(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 708 805**

(51) Int. CI.:

G06Q 20/18 (2012.01)
G06Q 20/38 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **12.09.2014 E 14290273 (3)**

(97) Fecha y número de publicación de la concesión europea: **14.11.2018 EP 2996079**

(54) Título: **Terminal de pago de uso compartido**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
11.04.2019

(73) Titular/es:

AMADEUS S.A.S. (100.0%)
485 Route du Pin Montard Sophia Antipolis
06410 Biot, FR

(72) Inventor/es:

TAHON, MATHIEU;
BOSCO, LORENZO;
HIREL, NICOLAS;
MILANI, VERONICA y
DIANA, REMI

(74) Agente/Representante:

SUGRAÑES MOLINÉ, Pedro

DESCRIPCIÓN

Terminal de pago de uso compartido

Campo de la invención

La invención se refiere al uso compartido de un terminal de pago.

Antecedentes

Los pagos no realizados en efectivo a las expendedoras pueden realizarse en los terminales de pago por medio de tarjetas, por ejemplo, tarjetas de crédito. Habitualmente los terminales de pago permiten realizar transacciones punto a punto conformes con la industria de tarjetas de pago (PCI). Tales terminales de pago, por ejemplo, se utilizan también en los aeropuertos para la compra de billetes en los mostradores, así como para las compras de última hora, por ejemplo, en las puertas de embarque.

El documento EP 2.541.517 A1 se refiere a un sistema de pago con tarjeta en una máquina TPV. La información del vendedor en una base de datos puede descargarse en un terminal de una máquina TPV, y así permitir al terminal de la máquina TPV la realización de la operación de pago con tarjeta basada en la información descargada del vendedor.

El documento US 5.745.576 A se refiere a la inicialización de terminales criptográficos en un sistema criptográfico. Se facilita una clave base que es común a todos los controladores, producida por un fabricante de sistemas criptográficos. El fabricante de terminales criptográficos instala la clave base en cada controlador antes de realizar el envío de los controladores. Cada terminal criptográfico que contiene la clave base común cuenta con una clave inicial proporcionada por el fabricante del terminal. Cada clave inicial se deriva del número de serie del terminal en particular y de la clave base común. Tras la instalación, el controlador y el terminal establecen una comunicación, a través de la cual, el controlador puede determinar de manera segura la clave inicial contenida en el terminal, mientras que el controlador contiene la clave base.

Sumario de la invención

La invención se define por las reivindicaciones independientes. Según esto, se proporciona un método para configurar un terminal de pago que pueda utilizarse como terminal de pago compartido por una pluralidad de operadores con segregación criptográfica entre los distintos operadores del terminal de pago. El terminal de pago está dispuesto para establecer comunicación con al menos un proveedor de pago para realizar transacciones de pago. El terminal de pago está asociado con una entidad de control que controla la utilización del terminal de pago de manera selectiva según el operador. El terminal de pago tiene almacenada una clave de acceso específica de terminal, y tiene un número de identificación de terminal. El método comprende transmitirir una clave de transporte específica de operador y de terminal, cifrada por la clave de acceso específica de terminal, al terminal de pago. La clave de transporte específica de operador y de terminal cifrada se descifra en el terminal de pago con la clave de acceso específica de terminal almacenada. La utilización del terminal de pago por parte de los operadores y/o proveedores de pago se garantiza a través de la entidad de control de manera remota sin contacto físico con el terminal de pago. Por tanto la clave de transporte específica de operador y de terminal se introduce en el terminal de pago almacenando la clave de transporte específica de operador y de terminal en el terminal de pago de forma cifrada o no cifrada. La clave de transporte específica de operador y de terminal se deriva, del proveedor de pago, a partir de una derivación base de la clave específica de operador usando el número de identificación de terminal, o un número adicional de identificación de terminal de pago. La clave de cifrado inicial específica de operador y de terminal está cifrada simétricamente con la clave de transporte específica de operador y de terminal. La clave de cifrado inicial específica de operador y de terminal cifrada se transmite al terminal de pago. La clave de cifrado inicial específica de operador y de terminal cifrada se descifra en el terminal de pago con la clave de transporte específica de operador y de terminal descifrada. La clave cifrada específica de operador y de la transacción se deriva, en el proveedor de pago y en el terminal de pago, a partir de la clave de cifrado inicial específica de operador y de terminal usando un número específico de transacción asociado con esa transacción, cuando se realiza una transacción con el terminal de pago. La transacción se realiza con el terminal de pago.

Según otro aspecto, un sistema que comprende un sistema informatizado con entidad de control, un sistema informatizado con proveedor de pago, y al menos un terminal de pago. El sistema está dispuesto para configurar al menos un terminal de pago para ser utilizado como terminal de pago compartido por una pluralidad de operadores con segregación criptográfica entre los diferentes operadores del terminal de pago. El sistema también está dispuesto para configurar el terminal de pago de tal forma que establezca comunicación con un operador o al menos un proveedor de pago para realizar transacciones de pago. El sistema también está dispuesto para configurar el terminal de pago de tal forma que esté asociado con un sistema de entidad de control que controla la utilización del terminal de pago de manera selectiva según el operador y remota, sin contacto físico con el terminal de pago. Por tanto la clave de transporte específica de operador y de terminal se introduce en el terminal de pago, almacenando la clave de transporte específica de operador y de terminal en el terminal de pago de forma cifrada o no cifrada. El

terminal de pago está programado para almacenar un número de identificación de terminal. El terminal de pago comprende al menos un almacenamiento seguro (TRSM), el cual está programado para almacenar una clave de acceso específica de terminal para permitir la utilización del terminal de pago para ser controlado con el sistema con entidad de control de manera selectiva según el operador. El sistema está dispuesto para recibir, en el terminal de pago, una clave de transporte específica de operador y de terminal, que está cifrada por la clave de acceso específica de terminal. El sistema también está dispuesto para descifrar, en el terminal de pago, el clave de transporte específica de operador y de terminal cifrada con la clave de acceso específica de terminal almacenada. El sistema también está dispuesto para recibir, en el terminal de pago del sistema con proveedor de pago, una clave de cifrado inicial específica de operador y de terminal derivada de una clave de derivación base específica de operador basada en el número de identificación de terminal o un número adicional de identificación de terminal de pago. La clave de cifrado inicial específica de operador y de terminal está cifrada simétricamente por la clave de transporte específica de operador y de terminal. El sistema está dispuesto para descifrar, en el terminal de pago, la clave de cifrado inicial específica de operador y de terminal cifrada con la clave de transporte específica de operador y de terminal descifrada. El sistema también está dispuesto para derivar, en el sistema de proveedor de pago y en el terminal de pago, una clave de específica de operador y de la transacción cifrada de la clave de cifrado inicial específica de operador y de terminal usando número específico de transacción asociado con esa transacción, cuando se realiza una transacción con el terminal de pago. El sistema también está dispuesto para realizar la transacción con el terminal de pago.

Otras funciones son inherentes en los métodos y sistemas que se han dado a conocer o serán evidentes para los expertos en la materia a partir de la siguiente descripción de ejemplos y sus dibujos adjuntos.

Descripción general, también de realizaciones opcionales de la invención

El método divulgado se refiere a la configuración de un terminal de pago, por ejemplo un lector de tarjetas de crédito, para convertirse en un terminal de pago compartido por una pluralidad de operadores con segregación criptográfica entre los diferentes operadores del terminal de pago. Tal operador podría ser, por ejemplo, una aerolínea realizando una facturación para un vuelo.

La segregación criptográfica permite la utilización, esto es, transmitir transacciones de pago, del mismo terminal de pago por parte de diferentes operadores, por ejemplo diferentes aerolíneas en una puerta de embarque, protegidas por claves de cifrado específicas del operador, y de ese modo asegurando la privacidad específica de operador, como si cada uno de esos operadores fuesen un único operador al utilizar el terminal de pago.

El terminal de pago está dispuesto para establecer comunicación con al menos un proveedor de pago para realizar transacciones de pago. El proveedor de pago, por ejemplo, puede ser una pasarela de pago, una compañía de tarjetas de crédito (una compañía de tarjetas de crédito también puede denominarse “switch”), o un adquiriente. Una pasarela de pago podría agrupar transacciones con diversas compañías de tarjetas de crédito.

El terminal de pago está asociado con una entidad de control que controla la utilización del terminal de pago de manera selectiva según el operador. La entidad de control es, por ejemplo, el propietario de un aeropuerto que encargó los terminales de pago para el aeropuerto. Una compañía aeroportuaria encargada de gestionar el aeropuerto podría encargar terminales de pago a un fabricante para distribuir las terminales de pago en los mostradores de facturación, puertas de embarque, quioscos, y similares.

La entidad de control concede la utilización a los diferentes operadores usando una clave de acceso específica de terminal, la cual permite a la entidad de control gestionar la autorización de acceso para cada operador individual del terminal de pago. Es decir, la autorización de los proveedores de pago contratados por los operadores, esto es los adquirientes de los operadores, puede controlarse con la entidad de control de esta manera. Más específicamente, la autorización de un operador se establece al proporcionar al terminal de pago una clave de transporte específica de operador y de terminal, cifrada por la clave de acceso específica de terminal.

En algunos ejemplos la clave de transporte específica de operador y de terminal se verifica tras el descifrado por la clave de acceso específica de terminal con un valor de clave de control (KCV), el cual también se transmite junto con el clave de transporte específica de operador y de terminal cifrada. El KCV es, por ejemplo, el resultado de una aplicación de una “función unidireccional” a la clave de transporte específica de operador y de terminal que tiene que verificarse. Una “función unidireccional” es una función que prácticamente no puede invertirse; esto es una función que no facilita los datos de entrada, los cuales tienen que verificarse para reconstruirse a partir del resultado de la aplicación de la función unidireccional a los datos de entrada. Ejemplos de funciones unidireccionales son las funciones resumen. Para verificar la clave de transporte específica de operador y de terminal, la función unidireccional (por ejemplo, la función resumen) se aplica al clave de transporte específica de operador y de terminal descifrada, y el resultado de la aplicación se compara al KCV transmitido. Si el resultado es coherente con el KCV (por ejemplo, si es idéntico al KCV), se considera que la clave de transporte específica de operador y de terminal es la clave de transporte válida específica de operador y de terminal.

En otros ejemplos (sin verificación con un KCV) la validez de la clave de transporte específica de operador y de

terminal descifrada se vuelve evidente durante una posterior transacción de pago. Si una secuencia de bits, esto es una (supuesta) clave de transporte específica de operador y de terminal, sin cifrar por la clave correcta de acceso específica de terminal, se transmite al terminal de pago, la secuencia de bits descifrada, esto es la (supuesta) clave de transporte específica de operador y de terminal que resulta al descifrar con la clave de acceso específica de terminal almacenada, no será la clave de transporte correcta específica de operador y de terminal. De ahí que todas las claves que se derivan de esta clave de transporte incorrecta específica de operador y de terminal serán también incorrectas. Por lo tanto, las comunicaciones cifradas con estas claves incorrectas que se han obtenido, por ejemplo, las peticiones de autenticación del usuario o titular de la tarjeta, que se han realizado por el terminal de pago en la posterior transacción de pago, no contendrán información útil, y por tanto fallarán.

El terminal de pago tiene un número de identificación de terminal, esto es una cadena de dígitos alfanuméricos de una longitud determinada, y tiene la clave de acceso específica de terminal almacenada en él, por ejemplo almacenada en una memoria de sólo lectura (ROM).

El proceso de facilitar una clave de transporte específica de operador y de terminal, cifrada por la clave de acceso específica de terminal, al terminal de pago puede realizarse de varias maneras alternativas, designadas abajo con “A1”, “A2”, y “A3”. El inicio y fin de la descripción de estas alternativas se marca con “(Inicio A1)”, “(Fin A1)”, “(Inicio A2)”, etcétera.

(Inicio A1) En algunas realizaciones, la clave de transporte maestro específica de operador se transmite desde al menos un proveedor de pago a la entidad de control de una manera que asegura la confidencialidad.

Esta clave de transporte maestro específica de operador es única para cada operador y entidad de control. Es, por ejemplo, generada de manera segura en el almacenamiento seguro (TRSM) del proveedor de pago, y luego comunicada a la entidad de control de una manera que asegura la confidencialidad. La entidad de control almacena la clave de transporte maestro específica de operador, por ejemplo, en otro almacenamiento seguro (TRSM).

Un clave de transporte específica de operador y de terminal se deriva, en el extremo del proveedor de pago y en el extremo de la entidad de control, por ejemplo en los respectivos TRSM, de la clave de transporte maestro específica de operador usando el número de identificación de terminal, que es, por ejemplo, un número de serie del terminal de pago.

La clave de transporte específica de operador y de terminal, que se deriva de la entidad de control, se cifra simétricamente, con la clave de acceso específica de terminal y luego la clave de transporte específica de operador y de terminal cifrada se transmite al terminal de pago (Fin A1).

(Inicio A2) En realizaciones alternativas, una clave de transporte maestro específica de operador que es única para cada operador y entidad de control es, por ejemplo, generada de manera segura en el almacenamiento seguro (TRSM) del proveedor de pago.

Una clave de transporte específica de operador y de terminal se deriva, en el extremo del proveedor de pago, por ejemplo en el TRSM, a partir de la clave de transporte maestro específica de operador usando el número de identificación de terminal, y se transmite a la entidad de control de una manera que asegura la confidencialidad.

Esta clave de transporte específica de operador y de terminal se cifra simétricamente, por la entidad de control, con la clave de acceso específica de terminal y luego la clave de transporte específica de operador y de terminal cifrada se transmite al terminal de pago (Fin A2).

(Inicio A3) En otras realizaciones alternativas, la clave de transporte específica de operador y de terminal se proporciona al terminal de pago al introducir manualmente la clave de transporte específica de operador y de terminal, cifrada simétricamente por la clave de acceso específica de terminal, en el terminal de pago.

Esta entrada manual puede ser una interacción manual con el terminal de pago, por ejemplo navegando a través del menú guiado del terminal de pago e introduciendo la clave de transporte específica de operador y de terminal, cifrada con la clave de acceso específica de terminal, en formato decimal cifrado en binario (BCD). De manera alternativa, la entrada manual puede ser la inserción de un dispositivo de almacenamiento extraíble en el terminal de pago, por ejemplo, de una unidad flash USB o de una tarjeta de memoria. (Fin A3)

En todas estas alternativas (A1, A2, A3), la entidad de control es capaz de controlar la utilización del terminal de pago de manera selectiva según el operador con la clave de transporte específica de operador y de terminal, cuando se utiliza esta clave para descifrar posteriores comunicaciones entre un proveedor de pago y el terminal de pago si un operador, asociado con ese proveedor de pago, inicia una transacción de pago.

Por un lado, la utilización de cifrado simétrico para la clave de transporte específica de operador y de terminal permite un manejo de clave menos complejo que, por ejemplo el cifrado asimétrico, puesto que no hay autoridad de certificación (CA) independiente requerida para gestionar la distribución de claves públicas verificadas. Por otro lado,

la transmisión de la clave simétrica se acepta desde la perspectiva de la seguridad dado que un “secreto compartido” se obtiene en ambos extremos de la transmisión y puede, como se describe anteriormente, verificarse con un KCV o similares. Además, la clave criptográfica inicial, usada para el cifrado y el descifrado de posteriores claves transmitidas al terminal de pago, se introduce en el terminal de pago de una manera que asegura la confidencialidad, por ejemplo, en una sala segura localizada en las instalaciones de fabricación del proveedor del terminal.

Los módulos de seguridad mencionados anteriormente podrían ser dispositivos de almacenamiento con propiedades físicas que hacen que las manipulaciones satisfactorias sean difíciles e improbables. La manipulación podría incluir penetración sin zeroización de los parámetros de seguridad, modificación no autorizada de una operación interna del TRSM, o inserción de mecanismos de pulsación o métodos de interceptación no intrusiva para determinar, registrar, o modificar datos secretos.

La clave de transporte específica de operador y de terminal cifrada se descifra en el terminal de pago con la clave de acceso específica de terminal almacenada, como se describe anteriormente.

En algunos ejemplos, la clave de transporte específica de operador y de terminal cifrada se descifra con la clave de acceso específica de terminal en el terminal de pago tras su recepción, y la clave de transporte específica de operador y de terminal descifrada se almacena en un almacenamiento seguro del terminal de pago, tal como el TRSM.
En ejemplos alternativos, la clave de transporte específica de operador cifrado recibido y de terminal se almacena primero en el terminal de pago de manera cifrada y sólo después se descifra “sobre la marcha” con la clave de acceso específica de terminal en el terminal de pago, esto es sólo cuando la versión descifrada de la clave de transporte específica de operador y de terminal se necesite para el descifrado de la clave de cifrado inicial específica de operador y de terminal cifrada para realizar una transacción con el terminal de pago, por ejemplo una transacción de pago.

La entidad de control puede garantizar la utilización del terminal de pago a un operador con su clave de transporte correspondiente específica de operador y de terminal cuando esta clave se usa para descifrar posteriores comunicaciones entre el terminal de pago y el proveedor de pago asociado con el operador que realiza transacciones con el terminal de pago.

Una clave de cifrado inicial específica de operador y de terminal se deriva, del proveedor de pago, a partir de la clave de derivación base específica de operador usando el número de identificación de terminal, o un número adicional de identificación de terminal de pago.

La clave de derivación base específica de operador, por ejemplo, podría ser única para cada operador y proveedor de pago y se genera de manera segura en el TRSM del proveedor de pago y, en circunstancias normales, nunca sale de este entorno seguro. La clave de cifrado inicial específica de operador y de terminal es única para cada terminal de pago y es generada, por ejemplo, en el TRSM del proveedor de pago derivándose de la clave base de derivación específica de operador usando obtención de datos basada en el número de identificación de terminal del terminal de pago.

La clave de cifrado inicial específica de operador y de terminal se cifra simétricamente con la clave de transporte específica de operador y de terminal. La versión cifrada de esa clave se transmite al terminal de pago. La versión cifrada recibida en el terminal de pago se descifra en el terminal de pago usando la clave de transporte específica de operador y de terminal anteriormente almacenada.

En algunos ejemplos, la versión descifrada de la clave de cifrado inicial específica de operador y de terminal se almacena en un almacenamiento seguro del terminal de pago, por ejemplo, en el TRSM del terminal de pago.

En algunos ejemplos, la clave de cifrado inicial específica de operador y de terminal cifrada se descifra con la clave de transporte específica de operador y de terminal en el terminal de pago tras su recepción o se introduce, y la clave de cifrado inicial específica de operador descifrado y de terminal se almacena en un almacenamiento seguro del terminal de pago, por ejemplo el TRSM.

El proceso de transmitirir la clave de cifrado inicial específica de operador y de terminal cifrada, descifrar la clave de cifrado inicial específica de operador y de terminal cifrada, y almacenando la clave de cifrado inicial específica de operador y de terminal descifrada en el terminal de pago puede considerarse un proceso de alimentación (o, en sentido figurado, "inyectado") de la clave de cifrado inicial específica de operador y de terminal en el terminal de pago.

En un ejemplo alternativo, la clave de cifrado inicial recibida específica de terminal se almacena primero en el terminal en su forma cifrada tras su recepción o se introduce, y sólo es descifrada más tarde con la clave de transporte específica de operador y de terminal en el terminal de pago cuando la clave de cifrado inicial específica de terminal se requiere para obtener la clave de cifrado específica de operador y de terminal, usando la clave de

cifrado inicial específica de operador y de terminal descifrada para realizar una transacción con el terminal de pago, por ejemplo una transacción de pago.

En este ejemplo alternativo, la clave de cifrado inicial específica de operador y de terminal se almacena todavía en su forma cifrada en el terminal de pago en una memoria que no es segura, por ejemplo en una memoria normal fuera del TRSM, y sólo se descifra cuando sea necesario, es decir es un "descifrado sobre la marcha". En este ejemplo alternativo, la seguridad de la clave de cifrado inicial específica de operador y de terminal se proporciona por el cifrado, en lugar de almacenarla de forma descifrada en una memoria segura, tal como un TRSM. En este ejemplo alternativo, el proceso de alimentación (o de "inyección") de la clave de cifrado inicial específica de operador y de terminal en el terminal de pago puede verse en la transmisión de la clave de cifrado inicial específica de operador cifrado y de terminal al terminal de pago, y su almacenamiento en la todavía forma cifrada en el terminal de pago. El posterior descifrado "sobre la marcha" de esta clave puede considerarse como parte de la actividad posterior de derivar una clave de cifrado específica de operador y de terminal.

Una clave de cifrado específica de operador y de terminal se deriva, en el extremo del proveedor de pago y en el terminal de pago, a partir de la clave de cifrado inicial específica de operador y de terminal usando un número específico de transacción asociado con esa transacción, cuando una transacción se realiza con el terminal de pago. Tal transacción se realizaría cuando, por ejemplo, el pago no realizado en efectivo se realiza por medio de una tarjeta de pago, tal como una tarjeta de crédito, siendo insertada en el terminal de pago, por ejemplo para la compra de billetes en el mostrador de un aeropuerto, o para una compra de última hora, por ejemplo, en la puerta de embarque de un aeropuerto.

En algunos ejemplos el "al menos único proveedor de pago" es un único proveedor de pasarela de pago que, por ejemplo, valida pagos en aerolíneas, combate el fraude y permite la recaudación de fondos. El proveedor de pasarela de pago podría permitir a la aerolínea proteger los ingresos a través de varias comprobaciones de reserva y/o datos de pago. El único proveedor de pasarela de pago podría proporcionar una interfaz a una pluralidad de compañías de tarjetas de crédito, bancos, etcétera, y puede por tanto considerarse un mediador entre el operador del terminal de pago y las diversas compañías de tarjetas de crédito, bancos, etcétera., y agrupa las comunicaciones con las diversas compañías de tarjetas de crédito, bancos, etcétera. Por tanto, en las transacciones de pago, el operador del terminal de pago opera sólo indirectamente con las diversas compañías de tarjeta de crédito, bancos, etcétera. a través del único proveedor de pasarela de pago.

En otros ejemplos, el "al menos único proveedor de pago" es uno de una pluralidad de proveedores de pago, por ejemplo unacompañía de tarjetas de crédito que liquida los pagos con el operador del terminal de pago. En estos otros ejemplos, el operador del terminal de pago interactúa directamente con las diversas compañías de tarjetas de crédito, bancos, etc., sin el efecto de agrupamiento mencionado para el caso de un único proveedor de pasarela de pago.

En algunos ejemplos, al menos una de las claves de acceso específica de terminal, la clave de transporte maestro específica de operador, la clave de transporte específica de operador y de terminal, la clave base de derivación específica de operador, la clave de cifrado inicial específica de operador y de terminal, y la clave de cifrado específica de operador y de terminal es una clave de cifrado simétrico. En algunos ejemplos algunas o todas esas claves son claves de cifrado simétrico.

En este contexto, la clave de cifrado simétrico representa la utilización de las mismas claves criptográficas para el cifrado de texto plano y descifrado de texto cifrado. El cifrado y descifrado de claves podría ser idéntico o podría haber una simple transformación entre ellos como, por ejemplo, en el Algoritmo Internacional de Cifrado de Datos (IDEA). Las claves, en la práctica, representan un secreto compartido entre dos o más partes que pueden utilizarse para mantener un vínculo de información privada.

En algunos de estos ejemplos, el al menos uno, de algunos, o todas las claves de cifrado simétrico son triples claves según el algoritmo de triple cifrado (TDEA), el cual aplica el algoritmo de cifrado Estándar de Cifrado de Datos (DES) tres veces a cada bloque de datos.

DES es un cifrado en bloque y cifra datos en bloques de 64-bit. Un bloque de 64-bit de texto plano es la entrada de un algoritmo, y un bloque de texto cifrado de 64-bit es la salida. DES es simétrico: En principio, el mismo algoritmo y clave se usan para cifrado y descifrado (excepto cuando hay pequeñas diferencias en la planificación de la clave). Más específicamente, DES usa claves con una longitud de clave de 56 bits. La clave se expresa habitualmente como un número de 64-bit, pero el octavo bit se ignora y se usa para el bit de paridad. En su forma más simple, el algoritmo es una combinación de dos técnicas básicas de cifrado: confusión y difusión. La construcción fundamental de bloque de DES es una combinación de estas técnicas, es decir una sustitución seguida por una permutación, en el texto, basada en la clave. Esto se conoce como ronda. DES tiene 16 rondas, y por tanto aplica la misma combinación de técnicas 16 veces al bloque de texto plano. El algoritmo utiliza aritmética estándar y operaciones lógicas en números de 64 bits como máximo.

Triple DES (3DES) utiliza una "agrupación de claves" que comprende tres claves DES, K1, K2 y K3, cada una de 56

bits (excluyendo los bits de paridad). El procedimiento es el que sigue: cifrado DES con K1, descifrado DES con K2, luego cifrado DES con K3. El descifrado es inverso, es decir, descifrado con K3, cifrado con K2, luego descifrado con K1. Cada triple cifrado cifra un bloque de 64 bits de datos.

El estándar 3DES define tres opciones de clave: (i) todas las tres claves son independientes, (ii) K1 y K2 son independientes, y K3 = K1, y (iii) todas las tres claves son idénticas, es decir K1 = K2 = K3. La opción de clave 1 es la más robusta con 3 x 56 = 168 bits de clave independientes. Cada clave DES es almacenada de forma nominal o transmitida como 8 bytes, cada uno de paridad impar. Por tanto, una agrupación de claves requiere 24, 16 o 8 bytes para la opción de clave (i), (ii), o (iii), respectivamente.

En algunos ejemplos el terminal de pago está dispuesto para proporcionar al menos dos modos de uso, un modo de uso directo en el que los datos de la transacción se intercambian entre el terminal de pago y uno de los operadores, y un modo autorizado en el que los datos de la transacción se intercambian entre el terminal de pago y al menos un proveedor de pago. El terminal de pago se preconfigura por una disposición de modos de uso a los operadores de la pluralidad de operadores (4). Por ejemplo, considerando los operadores A, B, C, D, E, el modo de uso directo podría asignarse a los operadores A, B, D, y el modo autorizado podría asignarse a los operadores C y E; y el terminal de pago se preconfigura según esta disposición. Cuando uno de los operadores de la pluralidad de operadores, por ejemplo el operador A o el operador C, empieza a utilizar el terminal de pago, por ejemplo para realizar una transacción, el modo de uso asignado a este operador, es decir en este ejemplo el modo de uso directo y el modo autorizado, respectivamente, se seleccionan automáticamente por el terminal de pago, y el terminal de pago realiza la transacción usando el modo de uso seleccionado, es decir en este ejemplo el modo de uso directo y el modo autorizado, respectivamente.

El método descrito hasta ahora empezó desde un estado en el que el terminal de pago tiene una clave de acceso específica de terminal almacenada en él. Hay diversas opciones de cómo la clave de acceso específica de terminal se obtiene y almacena. En algunos ejemplos opcionales, la clave de acceso específica de terminal utilizada por la entidad de control para el cifrado simétrico se deriva de una clave maestra de acceso específica de la entidad de control usando el número de identificación de terminal, por ejemplo el número de serie del terminal de pago, o un número adicional de identificación de terminal de pago, por ejemplo un número aleatorio generado para cada terminal de pago individual. La clave maestra de acceso específica de la entidad de control podría ser única para cada entidad de control y el fabricante del terminal de pago. La clave maestra de acceso específica de la entidad de control se genera de manera segura en el TRSM de la entidad de control, y se transmite de manera opcional al fabricante, es decir el proveedor del terminal, de una manera que asegura la confidencialidad, y se almacena de manera opcional ahí en otro TRSM.

En algunos ejemplos, la clave de acceso específica de terminal se almacena en el terminal de pago después de transmitirirse al terminal de pago de una manera que asegura la confidencialidad por el proveedor del terminal, es decir el fabricante del terminal de pago. La clave de acceso específica de terminal puede cargarse en el terminal de pago en una sala segura en las instalaciones del proveedor del terminal, es decir en las instalaciones de fabricación del proveedor del terminal, antes de que el terminal de pago se entregue a la entidad de control.

En algunos ejemplos, la clave de acceso específica de terminal se deriva, por el proveedor del terminal, de una clave maestra de acceso específica de la entidad de control usando el número de identificación de terminal, o un número adicional de identificación de terminal de pago. El proveedor del terminal recupera la clave maestra de acceso específica de la entidad de control, por ejemplo, a partir de un TRSM en el que está almacenada la clave.

El proveedor del terminal podría entonces realizar una operación de derivación en la clave maestra de acceso específica de la entidad de control usando el número de identificación de terminal de ese terminal de pago. Por ejemplo, podría utilizarse el encadenamiento cifrado en bloque. El algoritmo de encadenamiento cifrado en bloque (CBC) descrito en ISO 9797-1, por ejemplo, utiliza 16 bytes (longitud de una clave de doble longitud) de datos de derivación. Esta derivación puede componerse de los últimos ocho bytes (parte derecha) del número de identificación de terminal en decimales en código binario (BCD) con un relleno de ceros binarios a la izquierda y los primeros ocho bytes (parte izquierda) del número de identificación de terminal en decimales en código binario (BCD) con un relleno de 8 bytes XOR [FF FF FF FF FF FF FF FF]. En este contexto, F representa el mayor valor hexadecimal y XOR representa el "o-exclusivo", que es una operación lógica que resulta verdadera siempre que las entradas sean diferentes, es decir una es verdadera, la otra es falsa.

Un número de identificación de terminal de, por ejemplo, 123456789 produce una parte derecha de [00 00 00 01 23 45 67 89] y una parte izquierda de [00 00 00 01 23 45 67 89] XOR [FF FF FF FF FF FF FF FF]= [FF FF FF FE DC BA 98 76]. Esto resulta en una derivación de bloque de datos de [FF FF FF FE DC BA 98 76 00 00 00 01 23 45 67 89] usada para la derivación de la clave maestra de acceso específica de la entidad de control, que lleva a la clave de acceso específica de terminal.

Una vez que la clave se alimenta (o "inyecta") en el terminal de pago, el terminal de pago puede entregarse e instalarse en el establecimiento del propietario.

En algunos ejemplos, la clave maestra de acceso específica de la entidad de control se transmite al proveedor del terminal en una manera que asegura la confidencialidad por la entidad de control. La entidad de control, por ejemplo, genera la clave maestra de acceso específica de la entidad de control, la cual se usa para derivar la clave de acceso específica de terminal en el extremo de la entidad de control, y para la implantación de la clave de acceso específica de terminal en el terminal de pago por el proveedor del terminal.

En algunos ejemplos, la autorización para cualquier número de operadores y/o proveedores de pago, y de ese modo utilización del terminal de pago por esos operadores y/o proveedores de pago, puede añadirse dinámicamente, sin intervención física en el terminal de pago. En otras palabras, la utilización del terminal de pago por esos operadores y/o proveedores de pago puede ser concedida por la entidad de control de manera remota, sin contacto físico con el terminal de pago.

Desde que la clave de transporte específica de operador y de terminal se determina por el proveedor de pago, por ejemplo, transmitir la clave maestra de la que se derivan las claves de transporte específica de operador y de terminal individuales, o transmitir la clave de transporte específica de operador y de terminal en sí misma, la utilización del terminal de pago por diferentes operadores no se limita a un número máximo predefinido de usuarios diferentes.

Solo la clave de acceso específica de terminal se preinstala en el terminal de pago, todas las demás claves que se necesitan para las transacciones de pago realizadas por los diferentes operadores se proporcionan al terminal de pago en posteriores transmisiones cifradas. Estas transmisiones se cifran con la clave de acceso específica de terminal o se cifran con claves derivadas de claves ya recibidas.

En algunos ejemplos, la manera que asegura la confidencialidad, en la que la clave de transporte maestro específica de operador se transmite desde el proveedor de pago a la entidad de control, es un algoritmo asimétrico de cifrado de clave. Generalmente, una comunicación que se envía no debería ser legible durante el tránsito (preservando la confidencialidad) y la comunicación no debería ser modificable durante el tránsito (preservando la integridad de la comunicación). Combinar criptografía de clave pública con un método de cifrado de envoltorio de clave pública (EPKE), permite una comunicación relativamente segura en un entorno de red abierta. En criptografía de clave pública, se utilizan algoritmos de clave asimétrica, donde una clave utilizada para cifrar un mensaje no es la misma que la clave utilizada para descifrar el mensaje. Cada usuario tiene un par de claves criptográficas – una clave pública de cifrado y una clave privada de descifrado. Las claves están relacionadas matemáticamente, pero los parámetros se escogen de tal manera que calcular la clave privada a partir de la clave publíca es o imposible o extremadamente costoso.

El sistema informatizado de la entidad de control divulgado está dispuesto para configurar un terminal de pago, el cual tiene un número de identificación de terminal, para poder utilizarse como terminal de pago compartido por una pluralidad de operadores con segregación criptográfica entre los diferentes operadores del terminal de pago.

El sistema de la entidad de control podría estar dispuesto para derivar una clave de transporte específica de operador y de terminal a partir de una clave de transporte maestro específica de operador usando el número de identificación de terminal.

El sistema de la entidad de control podría estar dispuesto para cifrar la clave de transporte específica de operador y de terminal simétricamente con la clave de acceso específica de terminal y transmitirir la clave cifrada de transporte específica de operador y de terminal al terminal de pago.

En algunos ejemplos, el sistema informatizado de la entidad de control está dispuesto para configurar el terminal de pago según alguno o todos los ejemplos mencionados anteriormente.

El sistema informatizado del proveedor de pago divulgado está dispuesto para configurar un terminal de pago, el cual tiene un número de identificación de terminal, para poder utilizarse como terminal de pago compartido por una pluralidad de operadores con segregación criptográfica entre los diferentes operadores del terminal de pago.

El sistema del proveedor de pago podría derivar una clave de transporte específica de operador y de terminal a partir de una clave de transporte maestro específica de operador usando el número de identificación de terminal, y podría derivar una clave de cifrado inicial específica de operador y de terminal a partir de la clave base de derivación específica de operador usando también el número de identificación de terminal, o usando un número adicional de identificación de terminal de pago.

El sistema del proveedor de pago está dispuesto para transmitir la clave de transporte maestro específica de operador a una entidad de control de una manera que asegura la confidencialidad, en la cual el terminal de pago está asociado con la entidad de control. Alternativamente, el sistema del proveedor de pago está dispuesto para transmitir la clave de transporte específica de operador y de terminal a la entidad de control de una manera que asegura la confidencialidad.

El sistema del proveedor de pago podría cifrar la clave de cifrado inicial específica de operador y de terminal simétricamente con la clave de transporte específica de operador y de terminal, y podría alimentar la clave de cifrado inicial específica de operador y de terminal en el terminal de pago transmitir la clave de cifrado inicial específica de operador cifrado y de terminal al terminal de pago.

El sistema del proveedor de pago podría derivar una clave de cifrado específica de operador y de terminal a partir de la clave de cifrado inicial específica de operador y de terminal usando un número específico de transacción asociado con la transacción, cuando se realiza una transacción con el terminal de pago.

En algunos ejemplos, el sistema informatizado del proveedor de pago está dispuesto para configurar el terminal de pago según alguno o todos los ejemplos mencionados anteriormente.

El terminal de pago divulgado está dispuesto para utilizarse como terminal de pago compartido por una pluralidad de operadores con segregación criptográfica entre los diferentes operadores del terminal de pago. El terminal de pago está dispuesto para comunicarse con al menos un proveedor de pago para realizar transacciones de pago y está dispuesto para asociarse con una entidad de control que controla la utilización del terminal de pago de manera selectiva según el operador.

El terminal de pago tiene al menos un almacenamiento seguro (TRSM) utilizado para la gestión de la clave. El al menos uno TRSM, como se menciona anteriormente, por ejemplo, tiene características físicas que hacen que las manipulaciones satisfactorias sean difíciles e improbables, por ejemplo como se define en el document ANSI X9,24-1-2009 *(Retail Financial Services Symmetric Clave Management Part 1: Using Symmetric Techniques).* Tales características físicas podrían incluir, por ejemplo, una memoria en la que las claves criptográficas se almacenan, la cual se oxida cuando entra en contacto con el aire, es decir se autodestruye, para hacer ilegible cualquier clave criptográfica almacenada.

El (los) modulo(s) de seguridad a prueba de manipulaciones del terminal de pago está (están) dispuesto(s) para almacenar y gestionar una o más claves criptográficas en el TRSM, esto es al menos la clave de acceso específica de terminal, para permitir la utilización del terminal de pago para que la entidad de control pueda controlarlo de manera selectiva según el operador.

En algunos ejemplos la al menos una clave de transporte específica de operador y de terminal y/o la al menos una clave de cifrado inicial específica de operador cifrado y de terminal podría descifrarse en el terminal de pago tras su recepción o se introduce. La al menos una clave de transporte específica de operador y de terminal y/o la al menos una clave de cifrado inicial específica de operador y de terminal podría también almacenarse y gestionarse en la memoria segura, por ejemplo el TRSM: La clave de transporte específica de operador descifrado y de terminal almacenada con seguridad y/o la clave de cifrado inicial específica de operador descifrado y de terminal almacenada con seguridad está/están entonces fácilmente disponibles para el descifrado de la clave de cifrado inicial específica de operador cifrado y de terminal y/o para obtener la clave de cifrado específica de operador y de terminal.

En otros ejemplos en los que la versión descifrada de la clave de transporte específica de operador y de terminal y/o la clave de cifrado inicial específica de operador y de terminal no está/están almacenada(s) en un almacenamiento seguro del terminal de pago, por ejemplo, el TRSM del terminal de pago, la clave de transporte específica de operador cifrado y de terminal y/o la clave de cifrado inicial específica de operador cifrado y de terminal pueden almacenarse en una memoria normal (poco segura), y sólo se descifra(n) "sobre la marcha" cuando se necesita para el descifrado de la clave de cifrado inicial específica de operador cifrado y de terminal, y/o para obtener la clave de cifrado específica de operador y de terminal para realizar una transacción con el terminal de pago, por ejemplo una transacción de pago.

En algunos ejemplos el terminal de pago se configura según alguno o todos los ejemplos mencionados anteriormente.

Breve descripción de los dibujos

Realizaciones ejemplares de la invención se describen ahora, también relacionadas los dibujos adjuntos, donde

la Figura 1 ilustra un diagrama que resume las generaciones de clave criptográfica, derivaciones, e intercambios entre diferentes agentes de la transacción del pago,

la Figura 2 ilustra un algoritmo ejemplar de derivación de clave que genera una nueva clave derivada de una clave básica,

la Figura 3 ilustra relaciones funcionales entre los diferentes agentes de la transacción del pago mostrados en la Figura 1,

la Figura 4 ilustra intercambios de clave para una transmisión de datos cifrados,

la Figura 5 ilustra un terminal de pago ejemplar para tarjetas de pago,

'la Figura 6 ilustra un almacenamiento seguro del terminal de pago mostrado en la Figura 5,

la Figura 7 ilustra un sistema informático ejemplar, según el sistema de la entidad de control y el sistema del proveedor de pago descrito en el presente documento, dispuesto para configurar el terminal de pago.

Los dibujos y la descripción de los dibujos son de ejemplos de la invención, y no son de la invención en sí misma.

Descripción de realizaciones

En la realización ejemplar ilustrada por la Figura 1, se muestran los intercambios de clave entre el proveedor de pago 2, por ejemplo el adquiriente de una aerolínea, la entidad de control 3, por ejemplo el propietario del aeropuerto, el fabricante del terminal de pago, es decir el proveedor del terminal 5, y el terminal de pago 1.

Las flechas curvas indican una derivación, ya sea usando el número de identificación de terminal 44 del terminal de pago 1, o un número específico de transacción 27 de una transacción en curso 26. Las derivaciones de clave basadas en el número de identificación de terminal 44 se indican como S1, S3, S5, S7, y S10. Las derivaciones de clave basadas en un número específico de transacción 27 se indican como S13 y S14. Las flechas con línea discontinua indican cifrados simétricos S8 y S11, mientras que las flechas discontinuas indican transmisiones seguras S2, S4, y S6, por ejemplo por un mensajero. Las cajas con línea discontinua alrededor de las claves indican las copias enviadas de esas claves.

La entidad de control 3 genera una clave maestra de acceso específica de la entidad de control K1, y transmite de manera segura S2 la clave maestra de acceso específica de la entidad de control K1 al proveedor del terminal 5 que fabrica el terminal de pago 1 para la entidad de control 3. El proveedor del terminal 5 almacena esta clave, así como lo hace con las claves de todas las demás entidades de control con las que el proveedor del terminal 5 negocia. Esta clave maestra de acceso específica de la entidad de control K1 es única para cada relación entidad de control-a-terminal, es decir contrato de negocio.

El proveedor del terminal 5 deriva S3 una clave de acceso específica de terminal K2 para cada terminal de pago 1 basada en la clave maestra de acceso específica de la entidad de control K1 y el número de identificación 44 del terminal de pago 1. El futuro propietario del terminal de pago 1, es decir la entidad de control 3, puede derivar S1 la clave individual de acceso específica de terminal K2 de la misma forma, ya que el proveedor del terminal 5 y la entidad de control 3 comparten el mismo algoritmo de derivación de clave (ver la Figura 2). La clave de acceso específica de terminal K2 se implanta S4 en el terminal de pago 1 correspondiente en una sala segura en las instalaciones de fabricación del proveedor del terminal.

La forma de implantación de la clave de acceso específica de terminal K2 en el terminal de pago 1 descrita anteriormente es opcional. También se cubren varias formas alternativas para la implantación de la clave de acceso específica de terminal.

El proveedor de pago 2 genera una clave de transporte maestro específica de operador K3 y transmite de manera segura S6 la clave de transporte maestro específica de operador K3 a la entidad de control 3, por ejemplo, por medio de un algoritmo de cifrado asimétrico o por un mensajero certificado. Esta clave de transporte maestro específica de operador K3 es única para cada relación entidad de control-a-operador, es decir contrato de negocio.

La entidad de control 3 deriva S7 una clave de transporte específica de operador y de terminal K4 a partir de la clave de transporte maestro específica de operador K3 y el número de identificación de terminal 44 del terminal de pago 1. El proveedor de pago 2 puede derivar S5 la clave individual de transporte específica de operador y de terminal K4 de la misma forma, ya que el proveedor de pago 2 y la entidad de control 3 comparten el mismo algoritmo de derivación de clave (ver la Figura 2).

La entidad de control 3 cifra S8 la clave individual de transporte específica de operador y de terminal K4 con la correspondiente clave de acceso específica de terminal K2 antes de transmitir la clave de transporte específica de operador y de terminal K4 al correspondiente terminal de pago 1. La entidad de control 3 transmite S9 la clave de transporte específica de operador y de terminal K4 al correspondiente terminal de pago 1. En otras palabras, cada clave de transporte específica de operador y de terminal K4 se cifra S8 por una clave de acceso individual específica de terminal K2 correspondiente al mismo número de identificación de terminal 44, y solo puede ser descifrado en el correspondiente terminal de pago 1, el cual puede cargarse S4 con la misma clave de acceso específica de terminal K2. En algunas realizaciones, la clave de transporte específica de operador y de terminal K4 se descifra con la correspondiente clave de acceso específica de terminal K2 tras su recepción en el terminal de pago 1, y la clave de transporte específica de operador descifrado y de terminal K4 se almacena en el terminal de pago 1, por ejemplo de una manera segura, por ejemplo en un almacenamiento seguro (TRSM) 45 (Figura 6).

En una realización alternativa, la clave de transporte específica de operador y de terminal K4 no se descifra tras su recepción, pero se almacena aún de forma cifrada en el terminal de pago 1, y solo se descifra cuando se necesita, es decir se "descifra sobre la marcha". En esta realización alternative, la seguridad para la clave de transporte específica de operador y de terminal K4 se proporciona manteniéndola cifrada, preferiblemente a almacenarla de forma cifrada en un almacenamiento seguro, tal como un TRSM 45. Por lo tanto, en esta realización alternativa, la clave de transporte específica de operador y de terminal K4 puede ser almacenada opcionalmente en una memoria no segura, por ejemplo una memoria normal (por ejemplo, un ROM) fuera del TRSM 45.

El proveedor de pago 2 genera una clave base de derivación específica de operador K5, que es única para cada relación operador-a-proveedor de pago, es decir contrato de negocio. El proveedor de pago 2 deriva S10 una clave inicial individual de cifrado específica de operador y de terminal K6 para cada terminal de pago 1 a partir de la clave base de derivación específica de operador K5 y el número de identificación de terminal 44 del terminal de pagos 1.

El proveedor de pago 2 cifra S11 las claves iniciales individuales específicas del operador y específicas del terminal K6 con las correspondientes claves de transporte específicas del operador y específicas del terminal K4 antes de transmitir las claves iniciales de cifrado específicas del operador y específicas del terminal K6 al correspondiente terminal de pagos 1. El proveedor de pago 2 transmite S12 la clave de cifrado inicial específica de operador cifrado y de terminal K6 al correspondiente terminal de pago 1. En otras palabras, cada clave de cifrado inicial específica de operador y de terminal K6 se cifra S11 con una clave individual de transporte específica de operador y de terminal K4 que se corresponde con el mismo número de identificación de terminal 6 y solo puede descifrarse en el correspondiente terminal de pago 1, el cual se ha alimentado en S9' con la clave de transporte específica de operador y de terminal respectiva K4. En algunas realizaciones, la clave de cifrado inicial específica de operador y de terminal K6 se descifra con la correspondiente clave de transporte específica de operador y de terminal K4 tras su recepción en el terminal de pago 1, y la clave de cifrado inicial específica de operador descifrado y de terminal K6 se almacena en el terminal de pago 1, por ejemplo de una manera segura, por ejemplo en un almacenamiento seguro (TRSM) 45 (la Figura 6).

En una realización alternativa, la clave de cifrado inicial específica de operador y de terminal K6 no se descifra tras su recepción, pero todavía se almacena en la forma cifrada en el terminal de pago 1, y solo se descifra cuando se necesita, es decir se "descifra sobre la marcha". En esta realización alternative, la seguridad para la clave de cifrado inicial específica de operador y de terminal K6 se proporciona manteniéndola cifrada, preferiblemente a almacenarla en forma cifrada en un almacenamiento seguro, tal como un TRSM 45. Por lo tanto, en esta realización alternativa, la clave de cifrado inicial específica de operador y de terminal K6 puede ser almacenada opcionalmente en una memoria no segura, por ejemplo una memoria normal (por ejemplo, un ROM) fuera del TRSM 45.

El terminal de pago 1 deriva S14 una clave de cifrado específica de operador y de terminal K7 a partir de la clave de cifrado inicial específica de operador y de terminal K6 y el número específico de transacción 27 de una transacción en curso 26. El proveedor de pago 2 puede derivar S13 la clave individual de cifrado específica de operador y de terminal K7 de la misma forma, ya que el terminal de pago 1 y el proveedor de pago 2 comparten el mismo algoritmo de derivación de clave (ver la Figura 2).

La clave de cifrado específica de operador y de terminal K7 es la base de la derivación, por ejemplo, una clave de cifrado PIN, claves de cifrado de datos confidenciales, y claves de firma MAC utilizadas en la transmisión de datos cifrados S17 entre el terminal de pago 1 y el proveedor de pago 2, por ejemplo operaciones de transferencia de fondos, peticiones de autenticación, o similares, durante una transacción 26.

Un algoritmo de derivación de clave ejemplar, el encadenamiento cifrado en bloque (CBC) algoritmo descrito anteriormente, se muestra en la Figura 2. Una clave básica que tiene n bloques 10, 11, 12 de clave de base se utiliza para crear nuevas claves, que se basan en la clave de base y datos de derivación 15, y tiene n bloques 18, 19, 20 de clave de derivación. Estos datos de derivación 15 pueden ser un número hexadecimal, basado en el número de identificación de terminal 44 o un número específico de transacción 27, con una longitud correspondiente a la clave de base, por ejemplo el doble de la longitud de la clave.

Se genera una nueva clave, es decir se deriva, a partir de la clave de base cifrando todos los bloques 10, 11, a 12 de clave de base con un cifrado en bloque 16, que tiene un tamaño de cifrado de bloque determinado. El cifrado es secuencial, y la clave de base se rellena a un múltiplo del tamaño de cifrado de bloque.

El primer bloque 10 de clave de base es o-exclusivo 14, es decir se suma en módulo dos, con un vector de inicialización (IV) 13. Sin este vector de inicialización 13, cada posterior derivación del mismo primer bloque produciría el mismo bloque de derivación.

Puesto que este algoritmo se usa para la derivación de clave, basado en un número específico del terminal o específico de transacción 44, 27, y no para el cifrado de datos, es decir los datos de derivación 15 utilizados para el cifrado en bloque 16 cambian para cada clave derivada, el o-exclusivo del primer bloque de clave de base 10 con un vector de inicialización 13 es opcional.

El segundo bloque de clave de base 11 se combina 17 con el primer bloque de derivación de clave 18 haciendo o-exclusivo 14. Por tanto, una entrada del cifrado en bloque 16 es dependiente de una salida de un previo cifrado en bloque 16. El algoritmo es, por tanto, denominado algoritmo de encadenamiento cifrado en bloque (CBC). El segundo bloque de clave de base 11 o-exclusivo el primer bloque de derivación de clave 18 produce el segundo bloque de derivación de clave 19 tras un cifrado en bloque 16 con los datos de derivación 15.

Este proceso se repite hasta que todas las n claves de los bloques de base han hecho o-exclusivo con el previo bloque de derivación de clave y se han cifrado con los datos de derivación 15. De esta forma, cada bloque de derivación de clave depende de todos los bloques de clave de base procesados hasta el momento. La clave derivada resultante tiene la misma longitud que la clave de base. Dado que esta derivación es una regla de mapeo única, entidades diferentes en ubicaciones diferentes pueden derivar la misma clave a partir de la misma clave de base con el algoritmo descrito anteriormente.

Las relaciones funcionales y un orden cronológico de actividades (se refiere a los símbolos 21 a 26 en orden ascendente) para una transacción de pago, ejecutadas por diferentes agentes de pago y transacción, se ilustran en un ejemplo mostrado en la Figura 3.

La entidad de control 1 encarga un proveedor del terminal 5, es decir un fabricante del terminal de pago, para producir el terminal de pago 1 realizando un contrato de negocio, es decir encargando 21 el terminal de pago 1 a partir del proveedor del terminal 5.

El proveedor del terminal 5 entrega 22 el terminal de pago 1 basado en las especificaciones de la entidad de control a la entidad de control 3 una vez terminado el terminal de pago 1. Las especificaciones incluyen, por ejemplo, una determinada clave de acceso implantada, por ejemplo una clave de acceso específica de terminal K2, derivada de una clave maestra de acceso específica de la entidad de control K1 y el número de identificación de terminal 44 del terminal de pago 1.

Tras la entrega 22 del terminal de pago 1 a la entidad de control 3, un operador 4 puede solicitar la utilización 23 del terminal de pago 1. El operador puede, por ejemplo, alquilar el terminal de pago 1 para la entidad de control 3 para la duración de un contrato de negocio.

Una vez que la entidad de control 3 concede al operador 4 el derecho a utilizar el terminal de pago 1 (la concesión se etiqueta como 24) una clave de transporte específica de operador y de terminal K4 se inyecta S9' en el terminal de pago 1 por la entidad de control 3. La clave de transporte específica de operador y de terminal K4 se escoge individualmente para el operador 4 y permite al operador 4 operar el terminal de pago 1.

El terminal de pago 1 puede entonces usarse 25 por el operador 4 para realizar transacciones 26 con uno o más proveedores de pago 2, es decir adquirientes del operador 4. Durante estas transacciones 26 se intercambian transmisiones cifradas de datos confidenciales S17 entre el terminal de pago 1 y un proveedor de pago 2.

Se muestran, en la Figura 4, actividades ejemplares para preparar una transacción de pago 26 en un mostrador de facturación. En S15, la utilización del terminal de pago 1, en primer lugar, se solicita en 23 por un operador 4, por ejemplo cuando el operador 4 abre una relación contractual con la entidad de control 3.

Si la utilización del terminal de pago 1 se concede en 24 por la entidad de control 3 del aeropuerto al operador 2, una clave de transporte específica de operador y de terminal K4 se alimenta en el terminal de pago S9'.

La clave de transporte específica de operador y de terminal K4 se cifra simétricamente S8 con la clave de acceso específica de terminal K2, donde ambas claves se derivan S1, S7 con el mismo número de identificación de terminal 44. La inyección de la clave de transporte específica de operador y de terminal K4, etiquetada como S9' en la Figura 4, implica transmitir S9 la clave de transporte K4 específica de operador simétricamente cifrado y de terminal a partir la entidad de control 3 al terminal de pago 1. En algunas realizaciones, la clave de inyección S9' también implica descifrar la clave de transporte específica de operador cifrado y de terminal K4 con la clave de acceso específica de terminal K2, la cual se almacenó previamente en el terminal de pago 1, por ejemplo durante la producción, y el almacenamiento de la clave de transporte específica de operador y de terminal K4 en el terminal de pago 1 cuando se descifra, por ejemplo de una manera segura. En otras realizaciones, el descifrado de la clave de transporte específica de operador y de terminal K4 podría aplazarse hasta que la clave de transporte específica de operador cuando se descifra y de terminal K4 se necesite realmente. Puede, por tanto, almacenarse de una manera poco segura. La actividad de descifrar la clave de transporte específica de operador cifrado y de terminal K4 con la clave de acceso específica de terminal almacenada K2 en el terminal de pago 1 "sobre la marcha" formará parte de la parte inicial del descifrado de la clave de cifrado inicial específica de operador cifrado y de terminal K6 descrita abajo.

Como el nombre sugiere, la clave de transporte específica de operador y de terminal K4 se usa para transportar otra clave de cifrado de una manera que asegura la confidencialidad, es decir con cifrado. Una clave de cifrado inicial

específica de operador y de terminal K6 se alimenta en el terminal de pago S12', que es la base de las claves de cifrado de la transacción.

La clave de cifrado inicial específica de operador y de terminal K6 se cifra simétricamente S11 con la clave de transporte específica de operador y de terminal K4, donde ambas claves se derivan S7, S10 con el mismo número de identificación de terminal 44. La inyección de la clave de cifrado inicial específica de operador y de terminal K6, etiquetada como S12' en la Figura 4, implica transmitir S12 la clave de cifrado inicial específica de operador simétricamente cifrado y de terminal simétricamente cifrado K6 a partir del proveedor de pago 2 al terminal de pago 1. En algunas realizaciones, la clave de inyección S12' también implica descifrar la clave de cifrado inicial específica de operador cifrado y de terminal K6 con la clave de transporte específica de operador descifrado y de terminal K4 en el terminal de pago 1, y el almacenamiento de la clave de cifrado inicial específica de operador y de terminal K6 cuando se descifra en el terminal de pago 1, por ejemplo de una manera segura. En otras realizaciones, el descifrado de la clave de cifrado inicial específica de operador cifrado y de terminal K6 podría aplazarse hasta que el descifrado de la clave de cifrado inicial específica de operador y de terminal K6 se necesite realmente. Puede, por tanto, almacenarse de una manera poco segura. La actividad de descifrar la clave de cifrado inicial específica de operador cifrado y de terminal K6 con la clave de transporte específica de operador y de terminal K4 descifrado en el terminal de pago 1 "sobre la marcha" formará parte de la derivación S14 de la clave de cifrado específica de operador y de terminal K7 descrita abajo.

En cierta etapa, se necesitará comenzar a realizar algunas transacciones con el terminal de pago 1 para uno de los operadores 4. Por ejemplo, en el caso de quioscos de aeropuerto compartidos, un cliente seleccionaría la aerolínea en cuestión (= operador 4) en la pantalla del quiosco; y en el caso de estaciones de trabajo de facturación compartidas, un agente de una aerolínea (= agente del operador 4) se registraría en el terminal de pago para comenzar la facturación del vuelo.

Como primer subproceso, se selecciona la clave de cifrado inicial específica de operador y de terminal K6 asociada con el operador 4 (por ejemplo la aerolínea) en cuestión, dependiendo del operador asociado con el cliente o el agente que realiza la transacción.

En algunas realizaciones opcionales, el terminal de pago 1 proporciona más de un modo de uso, o más de un tipo de "comportamiento de dispositivo". El terminal de pago 1 se dispone para proporcionar varios tipos de comportamiento de dispositivo. En estas realizaciones, como otro subproceso opcional, cuando se empieza a utilizar el terminal de pago 2 para realizar una transacción, el comportamiento de dispositivo asociado con el operador en cuestión se selecciona de manera automática y dinámica. Por ejemplo, dos modos de uso diferentes podrían proporcionarse en algunas realizaciones: Un "modo de uso directo" y un "modo autorizado". En el modo de uso directo el terminal de pago 1 se inicializa para retornar todos los datos de pago a una solicitud del operador sobre una conexión en serie al operador 4; y depende entonces de la solicitud de operador transmitir los datos al proveedor de pago 2. En el modo autorizado, el terminal de pago 1 se inicializa para establecer una conexión directa sobre una interfaz de red proporcionando acceso a una red de área extendida (WAN) al proveedor de pago 2. En realizaciones en las que el terminal de pago 1 para proporcionar el modo autorizado el terminal de pago , está por tanto equipado con una interfaz de red adecuada, y el terminal de pago 1 está preconfigurado con parámetros de red (tales como IP, DNS, DHCP, Cortafuegos, VPN, ..) adecuados para comunicar directamente con el proveedor de pago 2 sobre la WAN. Si se selecciona el modo autorizado, una conexión TCP/IP se establece con el host del proveedor de pago, y todos los mensajes de configuración adicionales se iniciarán por el host del proveedor de pago usando esta conexión.

El código XML ejemplar de abajo muestra un ejemplo de la inicialización del modo autorizado. Puede verse a partir del código XML ejemplar que la selección automática se controla por una variable llamada "<modoUso>" que, en este ejemplo, puede tomar los valores "autorizado" y "directo":

```
<?xml version=" 1,0" ?>
<solicitudOperadorUtilizacion>
<codigoOperador> M1 </codigoOperador>
<codigoProveedorPago>P1 </codigoProveedorPago>
<modoUso>autorizado</modoUso>
<parametrosRed>
<host>pago.com</host>
<puerto> 1234</puerto>
</parametrosRed>
<datosAutenticacion>66678d4fOea8bda1 </datosAutenticacion>
</solicitudOperadorUtilizacion>
```

Como otro subproceso, después de que la clave de cifrado inicial específica de operador y de terminal K6 se haya obtenido y descifrado en el terminal de pago 1 (ya sea previamente, o "sobre la marcha" durante la etapa de la inicialización-de-una-transacción), las claves de transacción para actividades adicionales de la transacción pueden derivarse de la clave de cifrado inicial específica de operador descifrado y de terminal K6 usando un número

específico de transacción 27, que es etiquetado como S14 en la Figura 4. Como se indica en el etiquetado, la derivación S14 de la clave de cifrado específica de operador y de terminal K7 a partir de la clave de cifrado inicial específica de operador y de terminal K6 por el terminal de pago 1 usando el número específico de transacción 27 es una de esas claves de la transacción. La derivación se realiza de forma análoga en el proveedor de pago 2, etiquetado ahí como S13.

Las claves adicionales de la transacción, derivadas a partir de la clave de cifrado específica de operador y de terminal K7 usando el número específico de transacción 27 u otro número específico de transacción, por ejemplo una clave de cifrado PIN, claves de cifrado de datos confidenciales, y claves de firma MAC, también se cubren por la actividad etiquetada S13, S14 en la Figura 4.

En la Figura 4, en realizaciones en las que el terminal de pago 1 tiene una funcionalidad de modo de uso opcional, la etiqueta S14 también representa la actividad opcional de la selección dependiente del operador del modo de uso (por ejemplo la selección del modo de uso directo o el modo autorizado).

Estas claves adicionales de la transacción se utilizan para cifrar S16 datos confidenciales para la transmisión entre el terminal de pago 1 y el proveedor de pago 2, por ejemplo un PIN para una cuenta que va a ser debitada.

Por tanto, la verdadera transmisión cifrada de datos confidenciales S17 de la transacción de pago 26 entre el terminal de pago 1 y el proveedor de pago 2 puede realizarse usando las anteriormente claves de la transacción.

Un terminal de pago 1 ejemplar, en el que se realizan inyecciones de clave etiquetadas S9' y S12' en la Figura 4 y descritas en conjunción con la Figura 1 y la Figura, se ilustra en la Figura 5.

El terminal de pago 1 mostrado en la Figura 5 tiene un teclado de PIN 41 para aceptar y cifrar el número personal de identificación (PIN) del titular de una tarjeta. El teclado de PIN 41 utiliza acceso a una tarjeta de pago 50 (en el caso de una tarjeta con chip) y permite la segura introducción del PIN en el terminal de pago 1 y posterior cifrado del PIN por el terminal de pago 1.

El PIN se cifra inmediatamente cuando se introduce y se crea un bloque PIN cifrado. Este bloque PIN cifrado se elimina tan pronto como se haya enviado desde el teclado de PIN 41 al terminal de pago adjunto 1 y/o la tarjeta con chip 50. Los PIN se cifran usando un algoritmo triple DES.

El terminal de pago 1 está equipado con una pantalla 40 para mostrar datos relevantes al cliente, por ejemplo un pasajero, y al operador 4, como por ejemplo, una cantidad de orden de pago o un estado de autenticación del PIN introducido.

De manera adicional, el terminal de pago 1 está equipado con un lector con una ranura para tarjetas de pago 42, donde la tarjeta de pago 50 se inserta en el terminal de pago 1 y los datos de la tarjeta se leen de la tarjeta de pago 50, por ejemplo para la verificación de la identidad del cliente, es decir comprobar si el cliente puede proporcionar el PIN correcto para la tarjeta de pago 50.

En realizaciones alternativas el terminal de pago 1 está además equipado con un lector de banda magnética de tarjetas de pago, o como alternativa, al lector con una ranura para tarjetas de pago 42. En estas realizaciones alternativas los datos de la tarjeta se leen de la tarjeta de pago 50 pasando the tarjeta de pago 50 por el lector de banda magnética.

La Figura 6 describe características adicionales del terminal de pago 1 ejemplar ilustrado en la Figura 5. El terminal de pago 1 tiene una memoria 43 y un almacenamiento seguro (TRSM) 45. El TRSM 45 puede ser una partición lógica de la memoria 43 o puede, alternativamente, ser un módulo individual lectura-segura-e-intercambio-de-datos-seguro(SRED), en el que se almacenan las claves individuales de acceso específicas del terminal, de transporte y cifrado K2, y opcionalmente las claves de cifrado K4 y K6. La memoria 43 incluye una memoria no volátil donde se almacena código ejecutable de programas, por ejemplo código C compilado, y/o código script interpretable.

El número único de identificación de terminal 44 del terminal de pago está grabado en la cubierta del terminal de pago 1. En un ejemplo alternativo del terminal de pago 1, el número de identificación de terminal 44 se almacena en la memoria 43 y puede leers por partes autorizadas. De esta forma, el número de identificación de terminal 44 no es visible para nadie que no esté autorizado.

Una representación gráfica de un sistema informatizado 100 ejemplar dispuesto para ejecutar una serie de instrucciones 110, para provocar que el sistema informatizado realice cualquiera de las metodologías utilizadas para la configuración del terminal de pago 1 para una transacción de pago 26, como se describe en el presente documento, se muestra en la Figura 7. El sistema informatizado de la entidad de control y el sistema informatizado del proveedor de pago podrían ser tal sistema informatizado 100.

El sistema informatizado 100 incluye un procesador 102, una memoria principal 104 y una interfaz de red 108. La

memoria principal 104 incluye un espacio de usuario 104', que está asociado con aplicaciones ejecutadas por el usuario, y un espacio de núcleo 104", que está reservado para las aplicaciones asociadas con el sistema operativo y asociadas con el hardware. El sistema informatizado 100 además incluye una memoria estática 106, por ejemplo unidades flash no extraíbles y/o unidades de estado sólido y/o a una tarjeta extraíble SD Micro o Mini, que almacena permanentemente software que permite al sistema informatizado 100 ejecutar funciones del sistema informatizado 100. Además, podría incluir una visualización de vídeo 103, un módulo de control de interfaz de usuario 107 y/o un dispositivo de entrada alfanumérica y de cursor 105. Opcionalmente, podrían presentarse interfaces E/S 109, tales como lector de tarjetas e interfaces USB. Los componentes del sistema informatizado 102 a 109 están interconectados por un bus de datos 101.

En algunas realizaciones ejemplares, el software programado para llevar a cabo el método de configuración del terminal de pago 1 tratado en el presente documento se almacena en la memoria estática 106; en otras realizaciones ejemplares, se utilizan bases de datos externas. El método de configuración del terminal de pago 1 tratado en el presente documento se realiza a través de la interfaz de red del dispositivo 108.

Una serie de instrucciones ejecutables (es decir software) 110 que realizan alguna, o todas, las metodologías descritas anteriormente, residen de manera permanente completa, o al menos parcialmente, en la memoria no volátil 106. Cuando las instrucciones se ejecutan, los datos del proceso residen en la memoria principal 104 y/o en el procesador 102. The software 110 podría además transmitirse o recibirse como señal propagada 111 a través de la interfaz de red del dispositivo 108 desde/a un servidor software en una red de area local o Internet.

Aunque ciertos métodos y productos construídos según las instrucciones de la invención se han descrito en el presente documento, el alcance de cobertura de esta patente no se limita a ello.

REIVINDICACIONES

1. Método de configuración de un terminal de pago (1) para poder utilizarse como terminal de pago (1) compartido por una pluralidad de operadores (4) con segregación criptográfica entre los diferentes operadores (4) del terminal de pago (1), disponiéndose el terminal de pago (1) para comunicarse (S17) con al menos un proveedor de pago (2) para realizar transacciones de pago (26), y asociándose con una entidad de control (3) que controla la utilización del terminal de pago (1) de manera selectiva según el operador, teniendo el terminal (1) una clave de acceso específica de terminal (K2) almacenada en el mismo, y un número de identificación de terminal (44), comprendiendo el método:

transmitir una clave de transporte específica de operador y de terminal (K4), cifrada por la clave de acceso específica de terminal (K2), al terminal de pago (1);

descifrar la clave de transporte específica de operador y terminal cifrada (K4) en el terminal de pago (1) con la clave de acceso específica de terminal almacenada (K2);

en el que la utilización del terminal de pago (1) por parte de los operadores (4) y/o de los proveedores de pago (2) se concede por la entidad de control (3) de manera remota, sin contacto físico con el terminal de pago (1), introduciendo la clave de transporte específica de operador y de terminal (K4) en el terminal de pago (1), es decir almacenando la clave de transporte específica de operador y de terminal (K4) en el terminal de pago (1) de forma cifrada o no cifrada;

derivar (S10), por parte del proveedor de pago (2), una clave de cifrado inicial específica de operador y de terminal (K6) a partir de una clave de derivación de base específica de operador (K5) usando el número de identificación de terminal (44), o un número de identificación adicional del terminal de pago (1), y cifrar simétricamente (S11) la clave de cifrado inicial específica de operador y de terminal (K6) con la clave de transporte específica de operador y de terminal (K4);

transmitir (S12) la clave de cifrado inicial específica de operador y de terminal cifrada (K6) al terminal de pago (1);

descifrar la clave de cifrado inicial específica de operador y de terminal cifrada (K6) en el terminal de pago (1) con la clave de transporte específica de operador y de terminal descifrada (K4);

derivar (S13, S14), tanto en el proveedor de pago (2) como en el terminal de pago (1), una clave de cifrado específica de operador y de transacción (K7) a partir de la clave de cifrado inicial específica de operador y de terminal (K6) usando un número específico de transacción (27) asociado con esta transacción (26), cuando se realiza una transacción (26) con el terminal de pago (1);

realizar la transacción (26) con el terminal de pago (1).

2. Método según la reivindicación 1, en el que se facilita la clave de transporte específica de operador y de terminal (K4) al terminal de pago (1) mediante

transmitir (S6) una clave de transporte maestro específica de operador (K3) desde al menos un proveedor de pago (2) a la entidad de control (3) de manera que se garantice la confidencialidad y derivar (S5, S7), tanto en el proveedor de pago(2) como en la entidad de control (3), la clave de transporte específica de operador y de terminal (K4) a partir de la clave de transporte maestro específica de operador (K3) usando el número de identificación de terminal (44),

cifrar simétricamente (S8), por parte de la entidad de control (3), la clave de transporte específica de operador y de terminal (K4) con la clave de acceso específica de terminal (K2), y

transmitir (S9) la clave de transporte específica de operador y de terminal cifrada (K4) al terminal de pago (1),

controlar por parte de la entidad de control (3) la utilización del terminal de pago (1) de manera selectiva según el operador mediante dicha transmisión (S9) de la clave de transporte específica de operador y de terminal (K4).

3. Método según la reivindicación 1, en el que el clave de transporte específica de operador y de terminal (K4) se facilita al terminal de pago (1) mediante

derivar (S5) en el proveedor de pago (2) la clave de transporte específica de operador y de terminal (K4) a partir de la clave de transporte maestro específica de operador (K3) usando el número de identificación específico del terminal (44),

transmitir la clave de transporte específica de operador y de terminal (K4) desde al menos un proveedor de pago (2) a la entidad de control (3) de manera que se garantice la confidencialidad,

cifrar simétricamente (S8), por parte de la entidad de control (3), la clave de transporte específica de operador y de terminal (K4) con la clave de acceso específica de terminal (K2), y

transmitir (S9) la clave de transporte específica de operador y de terminal cifrada (K4) al terminal de pago (1),

controlar por parte de la entidad de control (3) la utilización del terminal de pago (1) de manera selectiva según el operador mediante dicha transmisión (S9) de la clave de transporte específica de operador y de terminal (K4).

4. Método según cualquiera de las reivindicaciones 1 a 3, en el que

la clave de transporte específica de operador y de terminal cifrada (K4) se descifra con la clave de acceso específica de terminal (K2) en el terminal de pago (1) tras su recepción, y la clave de transporte específica de operador y de terminal descifrada (K4) se almacena en un almacenamiento seguro (TRSM) del terminal de pago (1); o

la clave de transporte específica de operador y de terminal cifrada recibida (K4) se almacena en primer lugar en el terminal de pago (1) de forma cifrada y sólo puede descifrarse más adelante con la clave de acceso específica de terminal (K2) en el terminal de pago (1) cuando se solicita la clave de transporte específica de operador y de terminal descifrada (K4) para descifrar la clave de cifrado inicial específica de operador y de terminal cifrada (K6) para realizar la transacción (26) con el terminal de pago (1).

5. Método según una cualquiera de las reivindicaciones 1 a 4, en el que

la clave de cifrado inicial específica de operador y de terminal cifrada (K6) se descifra con la clave de transporte específica de operador y de terminal (K4) en el terminal de pago (1) tras su recepción, y el la clave de cifrado inicial específica de operador y de terminal descifrada (K6) se almacena en un almacenamiento seguro (TRSM) del terminal de pago (1); o

la clave de cifrado inicial específica de operador y de terminal cifrada (K6) se almacena en el terminal de pago (1) de forma cifrada tras su recepción, y solo puede descifrarse más adelante con la clave de transporte específica de operador y de terminal (K4) en el terminal de pago (1) cuando se solicita la clave de cifrado inicial específica de operador y de terminal descifrada (K6) para obtener la clave de cifrado específica de operador y de la transacción (K7) usando la clave de cifrado inicial específica de operador y de terminal descifrada (K6) para realizar la transacción (26) con el terminal de pago (1).

6. Método según cualquiera de las reivindicaciones 1 a 5, en el que al menos un proveedor de pago (2) es un único proveedor de pasarela de pago, o al menos un proveedor de pago (2) es uno de entre una multiplicidad de proveedores de pago (2).

7. Método según cualquiera de las reivindicaciones 1 a 6, en el que al menos una clave de acceso específica de terminal (K2), una clave de transporte maestro específica de operador (K3), la clave de transporte específica de operador y de terminal (K4), una clave de derivación de base específica de operador (K5), la clave de cifrado inicial específica de operador y de terminal (K6), y una clave de cifrado específica de operador y de la transacción (K7) es una clave de cifrado simétrica.

8. Método según la reivindicación 7, en el que al menos una clave de cifrado simétrica tiene tres claves según el algoritmo que realiza triple cifrado Triple Data Encription Algorithm (TDEA).

9. Método según cualquiera de las reivindicaciones 1 a 8, en el que

el terminal de pago (1) se dispone para ofrecer al menos dos modos de uso, un modo de uso directo en el que se realiza un intercambio de los datos de la transacción entre el terminal de pago (1) y uno de los operadores (4), y un modo de uso autorizado en el que se realiza un intercambio de los datos de la transacción entre el terminal de pago (1) y al menos un proveedor de pago (2), estando el terminal de pago preconfigurada con los distintos modos de uso para los operadores de la pluralidad de operadores (4), y

a uno de los operadores (4) de la pluralidad de operadores (4) que comienza a utilizar este terminal de pago (1) el modo de uso que se le asigna a este operador (4) es seleccionado automáticamente por el terminal de pago (1), y el terminal de pago (1) realiza la transacción (26) usando el modo de uso seleccionado.

10. Método según cualquiera de las reivindicaciones 1 a 9, en el que la clave de acceso específica de terminal (K2) utilizada por la entidad de control (3) para el cifrado simétrico (S8) se deriva (S1) de una clave de acceso maestra específica de la entidad de control (K1) usando el número de identificación de terminal (44), o un número adicional de identificación de terminal de pago (1).

11. Método según cualquiera de las reivindicaciones 1 a 10, en el que la clave de acceso específica de terminal (K2) se almacena en el terminal de pago (1) tras su transmisión (S4) al terminal de pago (1) por un proveedor del terminal (5) de manera que se garantice la confidencialidad.

12. Método según la reivindicación 11, en el que la clave de acceso específica de terminal (K2) se deriva (S3), a partir del proveedor del terminal (5), de una clave de acceso maestra específica de la entidad de control (K1) usando el número de identificación de terminal (44), o un número adicional de identificación de terminal de pago (1).

13. Método según la reivindicación 12, en el que la clave de acceso maestra específica de la entidad de control (K1) se transmite (S2) al proveedor del terminal (5) por la entidad de control (3) garantizando la confidencialidad.

14. Sistema que comprende un sistema informatizado con entidad de control, un sistema informatizado con proveedor de pago, y al menos un terminal de pago (1), en el que el sistema se configura para que al menos un terminal de pago (1) se utilice como terminal de pago (1) compartido por una pluralidad de operadores (4) con segregación criptográfica entre los diferentes operadores (4) del terminal de pago (1), y programado para establecer comunicación con un operador (4) o al menos con un proveedor de pago (2) para realizar transacciones de pago (26), y asociado con la entidad de control (3) que controla la utilización del terminal de pago (1) de manera selectiva según el operador, sin contacto físico con el terminal de pago (1), introduciendo la clave de transporte específica de operador y de terminal (K4) en el terminal de pago (1), es decir almacenando el clave de transporte específica de operador y de terminal (K4) en el terminal de pago (1) de forma cifrada o no cifrada, estando el terminal de pago (1) dispuesto para almacenar un número de identificación de terminal (44), el terminal de pago (1) que comprende al menos un almacenamiento seguro (TRSM) (45) dispuesto para almacenar una clave de acceso específica de terminal (K2) para permitir la utilización del terminal de pago (1) controlado por el sistema de entidad de control de manera selectiva según el operador, en el que el sistema está programado para

recibir, en el terminal de pago (1), una clave de transporte específica de operador y de terminal (K4), cifrada por la clave de acceso específica de terminal (K2); y

descifrar, en el terminal de pago (1), la clave de transporte específica de operador y de terminal cifrada (K4) con la clave de acceso específica de terminal (K2) almacenada; y

recibir, en el terminal de pago (1) del sistema con proveedor de pago, una clave de cifrado inicial específica de operador y de terminal (K6) derivada (S10) de una clave de derivación de base específica de operador (K5) basada en el número de identificación de terminal (44), o un número adicional de identificación de terminal de pago (1), cifrado simétricamente por la clave de transporte específica de operador y de terminal (K4); y

descifrar, en el terminal de pago (1), la clave de cifrado inicial específica de operador y de terminal cifrada (K6) con la clave de transporte específica de operador y de terminal descifrada (K4); y

derivar (S13, S14), en el sistema con proveedor de pago y en el terminal de pago (1), una clave de cifrado específica de operador y de la transacción (K7) de la clave de cifrado inicial específica de operador y de terminal (K6) usando un número específico de transacción (27) asociado con esa transacción (26), al realizar la transacción (26) con el terminal de pago (1); y

realizar la transacción (26) con el terminal de pago (1).

15. Sistema según la reivindicación 14, en el que al menos un almacenamiento seguro (TRSM) se programa para almacenar al menos:

al menos una clave de transporte específica de operador y de terminal (K4) para descifrar una clave específica de operador cifrada simétricamente, y

al menos una clave de cifrado inicial específica de operador y de terminal (K6) para derivar (S14) una clave de cifrado específica de operador y de transacción (K7).

16. Sistema según la reivindicación 14 o 15 dispuesto para configurar al menos una terminal de pago (1) según cualquiera de las reivindicaciones 2 a 13.

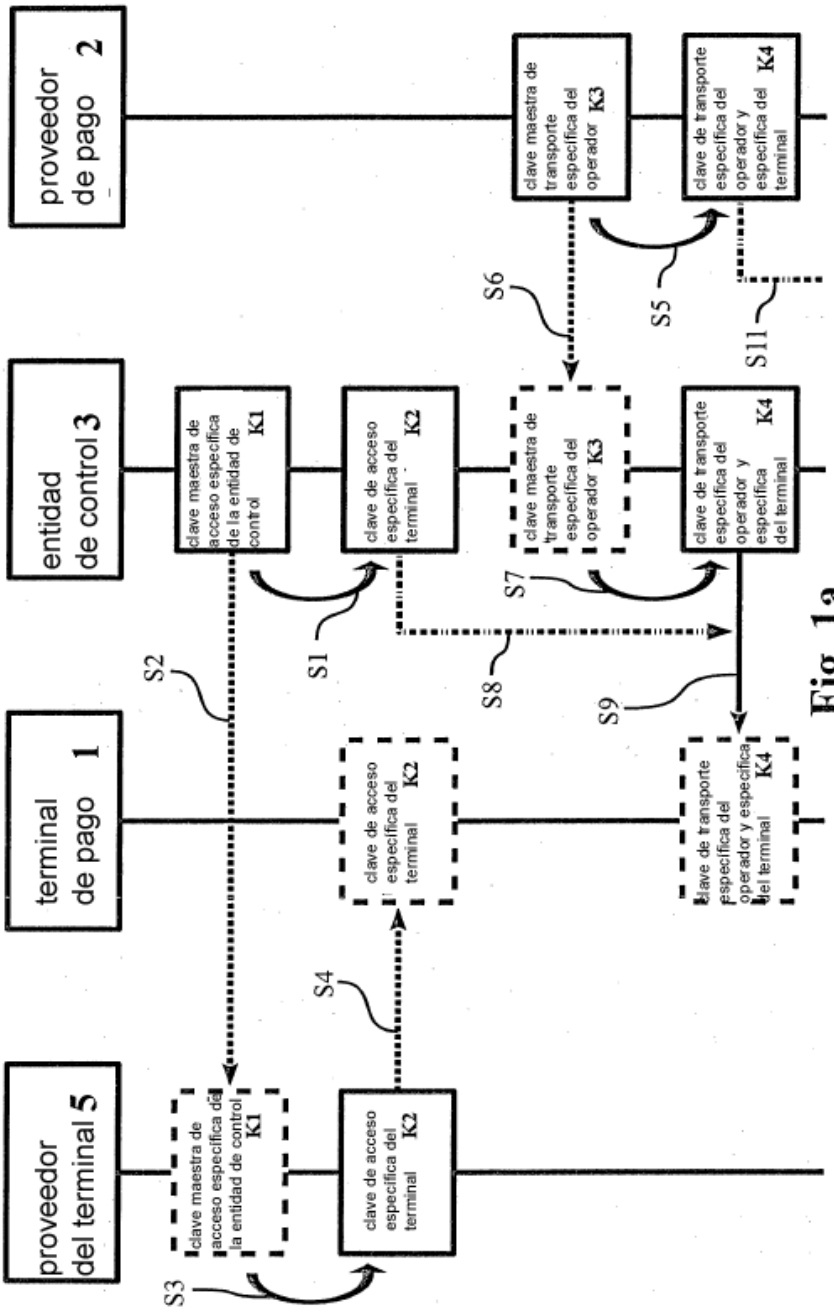
proveedor de pago 2
entidad de control 3
terminal de pago 1
proveedor del terminal 5
clave maestra de acceso especifica de la entidad de control K1
clave de acceso especifica del terminal K2
clave maestra de transporte especifica del operador K3
clave de transporte especifica del operador y especifica del terminal K4
S1
S2
S3
S4
S5
S6
S7
S8
S9
S11

Fig. 1a

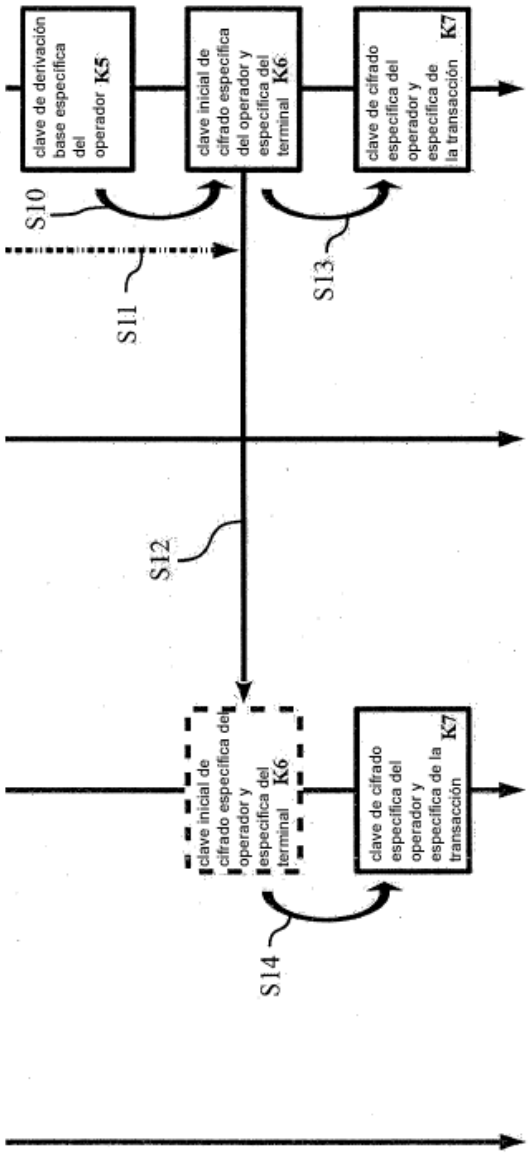
clave de derivación base específica del operador K5
clave inicial de cifrado específica del operador y específica del terminal K6
clave de cifrado específica del operador y específica de la transacción K7
S10
S11
S12
S13
S14
clave inicial de cifrado específica del operador y específica del terminal K6
clave de cifrado específica del operador y específica de la transacción K7

Fig. 1b

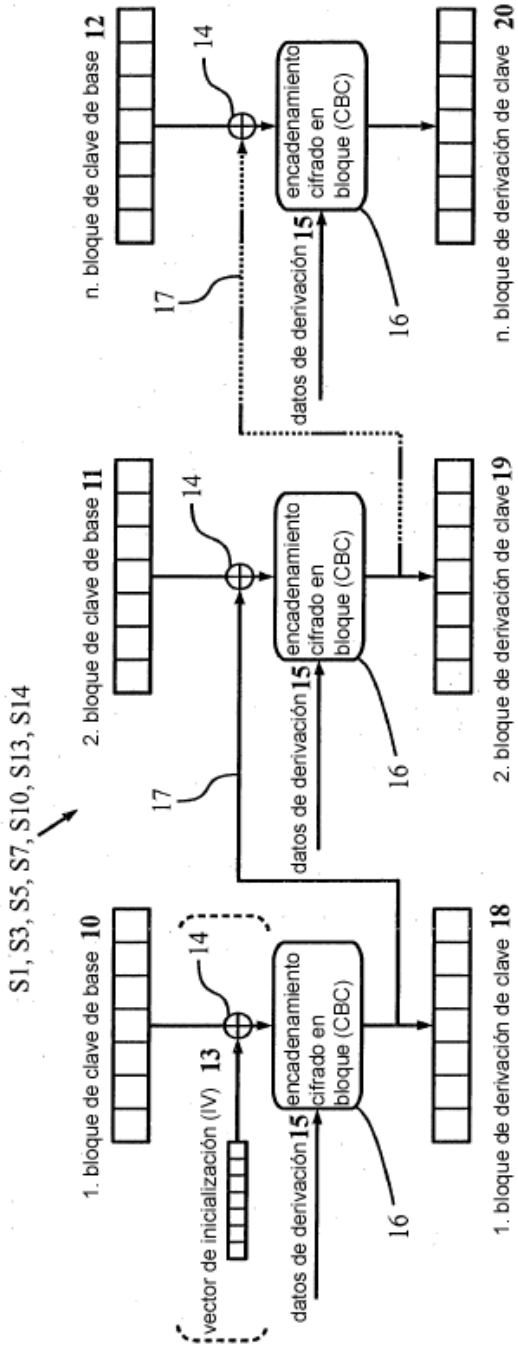
S1, S3, S5, S7, S10, S13, S14
1. bloque de clave de base 10
2. bloque de clave de base 11
n. bloque de clave de base 12
vector de inicialización (IV) 13
14
encadenamiento cifrado en bloque (CBC)
15
datos de derivación
16
17
1. bloque de derivación de clave 18
2. bloque de derivación de clave 19
n. bloque de derivación de clave 20

Fig. 2

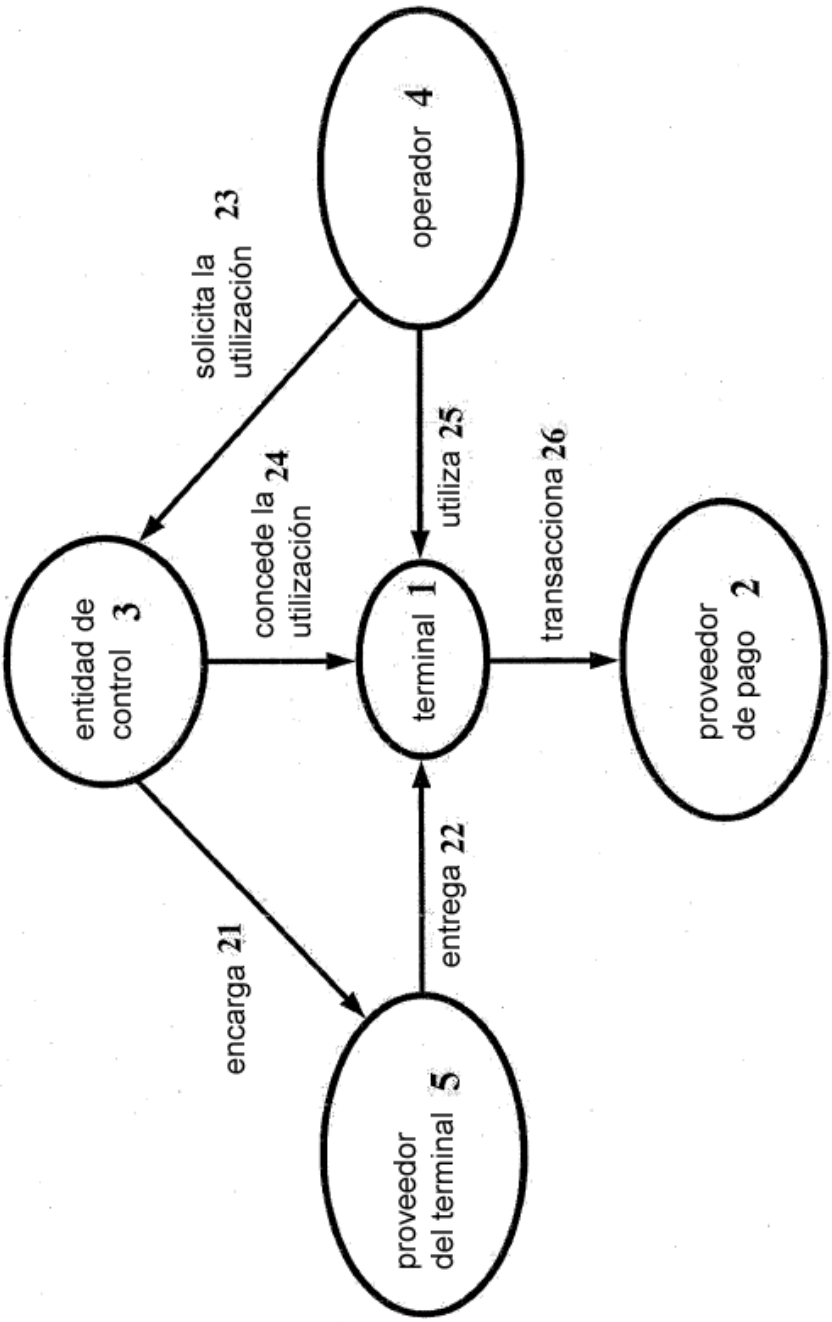
operador 4
solicita la utilización 23
entidad de control 3
concede la utilización 24
utiliza 25
terminal 1
transacciona 26
proveedor de pago 2
encarga 21
entrega 22
proveedor del terminal 5

Fig. 3

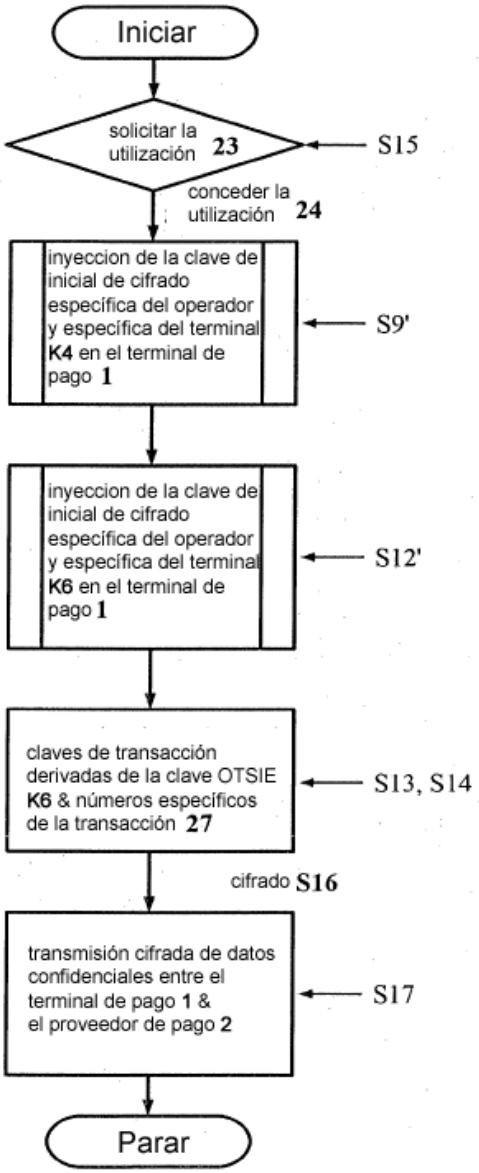
Iniciar
solicitar la utilización 23
S15
conceder la utilización 24
inyeccion de la clave de inicial de cifrado específica del operador y específica del terminal K4 en el terminal de pago 1
S9'
inyeccion de la clave de inicial de cifrado específica del operador y específica del terminal K6 en el terminal de pago 1
S12'
claves de transacción derivadas de la clave OTSIE K6 & números específicos de la transacción 27
S13, S14
cifrado S16
transmisión cifrada de datos confidenciales entre el terminal de pago 1 & el proveedor de pago 2
S17
Parar

Fig. 4

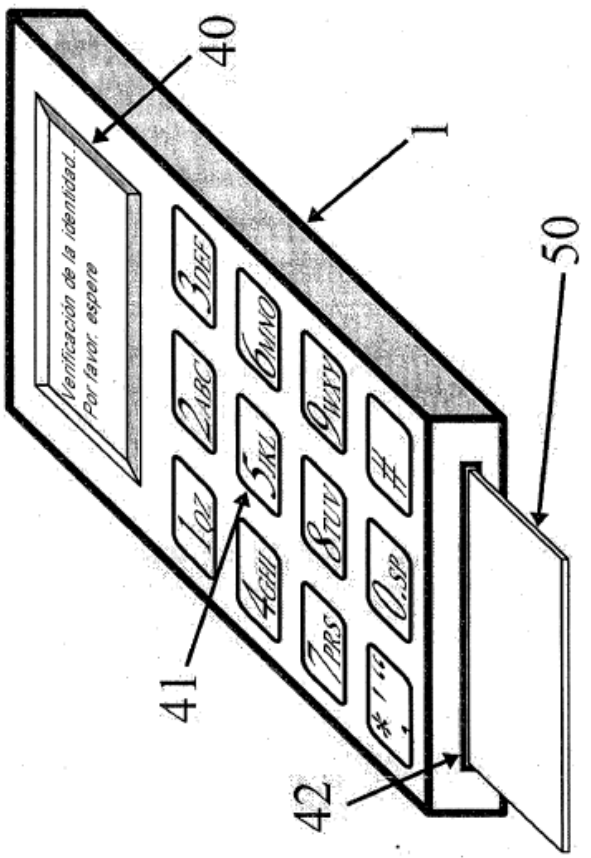

Fig. 5

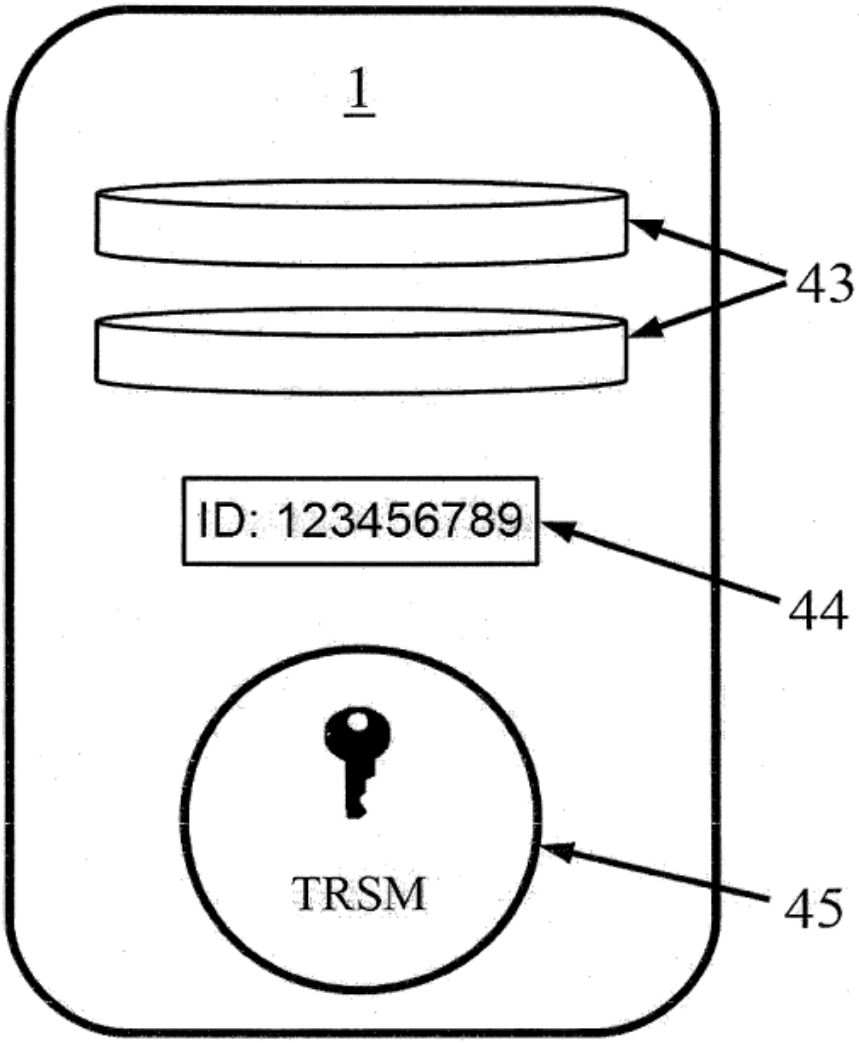

Fig. 6

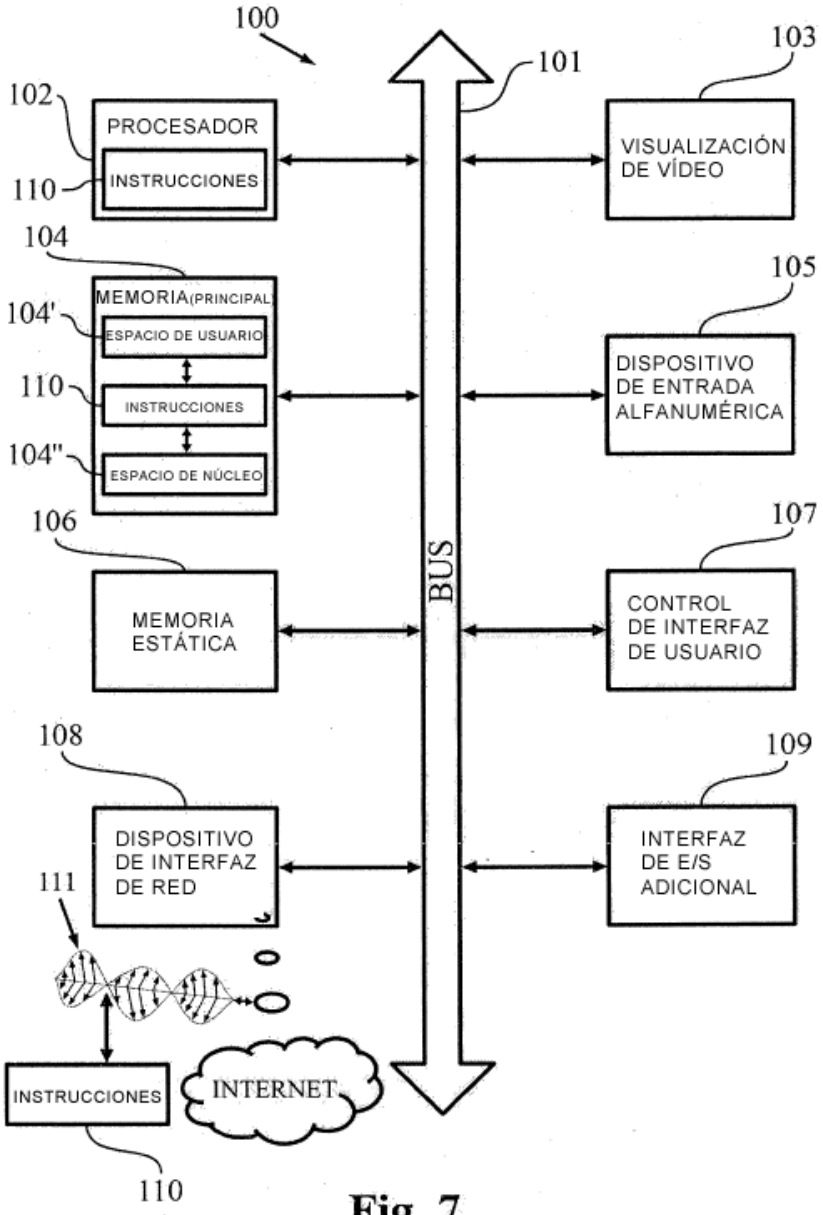
100
101
102
PROCESADOR
110
INSTRUCCIONES
103
VISUALIZACIÓN DE VÍDEO
104
MEMORIA (PRINCIPAL)
104'
ESPACIO DE USUARIO
110
INSTRUCCIONES
104"
ESPACIO DE NÚCLEO
105
DISPOSITIVO DE ENTRADA ALFANUMÉRICA
106
MEMORIA ESTÁTICA
BUS
107
CONTROL DE INTERFAZ DE USUARIO
108
DISPOSITIVO DE INTERFAZ DE RED
109
INTERFAZ DE E/S ADICIONAL
111
INSTRUCCIONES
INTERNET
110

Fig. 7