(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 698 219**

(51) Int. CI.:

H04W 12/06 (2009.01)
G06Q 20/32 (2012.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **11.06.2013 PCT/FR2013/051352**

(87) Fecha y número de publicación internacional: **03.01.2014 WO14001677**

(96) Fecha de presentación y número de la solicitud europea: **11.06.2013 E 13734134 (3)**

(97) Fecha y número de publicación de la concesión europea: **08.08.2018 EP 2867837**

(54) Título: **Sistema de transmisión segura de datos digitales**

(30) Prioridad:

29.06.2012 FR 1256217
05.06.2013 FR 1355175

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
01.02.2019

(73) Titular/es:

NEPTING (100.0%)
18 rue Auguste Comte
34000 Montpellier, FR

(72) Inventor/es:

AUBRY-TRIAL, MARTINE;
COTTE, JEAN-FRANÇOIS;
DALMAS, JEAN-PAUL y
RENAULT, FRÉDÉRIC

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Sistema de transmisión segura de datos digitales

La presente invención entra en el campo de la comunicación, en particular, de la transmisión segura de datos digitales a través de una red de comunicación.

La invención se refiere, de este modo, a un sistema de transmisión segura de datos digitales a través de una red de comunicación.

La invención encontrará una aplicación preferiblemente, pero de ninguna manera limitante, en el marco de intercambios transaccionales, en particular, de transacciones bancarias.

La reciente expansión de terminales portátiles y personales, como los teléfonos celulares de tipo “Smartphone” (para teléfono inteligente), conectados a una red de comunicación, en particular informática, tal como Internet, ha dado lugar a una evolución en las prácticas en materia de pago por medio de una tarjeta bancaria.

Recordemos que actualmente, se ha recurrido al estándar adoptado internacionalmente para las tarjetas bancarias con chip: la EMV para “EUROPAY MASTERCARD VISA”. Esta estándar específica el formato de los datos bancarios almacenados e intercambiados, el procesamiento asociado y las restricciones para los elementos de pago que almacenan tales datos, ya sea una tarjeta con chip o bien un elemento de memoria segura de un teléfono celular.

En paralelo, la llegada de las tecnologías de comunicación inalámbrica ha permitido implementar protocolos de transmisión de datos entre una tarjeta bancaria con chip o un terminal portátil personal, tal como un teléfono celular, propio de un usuario y un terminal de pago en poder de un comerciante, en el momento de una transacción bancaria, situado en un punto de venta.

Un ejemplo de protocolo utilizado actualmente es la NFC para “Near Field Communication” (comunicación de campo cercano). Esta tecnología recurre a la tecnología de identificación por radio RFID (para “Identificación por Radiofrecuencia”) y permite el envío y la recepción de datos de corto alcance, de alrededor de una decena de centímetros, emitidos en forma de ondas de alta frecuencia, en particular 13,56 Megahertzios (MHz).

Una tecnología tal ya se utiliza con tarjetas bancarias con chip específicas, que autorizan el pago sin contacto (“contactless”), por medio de un TPE para “Terminal de Pago Electrónico” equipado con una antena RFID. En lugar de insertar la tarjeta en el lector del TPE, es suficiente colocarla cerca, dentro del campo emitido por la antena de dicho terminal, para que este último la detecte y realice los intercambios con ella, a fin de efectuar los procesamientos necesarios. Sin embargo, esta práctica impone una restricción a la realización de intercambios con la tarjeta, que se debe operar en una duración corta (inferior al segundo), a fin de asegurar completamente la transacción con un solo y simple gesto del usuario, comúnmente conocido como “golpecito”.

Dado que los terminales portátiles personales conectados a una red de comunicación están equipados con una tarjeta con chip, de tipo UICC (para “Tarjeta Universal de Circuito Integrado”), preferiblemente del tipo SIM (para “Módulo de identidad de Abonado”), se ha pensado utilizar esta tarjeta con chip, considerada como un elemento de memoria incorporada extraíble y segura, para introducir los datos EMV, que están presentes dentro del chip de una tarjeta bancaria. De este modo, un teléfono móvil NFC sustituye la tarjeta bancaria con chip y se puede utilizar de la misma forma en un “golpecito”. El documento EP 1 965 596 describe un ejemplo de un terminal portátil equipado con una tarjeta con chip de tipo SIM que comprende datos EMV. La presente invención se basa en el contexto anterior y la adapta a las transacciones bancarias efectuadas durante un pago en línea, en el marco del comercio electrónico (“e-commerce”) o del comercio móvil (“m-commerce”). Estos tipos de comercio se efectúan a través de una red informática, en particular, Internet, a la que está conectado el terminal personal de un usuario.

Más específicamente, un comerciante hace accesible a través de dicha red, un portal de venta de productos y de servicios. Un portal tal está alojado en un servidor remoto y conectado a dicha red. Incluye, de este modo, una interfaz bancaria que permite a un usuario pagar los productos y servicios solicitados a través de este portal, en particular, a través de la entrada de informaciones concernientes a su tarjeta bancaria. Una interfaz bancaria tal pone en relación el servidor de dicho portal con uno o más servidores bancarios, en particular el servidor bancario del comerciante y el del usuario. Esta interfaz permite realizar, por lo tanto, la transacción bancaria entre el comerciante y el usuario.

Actualmente, las interfaces existentes establecen etapas tediosas para intentar autenticar de una manera sólida al usuario, con el fin de protegerse contra una utilización fraudulenta de una tarjeta bancaria. Estas soluciones hacen que sea difícil autenticar al usuario de una manera sólida, a diferencia de la utilización de una tarjeta bancaria con chip al introducir un código PIN, usando el principio de “algo que se tiene con algo que se sabe”, esto es, recíprocamente dicha tarjeta bancaria y dicho código PIN asociado. En otras palabras, para un pago en Internet, los bancos ofrecen al usuario obtener informaciones adicionales por diferentes vías de comunicación, dichas informaciones que deben ser introducidas a fin de asegurar que la persona que utiliza los datos bancarios de la tarjeta es su propietario. Tales informaciones adicionales son difícilmente memorizables, incluso subiendo un código único transmitido únicamente al propietario para cada transacción.

Además, dado que los datos bancarios introducidos y transmitidos en Internet se pueden desviar, incluso en el caso de una transmisión cifrada, no es factible solicitar al usuario la introducción de un código de identificación secreto, conocido por él sólo y más fácilmente memorizable. De hecho, este código entonces podría ser interceptado y desviado con dichos datos bancarios.

La presente invención tiene por objetivo superar los inconvenientes del estado de la técnica, proponiendo un sistema de transmisión segura de datos digitales a través de una red de comunicación. Un sistema tal es capaz de aprovechar las transacciones bancarias realizadas en el sitio por medio de un TPE, evitando este último, y aplicándolo a las transacciones bancarias realizadas a través de un acceso a un portal alojado en un servidor remoto.

En otras palabras, y preferiblemente, la invención proporciona la creación de una arquitectura que incorpora la eficiencia y la seguridad del pago con un TPE físico, aplicándolo al pago en Internet a través de un teléfono inteligente que lleva un elemento de memoria segura, tal como una tarjeta SIM bancaria.

Para hacer esto, dicho sistema que proporciona una arquitectura específica, es equivalente a un terminal de pago físico. Esta arquitectura se distribuye al menos entre un servidor y el terminal personal del usuario en el que se realiza el acto de compra, tal como un teléfono celular, una tableta táctil, un ordenador personal o similar.

En particular, una arquitectura tal presenta una parte de software que comprende, por una parte, una interfaz de software local instalada y que se ejecuta en dicho terminal personal para acceder a los datos personales de pago y, por otra parte, en el lado del servidor, un módulo de comunicación con dicha interfaz y de gestión de dichos datos personales de pago, así como un módulo de aplicación de pago unido a al menos un servidor bancario remoto.

De este modo, dicho sistema de transmisión segura de datos digitales opera entre un servidor y un terminal personal a través de una red de comunicación, dicho sistema que comprende:

- dicho servidor provisto de un módulo de comunicación con dicho terminal y de un módulo de aplicación bancaria almacenado y ejecutado en dicho servidor; y

- dicho terminal personal provisto de medios de conexión a dicha red y a dicho módulo de comunicación;

- dicho terminal que comprende también datos personales de pago almacenados dentro de un elemento de memoria segura y al menos un canal de acceso autenticado a dichos datos.

Un sistema tal se caracteriza por el hecho de que:

- dicho terminal comprende una interfaz almacenada y que se ejecuta en dicho terminal;

- dicha interfaz que está conectada a través de dichos medios de conexión al módulo de aplicación bancaria de dicho servidor a través de dicho módulo de comunicación;

y por el hecho de que:

- dicha interfaz consiste en un encaminador de acceso a dichos datos a través de dicho canal de acceso seguro y de autenticación de dicho módulo de aplicación bancaria.

Un punto esencial de una arquitectura tal reside en el papel de encaminador de la interfaz de software local entre el servidor remoto y los datos personales de pago, almacenados en el elemento de memoria segura, esto es, la tarjeta SIM EMV del teléfono inteligente.

El encaminador gestiona la comunicación con el elemento de memoria segura a través de los canales, existentes y disponibles, de acceso a los datos personales de pago. Estos canales que provienen en particular de una interfaz sin contacto de tipo NFC, o bien una interfaz de contacto, esto es, una aplicación de software que permite dialogar directamente con el elemento de memoria segura cuando está integrado en el terminal personal que aloja dicho encaminador.

Además, según otras características adicionales, dicha interfaz puede ser un software que comprende una capa de comunicación de bajo nivel que tiene una función de tipo encaminador que permite la comunicación de dicha interfaz con el elemento de memoria segura que contiene los datos personales de pago a través de dicho canal de acceso.

Según una realización particular, dicho terminal puede comprender medios de comunicación sin contacto en forma de un controlador NFC, estando dicho canal de acceso conectado a dicho controlador NFC en un punto de conexión, y por el hecho de que dicha interfaz comprende medios de conexión a dicho punto de conexión y de cortocircuito de dicho controlador NFC.

Preferiblemente, dicho canal de acceso puede conectar una aplicación bancaria a dichos datos y por el hecho de que dicha interfaz accede a dicho canal a través de una conexión a dicha aplicación bancaria.

En particular, dicho canal de acceso puede conectar una aplicación bancaria a dichos datos y por el hecho de que dicha interfaz comprende medios de conexión a dicho canal mediante un punto de conexión y de cortocircuito de dicha aplicación bancaria.

Además, dicho módulo de comunicación se puede conectar a dicha interfaz a través de dicha red por medio de un protocolo propietario que encapsula los datos necesarios para intercambios normalizados, del tipo ISO 7816-4, con dichos datos personales de pago

Además, durante una transacción, dichos módulos y la interfaz pueden ser conectados entre sí de manera para simular un terminal de pago a petición a través de dicha red.

Por otra parte, dicho servidor puede comprender el conjunto de parámetros relativos a los comerciantes almacenados dentro de dicho módulo de aplicación bancaria.

Según una característica adicional, el terminal de pago simulado se configura para un comerciante dado para cada transacción.

Otras características y ventajas de la invención surgirán de la descripción detallada que sigue de las realizaciones no limitativas de la invención, con referencia a las figuras anexas, en las que:

- la figura 1 representa una vista esquemática de una primera realización de la arquitectura de dicho sistema, en la que la interfaz accede al canal de comunicación entre la aplicación bancaria y los datos personales;

- la figura 2 representa una vista esquemática de una segunda realización de la arquitectura, en la que la interfaz accede a los datos a través de dicha aplicación bancaria; y

- la figura 3 representa una vista esquemática de una tercera realización de la arquitectura, en la que la interfaz utiliza un punto de acceso al canal de conexión entre los datos y un controlador sin contacto, para cortocircuitar esta conexión.

La presente invención se refiere a un sistema 1 de transmisión segura de datos digitales a través de una red de comunicación 2, más particularmente, una red de telecomunicación. También puede consistir, al menos en parte, en una red informática, preferiblemente Internet, y al menos en parte, en una red de telecomunicación telefónica, preferiblemente de telecomunicación móvil.

Además, dicho sistema 1 efectúa una transmisión de datos entre un servidor 4 y un terminal personal 3 a través de dicha red 2 de comunicación.

Dicho sistema 1 comprende una arquitectura distribuida entre un terminal personal 3 de un usuario y un servidor remoto 4, estos dos elementos que están conectados a través de dicha red 2.

Además, dicho terminal personal 3 puede ser provisto portátil, como un teléfono celular, de tipo “Smartphone”, pero también una tableta táctil, un asistente electrónico personal PDA (para “Asistente Personal Digital”), incluso otros tipos de terminales como, por ejemplo, un ordenador portátil o fijo o una televisión conectada a Internet.

Además, dicho terminal personal 3 está provisto de medios 30 de conexión a dicha red 2.

Tan pronto como se implementan las capas TCP IP (para “Protocolo de Control de Transmisión” y “Protocolo de Internet”, dicha red 2 también puede consistir en parte de al menos una red de telecomunicación telefónica inalámbrica de tipo hertziana o analógica, en particular para la comunicación móvil a través de un teléfono celular.

Además, en la aplicación preferencial de intercambios transaccionales, el terminal personal 3 integra los datos personales de pago 5 almacenados dentro de un elemento de memoria segura 10 y al menos un canal 100 de acceso autenticado a dichos datos 5. Se observará que dicho elemento de memoria segura puede ser, por ejemplo, una tarjeta SIM 10.

Según el modo preferencial de realización, dichos datos 5 están normalizados y son de tipo bancarios, preferiblemente del formato EMV, dichos “datos EMV” (para “EurocardMasterCardVisa”), o bien formalizados bajo otra norma, en particular una norma bancaria. En resumen, en el caso de un terminal 3 bajo la forma de un teléfono celular, los datos bancarios se almacenan dentro de un espacio de memoria dedicada, por ejemplo, su tarjeta SIM.

Además, dicho servidor remoto 4 se puede conectar, a través de dicha red 2 o bien de una red conexa, a servidores bancarios 6 distintos para la gestión de autorización de pago y o la entrega de la transacción.

Ventajosamente, dicha arquitectura según la invención comprende, por una parte, una interfaz de software local 7, instalada y que se ejecuta en dicho terminal 3, para acceder a los datos personales de pago 5 almacenados en el elemento de memoria segura contenido dentro de este terminal personal 3.

Por otra parte, del lado del servidor 4, la arquitectura comprende un módulo de comunicación 8 con dicha interfaz 7 y de gestión de dichos datos 5, así como un módulo de aplicación bancaria 9. Estos módulos se almacenan y ejecutan en dicho servidor 4. Como se ha mencionado anteriormente, este último se puede conectar al menos a uno de dichos servidores bancarios distantes 6 a través de dicho módulo 9. Además, dicho terminal personal 3 está provisto de medios 30 de conexión a dicha red 2 y a dicho módulo de comunicación 8. En resumen, dicha interfaz 7 está conectada a través de dichos medios de conexión 30 al módulo de aplicación bancaria 9 de dicho servidor 4 a través de dicho módulo de comunicación 8.

En resumen, una característica esencial de la presente invención reside en la separación de un único conjunto, contenido actualmente en un terminal de pago físico, en dos partes distintas del lado del cliente por dicha interfaz 7 y del lado del servidor 4 con los módulos 8 y 9, estando dichas partes fuertemente unidas entre ellas a través de la red 2. Este conjunto, durante la transacción, constituye un terminal de pago electrónico virtual y de forma temporal. Más específicamente, la invención es capaz de simular un terminal de pago electrónico, que utiliza estas herramientas físicas y software para simular un terminal tal.

Además, el funcionamiento de cada una de las partes cliente y servidor partes se efectúa de manera diferente. De hecho, dicha interfaz 7 es un software “ligero”, esto es, que comprende una capa de comunicación de bajo nivel que tiene una función de tipo encaminador. Este último permite la comunicación de dicha interfaz 7 directamente con los datos 5 almacenados dentro de dicho terminal de datos 3, a través de dicho canal de acceso seguro 100.

Más específicamente, el software de dicha interfaz 7 está programado a nivel de hardware fuera de la capa de aplicaciones, esto es, que opera a nivel de al menos una de las siguientes capas: transporte, sesión o presentación (según el modelo OSI para “Open Systems Interconnection” o “Interconexión de Sistemas Abiertos”). Este software que actúa como convertidor de protocolo entre los intercambios con el servidor 4 y los intercambios con los datos 5, que sigue un protocolo normalizado de encapsulación de datos durante su intercambio, en particular, el protocolo ISO7816-4.

Por lo tanto, dicha interfaz 7 consiste en un encaminador de acceso a dichos datos 5 a través de dicho canal 100 de acceso seguro y de autenticación de dicho módulo de aplicación bancaria 9.

En resumen, la función de tipo encaminador de la interfaz 7 consiste en un procesamiento de conversión de los datos recibidos desde el módulo de comunicación 8 al elemento de memoria segura, el tipo de tarjeta SIM y viceversa. Esta conversión permite transcribir los datos recibidos y enviados a los diferentes formatos y los encapsula en paquetes que siguen los protocolos respectivos utilizados.

Ventajosamente, de forma global, esta interfaz 7 está programada a nivel de hardware con el fin de comunicarse con los datos almacenados 5 en el elemento de memoria segura 10, a través del canal de acceso 100. En particular, dicha interfaz 7 comprende medios de autenticación que permiten acceder directamente a dichos datos 5.

Se observará que esta autenticación puede estar sometida a protocolos y claves de acceso dedicados y específicos a cada uno de los datos 5, en particular, protocolos y claves bancarias. Estos protocolos y parámetros de autenticación bancaria son preferiblemente dedicados al formato EMV de los datos 5.

Según una primera realización, representada en la figura 1, dicho terminal 3 comprende una aplicación bancaria 15, instalada y ejecutada localmente dentro de la memoria interna 14 del terminal 3. Dicha aplicación 15 está conectada por dicho canal de acceso 100 a dichos datos 5. En resumen, es esta aplicación bancaria 15 la que contiene los protocolos y las claves de autenticación que permiten al usuario ser autenticado y acceder a los datos 5.

En otras palabras, dicha aplicación bancaria 15 está dedicada al formato de datos bancarios 5 almacenados dentro del elemento seguro 10. De hecho, durante la instalación de dichos datos 5 dentro de una tarjeta SIM 10, es el banco del usuario, quien personaliza dicha tarjeta SIM 10. Entonces se configura para aceptar solo la interacción con una aplicación bancaria 15 específica para dicho banco.

En particular, en el caso de los datos 5 en el formato del estándar EMV, la aplicación bancaria 15 se comprende una API UICC (para “Interfaz de Programación de Aplicaciones”) que permite comunicarse con el microcontrolador de acceso a la memoria de la tarjeta con chip que almacena los datos 5, en particular, el espacio seguro que encierra estos datos bancarios 5.

Un ejemplo de un estándar existente ha sido detallado en las especificaciones AEPM (de “Asociación Europea de Pago Móvil”), que utiliza, en particular, el lenguaje informático Java y una máquina virtual Java (JVM para “Máquina Virtual Java”) en un entorno. JCRE (para “Entorno de Ejecución de Tarjeta de Java”).

Ventajosamente, la interfaz 7 accede directamente, a nivel de hardware, a dicho canal 100, en particular, a nivel de un punto de unión 51.

En este caso, la interfaz 7 permite recuperar las informaciones intercambiadas con la aplicación 15, para su uso directamente con los datos bancarios 5.

Una segunda realización, representada en la figura 2, es similar a la anterior, en que es la aplicación bancaria 15 la que accede a los datos 5 por el canal 100.

La diferencia reside en el hecho de que, en esta configuración, dicha interfaz 7, programada a nivel de hardware, accede a dicho canal 100 a través de una conexión 16 a dicha aplicación bancaria 15. La conexión 16 de la interfaz 7, programada a nivel de hardware como se ha mencionado anteriormente, consiste entonces en una interfaz de software, de nivel más alto en la capa de aplicaciones, a fin de permitir comunicar con la aplicación 15. Esta última, por lo tanto, actúa como pasarela para que la interfaz 7 acceda a los datos 5.

Además, en esta realización, se implementa un método de autenticación adicional entre la aplicación bancaria 15 y el encaminador 7. Un método tal también puede ser común al método de identificación del usuario, ya existente, para acceder a dicha aplicación bancaria 15.

Según otra realización particular, visible en la figura 3, dicho terminal 3 comprende medios de comunicación sin contacto, en forma de un controlador NFC 13. Dicho canal de acceso 100 se conecta entonces a dicho controlador NFC en un punto de conexión 51.

Se observará que, según una realización específica, con la misma configuración, una aplicación bancaria 15 también se puede conectar a dichos datos 5.

Por lo tanto, la interfaz 7 comprende medios de conexión a dicho punto de conexión 51 y de cortocircuito de dicho controlador NFC.

En otras palabras, cuando la interfaz 7 se comunica con el controlador NFC 13, éste permite simular un terminal de pago, en lugar de un terminal de pago físico utilizado normalmente para efectuar un pago sin contacto. De este modo, el controlador NFC 13 cree estar en presencia de un terminal de pago y solicita acceso a los datos 5.

Para hacer esto, los medios de cortocircuito se conectan al punto de conexión 51 del controlador NFC, para desviar y utilizar su transmisión existente al elemento seguro 10 y los datos que contiene. De este modo, la interfaz 7 no requiere, de este modo, claves de autenticación.

Se observará que la interfaz 7 integra únicamente los protocolos y los parámetros de intercambio, permitiendo que la interfaz 7 se conecte a dicho punto 51 y se comunique a través del controlador NFC 13. Más específicamente, la interfaz 7 se comunica con el controlador NFC 13 para simular un terminal de pago virtual, en lugar de un terminal de pago físico utilizado normalmente para efectuar un pago sin contacto.

De este modo, el controlador NFC 13 cree estar en presencia de un terminal de pago físico y solicita acceso a los datos 5. Por lo tanto, la interfaz 7 cortocircuita el envío de los datos por dicho controlador NFC 13 a un terminal de pago físico inexistente, para recuperarlos y utilizarlos a través de otra red de comunicación 2, en particular, Internet.

Además, incluye los protocolos de intercambio utilizados usualmente entre dicho controlador NFC 13 y un terminal de pago físico, de modo que el controlador NFC 13 cree estar en presencia de un terminal físico tal.

Más específicamente, según una realización particular, la interfaz 7 posee un módulo de software para conmutar intercambios entre los datos 5 y el controlador NFC 13, en particular, su antena RFID. Este módulo de conmutación es preferiblemente del tipo “controlador de conmutador”, permitiendo reencaminar estos intercambios a la interfaz 7 en lugar del controlador NFC 13 y su antena RFID.

Por otra parte, la comunicación entre la interfaz 7 y el servidor 4 se efectúa a partir de dicho módulo de comunicación 8 por medio de un protocolo de intercambio para permitir el acceso a los datos 5 a través de la red 2 y los medios de conexión a través de dicha interfaz 7. Un protocolo tal asegura una conexión segura a través de la red 2 entre la interfaz 7 y el módulo 8, con cifrado de datos y autenticación del servidor 4, en particular, por medio de protocolos seguros de comunicación, como por ejemplo SSL para “Capa de Conexión Segura” o TLS para “Seguridad de Capa de Transporte”, o bien HTTPS para “Protocolo de Transferencia Hipertexto Seguro”.

Por otra parte, dicho módulo de comunicación 8 que se ejecuta en el servidor 4 está dedicado a la gestión de datos personales de pago. Se trata de una aplicación de software que gestiona los intercambios con el elemento seguro que contiene los datos 5 para realizar las diferentes fases de una transacción, esto es, de forma no exhaustiva: selección de aplicación, tarjeta de autenticación, autenticación de portador si es necesario, generación del certificado o de los certificados.

Además, dicho módulo 8 comunica las informaciones a partir de los datos 5 al módulo de aplicación bancaria 9 y necesarias para adquirir y transmitir procesamientos de control bancario. Estas informaciones se transmiten desde el módulo 8 al módulo 9 y viceversa para compartir un objeto de memoria del servidor 4. De hecho, este módulo de aplicación bancaria 9 asegura el procesamiento de los datos 5 presentes en la tarjeta SIM 10 y la conexión con uno de los servidores bancarios remotos 6.

Se observará que los parámetros y los datos bancarios del comerciante se almacenan en el servidor 4, a nivel de dicho módulo bancario 9, configurados específicamente para cada comerciante.

Ventajosamente, en cada transacción y únicamente durante su duración, los parámetros de dicho comerciante se activan y transmiten desde dicho módulo de aplicación bancaria 9 a dicha interfaz 7. En resumen, la arquitectura según la invención reagrupa y conecta, en el momento de efectuar una transacción bancaria, la interfaz 7 a nivel del cliente, el módulo 8 y el módulo de aplicación bancaria 9 a nivel del servidor 4, permitiendo simular provisionalmente un TPE, que se asimila como un terminal de pago físico real. Una vez que se finaliza la transacción, la interfaz 7 no conserva ninguno de los parámetros relativos al comerciante, no almacenando datos sensibles a nivel de dicho terminal 3.

Según las realizaciones, representadas en las figuras, la interfaz 7 está instalada directamente dentro de dicho terminal 3, en su memoria interna 14, y se ejecuta localmente en este último. En el lado del servidor 4, los módulos 8 y 9 aseguran sus papeles respectivos.

En el marco de un acto de compra realizado en el terminal 3, la selección de la función de pago activa el encaminador 7 y su comunicación por una parte con el servidor 4 y por otra parte con el elemento seguro que contiene los datos 5. El control del código confidencial, cuando se requiere, se gestiona por la aplicación del transmisor bancario instalado en el terminal 3, que soporta en particular la interfaz de usuario para su entrada. El estado de la verificación del código confidencial es una información almacenada en los datos 5. Después de los controles y autorizaciones necesarias, un estado que concierne a la transacción se devuelve a la aplicación de ventas del origen del pago que informa al usuario de la aceptación o no del pago.

Por otra parte, para una arquitectura dada, la interfaz 7 se puede integrar dentro de una aplicación dedicada de un comerciante o de un banco. Por lo tanto, se instala y ejecuta únicamente dentro de esta aplicación móvil, banco o comerciante, como por ejemplo dentro de la aplicación bancaria 15.

Para otra arquitectura, dicha interfaz 7 es una aplicación independiente, descargada desde el servidor 4 e instalada durante la primera transacción o cada transacción.

De este modo, la presente invención integra, dentro de un terminal personal 3, en particular, del tipo de teléfono celular, una interfaz 7 que permite acceder directamente a los datos 5 almacenados en un elemento de memoria segura, en particular, en la tarjeta SIM 10, desde un servidor 4 en el que se ejecuta un módulo de comunicación 8 y un módulo bancario 9, el conjunto de estos tres elementos que forma, en el momento de una transacción, un terminal de pago electrónico virtual.

REIVINDICACIONES

1. Un sistema de transmisión segura de datos digitales (1) adaptado para permitir una transmisión segura entre un terminal (3) personal y un servidor bancario (6), el terminal (3) que comprende un elemento de memoria segura (10), caracterizado por que el sistema de transmisión seguro de datos digitales (1) comprende una arquitectura distribuida entre el terminal (3) y un servidor remoto (4) que está conectado al terminal (3) por una primera red de comunicación (2), el servidor remoto (4) que está adaptado para ser conectado al servidor bancario (6) por una segunda red de comunicación, el servidor remoto (4) que comprende, por una parte, un módulo de comunicación (8) que permite su conexión a la primera red de comunicación (2) y, por otra parte, un módulo de aplicación bancaria (9) conectado al módulo de comunicación (8) y adaptado para ser conectado al servidor bancario (6), el módulo de comunicación (8) y el módulo de aplicación bancaria (9) que se almacenan y ejecutan en el servidor remoto (4), el elemento de memoria segura (10) que comprende datos personales de pago (5), el terminal (3) que comprende medios de conexión (30) que permiten su conexión a la primera red de comunicación (2) y un canal de acceso seguro autenticado (100) que permite el acceso a los datos personales de pago (5), una interfaz (7), almacenados y que se ejecutan en el terminal (3), estando conectado al canal de acceso seguro autenticado (100) y a los medios de conexión (30) de manera que forme un encaminador de acceso a los datos personales de pago (5) y de autenticación del módulo de aplicación bancaria (9), de modo que la arquitectura reagrupe y se conecte temporalmente, durante una operación de pago, al módulo de comunicación (8), al módulo de aplicación bancaria (9) y a la interfaz (7), que simulan de este modo un terminal de pago electrónico.

2. El sistema (1) según la reivindicación 1, caracterizado por que la interfaz (7) es un software que comprende una capa de comunicación de bajo nivel.

3. El sistema (1) según una de las reivindicaciones 1 o 2, caracterizado por que el terminal (3) comprende medios de comunicación sin contacto que están en forma de un controlador NFC (13) y que están conectados al canal de acceso seguro autenticado (100) en un punto de conexión (51), la interfaz (7) que comprende medios de conexión al punto de conexión (51) y de cortocircuito del controlador NFC (13).

4. El sistema (1) según una de las reivindicaciones 1 o 2, caracterizado por que el terminal (3) comprende una aplicación bancaria (15) que está conectada a los datos personales de pago (5) por el canal de acceso seguro autenticado (100), la interfaz (7) que accede al canal de acceso seguro autenticado (100) por una conexión (16) que lo conecta a la aplicación bancaria (15).

5. El sistema (1) según una de las reivindicaciones 1 o 2, caracterizado por que el terminal (3) comprende una aplicación bancaria (15) que está conectada a los datos personales de pago (5) por el canal de acceso seguro autenticado (100), la interfaz (7) que comprende medios de conexión al canal de acceso seguro autenticado (100) por un punto de conexión (51) y de cortocircuito de la aplicación bancaria (15).

6. El sistema (1) según una de las reivindicaciones 1 a 5, caracterizado por que el módulo de comunicación (8) está conectado a la interfaz (7) por medio de un protocolo propietario que encapsula los datos necesarios para los intercambios normalizados con los datos personales de pago (5).

7. El sistema (1) según una de las reivindicaciones 1 a 6, caracterizado por que el módulo de aplicación bancaria (9) comprende el conjunto de parámetros relativos a los comerciantes asociados con el pago.

8. El sistema (1) según las reivindicaciones 1 a 7, caracterizado por que el terminal de pago electrónico simulado está configurado para cada comerciante dado de cada transacción.

9. El sistema (1) según una de las reivindicaciones 1 a 8, caracterizado por que la interfaz (7) está programada a nivel de hardware fuera de la capa de aplicaciones.

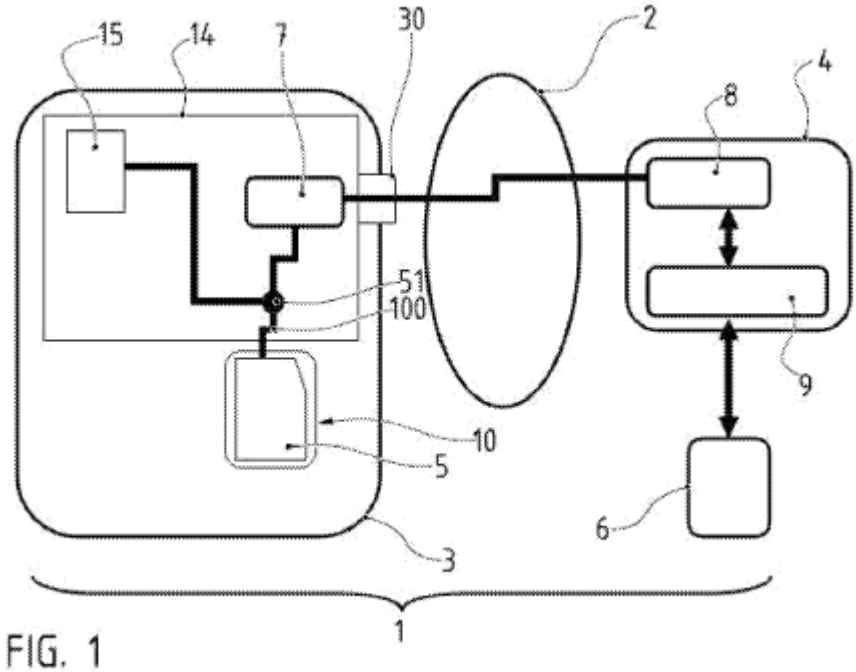
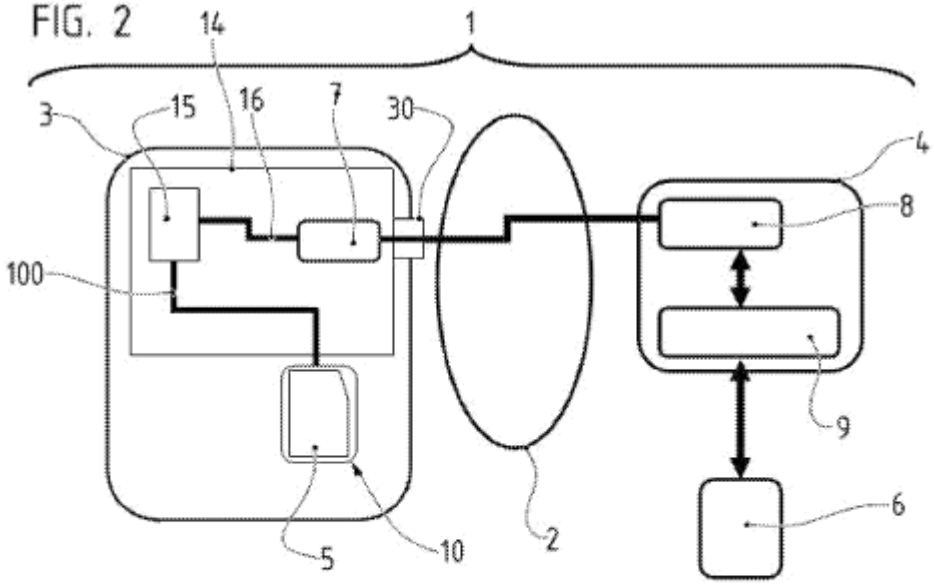


FIG. 1

FIG. 2



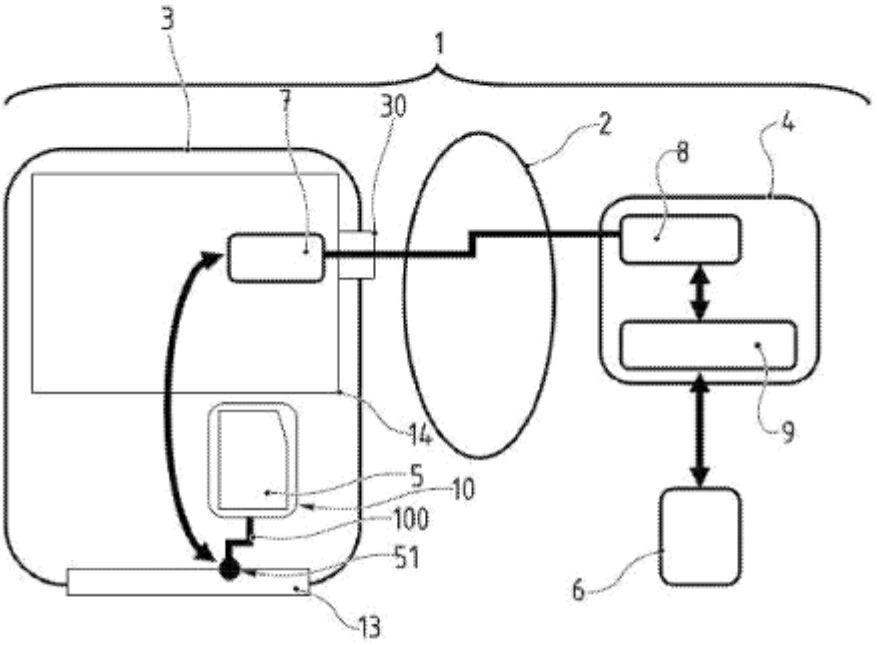


FIG. 3