemplo, un nuevo iPhone™ o un nuevo iPod™).

Resumen de la invención

- 50 La invención no presenta estos inconvenientes del estado de la técnica.

La invención se define en las reivindicaciones independientes 1, 6, y 7.

La invención se refiere más particularmente a un procedimiento de multiplexación de mensajes intercambiados entre

un terminal de pago y un terminal de comunicación por medio de una conexión entre dicho terminal de pago y dicho terminal de comunicación, utilizando el protocolo *iAP*. Según la invención, un tal procedimiento comprende:

- una etapa de inicialización de una interfaz de comunicación externa con dicho terminal de comunicación;
- una primera etapa de transmisión, por dicho terminal de pago, a dicho terminal de comunicación, de una solicitud de creación de canales virtuales distantes, por medio de dicha interfaz de comunicación externa;
- una etapa de creación, en el seno de dicho terminal de pago, de canales virtuales locales correspondientes a dichos canales virtuales distantes;
- una segunda etapa de transmisión de tramas de datos asociados a dichos canales virtuales locales por medio de dicha interfaz de comunicación externa.

De este modo, la invención permite realizar una transmisión de datos por medio de canales múltiples utilizando una interfaz de comunicación en serie.

Según una característica particular de dicha interfaz de comunicación externa es una interfaz RS232.

Según un modo de realización particular, dicho procedimiento comprende, además, antes de dicha etapa de inicialización de interfaz de comunicación comprende una etapa de autenticación de dicho terminal de pago con respecto a dicho terminal de comunicación que comprende:

- una etapa de obtención de un certificado de autenticación; y
- una etapa de verificación, de la autorización del terminal de pago que se emparejará con dicho terminal de comunicación con ayuda de dicho certificado de autenticación.

Según un modo de realización particular, dicha segunda etapa de transmisión de tramas de datos asociados a dichos canales virtuales locales comprende:

- una etapa de verificación, en el seno de dichos canales virtuales, de una presencia de una trama TLV destinada al terminal de comunicación;

y cuando uno de los canales comprende una tal trama:

- una etapa de encapsulación de esta trama TLV en un mensaje *iAP*.

Según una característica particular, dichos canales virtuales pertenecen al grupo que comprende:

- un canal virtual "transaction" de intercambio de datos relativos a las transacciones bancarias;
- un canal virtual "configuration" de intercambio de información de servicio;
- un canal virtual "SSL", de cifrado de transmisión de datos entre dicho terminal de pago y dicho terminal de comunicación;
- un canal virtual "Printer" de transmisión de datos de impresión;
- un canal virtual "Barcode" de gestión de la lectura de códigos de barras.

Según una característica particular, que un canal virtual se cree bajo la forma de una cola, configurándose dicha cola para permitir la recepción, el registro y la eliminación de tramas TLV destinadas a dicho canal virtual.

Según otro aspecto, la invención se refiere igualmente a un dispositivo de multiplexación de mensajes intercambiados entre un terminal de pago y un terminal de comunicación por medio de una conexión entre dicho terminal de pago y dicho terminal de comunicación utilizando el protocolo *iAP*.

Según la invención, un tal dispositivo comprende:

- medios de inicialización de una interfaz de comunicación externa con dicho terminal de comunicación;
- medios de transmisión, por dicho terminal de pago, a dicho terminal de comunicación, de una solicitud de creación de canales virtuales distantes, por medio de dicha interfaz de comunicación externa;
- medios de creación, en el seno de dicho terminal de pago, de canales virtuales locales correspondientes a dichos canales virtuales distantes;
- medios de transmisión de tramas de datos asociados a dichos canales virtuales locales por medio de dicha interfaz de comunicación externa.

Según una implementación preferente, las diferentes etapas del procedimiento según la invención se implementan por un software o programa informático, comprendiendo este software instrucciones de software que se ejecutarán por un procesador de datos de un terminal de pago según la invención y concibiéndose para controlar la ejecución de las diferentes etapas de este procedimiento.

En consecuencia, la invención apunta también a un programa, susceptible de ejecutarse por un ordenador o por un procesador de datos, constando este programa de instrucciones para controlar la ejecución de las etapas de un procedimiento tal como se mencionó anteriormente.

Este programa puede utilizar cualquier lenguaje de programación, y ser bajo la forma de código fuente, código objeto, o de código intermediario entre código fuente y código objeto, tal como en una forma parcialmente compilada, o en cualquier otra forma deseada.

5 La invención apunta también a un soporte de informaciones legibles por un procesador de datos, y consta también de las instrucciones de un programa tal como se mencionó anteriormente.

El soporte de informaciones puede ser cualquier entidad o dispositivo capaz de almacenar el programa. Por ejemplo, el soporte puede constar de un medio de almacenamiento, tal como una ROM, por ejemplo, un CD-ROM o una ROM de circuito microelectrónico, o aún un medio de registro magnético, por ejemplo, un disquete (floppy disc) o un disco duro.

10 Por otra parte, el soporte de informaciones puede ser un soporte transmisible tal como una señal eléctrica u óptica, que puede distribuirse a través de un cable eléctrico u óptico, por radio o por otros medios. El programa según la invención puede descargarse en particular sobre una red de tipo Internet.

Alternativamente, el soporte de informaciones puede ser un circuito integrado en el que el programa se incorpora, adaptándose el circuito para ejecutar o para utilizarse en la ejecución del procedimiento en cuestión.

15 Según un modo de realización, la invención se implementa a través de componentes de software y/o de hardware. En esta óptica, el término "módulo" puede corresponder en este documento tanto a un componente de software, como a un componente de hardware o a un conjunto de componentes de hardware y de software.

20 Un componente de software corresponde a uno o varios programas de ordenador, uno o varios subprogramas de un programa, o de manera más general, a cualquier elemento de un programa o de un software apto para implementar una función o un conjunto de funciones, según lo que se describe a continuación. Un tal componente de software se ejecuta por un procesador de datos de una entidad física (terminal de pago) y es susceptible de acceder a los recursos de hardware de esta entidad física (memorias, soportes de registro, bus de comunicación, tarjetas electrónicas de entradas/salidas, interfaces de usuario, etc.).

25 De la misma manera, un componente de hardware corresponde a cualquier elemento de un conjunto de hardware apto para implementar una función o un conjunto de funciones, según lo que se describe a continuación para el módulo relacionado. Puede tratarse de un componente de hardware programable o con un procesador integrado para la ejecución del software, por ejemplo, un circuito integrado, una tarjeta inteligente, una tarjeta de memoria, una tarjeta electrónica para la ejecución de un microsoftware (firmware), etc.

Lista de las figuras

30 Otras características y ventajas de la invención se aparecerán más claramente tras la lectura de la descripción siguiente de un modo de realización preferente, dado a título de simple ejemplo ilustrativo y no limitante, y de los dibujos adjuntos, entre los cuales:

- la figura 1, ya presentada, ilustra la arquitectura de hardware de un sistema de pago en el que un terminal de pago interviene;
- 35 - la figura 2 es un diagrama de bloques que describe las capas de software implementadas en el seno de un terminal de pago;
- la figura 3 describe el procedimiento de multiplexación según un modo de realización;
- la figura 4 describe el formato de un mensaje iAP;
- la figura 5 presenta colas que corresponden a los canales virtuales creados en el momento de la implementación
- 40 - la figura 6 describe resumidamente la arquitectura de hardware del dispositivo de multiplexación.

Descripción detallada de la invención

1.1 Recordatorio del principio de la invención

45 La invención tiene como objetivo reutilizar un terminal de pago existente para emparejarse con un terminal de comunicación (por ejemplo, un iPod™ o un iPhone™), sin que sea necesario certificar (en el seno de las certificaciones PCI/PED) el conjunto constituido del terminal de comunicación y del terminal de pago.

Para ello, la invención propone implementar un dispositivo de multiplexación que realice una multiplexación bidireccional de mensajes intercambiados entre el terminal de pago y el terminal de comunicación. La arquitectura de software propuesta permite reutilizar las aplicaciones existentes, ya aprobadas para soluciones que funcionan

50 cuando el terminal de comunicación y el terminal de pago se intercambian datos en IO (igualmente llamado "stack IP"), con productos móviles que no soportan la utilización de "stack ip" en vivo (tipo iPhone™).

Más particularmente, la multiplexación implementada por medio del protocolo iAP, el cuál es el origen del problema al que la invención permite aportar una solución (cuello de botella formado por el iAP). De este modo, el terminal de pago se ve como un accesorio del terminal de comunicación. De hecho, el terminal de comunicación, que

comprende numerosas funcionalidades que no se pueden presentar en el terminal de pago puede ventajosamente completar el funcionamiento de este último.

El dispositivo de multiplexación implementa una secuencia de etapas que conducen a la transmisión y/o a la recepción, por el terminal de pago, de datos para y provenientes del terminal de comunicación. Según un modo de realización particular, el procedimiento de multiplexación de mensaje por medio de una conexión que utiliza el protocolo *iAP* comprende: El "iPod Accessory Protocol/iAP" (igualmente conocido bajo el nombre de Apple Accessory Protocol/AAP) se utiliza para la comunicación entre iPod™/iPhone™ y accesorios tales como estaciones de acoplamiento y adaptadores para coches. El *iAP* se utiliza principalmente para controlar la lectura del iPod/iPhone y para transferir datos tales como los metadatos sobre la pista en curso de lectura y la carátula del álbum. Con las versiones recientes del *iAP*, es igualmente posible que los accesorios se comuniquen con las aplicaciones que funcionan en iPhone OS.

Sin embargo, el *iAP* y su implementación en los terminales de Apple sufren un problema grave: el débito. En efecto, el *iAP* tiene un débito reducido que va aproximadamente desde los 19.200 hasta los 57.600 baudios, en función de las versiones utilizadas en los datos que se transmitirán. De hecho, la comunicación entre los terminales y los accesorios se efectúa con ayuda de una interfaz RS232 (una interfaz en serie) que utiliza el *iAP*.

Ahora bien, esta interfaz no se adapta a la transmisión de datos entre un terminal de pago y un terminal de comunicación. Esta transmisión de datos tiene más bien que realizarse por medio de una interfaz USB. Esta interfaz USB permite transmitir, a gran velocidad, grandes cantidades de datos. Más particularmente, el terminal de comunicación y el terminal de pago se conectan entre sí por medio de una interfaz USB y la transmisión de datos se efectúa realizando una emulación de un enlace en serie implementando el protocolo PPP ("Point-to-Point Protocol"), implementando él mismo el protocolo IP ("Internet Protocol") que permite al terminal de pago y al terminal de comunicación disponer cada uno de una dirección IP. Los datos de longitud variable so en cuanto a ellos, transmitidos según la técnica llamada de "TLV" ("Type-length-value").

En otras palabras, el enlace USB entre los dos terminales y es sin duda más rápido, pero se realizan muchas encapsulaciones de datos. Ello da como resultado una pérdida de eficacia del enlace USB bastante considerable: las múltiples encapsulaciones (IP, PPP, USB) sin permitir utilizar las mismas técnicas para una transmisión por medio de una interfaz RS232.

Además, para poder comunicar con los terminales de Apple es necesario implementar "lingos". El protocolo *iAP* define cuatro "lingos" (que son canales de intercambio de datos entre el terminal de comunicación de Apple™ (iPhone™, iPod™, etc.) y el accesorio (estación de acoplamiento, auriculares, etc.) conectado al terminal de comunicación. Los cuatro "lingos" son los siguientes: General Lingo (genérico), Display Remote Lingo (transferencia de visualización), Extended Interface Lingo (interfaz extendida), Digital Audio Lingo (transmisión de datos de audio). No es posible utilizar otros medios de comunicación con el terminal de comunicación. Los inventores han tenido pues que implementar una técnica para permitir una transmisión de datos adaptada al terminal de pago. De hecho, los medios de transmisión ("lingos") ofrecidos por el terminal de comunicación que utilizan el protocolo *iAP* no se manifiestan adaptados a una implementación de aplicaciones de pago.

De este modo, la invención propone la implementación de una capa de enlace que permite soportar la transmisión de datos entre el terminal de pago y el terminal de comunicación. Esta capa de enlace permite administrar el flujo de datos (bajo la forma de tramas TLV) que se transmite entre los terminales.

Se presenta, en relación con la figura 2, un diagrama de bloques que describe las capas de software implementadas en el seno del terminal de pago según un modo de realización.

Las capas de software comprenden una capa llamada "nivel bajo" que comprende los módulos de software que interactúan directamente con los componentes de hardware del terminal. Esta capa "nivel bajo" permite pilotar los dispositivos de hardware del terminal de pago y comprende pilotos ("drivers", en inglés). Esta capa de software nivel bajo se utiliza por medio de un sistema operativo ("OS, Operating System" en inglés). El sistema operativo comprende en particular bibliotecas ("libraries" en inglés). El propio sistema operativo se utiliza por un gestor de aplicación ("Manager") que controla las diferentes aplicaciones del terminal de pago. Entre las aplicaciones posibles, se pueden citar las aplicaciones de pago (simple, diferido, en varios plazos), la gestión de tarjetas de fidelidad, el monedero electrónico, etc.

1.2 Descripción de un modo de realización

Para permitir la transmisión de datos por medio de un enlace de tipo "en serie", no adaptado para este uso en el ámbito de un enlace entre el terminal de pago y un terminal de comunicación de tipo iPod™ o iPhone™, la invención propone, en este modo de realización, implementar una multiplexación de los mensajes.

Más particularmente, en la medida en la que el objetivo es poder reutilizar un terminal de pago existente para emparejarse con un terminal de comunicación (iPod™ o iPhone™), sin que sea necesario certificar (en el seno de los certificados PCI/PED) el conjunto constituido por el terminal de comunicación y el terminal de pago, los inventores aportan una solución simple, que se puede actualizar. Para esto, los inventores han implementado un

dispositivo de multiplexación que tiene la función de interfaz entre el terminal de pago y el iPhone™ o el iPod™.

Más particularmente, en un modo de realización, esta interfaz es un módulo de interfaz, de software o de hardware, que permite por una parte transmitir y recibir mensajes hacia el terminal móvil. Según un primer modo de realización particular, el dispositivo de multiplexación se implementa en el seno del terminal de pago. Debido a esto, tiene las medidas de seguridad implementadas en el seno del terminal de pago (medidas que se toman para permitir el certificado PCI-PCE). Según un segundo modo de realización particular, el dispositivo de multiplexación de una interfaz se implementa en el seno de una tarjeta electrónica de conexión entre el terminal de pago y el terminal móvil. En este segundo modo de realización, la tarjeta electrónica de conexión comprende un circuito impreso sobre el que se fija:

- un primer conector, que permite conectar la tarjeta al dispositivo de pago,
- un segundo conector, que permite conectar la tarjeta al terminal de comunicación, y
- un tercer conector, que permite conectar la tarjeta a un dispositivo externo (por ejemplo, un cargador).

Según la invención, el dispositivo de multiplexación de interfaz se configura para implementar un procedimiento de multiplexación de mensajes entre el terminal de pago y el terminal móvil. Este procedimiento de multiplexación, presentado en relación con la figura 3, comprende, desde el punto de vista del terminal de pago, las etapas siguientes:

- una etapa (311) de inicialización de una interfaz de comunicación externa con dicho terminal de comunicación;
- una primera etapa (312) de transmisión, a dicho terminal de comunicación, de una solicitud de creación de canales virtuales distantes, por medio de dicha interfaz de comunicación externa;
- una etapa (313) de creación, en el seno de dicho terminal de pago, de canales virtuales locales correspondientes a dichos canales virtuales distantes;
- una segunda etapa (32) de transmisión de tramas de datos asociados a dichos canales virtuales locales por medio de dicha interfaz de comunicación externa.

De este modo, el terminal de pago es capaz de transmitir datos al terminal de comunicación por medio de canales virtuales.

La lista de canales virtuales es la siguiente:

- un canal virtual "transaction" destinada a emitir y recibir los datos relativos a las transacciones bancarias;
- un canal virtual "configuration" destinado a permitir el intercambio de informaciones de servicio (sincronización, ajuste de la hora, etc.);
- un canal "SSL", por el nombre del protocolo homónimo, destinado a asegurar la transmisión de datos entre el terminal de pago y el terminal de comunicación;
- un canal "Printer" destinado a transmitir datos llamados de impresión, tal como datos que resultan de una transacción (comúnmente llamados "tarjeta de ticket");
- un canal virtual "Barcode" destinado a permitir la gestión de la lectura de códigos de barras cuando el terminal de pago dispone de un lector de código de barras.

Antes de la inicialización de la interfaz de comunicación externa con el terminal de comunicación, el método de la invención comprende además una primera etapa (30) de autenticación de dicho terminal de pago respecto a dicho terminal de comunicación. Esta etapa permite asegurar que el terminal de pago se autoriza a acoplarse con el terminal de comunicación.

Esta primera etapa (30) de autenticación comprende, desde el punto de vista del terminal de pago, una etapa (301) de obtención de un certificado (por ejemplo, de un procesador dedicado situado en el seno del terminal de pago) y una etapa (302) de verificación, de tipo "desafío/respuesta", en la que el terminal de comunicación verifica la autorización del terminal de pago que se emparejará. El procesador dedicado para ello que se instala en el seno del terminal de pago puede ser un procesador proporcionado por el fabricante del terminal de comunicación (por ejemplo, Apple™).

Esta primera etapa de autenticación puede seguirse ventajosamente en un modo de realización específico de la invención no representado, de una segunda etapa de autenticación en la que la carga se de la prueba no estará en el lado del terminal de pago sino en el lado del terminal de comunicación. Esta segunda etapa tendrá, de este modo, por objetivo asegurar que el terminal de comunicación tiene derecho a emparejarse con el terminal de pago al que se empareja. Esta etapa de autenticación puede ser igualmente del tipo "desafío/respuesta" o de cualquier otro tipo adecuado. Esta segunda etapa de autenticación puede utilizar ventajosamente hardware criptográfico que está comprendido en la tarjeta SIM del terminal de comunicación. De este modo, esta utilización, con el propósito de autenticación mutua, evita tener que colocar datos sensibles en el terminal de comunicación (que no está previsto para ello), y evita desarrollar una solución costosa para esto.

Según un modo de realización de la invención, después de la etapa (313) de creación, en el seno de dicho terminal de pago, de los canales virtuales correspondientes a dichos canales virtuales creados por el terminal de comunicación, el procedimiento de multiplexación comprende una etapa (321) de verificación, en el seno de dichos

canales virtuales, de una presencia de una trama TLV destinada al terminal de comunicación y cuando uno de los canales comprende una tal trama, una etapa (322) de encapsulación de esta trama TLV en un mensaje (3221) *iAP*.

Según un modo de realización particular de la invención, el formato del mensaje (3221) *iAP* transmitido, presentado en relación con la figura 4, es el siguiente:

- 5 - un identificador (401) de "lingo" de una longitud de 1 byte;
- un identificador (402) de trama de una longitud de 1 byte;
- un identificador (403) de transacción de una longitud de 2 bytes;
- un identificador de sesión (que corresponde al número de canal (404) virtual) de una longitud de 2 bytes;
- datos (405) de longitud variable TLV;
- 10 - un código (406) de control integrado CRC.

De este modo, se minimiza enormemente los datos de encapsulación y se transmiten pues datos útiles en un canal físico limitado.

15 Según un modo de realización de la invención, el procedimiento de multiplexación comprende igualmente, en el lado del terminal de comunicación, una etapa (323) de verificación, en el seno de canales virtuales del terminal de comunicación, de una presencia de una trama TL destinada al terminal de pago y cuando uno de los canales comprende una tal trama, una etapa (324) de encapsulación de esta trama en un mensaje *iAP*.

De este modo, se utiliza una interfaz de comunicación de manera bidireccional.

20 Más particularmente, los canales virtuales, en un modo de realización particular, se describen en relación con la figura 5, creados bajo la forma de una pluralidad de colas de tipo "FIFO" (F1 a F5 en el lado del terminal de pago y F'1 a F'5 en el lado del terminal de comunicación). El funcionamiento de estas colas es el siguiente.

25 Las colas son invisibles, desde el punto de vista de las aplicaciones (APPx, APPy, APPz) del terminal de pago. Esto es lo que permite no modificar estas aplicaciones que ya han sido aprobadas. De hecho, las aplicaciones del terminal de pago utilizan canales de transmisión de datos. De este modo, para las aplicaciones del terminal de pago, el funcionamiento es idéntico al funcionamiento anterior: las aplicaciones utilizan los canales de los que tienen necesidad para ejecutarse.

30 La diferencia reside en la "materialización" del canal. De hecho, ahí donde el canal era una vía real de transmisión de datos entre dos equipos, la invención materializa el canal bajo la forma de una cola de tipo FIFO. Hay por lo tanto cinco colas (sea tantas como canales virtuales) en las que las tramas TLV se insertan (por las aplicaciones del terminal de pago) o se obtienen (provenientes del terminal de comunicación). Las colas se gestionan por el dispositivo de multiplexación (MP). Este se encarga de verificar el contenido de las colas (F1 a F5) y de encapsular las tramas TLV bajo la forma de mensajes anteriormente descritos en relación con la figura 4 y de transmitir mensajes al terminal de comunicación. Por el contrario, recibe los mensajes *iAP* provenientes del terminal de comunicación e identifica la cola (F1 a F5) en la que la trama TLV contenida en ese mensaje debe insertarse. Abre el mensaje *iAP* (es decir, elimina las informaciones de encabezamiento TLV) y, con ayuda del número de canal virtual contenido en el mensaje, coloca la trama TLV en la cola. La aplicación a la que esta trama TLV se destina la recupera para el tratamiento y la trama TLV se elimina de la cola para el dispositivo de multiplexación. El dispositivo de multiplexación puede implementarse bajo la forma de un componente de hardware o de un componente de software.

1.3 Otras características opcionales y ventajas

40 Se presenta, en relación con la figura 6, un modo de realización de un dispositivo de multiplexación de mensaje según la invención.

Por ejemplo, el dispositivo de multiplexación comprende una memoria 61 constituida de una memoria búfer, una unidad 62 de tratamiento, equipada, por ejemplo, de un microprocesador y de una memoria RAM, y pilotada por el programa 63 informático, implementando un procedimiento de multiplexación según la invención.

45 En la inicialización, las instrucciones del código del programa 63 informático se cargan, por ejemplo, en una memoria antes de ejecutarse por el procesador de la unidad 62 de tratamiento.

La unidad 62 de tratamiento recibe como entrada una trama TLV emitida por una aplicación del terminal de pago. Esta trama TLV se destina originalmente a transmitirse por un canal de comunicación. El dispositivo intercepta esta trama TLV y la almacena en una cola correspondiente en el canal virtual que emula el canal de comunicación.

50 La unidad 62 de tratamiento realiza en paralelo una encapsulación, bajo la forma de un mensaje *iAP*, de la trama TLV que acaba de insertarse en la cola y realiza la transmisión de este mensaje *iAP* al terminal de comunicación. Según un modo de realización de la invención, esta transmisión se implementa por medio de lingo "genérica" del protocolo *iAP*.

El microprocesador de la unidad 62 de tratamiento implementa las etapas del procedimiento de multiplexación para

permitir la transmisión de mensajes *iAP* según las instrucciones del programa 63 informático.

- 5 Para ello, el dispositivo de multiplexación comprende, además de la memoria 61 búfer, medios de inicialización de una interfaz de comunicación externa con dicho terminal de comunicación, medios de transmisión, a dicho terminal de comunicación, de una solicitud de creación de canales virtuales distantes, por medio de dicha interfaz de comunicación externa, medios de creación, en el seno de dicho terminal de pago, de canales virtuales locales correspondientes a dichos canales virtuales distantes, medios de transmisión de tramas de datos asociados a dichos canales virtuales locales por medio de dicha interfaz de comunicación externa. Estos medios se pilotan por el microprocesador de la unidad 62 de tratamiento.

REIVINDICACIONES

1. Procedimiento de multiplexación de mensajes intercambiados entre un terminal de pago y un terminal de comunicación por medio de una conexión entre dicho terminal de pago y dicho terminal de comunicación, utilizando el protocolo *iAP*, iPod Accessory Protocol, comprendiendo dicho procedimiento:

- 5 - una etapa (311) de inicialización de una interfaz de comunicación externa con dicho terminal de comunicación;
- una primera etapa (312) de transmisión, por dicho terminal de pago, a dicho terminal de comunicación, de una solicitud de creación de canales virtuales distantes, por medio de dicha interfaz de comunicación externa;
- una etapa (313) de creación, en el seno de dicho terminal de pago, de canales virtuales locales correspondientes a dichos canales virtuales distantes;
- 10 - una segunda etapa (32) de transmisión de tramas de datos asociados a dichos canales virtuales locales por medio de dicha interfaz de comunicación externa, dicho procedimiento en el que un canal virtual se crea bajo la forma de una cola, configurándose dicha cola para permitir la recepción, el registro y la eliminación de tramas TLV, Tipo-Longitud-Valor, destinadas a dicho canal virtual.

15 2. Procedimiento según la reivindicación 1, **caracterizado porque** dicha interfaz de comunicación externa es una interfaz RS232.

3. Procedimiento según la reivindicación 1, **caracterizado porque** comprende, además, antes de dicha etapa (311) de inicialización de interfaz de comunicación comprende una etapa (30) de autenticación de dicho terminal de pago con respecto a dicho terminal de comunicación que comprende:

- 20 - una etapa (301) de obtención de un certificado de autenticación; y
- una etapa (302) de verificación, de la autorización del terminal de pago que se emparejará con dicho terminal de comunicación con ayuda de dicho certificado de autenticación.

4. Procedimiento según la reivindicación 1, **caracterizado porque** dicha segunda etapa (32) de transmisión de tramas de datos asociados a dichos canales virtuales locales comprende:

- 25 - una etapa (321) de verificación, en el seno de dichos canales virtuales, de una presencia de una trama TLV destinada al terminal de comunicación;

y cuando uno de los canales comprende una tal trama:

- una etapa (322) de encapsulación de esta trama TLV en un mensaje (3221) *iAP*.

5. Procedimiento según la reivindicación 1, **caracterizado porque** dichos canales virtuales pertenecen al grupo que comprende:

- 30 - un canal virtual "transaction" de intercambio de datos relativos a las transacciones bancarias;
- un canal virtual "configuration" de intercambio de información de servicio;
- un canal virtual "SSL", de cifrado de transmisión de datos entre dicho terminal de pago y dicho terminal de comunicación;
- un canal virtual "Printer" de transmisión de datos de impresión;
- 35 - un canal virtual "Barcode" de gestión de la lectura de códigos de barras.

6. Dispositivo de multiplexación de mensajes intercambiados entre un terminal de pago y un terminal de comunicación por medio de una conexión entre dicho terminal de pago y dicho terminal de comunicación, utilizando el protocolo *iAP*, iPod Accessory Protocol, comprendiendo dicho dispositivo:

- 40 - medios (311) de inicialización de una interfaz de comunicación externa con dicho terminal de comunicación;
- primeros medios (312) de transmisión, por dicho terminal de pago, a dicho terminal de comunicación, de una solicitud de creación de canales virtuales distantes, por medio de dicha interfaz de comunicación externa;
- medios (313) de creación, en el seno de dicho terminal de pago, de canales virtuales locales correspondientes a dichos canales virtuales distantes;
- 45 - segundos medios (32) de transmisión de tramas de datos asociados a dichos canales virtuales locales por medio de dicha interfaz de comunicación externa, configurándose el dispositivo para crear un canal virtual bajo la forma de una cola, configurándose dicha cola para permitir la recepción, el registro y la eliminación de tramas TLV, Tipo-Longitud-Valor, destinadas a dicho canal virtual.

7. Producto de programa de ordenador descargable desde una red de comunicación y/o almacenado en un soporte legible por ordenador y/o ejecutable por un microprocesador, **caracterizado porque** comprende instrucciones de código de programa para la ejecución del procedimiento de producción según la al menos una de las reivindicaciones 1 a 5, cuando se ejecuta en un ordenador.

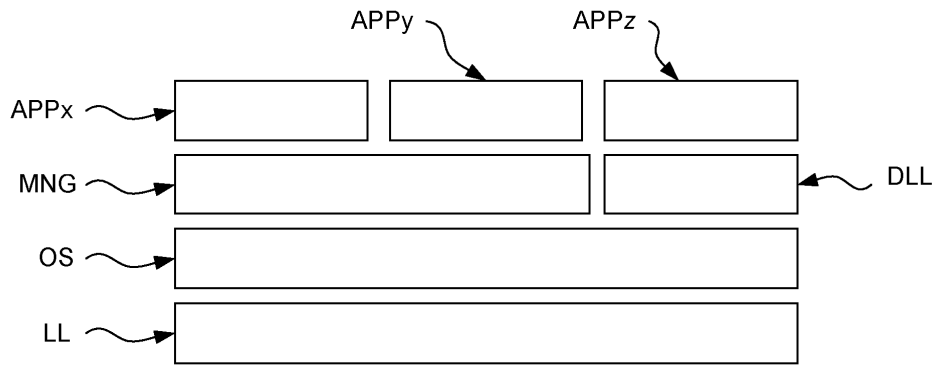


Figura 2

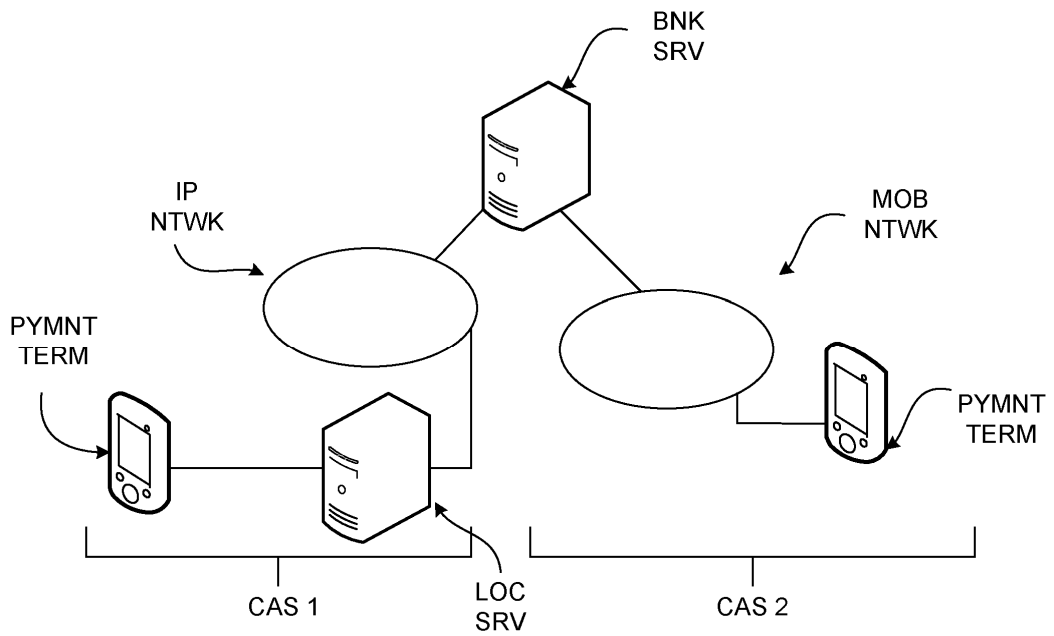


Figura 1

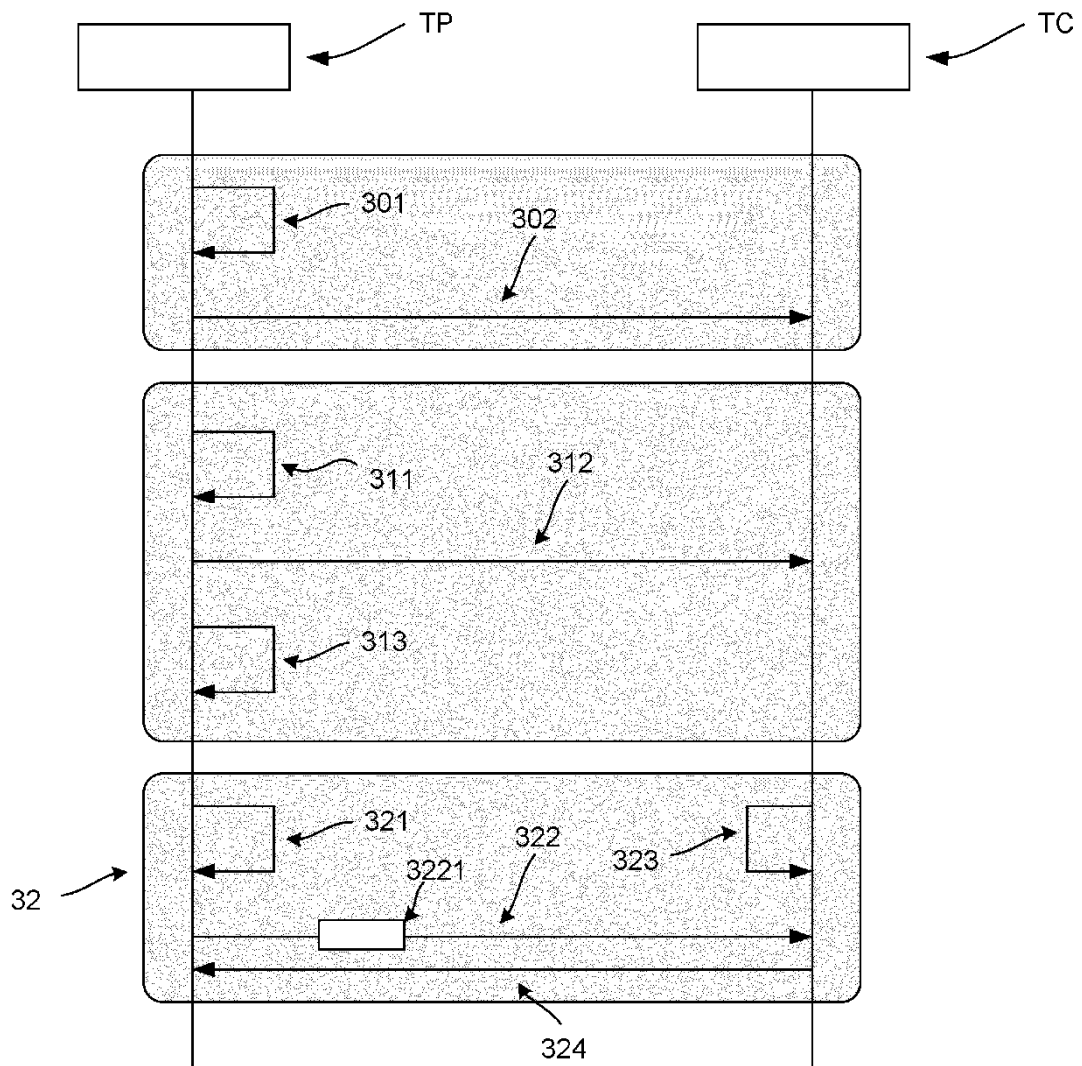


Figura 3

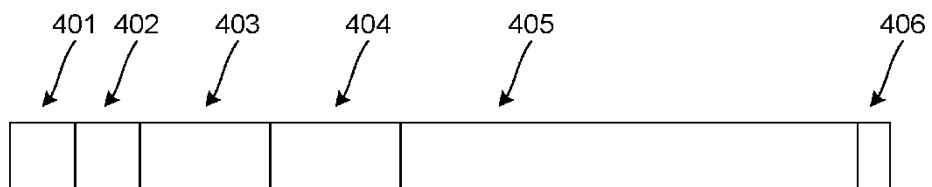


Figura 4

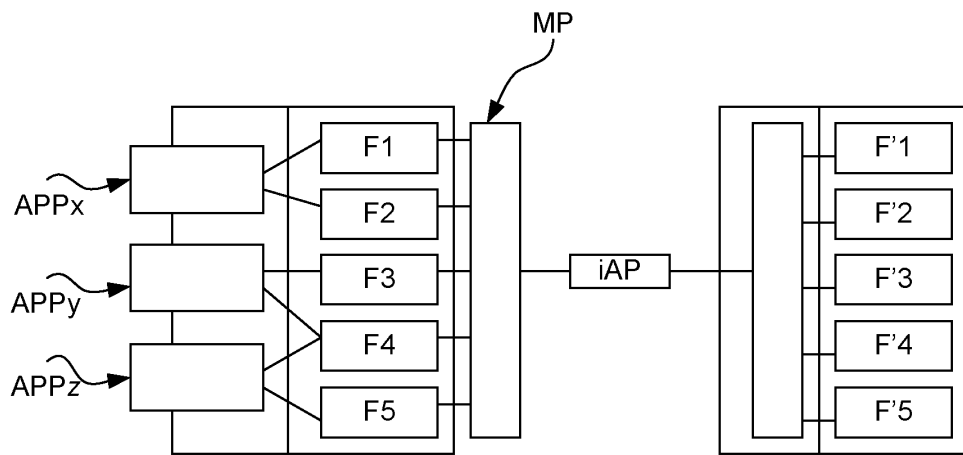


Figura 5

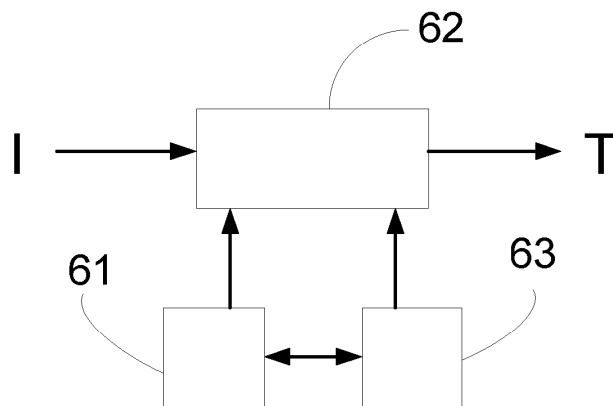


Figura 6