

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 606 940**

51 Int. Cl.:

H04L 29/06

(2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

86 Fecha de presentación y número de la solicitud internacional: **11.07.2002 PCT/FR2002/02455**

87 Fecha y número de publicación internacional: **13.02.2003 WO03013100**

96 Fecha de presentación y número de la solicitud europea: **11.07.2002 E 02764979 (7)**

97 Fecha y número de publicación de la concesión europea: **15.06.2016 EP 1415454**

54 Título: **Método y dispositivo para el establecimiento de compatibilidad de una comunicación entre terminales en la red, por ejemplo para permitir el diálogo con una aplicación de tarjeta inteligente**

30 Prioridad:

02.08.2001 FR 0110390

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

28.03.2017

73 Titular/es:

**GEMALTO SA (100.0%)
6, RUE DE LA VERRERIE
92190 MEUDON, FR**

72 Inventor/es:

**LAGOSANTO, LAURENT y
VANDEWALLE, JEAN-JACQUES**

74 Agente/Representante:

ISERN CUYAS, María Luisa

ES 2 606 940 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

Método y dispositivo para el establecimiento de compatibilidad de una comunicación entre terminales en la red, por ejemplo para permitir el dialogo con una aplicación de tarjeta inteligente

La invención se refiere a la comunicación en la red, por ejemplo, entre un terminal servidor y un terminal aplicación. Conciene más particularmente a un método y dispositivo que permiten establecer un canal de comunicación en una red, mientras que los terminales no tienen la misma interfaz de software de intercambio de mensajes en la red. Tal situación se produce, por ejemplo, cuando el terminal servidor se materializa en forma de tarjeta inteligente o similar.

En lo que sigue, se considera el caso de una comunicación con una tarjeta inteligente que comprende una aplicación de servicio (Applet) escrito en lenguaje de alto nivel, particularmente un lenguaje orientado a objetos, tales como Java, C ++, etc. El conjunto constituido por la tarjeta y la aplicación de servicio forma una aplicación en la tarjeta. Este conjunto constituye un terminal servidor que puede participar en una comunicación con un terminal cliente local o en la red.

La figura 1 muestra esquemáticamente los elementos funcionales que intervienen en una comunicación en modo local entre una tarjeta inteligente 2 y una máquina cliente 4, esta última pudiendo ser un terminal en un sistema centralizado. Una conexión local LL garantiza el intercambio bidireccional entre la máquina cliente 4 y la tarjeta 2 a través de las interfaces de comunicación respectivas 6 y 8. La conexión local LL puede ser un cable en serie o paralelo entre la máquina cliente 4 y la tarjeta (o su lector) o también una conexión hertziana si la tarjeta 2 funciona en modo sin contacto.

La máquina cliente 4 incluye 10 LA aplicación cliente 10 que debe establecer un dialogo con una aplicación de servicio 12 integrada en la tarjeta 2 y designada de aquí en adelante "aplicación tarjeta". En el ejemplo, la aplicación tarjeta se realiza bajo una forma llamada "Applet", que es un término acuñado en el ámbito del lenguaje "Java Card". En el nivel de las aplicaciones cliente y de servicios, el dialogo se lleva a cabo a través de mensajes en el lenguaje de alto nivel emitido por la aplicación cliente 10 de la máquina 4. Estos mensajes incluyen generalmente órdenes de procesamiento a realizar en los datos que son almacenados en el seno de la tarjeta 2. Tendremos, por ejemplo, para un monedero electrónico en la tarjeta: m = débito monedero (parámetro = suma (valor numérico), n = crédito monedero (parámetro = suma (valor numérico), O = saldo (sin parámetros) (balance de las operaciones). A título ilustrativo, las órdenes tienen una estructura sintáctica del tipo "débito (suma)" (para el caso de la orden m precitada).

Estas órdenes no pueden pasar como tales en la conexión local LL, ya que requiere el uso de un protocolo y un formato específico. Se instala entonces, el lado de la máquina cliente de la conexión local LL, una sucesión de capas de software entre la aplicación cliente y la interfaz de comunicación 6.

A partir de la aplicación cliente 10, una primera capa de software constituye lo que se llama el representante de la aplicación tarjeta 14, también conocido por el término anglosajón de "proxy". El representante es una capa desarrollada y codificada por el desarrollador de la aplicación tarjeta 12, que se utiliza para presentar una interfaz de software que permite la comunicación con esta aplicación. Se trata de una interfaz del

punto de vista funcional de la aplicación tarjeta, es decir del lado "técnico" de la aplicación, completamente dedicada a ella. El representante 14 sirve entonces para establecer la compatibilidad de las órdenes de la aplicación cliente 10 con las reconocidas por la aplicación tarjeta 12. Por lo tanto, es necesario producir el código del representante en función de la aplicación tarjeta.

El doble enmarcado de un elemento en las figuras, utilizado particularmente para identificar el representante 14, indica los códigos a desarrollar y transmitir a la máquina cliente 4 con el fin de poder utilizar la aplicación tarjeta 12.

Así, para retomar el ejemplo de una orden de la aplicación cliente 10 de estructura sintáctica "do Sthg" con los parámetros, sea "do Sthg(parámetros)", el representante producirá -en el supuesto que dicha orden sea reconocida por la aplicación tarjeta 12- una orden llamada de formato, sea "formato(do Sthg (parámetros))". Téngase en cuenta que los parámetros pueden, si es necesario, ser inexistentes, dando la estructura "do Sthg()". A continuación, los parámetros no son designados explícitamente. Por lo tanto, para retomar el ejemplo de la orden m precitado, su representación en la forma general será "do Sthg (parámetros)".

Esta orden de formato se transmite a una capa 16 en ejecución, llamada de formato de tarjeta CFcarte, que garantiza la transformación del código emitido de esta orden en un formato de mensaje adaptado al dispositivo de comunicación. Tienen por función principal estructurar el mensaje a enviar a la aplicación tarjeta. A título de ejemplo, si la orden está directamente destinada a la tarjeta 2, el formato producido por la capa de formato 16 será del tipo APDU (del anglosajón "aplication protocol data unit"); si pasa por un protocolo inalámbrico, será conforme a un código SMS (del anglosajón "short message service"); también puede ser un formato específico para una tarjeta, como el formato JC21 RMI (del anglosajón "Java Card 2.1 RMI").

Una vez el mensaje estructurado, está listo para ser enviado a través de la conexión local LL. Para este fin, se utiliza un protocolo de comunicación, sea una capa 18 de transporte TRcarte, que es responsable de la emisión del mensaje. Esta capa 18 garantiza el transporte del mensaje de acuerdo con un protocolo determinado, por ejemplo: OTA (del anglosajón "over the air"). PCMCIA, "Puerto de serie". etc. La capa de transporte 18 TRcarte "empaqueta" así los mensajes que se han formateado en una estructura adaptada para el transporte en la conexión local LL. Los mensajes así empaquetados son transmitidos entonces a la tarjeta 2, a través de las interfaces de comunicación 6 y 8 y la conexión local LL.

En el lado de la tarjeta 2. nos encontramos las mismas capas que en la máquina cliente 4 para realizar sucesivamente las operaciones inversas (llamadas operaciones "duals") para lograr. a partir de los datos transmitidos desde la capa de transporte 18 para controlar TRcarte a la orden de alto nivel, en este caso "do Sthg".

Por lo tanto, a nivel de la tarjeta 2, la primera capa del lado de la interfaz 8 es una capa de transporte dual 20 TRcarte⁻¹ que tiene la función de "desempaquetar" cada mensaje recibido en la conexión local LL. En el caso del mensaje proveniente de la orden "do Sthg", la capa dual 20 TRcarte⁻¹ produce una orden de "desformatear" el mensaje "Msg tarjeta", sea "desformato (MSG tarjeta)".

Esta orden es recibida por una capa de desformateo 22 CFcarte¹, dual vis-a-vis de la capa 16 CFcarte, que produce en respuesta a la orden de transmitir la orden "do Sthg (parámetros)" a un piloto de orden de tarjeta 24.

- 5 El piloto 24 actúa esencialmente como router, siendo su función la de dirigir la orden así desformateada hacia la aplicación tarjeta 12 que le es destinada.

La flecha F1 "código específico Applet" en la figura, entre la aplicación tarjeta 12 y el representante 14, indica que para el desarrollo de una aplicación tarjeta (por ejemplo. una "Applet"), se debe instalar el representante de esta aplicación en la aplicación, cliente.

Por supuesto, se aplica el mismo procesamiento de los mensajes, en orden inverso, para los retornos de la aplicación tarjeta 12 hacia la aplicación cliente 10, como muestran las flechas punteadas.

15 Téngase en cuenta que en la figura. todo lo que existe entre los diferentes rectángulos son llamados de rutina del rectángulo situado abajo.

La entidad "Mensaje tarjeta" (Msg tarjeta) es un formato de intercambio que contiene el nombre del método (por ejemplo, "do Sthg") y que estructura los parámetros según el protocolo que va a ser utilizado a continuación. El mensaje tarjeta constituye todo el nombre del método, por tanto su nombre y sus parámetros, que serán estructurados según un protocolo de comunicación.

25 Cuando este mensaje se envía a la capa de transporte 18 TRcarte, pasa el protocolo APDU al protocolo llamado TPDU, que constituye el protocolo de transporte. Para enviar el mensaje, se descompone en una serie de bits y de paquetes en la línea. El mensaje es entonces efectivamente una codificación de una función. Cuando pasa sobre una capa de transporte, se presenta en forma de tramas.

30 Se entiende que el representante constituye una pasarela que permite a la aplicación cliente dialogar como si la aplicación tarjeta 12 estuviera presente en la máquina cliente; dicho de otra manera, "representa" la aplicación de servicio en el sentido de que la aplicación cliente interactúa con el representante a través de los mismos mensajes de alto nivel. El representante presenta, por tanto, la misma interfaz funcional, al mismo nivel de acceso, que la aplicación de servicio en la tarjeta. De ese modo, cuando se requiere que la aplicación cliente se comunique con la aplicación de servicio en la tarjeta, esta aplicación cliente no tendrá que codificar los mensajes para pasarlos a un módulo de pilotaje (conocido por el termino Ingles de "driver"), sino que tendrá que emitir el comando deseado.

Las capas son siempre las mismas, independientemente de cuales sean los dispositivos. Por lo tanto, para la comunicación entre un cliente y un terminal remoto, la estratificación de las capas permanece invariable.

45 Esta comunidad de las capas se ilustra en la figura 2, que representa una estructura análoga a la de la figura 1, pero aplicado al caso de una comunicación en una red R. como la de Internet, entre una máquina cliente 30 y una máquina servidor 32.

Más particularmente, la comunicación se establece entre una aplicación cliente 10 instalada en la máquina cliente 30 y un servidor de red 34, análoga a la aplicación tarjeta 12 de la figura 1, instalada en la máquina servidor 32.

- 5 El servidor red 34 se representa entonces, a nivel de la máquina cliente 30, por un representante servidor de red 36, al igual que el representante tarjeta 14 de la figura 1.

En la figura 2, y las que siguen, las interfaces materiales de comunicación no se muestran por razones de simplicidad, dado que estos medios ya son bien conocidos

10

Los comandos del representante servidor de red 36 son sucesivamente procesados por capa con formato de red 38 CFnet y una capa de transporte de red 40 TRnet, respectivamente análogas a las capas 16 CFcarte y 18 TRcarte de la figura 1. La capa 40 TRnet asegura principalmente el desglose de los mensajes en tramas adaptadas a las

15

Del lado de la máquina servidor 32, se encuentra la capa de transporte dual 42 TRnet¹ que recibe las tramas recibidas de la red R y las reconstruye en mensajes como lo eran a la salida de la capa 38 CFnet.

20

La capa 42 TRnet¹ es sucedida por la capa dual 44 CFnet¹, que es un código de desformateado de red cuya función es la de transformar los mensajes reconstituidos en lenguaje de alto nivel, por ejemplo bajo la forma "enviar" "do Sthg".

25

Los comandos de la capa CFnet¹ se transmiten a un piloto de comando de red 46, que los distribuye hacia la aplicación destinada a tratarlos, en este caso el servidor de red 34.

Observamos que siempre resulta necesario desarrollar el código específico para el representante servidor de red 36 en función del servidor 34 que lo debe representar.

30

La utilización del representante servidor de red 36 y del piloto de comando de red 46 en los extremos respectivos de la red R permite a la aplicación cliente 10 de la máquina cliente 30 abstraerse de los protocolos de comunicación, su funcionamiento por lo que respecta a la comunicación que sigue a nivel del formato general. El representante y el

35

A partir de las estructuras de transmisión de mensajes según las figuras 1 y 2, es posible, por simple concatenación de medios, comunicar una aplicación tarjeta con una aplicación cliente a través de una red R. y así comunicar la tarjeta con cualquier terminal remoto.

40

En este caso, la aplicación tarjeta será conectada a un servidor de red a través de un enlace local, y la aplicación cliente se conectará al servidor de red a través de una conexión de red.

45

La puesta en práctica consiste entonces en una concatenación de las cadenas de transmisión de las figuras 1 y 2, como muestra la figura 3. Los elementos de esta figura ya mencionados en relación con la figura 1 ó 2 tienen las mismas referencias y no se describirán de nuevo por razones de brevedad.

50

Según esta concatenación, la aplicación cliente 10 se encuentra al lado de la máquina cliente 30, seguida de sus tres capas: el representante "Applet de red" (llamada al

melado) 36, el código de formato red (codificación de la llamada) 38 CFnet y la capa de transporte red 40 TRnet. En este caso, el representante servidor 36 de la figura 2 se convierte aquí el representante de la aplicación tarjeta (Applet), designado por la referencia 36'.

A nivel del terminal 31 asociado a la tarjeta 2, en la red R de la capa de transmisión de paquetes TRnet, se vuelve a todas las capas dobles, a saber, sucesivamente: 42 TRnet⁻¹ y 44 CFnet⁻¹ para transmitir una orden ("do Sthg") al controlador de la orden 46, de modo que se oriente automáticamente hacia el servidor de red 34.

A continuación, el comando "do Sthg" es redirigido desde el servidor de red 34 hacia el representante de la aplicación tarjeta 14 en el terminal 31. El representante emite en respuesta la orden "formato ("do Sthg") a la capa 16 CFcarte quien emite entonces el mensaje tarjeta (Msg tarjeta) a la capa 18 de transporte 18 18TRcarte para para este mensaje sea transmitido en forma de paquetes a través de la conexión local LL a la tarjeta 2.

En la tarjeta 2, los paquetes se procesan sucesivamente por capas dobles 20 TRcarte⁻¹, y 22 CFcarte⁻¹ para conseguir la orden de transmitir el comando ("do Sthg") al controlador de comando tarjeta 24. Este último transmite finalmente el comando "do Sthg" a la aplicación tarjeta 12.

En resumen, el desarrollo de una aplicación de servicio y una aplicación cliente incluye las siguientes etapas:

- escritura de una aplicación de servicio.
- escritura de un representante para los terminales.
- realización de la aplicación cliente con, por ejemplo, interfaces de usuario (ventanas, menús, etc.), comunicando en un lenguaje de alto nivel con el representante de la aplicación tarjeta

Se observa que los enlaces principales de la cadena de comunicación entre la aplicación cliente en la máquina cliente 30 y la aplicación tarjeta 2 en el terminal 31 incluye: un servidor de red 34, un representante del servidor de red 36', y un representante 14 de la aplicación tarjeta 12 a nivel del terminal 31. Cada uno de estos elementos 34, 36' y 14 incluye un código informático que es pesado de escribir y mantener. Si la aplicación cambia para que pueda explotar otros mensajes, entonces se hace necesario intervenir por separado en el código de cada uno de estos tres enlaces, debiendo así ser modificado el representante de red 36' para todas las máquinas susceptibles de comunicar con la aplicación cliente.

Una parte de este código puede ser desarrollado por técnicas de generación de representantes, pero lo cierto es que la implementación o modificación de una aplicación en un entorno de red es tedioso.

Este código también debe extenderse, es decir, que es necesario instalar el representante tarjeta 14 y el servidor de red 34 en los respectivos terminales, conectar estos dos enlaces 14 y 34, y luego instalar el representante en la aplicación cliente. Seguidamente, se debe realizar la unión del conjunto de los tres enlaces para asegurar la

buena comunicación, en particular entre el servidor de red 34 y el representante tarjeta 14.

5 Las dificultades de desarrollo se encuentran entonces en el ámbito de gestión y mantenimiento. Los riesgos de error son incluso más grandes que el hecho de que el código de estos enlaces sea complejo y largo de producir, sobre todo si está escrito a mano.

10 Además, debido a la gran cantidad de capas de software entre la aplicación cliente 10 y la aplicación de servicio 12, la comunicación puede sufrir un retraso significativo en el tiempo de respuesta. Por otro lado, las conexiones entre cada capa de software implican problemas de interfaz, que se añaden a los retrasos antes mencionados.

15 Esto se traduce en un retraso significativo en el tiempo de respuesta, ya que el procesamiento se realiza en cada enlace.

20 Por último, este enfoque se presta mal a la aseguración de un extremo a otro de la cadena. En efecto, es entonces necesario prever un etapa de cifrado y descifrado de mensajes, respectivamente, aguas arriba y aguas abajo de cada enlace 36', 34 y 14 de modo que los mensajes pueden ser comprendidos por estos últimos.

25 Se ha propuesto recientemente en "objetos móviles incorporados en una tarjeta inteligente con internet, para el comercio de objetos virtuales multimedia" P Urien Bull R&D. Conferencia OCM 2000, Objetos, Componentes. Modelos "Pasado, Presente, Futuro", 18 mayo 2000, Escuela de Minas de Nantes, a resolver estos problemas de acceso por red a una tarjeta remota poniendo la tarjeta en formato de red. La idea es. Entonces, que en lugar de tener un protocolo particular para comunicarse con la tarjeta, lo que obliga a instalar un controlador entre el terminal y la tarjeta, la tarjeta es directamente accesible como si se tratara de un servidor en la red.

30 Con este enfoque. la conexión se establece con un cliente remoto, un representante de red estándar, la red y la tarjeta directamente conectada a la red. No hay más enlaces intermedios entre la tarjeta y la red.

35 Sin embargo, resulta que es imposible producir una tarjeta de este tipo en el actual estado de la técnica.

40 Una primera técnica de acceso por red a una tarjeta de chip, en un dispositivo de comunicación, se describe en el documento de patente WO 01/31880 A1. Esta primera técnica citada concierne a una arquitectura que permite comunicar un servidor, en una aplicación cliente, y una aplicación tarjeta de chip. en una aplicación de servicio. Para realizar esto, la arquitectura integra un nudo de comunicación, primero en un terminal conectado a la tarjeta de chip, y después en marco seguro previsto en el terminal y dotado de un lector de tarjeta de chip, dirigiéndose a la tarjeta de chip como a un servidor HTTP de red.

50 Una segunda técnica de acceso por red a una tarjeta de chip, en un dispositivo de comunicación, se describe en el documento de patente WO 01/24475 A2. Esta segunda técnica citada concierne a una arquitectura que permite comunicar un servidor, en una aplicación cliente, y una aplicación tarjeta de chip, en una aplicación de servicio. Para realizar esto, la arquitectura prevé integrar en un terminal conectado a la tarjeta de chip,

un navegador Web y un servidor TCP/IP, para dirigirse, a través del servidor TCP/IP, a la tarjeta de chip.

5 En vista de lo anterior, la invención tiene por objetos, un sistema, un procedimiento, y una utilización de una pasarela del tipo red-dispositivo de comunicación según las reivindicaciones 1, 9 y 14 aquí anexas respectivamente.

10 Las características opcionales de la invención presentadas como parte del sistema pueden aplicarse, *mutatis mutandis*, al procedimiento anterior según el segundo aspecto, y no serán repetidas por razones de brevedad.

15 La invención y las ventajas derivadas aparecerán más claramente en la lectura de las formas de realización preferidas, dadas únicamente a título de ejemplos no limitativos, con referencia a los dibujos que se acompañan, en los cuales:

- la figura 1, ya descrita, es un diagrama sinóptico de los enlaces que intervienen para realizar una comunicación entre una aplicación cliente y una aplicación tarjeta a través de una conexión local según una técnica conocida;

20 - la figura 2, ya descrita, es un diagrama sinóptico de los enlaces que intervienen para realizar una comunicación entre una máquina cliente y una máquina servidor a través de red, como internet, según una técnica conocida;

25 - la figura 3, ya descrita, es un diagrama sinóptico de los enlaces que intervienen para realizar una comunicación entre una aplicación cliente en una máquina cliente y una aplicación tarjeta a través de red, por una simple combinación de los medios de las figuras 1 y 2;

30 - la figura 4 es un diagrama sinóptico de los enlaces que intervienen para realizar una comunicación entre una aplicación cliente en una máquina cliente y una aplicación tarjeta a través de una red según una primera forma de realización de la invención;

- la figura 5 es un diagrama análogo al de la figura 4, que representa una variante que constituye una segunda forma de realización de la invención; y

35 - la figura 6 es un diagrama análogo al de la figura 4, que representa otra alternativa para el caso de una conexión directa entre la máquina cliente y la tarjeta, que constituye una tercera forma de realización de la invención.

40 En el conjunto de las figuras 4 a 6, los elementos ya presentados en el contexto de las figuras 1 a 3 llevan las mismas referencias y no se describirán de nuevo por razones de brevedad.

45 La figura 4 muestra los elementos principales que intervienen en una primera forma de realización de la invención.

50 Conforme a este modo, se establece una cadena de transmisión de mensajes entre una aplicación cliente 10 situada en una máquina cliente 30 y una aplicación de tarjeta (Applet) 12 situada en una tarjeta de chip 2 o cualquier otro dispositivo portátil comunicador, asociado a un terminal 31. La transmisión de mensajes entre el terminal 31

y la tarjeta 2 es garantizada por una conexión local LL. La máquina cliente 30 es remota y comunica con el terminal 31 a través de una red R, tal como Internet.

5 La cadena de transmisión se describirá en el contexto de un mensaje, en este caso el comando "do Sthg" transmitido desde la aplicación cliente 10 a la aplicación de tarjeta 12.

En la máquina cliente 30, se prevé un representante "Applet de red" 50 para emitir comandos de formato apropiados a partir de los mensajes de la aplicación cliente 10. Por lo tanto, en el caso del mensaje "do Sthg", el representante "Applet de red" 50 producirá un comando de formato "formato ("do Sthg").

De acuerdo con la invención, el mensaje "do Sthg" ya no se codifica en formato de red R, sino directamente en un formato comprensible por la aplicación tarjeta 12. Con este fin, se prevé aguas abajo del representante "Applet de red" 50 una capa 16' de código de formato tarjeta CFcarte. Esta capa 16' tiene como función crear un mensaje Msg tarjeta, comprensible por una capa doble de 22 CFcarte⁻¹ en la tarjeta 2, que corresponde al comando de alto nivel "do Sthg". La capa doble 22 podrá entonces dictar el comando "do Sthg" en respuesta a un comando de desformateado del mensaje Msg Tarjeta.

20 Para garantizar el transporte del mensaje Msg Tarjeta, la capa 16' CFcarte inicializa el proceso de encapsulación del mensaje solicitando que sea integrado en un formato de cuadro de octetos "byte[]", que constituye un envoltorio para el mensaje, comprensible por la red R, y dentro del cual puede ser también transportado como tal a través de la red R. Con este fin, la capa 16' CFcarte será seguida de un conjunto de capas que permitirá la transferencia del mensaje en la red R.

En el ejemplo, esta disposición se consigue mediante una operación "exchange" (intercambio) que actúa sobre el mensaje Msg Tarjeta. De este modo, se obtiene de salida de la capa 16' CFcarte el comando "exchange (Msg Tarjeta)".

30 Este comando "exchange (Msg Tarjeta)" se transmite a continuación desde la capa 16' CFcarte a un representante GTW 52 de la pasarela 54. La función de este representante GTW 52 es controlar el formato de los mensajes que se le son presentados en vista de su transporte en la red. El representante GTW es una capa de software desarrollado específicamente para representar una pasarela GTW red-tarjeta 54 situada en el terminal 31. El termino pasarela se conoce igualmente por la denominación anglosajona "gateway".

40 Se ha de tener en cuenta que el representante de la pasarela GTW 52 sustituye al servidor de red 34 de las figuras 2 y 3. Es genérico que no tiene la misma interfaz que la aplicación tarjeta (Applet) 12 contenida en la tarjeta. En efecto, a diferencia del servidor de red 34 antes citado, no es necesario para el representante GTW 52 interpretar el contenido de los mensajes que hace transitar. Para esto, se utiliza la capa CFnet 38 para "encapsular", o insertar en un envoltorio, el mensaje (Msg Tarjeta) a transitar por la pasarela GTW red-tarjeta 54 según un formato de cápsula (o de envoltorio) que sea comprensible por una pasarela genérica. En este contexto, el operador "exchange" 45 constituye con el representante GTW 52 una nueva interfaz vis-a-vis de la pasarela red-carta 54 en el terminal 31, como aparecerá más adelante.

Por lo tanto, el representante de la pasarela GTW 52 transmite a destino de una capa 38 de formato de red CFnet un comando de formato del tipo "formato ("exchange (Msg Tarjeta)").

5 La capa CFnet 38 transmite entonces el comando bajo la forma de mensaje de red "Msg Red" hacia una capa de transporte 40 TRnet. Esta última garantiza la transmisión en la red R del comando bajo la forma de paquetes TRnet al formato de los mensajes de red. Las funciones de las capas 38 CFnet y 40 TRnet son todas análogas a las de las capas correspondientes de la figura 2.

10 Se observa que el formato del mensaje en la salida de la capa 40 TRnet se compone de dos capas:

15 - una capa "interior", donde se encuentra el formato de tipo tarjeta, comprensible por la aplicación tarjeta 12, por ejemplo, del tipo APDU, SMS o tarjeta de Java RMI, y

- un recubrimiento, que corresponde al formato de la red, por ejemplo según el protocolo de Internet.

20 Conceptualmente, se pone el mensaje, en este caso el comando "do Sthg" en un envoltorio llamado "exchange", que esta formateado con una dirección y transmitido por la capa de transporte 40 TRnet.

25 En el otro lado de la red, en el terminal 31, el mensaje procedente de la capa 40 TRnet es tratado sucesivamente por las capas dobles 42 TRnet⁻¹ y 44 CFnet⁻¹, que producen las funciones inversas respectivamente de las capas 40 TRnet y 38 CFnet de la máquina cliente 30. Como se describe en el contexto de la figura 2, se obtiene entonces sucesivamente el comando "deformato (Msg Red)". a la salida de la capa 42 TRnet⁻¹ y el comando "enviar("exchange (Msg tarjeta) ") de la capa 44 CFnet⁻¹.

30 A la salida de la capa CFnet⁻¹, el comando "enviar ("Exchange (Msg Tarjeta)")" es recepcionado por un controlador de comando de red 46, que lo dirige hacia la pasarela GTW red-tarjeta 54 del terminal. La pasarela GTW 54 envía entonces el mensaje "Msg Tarjeta" a una capa de transporte 18 TRcarte del terminal 31. Esto garantiza la conversión al formato de transporte, según un desglose por paquete específico, para la transmisión por la conexión LL a la tarjeta 2.

40 A nivel de la tarjeta el mensaje así transmitido es tratado por las capas dobles 20 TRcarte⁻¹ y 22 CFcarte⁻¹ que producen respectivamente el comando "deformato (Msg Tarjeta) y el comando "enviar (do Sthg ")". Este último es recibido por un controlador de comando de control 24 que transmite la orden "do Sthg" a la aplicación tarjeta (Applet) 12.

45 La organización de acuerdo con la figura 4 es remarcable por el hecho de que necesita desarrollar un solo código específico para la aplicación tarjeta, a saber el representante "Applet de red" 50 de esta aplicación a nivel de la máquina cliente 30 (flecha F3) Contrariamente al caso de la figura 3, resulta inútil desarrollar, codificar y gestionar un servidor de red específico, ni un representante de la aplicación tarjeta en el servidor. Esto resulta en una gran simplificación de la implementación de una comunicación en red entre la aplicación cliente 10 y la aplicación tarjeta 12.

Por otra parte, la implementación de la pasarela GTW red-tarjeta 54 es fácil, ya que no es específica para la aplicación tarjeta 12. En efecto, bastará que la pasarela GTW red-tarjeta 54 sea específica simplemente para los protocolos de comunicación establecidos, ya sea un protocolo de entrada y un protocolo de salida, para garantizar la comunicación.

En el ejemplo, la pasarela GTW red-tarjeta 54 es capaz de recibir un mensaje de acuerdo con un protocolo de Internet para remitirlo de acuerdo con un protocolo tarjeta.

La figura 5 muestra la organización de una segunda forma de realización de la invención, adaptada para una comunicación entre la máquina cliente 30 y el terminal 31 según un modo conocido por el término "socket". De acuerdo con el modo "socket", se establece un formato de intercambio entre el cliente y el servidor, lo que permite liberarse del representante de pasarela de red GTW 52 y de la capa 38 CFnet de la máquina cliente 31, y de la capa doble 44 CFnet¹ y del controlador de comando de red 46 del terminal 31. Excepto por la supresión de estos elementos, la configuración y el principio de funcionamiento de esta forma de realización son idénticos a los de la figura 4.

La Figura 6 muestra la organización de una tercera realización de la invención, adaptado para el caso de una aplicación cliente 10 situada en el mismo soporte físico que el terminal que incorpora GTW 54.

Según esta configuración, el soporte físico 60 incorpora una conexión interna y directa LL' entre la capa CFcarte 16' y la pasarela GTW 54. Se observa que se trata de una pasarela del tipo conexión interno-tarjeta. Los comandos de tipo "intercambio" en la salida de la capa 16' así enviados directamente a la pasarela GTW red-tarjeta 54 son retransmitidos por esta última a la aplicación tarjeta 12 por las capas sucesivas 18 a 24, como en los casos precedentes.

Por otra parte, el conjunto 60 puede conectarse a través de la misma pasarela GTW red-tarjeta 54 tanto en la aplicación cliente 10 que integra como en cualquier otra aplicación cliente conectada por red, lo que confiere una polivalencia a nivel de arquitectura del sistema.

Por supuesto, los sistemas de comunicación de las figuras 4 a 6 permiten igualmente gestionar las devoluciones de mensajes (camino por las flechas de trazos) de la aplicación tarjeta 12 a la aplicación cliente 10 por simple inversión de las transformaciones a las capas sucesivas.

En todas las realizaciones, es fácil lograr una seguridad "de extremo a extremo" entre la aplicación cliente 10 y la aplicación tarjeta 12. En efecto, como la pasarela GTW red-tarjeta 54 no tiene que interpretar el contenido de los mensajes, se hace posible asegurar los mensajes en la capa 16 CFcarte de la máquina cliente y mantenerlos seguros hasta la capa doble 22 CFcarte¹ de la tarjeta 2, donde pueden ser decodificados.

La invención se ha descrito en el contexto de aplicación de la tarjeta inteligente 2 accedida por una aplicación cliente en un terminal remoto (figuras 4 y 5) o local (figura 6). Sin embargo resulta obvio que los principios de la invención tienen un ámbito de aplicación mucho más amplio, que abarca todo el campo de compatibilidad de los sistemas de comunicación. A modo de ejemplo no limitativo, la invención puede implementarse también con:

- cualquier dispositivo comunicador, portátil o no;

- cualquier tipo de protocolo de comunicación de red o conexión local;
- cualquier tipo de aplicación en cada extremo de la cadena de comunicación;
- 5 - cualquier protocolo de estructuración y formato de mensajes según las capas de software y los lenguajes utilizados;
- un número ilimitado de máquinas comunicantes conectadas.

REIVINDICACIONES

1. Sistema para establecer un canal de comunicación en una conexión (R; LL') que conecta, de una parte, una aplicación cliente (10) en una máquina cliente (30) y, de otra parte, una aplicación de servicio (12), estando presente la aplicación de servicio en un dispositivo (2) comunicante, el dispositivo comunicante estando conectado a un terminal (31),

caracterizado porque el sistema comprende además:

- un representante (50) de la aplicación de servicio situado en la máquina cliente (30), para emitir las órdenes de formateado a partir de los mensajes de la aplicación cliente,

- un módulo de formateado (16') situado en la máquina cliente (30), en dicho representante (50), para dar formato a los mensajes de la aplicación cliente en una forma (intercambio (Msg tarjeta)) comprensible por la aplicación de servicio (12), y

- una pasarela (54) situada en el terminal (31), para recibir dichos mensajes comprensibles por el dispositivo comunicante y transmitir dichos mensajes comprensibles por el dispositivo comunicante a la aplicación de servicio (12).

2. Sistema según la reivindicación 1, en el que el dispositivo comunicante es una tarjeta de chip (2), siendo la aplicación de servicio una aplicación tarjeta (12).

3. Sistema según la reivindicación 1 o 2, en el que el sistema comprende, además, medios de aseguramiento de los mensajes que operan en el módulo de formateado (16') o con anterioridad al módulo de formateado, con el fin de permitir a los mensajes seguros provenientes del módulo de formateado transitar, de forma segura, a través de la pasarela (54) y hasta el dispositivo comunicante (2).

4. Sistema según una cualquiera de las reivindicaciones 1 a 3, en el que dicha conexión comprende una red (R) que conecta la máquina cliente (30) y el terminal (31), siendo dicha pasarela (54) del tipo red-dispositivo comunicante.

5. Sistema según la reivindicación 4, en el que el módulo de formateado (16') está conectado a la red (R) a través de una concatenación de módulos que comprende sucesivamente:

- un representante (52) de dicha pasarela (54), para recibir los comandos de formateado (intercambio (Msg tarjeta)) del módulo de formateado (16') y producir en respuesta comandos (formato ("intercambio (Msg tarjeta))) de formateado de estos comandos según un formato comprensible por dicha pasarela (54);

- un módulo de formateado de red (38) para formatear dichos comandos del representante (52) de la pasarela en mensajes (intercambio Msg Red) de formato de red; y

- un módulo de transporte (40) para la adaptación de dichos mensajes (intercambio Msg Red) al estándar de la red (R),

y en el que dicha pasarela (54) está conectada a la red (R) a través de una concatenación de modules que comprende sucesivamente:

- un módulo (42) dual al módulo de transporte (40) conectado a la red (R) para recuperar dichos mensajes (intercambio Msg Red) provenientes de la red;

- un módulo (44) dual al módulo de formateado de red (38) para recuperar los comandos como los provenientes del representante (52) de dicha pasarela (54); y

- un controlador de comandos de red (46) para transmitir los mensajes (intercambio (Msg tarjeta) desde el módulo (44) dual al módulo de formateado de red (38) hacia dicha pasarela (54).

6. Sistema según la reivindicación 4. en el que el módulo de formateado (16') está conectado a la red (R) a través de un módulo de transporte (40) destinado a recibir directamente del módulo de formateado dichos mensajes (intercambio (Msg tarjeta)) comprensibles por el dispositivo comunicante y empaquetar dichos mensajes comprensibles por el dispositivo comunicante, los mensajes resultantes de una operación de empaquetar estando así empaquetados, para transportar dichos mensajes comprensibles por el dispositivo comunicante a través de la red (R),

y en el que, la pasarela red-dispositivo comunicante (54) está conectada a la red (R), a través de un módulo (42) dual al módulo de transporte (40), el módulo dual al módulo de transporte (40) desempaqueta los mensajes empaquetados para recuperar dichos mensajes (intercambio (Msg tarjeta)) comprensibles por el dispositivo comunicante y retransmite directamente a la citada pasarela (54) dichos mensajes comprensibles por el dispositivo comunicante.

7. Sistema según una cualquiera de las reivindicaciones 1 a 3, en el que dicha máquina cliente (30) y dicho terminal (31), montados sobre un mismo soporte físico (60), están conectados por una conexión interna (LL'),

y en el que el módulo de formateado (16') está previsto para transmitir directamente, por dicha conexión interna, los mensajes de la aplicación cliente formateados (intercambio (Msg tarjeta)) a dicha pasarela (54).

8. Conjunto que forma el terminal (31; 60) adaptado específicamente al sistema según cualquiera de las reivindicaciones 1 a 7, en el que el conjunto comprende una pasarela del tipo red-dispositivo comunicante (54) adaptada para recibir y procesar indiferentemente los mensajes de una aplicación cliente con formato de la red suministrados por conexión interna (LL') o por red (R).

9. Método para establecer un canal de comunicación en una conexión (R; LL') que conecta, por un lado, una aplicación cliente (10) en una máquina cliente (30) y, por otro lado, una aplicación de servicio (12), estando presente la aplicación de servicio en un dispositivo comunicante (2), estando conectado el dispositivo comunicante a un terminal (31),

caracterizado porque el método comprende:

- una etapa de representación (50) de la aplicación de servicio realizada a nivel de la máquina cliente (30), emitir comandos de formateado a partir de los mensajes de la aplicación cliente,

5 - un etapa de formateado (16') realizada a nivel de la máquina cliente (30), en dicho representante (50), para formatear los mensajes de la aplicación cliente en una forma (intercambio (Msg tarjeta)) comprensible para la aplicación servicio (12), y

10 - la formación de una pasarela (54) en el terminal (31) para recibir dichos mensajes comprensibles por el dispositivo comunicante y transmitir dichos mensajes comprensibles por el dispositivo comunicante a la aplicación de servicio (12).

10. Método según la reivindicación 9, en el que el método se implementa con un dispositivo comunicante del tipo tarjeta de chip (2), siendo la aplicación de servicio una aplicación tarjeta (12).

11. Método según la reivindicación 9 ó 10, en el que el método comprende, además, una etapa de cifrado de los mensajes, o antes de la etapa de formateado (16'), a fin de permitir transitar a los mensajes cifrados provenientes del módulo de formateado, en forma cifrada, a través de la pasarela (54) y hasta el dispositivo comunicante (29).

12. Método según una cualquiera de las reivindicaciones 9 a 11, en el que la máquina cliente (30) conectada al terminal (31) por una red (R), la etapa de formateo (16') irá seguida, en la máquina cliente (30), sucesivamente de las etapas:

25 - representación (52) de dicha pasarela (54), para recibir comandos de formateado (intercambio (Msg tarjeta)) del módulo de formateado (16') y producir en respuesta comandos de formateado de estos comandos en un formato comprensible por dicha pasarela (54);

30 - formateado de los mensajes provenientes de dicha representación (52) de la pasarela (54) en mensajes (intercambio Msg Red) en formato de red; y

35 - adaptación (40) de dichos mensajes (intercambio MSG Red) a los estándares de la red (R);

y en el que los mensajes recibidos de la red (R) en el terminal (31) se procesan sucesivamente por las etapas de:

40 - recuperación (42) de los citados mensajes (intercambio Msg Red) a partir de los mensajes provenientes de la red;

45 - recuperación (44) de los comandos como los provenientes del representante (52) de dicha pasarela (54); y

- control de los comandos de red (46) para transmitir los mensajes (intercambio Msg tarjeta) provenientes del módulo anterior (44) hacia dicha pasarela (54).

13. Método según una cualquiera de las reivindicaciones 9 a 12, en el que:

50

- la etapa de formateado (16') va seguida directamente por una etapa de empaquetado (40) de dichos mensajes (intercambio Msg tarjeta) comprensibles por el dispositivo comunicante, los mensajes resultantes de una etapa de empaquetado estando así empaquetados, para transportar dichos mensajes comprensibles por el dispositivo comunicante a través de la red (R);

5 y en el que dichos mensajes empaquetados son desempaquetados en el curso de una etapa de desempaquetado (42) en el terminal (31) para recuperar dichos mensajes (intercambio Msg tarjeta) provenientes de la etapa formateado y retransmitir
10 directamente a dicha pasarela (54) dichos mensajes comprensibles por el dispositivo comunicante.

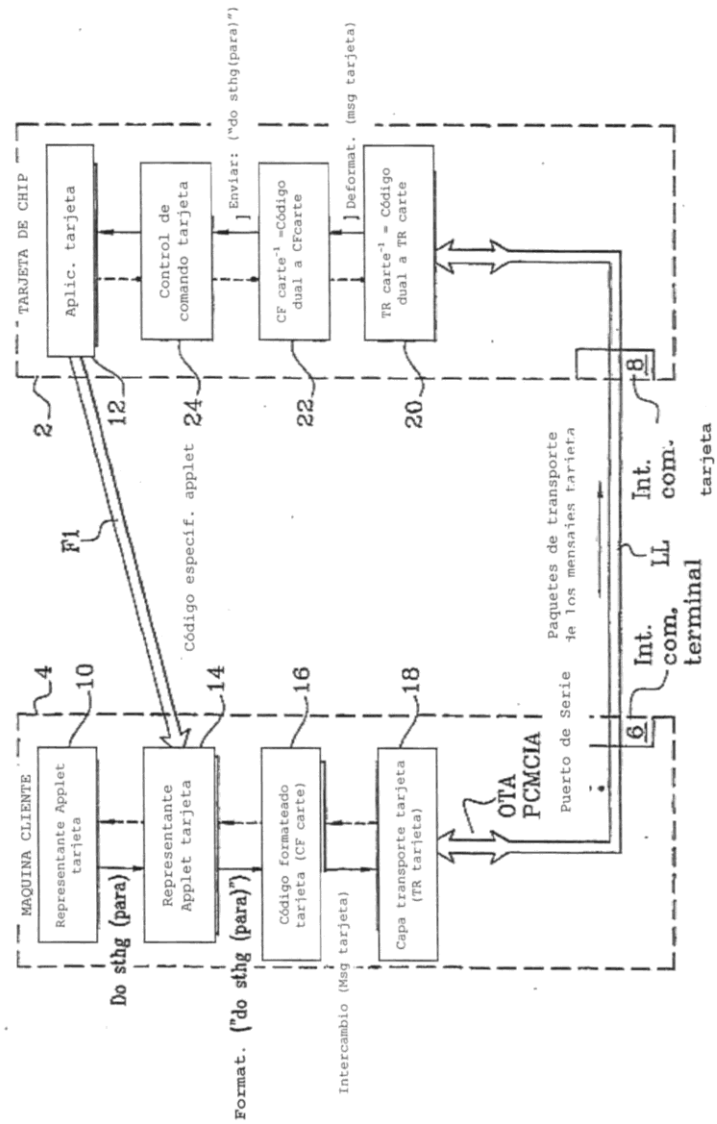


Fig. 1

ARTE ANTERIOR

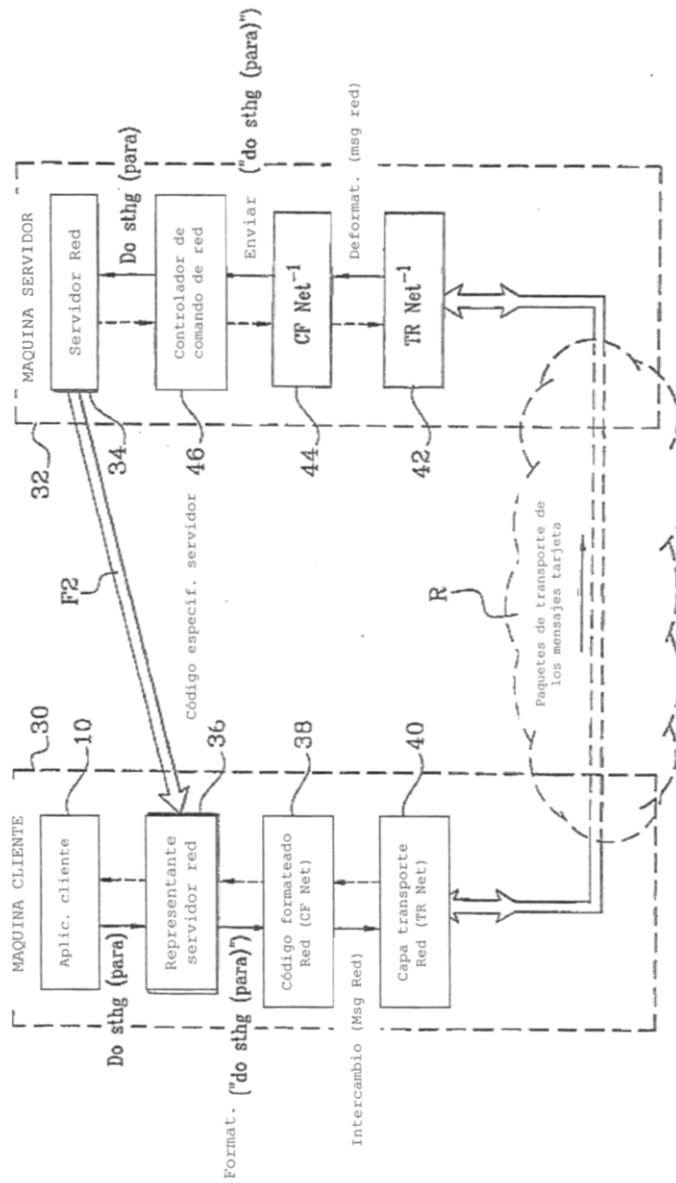


Fig. 2

ARTE ANTERIOR

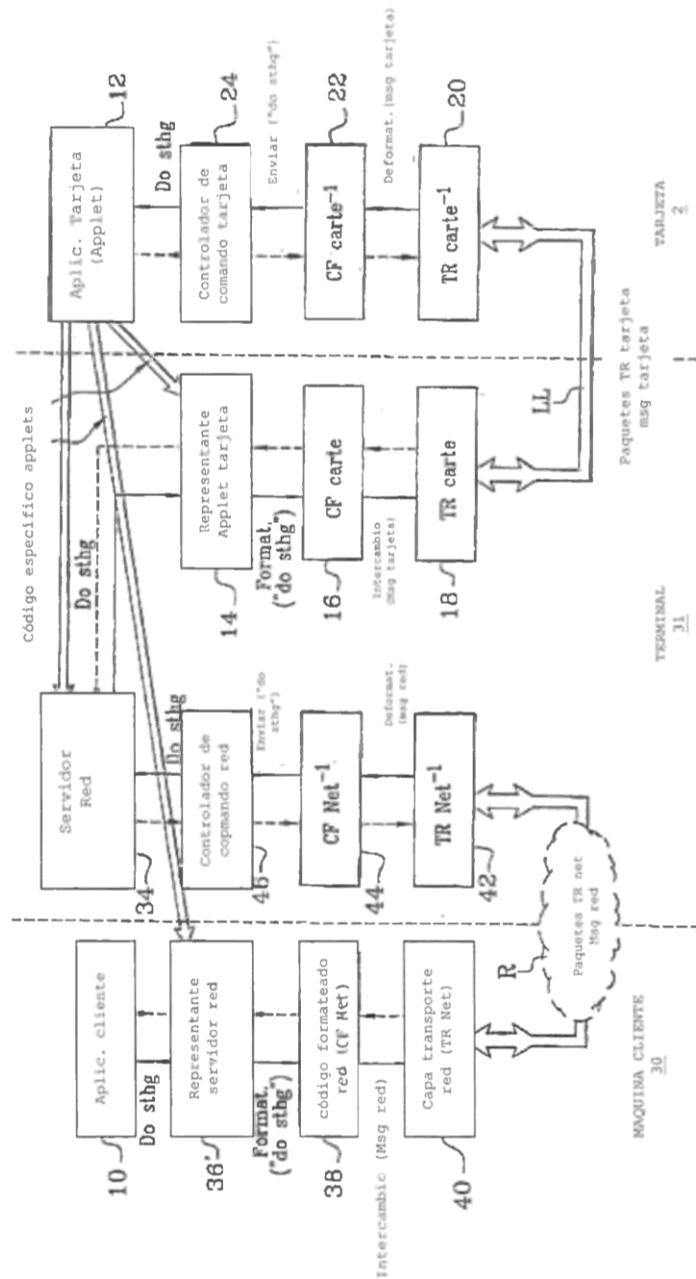
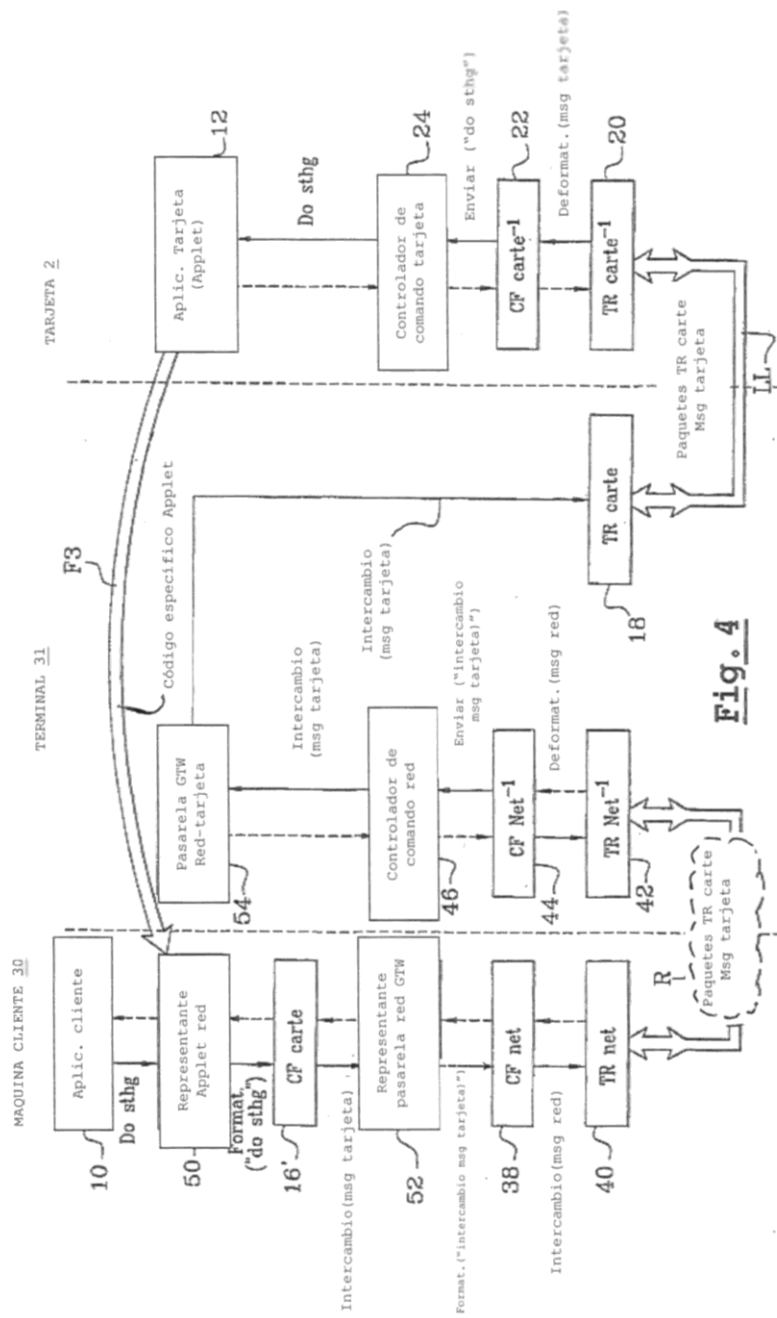
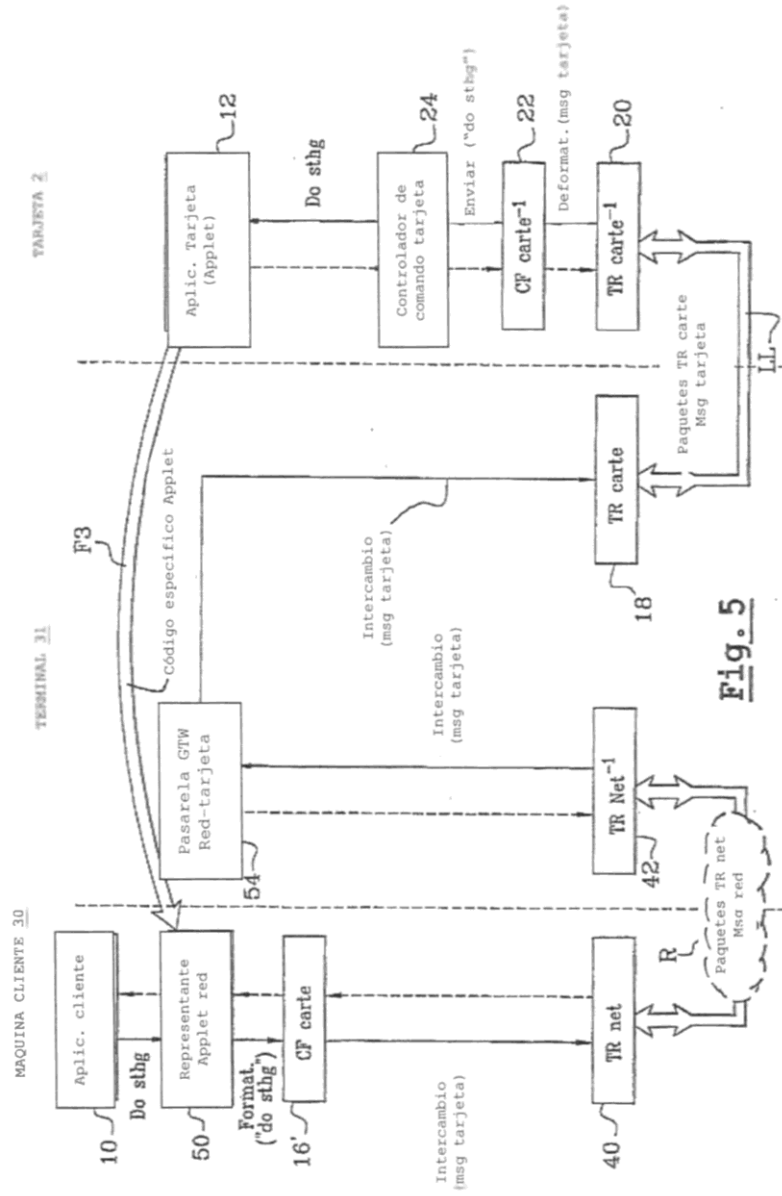


Fig. 3





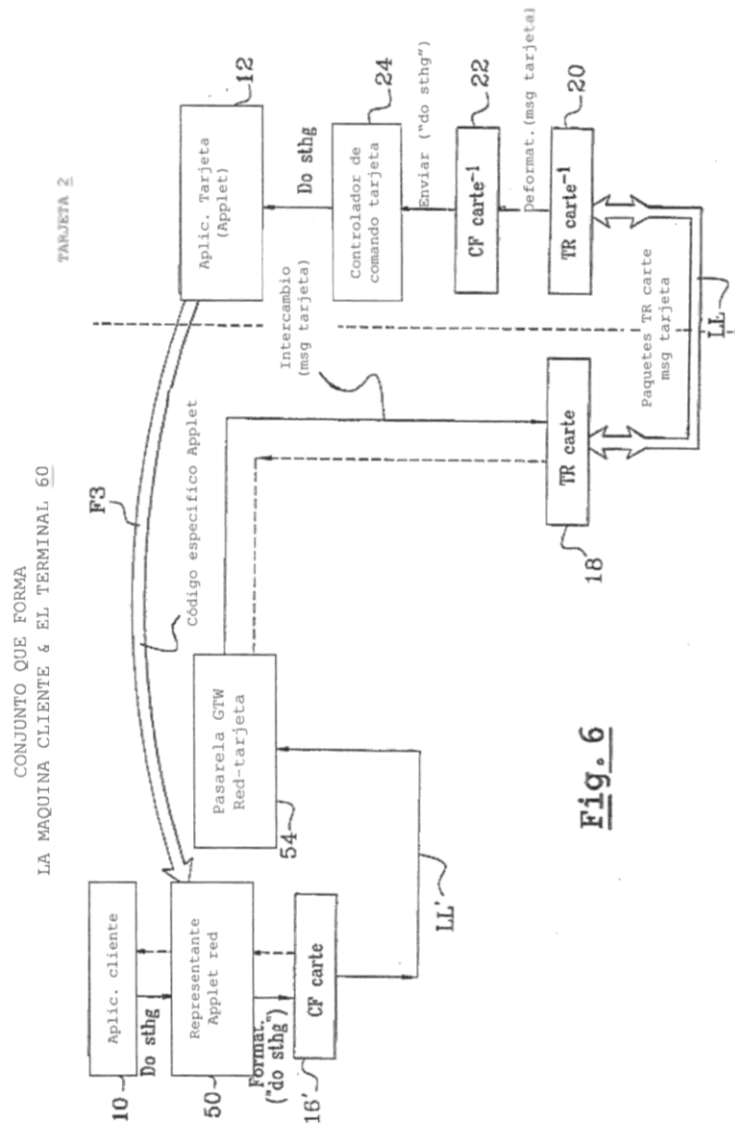


Fig. 6