(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 881 873**

(51) Int. CI.:

G06F 21/44 (2013.01)
H04W 12/06 (2011.01)
H04W 12/00 (2011.01)
H04W 4/80 (2008.01)
G06Q 20/32 (2012.01)
G06Q 20/38 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **16.11.2015 PCT/FR2015/053079**

(87) Fecha y número de publicación internacional: **26.05.2016 WO16079403**

(96) Fecha de presentación y número de la solicitud europea: **16.11.2015 E 15816814 (6)**

(97) Fecha y número de publicación de la concesión europea: **19.05.2021 EP 3221815**

(54) Título: **Procedimiento de protección de una ficha de pago**

(30) Prioridad:

17.11.2014 FR 1461087

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
30.11.2021

(73) Titular/es:

IDEMIA FRANCE (50.0%)
2, Place Samuel de Champlain
92400 Courbevoie, FR y
IDEMIA AMERICA CORP. (50.0%)

(72) Inventor/es:

LASSOUAOUI, ERIC;
LEDRU, PHILIPPE y
LIMOUSY, FRANCIS

(74) Agente/Representante:

DEL VALLE VALIENTE, Sonia

DESCRIPCIÓN

Procedimiento de protección de una ficha de pago

El campo de la invención se refiere a un procedimiento de protección de una ficha de pago derivada de un instrumento de pago, a un terminal móvil y a un servidor de generación de una ficha de pago.

En la actualidad aún existen los fraudes de tarjeta bancaria, a pesar de la sofisticación de la protección de los datos bancarios y las medidas de verificación de una transacción por la red de pago. Una tarjeta de pago se protege mediante una verificación de un código personal memorizado en un chip electrónico, así como mediante el uso de algoritmos dinámicos para la verificación de los datos de la transacción bancaria.

Con el desarrollo de la economía digital, la parte de las transacciones realizada en Internet aumenta cada día. Una nueva tendencia también es la integración de una tarjeta de pago virtual alojada en una aplicación de pago móvil de un teléfono portátil. Un abonado dispone por tanto de una versión desmaterializada de su tarjeta bancaria que puede usar para un pago en campo cercano por medio de la tecnología NFC ("Near Field Contact", en inglés).

Esta nueva economía es una oportunidad para las instituciones bancarias pero también presenta riesgos de fraudes no insignificantes debido a la exposición de los datos bancarios, concretamente, el número de tarjeta bancaria, el criptograma de seguridad y la fecha de validez de la tarjeta. Los reacios a la tecnología de pago en campo cercano denuncian, concretamente, la vulnerabilidad de los datos bancarios durante la comunicación en campo cercano ya que los datos se transmiten sin cifrado. En particular, existen dispositivos de intercepción de los datos que pueden usarse durante una transacción.

Por otro lado, no es extraño que los piratas informáticos roben los datos bancarios del servidor de un comerciante en línea.

En respuesta a estos fraudes bancarios, las instituciones bancarias buscan soluciones para no exponer los datos bancarios de un abonado de tarjeta bancaria. En la actualidad existen sistemas de alojamiento de datos bancarios en servidores protegidos de los bancos y soluciones de generación de fichas de pago restrictivas (denominadas "payment token" en inglés) que se derivan de la tarjeta de pago de un abonado. Estas fichas son restrictivas en el sentido en el que pueden comprender restricciones de uso, por ejemplo, ser válidas en un periodo limitado, ante un único comerciante o estar limitadas a un montante máximo de transacción. Estas soluciones de pago se denominan HCE por "Host Card Emulation" en inglés (emulación de tarjeta de anfitrión). En caso de robo de los datos de la ficha, se reduce la exposición financiera.

Una arquitectura de HCE necesita un servidor de generación de fichas derivadas de una tarjeta bancaria mediante algoritmos de diversificación, servidores remotos de suministro de fichas en una aplicación bancaria alojada en el entorno operativo de un terminal portátil (teléfono celular o tableta, por ejemplo) y un servidor de verificación de la ficha que pueda determinar los datos bancarios de un abonado correspondiente a la ficha de pago.

En esta arquitectura, un abonado de una tarjeta bancaria puede disponer de una tarjeta bancaria en diversas formas, una tarjeta física de chip electrónico o de banda magnética, una tarjeta virtual alojada en un monedero electrónico en su teléfono portátil (habitualmente denominado "Mobile Wallet" en inglés) o una tarjeta virtual alojada en un servidor remoto (habitualmente denominado "Cloud Wallet" en inglés). Se conoce la solicitud de patente estadounidense US-20130200146A1 que describe una solución de alojamiento en un servidor remoto de una tarjeta bancaria virtual.

No obstante, aunque una ficha de pago presenta restricciones de uso, sigue estando expuesta al robo entre el momento en el que se suministra en un teléfono portátil y el momento de su uso. En efecto, el abonado puede prever suministrar en su teléfono un lote de fichas para múltiples pagos.

Además, los fabricantes de teléfonos y las instituciones bancarias desean proponer monederos electrónicos en un teléfono portátil desprendiéndose de las restricciones de un chip protegido y proponer una solución de pago totalmente de software. Una solución de este tipo está particularmente expuesta al robo de datos.

Por tanto, existe una necesidad de encontrar nuevas medidas de protección de las fichas de pago en un teléfono portátil, concretamente, cuando las fichas están alojadas fuera de un chip protegido.

El documento US-2012/040377-A1 del estado de la técnica describe un procedimiento de pago que usa un teléfono portátil. El documento US-2014/0279476-A1 del estado de la técnica describe un procedimiento de pago y una tarjeta de crédito.

La invención se refiere a un procedimiento de protección de una primera ficha derivada de un instrumento de pago de un abonado que puede estar alojado en un terminal móvil mediante una aplicación de pago.

Según la invención, el procedimiento comprende las siguientes etapas sucesivas:

- emparejar por un lado un identificador del terminal móvil y el instrumento de pago y por otro lado un criptograma personal y el instrumento de pago,

- suministrar la primera ficha a la aplicación de pago,

- recibir datos de una transacción de pago por la aplicación de pago,

- generar una segunda ficha de pago protegida mediante el cifrado de al menos la primera ficha, los datos de transacción, el identificador del terminal y el criptograma personal.

Más precisamente, el emparejamiento se realiza tras un protocolo de autenticación satisfactorio entre la aplicación de pago y un servidor remoto de autenticación.

Según una variante, el emparejamiento se realiza cuando el instrumento de pago se registra en la aplicación de pago.

Según una variante, la primera ficha es un dato aleatorio derivado de un dato que representa el número de cuenta bancaria vinculado al instrumento de pago.

Según una variante, el cifrado de la primera ficha se ejecuta por medio de una clave temporal recibida a partir de un servidor de generación de la ficha de pago.

Según una variante, el procedimiento comprende, además, la generación del identificador del terminal y del criptograma personal mediante la aplicación de pago, activándose la generación mediante la recepción de los datos de la transacción.

Según una variante, la generación del identificador del terminal y del criptograma personal mediante la aplicación de pago comprende la lectura en una memoria protegida del terminal condicionada a la introducción de una contraseña personal o, en otra variante, la ejecución de un cálculo criptográfico condicionada a la introducción de una contraseña personal.

Según una variante, la generación del identificador del terminal y del criptograma personal mediante la aplicación de pago se activa mediante una petición de autenticación del abonado durante la transacción de pago, siendo la transacción de pago una transacción de pago sin contacto según la norma ISO/IEC 14443.

Preferiblemente, durante la ejecución de la transacción bancaria, el identificador y el criptograma personal se memorizan en una memoria volátil del terminal.

Se prevé que el suministro de la primera ficha comprenda la escritura de la primera ficha en una memoria no volátil del terminal.

Según la invención, se prevé que un terminal móvil que comprende una aplicación de pago comprenda un agente de procesamiento de una primera ficha derivada de un instrumento de pago de un abonado y un medio de recepción de datos de una transacción de pago. La aplicación de pago comprende además:

- un medio de emparejamiento de un identificador del terminal móvil y de un criptograma personal con el instrumento de pago,

- y el agente de procesamiento de la ficha comprende un medio de generación de una segunda ficha de pago protegida mediante el cifrado de al menos la ficha, los datos de transacción, el identificador del terminal móvil y el criptograma personal.

Según una variante, la aplicación de pago comprende, además, un medio de generación del identificador del terminal móvil y del criptograma personal mediante la aplicación de pago.

También se prevé que la invención se refiera a un servidor de generación de una primera ficha que comprende un medio de generación de una primera ficha derivada de un instrumento de pago de un abonado, caracterizado por que comprende, además,

- un medio de emparejamiento de un identificador del terminal móvil y de un criptograma personal del abonado con el instrumento de pago,

- un medio de verificación de una segunda ficha de pago protegida generada mediante el cifrado de al menos la primera ficha, datos de transacción, el identificador del terminal móvil y el criptograma personal.

Según una variante, el identificador del terminal móvil y el criptograma personal del abonado se reciben a partir de un servidor de autenticación.

Según una variante, la primera ficha se genera por medio de un generador aleatorio en función de al menos un dato que representa el número de cuenta bancaria vinculado al instrumento de pago.

Gracias a la invención, el uso de la ficha de pago se protege mediante el emparejamiento previo con el usuario, mediante un criptograma personal, y con su terminal móvil, registrado mediante un identificador único. La integración de los datos de identificación del terminal y del usuario permite al servidor de verificación de la transacción bancaria controlar que la ficha se haya usado por el terminal y el usuario registrados.

Otras características y ventajas de la presente invención se desprenderán más claramente tras la lectura de la siguiente descripción detallada de realizaciones de la invención facilitadas a modo de ejemplos en absoluto limitativos e ilustradas mediante los dibujos adjuntos, en los que:

La Figura 1 representa el ecosistema de una arquitectura de pago de tipo HCE.

La Figura 2 representa el entorno operativo de software de un teléfono portátil para el alojamiento y la generación de una ficha de pago protegida.

La Figura 3 representa un flujo de secuencias para el emparejamiento de un usuario y de un terminal móvil antes del suministro y la generación de una ficha de pago al abonado.

La Figura 4 representa un flujo de secuencias durante la ejecución de una transacción bancaria y la generación de una ficha de pago protegida.

La invención se aplica en el contexto de un sistema de pago que suministra, a un abonado de un instrumento de pago, fichas de pago protegidas. Este sistema de pago se denomina habitualmente mediante el acrónimo HCE y las fichas de pago se denominan mediante el término “payment token” en inglés.

La Figura 1 representa el ecosistema de una solución de pago de tipo HCE. Se prevé una entidad 16 bancaria, un banco o un servicio de pago, que puede emitir un instrumento 17 de pago. El instrumento 17 de pago puede comprender varios productos de pago en forma de una tarjeta bancaria, de un servicio de pago en línea a través de un portal de Internet o de un servicio de pago por medio de fichas de pago que pueden suministrarse a un terminal 12 móvil del abonado.

El instrumento 17 de pago está definido:

- por datos bancarios del abonado, tales como un número de cuenta vinculado al instrumento de pago y datos personales,

- por criterios de uso del instrumento de pago, concretamente, un periodo de validez, una zona geográfica, un límite de transacción,

- y por datos de protección, tales como, por ejemplo, el criptograma de seguridad o mecanismos de seguridad electrónicos a bordo de una tarjeta de pago que permiten la verificación de los datos de una transacción bancaria.

En el caso de un terminal 12 móvil destinado a recibir fichas de pago, los mecanismos de seguridad pueden estar alojados en un módulo protegido soldado al terminal, por ejemplo, un circuito integrado de tipo NFC, o estar alojados a nivel de un entorno protegido (denominado TEE, por “Trusted Execution Environment” en inglés, [entorno de ejecución de confianza]). En este último caso se trata de una solución totalmente en software en la que se considera que la zona de aplicación del entorno operativo del terminal móvil que ejecuta una aplicación de pago es de confianza mediante diversos mecanismos de seguridad. Estos mecanismos pueden ser la verificación de la zona de memoria o protocolos de autenticación con un servidor 10 remoto de autenticación para la instalación de aplicaciones o de perfiles de pago. A continuación se estudiarán en más detalle las funciones del terminal 12 móvil que puede generar la ficha 104 de pago protegida en el contexto de la invención.

Preferiblemente, el terminal 12 móvil comprende medios de comunicación para recibir y emitir datos a distancia a través de la red telefónica celular, una red de datos de tipo IP a través de la red telefónica o una red de datos de tipo IP a través de una red de medio alcance, por ejemplo WIFI.

En el contexto de la invención se prevé un servidor 10 de autenticación gestionado por la institución 16 bancaria o por un operador tercero de servicios de autenticación. El servidor 10 de autenticación intercambia medios 102 criptográficos con el terminal 12 móvil. Estos medios 102 criptográficos son, por ejemplo, claves criptográficas de sesiones, números de transacción temporales o algoritmos de criptografía que permiten realizar un protocolo de

intercambio protegido. Estos medios criptográficos se intercambian a través de un canal protegido que puede ser un protocolo de comunicación de HTTPS (“Hyper Text Transfert Protocol Secure” en inglés, [protocolo seguro de transferencia de hipertexto]), CAT_TP (“Card Application Toolkit Transport Protocol” [protocolo de transporte de kit de herramientas de aplicación de tarjeta]) o SMS (“Short Message Service” [servicio de mensajes cortos]).

Por otro lado, el servidor 10 de autenticación puede intercambiar información con la entidad 16 bancaria a través de una red protegida de comunicación de datos a distancia inalámbrica o a través de una red de comunicación por cable si el servidor 10 de autenticación se hace funcionar por la entidad 16 bancaria. Por tanto, la entidad 16 bancaria puede transmitir datos personales y bancarios de un abonado al servidor 10 de autenticación para las necesidades de los protocolos de autenticación entre el terminal 12 móvil del abonado y el servidor de autenticación.

También se prevé un servidor 11 de generación de fichas 103 derivadas del instrumento 17 de pago. El servidor 11 comprende medios criptográficos para generar una ficha 103 a partir de datos 105 bancarios vinculados al instrumento 17 de pago.

Un generador de datos aleatorios puede generar una ficha 103 a partir de los datos 105 bancarios y de un medio de diversificación o derivación, por ejemplo un contador. Pueden ponerse en práctica otros medios de diversificación para la generación de la ficha 103 en el servidor 11.

Se observará que se prevé que los datos 105 bancarios empleados por el generador de datos aleatorios pueden recuperarse por el servidor 11 de generación de fichas o por un servidor de verificación asociado basándose en información de la ficha 104 de pago protegida. De este modo, los datos bancarios se protegen y se mantienen secretos en el servidor 11.

Por otro lado, el servidor 11 de generación de la ficha 103 puede intercambiar información con la entidad 16 bancaria a través de una red protegida de comunicación de datos a distancia inalámbrica o a través de una red de comunicación por cable si el servidor 11 de autenticación se hace funcionar por la entidad 16 bancaria. Por tanto, la entidad 16 bancaria puede transmitir datos personales y bancarios de un abonado al servidor 10 de autenticación para las necesidades de los protocolos de autenticación entre el terminal 12 móvil del abonado y el servidor de autenticación.

Además, el servidor 11 de generación de ficha puede intercambiar información con el servidor 10 de autenticación a través de una red protegida de comunicación de datos a distancia inalámbrica o a través de una red de comunicación por cable si los servidores 10 y 11 se gestionan por el mismo operador. El servidor 10 de autenticación intercambia medios 101 criptográficos con el servidor 11 de generación de las fichas 103. Estos medios 101 criptográficos son, por ejemplo, claves criptográficas de sesiones, números de transacción temporales o algoritmos de criptografía que permitan realizar un protocolo de intercambio protegido con el terminal 12.

El protocolo de intercambio protegido con el terminal 12 permite concretamente intercambiar fichas 103 a través de un canal protegido que puede ser un protocolo de comunicación de tipo HTTPS, CAT_TP o SMS.

Puede preverse una red 15 protegida de pago para transmitir los datos bancarios de los abonados y los datos de transacciones bancarias respetando las especificaciones de las normas EMV, por ejemplo los datos de transacción convencionales y las fichas de pago protegidas. La red 15 protegida de pago se hace funcionar por un operador 14 de servicio de pago encargado de realizar las transacciones bancarias de pago.

El operador de servicio de pago usa la red 15 protegida para transmitir los datos de transacción recibidos a partir de los comerciantes 13, por medio de un terminal de pago o un servidor remoto de pago. La red 15 usa una red de comunicación inalámbrica o por cable protegida entre los terminales de pago.

La Figura 2 describe más precisamente el terminal 12. Comprende una aplicación 24 de pago, alojada por el entorno operativo del terminal 12 móvil o en un módulo protegido, por ejemplo eUICC (por “Embedded Universal Integrated Circuit Card”, [tarjeta de circuito integrado universal incorporada]).

El terminal 12 móvil comprende memorias no volátiles, de tipo ROM (“Read Only Memory” en inglés, [memoria de sólo lectura]), EEPROM “Elecrtically Erasable Read Only Memory” [memoria de sólo lectura borrable eléctricamente] o FLASH para la grabación de parámetros y del código de ejecución de aplicaciones y del programa informático que comprenda las instrucciones para la puesta en práctica del procedimiento de protección de las fichas de pago, por ejemplo, el entorno operativo del terminal, aplicaciones o bibliotecas de funciones específicas que puedan usarse por las aplicaciones.

El terminal comprende concretamente bibliotecas de funciones, clases o métodos, denominadas API por “Application Progamming Interface” en inglés, (interfaz de programación de aplicaciones), para los intercambios con el servidor 11 de generación de fichas, para la ejecución de transacciones de pago con un terminal 13 de pago y

para la autenticación con el servidor 10 de autenticación. La aplicación 24 puede recurrir a las funciones proporcionadas por las API.

El terminal móvil también comprende una memoria de acceso aleatorio, de tipo RAM (“Random Acess Memory” en inglés) para la grabación de parámetros temporales, por ejemplo, de los datos de transacción bancaria o una ficha 104 de pago protegida. La memoria de acceso aleatorio comprende registros adaptados para la grabación de variables y parámetros creados durante la ejecución del programa informático que comprende las instrucciones para la puesta en práctica del procedimiento de protección de las fichas de pago durante su ejecución.

El terminal 12 comprende además interfaces hombre-máquina para la introducción y la visualización de datos con el abonado, por ejemplo, para la introducción de un código personal (código PIN en inglés, “Personal Identification Number”, [número de identificación personal]) y para la interacción con la aplicación 24 de pago. Se prevé que la aplicación de pago visualice peticiones en una pantalla del terminal móvil, por ejemplo, una petición de acercar el terminal 12 al terminal 13 de pago, una petición de introducir un código personal o una petición de elegir un instrumento de pago.

El terminal móvil comprende el procesador de cálculo para la ejecución de las funciones de las aplicaciones del terminal 12 móvil.

La aplicación 24 de pago comprende un agente 23 de procesamiento de una ficha 103 derivada de un instrumento 17 de pago de un abonado y un medio 25 de recepción de datos de una transacción de pago. El agente 23 de procesamiento es una función de la aplicación 24 de pago que permite la recepción de la ficha 103 enviada a partir del servidor 11 de generación de fichas y su memorización en una memoria no volátil del terminal móvil. El agente 23 de procesamiento es una aplicación de software que emplea las funciones de software API que permiten interaccionar con el servidor 11 de generación de la ficha 103.

Por otro lado, la aplicación 24 de pago aloja uno o varios instrumentos 17 de pago. Una tarjeta virtual se registra en forma de una aplicación específica del perfil de la tarjeta de pago y puede memorizarse por medio de un identificador de aplicación.

El instrumento de pago se registra en la aplicación de pago previamente al primer suministro de una ficha de pago.

El medio 25 de recepción de datos de transacción bancaria es una función de la aplicación 24 de pago que permite la comunicación con el terminal 13 de pago. La función de recepción puede controlar un protocolo de intercambio sin contacto según la norma ISO/IEC 14443, grabar los datos de la transacción en una memoria y devolver las respuestas al terminal 13 de pago.

Además, la aplicación 24 de pago comprende un medio 26 de emparejamiento de un identificador 22 del terminal móvil y de un criptograma 21 personal con el instrumento de pago. Se trata de una función que recurre a funciones de software API para la autenticación con el servidor 10 de autenticación y el servidor 11 de generación de ficha. El emparejamiento comprende, concretamente, medios para generar el identificador 22 atribuido al terminal 12 y el criptograma 21 personal atribuido al abonado.

El identificador 22 del terminal puede generarse por el servidor 10 de autenticación y transmitirse al terminal 12 para grabarse de manera protegida, por ejemplo, cifrado por medio de una clave. En otra variante, el identificador 22 puede ser el número IMEI (“International Mobile Equipment Identity” en inglés, [identidad internacional de equipo móvil]) del terminal 12 y transmitirse al servidor 10 de autenticación. Puede transmitirse por el terminal 12 durante el emparejamiento o por la entidad 16 bancaria.

El criptograma 21 personal puede ser una contraseña, un código personal o una huella biométrica digital conocido por el abonado y por el servidor de autenticación. El criptograma personal también puede generarse mediante una función tras una autenticación satisfactoria de código PIN o autenticación biométrica. En una variante, el criptograma 21 personal puede generarse a partir de un valor aleatorio conocido únicamente por el terminal 12 y por el servidor de autenticación o de una clave de cifrado. Métodos conocidos denominados salado también permiten generar el criptograma 21 personal a la vez mediante la aplicación 24 de pago y a la vez mediante el servidor 10 de autenticación.

El emparejamiento es efectivo cuando la aplicación 24 de pago ha vinculado un instrumento 17 de pago con el identificador 22 del terminal y el criptograma 21 personal.

Asimismo, el servidor 11 de generación vincula el identificador 22 y el criptograma 21 con el instrumento 17 de pago. El identificador 22 del terminal 12 y el criptograma 21 personal que permiten el emparejamiento en el servidor 11 se transmiten por el servidor 10 de autenticación, el cual ha realizado previamente de manera satisfactoria el protocolo de autenticación con el terminal 12 y el abonado.

El emparejamiento se realiza preferiblemente durante el registro del instrumento 17 de pago en el terminal móvil. El registro corresponde a la instalación de un perfil de pago digital en la memoria no volátil del terminal 12 móvil.

El emparejamiento del terminal se protege mediante la autenticación con el servidor 10 de autenticación.

Además, el agente 23 de procesamiento de una ficha 103 comprende un medio de generación de una ficha 104 de pago protegida mediante el cifrado de al menos la ficha 103, los datos de transacción, el identificador 22 del terminal móvil y el criptograma 21 personal. Una clave de cifrado de la ficha y un algoritmo de cifrado de tipo HMAC (por "keyed-hash message authentication code" en inglés, [código de autenticación de mensajes basado en resumen criptográfico]), por ejemplo, según las recomendaciones de OATH ("Initiative for Open Authentication"), se usan para la ejecución del cifrado y obtener la ficha 104 de pago protegida. El algoritmo de cifrado permite una autenticación mutua con el servidor 11 de generación de ficha. La clave de cifrado se transmite a la aplicación 24 de pago por el servidor 11 de generación de ficha. La clave se memoriza en una zona protegida del terminal móvil, cifrada o no cuando no se usa. La clave de cifrado puede ser temporal. Puede estar asociada a una única ficha 103 de pago, a un lote de fichas 103 de pago o estar limitada en el tiempo.

Más precisamente, los datos de la ficha 103, los datos de transacción del terminal 13 de pago (montante de la transacción, número de transacción), el identificador 22 del terminal y el criptograma 21 personal se concatenan en un bloque de datos (que puede alcanzar, por ejemplo, 128 bits). A continuación se cifran estos datos concatenados mediante el algoritmo de cifrado por medio de la clave de cifrado. La ficha 104 de pago protegida generada mediante la aplicación 24 de pago se presenta en forma de un criptograma que acompaña a una petición de verificación de una transacción bancaria que comprende al menos los datos de la transacción.

Se observará que la generación de la ficha 104 de pago protegida puede realizarse en modo fuera de línea, es decir que una conexión con el servidor 11 de generación de la ficha 103 no es necesaria durante la transacción.

Por otro lado, el agente 23 de procesamiento comprende un medio de inserción de la ficha 104 de pago protegida en un protocolo de transacción bancaria convencional. Puede insertarse en un campo de datos normalizado en los protocolos de transacción de EMV ("Europay MasterCard Visa", marcas registradas), por ejemplo.

Por tanto, la ficha 104 de pago protegida puede transmitirse por un terminal de pago sin modificación de su protocolo de comunicación con la red 15 de pago.

El servidor 11 de generación de una ficha 103 comprende un medio de generación de una ficha derivada a partir del instrumento 17 de pago. La ficha derivada es un dato aleatorio. La ficha 103 se genera a partir de los datos 105 bancarios del instrumento 17 de pago (número de cuenta asociado) y de un diversificador. El diversificador representa una autorización para una transacción de pago con criterios de restricción de uso determinados por el servidor 11, por ejemplo, una validez para una o varias transacciones bancarias, una validez temporal, una validez para un límite de transacción.

En el contexto de la invención, el servidor 11 comprende, además, un medio de emparejamiento del identificador 22 del terminal móvil y del criptograma 21 personal del abonado con el instrumento 17 de pago. Comprende, concretamente, en sus bases de datos bancarias, los datos 105 bancarios asociados al instrumento 17 de pago (número de cuenta asociado) y el identificador 22 del terminal 12 y el criptograma 21 personal del abonado que se atribuyen al instrumento 17 de pago.

Además, comprende un medio de verificación de la ficha 104 de pago protegida generada mediante el cifrado de al menos la ficha 103, los datos de transacción, el identificador 22 del terminal móvil y el criptograma 21 personal. Comprende, concretamente, los medios criptográficos complementarios a los de la aplicación 24 de pago para generar una segunda ficha con fines de verificación, en función de los datos de transacción transmitidos por la petición de verificación de una transacción bancaria. Los medios de verificación comprenden un medio de generación de un criptograma de verificación mediante el cifrado de al menos la ficha 103, los datos de transacción, el identificador 22 del terminal móvil y el criptograma 21 personal. Una comparación de la ficha 104 de pago protegida con el criptograma de verificación permite autorizar o no la transacción.

Se observará que el identificador del terminal 22 móvil y el criptograma 21 personal del abonado se reciben a partir del servidor 10 de autenticación o pueden generarse de manera dinámica durante la recepción de la ficha 104 de pago protegida para una verificación de la transacción bancaria.

La Figura 3 representa un flujo de secuencias de etapas para el emparejamiento de un instrumento de pago con un identificador 22 del terminal 12 y un criptograma 21 personal. El emparejamiento se realiza durante el registro del instrumento 17 de pago en la aplicación 24 de pago del terminal 12 del abonado.

En una etapa 31 de petición de registro, el abonado, a través de su aplicación 24 de pago, procede a su registro para el uso del instrumento 17 de pago. La petición de registro se transmite a la entidad 16 bancaria operadora del instrumento de pago.

En una variante, la etapa 31 de petición de registro puede realizarse a través de un portal web o directamente en la agencia de la entidad bancaria.

La entidad 16 bancaria inicia una solicitud de registro en una etapa 32. Durante la etapa 32, pueden generarse identificadores y una contraseña personal de un único uso y transmitirse al abonado para iniciar una autenticación ante el servidor 10 de autenticación. En paralelo, se comunican los identificadores y la contraseña al servidor 11 de generación de una ficha de pago durante una etapa 33 y después al servidor 10 de autenticación durante una etapa 34.

Durante la etapa 33, la entidad 16 bancaria también transmite los datos bancarios del instrumento 17 de pago permitiendo la realización de un pago (concretamente, número de cuenta bancaria y criterios de restricción).

Durante la etapa 35, el servidor 10 de autenticación inicia un protocolo de autenticación en espera de recibir una petición de emparejamiento procedente de la aplicación 24 de pago del usuario. Se preparan juegos de claves de cifrado y de identificadores de transacción de autenticación para permitir la transmisión protegida de un identificador de terminal y de un criptograma personal entre la aplicación de pago y el servidor de autenticación.

Durante una etapa 37, la aplicación 24 de pago inicia una solicitud de emparejamiento y ejecuta las operaciones de descifrado y cifrado necesarias para la realización de las peticiones y respuestas que intervienen en el protocolo 36 de autenticación.

En paralelo, el servidor 10 de autenticación, en una etapa 38, ejecuta las operaciones complementarias para la realización del protocolo de autenticación para el emparejamiento 36 entre un identificador del terminal móvil y el instrumento de pago y un criptograma personal del abonado y el instrumento de pago.

En una variante, el protocolo de autenticación puede iniciarse mediante el servidor de autenticación en dirección a la aplicación 24 de pago.

Durante el protocolo de autenticación correspondiente a la ejecución del emparejamiento 36, se generan el identificador 22 del terminal 12 y el criptograma 21 personal, o bien por el servidor 10 o bien por la aplicación 24 de pago, y se intercambian mutuamente.

Se observará que el emparejamiento 36 comprende la memorización del identificador 22 del terminal y del criptograma 21 personal en el servidor 10 de autenticación o la memorización de funciones de cálculo para la generación del identificador 22 del terminal y del criptograma 21 personal en el servidor 10 de autenticación.

En una variante, el identificador 22 del terminal y el criptograma 21 personal se generan de manera dinámica durante cada transacción bancaria. La aplicación 24 de pago y el servidor 10 disponen de medios de generación que se intercambian durante la fase 36 de autenticación. Esto puede ser una aplicación de autenticación específica y los algoritmos criptográficos. Estos medios de generación del identificador 22 y del criptograma 21 personal pueden obtenerse igualmente a través de un portal de aplicación o estar ya instalados con la aplicación 24 de pago.

La aplicación 24 de pago se instala mediante un protocolo de instalación protegido que comprende la instalación de un perfil de una aplicación bancaria en un módulo protegido NFC para la realización de transacciones bancarias según la norma ISO/IEC 14443.

Cuando el protocolo de autenticación, para la operación de emparejamiento 36, se termina de manera satisfactoria, durante una etapa 39, el servidor 10 de autenticación comunica al servidor 11 de generación de la ficha 103 de pago el identificador 22 del terminal y el criptograma 21 personal de entre los medios 101 criptográficos. Esto se realiza con fines de verificación de las transacciones de pago usando las fichas de pago.

En la etapa 40, el servidor 11 instala el identificador 22 del terminal y el criptograma 21 personal o los medios de generación asociados al instrumento 17 de pago del abonado.

En una etapa 41, se informa a la entidad 16 bancaria de la autenticación satisfactoria y del emparejamiento para el funcionamiento de la solución de pago por medio de la ficha de pago protegida.

La Figura 4 representa un flujo de secuencias durante la generación de una ficha 104 de pago protegida a lo largo de una transacción bancaria.

En una primera etapa 50, la aplicación 24 de pago procede a una petición de suministro de una ficha. Se realiza una etapa de autenticación del abonado con el servidor 10 de autenticación. Mediante la verificación de un identificador y contraseña personal, o, en una variante, por medio del identificador 22 del terminal 12 y del criptograma 21 personal generados durante la etapa de emparejamiento.

Si la autenticación resulta satisfactoria con el servidor 10 de autenticación, la aplicación 24 realiza, en una etapa 51, una solicitud de suministro de una ficha 103 ante el servidor 11 de generación de ficha. La solicitud de suministro se realiza a través de un canal de comunicación protegido entre la aplicación 24 de pago y el servidor 11, por ejemplo, un protocolo de comunicación de tipo HTTPS, CAT_TP o SMS.

Durante la etapa 52, el servidor 11 de generación de ficha genera una primera ficha 103 derivada a partir del instrumento 17 de pago. La ficha 103 es un dato aleatorio derivado de un dato 105 que representa el número de cuenta bancaria vinculado al instrumento 17 de pago. Este dato puede ser el número de cuenta bancaria. La ficha 103 es un dato aleatorio definido mediante criterios de restricción de uso, por ejemplo, un número de transacción bancaria, una duración de validez o un montante de la transacción. Preferiblemente, se usa un generador aleatorio en función de al menos el dato 105 que representa el número de cuenta bancaria vinculado al instrumento 17 de pago. Un contador que proporciona un dato de entrada al generador permite diversificar el dato 105.

En una etapa 53, el servidor 11 transmite la ficha 103 a la aplicación 24 de pago a través del mismo canal protegido usado durante la etapa 51.

En una etapa 54, la aplicación 24 de pago memoriza la ficha 103 en una zona de memoria protegida (no volátil) del terminal 12 móvil. El agente 23 de procesamiento graba la ficha 103 en una zona de memoria cuyo acceso está condicionado a una autenticación con el servidor 10 de autenticación. En una variante, la ficha 103 se transmite cifrada en espera de un uso por medio de una clave proporcionada por el servidor 11.

Durante una etapa 55, se inicia un protocolo de transacción bancaria con un terminal 13 de pago. La aplicación 24 recibe peticiones de transacción y emite respuestas a esas peticiones. La transacción realizada es una transacción de pago NFC sin contacto en campo cercano, por ejemplo, según la norma ISO/IEC 14443. Durante un primer intercambio, pueden transmitirse datos de transacción, por ejemplo un montante de transacción.

En una etapa 56, la aplicación 24 de pago procede a la generación del identificador 22 del terminal y del criptograma 21 personal. La generación puede ser una lectura en una memoria protegida del terminal 12 o la generación de los datos mediante cálculos criptográficos, por ejemplo, un descifrado o cifrado. La generación 56 está, preferiblemente, condicionada a la introducción y la verificación de una contraseña personal (código PIN, frase, lectura de un dato biométrico de tipo huella digital o lectura del iris).

Durante la generación 56, el identificador 22 y el criptograma 21 pueden memorizarse en una memoria volátil del terminal 12 durante la ejecución de la transacción bancaria. Después de la realización de la transacción bancaria, a continuación se borran para no estar expuestos a eventuales defraudadores.

Se observará que la generación 56 del identificador 22 del terminal y del criptograma 21 personal puede activarse mediante una petición de autenticación del abonado durante una transacción de pago sin contacto, según la norma ISO/IEC 14443.

En una etapa 57, la aplicación 24 de pago realiza la generación de una segunda ficha 104 de pago protegida. La aplicación 24 de pago realiza el cifrado de al menos la primera ficha 103, los datos de transacción, el identificador 22 del terminal y el criptograma 21 personal. La aplicación 24 usa el algoritmo de cifrado del agente 23 de procesamiento de la ficha para generar la ficha 104 de pago protegida. El algoritmo de cifrado tiene como consecuencia hacer que la ficha 104 de pago protegida sea única por cada terminal 12 y única por cada abonado.

Si la ficha 104 de pago se usa por otro terminal, que no se haya registrado durante el emparejamiento previo y que no esté en condiciones de reproducir el identificador 22 del terminal, el servidor 11 de verificación de la ficha 104 de pago protegida puede detectar la situación y denegar la transacción bancaria.

Asimismo, si la ficha 104 de pago se usa por otro abonado, que no se haya registrado durante el emparejamiento previo y que no esté en condiciones de reproducir el criptograma 21 personal, el servidor 11 de verificación de la ficha 104 de pago protegida puede detectar la situación y denegar la transacción bancaria.

Opcionalmente, el formato de la ficha 104 de pago protegida puede modificarse, por ejemplo, mediante una función de resumen criptográfico, para insertarse a continuación en un campo de datos según una transacción bancaria.

A continuación, durante una etapa 58 se transmite la ficha 104 de pago protegida al terminal 13 de pago durante la ejecución de la transacción bancaria. Se transmite en campo cercano mediante los medios de comunicación NFC, acompañada por datos de la transacción bancaria, tal como se realiza convencionalmente en la norma EMV.

A continuación, el terminal 13 de pago transmite la ficha 104 de pago protegida al servidor 11 de generación de la ficha 103 de pago con fines de verificación de la transacción a través de la red 15 de pago. El servidor 11 de verificación puede ser distinto del servidor 11 de generación de la ficha.

Puede preverse que un mismo abonado realice un emparejamiento con un segundo terminal móvil, por ejemplo, una tableta multimedia, si el primer terminal móvil es un teléfono celular. Se prevé, durante el emparejamiento con el segundo terminal móvil, que el servidor 10 asocie al instrumento 17 de pago el segundo terminal, con un segundo identificador de terminal. El criptograma 21 personal puede ser idéntico.

Cuando el servidor de verificación recibe la ficha 104 de pago protegida, realiza el mismo cálculo criptográfico que el agente 23 de procesamiento de la aplicación 24 de pago. Una vez validada, se transmite la orden de autorización con los datos 105 bancarios del instrumento 17 asociado a la ficha 103 a la entidad 16 bancaria a través de la red 15 de pago.

Se observará que la primera ficha 103, transmitida por el servidor 11 al terminal 12, puede usarse para varias transacciones de pago. Su uso puede estar restringido para una duración determinada, un número de transacciones de pago o un montante de transacción que pueda ser la suma de varias transacciones de pago.

REIVINDICACIONES

1. Procedimiento de protección de una primera ficha (103) derivada de un instrumento (17) de pago de un abonado que puede estar alojado en un terminal (12) móvil mediante una aplicación (24) de pago, caracterizado por que comprende las siguientes etapas sucesivas:

- emparejar (36) por un lado un identificador (22) del terminal (12) móvil y el instrumento de pago y por otro lado un criptograma (21) personal y el instrumento de pago,
- suministrar (53) la primera ficha (103) a la aplicación (24) de pago,
- recibir (55) datos de una transacción de pago por la aplicación de pago,
- generar (57) una segunda ficha (104) de pago protegida mediante el cifrado de al menos la primera ficha (103), los datos de transacción, el identificador (22) del terminal y el criptograma (21) personal,

caracterizado por que:

- el emparejamiento (36) se realiza cuando el instrumento (17) de pago se registra en la aplicación (24) de pago,
- la primera ficha (103) es un dato aleatorio derivado de un dato (105) que representa el número de cuenta bancaria vinculado al instrumento (17) de pago.

2. Procedimiento según la reivindicación 1, caracterizado por que el emparejamiento (36) se realiza tras un protocolo de autenticación satisfactorio entre la aplicación (24) de pago y un servidor (10) remoto de autenticación.

3. Procedimiento según una cualquiera de las reivindicaciones anteriores, caracterizado por que el cifrado de la primera ficha (103) se ejecuta por medio de una clave temporal recibida a partir de un servidor (11) de generación de la primera ficha (103).

4. Procedimiento según una cualquiera de las reivindicaciones anteriores, caracterizado por que comprende, además, la generación (56) del identificador (22) del terminal y del criptograma (21) personal mediante la aplicación (24) de pago, activándose la generación mediante la recepción (55) de los datos de la transacción.

5. Procedimiento según la reivindicación 4, caracterizado por que la generación del identificador (22) del terminal y del criptograma (21) personal mediante la aplicación (24) de pago comprende la lectura en una memoria protegida del terminal (12) condicionada a la introducción de una contraseña personal o la ejecución de un cálculo criptográfico condicionada a la introducción de una contraseña personal.

6. Procedimiento según las reivindicaciones 4 o 5, caracterizado por que la generación del identificador (22) del terminal y del criptograma (21) personal mediante la aplicación (24) de pago se activa mediante una petición de autenticación del abonado durante la transacción de pago, siendo la transacción de pago una transacción de pago sin contacto según la norma ISO/IEC 14443.

7. Procedimiento según una cualquiera de las reivindicaciones 4 a 6, caracterizado por que, durante la ejecución de la transacción bancaria, el identificador (22) y el criptograma (21) personal se memorizan en una memoria volátil del terminal (12).

8. Procedimiento según una cualquiera de las reivindicaciones anteriores, caracterizado por que el suministro comprende la escritura de la primera ficha (103) en una memoria no volátil del terminal (12).

9. Terminal móvil que comprende una aplicación de pago que comprende un agente (23) de procesamiento de una primera ficha (103) derivada de un instrumento (17) de pago de un abonado y un medio de recepción de datos de una transacción de pago, caracterizado por que la aplicación (24) de pago comprende, además:

- un medio (26) de emparejamiento de un identificador (22) del terminal móvil y de un criptograma (21) personal con el instrumento de pago,
- y por que el agente de procesamiento de la primera ficha (23) comprende un medio de generación de una segunda ficha (104) de pago protegida mediante el cifrado de al menos la primera ficha (103), los datos de transacción, el identificador (22) del terminal móvil y el criptograma (21) personal,

caracterizado por que:

- el emparejamiento (36) se realiza cuando el instrumento (17) de pago se registra en la aplicación (24) de pago,
- la primera ficha (103) es un dato aleatorio derivado de un dato (105) que representa el número de cuenta bancaria vinculado al instrumento (17) de pago.

10. Terminal según la reivindicación 9, caracterizado por que comprende, además, un medio de generación del identificador (22) del terminal (12) móvil y del criptograma (21) personal mediante la aplicación (24) de pago.

11. Servidor de generación de una primera ficha (11) que comprende un medio de generación de una primera ficha (103) derivada de un instrumento (17) de pago de un abonado, caracterizado por que comprende, además,

- un medio de emparejamiento de un identificador (22) del terminal (12) móvil y de un criptograma (21) personal del abonado con el instrumento (17) de pago,
- un medio de verificación de una segunda ficha (104) de pago protegida generada mediante el cifrado de al menos la primera ficha (103), datos de transacción, el identificador (22) del terminal móvil y el criptograma (21) personal,

caracterizado por que:

- el emparejamiento (36) se realiza cuando el instrumento (17) de pago se registra en la aplicación (24) de pago,
- la primera ficha (103) es un dato aleatorio derivado de un dato (105) que representa el número de cuenta bancaria vinculado al instrumento (17) de pago.

12. Servidor según la reivindicación 11, caracterizado por que el identificador (22) del terminal móvil y el criptograma (21) personal del abonado se reciben a partir de un servidor (10) de autenticación.

13. Servidor según las reivindicaciones 11 o 12, caracterizado por que la primera ficha (103) se genera por medio de un generador aleatorio en función de al menos un dato (105) que representa el número de cuenta bancaria vinculado al instrumento (17) de pago.

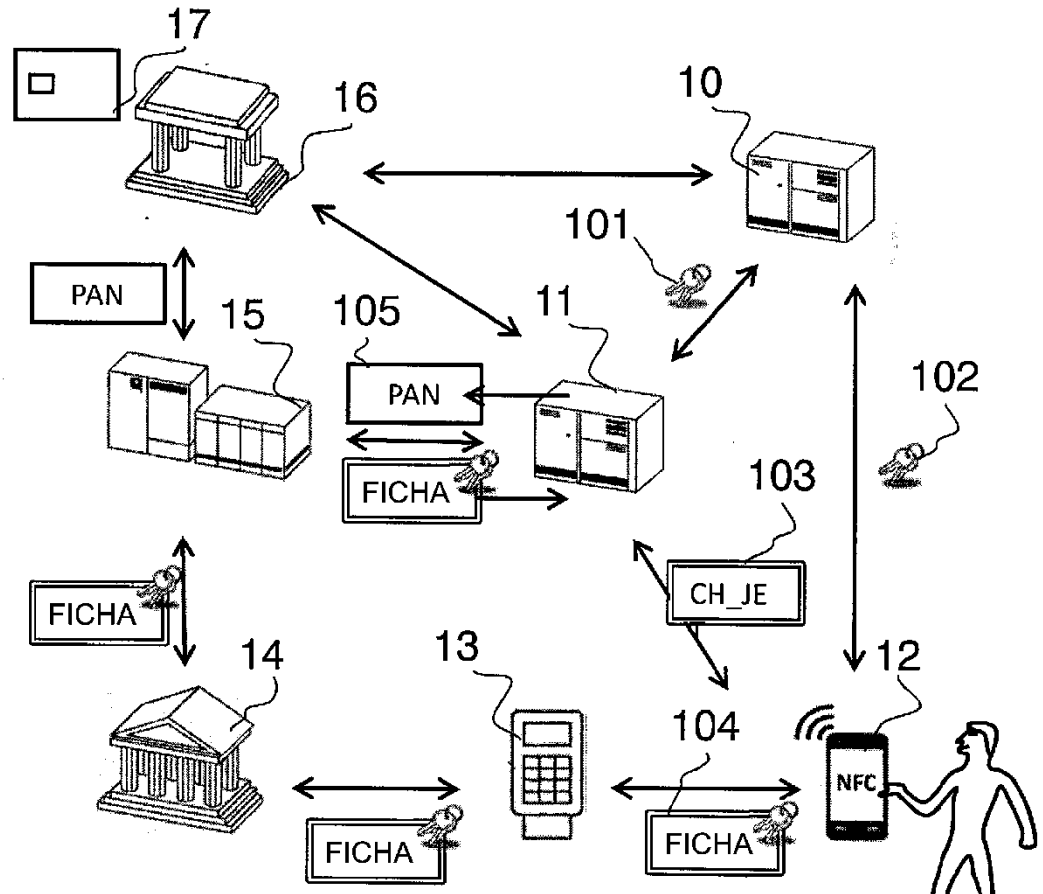
17
16
10
101
PAN
15
105
11
PAN
FICHA
102
103
CH_JE
FICHA
14
13
12
104
NFC
FICHA
FICHA

Fig. 1

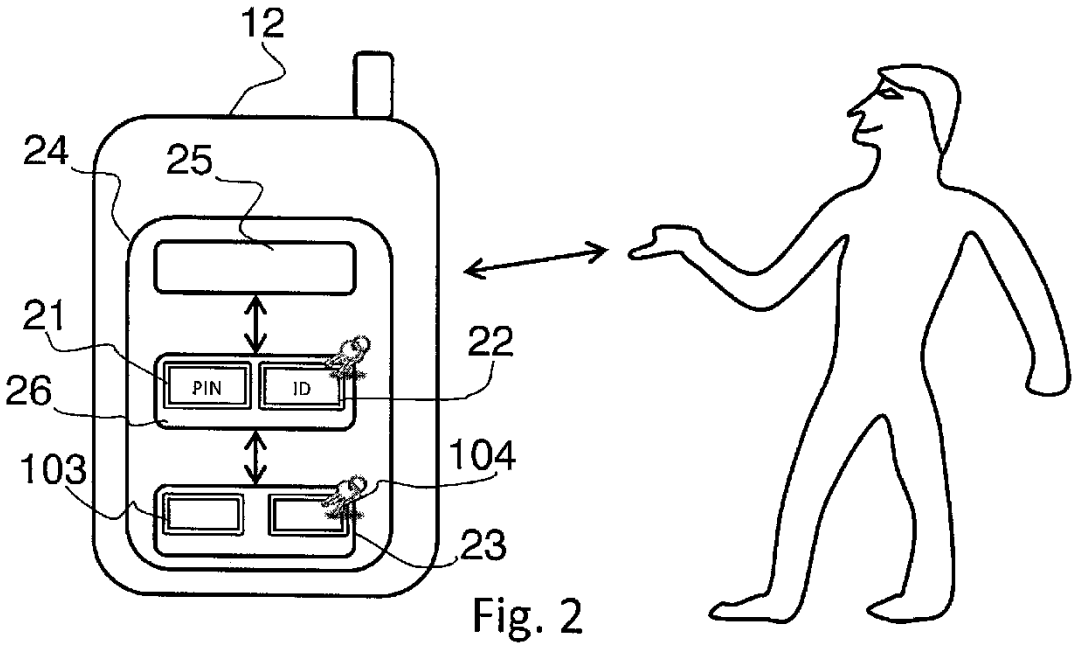
12
24
25
21
22
PIN
ID
26
104
103
23

Fig. 2

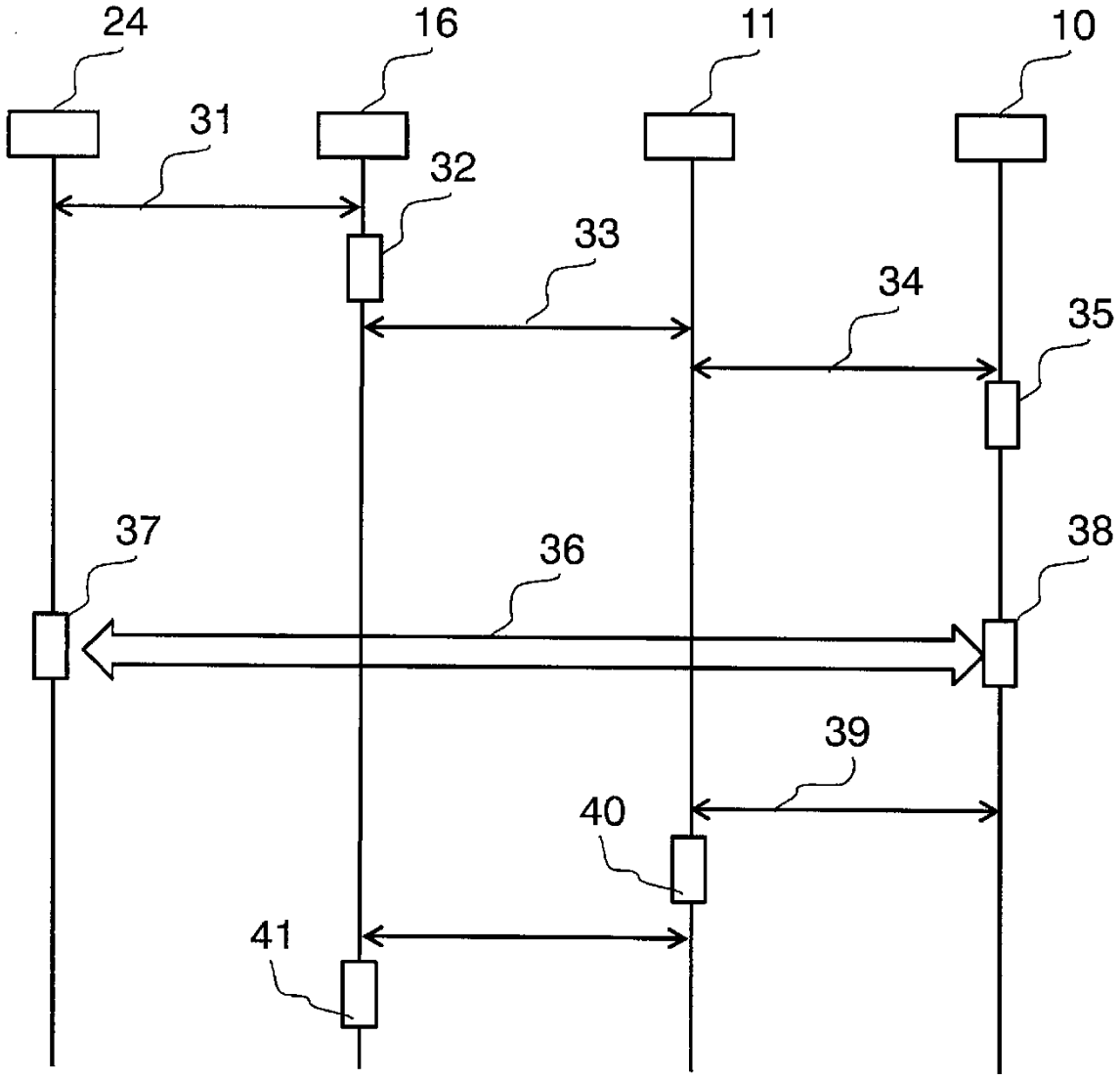

Fig. 3

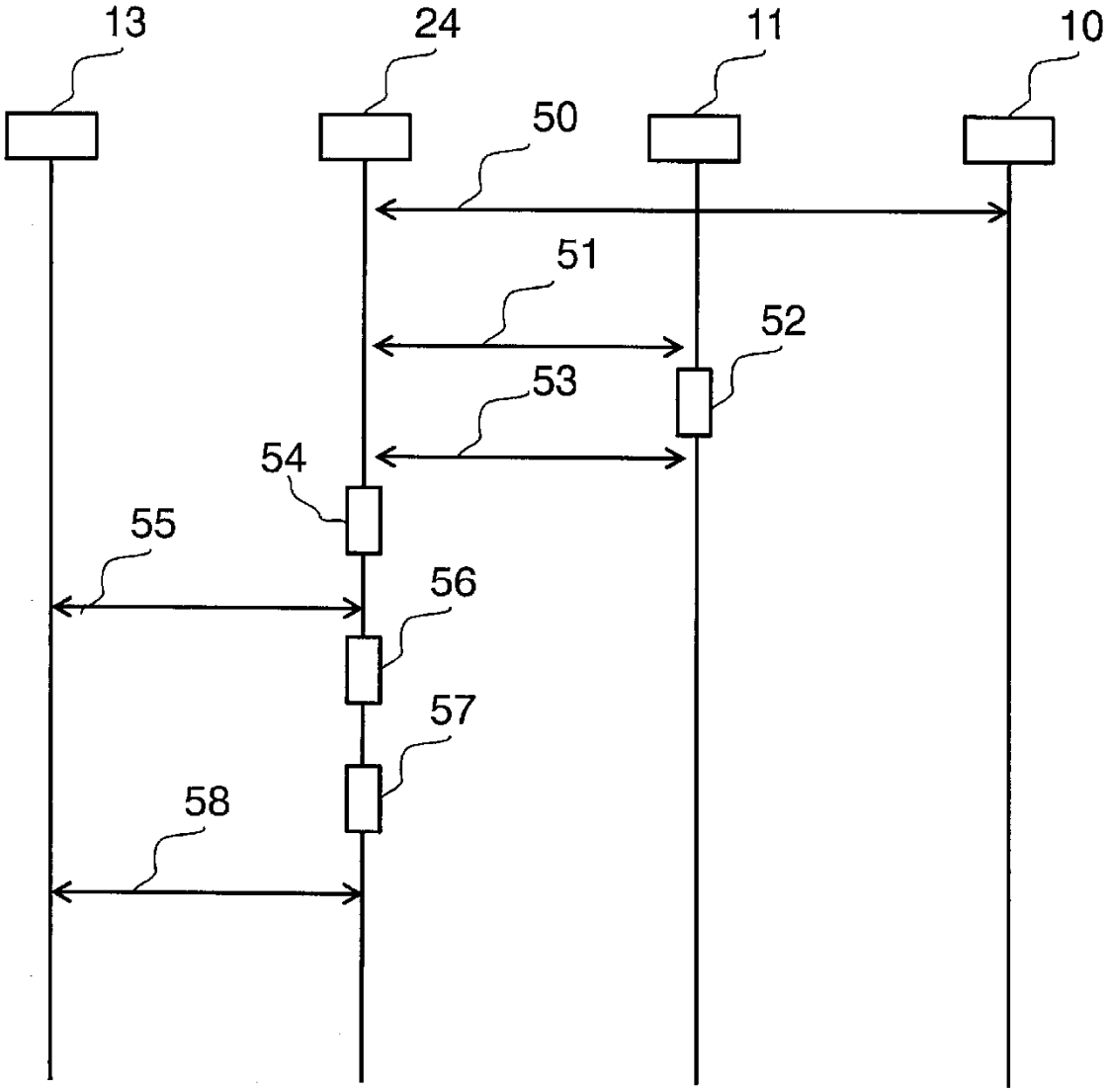

Fig. 4