(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 952 732**

(51) Int. CI.:

***G06Q 20/34*** (2012.01)
***G07F 7/08*** (2006.01)
***H04L 9/32*** (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **30.06.2017 PCT/EP2017/066362**

(87) Fecha y número de publicación internacional: **04.01.2018 WO18002349**

(96) Fecha de presentación y número de la solicitud europea: **30.06.2017 E 17733482 (8)**

(97) Fecha y número de publicación de la concesión europea: **31.05.2023 EP 3479325**

(54) Título: **Procedimiento para autentificar datos de pago, dispositivos y programas correspondientes**

(30) Prioridad:

**30.06.2016 FR 1656239**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
**03.11.2023**

(73) Titular/es:

**BANKS AND ACQUIRERS INTERNATIONAL HOLDING (100.0%)**
**28-32 boulevard de Grenelle**
**75015 Paris, FR**

(72) Inventor/es:

**GERAUD, RÉMI**

(74) Agente/Representante:

**LEHMANN NOVO, María Isabel**

## DESCRIPCIÓN

Procedimiento para autentificar datos de pago, dispositivos y programas correspondientes

1. Campo

La invención se refiere al campo de la seguridad de los datos intercambiados a través de un protocolo de transmisión de datos sin contacto. La técnica se refiere más particularmente a la transmisión de datos de tipo NFC, en la que se lleva a cabo una transmisión entre un primer dispositivo y un segundo dispositivo separados por una distancia del orden de una decena de centímetros como máximo. La técnica no se aplica y no está destinada a aplicarse en el contexto de técnicas de transmisión de datos de tipo WiFi, WiMax, LTE, cuyas tecnologías de transmisión son diferentes.

2. Técnica anterior

Muchos dispositivos de la vida cotidiana son capaces de comunicarse e intercambiar datos entre sí. Una parte cada vez mayor de dispositivos utiliza, para ello, protocolos de intercambio de datos denominados “de campo cercano” o incluso NFC. A veces, estas técnicas de transmisión de datos también se denominan RFID. Esta denominación no es correcta ya que NFC significa comunicación de campo cercano, mientras que RFID se refiere a medios de identificación por radiofrecuencia. Ambos utilizan señales de radio para todo tipo de fines de seguimiento y localización, sustituyendo a veces los códigos de barras. Ambos utilizan medios de transmisión de datos de corto alcance.

Ahora bien, el uso de este tipo de tecnología aún genera temores y dudas por parte de los usuarios. Muchas personas tienen poca o ninguna confianza en estas tecnologías, más particularmente cuando se trata de utilizarlas para fines de tratamiento de datos personales y/o confidenciales. Este es por ejemplo el caso del pago. Hace relativamente poco tiempo aparecieron los dispositivos de pago sin contacto. Se tratan, por ejemplo, de tarjetas de pago sin contacto que le permiten realizar un pago (cuyo importe máximo generalmente tiene un tope) colocando (o acercando) la tarjeta de pago a una terminal de pago compatible. También se trata de terminales de comunicación, que también incorporan “chips” sin contacto: estos chips (también llamados “*contactless chip*”) y que proporcionan capacidades de intercambio de datos a los terminales de comunicación, capacidades que pueden utilizarse para realizar pagos, un poco como si la terminal de comunicación imitara el comportamiento de una tarjeta de pago sin contacto. Muchos rumores, a menudo infundados, dejan entender que la comunicación o que el pago realizado sin contacto no sería seguro. También se informa a menudo que los dispositivos serían poco seguros y que sería posible recuperar los datos contenidos en estos dispositivos sin el conocimiento del usuario. Aunque estos rumores a menudo son infundados, existen no obstante riesgos durante la transmisión de datos entre los dispositivos y en particular durante la transmisión de datos de pago. Los riesgos, sin embargo, no provienen de la tecnología utilizada en sí misma (NFC), sino generalmente del propio usuario. Así, por ejemplo, en el caso de una terminal de comunicación que utilice la interfaz NFC para realizar un pago, es posible que el usuario haya instalado una aplicación no segura, o incluso una aplicación maliciosa, cuyo objetivo es utilizar los datos de pago con fines de realizar fraudes. La situación es la misma en el lado de la terminal del comerciante.

Por ejemplo, en el ámbito de la comunicación entre un dispositivo de usuario (una terminal de comunicación de tipo smartphone) y una terminal de pago, en particular mediante el uso de protocolos NFC para el pago, es necesario que el dispositivo y la terminal autentiquen los datos. Para ello, el dispositivo implementa un protocolo de autentificación con la terminal (por ejemplo, una terminal de pago, un borne de comercio, o cualquier otro dispositivo adecuado). La terminal comprueba que la fase de autentificación se ha realizado correctamente y, en caso contrario, rechaza la transacción o activa una alerta, o implementa cualquier otro comportamiento apropiado en tal situación.

En escenarios típicos, la terminal que lleva a cabo estas comprobaciones es un dispositivo seguro (como una terminal de pago). Se ha diseñado para prevenir la mayoría de los posibles tipos de intrusión, tanto materiales como de programas. Pero si la terminal de pago es un dispositivo de terceros (terminal de comunicación de tipo tableta, smartphone, pantalla), entonces no se puede garantizar la seguridad de este terminal de comunicación (de terceros), ni el origen de las aplicaciones instaladas en este terminal (por el propio comerciante). Si el comerciante no está atento, las aplicaciones instaladas en este terminal pueden ser fraudulentas.

Se presenta a continuación un caso de posible mal funcionamiento, implementado durante un pago entre una terminal de comunicación y un dispositivo de usuario. Se denomina “V” el verificador (por ejemplo la terminal o el dispositivo del comerciante) y “*P*” el probador (dispositivo del usuario: smartphone, tableta).

Los protocolos de pago suelen funcionar de la siguiente manera, durante la transacción: *V* pregunta a *P* para firmar datos digitalmente. *P* firma los datos, conforme a lo solicitado por *V* y transmite los datos firmados a *V*. Esta firma es verificada por *V* y, si es correcta, la transacción se acepta entonces y se transfiere al resto de la cadena de procesamiento de pagos. Tal procedimiento se denomina “impugnación respuesta” (*challenge response*) y se utiliza, por ejemplo, en las especificaciones EMV.

El problema a resolver es el siguiente: si *V* funciona en un dispositivo no seguro (es decir, una terminal de tipo tableta, PC u otro, al que se le han añadido funcionalidades de pago) que está infectado por un malware (instalado por el comerciante o por un tercero mal intencionado), entonces este programa puede aprovecharse de la terminal del cliente P. Tal aprovechamiento puede, por ejemplo, tomar la forma de una sucesión de transacciones (invisibles). Esto se puede llevar a cabo, por ejemplo, cuando la terminal del comerciante obliga al dispositivo del usuario a firmar mensajes arbitrarios. El dispositivo del usuario, en posición de "esclavo", está entonces obligado a firmar estos datos. El malware instalado en la terminal del comerciante se sirve entonces de estos datos firmados para crear transacciones fraudulentas.

Esta es la paradoja de estos procesamientos criptográficos: es cierto que los procesamientos que se llevan a cabo son buenos (ya que implementan procesamientos criptográficos), no obstante, no se puede garantizar el uso que se hace de los resultados de estos procesamientos criptográficos.

3. Resumen

La invención no plantea estos problemas de la técnica anterior. Más particularmente, la invención proporciona una solución sencilla al problema identificado anteriormente. Esta solución es totalmente compatible con los dispositivos de materiales existentes.

Más particularmente, se propone un procedimiento de autentificación de al menos un dato, procedimiento implementado durante una transacción de pago que se produce entre una terminal de comunicación de un comerciante y un dispositivo de usuario, procedimiento de tipo que comprende la transmisión por la terminal de comunicación de al menos un dato a firmar al dispositivo del usuario, por medio de un enlace de datos inalámbrico de campo cercano.

Tal procedimiento comprender:

- una etapa de obtención de dicho dato a firmar;
- una etapa de obtención de un identificador de dicha terminal de comunicación;
- una etapa de firma, con la ayuda de una clave de dicha terminal de comunicación, de dicho dato a firmar y de dicho identificador de la terminal de comunicación, proporcionando un par de datos firmados;
- una etapa de transmisión del par de datos firmados a dicho dispositivo de usuario; y
- una etapa de recepción, desde dicho dispositivo de usuario, de un dato encriptado, estableciendo la autentificación de dicho par de datos firmados.

Así, al firmar los datos que transmite al dispositivo de usuario, la terminal de comunicación permite certificar el origen de estos datos y por tanto permite al dispositivo de usuario verificar el origen de los datos que recibe.

Según una característica particular, el procedimiento comprende, posteriormente a dicha etapa de recepción de un dato encriptado que proviene de dicho dispositivo de usuario:

- una etapa de desencriptación, por parte de una unidad de procesamiento segura de dicha terminal de comunicación, de dicho dato encriptado, proporcionando un dato firmado;
- una etapa de verificación de la validez de dicho dato firmado con respecto a un dato de referencia.

Así, el procedimiento permite que la terminal del comerciante verifique que él mismo no es víctima de un intento de fraude por parte del dispositivo del usuario; se dispone así de un refuerzo bilateral de la seguridad de la transacción en el campo cercano.

Según una característica particular, dicho dato de referencia es igual a dicho dato a firmar.

Así, existe una uniformidad de los datos que se intercambian entre la terminal de comunicación y el dispositivo de usuario: como la terminal de comunicación ya posee los datos a firmar, es fácil comprobar que los datos que recibe por parte del dispositivo del usuario son correctos.

Según una característica particular, que después de que la etapa de verificación de la validez de dicho dato firmado con respecto al dato de referencia proporciona un resultado positivo, el procedimiento comprende una etapa de transmisión, por parte de la terminal de comunicación, de dicho dato firmado a un sistema de procesamiento de transacción de pago.

Así, cuando la autentificación de los datos se lleva a cabo correctamente, se lleva a cabo la transacción de pago.

Dicha etapa de firma comprende:

- una etapa de transmisión de dicho dato a firmar y de dicho identificador de la terminal de comunicación, a una unidad de procesamiento segura de dicha terminal de comunicación, por una unidad de procesamiento general de dicha terminal de comunicación;

- una etapa de firma, por dicha unidad de procesamiento segura, con la ayuda de dicha clave de la terminal de comunicación, de dicho dato a firmar y de dicho identificador de la terminal de comunicación, proporcionando respectivamente un dato firmado y un identificador firmado;

- una etapa de transmisión de dicho dato firmado y del identificador firmado a dicha unidad de procesamiento general de dicha terminal de comunicación.

Se asegura así la producción de los datos que se transmiten al dispositivo de usuario impidiendo que estos datos sean falsificados por otras aplicaciones presentes en la terminal de comunicación.

Dicha clave de la terminal de comunicación es una clave privada que pertenece a un par {clave privada; clave pública}.

Así, se garantiza una mayor seguridad mediante el uso de una arquitectura de clave pública. El procedimiento comprende, dentro del dispositivo del usuario, entre la etapa de transmisión del par de datos firmados y la etapa de recepción del dato encriptado:

- una etapa de recepción del par de datos firmados por el dispositivo de usuario;

- una etapa de verificación, mediante una clave, de la firma de los datos del par de datos firmados; y

  cuando la firma de los datos del par de datos firmados es correcta:

  - una etapa de firma, con la ayuda de una clave de firma *tk*, de al menos uno de los datos previamente recibidos por parte de la terminal del comerciante, proporcionando un dato firmado;

  - una etapa de encriptado de dicho dato firmado con la ayuda de una clave de encriptación que proporciona el dato encriptado;

  - una etapa de transmisión del dato encriptado a dicha terminal del comerciante.

Según otro aspecto, la invención también se refiere a una terminal de comunicación que comprende una unidad general de procesamiento, una memoria. Tal terminal comprende una unidad de procesamiento segura y una memoria segura y al menos un circuito reconfigurable de procesamiento de transacción de pago con una terminal de usuario que comprende, en particular, una autentificación de un dato, comprendiendo dicha terminal de comunicación:

- medios para la obtención de un dato a firmar;

- medios para la obtención de un identificador de dicha terminal de comunicación;

- medios para firmar, con la ayuda de una clave de dicha terminal de comunicación, dicho dato a firmar y dicho identificador de la terminal de comunicación, proporcionando un par de datos firmados;

- medios para transmitir el par de datos firmados a dicho dispositivo de usuario; y

- medios para recibir, desde dicho dispositivo de usuario, un dato encriptado, estableciendo la autentificación de dicho par de datos firmados.

Según otro aspecto, la técnica también se refiere a una terminal de usuario que comprende medios para implementar el procedimiento tal como se ha descrito anteriormente.

Según una implementación preferida, las diversas etapas de los procedimientos según la invención se implementan mediante uno o más programas o programas informáticos, que comprenden instrucciones de programas destinadas a ser ejecutadas por un procesador de datos de un módulo de relés según la invención y que está concebido para controlar la ejecución de las diferentes etapas de los procedimientos.

En consecuencia, la invención también se refiere a un programa, capaz de ser ejecutado por un ordenador o por un procesador de datos, comprendiendo este programa instrucciones para controlar la ejecución de las etapas de un procedimiento tal como se ha mencionado anteriormente.

Este programa puede usar cualquier lenguaje de programación, y estar en forma de código fuente, código objeto, o código intermedio entre el código fuente y el código objeto, tal como en forma parcialmente compilada, o en cualquier otra forma deseable.

La invención también se refiere a un soporte de informaciones legible por un procesador de datos, y que comprende 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 medio puede comprender un medio de almacenamiento, como una ROM, por ejemplo, un CD-ROM o una ROM de circuito microelectrónico, o incluso un medio magnético de grabación, por ejemplo, un disquete (floppy disk) o un disco duro.

Por otro lado, el soporte de información puede ser un soporte transmisible tal como una señal eléctrica u óptica, que puede transmitirse a través de un cable eléctrico u óptico, por radio o por otros medios. El programa según la invención puede ser descargado, en particular, de una red de tipo Internet.

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

El término “módulo” puede corresponder aquí tanto a un componente de programa, como a un componente de material o a un conjunto de componentes de material y programa.

Un componente de programa corresponde a uno o más programas informáticos, uno o más subprogramas de un programa, o más generalmente a cualquier elemento de un programa o de un software capaz de llevar a cabo una función o un conjunto de funciones, según se describe a continuación para el módulo en cuestión. Tal componente de software es ejecutado por un procesador de datos de una entidad física (terminal, servidor, puerta de enlace, enrutador, etc.) y es susceptible de que acceda a los recursos materiales de esta entidad física (memorias, soportes de grabación, bus de comunicación, tarjetas electrónicas de entradas/salidas, interfaces de usuario, etc.).

De la misma manera, un componente material corresponde a cualquier elemento de un conjunto material (o hardware) capaz de llevar a cabo una función o un conjunto de funciones, según lo que se describe a continuación para el módulo en cuestión. Puede tratarse de un componente material que se puede programar o que tiene un procesador integrado para ejecutar un programa, por ejemplo un circuito integrado, una tarjeta de chip, una tarjeta de memoria, una tarjeta electrónica para la ejecución de un microprograma (firmware), etc.

Cada componente del sistema descrito anteriormente implementa por supuesto sus propios módulos de programa.

## 4. Dibujos

Otras características y ventajas de la invención aparecerán más claramente con la lectura de la siguiente descripción de una realización preferida, dada a modo de simple ejemplo ilustrativo y no limitativo, y de los dibujos adjuntos, entre los cuales:

- la figura 1 presenta un sinóptico de la técnica propuesta que autentifica los datos transmitidos entre una terminal de comunicación de un comerciante y un dispositivo de usuario;
- la figura 2 presenta un sinóptico de la técnica propuesta que lleva a cabo una firma de datos dentro de la terminal de comunicación del comerciante;
- la figura 3 representa esquemáticamente una terminal de comunicación de un comerciante según la presente invención;
- la figura 4 representa esquemáticamente un dispositivo de usuario según la presente.

## 5. Descripción

### 5.1. Principio general

Como se ha explicado anteriormente, el principio general de la invención consiste en particular en integrar, en el esquema de “*impugnación-respuesta*”, una o más restricciones adicionales. La presente invención propone una modificación de protocolo que permite resistir a los ataques de terminales que comprenden softwares maliciosos. De forma secundaria, esta modificación del protocolo también permite proteger los propios terminales de los comerciantes frente a respuestas no solicitadas de otros dispositivos (es decir, dispositivos maliciosos que intentarían atacar una terminal comercial auténtica). Esta modificación del protocolo ofrece así una capa adicional de protección contra otro tipo de ataques. (DoS “Deny of Serverce”, Concurency Attaks - ataques por competencia de acceso a los recursos-).

Así, cuando se lleva a cabo una transacción de pago entre una terminal de un comerciante y un dispositivo de un usuario, un proceso del tipo "*challenge/response*" ("impugnación/respuesta" en francés) se lleva a cabo para que la terminal del comerciante identifique (autentifique) el dispositivo del usuario (y viceversa). Se supone que la terminal del comerciante no es seguro como tal (se trata de un teléfono, una tableta o un PC), pero que dispone de recursos de seguridad. Estos recursos de seguridad pueden adoptar, por ejemplo, la forma de un "*secure element* - SE" (elemento seguro en francés), de un "Truster Execution Environment - TEE" (entorno de ejecución seguro en francés) o también de otro componente material o software dedicado. Se supone, para las siguientes explicaciones, que la aplicación de pago de la terminal del comerciante se denomina *TPC*, y que comprende un módulo de verificación (identificación) denominado *V* (se trata, por ejemplo, de un SE, de un TEE o, más generalmente, de una unidad de procesamiento segura). También se supone que existe una aplicación de pago en el dispositivo de usuario DU, y que el dispositivo de usuario (*DU*) comprende un módulo de prueba (confirmación de identidad) denominado *P* (se trata, por ejemplo, de un SE, de un TEE o, más generalmente, de una unidad de procesamiento segura). En otra realización, el dispositivo de usuario puede ser una tarjeta de pago convencional, en la que se han llevado a cabo modificaciones de protocolo y materiales que permiten implementar la presente técnica.

Durante el uso conjunto de las aplicaciones de pago *TPC* y *DU*, el procedimiento implementado es globalmente el siguiente:

- los datos de autentificación que se transmiten por *V* a *P* (es decir, los datos de "*impugnación*") están firmados digitalmente por *V* en sí.

- la respuesta transmitida por P está encriptada, de modo que sólo *V* puede comprobar su validez.

Con el fin de permitir tal implementación, es suficiente proporcionar *V* de una clave (pública) conocida por *P*.

La lógica subyacente de este procedimiento es que *P* ignora pura y simplemente las solicitudes de firma que no provienen directamente de la parte segura de *V* (es decir, por ejemplo, desde el "*secure element*" al que *V* tiene acceso o desde el entorno de confianza al que *V* tiene acceso): en efecto, se supone que sólo esta arquitectura es capaz de lograr una firma digital válida del *challenge* (impugnación) antes de su transmisión a *P*.

Existe una razón por la cual se hace esta suposición: los inventores han tenido la idea de disponer la clave pública de firma (de *V*) accesible directamente por los recursos de seguridad de la terminal del comerciante. Los recursos de seguridad conservan esta clave y sólo la hacen accesible a un número limitado de aplicaciones de confianza (por ejemplo sólo una: la aplicación de pago instalada en la terminal del comerciante). Además, el "*secure element*" lleva a cabo por sí mismo las operaciones de encriptado para la cuenta de la aplicación de pago de la terminal del comerciante. Así, en la primera etapa, antes de la transmisión de la impugnación ("*challenge*") al terminal de comunicación del usuario, la impugnación es firmada por los recursos de seguridad utilizando la clave de *V* (la clave de la aplicación de pago). Según la invención, esta clave es una clave pública.

Además, el hecho de que la respuesta transmitida por P esté encriptada permite prevenir situaciones en las que un estafador detecta y reproduce rastros de autentificación válidos (ataque de repetición). El ataque puede ser implementado tanto por una aplicación maliciosa instalada en el dispositivo del comerciante como por una aplicación maliciosa instalada en el dispositivo del cliente.

Se describe, con respecto a la figura 1, la técnica propuesta que autentifica los datos transmitidos entre una terminal de comunicación de un comerciante y un dispositivo de usuario. Se recuerda que se desea asegurar que el dispositivo del usuario sólo firme datos que proceden legítimamente de la terminal de comunicación (que actúa como terminal de pago) del comercio. Así, la técnica comprende:

- una etapa para obtener (10) los datos a firmar (*DaS*);

- una etapa para obtener (20) un identificador de la terminal de comunicación (*UiD*);

- una etapa de firmar (30), con la ayuda de una clave (K) de la terminal de comunicación, los datos a firmar (*DaS*) y del identificador de la terminal de comunicación (*UiD*), proporcionando un par de datos firmados (*CDS*);

- una etapa de transmitir (40) el par de datos firmados (*CDS*) al dispositivo del usuario; y

- una etapa de recibir (50), desde el dispositivo del usuario, un dato encriptado (*DC*), estableciendo la autentificación del par de datos firmados.

En efecto, según la presente descripción, el hecho de recibir un dato encriptado desde el dispositivo de usuario confirma el hecho de que el par de datos firmados está efectivamente autentificado por el dispositivo de usuario. Esto es práctico ya que no es necesario transmitir un acuse de recibo específico o una confirmación de autentificación. Esto reduce por lo tanto los intercambios. En caso de ausencia de respuesta por parte del dispositivo del usuario, se puede deducir que los datos transmitidos son erróneos (error en la recepción de los datos transmitidos por ejemplo). Por su

parte, el dispositivo del usuario verifica la firma de los datos transmitidos y no transmite ninguna respuesta en caso de ausencia de autentificación.

Si el dispositivo del usuario responde, entonces el procedimiento continúa mediante una verificación de los datos recibidos del dispositivo del usuario y comprende:

- una etapa de desencriptar (60), por parte de la unidad de procesamiento segura de la terminal de comunicación, de los datos encriptados (*DC*), proporcionando un dato firmado (*DS*);
- una etapa de verificar (70) la validez del dato firmado (*DS*) con respecto a un dato de referencia (*DR*);
- una etapa de transmitir (80), por la terminal de comunicación, el dato firmado (*DS*) a un sistema de procesamiento de transacción de pago (STTP).

Estas tres últimas etapas permiten que la terminal del comerciante no sea engañado por datos “reproducidos” arbitrariamente por un dispositivo de usuario que en sí mismo sería fraudulento.

Así, la solución proporcionada tiene la ventaja de proteger el dispositivo del usuario (y al propio usuario) contra solicitudes de firmas fraudulentas, y proteger al comerciante contra intentos de usurpación recibidos por parte del usuario. La ventaja es por lo tanto doble debido a la protección bilateral.

En función de las realizaciones, las claves utilizadas para la firma y el encriptado pueden ser pares de claves públicas/privadas o claves simétricas que sirven al mismo tiempo para el encriptado y para el desencriptado.

Se describe, en relación con la figura 2, la técnica propuesta que lleva a cabo una firma de datos dentro de la terminal de comunicación del comerciante. Esta técnica comprende:

- una etapa de transmitir (301) dicho dato a firmar (DaS) y/o dicho identificador de la terminal de comunicación (UiD) a una unidad de procesamiento segura (UTS) de dicha terminal de comunicación, por una unidad de procesamiento general (UTG) de dicha terminal de comunicación;
- una etapa de firmar (302), por parte de dicha unidad de procesamiento segura, con la ayuda de dicha clave de la terminal de comunicación (K), de dicho dato a firmar (Das) y dicho identificador (UiD) de la terminal de comunicación, proporcionando respectivamente un dato firmado (DS) y un identificador firmado (UiDs);
- una etapa de transmitir (303) dicho dato firmado (DS) y del identificador firmado (UiDs) a dicha unidad de procesamiento general de dicha terminal de comunicación.

5.2. Descripción de una realización

En esta realización puramente ilustrativa, se supone, por simplicidad, que se utilizan mecanismos de firma y encriptado de tipo RSA (tanto del lado de la terminal del comerciante como del dispositivo del usuario). En esta realización, previamente a la implementación del protocolo de intercambio seguro, se supone que se han llevado a cabo dos fases de instalación: una del lado de la terminal del comerciante y otra del lado del dispositivo del usuario.

5.2.1. Fase de instalación del lado de la terminal del comerciante

La terminal del comerciante tiene una clave privada *sk*. Esta dotación se puede implementar en cualquier momento. Se supone que esta clave privada *sk* se genera según técnicas anteriores conocidas y que se coloca dentro de un recurso seguro de la terminal del comerciante. Idealmente, esta clave privada se coloca dentro de un TEE (que actúa como una unidad de procesamiento segura) de la terminal del comerciante. También se dispone, para la terminal del comerciante, de un identificador único (*uid*) que está generado y firmado (por ejemplo, por el operador de la aplicación de pago). La aplicación de pago también se instala en la terminal del comerciante. Estos materiales (aplicación de pago, clave privada *sk* e identificador único uid) se pueden instalar inteligentemente al mismo tiempo en la terminal del comerciante, por medio de un proceso de instalación seguro (que puede implementarse en línea o en el sitio por un técnico autorizado, por ejemplo).

Finalmente, la clave pública pk (que corresponde a la clave privada *sk*) se pone a disposición en una base de datos, con el identificador único *uid*, a fin de formar un par {clave pública *pk*; identificador único *uid*}. El par {*pk*; *uid*} es objeto de una firma (por ejemplo, por parte del operador de la aplicación de pago si es él quien firmó el identificador único *uid*).

En una realización específica, la fase de instalación se lleva a cabo durante la instalación de una aplicación de pago en una terminal de comunicación (del tipo smartphone, tableta u ordenador) del comerciante, estando dicha terminal de comunicación equipado con un TEE y/o un SE (también denominado módulo V). Esta realización tiene la ventaja de no tener que comunicar la clave privada *sk* al terminal de comunicación como tal: este dato sólo se comunica al SE

o al TEE. Así, se asegura que la terminal de comunicación (y sobretodo las eventuales aplicaciones fraudulentas de este terminal) no puedan tener acceso a esta clave privada.

5.2.2. Fase de instalación del lado del dispositivo del usuario

El dispositivo del usuario, que es por ejemplo una terminal de comunicación de tipo smartphone, una tableta, está también equipado con un SE o un TEE (que actúa como unidad de procesamiento segura). Se recuerda que en esta realización, el cliente desea pagar con su dispositivo. Este dispositivo tiene por lo tanto los datos necesarios para realizar un pago. Pueden tratarse, en una realización específica, de datos de tarjetas bancarias (nombre del titular, número de tarjeta PAN, fecha de validez, código de verificación). También puede tratarse de otros datos, en función de las realizaciones.

En el ámbito de la presente técnica, la fase de instalación consiste en depositar, en el SE o el TEE del dispositivo del usuario (también denominado módulo *P*), la clave de firma *tk*, que se utiliza para realizar una firma de los datos firmados (data y uid) transmitidos por la terminal del comerciante, después de que el dispositivo del usuario haya verificado la validez de las firmas colocadas por la terminal del comerciante.

Esta instalación se puede implementar típicamente mediante la instalación de una aplicación de pago, como es el caso de la aplicación de pago instalada en la terminal del comerciante.

Una posibilidad ventajosa es instalar esta clave de firma al mismo tiempo que una aplicación bancaria: por ejemplo, la aplicación bancaria del cliente. En efecto, con el desarrollo de las aplicaciones bancarias (aplicaciones que permiten gestionar sus cuentas desde un smartphone o una tableta), una solución interesante, tanto para el cliente como para el banco, puede consistir en disponer de una aplicación bancaria que permite también realizar pagos. En este caso, los datos necesarios para el pago no son necesariamente datos de la tarjeta bancaria, sino que pueden ser datos específicamente preparados por la aplicación bancaria del banco, o incluso específicamente preparados, en el momento del pago, por la propia entidad financiera (es decir, por un servidor al que está conectada la aplicación bancaria del cliente).

Para realizar un pago, en este caso particular, el cliente abre su aplicación bancaria; selecciona el hecho de que desea realizar un pago; ingresa un eventual código confidencial (o se autentifica por ejemplo por vía biométrica); y coloca su dispositivo en la terminal del comerciante. La aplicación bancaria reacciona a las solicitudes de la terminal del comerciante (como se explica aquí) y se lleva a cabo el pago. Para el banco, como para el cliente, los beneficios son reales, tanto en términos de seguridad de la transacción (realizada por la aplicación bancaria), como en términos de fidelización del cliente (que ya no está obligado a realizar un pago con una aplicación de terceros, del cual no tiene ninguna garantía, por ejemplo a nivel de seguridad y confidencialidad de los datos transmitidos y procesados).

5.2.3. Desarrollo del intercambio de datos de autentificación

En esta realización, la autentificación se lleva a cabo de la siguiente manera:

- La terminal del comerciante (o el módulo *V*) transmite el par {[*uid*]$_{sk}$, [*data*]$_{sk}$} al dispositivo del usuario (o al módulo P); el par de datos {[*uid*]$_{sk}$, [*data*]$_{sk}$} comprende [*uid*]$_{sk}$ que es el identificador único firmado con la clave *sk* y datos [*data*]$_{sk}$ también firmados con la clave *sk*;

- el dispositivo del usuario (o módulo *P*) usa el identificador único *uid* para obtener la clave pública *pk*; por ejemplo, descarga esta clave pública en un servidor dedicado a ello o también busca esta clave en una base de datos interna (por ejemplo, un archivo de texto o un archivo xml) proporcionada por la aplicación de pago;

- el dispositivo del usuario (o módulo *P*) utiliza la clave pública *pk* para verificar la validez de la firma de *uid* y de *data*; en caso de error en una u otra de estas firmas (por ejemplo *uid* claramente no lo es el *uid* que posee el cliente), entonces el cliente detiene el proceso (y no responde a la terminal del comerciante);

- cuando las dos firmas son correctas (y se puede deducir que se llevaron a cabo por la terminal del comerciante), el dispositivo del usuario continúa procesando firmando los datos [*data*] con la clave *tk* y encriptando estos datos firmados con la clave pública de la terminal del comerciante pk: $Enc_{pk}$([*data*]*tk*); después transmite estos datos al terminal del comerciante;

- la terminal del comerciante recibe los datos que provienen del dispositivo del usuario, después desencripta estos datos con la ayuda de su clave privada *sk*, y verifica la firma de los datos. Si la firma de los datos es incorrecta, el proceso se detiene; de lo contrario, la firma se transmite a la red de procesamiento de pagos.

Así, la autentificación de los datos transmitidos, durante una operación de pago, entre una terminal de un comerciante y un dispositivo de usuario, usando una comunicación de campo cercano (NFC), permite validar una transacción de forma segura.

5.3. Otras características y ventajas

Se describe, en relación con la figura 3, una terminal de comunicación implementado para realizar una autentificación de datos en el ámbito de un proceso de pago, según el procedimiento descrito anteriormente.

Por ejemplo, la terminal de comunicación, que actúa como terminal de pago, comprende una memoria 31 que comprende en particular una memoria intermedia, una unidad de procesamiento general 32, equipada por ejemplo con un microprocesador, y controlada por un programa informático 33, y una unidad de procesamiento segura 34 (anotado V antes), controlada por un programa informático 35, implementando estas unidades de procesamiento el procedimiento de autentificación tal como se describe antes para llevar a cabo un pago al comerciante.

En la inicialización, las instrucciones de código del programa informático 35 se cargan, por ejemplo, en una memoria antes de ser ejecutadas por el procesador de la unidad de procesamiento segura 34. La unidad de procesamiento 34 recibe como entrada al menos un dato que debe ser autentificado. El microprocesador de la unidad de procesamiento segura 34 lleva a cabo las etapas del procedimiento de autentificación, según las instrucciones del programa informático 35 para proporcionar, a la unidad de procesamiento general 32, un dato firmado y, llegado el caso, un dato representativo del identificador de la terminal de comunicación (también firmado). La unidad de procesamiento general 32 lleva a cabo un procesamiento de estos datos para transmitirlos a un dispositivo de un cliente (por ejemplo un smartphone, una tableta) en el ámbito de una transacción de pago.

Para ello, la terminal de comunicación comprende, además de la memoria intermedia 31, medios de comunicación, tales como módulos de comunicación de red, medios de transmisión de datos y circuitos de transmisión de datos entre los distintos componentes de la terminal de comunicación.

Estos medios pueden presentarse en forma de un procesador particular implementado dentro de la terminal de comunicación. Según una realización particular, este dispositivo usa una aplicación específica que se encarga de realizar las transacciones, siendo dicha aplicación por ejemplo proporcionada por el fabricante del procesador en cuestión a fin de permitir el uso de dicho procesador, o por un proveedor de solución de pago para terminales “abiertos”. Para ello, el procesador comprende medios de identificación únicos. Estos medios de identificación únicos permiten asegurar la autenticidad del procesador.

Por otro lado, el dispositivo comprende además medios de comunicación de campo cercano, denominados NFC, y medios para transmitir y recibir datos que provienen de redes de comunicación. Estos medios se presentan también como interfaces de comunicación que permiten intercambiar datos en redes de comunicación, medios de consulta y actualización de la base de datos.

Se describe, en relación con la figura 4, un dispositivo de usuario implementado para llevar a cabo una autentificación de datos en el ámbito de un proceso de pago, según el procedimiento descrito anteriormente.

Por ejemplo, el dispositivo de usuario comprende una memoria 41 que consta de una memoria intermedia, una unidad de procesamiento general 42, equipada por ejemplo con un microprocesador y controlada por un programa informático 43, y una unidad de procesamiento segura 44 (anotada *P*, anteriormente), controlada por un programa informático 45, llevando a cabo estas unidades de procesamiento el procedimiento de autentificación tal como se describe anteriormente para realizar un pago al comerciante.

En la inicialización, las instrucciones de código del programa informático 45 se cargan, por ejemplo, en una memoria, antes de ser ejecutadas por el procesador de la unidad de procesamiento segura 44. La unidad de procesamiento segura 44 recibe como entrada, proveniente de la unidad de procesamiento general, al menos un dato para ser autentificado (dato firmado por la terminal de comunicación). El microprocesador de la unidad de procesamiento segura 44 lleva a cabo las etapas del procedimiento de autentificación, según las instrucciones del programa informático 45 para proporcionar, a la unidad de procesamiento general 42, al menos un dato sin firmar. La unidad de procesamiento general 42 lleva a cabo un procesamiento de estos datos para, por un lado, comparar los datos de referencia y los datos resultantes de la retirada de las firmas y después, si estos datos son correctos, transmitir al menos uno de ellos a la unidad de procesamiento segura para firmar estos datos con una clave de firma y encriptar estos nuevos datos firmados con una clave de la terminal de comunicación. La unidad de procesamiento segura transmite este dato a la unidad de procesamiento general que lo transmite nuevamente al terminal de comunicación (por ejemplo, un smartphone, una tableta) de un comerciante.

Para ello, el dispositivo de usuario comprende, además de la memoria intermedia 41, medios de comunicación, tales como módulos de comunicación de red, medios de transmisión de datos y circuitos de transmisión de datos entre los distintos componentes del dispositivo de usuario.

Estos medios pueden presentarse en la forma de un procesador particular implementado dentro del dispositivo del usuario. Según una realización particular, este dispositivo usa una aplicación específica que se encarga de realizar las transacciones, siendo dicha aplicación por ejemplo proporcionada por el fabricante del procesador en cuestión a fin de permitir el uso de dicho procesador o por un proveedor de solución de pago para terminales “abiertos”. Para

ello, el procesador comprende medios de identificación únicos. Estos medios de identificación únicos permiten asegurar la autenticidad del procesador.

Por otro lado, el dispositivo comprende además medios de comunicación de campos cercanos, denominados NFC, y medios para transmitir y recibir datos que provienen de redes de comunicaciones. Estos medios se presentan también como interfaces de comunicaciones que permiten intercambiar datos en redes de comunicación, medios de consulta y actualización de la base de datos.

**REIVINDICACIONES**

1. Procedimiento para autentificar al menos un dato, llevándose a cabo el procedimiento durante una transacción de pago que tiene lugar entre la terminal de comunicación de un comerciante y un dispositivo de usuario, procedimiento del tipo que comprende la transmisión, por la terminal de comunicación, de al menos un dato a firmar al dispositivo de usuario por medio de un enlace de datos inalámbrico en campo cercano, caracterizándose dicho procedimiento por que comprende:

- una etapa para obtener (10) dicho dato a firmar (*DaS*)

- una etapa para obtener (20) un identificador de dicha terminal de comunicación (*UiD*);

- una etapa de firma (30), dentro de una unidad de procesamiento segura (UTS) de dicha terminal de comunicación, con la ayuda de una clave privada (sk) que pertenece a un par {clave privada; clave pública} de dicha terminal de comunicación, de dicho dato a firmar (*DaS*) y de dicho identificador de la terminal de comunicación (*UiD*), que proporciona un par de datos firmados (*CDS*), comprendiendo esta etapa de firmar:

  - una etapa de transmitir (301) dicho dato a firmar y dicho identificador de la terminal de comunicación a dicha unidad de procesamiento segura (UTS) de dicha terminal de comunicación, por una unidad de procesamiento general (UTG) de dicha terminal de comunicación;

  - una etapa de firmar (302), por dicha unidad de procesamiento segura, con la ayuda de dicha clave privada de la terminal de comunicación, de dicho dato a firmar y dicho identificador de la terminal de comunicación, proporcionando respectivamente un dato firmado y un identificador firmado;

  - una etapa de transmitir (303) dicho dato firmado y el identificador firmado a dicha unidad general de procesamiento de dicha terminal de comunicación;

- una etapa de transmitir (40) el par de datos firmados (*CDS*) a dicho dispositivo de usuario; y

- una etapa de recibir (50), desde dicho dispositivo de usuario, un dato encriptado (*DC*) estableciendo la autentificación de dicho par de datos firmados;

- una etapa de desencriptar (60), por medio de una unidad de procesamiento segura de dicha terminal de comunicación, de dicho dato encriptado (*DC*) proporcionando un dato firmado (*DS*);

- una etapa de verificar (70) la validez de dicho dato firmado (*DS*) con respecto a un dato de referencia (*DR*), siendo dicho dato de referencia (*DR*) igual a dicho dato a firmar (*Das*); y

- cuando la etapa de verificación proporcionar un resultado positivo, una etapa de transmitir (80), por parte de la terminal de comunicación, dicho dato firmado (*DS*) a un sistema de procesamiento de transacción de pago (STTP).

2. Procedimiento para autentificar según la reivindicación 1, caracterizado por que comprende, dentro del dispositivo de usuario, entre la etapa de transmisión (40) del par de datos firmados (CDS) y la etapa de recibir (50) el dato encriptado (DC):

- una etapa de recibir el par de datos firmados por el dispositivo del usuario;

- una etapa de verificar, con la ayuda de la clave pública de la terminal de comunicación, la firma de los datos del par de datos firmados; y

cuando la firma de los datos del par de datos firmados es correcta:

- una etapa de firmar, con la ayuda de una clave de firma *tk*, al menos uno de los datos previamente recibidos por parte de la terminal del comerciante, proporcionando un dato firmado;

- una etapa de encriptar dicho dato firmado con la ayuda de una clave de encriptado que proporciona el dato encriptado (DC)

- una etapa de transmitir el dato encriptado a dicha terminal del comerciante.

3. Terminal de comunicación que comprende una unidad de procesamiento general, una memoria, terminal caracterizada por que comprende una unidad de procesamiento segura y una memoria segura, y al menos un circuito reconfigurable de procesamiento de transacción de pago con una terminal de usuario, que comprende en particular una autentificación de un dato, comprendiendo dicha terminal de comunicación:

- medios para obtener un dato a firmar (*DaS*);

- medios para obtener un identificador de dicha terminal de comunicación (*UiD*);

- medios para firmar, dentro de una unidad de procesamiento segura (UTS) de dicha terminal de comunicación, con la ayuda de una clave privada (sk), que pertenece a un par {clave privada; clave pública} de dicha terminal de comunicación, de dicho dato a firmar (*DaS*) y de dicho identificador de la terminal de comunicación (*UiD*), proporcionando un par de datos firmados (*CDS*); comprendiendo estos medios:

  - medios para transmitir dicho dato a firmar y dicho identificador de la terminal de comunicación a dicha unidad de procesamiento segura (UTS) de dicha terminal de comunicación, por una unidad de procesamiento general (UTG) de dicha terminal de comunicación;

  - medios para firmar, por parte de dicha unidad de procesamiento segura, con la ayuda de dicha clave de la terminal de comunicación, dicho dato a firmar y dicho identificador de la terminal de comunicación, proporcionando respectivamente un dato firmado y un identificador firmado;

  - medios para transmitir, por parte de dicha unidad de procesamiento segura, dicho dato firmado y dicho identificador firmado a dicha unidad de procesamiento general de dicha terminal de comunicación;

- medios para transmitir el par de datos firmados (*CDS*) a dicho dispositivo de usuario; y

- medios para recibir, desde dicho dispositivo de usuario, un dato encriptado (*DC*) estableciendo la autentificación de dicho par de datos firmados;

- medios para desencriptar (60), por una unidad de procesamiento segura de dicha terminal de comunicación, dicho dato encriptado (*DC*) proporcionando un dato firmado (DS);

- medios para verificar (70) la validez de dicho dato firmado (DS) con respecto a un dato de referencia (DR), siendo dicho dato de referencia (*DR*) igual a dicho dato a firmar (*Das*); y

- medios para transmitir (80), por parte de la terminal de comunicación, dicho dato firmado (*DS*) a un sistema de procesamiento de transacción de pago (STTP).

4. Producto de programa informático descargable desde una red de comunicación y almacenado en un medio legible por un ordenador y ejecutable por un microprocesador, caracterizado por que comprende instrucciones de código de programa que conducen a la ejecución de un procedimiento de autentificación según la reivindicación 1, cuando dichas instrucciones de código de programa se ejecutan en un ordenador.

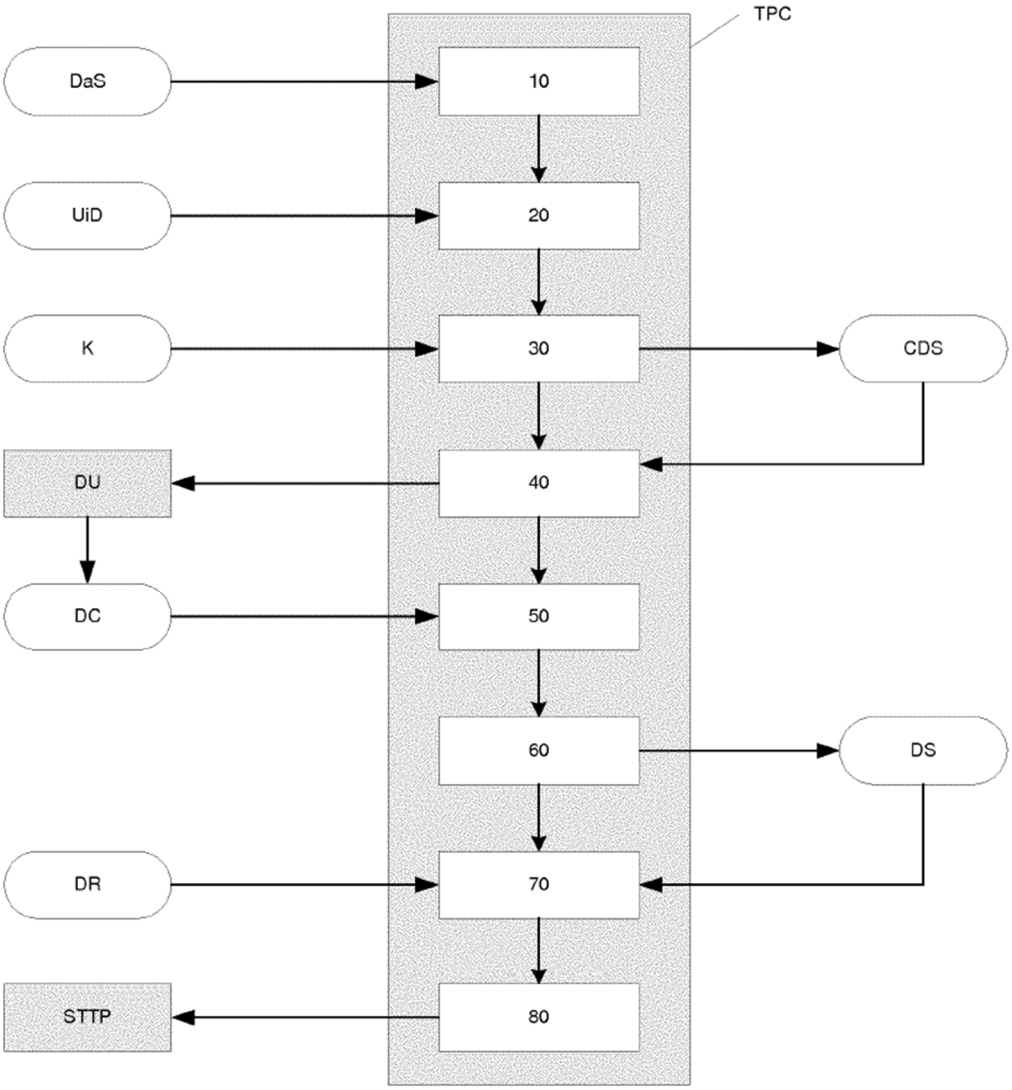


Figura 1

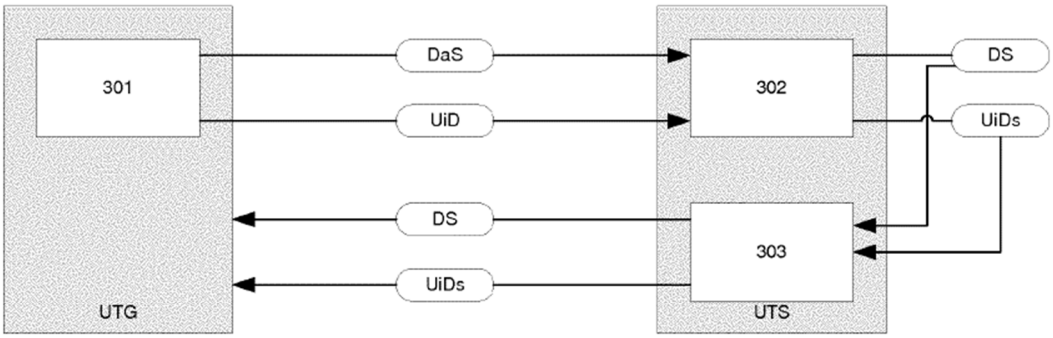


Figura 2

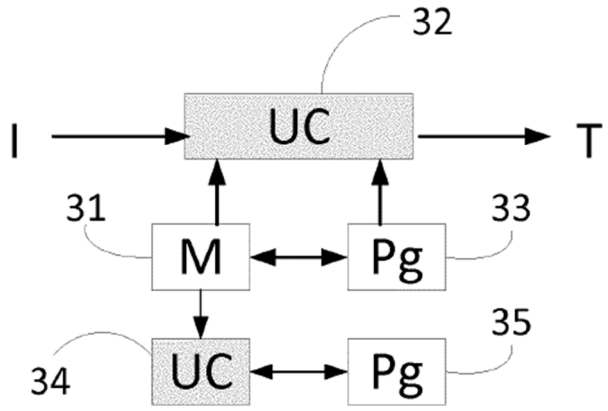


Figura 3

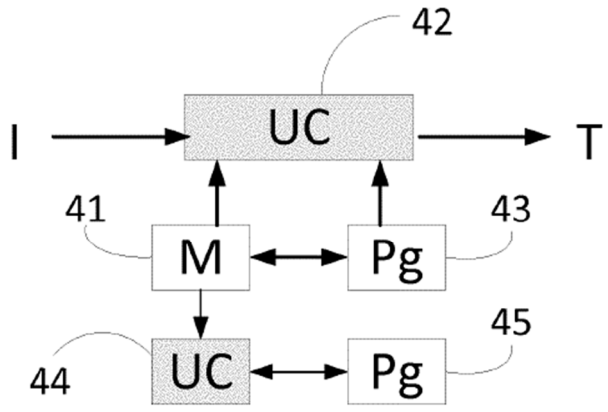


Figura 4