(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 896 274**

(51) Int. CI.:

G06Q 20/32 (2012.01)
G06Q 20/38 (2012.01)
G06F 21/32 (2013.01)
G06F 21/60 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **20.10.2016 PCT/EP2016/075258**

(87) Fecha y número de publicación internacional: **22.06.2017 WO17102142**

(96) Fecha de presentación y número de la solicitud europea: **20.10.2016 E 16787776 (0)**

(97) Fecha y número de publicación de la concesión europea: **18.08.2021 EP 3391266**

(54) Título: **Método, dispositivo, servidor y sistema para autenticar a un usuario**

(30) Prioridad:

16.12.2015 EP 15307028

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
24.02.2022

(73) Titular/es:

THALES DIS FRANCE SAS (100.0%)
6, rue de la Verrerie
92190 Meudon, FR

(72) Inventor/es:

DESJARDINS, JEAN-MICHEL y
LATHIERE, MARIE

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Método, dispositivo, servidor y sistema para autenticar a un usuario

Campo de la invención

La invención se refiere en general a un método para autenticar a un usuario.

Además, la invención también se refiere a un dispositivo para autenticar a un usuario.

Además, la invención se refiere a un servidor para autenticar a un usuario.

Por último, la invención también se refiere a un sistema para autenticar a un usuario.

Estado de la técnica

Como se conoce per se, una Emulación de Tarjeta de Equipo (o HCE) respaldada por un teléfono móvil permite generar un criptograma de transacción de pago teniendo en cuenta un Número de Identificación Personal (o PIN) que ingresa un usuario de teléfono en un sitio, como en una tienda. Luego, el teléfono envía el criptograma, a través de un terminal de Punto de Venta (o POS), en un lado del servidor, para realizar la transacción correspondiente. El criptograma se verifica en el lado del servidor, para autorizar una transacción así solicitada cuando el criptograma se valida en el lado del servidor.

Sin embargo, el lado del servidor tiene que acceder a un PIN de usuario de referencia, para verificar el criptograma. Tal necesidad de acceder al PIN de usuario de referencia hace que la solución basada en HCE sea compleja de administrar en el verificador de criptogramas.

Por tanto, existe la necesidad de proporcionar una solución alternativa que permita autenticar a un usuario. El documento de solicitud de patente US 2012/0297464 A1 describe un método para autenticar a un usuario basado en información biométrica. La información biométrica se combina con la información transaccional a través de una serie de procesos intermedios, de modo que permite al servidor autenticar al usuario.

Compendio de la invención

La invención propone una solución para satisfacer la necesidad que se acaba de especificar anteriormente al proporcionar un método para autenticar a un usuario.

Según la invención, el método comprende los siguientes pasos. Un dispositivo accede a una clave y a un vector inicial. La clave es una clave de un solo uso y no depende de los datos de autenticación del usuario. El vector inicial se genera previamente mediante el uso de un primer algoritmo, un vector de referencia y datos de autenticación del usuario de referencia. El vector de referencia se genera previamente sin utilizar los datos de autenticación del usuario de referencia. El dispositivo accede a los datos y proporciona datos de autenticación del usuario. El dispositivo genera un vector intermediario mediante el uso de un segundo algoritmo, el vector inicial y los datos de autenticación del usuario proporcionados. El dispositivo genera un criptograma mediante el uso de un tercer algoritmo, la clave, el vector intermediario y los datos. Un servidor recibe una solicitud de autenticación de un usuario acompañada del criptograma y los datos. El servidor accede a la clave y al vector de referencia. El servidor genera un criptograma de referencia mediante el uso del tercer algoritmo, la clave, el vector de referencia y los datos. El servidor verifica si el criptograma de referencia coincide o no con el criptograma. Si el criptograma de referencia coincide o no con el criptograma, entonces el servidor autentica o no al usuario respectivamente.

El principio de la invención consiste en que un dispositivo genera (u obtiene) un vector intermediario mediante el uso de un vector inicial predeterminado y datos de autenticación de usuario que introduce un usuario del dispositivo y/o que se captura del usuario del dispositivo en el lado del dispositivo. El vector inicial predeterminado depende de un vector de referencia y de los datos de autenticación del usuario de referencia. El vector de referencia no depende de los datos de autenticación del usuario de referencia. Luego, el dispositivo genera (u obtiene) un criptograma mediante el uso de los datos, una clave y el vector intermediario. Un servidor recibe el criptograma y los datos. Luego, el servidor genera (u obtiene) un criptograma de referencia mediante el uso de la clave, el vector de referencia y los datos. El servidor verifica si el criptograma recibido coincide o no con el criptograma de referencia. El servidor autentica o no al usuario basándose en el resultado de una comparación entre el criptograma recibido y el criptograma de referencia.

Un usuario del dispositivo que implementa el método de la invención está involucrado para permitir llevar a cabo una operación u operaciones, una función o funciones, una acción o acciones y/o un proceso o procesos a asegurar y, por lo tanto, es consciente de una solicitud pendiente ya que él o ella tiene que dar su consentimiento previo. Para dar su consentimiento previo, él o ella tiene que enviar, en el lado del dispositivo, los datos de autenticación del usuario que se utilizan para emitir un criptograma que depende de los datos de autenticación del usuario enviados y los datos relacionados con la operación u operaciones, la función o funciones, la acción o acciones y/o el proceso o procesos a asegurar.

Cabe señalar que los datos pueden estar relacionados con un usuario, una transacción o transacciones en particular, una transacción o transacciones de pago en particular, una operación u operaciones en particular, una función o funciones en particular, una acción o acciones en particular. y/o un proceso o procesos en particular y/o cualquier otro tipo de datos.

El dispositivo de la solución de la invención, como generador de criptogramas, no necesita acceder a los datos de autenticación del usuario de referencia, para generar un criptograma a verificar.

El servidor que verifica el criptograma recibido tiene que acceder a la clave, los datos y el vector de referencia, para producir un criptograma de referencia para compararlo con el criptograma recibido.

Cabe señalar que el vector de referencia predeterminado es independiente de los datos de autenticación del usuario de referencia, mientras que el criptograma de referencia es un criptograma que refleja que los datos de autenticación del usuario enviados coinciden con los datos de autenticación del usuario de referencia.

El criptograma recibido debe coincidir con el criptograma de referencia para autenticar al usuario, es decir, los datos de autenticación del usuario enviados deben coincidir con los datos de autenticación del usuario de referencia.

Los datos de autenticación del usuario de referencia pueden ser de cualquier tipo, es decir, datos que son conocidos por el usuario y/o datos que pertenecen al usuario.

El servidor de la solución de la invención, como verificador de criptogramas, no necesita acceder a los datos de autenticación del usuario de referencia para verificar el criptograma.

Debido a la ausencia de cualquier dato de autenticación del usuario de referencia en el lado del verificador de criptograma, la solución de la invención es más fácil de implementar que una implementación de una solución basada en HCE que necesita acceder a los datos de autenticación del usuario de referencia.

La solución de la invención es segura ya que el dispositivo emite un criptograma que se genera criptográficamente mientras se involucra a un usuario y se verifica en el lado del servidor mientras se autentica (o no) al usuario a través del criptograma emitido.

La solución de la invención es segura ya que ni el dispositivo que emite un criptograma ni el servidor que verifica el criptograma conocen los datos de autenticación del usuario de referencia.

La solución de la invención no necesita utilizar ningún Elemento Seguro (o SE) en el lado del dispositivo, para almacenar principalmente los datos de autenticación del usuario de referencia.

Dentro de la presente descripción, un SE es un objeto o dispositivo inteligente que incluye un chip que protege, como componente resistente a la manipulación, el acceso físico a los datos almacenados y está destinado a comunicar datos con el mundo exterior.

La solución de la invención se puede utilizar principalmente para una transacción de pago.

El método de la invención es principalmente aplicable para una transacción de pago por proximidad o una transacción de pago en línea, mediante el uso de un terminal de usuario, como por ejemplo un teléfono móvil o un ordenador personal (o PC), como dispositivo.

Cuando se utiliza para una transacción de pago, la solución de la invención no necesita modificar la infraestructura comercial existente.

Es de destacar que una aplicación de transacción correspondiente soportada por el dispositivo que permite llevar a cabo el método de la invención en el lado del dispositivo puede basarse en cualquier tipo de aplicación, como por ejemplo una aplicación de transacción de pago tipo Europay Mastercard Visa (o EMV).

Según otro aspecto, la invención es un dispositivo para autenticar a un usuario.

Según la invención, el dispositivo está configurado para acceder a una clave y un vector inicial. La clave es una clave de un solo uso y no depende de los datos de autenticación del usuario.

El vector inicial se genera previamente mediante el uso de un primer algoritmo, un vector de referencia y datos de autenticación del usuario de referencia. El vector de referencia se genera previamente sin utilizar los datos de autenticación del usuario de referencia. El dispositivo está configurado para acceder a los datos y proporcionar datos de autenticación del usuario. El dispositivo está configurado para generar un vector intermediario mediante el uso de un segundo algoritmo, el vector Vx inicial y los datos de autenticación del usuario proporcionados. Y el dispositivo está configurado para generar un criptograma mediante el uso de un tercer algoritmo, la clave, el vector intermediario y los datos.

El dispositivo puede ser un terminal de usuario, un terminal, un chip integrado o una tarjeta inteligente, como un SE, que incluye o está conectado a una Interfaz Hombre-Máquina (o MMI).

La invención no impone ninguna restricción en cuanto a un tipo del tipo de SE.

El chip del SE puede fijarse o quitarse de un dispositivo de equipo SE.

La invención es principalmente aplicable a un campo de radiocomunicación móvil en el que el dispositivo es un terminal móvil o un chip que puede estar integrado, como una Tarjeta de Circuito Integrado Universal integrada (o eUICC) dentro de un dispositivo de equipo SE, o extraíble de un dispositivo de equipo SE, como por ejemplo un chip incluido dentro de una tarjeta inteligente denominada Módulo de Identidad de Abonado (o tarjeta de tipo SIM) o similar.

Como SE extraíble, puede ser una tarjeta tipo SIM, un Módulo Extraíble Seguro (o SRM), una llave inteligente del tipo USB (acrónimo de "Universal Serial Bus"), una tarjeta de tipo (micro-) Secure Digital (o SD) o una tarjeta de tipo Multimedia (o MMC) o cualquier tarjeta de formato para acoplar o conectar a un dispositivo de equipo con chip.

En cuanto al dispositivo de equipo SE, puede estar constituido por cualquier dispositivo electrónico que comprenda medios de procesamiento de datos, medios de almacenamiento de datos y una o varias interfaces de Entrada/Salida (o I/O) que incluya o esté conectado a una MMI.

Según otro aspecto, la invención es un servidor para autenticar a un usuario.

Según la invención, el servidor está configurado para recibir una solicitud de autenticación de un usuario acompañada de un criptograma y datos. El servidor está configurado para acceder a una clave y un vector de referencia. La clave es una clave de un solo uso y no depende de los datos de autenticación del usuario. El vector de referencia se genera previamente sin utilizar ningún dato de autenticación del usuario de referencia. El servidor está configurado para generar un criptograma de referencia mediante el uso de un tercer algoritmo, la clave, el vector de referencia y los datos. El servidor está configurado para verificar si el criptograma de referencia coincide o no con el criptograma. El servidor está configurado para autenticar o no al usuario, si el criptograma de referencia coincide o no con el criptograma respectivamente.

Según otro aspecto más, la invención es un sistema para autenticar a un usuario.

Según la invención, el sistema comprende al menos un dispositivo y al menos un servidor. El dispositivo está conectado al servidor. El dispositivo está configurado para acceder a una clave y un vector inicial. La clave es una clave de un solo uso y no depende de los datos de autenticación del usuario. El vector inicial se genera previamente mediante el uso de un primer algoritmo, un vector de referencia y datos de autenticación de usuario de referencia. El vector de referencia se genera previamente sin utilizar los datos de autenticación del usuario de referencia. El dispositivo está configurado para acceder a los datos y proporcionar los datos de autenticación de usuario. El dispositivo está configurado para generar un vector intermediario mediante el uso de un segundo algoritmo, el vector inicial y los datos de autenticación del usuario proporcionados. Y el dispositivo está configurado para generar un criptograma mediante el uso de un tercer algoritmo, la clave, el vector intermediario y los datos. El servidor está configurado para acceder a la clave y al vector de referencia. El servidor está configurado para recibir una solicitud de autenticación de un usuario acompañada del criptograma y los datos. El servidor está configurado para generar un criptograma de referencia mediante el uso del tercer algoritmo, la clave, el vector de referencia y los datos. El servidor está configurado para verificar si el criptograma de referencia coincide o no con el criptograma. El servidor está configurado para autenticar o no al usuario, si el criptograma de referencia coincide o no con el criptograma respectivamente.

Breve descripción de los dibujos:

Las características y ventajas adicionales de la invención serán más claramente comprensibles después de leer una descripción detallada de una realización preferida de la invención, dada como un ejemplo indicativo y no limitativo, junto con los siguientes dibujos:

- La figura 1 es un diagrama simplificado de un teléfono móvil de usuario que está dispuesto para obtener datos de transacciones y transmitir un criptograma correspondiente que depende de un vector inicial y datos de autenticación del usuario proporcionados, a través de un terminal POS y un primer servidor, a un segundo servidor que verifica si el criptograma coincide o no con un criptograma de referencia generado sin usar datos de autenticación del usuario de referencia, para autenticar al usuario, según la invención;

- La figura 2 es un esquema simplificado para generar, en el lado del cliente de la figura 1, el criptograma mediante el uso de un algoritmo de generación de criptogramas, los datos de transacción, una clave y un vector intermediario dependiendo del vector inicial y los datos de autenticación del usuario proporcionados, el vector inicial que depende de un vector de referencia y datos de autenticación del usuario de referencia, según la invención;

- La figura 3 es un esquema simplificado para generar, en el lado del servidor de la figura 1, el criptograma de referencia mediante el uso del algoritmo de generación del criptograma, los datos de transacción, la clave y un vector de referencia independiente de los datos de autenticación del usuario de referencia, según la invención ; y

- La figura 4 ilustra un ejemplo simplificado de un flujo de mensajes intercambiados entre el usuario, el teléfono, el terminal POS y el segundo servidor de la figura 1, de modo que el teléfono emite mediante el esquema de la figura 2 un criptograma al segundo servidor que calcula mediante el uso del esquema de la figura 3, un criptograma de referencia a comparar, para autenticar al usuario.

Descripción detallada

A continuación se considera una realización en la que el método de la invención para autenticar a un usuario se implementa mediante un teléfono móvil, como una entidad independiente, es decir, sin cooperar con ningún otro dispositivo, como por ejemplo un SE, para emitir, principalmente, un criptograma. El teléfono móvil soporta una aplicación de autenticación de usuario de la invención que se almacena en un entorno no confiable.

Según una realización alternativa (no representada), el método de la invención para autenticar a un usuario se implementa, en el lado del cliente, mediante un sistema que comprende un SE y un dispositivo de equipo SE y al que se accede, a través de una MMI, por un usuario. El SE puede ser un eUICC, como un chip soldado (posiblemente de manera extraíble) en una Placa de Circuito Impreso (o PCB) del dispositivo de equipo SE, o extraíble del dispositivo de equipo SE en el lado del cliente.

Alternativamente, en lugar de un eUICC, el chip SE puede ser un Entorno de Ejecución de Confianza (o TEE), como un SE y un área segura de un procesador de terminal de usuario y un entorno de tiempo de ejecución seguro.

El SE puede tener diferentes factores de forma.

En lugar de estar integrado dentro de su dispositivo de equipo, el chip SE puede ser transportado por un medio, como una tarjeta inteligente o una llave, como por ejemplo una llave de tipo USB, para acoplarlo o conectarlo al dispositivo de equipo SE.

Según tal realización alternativa (no representada), el SE está adaptado para realizar al menos parte de las funciones que se describen a continuación y que son realizadas por el teléfono móvil.

Naturalmente, la realización que se describe a continuación en el presente documento es sólo para fines ilustrativos y no se considera que reduzca el alcance de la invención.

La Figura 1 muestra esquemáticamente, en el lado del cliente, un usuario 11, un teléfono 12 móvil, como terminal de usuario, un terminal 14 de tipo POS, un primer servidor 16 remoto, un segundo servidor 18 remoto y un tercer servidor 110 remoto.

En aras de la simplicidad, el teléfono 12 móvil, el terminal 14 de tipo POS 14el primer servidor 16 remoto, el segundo servidor 18 remoto y el tercer servidor 110 remoto se denominan infra TE 12, POS 14, primer servidor 16, segundo servidor 18 y tercer servidor 110 respectivamente.

El usuario 11 utiliza su teléfono 12 para cooperar localmente, por ejemplo dentro de una tienda o almacén, con el POS 14 mediante el uso de un enlace 13 de Radio Frecuencia (o RF) de Corto Alcance (o SR), como canal Sin Contacto (o CTL), para realizar una transacción (de pago) por proximidad. La transacción se procesa a través de un sistema de adquirente (banco) de transacciones (de pago) basado en una transacción de pago denominada Tarjeta No Presente (o CNP). La frecuencia del enlace de RF de SR puede fijarse en, por ejemplo, 13,56 MHz, como por ejemplo con una tecnología de tipo Comunicación de Campo Cercano (o NFC) (hasta 20 cm entre el teléfono 12 y el POS 14) o similares (como Bluetooth (marca comercial registrada), Bluetooth Low Energy (marca comercial registrada) y/o Zigbee (marca comercial registrada)).

Alternativamente, en lugar de utilizar un canal CTL, el teléfono 12 está vinculado, a través de un cable, como un canal Contacto (o CT), al POS 14 para realizar una transacción de proximidad con un comerciante.

Según otra realización (no representada), un dispositivo de usuario o un sistema de usuario se utiliza para una transacción de pago en línea, en un denominado comercio electrónico (es decir, A Través de Internet (u OTI)) o un comercio móvil (es decir, A Través del Aire (u OTA)), con un servidor comercial.

En lugar del teléfono 12, el terminal de usuario puede ser, entre otros, un Asistente Digital Personal (o PDA), un vehículo, un decodificador, una tableta, un ordenador de escritorio, un ordenador portátil, un PC, un video reproductor, un reproductor de audio, una Televisión (o TV) portátil, un reproductor multimedia, una consola de juegos, un portátil o un dispositivo electrónico con una Interfaz Hombre-Máquina (o MMI) o un acceso a una MMI.

El teléfono 12, como terminal de usuario, incluye (o está conectado o acoplado a) una pantalla 122 de visualización y un teclado 124, como una MMI de un teléfono.

Alternativamente, en lugar de un teclado físico separado de la pantalla de visualización, el teléfono 12 está equipado con una pantalla de visualización sensible al tacto, como un teclado virtual.

La MMI del teléfono o una MMI conectada o acoplada al teléfono 12 permite que el usuario 11 presente o introduzca un PIN o similar y/o permite que el teléfono 12 capture una o varias impresiones biométricas relacionadas con el usuario 11, como proporciona los Datos de Autenticación de Usuario (o UAD). Los UAD proporcionados, es decir, que introduce el usuario 11 y/o que son capturados por el teléfono 12 (y/o un dispositivo o dispositivos que cooperan con el teléfono 12), se utiliza para generar un criptograma que se enviará al lado del servidor.

Los UAD incluyen datos que son conocidos por el usuario 11, como por ejemplo un PIN, una contraseña, un código de acceso y/o credenciales de usuario, como una contraseña única (u OTP), y/o datos que pertenecen al usuario 11, como por ejemplo una o varias huellas dactilares, una o dos huellas de palmas, uno o dos iris y/o una cara, como una o varias huellas biométricas relativas al usuario 11.

El teléfono 12 comprende un (micro) procesador o procesadores, como medio para procesar datos, que comprende (o está conectado a) una o unas interfaces de Entrada/Salida (o I/O), como medio de comunicación para intercambiar datos con el exterior y que comprende (o está conectado a) una o unas memorias, como medio para almacenar datos.

La memoria del teléfono puede comprender una o varias memorias que incluyen una o varias memorias volátiles y una o varias memorias no volátiles.

La memoria del teléfono puede estar constituida por una o varias EEPROM (acrónimo de "Memoria de Sólo Lectura Programable y Borrable Eléctricamente"), una o varias ROM (acrónimo de "Memoria de Sólo Lectura"), una o varias memorias Flash y/o cualquier otra memoria de diferentes tipos, como una o varias RAM (acrónimo de "Memoria de Acceso Aleatorio").

Las interfaces de I/O del teléfono incluyen (o están conectadas a) una interfaz CTL (y/o CT) mientras se usa el enlace 13 de RF de SR.

El enlace 13 de RF de SR puede estar relacionado con cualquier tecnología que permita al teléfono 12 intercambiar datos con el POS 14, como por ejemplo para obtener del POS 14 una cantidad de transacción, una fecha de transacción y otros datos de transacción, como Datos de Transacción (o TD).

En lugar de pasar por un terminal POS, el teléfono 12 puede utilizar uno o varios enlaces de radiofrecuencia (o RF) de largo alcance (o LR) (no representados) para acceder, OTA, a través de una antena 126 y uno o varias redes (de radiocomunicaciones) móviles, al lado del servidor.

La RF de LR puede fijarse a varios cientos de MHz, por ejemplo, alrededor de 850, 900, 1800, 1900 y/o 2100 MHz.

Según otra realización (no representada), en lugar de utilizar una o unas redes móviles, el terminal se conecta, a través de un decodificador o similar, como un Punto de Acceso a la Red (o NAS), OTI al lado del servidor.

La o las memorias del teléfono almacenan un sistema operativo (o OS).

La o las memorias del teléfono (o un dispositivo, como por ejemplo un SE, que coopera con el teléfono 12) almacenan preferiblemente una o varias aplicaciones, entre las cuales hay una aplicación de transacción de pago, como por ejemplo, una aplicación de tipo EMV, que utiliza una aplicación de autenticación de usuario de invención.

La o las memorias del teléfono almacenan un Número de Cuenta Principal (o PAN), un Número de Cuenta Principal Dinámico (o DPAN), como un token (digital), un alias de PAN y/o un alternativo de PAN, como datos relacionados con una cuenta de usuario. Los datos relacionados con una cuenta de usuario se utilizan para identificar una cuenta de usuario bancaria o similar en el lado del servidor. Los datos relacionados con una cuenta de usuario se asociarán con un Criptograma de Transacción (de pago) (o TC), como un primer criptograma, que se emitirá desde el teléfono 12.

La o las memorias del teléfono almacenan preferiblemente de manera temporal los UAD proporcionados.

La o las memorias del teléfono (o un dispositivo, como por ejemplo un SE, que coopera con el teléfono 12) almacenan una (o varias) claves o claves que se comparten con el lado del servidor.

Cada clave se utiliza para generar un TC.

La clave puede ser una clave de uso limitado, como por ejemplo una clave de un solo uso o denominada clave de sesión, que se utiliza, por ejemplo, en un cierto período de tiempo predefinido y/o un cierto recuento de uso para un número predefinido de transacciones, como por ejemplo una, dos o más transacciones.

Alternativamente, en lugar de una clave de uso limitado, la clave es permanente.

La clave preferiblemente no depende de ningunos UAD proporcionados.

Es posible que la clave se haya cargado previamente durante un proceso de fabricación del teléfono antes de la emisión del teléfono o que se haya descargado de un servidor remoto después de la emisión del teléfono.

Una vez recuperado de una entidad externa, como por ejemplo el POS 14, la o las memorias del teléfono almacenan, al menos de manera temporal, el TD, tal como una cantidad de transacción, una moneda de transacción, una fecha de transacción y/u otros datos.

La memoria del teléfono puede almacenar un Contador de Transacciones de la Aplicación (o ATC) y/u otros datos que cambian de una transacción a otra. Como se conoce per se, un valor de ATC se incrementa en cada transacción. La o las memorias del teléfono pueden almacenar datos de tarjetas (bancarias), como por ejemplo:

- un Tipo de Tarjeta; un Nombre en la Tarjeta, un número de Tarjeta, un Valor de Verificación de Tarjeta (o CW); y/o
- una Fecha de Vencimiento (o ED).

Según una característica esencial de la invención, la o las memorias del teléfono 12 (o un dispositivo, como por ejemplo un SE, que coopera con el teléfono 12) almacenan un vector inicial (o Vx) o un conjunto de Vx. El teléfono 12 no genera el Vx ni el conjunto de Vx. El Vx incluye uno o varios elementos de datos. El Vx puede haber sido cargado previamente durante un proceso de fabricación del teléfono antes de la emisión del teléfono o descargado de un servidor remoto después de la emisión del teléfono. El Vx está predefinido, por ejemplo por un emisor bancario o en su nombre en el lado del servidor, mediante el uso por ejemplo de una función XOR, como primer algoritmo predeterminado, un vector de referencia (o Vref) y un PIN de referencia o similar, como referencia UAD.

Según una característica importante de la invención, el Vref está predefinido sin utilizar los UAD de referencia. Se ha generado previamente el Vref o un conjunto de Vref. El o cada Vref es preferiblemente un elemento variable. El o cada Vref es preferiblemente válido para una transacción dada y, por lo tanto, el valor de Vref cambia de una primera a una segunda transacción. La transacción es una transmisión de datos desde el teléfono 12 (o un dispositivo, como, por ejemplo, un SE, que está conectado o acoplado al teléfono 12) al primer servidor 16. El valor de Vref puede ser, por ejemplo un valor aleatorio o (pseudo) aleatorio.

El teléfono 12 (o un dispositivo, como por ejemplo un SE, que está conectado o acoplado al teléfono 12) se configura preferiblemente para generar un vector intermedio V o un conjunto de V. Para generar un V, el teléfono 12 usa, por ejemplo, una función XOR, como segundo algoritmo predeterminado, el Vx y los UAD proporcionado. El segundo algoritmo es un algoritmo inverso del primer algoritmo.

Por lo tanto, si los UAD proporcionados coincide con unos UAD de referencia, entonces V coincide con Vref. De lo contrario, es decir, si los UAD proporcionados no coincide con unos UAD de referencia, el V no coincide con el Vref. Los UAD de referencia no se almacenan en el lado del teléfono 12.

El teléfono 12 está configurado preferiblemente para generar un TC, como una especie de firma de usuario (digital).

Para generar un TC, el teléfono 12 usa un tercer algoritmo predeterminado compartido con el lado del servidor, la clave, el V y los datos, como por ejemplo el TD, como se describe a continuación en relación con la figura 2.

El teléfono 12 está dispuesto para enviar al lado del servidor una solicitud de autenticación del usuario acompañada del TC (generado). El teléfono 12 puede estar dispuesto para enviar además al servidor los datos que se utilizan para generar el TC.

El teléfono 12 está conectado, a través del enlace 13 bidireccional, al POS 14.

El POS 14 puede proporcionar a una entidad externa, como por ejemplo el teléfono 12, el TD posiblemente después de una solicitud procedente de la entidad externa.

El POS 14 comprende un o unos (micro) procesadores, como medio para procesar datos, que comprenden (o están conectados a) dos (o más) interfaces de I/O, como medio de comunicación para intercambiar datos con el exterior, y que comprenden (o están conectados a) memoria o memorias, como medio para almacenar datos.

La memoria del POS (no representada) puede comprender una o varias memorias que incluyen una o varias memorias volátiles y una o varias memorias no volátiles.

La memoria del POS puede almacenar datos relacionados con un identificador o identificadores uniformes de recursos (o URI), un localizador o localizadores uniformes de recursos (o URL) y/o una dirección o direcciones de protocolo de Internet (o IP) de una entidad o entidades externas que deben abordarse, como por ejemplo el primer servidor 16.

El POS 14 incluye (o está conectado o acoplado a) una pantalla 142 de visualización y un teclado 144, como una MMI del POS.

Alternativamente, en lugar de un teclado físico separado de la pantalla de visualización, el POS 14 está equipado con una pantalla de visualización sensible al tacto, como un teclado virtual.

La MMI del POS o una MMI conectada o acoplada al POS 14 permite a un usuario, como un comerciante, presentar o introducir una cantidad de transacción y/u otros datos, como TD. El TD proporcionado, es decir, que introduce el comerciante y/o que es almacenado por el POS 14 (y/o un servidor remoto que coopera con el POS 14), es utilizado por el dispositivo cliente, como por ejemplo el teléfono 12, para generar un TC correspondiente que se enviará, a través del POS 14, al lado del servidor.

El POS 14 puede recibir de una entidad externa, como por ejemplo el teléfono 12, una solicitud de autenticación del usuario acompañada del TC y posiblemente el TD (después de una posible solicitud procedente del POS 14).

El POS 14 puede enviar al lado del servidor una solicitud para autorizar una transacción acompañada del TC recibido y el TD.

El POS 14 puede recibir desde el lado del servidor, como respuesta a la solicitud de autorización de una transacción, un éxito o un fracaso relacionado con la transacción en base a una autenticación de usuario en el lado del servidor.

El POS 14 está conectado preferiblemente, a través de un enlace 15 por cable bidireccional, al primer servidor 16.

El primer servidor 16 está alojado en un ordenador con medios de procesamiento de datos, medios de almacenamiento de datos y varias interfaces de I/O.

El primer servidor 16 puede recibir un mensaje que se origina, a través del POS 14, desde un lado del dispositivo cliente, como por ejemplo el teléfono 12, y eso incluye una solicitud para autorizar una transacción que va acompañada de un TC y TD correspondiente, como por ejemplo una cantidad de transacción y/o una moneda de transacción. El TD se refiere a un producto o productos y/o un servicio o servicios que el usuario 11 desea comprar o alquilar.

El primer servidor 16 puede identificar un segundo servidor 18 que se usa para verificar un TC recibido, para autenticar (o no) al usuario involucrado en el lado del cliente.

El mensaje recibido que se origina, a través del POS 14, desde el lado del dispositivo cliente incluye, junto con una solicitud para autorizar una transacción, preferiblemente datos relacionados con una cuenta de usuario.

Los datos relacionados con una cuenta de usuario incluyen preferiblemente datos, como por ejemplo un Número de Identificación Bancaria (o BIN) o un Número de Identificación de Emisor (o IIN), como un identificador de emisor bancario, y/o un identificador o identificadores, como por ejemplo un URI y/o un URL, relacionado con un tercer servidor 110 al que se debe direccionar para una transacción de pago en curso después de una autenticación de usuario llevada a cabo en el segundo servidor 18.

El primer servidor 16 es capaz de identificar, basándose en los datos recibidos, un tercer servidor 110 que se utiliza para autorizar (o no) una transacción después de una autenticación de usuario llevada a cabo en el segundo servidor 18 y que gestiona una cuenta de usuario para ser identificado.

El primer servidor 16 desempeña un papel de entidad intermediaria entre el dispositivo cliente, como por ejemplo el teléfono 12, que emite el TC, el segundo servidor 18 que verifica el TC, y el tercer servidor 110 que autoriza (o no) una transacción solicitada en base a la autenticación de usuario realizada por el segundo servidor 18.

El primer servidor 16 permite enrutar datos que se originan en el lado del dispositivo cliente o en el lado del servidor al POS 14, el segundo servidor 18 o el tercer servidor 110.

El primer servidor 16 está conectado (o acoplado), preferiblemente a través de un enlace 17 por cable bidireccional, al segundo servidor 18.

El primer servidor 16 está conectado (o acoplado), preferiblemente a través de un enlace 19 por cable bidireccional, al tercer servidor 110.

El segundo servidor 18 está alojado en un ordenador con uno o varios procesadores, como medio de procesamiento de datos, una o varias memorias, como medio de almacenamiento de datos, y una o varias interfaces de I/O.

El o los procesadores del segundo servidor o servidores 18 procesan, controlan y comunican internamente datos con todos los demás componentes incorporados dentro del segundo servidor 18 y, a través de la o las interfaces de I/O del servidor, con el segundo servidor 18 exterior.

El segundo procesador del servidor 18 realiza o ejecuta al menos una aplicación de autenticación de usuario de la invención.

La memoria del segundo servidor 18 almacena o accede a la aplicación de autenticación de usuario de la invención que utiliza, como se describe en relación con la figura 3, un tercer algoritmo predeterminado y datos recibidos, como

datos de entrada al tercer algoritmo, para generar un TC de referencia (o TCref) para ser emparejado por un TC para ser recibido desde el lado del dispositivo cliente.

El segundo servidor 18 está configurado para recibir una solicitud de autenticación de un usuario acompañada de un TC y datos. Los datos se han utilizado para generar el TC y se utilizarán para generar un TCref.

Una memoria del segundo servidor 18 o una memoria conectada o acoplada al segundo servidor 18 almacena una clave compartida con el lado del cliente que se usa para generar un TCref.

Una memoria del segundo servidor 18 o una memoria conectada o acoplada al segundo servidor 18 almacena un Vref que se usa para generar un TCref.

Un PIN de referencia, credenciales de usuario de referencia, una contraseña de referencia, un código de acceso de referencia y/o datos biométricos relacionados con el usuario en cuestión, como UAD de referencia, no se almacenan en el lado del segundo servidor 18.

El segundo servidor 18 está configurado para acceder a una clave y al Vref.

La clave se comparte con el lado del cliente.

El Vref se genera previamente en el lado del servidor, por ejemplo por un banco emisor o en su nombre.

El Vref se genera previamente sin utilizar ningunos UAD de referencia.

El Vref se proporciona al segundo servidor 18 (u otra entidad accesible desde el segundo servidor 18).

El segundo servidor 18 está configurado preferiblemente para generar (o dejar generar) un TCref, como una firma de usuario (digital) que se debe comparar, con el fin de autenticar a un usuario que proporciona UAD en el lado del cliente.

Para generar un TCref, el segundo servidor 18 usa, como se describe más adelante en relación con la figura 3, un tercer algoritmo predeterminado compartido con el lado del cliente, la clave, el Vref y los datos recibidos, como por ejemplo TD, que se utiliza en el lado del cliente para emitir un TC a verificar.

El segundo servidor 18 está configurado preferiblemente para verificar (o permitir verificar) si el TCref coincide o no con el TC (recibido).

Si la verificación es positiva, es decir, el TCref coincide con el TC, entonces el segundo servidor 18 autentica al usuario.

De lo contrario, es decir, cuando la verificación es negativa, es decir, el TCref no coincide con el TC, el segundo servidor 18 no autentica al usuario.

El segundo servidor 18 está configurado preferiblemente para enviar al primer servidor 16, como respuesta a la solicitud (recibida) para autenticar a un usuario, un resultado de verificación correspondiente, es decir, un éxito o un fallo de la autenticación del usuario.

En lugar de intercambiar con el primer servidor 16 o el tercer servidor 110, el segundo servidor 18 puede realizar al menos parte de las funciones que se llevan a cabo, como se describe supra e infra, por el primer servidor 16 y/o el tercer servidor 110.

El segundo servidor 18 puede estar conectado (o acoplado), a través de un enlace por cable bidireccional (no representado), al tercer servidor 110.

El tercer servidor 110 está alojado en un ordenador con uno o varios procesadores, como medio de procesamiento de datos, una o varias memorias, como medio de almacenamiento de datos, y una o varias interfaces de I/O.

El tercer servidor 110 está configurado para recibir una solicitud para autorizar una transacción acompañada de datos relacionados con una cuenta de usuario en base a un resultado de autenticación de usuario emitido desde o a través del segundo servidor 18.

El tercer servidor 110 está configurado para identificar, en base a los datos recibidos, una cuenta de usuario, después de una posible destokenización (cuando los datos relacionados con la cuenta de usuario emitidos desde el lado del cliente incluyen un token, como por ejemplo un DPAN).

Una memoria del tercer servidor 110 o una memoria conectada o acoplada al tercer servidor 110 almacena preferiblemente una base de datos relacionada con una pluralidad de cuentas de usuario. La base de datos incluye datos relacionados con cada cuenta de usuario, como por ejemplo un saldo bancario.

El tercer servidor 110 puede recibir datos, como por ejemplo un DPAN, un alias de PAN, un alternativo de PAN y/o un PAN, relacionado con una cuenta de usuario.

El tercer servidor 110 puede acceder a datos, tales como un PAN o similares, relacionados con la cuenta de usuario.

El tercer servidor 110 puede recuperar, basándose en los datos recibidos relacionados con una cuenta de usuario, uno o varios identificadores relacionados con una cuenta de usuario, como por ejemplo un PAN.

El tercer servidor 110 está configurado para recibir, desde o a través del segundo servidor 18, como verificador de criptogramas, un resultado de autenticación de usuario.

El tercer servidor 110 está configurado preferiblemente, solo si el resultado de la autenticación del usuario es exitoso, para verificar (o permitir verificar) si los datos relacionados con la cuenta de usuario identificada permiten autorizar (o no) una transacción solicitada (pago).

Alternativamente, en lugar de una transacción de pago, otra entidad, como por ejemplo un servidor, se configura conectado o acoplado al segundo servidor 18, solo si el resultado de la autenticación del usuario es exitoso, después de una o varias verificaciones posibles, para autorizar (o no) realizar una o varias operaciones, una o varias funciones, una o varias acciones y/o uno o varios procesos.

Si la verificación es positiva, entonces el tercer servidor 110 autoriza la transacción solicitada y lleva a cabo (o permite llevar a cabo) la transacción solicitada.

De lo contrario, es decir, cuando la verificación es negativa, el tercer servidor 110 niega o rechaza la transacción solicitada.

El tercer servidor 110 está configurado preferiblemente para enviar al primer servidor 16, como respuesta a la solicitud (recibida) de autorizar una transacción, un resultado correspondiente, es decir, una autorización o una denegación (o un rechazo) de la transacción.

La Figura 2 es una realización ejemplar de un algoritmo 20 para generar un primer criptograma que es utilizado por el teléfono 12 (u otro dispositivo, como por ejemplo un SE, que coopera con el teléfono 12), como dispositivo cliente, para emitir el primer criptograma.

El primer algoritmo 20 de generación de criptogramas incluye un algoritmo 22 predeterminado para generar un criptograma.

El algoritmo 22 para generar un criptograma incluye un algoritmo criptográfico, como un tercer algoritmo predeterminado, tal como un Estándar de Encriptación de Datos (o DES), un DES triple, un algoritmo de tipo Código de Autenticación de Mensaje (o MAC) o cualquier otro algoritmo de clave simétrica que utiliza una clave que se comparte con el servidor u otra entidad que tiene que verificar el criptograma generado.

Tal algoritmo 22 de generación de criptogramas tiene una clave 24, como primera entrada, un vector V 26 intermedio, como segunda entrada, y datos 28, como tercera entrada.

La clave 24 es almacenada por el teléfono 12 u otro dispositivo, como por ejemplo un SE, que coopera con el teléfono 12. La clave 24 es accesible desde el teléfono 12. La clave 24 puede ser una clave de uso limitado o una clave permanente. La clave 24 puede tener, como primer valor de longitud, 16 bytes.

El V 26 es almacenado por el teléfono 12 u otro dispositivo, como por ejemplo un SE, que coopera con el teléfono 12. El V 26 es accesible desde el teléfono 12. El V 26 es generado por el teléfono 12 (u otro dispositivo, como por ejemplo un SE, que coopera con el teléfono 12) mediante el uso de los UAD proporcionados y el Vx que ha sido proporcionado por una entidad externa, como por ejemplo un servidor. El Vx depende del Vref (que es independiente de los UAD de referencia) y del UAD de referencia. El V 26 depende del Vref, los UAD de referencia y los UAD proporcionados. Si los UAD proporcionados coinciden con los UAD de referencia, entonces el V 26 es el Vref. De lo contrario, es decir, si los UAD proporcionados no coinciden con los UAD de referencia, el V 26 es distinto del Vref. Los UAD proporcionados y los UAD de referencia pueden tener, como segundo valor de longitud, 8 bytes. El V 26 y el Vref pueden tener, como segundo valor de longitud, 8 bytes. El uso de un cálculo con un segundo valor de longitud tal que sea menor que un tercer valor de longitud relacionado con el criptograma es rápido.

Los datos 28 son almacenados por el teléfono 12 u otro dispositivo, como por ejemplo un SE, que coopera con el teléfono 12. Los datos 28 son accesibles desde el teléfono 12. Los datos 28 pueden ser cualquier dato predeterminado, como por ejemplo TD que se relaciona con una transacción solicitada (pago), que se relaciona con una operación u operaciones, una función o funciones, una acción o acciones y/o un proceso o procesos que necesitan una autenticación de usuario.

El algoritmo 22 de generación de criptogramas puede utilizar otros datos predeterminados, como una o varias entradas adicionales, accesibles desde el teléfono 12.

Los otros datos son almacenados por el teléfono 12 u otro dispositivo, como por ejemplo un SE o el POS 14, que coopera con el teléfono 12, y/o proporcionado por el usuario 11, como por ejemplo datos de la tarjeta.

El algoritmo 22 de generación de criptogramas permite generar un primer criptograma 210, como por ejemplo un TC mediante el uso preferiblemente de una o varias piezas de TD predeterminada. El TC puede incluir un número predeterminado N de dígitos (como número o números hexadecimales) (o (una) otra unidad o unidades de información, como por ejemplo bit o bits o byte o bytes), como un tercer valor de longitud. El número predeterminado N de dígitos se incluye dentro de un primer rango, por ejemplo 16 a 19 dígitos.

Una generación del primer criptograma, como por ejemplo un TC, permite autenticar con éxito a un usuario, solo si se reconoce con éxito, es decir, se verifica, en el segundo servidor 18, mientras se asegura la autenticación del usuario, es decir, sin acceder a los UAD de referencia en el lado del dispositivo cliente.

La figura 3 es una realización ejemplar de un algoritmo 30 para generar un segundo criptograma que es utilizado como criptograma de referencia por el segundo servidor 18 para verificar si el primer criptograma es o no válido al comparar el primer criptograma con el segundo criptograma.

El segundo algoritmo 30 de generación de criptogramas incluye el algoritmo 22 para generar un criptograma que se comparte con el teléfono 12, como dispositivo cliente.

El algoritmo 22 para generar un criptograma incluye un algoritmo criptográfico, como un tercer algoritmo predeterminado, como un DES, un DES triple, un algoritmo de tipo MAC o cualquier otro algoritmo de clave simétrica que utilice una clave que se comparte con el lado del dispositivo del cliente u otra entidad que tiene que generar un criptograma para ser verificado.

Dicho algoritmo 22 de generación de criptogramas tiene la clave 24, como primera entrada, un Vref 36, como segunda entrada, y los datos 28, como tercera entrada.

La clave 24 se comparte con el dispositivo cliente.

El Vref 36 es almacenado por el segundo servidor 18 u otro servidor conectado al segundo servidor 18. El Vref 36 es accesible desde el segundo servidor 18. El Vref 36 es independiente de los UAD de referencia. El Vref 36 puede tener, como segundo valor de longitud, 8 bytes.

Los datos 28 se almacenan, después de su recepción desde el dispositivo cliente u otro dispositivo, como por ejemplo un SE, que coopera con el dispositivo cliente, en el lado del segundo servidor 18. Los datos 28 son accesibles desde el segundo servidor 18. Los datos 28 pueden ser cualquier dato predeterminado, como por ejemplo TD que se relaciona con una transacción solicitada, que se relaciona con una operación u operaciones, una función o funciones, una acción o acciones y/o un proceso o procesos que necesitan una autenticación de usuario.

El algoritmo 22 de generación de criptogramas puede utilizar otros datos predeterminados, como una o varias entradas adicionales, accesibles desde el segundo servidor 18.

Los otros datos son almacenados por el segundo servidor 18 u otra entidad que coopera con el segundo servidor 18.

El algoritmo 22 de generación de criptogramas permite generar un segundo criptograma 310, como un criptograma de referencia, como por ejemplo una TCref mediante el uso preferiblemente de una o varias piezas de TD predeterminada, como datos 28 que se van a recibir desde el dispositivo cliente o cualquier entidad que coopere con el dispositivo cliente. La TCref puede incluir un número predeterminado N de dígitos (como número o números hexadecimales) (o (una) otra unidad o unidades de información, como por ejemplo bit o bits o byte o bytes), como tercer valor de longitud. El número predeterminado N de dígitos se incluye dentro de un primer rango, por ejemplo 16 a 19 dígitos.

Una generación de un segundo criptograma, como por ejemplo un TCref, permite autenticar con éxito a un usuario, solo si se reconoce con éxito, es decir, se verifica, en el lado del segundo servidor 18, mientras se asegura la autenticación del usuario, es decir, sin acceder a los UAD de referencia en el lado del segundo servidor 18.

La figura 4 representa una realización ejemplar de un flujo de mensajes 40 que involucra al usuario 11, el teléfono 12, el POS 14 y el segundo servidor 18.

En el ejemplo explicado, se asume que el dispositivo cliente es el teléfono 12, como terminal de usuario, entidad autónoma y generador de un TC, como primer criptograma, para solicitar una transacción (de pago) que necesita una autenticación de usuario.

También se supone que el segundo servidor 18 desempeña un papel de verificador del TC que se genera en el dispositivo cliente.

El teléfono 12 accede 41 a una clave y un vector inicial Vx.

Un comerciante de un producto o productos y/o un servicio o servicios puede ingresar en el POS 14 una cantidad relacionada con una transacción (de pago), como datos relacionados con una transacción (de pago), que un usuario 11 del teléfono 12 desea comprar.

El POS 14 envía al teléfono 12 un mensaje 42 que incluye la cantidad de la transacción, una moneda de la transacción y/u otros datos de la transacción, como TD.

El teléfono 12 presenta al usuario 11 un mensaje 44, como por ejemplo "por favor introduzca su PIN", que solicita al usuario 11 que proporcione un PIN, como UAD.

El usuario 11 proporciona, a través del teléfono MMI, al teléfono 14 un PIN 46, como respuesta a la solicitud del usuario.

El teléfono 12 genera 48 un vector V intermedio mediante el uso por ejemplo de un algoritmo "XOR", como segundo algoritmo predeterminado, el Vx y el PIN proporcionado.

Entonces, el teléfono 12 genera 410 CRYPTO1, como un primer criptograma, mediante el uso por ejemplo de un algoritmo de tipo DES, como tercer algoritmo predeterminado, la clave, el V y el TD.

Una vez que se genera el CRYPTO1, el teléfono 12 envía al POS 14 un mensaje 412 que incluye una solicitud para autenticar a un usuario acompañado con el CRYPTO1 y preferiblemente, por ejemplo un DPAN, como datos relacionados con una cuenta de usuario.

Opcionalmente, el mensaje 412 incluye además el TD.

El POS 14 genera una solicitud para autorizar una transacción de pago.

El POS 14 envía, a través del primer servidor 16, al segundo servidor 18 la solicitud de autenticación de un usuario con el CRYPTO1 y el TD.

El segundo servidor 18 accede 416 a la clave y un vector de referencia Vref.

El segundo servidor 18 genera 418 CRYPTO2, como TCref, un segundo criptograma de referencia, mediante el uso por ejemplo del algoritmo de tipo DES, como tercer algoritmo predeterminado, la clave, el Vref y el TD.

Una vez que se genera el CRYPTO2, el segundo servidor 18 verifica 420 si el CRYPTO2 coincide o no con el CRYPTO1 (recibido).

Si el CRYPTO2 coincide con el CRYPTO1, entonces el segundo servidor 18 autentica 422 con éxito al usuario 11. Dicha verificación positiva del criptograma asegura una autenticación del usuario (los UAD proporcionados son correctos, es decir, los UAD de referencia), una autenticidad del teléfono 12 (solo el que soporta una aplicación de autenticación de usuario de la invención) y una integridad de los datos, es decir, los datos utilizados para generar el CRYPTO1 (y, por lo tanto, el CRYPTO2) no sufren una alteración de datos que conduzca a fallar la verificación del criptograma en el lado del servidor.

De lo contrario, es decir, si hay una discrepancia entre el CRYPTO2 y el CRYPTO1, el segundo servidor 18 no autentica 424 al usuario 11.

Independientemente de si la autenticación del usuario ha tenido éxito o no al comparar el primer criptograma generado por el segundo servidor 18 con el segundo criptograma generado por el teléfono 12, el segundo servidor 18 envía al primer servidor 16 un mensaje (no representado) que incluye un resultado de la autenticación del usuario, como por ejemplo "OK", como un éxito de autenticación de usuario, o "KO", como un error de autenticación de usuario.

El primer servidor 16 envía al tercer servidor 110 un mensaje (no representado) que incluye la solicitud de autorización de una transacción de pago acompañada del resultado de autenticación de usuario (recibido), el TD (recibido) y los datos (recibidos) relacionados con la cuenta de usuario.

El tercer servidor 110 recupera uno o más identificadores relacionados con una cuenta de usuario, como por ejemplo un PAN, basado en el DPAN (recibido), como datos (recibidos) relacionados con la cuenta de usuario.

El tercer servidor 110 verifica si la transacción solicitada está autorizada o rechazada mediante el uso de al menos ciertos datos relacionados con la cuenta de usuario identificada.

Si el resultado de la autenticación del usuario es negativo, es decir, el segundo servidor 18 no verifica satisfactoriamente la autenticación del usuario, entonces el tercer servidor 110 rechaza la transacción solicitada.

Si el resultado de la autenticación del usuario es positivo, es decir, la autenticación del usuario es verificada con éxito por el segundo servidor 18, entonces el tercer servidor 110 autoriza o rechaza, después de una o varias verificaciones de datos, como por ejemplo un saldo bancario superior al TD (recibido), la transacción solicitada.

Independientemente de si la transacción solicitada está autorizada o rechazada, el tercer servidor 110 envía, preferiblemente a través del primer servidor 16, al POS 14 un mensaje (no representado) que incluye un resultado de la transacción de pago, como por ejemplo "transacción rechazada" o "transacción autorizada".

Entonces, el POS 14 proporciona, a través de una MMI del POS o una MMI conectada o acoplada al POS 14, al comerciante el resultado de la transacción de pago.

La solución de la invención permite asegurar la autenticación de un usuario sin que el dispositivo involucrado conozca los datos de autenticación del usuario de referencia, ya que ni un dispositivo cliente que emite un criptograma ni un dispositivo de verificación de criptograma, como por ejemplo un servidor, que verifica que el criptograma conoce los datos de autenticación del usuario de referencia.

La solución de la invención no necesita utilizar ningún SE en el lado del dispositivo cliente.

La solución de la invención es especialmente compatible con la infraestructura comercial existente.

Un método de autenticación de usuario de la invención de este tipo permite reutilizar una infraestructura bancaria existente reduciendo así la complejidad técnica y los costes correspondientes para ofrecer un servicio de autenticación de usuario seguro.

La realización que se acaba de describir no pretende limitar el alcance de la invención en cuestión. Pueden darse otras realizaciones. Como otro ejemplo de realización, en lugar de dos servidores 16 y 18 involucrados, solo un servidor permite autenticar (o no) a un usuario. Como otro ejemplo de realización más, en lugar del teléfono 12 que está involucrado, otro dispositivo, como por ejemplo un SE, que coopera con el teléfono 12 permite emitir un criptograma generado a bordo para ser verificado en el lado del servidor, para autenticar (o no) a un usuario antes de continuar la ejecución de un proceso, como por ejemplo un proceso de autorización de la transacción de pago del usuario.

REIVINDICACIONES

1. Un método (40) para autenticar a un usuario, que comprende:

- acceder (41), mediante un dispositivo (12), una clave y al menos un vector inicial, siendo la clave una clave de un solo uso y no dependiente de los datos de autenticación del usuario, siendo generado previamente el al menos un vector inicial mediante el uso de un primer algoritmo, al menos un vector de referencia y datos de autenticación de usuario de referencia, siendo generado previamente el al menos un vector de referencia sin usar los datos de autenticación de usuario de referencia;

- acceder, por el dispositivo, a los datos (42) y los datos (46) de autenticación de usuario proporcionados;

- generar (48), mediante el dispositivo, al menos un vector intermediario mediante el uso de un segundo algoritmo, el al menos un vector inicial y los datos de autenticación de usuario proporcionados;

- generar (410), mediante el dispositivo, un criptograma mediante el uso de un tercer algoritmo (22), la clave, el al menos un vector intermediario y los datos;

- recibir (410), por parte de un servidor (18), una solicitud (414) para autenticar a un usuario acompañado con el criptograma y los datos;

- acceder (416), por parte del servidor, a la clave y al al menos un vector de referencia;

- generar (418), por parte del servidor, un criptograma de referencia mediante el uso del tercer algoritmo, la clave, el al menos un vector de referencia y los datos;

- verificar (420), por parte del servidor, si el criptograma de referencia coincide o no con el criptograma; y

- autenticar (422) o no (424), por parte del servidor, si el criptograma de referencia coincide o no con el criptograma, el usuario respectivamente.

2. Método según la reivindicación 1, en el que los datos que incluyen datos de transacciones de pago, la solicitud de autenticación de un usuario se acompaña además de una solicitud de autorización de una transacción de pago y los datos relacionados con una cuenta de usuario y el servidor u otro servidor recupera además al menos un identificador relacionado con una cuenta de usuario basado en los datos relacionados con la cuenta de usuario.

3. Método según la reivindicación 1 o 2, en el que el o cada vector de referencia es válido para una transacción determinada.

4. Método según cualquiera de las reivindicaciones 1 a 3, en el que los datos de autenticación del usuario incluyen al menos un elemento de un grupo que comprende:

- un Número de Identificación Personal;

- al menos una impresión biométrica;

- credenciales de usuario;

- una contraseña;

- un código de acceso,

5. Método según la reivindicación 2, en el que el al menos un identificador relacionado con una cuenta de usuario y/o los datos relacionados con la cuenta de usuario incluyen al menos un elemento de un grupo que comprende:

- un Número de Cuenta Principal;

- un Número de Cuenta Principal Dinámico;

- un alias de Número de Cuenta Principal;

- un Número de Cuenta Principal alternativo.

6. Método según cualquiera de las reivindicaciones 1 a 5, en el que el segundo algoritmo es un algoritmo inverso del primer algoritmo.

7. Método según cualquiera de las reivindicaciones 1 a 6, en el que el tercer algoritmo incluye al menos un elemento de un grupo que comprende:

- un Estándar de Encriptación de Datos o un algoritmo de tipo DES;

- un algoritmo de tipo Triple DES;

- un algoritmo del tipo de Código de Autenticación de Mensaje;

- un algoritmo que utiliza una clave simétrica.

8. Un dispositivo (12) para autenticar a un usuario, en el que el dispositivo está configurado para:

- acceder (41) a una clave y al menos un vector inicial, siendo la clave una clave de un solo uso y no dependiente de los datos de autenticación del usuario, siendo generado previamente el al menos un vector inicial mediante el uso de un primer algoritmo, al menos un vector de referencia y datos de autenticación de usuario de referencia, siendo generado previamente el al menos un vector de referencia sin utilizar los datos de autenticación de usuario de referencia;

- datos (42) de acceso y datos (46) de autenticación de usuario proporcionados;

- generar (48) al menos un vector intermediario mediante el uso de un segundo algoritmo, el al menos un vector inicial y los datos de autenticación de usuario proporcionados; y

- generar (410) un criptograma mediante el uso de un tercer algoritmo, la clave, el al menos un vector intermediario y los datos; y enviar a un servidor una solicitud de autenticación del usuario acompañada del criptograma y los datos.

9. Un servidor (18) para autenticar a un usuario, en el que el servidor está configurado para:

- recibir una solicitud (414) para autenticar a un usuario acompañado de un criptograma y datos;

- acceder (416) a una clave y al menos un vector de referencia, siendo la clave una clave de uso único y no dependiente de los datos de autenticación del usuario, generándose previamente el al menos un vector de referencia sin utilizar ningún dato de autenticación del usuario de referencia;

- generar (418) un criptograma de referencia mediante el uso de un tercer algoritmo (22), la clave, el al menos un vector de referencia y los datos;

- verificar (420) si el criptograma de referencia coincide o no con el criptograma;

- autenticar (422) o no (424) al usuario, si el criptograma de referencia coincide o no con el criptograma respectivamente.

10. Un sistema para autenticar a un usuario, en el que, comprendiendo el sistema al menos un dispositivo (12) y al menos un servidor (18), estando el dispositivo conectado al servidor, el dispositivo está configurado para:

- acceder (41) a una clave y al menos un vector inicial, siendo la clave una clave de un solo uso y no dependiente de los datos de autenticación del usuario, siendo generado previamente el al menos un vector inicial mediante el uso de un primer algoritmo, al menos un vector de referencia y datos de autenticación de usuario de referencia, siendo generado previamente el al menos un vector de referencia sin utilizar los datos de autenticación de usuario de referencia;

- datos (42) de acceso y datos (46) de autenticación de usuario proporcionados;

- generar (48) al menos un vector intermediario mediante el uso de un segundo algoritmo, el al menos un vector inicial y los datos de autenticación de usuario proporcionados; y

- generar (410) un criptograma mediante el uso de un tercer algoritmo, la clave, el al menos un vector intermediario y los datos;

y en eso el servidor está configurado para:

- acceder (416) a la clave y a al menos un vector de referencia;

- recibir una solicitud (414) para autenticar a un usuario acompañado con el criptograma y los datos;

- generar (418) un criptograma de referencia mediante el uso del tercer algoritmo, la clave, el al menos un vector de referencia y los datos;

- verificar (420) si el criptograma de referencia coincide o no con el criptograma;

- autenticar (422) o no (424) al usuario, si el criptograma de referencia coincide o no con el criptograma respectivamente.

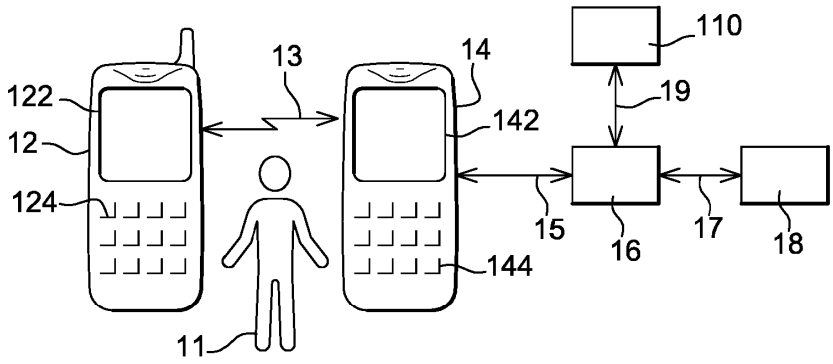

Fig. 1

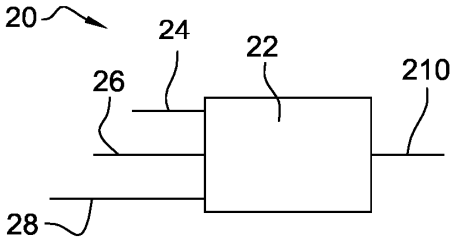

Fig. 2

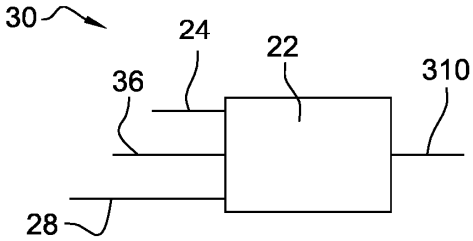

Fig. 3

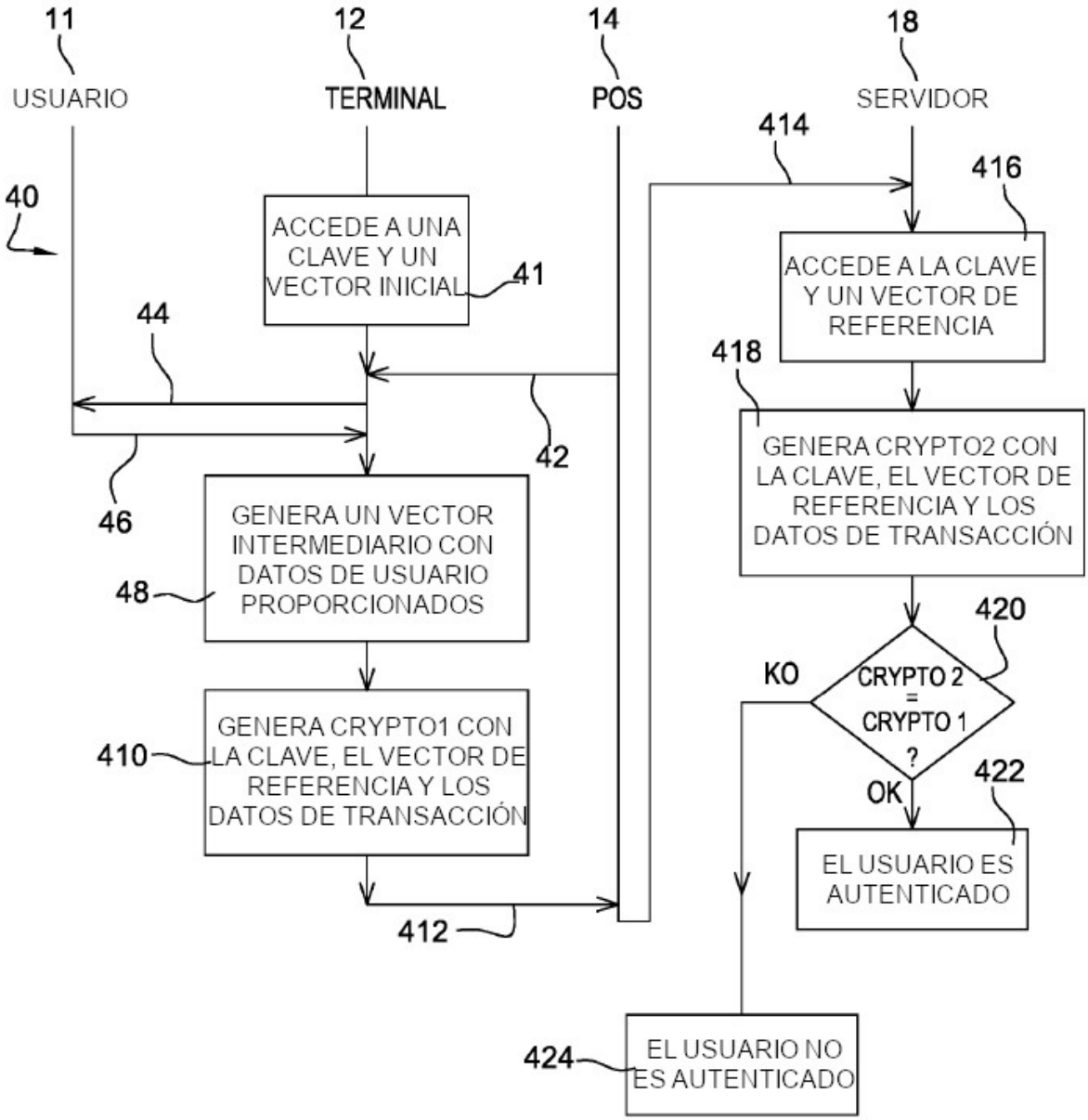
11
USUARIO
12
TERMINAL
14
POS
18
SERVIDOR
40
ACCEDE A UNA CLAVE Y UN VECTOR INICIAL
41
44
42
46
GENERA UN VECTOR INTERMEDIARIO CON DATOS DE USUARIO PROPORCIONADOS
48
GENERA CRYPTO1 CON LA CLAVE, EL VECTOR DE REFERENCIA Y LOS DATOS DE TRANSACCIÓN
410
412
414
416
ACCEDE A LA CLAVE Y UN VECTOR DE REFERENCIA
418
GENERA CRYPTO2 CON LA CLAVE, EL VECTOR DE REFERENCIA Y LOS DATOS DE TRANSACCIÓN
420
CRYPTO 2 = CRYPTO 1 ?
KO
OK
422
EL USUARIO ES AUTENTICADO
424
EL USUARIO NO ES AUTENTICADO

Fig. 4