(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 758 658**

(51) Int. CI.:

***G06Q 20/32*** (2012.01)
***G06Q 20/16*** (2012.01)
***G06Q 20/38*** (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **28.09.2012 PCT/FI2012/000038**

(87) Fecha y número de publicación internacional: **04.04.2013 WO13045743**

(96) Fecha de presentación y número de la solicitud europea: **28.09.2012 E 12834914 (9)**

(97) Fecha y número de publicación de la concesión europea: **28.08.2019 EP 2761553**

(54) Título: **Sistema de pago**

(30) Prioridad:

**28.09.2011 FI 20115945**
**15.12.2011 FI 20116274**
**27.12.2011 US 201161631040 P**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
**06.05.2020**

(73) Titular/es:

**UNITO OY (100.0%)**
**Munkkiniemen puistotie 25**
**00330 Helsinki , FI**

(72) Inventor/es:

**SALMINEN, SIMO y**
**KAJAVA, TUOMO**

(74) Agente/Representante:

**ELZABURU, S.L.P**

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

## DESCRIPCIÓN

Sistema de pago

**Campo de la invención**

La invención se refiere a procedimientos, dispositivos, sistemas y programas de ordenador para realizar pagos; particularmente a procedimientos, dispositivos, sistemas y programas de ordenador en los que el procesamiento de los datos de pago y la transacción del pago se producen por medio de una tarjeta de confianza.

**Antecedentes**

En los sistemas de pago conocidos, hay varios operadores, y su interacción y la cooperación requieren sistemas complejos y una relación de confianza entre los actores, en los que los costes aumentan como la multiplicación de los costes para cada actor. Los sistemas de la técnica anterior son difíciles o imposibles de implementar sin teleoperadores, lo que aumenta adicionalmente la complejidad de los sistemas de pago.

Los sistemas basados en el uso de una tarjeta SIM son conocidos a partir de la técnica anterior, incluyendo, por ejemplo, los procedimientos y sistemas conocidos a partir de los documentos FI 117586 B y FI 104937 B. Aquí, la información específica del abonado se almacena en una tarjeta SIM. Estos procedimientos se basan también en el uso de los teleoperadores. El documento EP2365469 describe un procedimiento para realizar una transacción de pago en el que la autorización se realiza en el banco emisor de tarjetas y en el banco comprador. En algunas soluciones de la técnica anterior, existe el problema de la gestión de una tarjeta de pago o una tarjeta de confianza con una funcionalidad de pago durante todo el ciclo de vida de la tarjeta. En general, la tarjeta se activa cuando se entrega a un cliente, y se desactiva tras una solicitud por parte del cliente o tras sobrepasar el límite de crédito. El período de tiempo entre la activación y la desactivación es totalmente incontrolable por el proveedor de servicios, lo que aumenta el riesgo de mal uso de la tarjeta.

En algunas soluciones de la técnica anterior, la falta de seguridad en el procesamiento de los datos de la tarjeta de confianza y otros datos sensibles supone un problema. En las soluciones de la técnica anterior, existe un riesgo de que un usuario no autorizado pueda acceder a datos sensibles, por ejemplo, en el terminal del usuario.

Por consiguiente, se necesitan formas mejores o alternativas para efectuar pagos.

**Breve descripción de la invención**

En el procedimiento según la invención para realizar un pago, los datos pago son recibos por un terminal de usuario desde un terminal de punto de venta, el terminal recibe un secreto para una aplicación de pago desde el sistema servidor del operador, se activa una tarjeta de confianza en dicho terminal de usuario mediante la utilización de dicho secreto de la aplicación de pago, y los datos de la tarjeta de confianza se transmiten desde dicho terminal de usuario a dicho terminal de punto de venta para la realización de la transacción de pago. En el procedimiento según la invención para realizar un pago en un sistema servidor, se crea una tarjeta de confianza en el sistema servidor, los datos de dicha tarjeta de confianza se transmiten al terminal a ser usado para realizar la transacción de pago, se forma un secreto de una aplicación de pago en el sistema servidor, y se proporciona acceso a dicho secreto de la aplicación de pago al terminal para activar dicha tarjeta de confianza para realizar la transacción de pago. Los dispositivos, el sistema servidor y los programas de ordenador a ser ejecutados en los mismos funcionan de manera que puedan implementarse las diferentes partes del procedimiento, y estos dispositivos y sistemas pueden comprender, por ejemplo, medios de comunicación para comunicarse con un punto de punto de venta u otros dispositivos.

El procedimiento según la invención tiene la ventaja de que, cuando se proporciona acceso al secreto para la aplicación de pago en el sistema servidor, el sistema es seguro. La tarjeta de confianza en el terminal puede ser activada por el secreto para la aplicación de pago obtenida desde el sistema servidor, posiblemente en combinación con el secreto del usuario, en el que la tarjeta de confianza no puede ser usada sin proporcionar el secreto de la aplicación de pago al terminal para activar la tarjeta. Esta provisión se realiza de manera segura utilizando criptografía, si el usuario se ha registrado con éxito en el sistema para proporcionar el secreto de la aplicación de pago. De esta manera, puede mejorarse la seguridad y, por ejemplo, si roban el terminal del usuario, no pueden realizarse pagos sin el sistema servidor. Además, es posible autenticar al usuario solicitando el secreto del usuario (por ejemplo, un código PIN), y la tarjeta de confianza puede ser activada con el secreto del usuario en combinación con el secreto de la aplicación de pago.

En la presente memoria, se presenta un sistema de pago para proporcionar datos electrónicos y de pago verificados al destinatario del pago, comprendiendo el sistema de pago el terminal del usuario y el sistema servidor del operador, y en cuyo sistema de pago el uso de la aplicación de pago está configurado para tener lugar en dos fases que comprenden el registro del usuario en el sistema servidor y el control de la validez de la aplicación de pago por medio del derecho de acceso mediante el uso de un elemento de encriptación y un secreto de la aplicación de pago obtenido desde el sistema servidor al menos a intervalos regulares. El terminal del usuario comprende una aplicación de pago para realizar

solicitudes de pago, una zona de confianza para el almacenamiento y el uso de un elemento de encriptación programado, y medios de comunicación RFID para suministrar los datos de pago al terminal del destinatario del pago. Además, el terminal del usuario comprende medios para comunicarse con el sistema servidor usando un protocolo de comunicaciones protegido, y medios relacionados con el elemento de encriptación para activar y desactivar el derecho a usar la aplicación de pago. A su vez, el sistema servidor del usuario comprende una aplicación de gestión para identificar y la gestionar un terminal, una base de datos para datos específicos de usuario y claves, incluyendo un secreto de cada aplicación de pago, y medios para comunicarse con el terminal mediante el uso de un protocolo de comunicaciones protegido.

Mediante el sistema de pago según la invención, el estado del elemento de encriptación, es decir, la tarjeta de confianza, puede ser gestionado posiblemente durante el ciclo de vida del elemento de encriptación, lo que aumenta la fiabilidad del sistema de pago desde el punto de vista del cliente. En adelante, el elemento de cifrado se denominará tarjeta de confianza.

El terminal puede comprender un contador de límite de crédito controlado por el elemento de encriptación. De esta manera, es posible garantizar que el cliente no pueda exceder un límite de crédito predeterminado dentro de un período de tiempo determinado. Esto aumenta la seguridad del sistema de pago, por ejemplo, en situaciones en las que el terminal del usuario ha sido robado.

Los medios de comunicación de RFID del terminal puede comprender un módulo NFC. Por medio del módulo NFC, los datos de pago se transfieren rápidamente desde el terminal del usuario.

En una realización, los terminales comprenden una aplicación de tarjeta Java programada en una zona de confianza y una aplicación autorizada por la misma en una zona no segura para establecer una interfaz de usuario y una conexión de servidor. La aplicación de tarjeta Java garantiza que cualquier dato que sea sensible con relación a la seguridad de los datos se mantenga secreto.

En otra realización, el terminal comprende una zona de confianza implementado mediante tecnología ARM a nivel de circuito, que comprende una aplicación de sistema de suministro Obc y un intérprete Obc y, en el lado no seguro, una aplicación de gestión de credenciales Obc, una aplicación cliente de provisión Obc y una base de datos Obc, que estén autorizadas. En esta realización, la cantidad de información en la zona de confianza es pequeña, en la que la capacidad de memoria requerida de la zona de confianza puede ser relativamente baja. El elemento de encriptación puede implementarse en la zona de confianza por medio del lenguaje de secuencia de comandos LUA usando un intérprete Obc.

De manera ventajosa, el terminal comprende una aplicación "middleware" entre el módulo NFC y la aplicación de gestión de credenciales OBC. Por medio de la aplicación de intérprete, los comandos recibidos en el módulo NFC pueden transmitirse a la aplicación de pago que gestiona el terminal.

El control de la validez de una solicitud de pago a intervalos regulares puede estar configurado para realizarse a intervalos de 2 a 48 h, de manera ventajosa en conexión con cada transacción de pago. De esta manera, la tarjeta de confianza se encuentra bajo gestión continua y puede garantizarse que la persona que usa el terminal es una persona autorizada.

El sistema servidor está configurado de manera ventajosa para realizar una verificación de transacción automática para cada solicitud de pago. De esta manera, no se necesita una tarea separada en el sistema servidor para realizar la verificación.

De manea ventajosa, el secreto para la aplicación de pago, obtenido desde el sistema del servidor, es aleatorio. Esto mejora adicionalmente la seguridad de los datos, ya que puede usarse un único secreto para una única transacción de pago.

De manera ventajosa, el elemento de encriptación está configurado para ser descargado dinámicamente y de manera autorizada desde el sistema servidor a la zona de confianza del terminal del usuario durante el registro. De esta manera, puede garantizarse que el elemento de encriptación es correcto y, al mismo tiempo, que se proporcionan todas las claves necesarias del elemento de encriptación.

La validez de la aplicación de pago puede estar configurada para ser controlada por medio de un código PIN de la aplicación de pago, cuyo código PIN comprende, en combinación, el secreto para la aplicación de pago y el secreto del usuario creado en la etapa de registro. El uso de dos secretos aumenta la seguridad de datos en ambos sentidos, ya que de esta manera es posible para garantizar que tanto el usuario como el sistema servidor son auténticos. A su vez, esto reduce la necesidad de confianza entre el usuario y el sistema servidor.

Los medios de RFID del terminal del usuario para la comunicación con el sistema servidor puede estar separados de los medios para controlar la validez de la solicitud de pago. De esta manera, el terminal del destinatario del pago no tiene

oportunidad, en ningún caso, de ver los secretos específicos del usuario.

En una realización, la zona de confianza perteneciente al terminal e implementada a nivel de circuito es un circuito SoC prefabricado conectado al terminal.

De manera ventajosa, el sistema de pago comprende además el terminal del destinatario del pago, equipado con medios de RFID, particularmente un módulo NFC, para la transferencia de datos de pago. De esta manera, los datos de pago pueden transferirse rápidamente y de manera inalámbrica desde el terminal del destinatario del pago al terminal del usuario y además al sistema servidor, para la autenticación.

El funcionamiento global del sistema consta de un número mínimo de operadores, lo que reduce el riesgo causado por su interacción mutua y control de confianza, lo que hace que el sistema sea simple de implementar. El pequeño número de operadores aumenta también la seguridad y la dinamicidad del sistema, así como el enfoque de contexto, tal como, por ejemplo, publicidad, relacionado con las transacciones y mostrado al usuario.

El sistema presentado en la presente memoria está diseñado para funcionar en un entorno en el que el terminal controlado por el usuario comprende un módulo de RFID, una zona de confianza, y que implementa además una funcionalidad ventajosa entre el módulo de RFID y la zona de confianza en vista de este sistema.

En adelante, se describirá el entorno de funcionamiento del sistema de pago. En este contexto, la expresión tarjeta de confianza se usa para hacer referencia a un elemento de identificación y de encriptación programado que contiene una clave secreta y una clave pública creadas en dicho elemento mediante software, un certificado, un certificado CA, los datos de identificación de la tarjeta de confianza (número de cuenta, código CV, etc., como en las tarjetas inteligentes), así como una aplicación para la gestión y/o el procesamiento de los mismos, y un protocolo definido en la aplicación para la comunicación con el servidor del operador. Los componentes completamente nuevos en el sistema de pago incluyen la aplicación y el protocolo de comunicaciones en la capa de aplicación, así como las claves y los certificados generados por la misma.

En el entorno de funcionamiento del sistema:

- El operador se refiere al proveedor que es responsable del funcionamiento del sistema servidor y la tarjeta de confianza.

- El terminal del usuario comprende una zona de confianza segura que está protegida mediante procedimientos según, y que cumplen, los requisitos de emisores que proporcionan tarjetas inteligentes o artículos digitales similares que aportan un valor añadido al usuario. Estos procedimientos pueden denominarse también credenciales. Una zona de confianza puede ser una zona virtual implementada por medio de software o una zona implementada a nivel de circuito. A su vez, una zona de confianza implementada a nivel de circuito puede ser una tecnología de un fabricante de componentes, tal como ARM o Inside Security. La zona de confianza puede ser también una tarjeta SIM o una parte de un módulo de chip externo o interno a insertar en el terminal. El módulo de chip puede ser también una parte de un módulo combinado a instalar interna o externamente como parte del terminal. Un módulo combinado se refiere a una combinación de circuitos integrados, por ejemplo, con WLAN, BT/NFC integrados en el mismo circuito.

- En este documento, una tarjeta de confianza se refiere a una tarjeta de confianza virtual almacenada en una zona de confianza del sistema operativo de un terminal, o en una zona de confianza de un dispositivo auxiliar incluido en el terminal, u otra área de memoria segura asignada e identificada para el operador, correspondiendo el uso de la tarjeta al de una tarjeta de débito o de crédito convencional. La tarjeta de confianza contiene datos confidenciales, así como un conjunto de propiedades y primitivas de seguridad, mediante las cuales las partes autorizadas pueden comunicarse con la misma. En pocas palabras, la tarjeta de confianza es una aplicación que controla el acceso a la aplicación de pago y contiene las claves y certificados necesarios para la encriptación de la aplicación de pago, un algoritmo de encriptación y posiblemente también un límite de crédito.

- En este sistema de pago, los datos sensibles incluyen códigos PIN, claves, certificados, así como cualquier otro dato sensible definido por el operador y relacionado directa o indirectamente con el sistema de pago.

- El uso de la tarjeta de confianza requiere la desencriptación de un denominado secreto compartido entre el usuario y el sistema servidor, para que pueda usarse la tarjeta de confianza. El secreto compartido (código PIN) es una combinación del secreto conocido por el usuario y el secreto almacenado en el sistema servidor, definido por el operador y cambiado a intervalos regulares.

- La tarjeta de confianza es autenticada por una identificación única de la tarjeta de confianza o por un valor de identificación derivado de la misma.

- La tarjeta de confianza se comunica de manera fiable y segura a través de Internet u otro medio con un sistema servidor conectado a la misma, un sistema propiedad de un tercero, una tarjeta de confianza, otra tarjeta de confianza o

un lector sin contacto externo que soporta la funcionalidad para realizar un pago.

- Puede implementarse una comunicación fiable mediante un mecanismo de seguridad bidireccional que cumple con el protocolo SSL/TLS mediante el uso de claves de tamaño optimizado con respecto a la capacidad de cálculo disponible, la facilidad de uso y los requisitos de seguridad únicos de las operaciones. De manera alternativa, toda la comunicación de datos fuera de la zona de confianza se encripta con un algoritmo de encriptación en la zona de confianza, mediante el uso de las claves de encriptación de la zona leída.

- La tarjeta de confianza recupera los datos necesarios para la funcionalidad de manera dinámica desde el sistema servidor conectado a la misma.

- La tarjeta de confianza funciona con el sistema servidor del operador.

- El sistema servidor del operador es responsable de la seguridad y la gestión de la tarjeta de confianza.

- El usuario es una persona que interactúa con el terminal y la tarjeta de confianza. El uso de la tarjeta de confianza requiere la autorización del usuario, de la tarjeta de confianza y del servidor por el sistema del operador.

- El usuario tiene un terminal compatible con la tecnología de RFID u otra tecnología de comunicación local, de manera que es posible establecer una conexión a Internet u otro medio.

- El sistema servidor está conectado a Internet u otro medio.

- El sistema servidor contiene una zona de confianza segura, en la que se almacenan los datos sensibles a ser usados para inicializar las tarjetas de confianza.

**Lista de figuras**

A continuación, la invención se describirá en detalle con referencia a las figuras adjuntas que ilustran algunas realizaciones de la invención, en las que

La Figura 1 muestra una descripción general de un sistema de pago según la invención,

La Figura 2 ilustra el registro de una tarjeta de confianza de un sistema de pago según la invención en un diagrama de bloques,

La Figura 3 ilustra una transacción de pago en una realización de un sistema de pago según la invención, en un diagrama de bloques,

La Figura 4 ilustra una transacción de pago en una realización de un sistema de pago según la invención, en un diagrama de bloques,

La Figura 5 ilustra la arquitectura de un sistema de pago según la técnica anterior,

La Figura 6 ilustra una arquitectura de tarjeta Java según una realización,

La Figura 7 ilustra una zona de confianza ("TrustZone") y una arquitectura Obc según otra realización.

**Descripción de las realizaciones de la invención**

En este contexto, una aplicación de pago se refiere a todos los componentes de software de un terminal, tanto en la zona de confianza como en la zona no segura que, en conjunto, utilizan datos y claves de un elemento de encriptación en la zona de confianza, así como medios de RFID y medios de comunicación. Además, los medios de comunicación se refieren a aquellos componentes de software que se ocupan de la comunicación con el sistema servidor a través de una conexión a Internet. En las Figuras 1 a 4, la tarjeta de confianza se denomina generalmente tarjeta de confianza (“Trust Card”).

Según la Figura 1, el sistema de pago según la invención consiste en un terminal 62, 84 gestionado por un usuario, y un sistema 68, 85 servidor de un operador, así como las entidades respectivas presentadas en la presente descripción. El sistema soporta transacciones de pago sin contacto autónomas, en las que el usuario puede realizar una transacción de pago a través de su terminal 62, 84 que soporta tecnología de RFID, y en particular a través de su aplicación de pago. Una copia personalizada de una tarjeta 100 de confianza almacenada en el sistema 68, 85 servidor se instala para cada usuario del sistema, o de manera alternativa, cada usuario tiene su propia tarjeta de confianza paralela en el sistema servidor, cuya tarjeta se instala de manera dinámica en el terminal del usuario. En ambos casos, el propietario de la cuenta conectada a la tarjeta es el operador, de manera que la funcionalidad del sistema sigue siendo el mismo en ambos casos. El sistema 68, 85 de servidor del operador es responsable de todo el ciclo de vida de la tarjeta 100 de confianza a ser transferida al terminal 62, 84, incluyendo su instalación, actualización, personificación, invalidación y

destrucción. De esta manera, puede minimizarse el número de partes que causan riesgos y costes en el sistema total, en la transacción de pago y en la funcionalidad relacionada con la misma.

En el sistema, un terminal externo, es decir, un lector 67, 81 de RFID, está con un comerciante, y el terminal 62, 84 con un cliente. En adelante, el lector de RFID externo se denominará también lector externo. De manera ventajosa, el terminal es un teléfono móvil, pero también puede ser una tableta digital, un dispositivo de muñeca digital, un ordenador portátil o cualquier dispositivo correspondiente que esté equipado con una pantalla y una interfaz de usuario y que puede ser complementado con un RFID. En el sistema según la invención, la comunicación de datos relacionada con la autenticación del cliente se realiza a través del terminal 62, 84 del cliente. Al principio, la autenticación se realiza a través del terminal 62, 84 en el sistema 68, 85 servidor, y el resultado se devuelve de nuevo al terminal 62, 84. A continuación, el lector 67, 81 externo del comerciante verifica ese resultado desde la tarjeta 100 de confianza, por ejemplo, según el protocolo NFC. El resultado no puede ser falsificado debido a la clasificación de seguridad y/o a la zona de confianza. Si el resultado es OK, la transacción es aceptada como tal, si lector 67, 81 externo del comerciante acepta verificaciones sin conexión con relación al pago móvil. De manera alternativa, el lector 67, 81 externo reenvía el resultado de la verificación además a un banco, si esto es lo que desea el comerciante. El sistema puede aplicarse sin esta etapa, particularmente si el operador es el emisor de la tarjeta.

A continuación, se explicará el registro del usuario en el sistema de pago con referencia a la Figura 2. Por defecto, el terminal del usuario comprende los certificados de CA preprogramados por el fabricante del dispositivo, un algoritmo de encriptación, una clave PK1 pública y una clave SK1 secreta para la encriptación y la autenticación en general. El usuario descarga la aplicación del sistema servidor desde un sitio definido por el sistema de pago, la abre en el terminal usado, y es autenticado para la aplicación, por ejemplo, aplicando el servicio TUPAS o el correspondiente servicio de autenticación certificado. Se muestra al usuario una vista para el registro en el servicio del sistema de pago, y los datos introducidos por el usuario se transmiten en una forma verificada al sistema servidor en la etapa 1. Los datos proporcionados por el usuario entran al sistema de servicio donde la identificación del usuario y la calificación de crédito se verifican en la etapa 2 del registro. Tras el registro, el usuario crea para sí mismo un secreto de usuario, es decir, una contraseña SS1, almacenándose en el sistema servidor sólo un código hash del mismo. En la etapa 3, se comprueba si el registro ha tenido éxito. Si se encuentra que los datos del usuario son válidos, los datos se almacenan en el sistema servidor y se concluye el proceso de registro. En una situación de fallo, el proceso de registro se cancela, se borran los datos proporcionados por el usuario, y se muestra al usuario una vista del registro fallido en la etapa 4. En este caso, la descarga de la tarjeta es dinámica, y el código PIN del usuario es seleccionable por el usuario. Esto hace que el código sea más fácil de recordar y reduce la cantidad de trabajo por parte del emisor de la tarjeta.

Un proceso de registro exitoso se continúa en el sistema servidor para crear datos para la identificación del usuario, y se transmite al terminal del usuario un resultado firmado del registro exitoso. Además, a través de una interfaz de solicitud proporcionada desde la zona de confianza, la aplicación del sistema servidor solicita la clave PK1 pública asignada al terminal y verificada en la etapa de su fabricación, y transmite la clave al sistema servidor en la etapa 5. El sistema servidor crea una clave SYK1 de encriptación simétrica que encripta con la clave PKS1 pública obtenida desde el terminal y transmite de vuelta al terminal del usuario en la etapa 6. En el terminal, la clave SYK1 simétrica encriptada es transferida a la zona de confianza a través de la interfaz de solicitud proporcionada, y se desencripta en la misma con la clave SK1 privada del terminal, después de lo cual la clave de encriptación simétrica se almacena en la etapa 7.

A continuación, el sistema servidor transmite la aplicación de pago, los datos sensibles relacionados con la misma, es decir, el secreto SS2 específico de la tarjeta de confianza, así como la clave PK2 pública del sistema servidor, encriptado con la clave SYK1 simétrica, al terminal en la etapa 8. En la etapa 9, el paquete transmitido por el sistema servidor se decodifica usando la clave SYK1 simétrica creada por el sistema servidor. La tarjeta de confianza personalizada para el usuario, así como el secreto SS2 del sistema servidor se almacenan en el terminal a través de la interfaz de solicitud proporcionada a la zona de confianza. Al mismo tiempo, se establece el código PIN del terminal, formado por la contraseña SS1 seleccionada por el usuario, y el secreto SS2 del sistema servidor. En este contexto, la clave pública se refiere, por ejemplo, a una clave pública relacionada con un algoritmo de encriptación RSA asimétrico.

En el sistema de pago según la invención, dependiendo del tamaño de la zona de confianza, los datos sensibles pueden almacenarse directamente en la zona de confianza o, de manera alternativa, los datos sensibles sólo pueden ser encriptados en la zona de confianza. De esta manera, después de la encriptación, los datos sensibles encriptados puede almacenarse en cualquier lugar en el espacio de memoria no segura fuera de la zona de confianza del terminal. En cualquier caso, el algoritmo de encriptación y sus claves se almacenan en la zona de confianza. Cuando los datos sensibles se encriptan fuera de la zona de confianza, la aplicación de pago emplea las claves almacenadas en la zona de confianza para la encriptación y la desencriptación de todas las transmisiones de datos.

Tras la formación del código PIN, se proporciona a la tarjeta de confianza del usuario una clave SK3 privada, y una solicitud de certificado con la identificación, encriptada con la clave SYK1 simétrica, se transmite al sistema servidor mediante el uso de un medio seguro en la etapa 10. En el sistema servidor, la encriptación se desencripta usando la clave SK2 privada del sistema servidor, y el certificado se firma con el certificado CA del sistema servidor en la etapa 11.

Después de esto, el certificado CA firmado se encripta de nuevo usando la clave SYK1 simétrica. Por último, el certificado C1 de tarjeta de confianza firmado se transmite a través de un medio encriptado y seguro al terminal del usuario, a la tarjeta de confianza específica del usuario, en la etapa 12. En la etapa 13, el certificado C1 de tarjeta confianza firmado se desencripta con la clave SYK1 y se almacena en la zona de confianza. El certificado C1 contiene también una clave PK3 pública. El certificado C1 de tarjeta confianza firmado y la clave PK3 pública se almacenan también en el sistema servidor para usos posteriores. Por último, se muestra al usuario una vista del resultado de registro exitoso en la etapa 14, y se da la oportunidad al usuario de iniciar sesión en el sistema servidor del operador.

A continuación, con referencia a la Figura 3, se describirá una transacción de pago en el sistema de pago según la invención. En la situación inicial, el usuario conoce una contraseña SS1, el sistema servidor tiene un secreto SS2 y una clave PK3 pública, y un certificado C1 y una clave PK3 pública se almacenan en el terminal. En la etapa 15, el comerciante introduce los datos de una transacción de pago en un lector de tarjetas de confianza sin contacto externo que soporta tecnología de RFID. En la etapa 16, el usuario abre la aplicación de pago en su terminal y activa la aplicación de pago de la tarjeta de confianza aplicando un botón especial destinado a ello. Como resultado, se muestra al usuario una ventana de inicio de sesión, en la que se le solicita que introduzca la contraseña SS1 (verificación) en la etapa 17. Los códigos hash de las entradas se transmiten de una manera encriptada y a través de un medio seguro al sistema servidor que procesa los datos recibidos de manera eficiente en la etapa 18. Al mismo tiempo, la contraseña SS1 (verificación) introducida se transmite también a la zona de confianza del terminal y se verifica allí. Si el inicio de sesión falla, se inicia un mecanismo de verificación en el terminal en la etapa 19, que comprende instrucciones de procesamiento para una situación de error, que incluye, por ejemplo, el número permitido de entradas incorrectas antes de que se restablezca la tarjeta de confianza. En este caso, el usuario puede obtener una nueva tarjeta solo registrándose de nuevo en el sistema. Cuando el inicio de sesión es exitoso en la etapa 20, el sistema servidor selecciona una clave SYK2 simétrica aleatoria desde su zona de confianza y la transmite al terminal del usuario, encriptada con la clave PK3 pública de la tarjeta de confianza.

En la etapa 21, el terminal recibe el paquete desde el sistema servidor y lo desencripta con la clave SK3 secreta. Después de esto, la clave SYK2 se almacena en la zona de confianza, que activa la tarjeta de confianza mediante su máquina de estado intrínseca. Primero después de esto, la tarjeta de confianza puede comunicarse con otras partes distintas del sistema servidor. Cuando un lector externo es una parte comunicante, la tarjeta de confianza siempre funciona en modo pasivo, pero sin la activación indicada anteriormente, la tarjeta de confianza no reacciona a una solicitud de conexión por el lector externo o cualquier otro terminal compatible con RFID, activo o pasivo, directamente o mediante un módulo RFID. Por otra parte, en otra realización, la tarjeta de confianza puede estar activa, tal como en la Figura 6, pero la operación aún requiere una interacción periódica con el servidor del operador.

Después de la activación, en la etapa 22 se muestra al usuario una vista para acercar el terminal a las proximidades del lector externo, y en la etapa 23 el usuario acerca el terminal a las proximidades de un lector externo, leyendo el lector externo los datos necesarios desde la tarjeta de confianza automáticamente desde la zona de confianza del terminal en la etapa 24. El lector externo devuelve los datos de la transacción de pago al lector, cuyos datos son transferidos automáticamente por el módulo de RFID a la zona de confianza del terminal. En la etapa 26, los datos de la transacción de pago, encriptados con la clave SYK2, se transmiten desde el terminal al sistema servidor para su procesamiento y almacenamiento. Se muestra una vista de procesamiento de esto al usuario en la etapa 25. En la etapa 27, el sistema servidor desencripta la transmisión de datos de pago con la clave SYK2 y realiza una verificación automática de si el cliente está autorizado para realizar la transacción. Si la verificación falla, el procedimiento se interrumpe y se muestra al usuario una vista de la razón del fallo en la etapa 28. Además, el mecanismo de verificación automática del operador verifica qué salió mal en la verificación y trata la situación de manera apropiada. Por ejemplo, si se determina que el error es muy grave, tal como un uso no autorizado de la tarjeta o que aparece en la lista de tarjetas robadas, la tarjeta de confianza se invalida.

Si la transacción de pago es aceptada por el sistema de verificación del servidor, el secreto SS2 (verificación) del sistema servidor, almacenado en el sistema servidor en una forma encriptada con la clave SYK2 y vinculado a la identificación de la tarjeta de confianza en cuestión y necesaria para su funcionamiento, se transmite al terminal en la etapa 29. En la etapa 30, la aplicación de cliente receptora transmite el mensaje adicionalmente a la tarjeta de confianza, en la que el desencriptado se realiza con la clave SYK2. El secreto SS2 (verificación) del sistema servidor y la contraseña SS1 del usuario (verificación) se combinan para formar un PIN (verificación), y el valor se introduce en la máquina de estado intrínseca de la tarjeta de confianza en el terminal. Además, en la etapa 31, se muestra al usuario una vista para acercar el terminal a un lector de RFID, en el que se verifica el PIN (verificación) comparándolo con el PIN generado en la etapa de registro y compuesto por los secretos SS1 y SS2. La verificación exitosa permite la comunicación por “middleware” con el módulo NFC. Una ventaja en la disposición descrita anteriormente puede ser que no es necesario establecer requisitos tan estrictos para la zona de confianza en el terminal, ya que un secreto que se usa para realizar el pago se obtiene desde el servidor para realizar la transacción de pago (para activar la tarjeta de confianza).

En general, los secretos SS1, SS2 reales se crean en la etapa de registro y, a partir de estos, un PIN, cuyos secretos, encriptados con la clave simétrica, se almacenan, por ejemplo, en la zona de confianza o en otro lugar en la memoria del

terminal. En conexión con la transacción de pago, el usuario proporciona el SS1 (verificación) y el sistema servidor el SS2 (verificación), cuyos secretos se usan para crear un PIN (verificación). De esta manera, puede asegurarse en conexión con la transacción de pago que el usuario es el usuario auténtico del terminal que conoce el SS1 de la etapa de registro, y el servidor es también el servidor auténtico que conoce el SS2 de la etapa de registro. Por consiguiente, el código PIN está descentralizado entre el usuario y el servidor, de manera que se necesita una doble autenticación para asegurar las autenticaciones de ambas partes. El usuario no conoce en ningún momento el código PIN real del terminal. La máquina de estado intrínseca de la tarjeta de confianza se activa comparando el PIN (verificación) con el PIN real y, si coinciden, se activa la máquina de estado intrínseca. Cabe señalar que, según el estándar de pago EMV, el código PIN no se verifica necesariamente o no se requiere para pagos pequeños.

En la etapa 32, el cliente mueve el terminal equipado con medios de comunicación de RFID a las proximidades de un lector externo. El lector externo lee los datos de la tarjeta de confianza y el resultado de la verificación del código PIN desde la zona de confianza en la etapa 33. En la etapa 34, los datos se reenvían al emisor de la tarjeta de confianza original del sistema servidor, que devuelve una respuesta de nuevo al terminal de punto de venta externo que participa en la transacción. El lector externo puede realizar también una verificación sin conexión en la etapa 34, en cuyo caso el resultado de la verificación del código PIN, leído desde el terminal y aceptado, conduce a la aceptación de la transacción de pago en el sistema del comerciante, y se imprime un recibo correspondiente a la transacción para el cliente desde el lector externo en la etapa 37. Los datos de la transacción de pago son transmitidos también automáticamente por el lector externo a la tarjeta de confianza en la etapa 35 y, además, al servidor en la etapa 40. Después de esto, se informa al usuario de la conclusión de la transacción, y el terminal puede retirarse de las proximidades del terminal del punto de venta en la etapa 36. Si la verificación falla en la etapa 34, los datos de la transacción de pago se transmiten en forma encriptada al sistema servidor en la etapa 38. El sistema servidor marca la transacción de la etapa 27 como fallida en la etapa 39. Finalmente, se informa al usuario del fallo de la transacción y se detiene la transacción de pago.

La transacción de pago puede realizarse también según otra realización, tal como se muestra en la Figura 4. La segunda realización del sistema de pago permite la transacción de pago sin comunicación directa con el servidor del operador. En esta realización, el servidor del operador comprende instrucciones generales y específicas del usuario acerca de la frecuencia con la que el usuario debe realizar la autenticación definida por el operador, la verificación del estado y las transacciones de la tarjeta de confianza, y la sincronización con el sistema servidor. De esta manera, la tarjeta de confianza puede funcionar y puede usarse para transacciones de pago de manera independiente sin autorización por el sistema servidor del operador, hasta que expira un límite de tiempo determinado o se cumple un límite de gasto almacenado en la tarjeta de confianza. Se informa al usuario de ambos eventos antes del vencimiento del período de validez o del agotamiento del límite de saldo. Si lo desea, el usuario puede realizar una reactivación en cualquier momento antes del vencimiento del plazo o después de este, en cuyo caso la tarjeta de confianza no puede usarse hasta que sea reactivada.

La reactivación puede realizarse, tal como se muestra en la Figura 4, iniciando sesión con el terminal en el sistema del operador en las etapas 42 a 45, tal como se presenta en la primera realización de la Figura 3. Además, el sistema servidor encripta el límite de pago, el plazo de validez de la tarjeta de confianza y el secreto del operador con el certificado de la tarjeta de confianza del terminal de dicho usuario en la etapa 46. Aquí, el plazo de validez de la tarjeta de confianza se refiere a la política de seguridad definida por el operador, ya que la tarjeta de confianza tiene que ser reactivada por el servidor para poder ser usada de nuevo. Un ejemplo del plazo de validez podría ser un día. A continuación, en la etapa 46, los datos encriptados se transmiten al terminal, en el que se transfieren a la zona de confianza y se almacenan en la etapa 47.

En la etapa 48, la transacción de pago se activa al iniciar la aplicación en cuestión y acercar el terminal a las proximidades de un lector externo en la etapa 49. Por otra parte, la activación de la transacción de pago puede realizarse también sin iniciar la aplicación, en cuyo caso la aplicación es iniciada por el lector externo. El lector externo recupera los datos de la tarjeta de confianza desde la zona de confianza en la etapa 50, y se muestra una vista de los datos de la transacción de pago en el terminal del usuario en la etapa 51. En la etapa 52, el usuario introduce la contraseña SS1 en el terminal y, como acuse de recibo, lo acerca al lector externo de nuevo en la etapa 53. El lector externo recupera el resultado de la verificación del código PIN de la tarjeta de confianza en la etapa 54 y procesa la transacción en la etapa 55. Además, el lector externo transmite los datos acerca de la transacción de pago a la tarjeta de confianza que en la etapa 56 los almacena en la zona de confianza y cambia el saldo restante según la transacción. Se muestra al usuario una vista correspondiente de esto en la etapa 57. En una realización, las etapas 50 a 54 pueden combinarse de manera que la contraseña SS1 se proporcione primero al terminal o al lector externo, después de lo cual el terminal se acerca a las proximidades del lector externo. Esto es seguido directamente por la aceptación o el rechazo, almacenándose el resultado de manera correspondiente en el terminal en la etapa 56, y se muestra al usuario una vista de la transacción de pago en la etapa 57. Cabe señalar que, según el estándar de pago EMV, el código PIN no se verifica ni se requiere necesariamente para pagos pequeños.

Cuando el plazo de validez de la tarjeta según la política de seguridad del operador expira, por ejemplo, después de un día desde la activación anterior, se muestra una vista al usuario en la etapa 58, solicitando al usuario que active la tarjeta

de confianza antes del siguiente uso Además, en la etapa 59, el terminal encripta una verificación y la añade a un archivo de registro que contiene las transacciones de pago, para ser transferidas en la etapa 60 desde la zona de confianza del terminal a través de una conexión segura al sistema servidor, y se almacena en la etapa 61 De manera correspondiente, la tarjeta de confianza y el usuario se autentican en la etapa 27 de la Figura 3, y la tarjeta de confianza se reactiva mediante las etapas 44 a 47 de la Figura 4.

La disposición de la Figura 4, en la que el secreto del programa de pago se recupera al terminal del usuario antes de la transacción de pago en el terminal del comerciante, puede proporcionar la ventaja de que la disposición es capaz de realizar la verificación de la transacción de pago automáticamente tras una solicitud por parte del terminal del comerciante, incluso en menos de medio segundo. Además, la disposición tiene la ventaja de que no se necesita conexión en línea desde el terminal del usuario al sistema servidor. Esta solución es ventajosa, por ejemplo, en una tienda de comestibles.

En las dos realizaciones presentadas anteriormente, la liquidación de cuentas al comerciante puede realizarse de la misma manera que en los sistemas de tarjetas de crédito convencionales. El comerciante transmite los datos de la transacción de pago exitosa en un paquete al banco o a la compañía de crédito para la liquidación de cuentas. En base a los datos de la transacción de pago, el banco o la compañía de crédito proporciona una cuenta al comerciante. Esta etapa no se ilustra en la Figura 3, pero debe entenderse como una parte natural del sistema.

En conexión con el sistema de pago según la invención, la RFID (Radio Frequency IDentification, identificación por radiofrecuencia) se usa para transmitir los datos de pago al destinatario del pago, es decir, al comerciante. La RFID es un procedimiento para la lectura remota y el almacenamiento de datos mediante etiquetas de RFID. De manera ventajosa, el sistema según la invención emplea una aplicación particular de RFID, NFC. En este contexto, NFC, o Near Field Communication, se refiere a una tecnología que permite la identificación remota por radiofrecuencia basada en RFID a distancias muy cortas de no más de unos pocos centímetros. La mayor diferencia con las etiquetas de RFID convencionales es el hecho de que un dispositivo NFC puede usarse tanto como un dispositivo lector como una etiqueta, a diferencia de los dispositivos de RFID convencionales. La NFC puede usarse en conexión con teléfonos móviles proporcionando funcionalidades NFC a los teléfonos. La NFC puede adaptarse también en los teléfonos mediante tarjetas SIM o microSD particulares. La conexión NFC se basa en la inducción de un campo electromagnético a la frecuencia de radio de 13,56 MHz. La velocidad de transmisión de datos puede ser 106, 212 o 424 kbit/s, que son adecuadas para la transmisión de pequeñas cantidades de datos. Cuando se procesan grandes cantidades de datos, la NFC puede usarse para establecer la conexión en la que se realiza la transmisión de datos real, por ejemplo, a través de Bluetooth.

La NFC solo se usa para la comunicación entre el terminal y el lector del comerciante en el sistema, según los estándares del foro NFC. La aplicación de pago se asegura de que los datos bancarios necesarios y el resultado de la autorización se proporcionen al lector externo a través de una conexión APDU (APDU = unidad de datos del protocolo de aplicación). Además, cuando se usa el término RFID o NFC, puede usarse también una WLAN (Wireless Local Area Network, red de área local inalámbrica), de manera que el terminal del punto de venta puede situarse lejos del cliente que realiza el pago, mientras está a una distancia de aproximadamente 5 cm en el caso de NFC. Ambos son formatos de conexión ya estandarizados. WLAN puede usarse, por ejemplo, de la siguiente manera. Un cliente entra a una tienda y activa la tarjeta de confianza mediante la NFC a través del servicio de un proveedor de servicios. La NFC se establece en un modo de escucha y, simultáneamente, se activa la WLAN. Esto puede hacerse en el estándar NFC, al igual que la activación de Bluetooth. El cliente va de compras a la tienda y compra artículos utilizando chips de póster NFC fijados por el comerciante sobre las etiquetas de precio. El usuario muestra su terminal con el chip NFC en un estado activo sobre la etiqueta de precio, y el precio y/o la cantidad se introduce a través del protocolo APDU al terminal en el sistema del proveedor de servicios. Una vez que el cliente ha terminado de comprar, puede pagar los artículos directamente a través de la WLAN o directamente a través de la NFC mediante el sistema según la invención. Cuando se paga a través de NFC, el comerciante debe tener un lector NFC externo y, en el caso de la WLAN, el comerciante debe proporcionar una red WLAN en el interior de la tienda.

Los comandos APDU presentados por el lector NFC externo del destinatario del pago, es decir el comerciante, al terminal del usuario en la transacción de pago se presentan al final de la sección de descripción. Al final de la descripción, hay también tablas 1a a 2b, en las que las Tablas 1a y 1b muestran las variables usadas en la transacción de pago de la Figura 3 y sus diferentes valores en las diferentes etapas de la transacción de pago. El valor TZ mostrado en las Tablas 1a y 1b corresponde a las etapas de las Figuras 2 y 3. De manera correspondiente, las Tablas 2a y 2b muestran las variables usadas en la transacción de pago de la Figura 4 sin una conexión de red, y sus valores en las diferentes etapas de la transacción de pago. El valor TZ mostrado en las Tablas 2a y 2b corresponde a las etapas de las Figuras 2 y 4.

La Figura 5 es una ilustración de un sistema que representa el estado de la técnica. Según la Figura, el terminal tiene una zona de confianza en la que se almacenan los datos confidenciales. Toda la comunicación entre el terminal y el sistema servidor tiene lugar a través de un teleoperador. El uso del teleoperador aumenta la complejidad del sistema y

aumenta el riesgo de una violación de la seguridad de los datos en forma de etapas adicionales en el proceso. Sin embargo, el mayor problema es el hecho de que en los sistemas controlados por teleoperadores, el secreto del sistema servidor se suministra al terminal del usuario en conexión con el registro o la activación solamente. Después de esto, la tarjeta de confianza del terminal no se gestiona en modo alguno en conexión con las transacciones de pago. Solo el cierre de la tarjeta de confianza, por ejemplo, en conexión con un uso fraudulento de la tarjeta de confianza, es una medida administrativa por parte del teleoperador. En los sistemas según la invención, la transacción de pago por el usuario normalmente requiere solo un código PIN, mediante el cual el usuario verifica el pago.

A continuación, se explicará la arquitectura de alto nivel de las realizaciones basadas en dos soluciones arquitectónicas diferentes del sistema de pago según la invención en vista de las características esenciales del sistema de pago, con referencia a las Figuras 6 y 7. En las Figuras 6 y 7, las entidades en negrita ilustran la aplicación y las soluciones del sistema propiedad de, y desarrolladas por, el sistema del operador, mientras que las entidades blancas son subconjuntos descritos en otros estándares y especificaciones. De manera correspondiente, las secuencias de comunicación en negrita representan procedimientos y realizaciones basadas en las propias soluciones del operador, mientras que las secuencias más delgadas representan soluciones definidas en otros estándares diferentes seleccionados de manera ventajosa por el operador en vista de la industria y la tecnología.

El terminal del usuario contiene una zona de confianza premontada en el terminal por el fabricante del dispositivo o una parte interesada. La zona de confianza puede ser una zona creada en el terminal en la etapa de fabricación, una zona colocada en una tarjeta SIM o una tarjeta de memoria externa, o una zona virtual creada mediante programación. La zona de confianza funciona en general en la zona TEE (Trust Execute Environment, entorno de ejecución de confianza); a dicha zona de confianza se hace referencia también con el acrónimo Tree. En situaciones ejemplares, se usa el término TEE. La clasificación de seguridad de la zona TEE se verifica mediante un procedimiento de encriptación particularmente fuerte y seguro. Normalmente, esto significa que la integridad del TEE desde el punto de vista de la seguridad es verificada por el fabricante del terminal en la etapa de fabricación mediante una cadena de caracteres encriptada integrada en la zona encriptada. Dichas zonas encriptadas incluyen, por ejemplo, eFuse, que se basa en la tecnología IBM. La cadena de caracteres no puede ser cambiada o leída por la aplicación que se ejecuta en la zona encriptada durante la ejecución. Dicho proceso se denomina secuencia de arranque encriptada.

Es característico del entorno TEE que en el mismo terminal sea posible realizar, no solo las operaciones limitadas por la zona segura aislada, sino también las operaciones de la zona no segura durante la misma secuencia de arranque. Los datos secretos y permanentes que permanecen en forma encriptada e integrada pueden almacenarse en la zona de confianza. La integridad del entorno TEE puede ser verificada, si es necesario. La zona no segura puede formarse en cualquier plataforma de sistema operativo, por ejemplo, Symbian. En la zona no segura, se usa un lenguaje de programación traducido al lenguaje máquina, que puede ser, por ejemplo, QML/QT/C++ o HTML5. El tráfico de datos en la zona no segura es encriptado por la tarjeta de confianza de la zona de confianza y, por lo tanto, permanece protegido. De esta manera, la mayoría de los datos confidenciales pueden almacenarse fuera de la zona de confianza.

En el entorno TEE, hay varias plataformas encriptadas con diferentes características y funciones como zona de confianza. La zona de confianza puede actuar como una parte virtual del sistema operativo, es decir, como un componente de software, como una zona de confianza implementada a nivel de circuito, como un módulo de chip físico externo, en ambos roles simultáneamente. Las plataformas de confianza más comunes incluyen TPM (Trusted Platform Module) y MTM (Mobile Trusted Module), ambas especificadas por TCG (Trusted Computing Group). Para algunas partes, MTM se identifica con dispositivos móviles, pero en otros aspectos, las plataformas TMT y TPM se parecen mucho una a la otra. Otras plataformas encriptadas incluyen MShield, que está basada en tecnología de Texas Instruments, y Java Card que está implementada por software y está basada en tecnología de Oracle, y TrustZone que está implementada a nivel de circuito y está basada en tecnología de ARM.

En este contexto, el acrónimo ARM (de las palabras Advanced RISC Machines) se refiere a un microprocesador de 32 bits realizado con arquitectura de microprocesador, es decir, circuito integrado SoC (System-on-a-chip). La ARM es una arquitectura RISC y, en la actualidad, es particularmente común en los procesadores de asistentes digitales personales, teléfonos móviles y sistemas integrados. ARM es muy adecuada para terminales de pequeño tamaño, ya que puede implementarse con relativamente poca lógica con relación a su rendimiento. A pesar de su pequeño tamaño, los procesadores ARM son procesadores considerables, ya que pueden contener, por ejemplo, una unidad de control de memoria que permite la ejecución de sistemas operativos sofisticados.

En el procesador ARM, la zona de confianza se denomina Zona de Confianza. Dicha zona de confianza se encuentra, entre otras cosas, en un procesador ARMv6KZ. La zona de confianza puede implementarse por medio de dos procesadores virtuales que son compatibles con un control de acceso basado en hardware. Como resultado, las aplicaciones pueden utilizar dos áreas en paralelo, siendo una de confianza y la otra no segura. El acceso a la zona de confianza solo se proporciona para ciertas aplicaciones que están aseguradas por la zona de confianza. Es posible usar un sistema operativo más grande en la zona no segura y un sistema protegido más pequeño en la zona de confianza. La zona de confianza y la zona no segura pueden usarse independientemente una de la otra.

De manera alternativa, el sistema puede implementarse de manera que la zona de confianza sea una tarjeta SIM o que la zona de confianza se proporcione en un módulo de chip externo o interno a ser instalado en el terminal. La zona de confianza implementada por software puede ser, por ejemplo, una tarjeta Java que contiene fuertes protecciones internas.

Es esencial que la zona de confianza cumpla con la clasificación de seguridad requerida para las tarjetas inteligentes sin contacto y los sistemas de pago por parte de las instituciones financieras y los emisores de tarjetas, tales como bancos, para cuya clasificación de seguridad se usa generalmente la especificación EMVCo como referencia. De esta manera, el operador propietario del sistema servidor adquiere y almacena también de manera segura las claves necesarias para operar con dicha zona de confianza. De manera más precisa, el sistema servidor contiene también una zona de confianza que cumple con la clasificación de seguridad requerida de los sistemas de pago. En la actualidad, la autenticación IMEI y el protocolo SIMLock que se usan en entornos SIM/UICC no cumplen en todos los aspectos los criterios de seguridad requeridos para dicho sistema. Se ha encontrado que, con poco esfuerzo, usando un cable USB y un ordenador personal, es posible circunvalar dicho procedimiento de autenticación.

La Figura 6 muestra cómo puede implementarse la aplicación 106 de pago, por ejemplo, como una solución basada en una tarjeta Java con un elemento 65 de seguridad. De esta manera, cuando el usuario está registrado en el sistema 68 servidor de la Figura 6 según la Figura 2, la aplicación 70 de gestión de tarjeta de confianza del sistema 68 servidor empaqueta la aplicación de tarjeta Java como un archivo JAR/CAP y genera secuencias de comandos APDU a partir del mismo para la instalación.

Después de esto, los archivos de instalación producidos se encriptan con las claves requeridas por la zona de confianza y se transmiten a través de una conexión https a la aplicación 63 host en el terminal del usuario según las etapas 5 a 9 de la Figura 2. La aplicación host actúa como “middleware” entre el sistema servidor y la tarjeta de confianza y proporciona al usuario una interfaz de usuario mediante funciones y vistas permitidas. Si las políticas de seguridad de la zona de confianza en el terminal lo permiten, la aplicación Java Card se comunica directamente con el servidor 69 www y, de esta manera, la aplicación 63 host solo se usa como una interfaz para las vistas mostradas al usuario. Por otra parte, la interfaz 87 de usuario puede ser un componente de software separado, tal como se muestra en la Figura 5. La aplicación 63 host es firmada también según los requisitos de seguridad del área de TEE, de manera que el paquete de instalación recibido para la misma pueda ser instalado en la zona de confianza en el entorno JCRE empleando la secuencia de comandos APDU contenida en el paquete de instalación. Por otra parte, si el operador lo desea por alguna razón, la instalación puede ser realizada también por un operador externo de confianza al que puede hacerse referencia mediante el acrónimo general TSM (Trusted Service Manager). De esta manera, la responsabilidad general de la instalación y administración de la tarjeta de confianza se transfiere a una tercera parte de confianza centralizada. El procesamiento, la autenticación y la gestión de las transacciones de pago son realizados por el operador, tal como se presenta en la descripción de la transacción de pago en las Figuras 3 y 4.

En la transacción de pago de la Figura 3, el usuario activa la tarjeta de confianza del operador al iniciar la aplicación de pago del usuario en el terminal. Cuando se inicia, la aplicación de pago del usuario realiza automáticamente una primitiva APDU SELECT que activa la tarjeta de confianza del operador de la presente memoria en base a su identificación (ID). Sin embargo, la tarjeta de confianza se configura interiormente en un estado en el que su activación real no es posible hasta que el secreto SS2 (verificación) del operador, que solo es conocido por el operador, se recibe desde el sistema servidor. El secreto es único para cada tarjeta de confianza instalada. En base al secreto del sistema servidor, se forma un PIN (verificación), que se compara con el código PIN real creado en el registro, para activar la máquina de estado de la tarjeta de confianza. La activación real se refiere al estado de la máquina de estado interna de la tarjeta de confianza, en cuyo estado la tarjeta de confianza puede actuar de manera independiente y directa con un lector 67 externo. Primero, después de un inicio de sesión exitoso, se realiza la activación real de la tarjeta de confianza, cuando el secreto SS2 del operador obtenido en forma encriptada desde el servidor se ha almacenado en la tarjeta 100 de confianza en la aplicación 65 Java Card de la zona 64 de confianza.

Para el inicio de sesión, se aplica una autenticación bidireccional, en la que tanto el sistema servidor como la Java Card se autentican mediante sus identificaciones y certificados intercambiados en la etapa de registro, tal como se muestra en la Figura 2. En este contexto, la Java Card 65 se usa como un medio para activar y desactivar el derecho de uso de la aplicación 106 de pago. La identificación del sistema servidor es su dirección web con el certificado, y la identificación usada para la tarjeta es la identificación única creada para la misma en la etapa de empaquetado antes de la instalación.

Después de esto, el usuario acerca el terminal a las proximidades del lector externo, habiendo recibido información a través de la interfaz de usuario acerca de la activación exitosa de la tarjeta de confianza. El lector 67 externo se comunica con la Java Card 65 mediante comandos APDU a través del módulo 66 NFC según el estándar ISO/IEC 14443, transmitiendo simultáneamente los datos de pago, tales como la suma total, desde el lector del comerciante a la interfaz 63 de usuario La aplicación de interfaz de usuario recibe los datos de pago desde la tarjeta inteligente aplicando el protocolo APDU, escuchando los eventos recibidos en la aplicación 106 de pago.

Cuando la aplicación 106 de pago transmite una solicitud de pago al sistema 68 servidor, un módulo 73 de verificación

automática de transacciones verifica el estado de la tarjeta, así como la disponibilidad de la suma a pagar con respecto a los límites de gasto personal del usuario desde la base 71 de datos en base al ID de la tarjeta de confianza. El límite de gasto personal, es decir, la línea de crédito, puede verificarse tanto en el terminal como en el sistema servidor. El resultado, encriptado con una clave simétrica, se devuelve a la tarjeta inteligente en el terminal. El resultado contiene un comando APDU encriptado que establece un código PIN en la primitiva APDU:Process de la Java Card. Después de esto, se reconoce el pago; es decir, el terminal del usuario se acerca de nuevo a las proximidades del lector externo, que lee el resultado de la verificación desde una variable protegida en la tarjeta inteligente de la Java Card usando comandos APDU según el estándar ISO/IEC 14443.

La Figura 7 muestra otra realización de una arquitectura usada posiblemente en el sistema. En el ejemplo, el TEE usado es una plataforma TrustZone, y la plataforma de credenciales es Obc (On Board Credential), que se basa en tecnología de Nokia, usada en plataformas de teléfonos inteligentes Nokia, tales como Windows Phone, Symbian y Meego. Dicha plataforma de credenciales cumple también los requisitos de la especificación EMVCo. La palabra "credencial" se refiere a una combinación en la que el programa y los datos encriptados necesitan un almacenamiento encriptado y un bus o una ruta encriptados para su comunicación mutua en el terminal del usuario. Otras plataformas de credenciales incluyen TEM, SKS, Flicker y TruWallet, que podrían usarse también como plataformas para el sistema de pago según la invención, con modificaciones que son obvias para una persona experta en la técnica. La función de la plataforma de credenciales es administrar las credenciales creadas en la zona de confianza y liberar algunas propiedades de encriptación de la plataforma del terminal para su uso por una aplicación, dependiendo la transparencia de las propiedades del nivel de fiabilidad requerido por la aplicación.

Para su funcionamiento, la plataforma de credenciales Obc necesita una zona de confianza definida, que en este ejemplo es el área TrustZone basada en tecnología ARM. En la práctica, esto significa que el entorno TEE debería comprender un área definida de la memoria RAM, que puede ser usada cuando se libera una cadena de caracteres encriptada en el proceso de inicio del terminal. Esta cadena de caracteres encriptada ha sido suministrada y codificada para ser específica del terminal por el fabricante del dispositivo, y no puede modificarse ni leerse desde la zona de confianza que funciona en el área TEE. En conexión con la plataforma de credenciales Obc, se usa el lenguaje de script LUA en la zona de confianza.

El terminal 84 de Obc según el sistema contiene una plataforma Obc instalada por el fabricante del terminal. En esta realización, el terminal 84 se caracteriza porque el terminal 84 comprende una aplicación 77 Obc Interpreter que es su núcleo y se usa para aislar las credenciales de otras posibles credenciales en el área 86 TEE. La tarjeta 100 de confianza se instala en el interior de la aplicación 77 Obc Interpreter para aislarla. Además, el terminal 84 comprende un Obc Provision Client 74 que representa la interfaz a ser proporcionada para la aplicación, y un Obc Credential Manager 75 que es responsable de las conexiones de las aplicaciones con el TEE 86 y de administrar la base 78 de datos Obc. Esta realización del sistema de pago se caracteriza también porque el terminal 84 está provisto de un conjunto de claves específicas del terminal instaladas por su fabricante, concretamente, OPK (Obc Platform Key), un par de claves internas (SK1, PK1) para el terminal, y un par de claves externas (SKe, PKe) para el terminal. Estas claves se usan para una comunicación encriptada y fiable con partes fuera de la zona de confianza.

La aplicación 106 de pago a ser descargada por el usuario en la etapa de registro comprende un programa 74 Obc Provision Client para comunicación protegida, así como un componente 87 de interfaz de usuario para comunicarse con el usuario. La distribución y el uso de la parte sensible de la aplicación y los secretos o credenciales relacionados con la misma generalmente se inician de manera que la aplicación 74 Obc Provision Client en el terminal 84 del usuario establezca una conexión con la aplicación 83 de administración del sistema 85 servidor del operador o una tercera parte de confianza, es decir, el servidor 85 de aprovisionamiento, que actúa de esta manera como medio del sistema servidor para comunicarse con el servidor 82 web operativo.

La aplicación 74 Obc Provision Client transmite una clave general certificada por el fabricante del dispositivo al servidor 85 de aprovisionamient. El servidor 85 de aprovisionamiento transmite un número definido de paquetes al terminal 84. Un paquete de aprovisionamiento puede contener, por ejemplo, un programa y datos encriptados para un proceso de autenticación, así como una autorización necesaria que proporciona a dicho programa acceso a los datos encriptados. Usando el Credential Manager 75, la aplicación 74 Obc Provision Client crea una nueva credencial, es decir, introduce el programa y los datos encriptados en el sistema Obc. De esta manera, la aplicación 74 Obc Provision Client se usa en esta realización como un medio para activar y desactivar el derecho de uso de la aplicación 106 de pago. El Obc Credential Manager 75 encripta el paquete transmitido desde el servidor 85 de aprovisionamiento aplicando la aplicación Provision System 76 y la parte privada de la clave del terminal, y encripta el secreto que pertenece a la credencial usando una OPK simétrico (Obc Platform Key) identificada para el terminal 84 e instalada por el fabricante del terminal. Finalmente, el Credential Manager 75 almacena el secreto protegido y el programa en la base 78 de datos Obc.

En la realización del sistema de pago mostrada en la Figura 7, la transacción de pago tiene lugar principalmente tal como se muestra en las Figuras 3 y 4. La diferencia con la realización mostrada en la Figura 6 radica en las etapas 23, 32 y 53 cuando el usuario ha iniciado sesión en el sistema de pago, el terminal 84 se acerca a un lector 81 externo. De esta

manera, el lector 81 externo activa el nombre de servicio activo seleccionado o la estación base del servidor a través del módulo 80 NFC de un protocolo P2P (punto a punto) o un protocolo NFC R/W (lectura/escritura), mediante el uso de una aplicación intermedia, es decir, un “middleware” 79, creado durante el registro En este contexto, el “middleware” 79 se refiere al componente de aplicación del operador que recibe y transmite los mensajes recibidos desde el módulo 80 NFC a través de una extensión del protocolo P2P, es decir Protocolo LLCP, después de lo cual activa los datos encriptados necesarios y recupera los datos del usuario y la autenticación del usuario desde la zona 86 de confianza mediante el uso de la interfaz del Credential Manager 75. El uso y la solicitud del protocolo LLCP se realiza a través de las interfaces de aplicación proporcionadas por el operador de la plataforma.

Como ejemplo, el lector 81 externo transmite una solicitud de pago (150;eur;02/12/2011;stockmann tapiola) al terminal 84 a través de NFC. El “middleware” 79 recibe los mensajes según el protocolo LLCP y transmite los datos recibidos a la aplicación 106 de pago que actúa en la zona 86 de confianza y activada por el usuario a través de la interfaz 87. La aplicación 106 de pago verifica si el valor almacenado en la variable saldo es suficiente para aceptar la transacción. Si se acepta el pago, los datos de pago se transmiten a la interfaz 87 de usuario UI del usuario y, además, al sistema 85 servidor. El código PIN de la tarjeta de confianza ha sido introducido previamente en el sistema, por ejemplo, en las etapas 30 y 47 de las Figuras 3 y 4.

Si la parte que se comunica es un lector externo de un comerciante u otro dispositivo compatible con el protocolo P2P, se devuelve el resultado de la verificación del código PIN o una contraseña de un solo uso a la misma a través del “middleware”. De manera alternativa, la aceptación del pago puede transmitirse en forma encriptada al lector externo a través del sistema servidor del operador a través de Internet o una red telefónica, si la solicitud de pago recibida contiene también la información necesaria para enrutar dicho lector externo u otro dispositivo, para encriptar un mensaje que denota la aceptación del pago. La información puede ser, por ejemplo, una dirección IP o un número de teléfono, así como la clave simétrica o pública del lector externo.

En la realización del sistema de pago según la Figura 7, el “middleware” 79 y la aplicación 74 Obc Provision Client son códigos de programa ventajosamente separados, realizando cada uno su propia tarea. La función de la aplicación 74 Obc Provision Client es la de encargarse de la comunicación del terminal 84 con el sistema 85 servidor y activar el derecho de uso de la aplicación 106 de pago. A su vez, el “middleware” es responsable de la comunicación del terminal con el lector NFC del destinatario del pago. De esta manera, el “middleware” no ve los datos recibidos por la aplicación Obc Provision Client, al menos no en texto claro, lo que aumenta la seguridad de los datos del sistema.

A continuación, se presentará un caso ejemplar del uso de NFC. El usuario tiene un terminal móvil que soporta, por ejemplo, la tecnología Nokia NFC, por ejemplo, Nokia N9 o Nokia 701, y que contiene una zona de confianza integrada y configurada en el terminal. La zona de confianza asegura los datos confidenciales y la aplicación instalada en la misma. En conexión con el registro de usuario, se ha instalado una tarjeta de confianza en la zona de confianza. La tarjeta de confianza contiene los datos bancarios y de cuenta del operador, el número de tarjeta personal del cliente y una clave secreta, un certificado CA, un certificado de tarjeta de confianza (el certificado que contiene la identificación de la tarjeta de confianza y la clave pública, así como una firma escrita por la CA del sistema servidor del operador), siendo el tamaño total de aproximadamente 20 a 50 kbytes. Los tamaños de los elementos individuales son: CA ≤ 2 kb, la clave secreta ≤ 2 kb, la clave pública/certificado ≤ 2 kb, los datos bancarios <0,5 kb y la aplicación de 15 a 30 kb.

Además, la tarjeta de confianza contiene una aplicación Java Cardlet que es responsable de la administración de los comandos APDU con el lector externo y de la creación y la administración de conexiones TLS/SSL con el sistema servidor. Además, la aplicación Java Cardlet es responsable del procesamiento de certificados y claves entre el terminal y el sistema servidor.

La compra de NFC se realiza, por ejemplo, en las siguientes etapas:

1. El cliente entra a una tienda, selecciona los artículos a comprar de la manera normal y, a continuación, en un momento adecuado, inicia la aplicación del operador. El cliente introduce el secreto SS1 del usuario en la aplicación, de manera que la tarjeta de confianza se autentica en la zona de confianza, y después de la autenticación exitosa, la tarjeta es activada por el sistema servidor del operador usando el secreto SS2 del sistema servidor. Además, el resultado de la autenticación se almacena en la tarjeta de confianza. El protocolo de comunicación es bidireccional sobre SSL/TLS GPRS, 3G o WLAN.

2. El cliente entra a la cola del cajero con sus compras.

3. El cajero introduce la suma de las compras en un lector externo equipado con un chip NFC.

4. El usuario acerca el terminal al lector externo, dentro de una distancia menor que 10 cm, de manera que el lector introduce los datos de la transacción de ventas mediante comunicación NFC/APDU en el terminal del usuario y recupera los datos bancarios desde el terminal del usuario según los estándares NFC. La suma y la selección ACEPTAR/RECHAZAR se muestran al usuario en la pantalla del terminal.

5. El terminal del usuario transmite los datos recibidos al sistema servidor del operador (a través de TLS GPRS, 3G o WLAN), que almacena los datos de la transacción de pago y recupera el resultado (si la suma es correcta). La suma puede estar almacenada ya en la tarjeta de confianza, en cuyo caso la etapa 5 no es necesaria.

6. El usuario muestra el terminal al lector externo del comerciante de nuevo, el cual lee la aceptación/el rechazo. Además, el lector externo toma su propia decisión en base a una verificación sin conexión o solicitando una verificación por parte de una compañía de crédito o del operador (de esta manera, los datos son recibidos por el lector en la etapa 4), recupera la solicitud ACEPTADA/RECHAZADA al terminal aplicando NFC/APDU e imprime un recibo.

7. El terminal del usuario transmite el resultado (confirmar/cancelar) recibido en la etapa 6 al sistema servidor. Si el pago ya se ha realizado anteriormente en el sistema servidor del operador, la etapa 7 no es necesaria. De esta manera, la variable numérica que representa el saldo de gasto interior disponible de la tarjeta de confianza se actualiza a través de NFC y APDU en base a la decisión tomada por el lector externo en la etapa 6.

8. El comerciante transmite un paquete que contiene los datos de la transacción de pago a un banco o una compañía de crédito para la liquidación de las cuentas.

A continuación, se presentarán los comandos APDU proporcionados por el destinatario del pago, es decir, el lector NFC externo del comerciante, a la tarjeta de confianza del terminal del usuario en conexión con una transacción de pago; en respuesta, el lector externo recibe los valores leídos desde la tarjeta de confianza y las funciones a ejecutar. En la etapa 24 de la Figura 3, el lector externo del comerciante transmite un comando APDU: GET PROCESSING OPTIONS, que solicita los siguientes datos que la tarjeta de confianza envía al lector externo:

- Perfil de intercambio de aplicaciones (qué formas de autenticación son compatibles con SDA (datos estáticos), DDA (autenticación de datos dinámicos)). Por ejemplo, se selecciona DDA.

- Localizador de archivos de aplicación (qué archivos y registros se leen desde la tarjeta de confianza, por ejemplo, registros que pertenecen a la autenticación de datos sin conexión))

En las etapas 24 y 25, el lector NFC transmite una solicitud APDU: READ RECORD (Leer datos de aplicación), en la que se solicitan los siguientes datos, que la tarjeta de confianza transmite al lector externo:

- Identificador de aplicación (AID) (ID de la tarjeta de confianza)

- Fecha de vencimiento de la solicitud (determinada en la etapa de registro)

- Fecha de efectiva de la solicitud (determinada en la etapa de registro)

- Código de moneda de la aplicación (moneda)

- Exponente de moneda de la aplicación ()

- Número de cuenta principal de la aplicación

- Lista 1 de objetos de gestión de riesgos de tarjeta número de secuencia número de cuenta principal de la aplicación (PAN) (la lista de objetos de riesgo es recibida desde el terminal por la tarjeta de confianza. La autenticación se ejecuta en la tarjeta de confianza. Por ejemplo, límite máximo, contador de intentos de pin)

- Lista 2 de objetos de gestión de riesgos de la tarjeta

- Nombre del titular de la tarjeta

- Nombre extendido del titular de la tarjeta

- Preferencia de idioma

- Lista de CVM (Reglas de verificación de la tarjeta: por ejemplo, "PIN sin conexión"; "autenticación de transacción con conexión").

En la misma etapa, el lector externo transmite también un comando APDU:GET DATA, mediante el cual recupera los datos de la transacción.

En la etapa 49 de una transacción de pago sin conexión de red, se realiza la autenticación dinámica de datos (autenticación de datos sin conexión, seleccionada en la etapa de obtención de opción de procesamiento), de manera que el terminal del usuario transmite primero la clave pública/el certificado de la tarjeta de confianza al lector externo del comerciante, que autentica la firma del certificado a partir del certificado CA que se encuentra en su propio almacenamiento. A continuación, el lector externo transmite datos aleatorios al terminal del usuario, el terminal firma los

datos con la clave privada de la tarjeta de confianza (clave privada ICC) y transmite la firma de los datos al lector externo. El terminal verifica la firma con la clave pública. Se verifican los siguientes elementos:

- Certificado de clave pública ICC (certificado de la tarjeta de confianza)
- Recordatorio de clave pública ICC
- Exponente de clave pública ICC
- Índice de clave pública CA
- Certificado de clave pública del emisor
- Recordatorio de clave pública del emisor
- Exponente de clave pública del emisor

En la etapa 32 de la Figura 3, el lector externo realiza una función de verificación del titular de la tarjeta (procesamiento de PIN sin conexión) mediante la transmisión de un comando APDU:VERIFY, en el que se solicita el resultado "exitoso" o "no exitoso" de la verificación del código PIN desde la tarjeta de confianza del terminal del usuario. El resultado de la verificación del código PIN se obtiene comparando el código PIN formado en el registro con el código PIN (verificación) formado durante la transacción de pago.

En la etapa 34 de la Figura 3, el lector externo ejecuta el comando APDU:GET_DATA, mediante el cual recupera la lectura del contador de transacciones de pagos desde el terminal. Además, en la etapa 34, el lector externo ejecuta el comando APDU:GENERATE AC (datos de transacción a la tarjeta - cantidad, fecha, hora, etc.), en el que el lector externo y el terminal acuerdan si se usa una verificación con conexión o sin conexión para la verificación, ARQC (con conexión) o certificado de transacción (sin conexión - aceptado) o AAC (sin conexión - rechazado). Si la tarjeta de confianza devuelve un criptograma de certificado de transacción al lector externo, se verifica el criptograma y, en el caso positivo, se acepta la transacción sin conexión (criptograma AAC transacción sin conexión rechazada). Si la tarjeta de confianza devuelve el criptograma ARQC formado con la clave del sistema servidor del operador (almacenado en la zona de confianza) al lector externo, es reenviado por el lector externo al sistema servidor, que comprueba y verifica el mensaje con su propia clave correspondiente. El sistema servidor devuelve el ARPC (Authorization Response Cryptogram, criptograma de respuesta de autorización) al lector externo y, a continuación, a la tarjeta de confianza. La decisión de aceptar la transacción se toma en base a estos datos.

Según el estándar EMV, el criptograma ARQC puede formarse tomando un código MAC a partir de los datos seleccionados del siguiente conjunto de valores, por ejemplo, según los requisitos de la compañía de tarjetas de confianza:

| **Valor** | **Fuente** |
|---|---|
| Cantidad, autorizada (numérico) | Terminal |
| Cantidad, otro (numérico) | Terminal |
| Código de país del terminal | Terminal |
| Resultados de la verificación del terminal | Terminal |
| Código de moneda de la transacción | Terminal |
| Fecha de la transacción | Terminal |
| Tipo de transacción | Terminal |
| Número impredecible | Terminal |
| Perfil de intercambio de aplicación | ICC |
| Contador de transacción de aplicación | ICC |

Aquí, la fuente se refiere a si los datos se reciben desde el terminal del comerciante (terminal) o desde la tarjeta (ICC). Además, la clave usada para formar el código MAC es una clave de sesión derivada de una clave maestra específica de la tarjeta. De manera correspondiente, el emisor de la tarjeta verifica el criptograma con una clave de sesión correspondiente, por ejemplo, derivándola de la clave maestra de la tarjeta, decide aceptar o rechazar la transacción y responde calculando ARPC = DES3 (ARQC XOR ARC), aplicando la misma clave de sesión que en la creación del

criptograma ARQC. Aquí, ARC es el código de respuesta de autorización del emisor de la tarjeta (aceptado, rechazado, etc.).

Tabla 1 a.

| | (fase de registro finalizada) | inicio de sesión | | | |
|---|---|---|---|---|---|
| Valor TZ | 14 | 17 | 19 | 20 | 21 |
| SS1 | 1234 | 1234 | 1234 | 1234 | 1234 |
| SS2 | 6789 | 6789 | 6789 | 6789 | 6789 |
| PIN_ACTIVE | 12346789 | 12346789 | 12346789 | 12346789 | 12346789 |
| PIN_EFFECTIVE | -1 | 1234 | 1234 | 1234 | 1234 |
| TRUST_CARD_STATE | SUSPENDIDA | SUSPENDIDA | SUSPENDIDA | SUSPENDIDA | ACTIVA |
| PIN-RETRY COUNTER | 3 | 3 | 2 | 3 | |
| SYK2 | -1 | -1 | -1 | -1 | 10010101 |
| Transacción de pago (fecha/ hora, cantidad, moneda, comerciante, ubicación ...) | -1 | -1 | -1 | -1 | -1 |
| Número de cuenta principal | 1111111-2222 | | | | |
| Valor de reintentos de pin máximo | 3 | 3 | 3 | 3 | 3 |
| Clave del emisor (clave del emisor de la tarjeta original. Si el operador es el emisor, la clave se genera con TZ) | 4,44444E + 11 | 4,44444E + 11 | 4,44444E + 11 | 4,44444E + 11 | 4,44444E + 11 |
| Límite máximo de la tarjeta | 200 | 200 | 200 | 200 | 200 |
| Fecha de expiración de la tarjeta | 1/1/2012 | 1/1/2012 | 1/1/2012 | 1/1/2012 | 1/1/2012 |
| | | | | | |
| | | | | | |
| Servidor | 14 | 18 | 27 | 39 | 40 |
| H(SS1) (código hash a partir de la contraseña de inicio de sesión introducida por el usuario) | -1 | 4132 | 4132 | 4132 | 4132 |
| Base de datos de usuario:H (SS1) | 4132 | 4132 | 4132 | 4132 | 4132 |
| Transacción de pago | -1 | -1 | 1.1.11;100;eur; stockmann tapiola ... | ROLLBACK (1.1.11; ...) | COMMIT (1.1.11) |

| | | | | | |
|---|---|---|---|---|---|
| | (fase de registro finalizada) | inicio de sesión | | | |
| | | | | | |
| POI | | | 15 | 24 | |
| Lista de Trust Card CVM (procedimiento de verificación del titular de la tarjeta) | | | -1 | sin conexión, con conexión | |
| Cantidad de transacción | | | 20 | | |
| Detalles de la transacción | | | | 1.1.11;100;eur: stockmann tapiola ... | |

Tabla 1b.

| Valor TZ | 26 | 28 | 30 | 35 | 38 |
|---|---|---|---|---|---|
| SS1 | 1234 | 1234 | 1234 | 1234 | 1234 |
| SS2 | 6789 | 6789 | 6789 | 6789 | 6789 |
| PIN_ACTIVE | 12346789 | 12346789 | 12346789 | 12346789 | 12346789 |
| PIN_EFFECTIVE | 1234 | 1234 | 12346789 | 12346789 | -1 |
| TRUST_CARD_STATE | ACTIVA | SUSPENDIDA | ACTIVA | SUSPENDIDA | SUSPENDIDA |
| PIN_RETRY_COUNTER | | | | | |
| SYK2 | 10010101 | -1 | 10010101 | 10010101 | -1 |
| Transacción de pago (fecha/hora, cantidad, moneda, comercio, ubicación ...) | 1.1.11;100;EUR; stockmann tapiola ... | | | FALLIDO / EXITOSO (..) | |
| Número de cuenta principal | | | | | |
| Valor máximo de reintentos de pin | 3 | 3 | 3 | 3 | 3 |
| Clave del emisor (clave del emisor de la tarjeta original. Si el operador es el emisor, la clave se genera con TZ) | 4,44444E + 11 | 4,44444E + 11 | 4.44444E + 11 | 4,44444E + 11 | 4,44444E + 11 |
| Límite máximo de la tarjeta | 200 | 200 | 200 | 200 | 200 |
| Plazo de validez de la tarjeta | 1/1/2012 | 1/1/2012 | 1/1/2012 | 1/1/2012 | 1/1/2012 |
| | | | | | |

| Valor TZ | 26 | 28 | 30 | 35 | 38 |
|---|---|---|---|---|---|
| | | | | | |
| Servidor | FIN DE SESIÓN | | | | |
| H(SS1) (código hash a partir de la contraseña de inicio de sesión introducida por el usuario) | -1 | | | | |
| Base de datos de usuario: H(SS1) | 4132 | | | | |
| Transacción de pago | ENCRYPT (base de datos.transacción de pago) | | | | |
| | | | | | |
| POI | | 33 | | | |
| Lista de Trust Card CVM (procedimiento de verificación del titular de la tarjeta) | | sin conexión, PIN CHECK = OK, límite de reintentos de PIN <contador de reintentos, cantidad de transacción <LIMIT | | | |
| Cantidad de transacción | | | | | |
| Detalles de la transacción | | | | | |

Tabla 2a.

| | (etapa de registro finalizada) | inicio de sesión | | | |
|---|---|---|---|---|---|
| Valor TZ | 14 | 43 | 47 (en esta etapa, el usuario puede cerrar sesión) | 52 | 56 |
| SS1 | 1234 | 1234 | 1234 | 1234 | 1234 |
| SS2 | 6789 | 6789 | 6789 | 6789 | 6789 |
| PIN_ACTIVE | 12346789 | 12346789 | 12346789 | 12346789 | 12346789 |
| PIN_ _EFFECTIVE | -1 | 1234 | 1234 | 12346789 | 12346789 |
| TRUST_CARD_STATE | SUSPENDIDA | SUSPENDIDA | ACTIVA | ACTIVA | ACTIVA |
| SYK3 | -1 | -1 | 2220020220 | -1 | -1 |

| | | | | | |
|---|---|---|---|---|---|
| | (etapa de registro finalizada) | inicio de sesión | | | |
| Transacción de pago (fecha/hora, cantidad, moneda, comercio, ubicación ...) | -1 | -1 | -1 | -1 | 2.2.2011;50;... |
| Límite de pago (saldo disponible) | -1 | -1 | 200 | 200 | 150 |
| Plazo de validez de la tarjeta | -1 | -1 | 24h | 20h | 20h |
| Número de cuenta principal | 1111111-2222 | 1111111-2222 | 1111111-2222 | 1111111-2222 | 1111111-2222 |
| Reintentar valor de reintentos de pin máximo | 3 | 3 | 3 | 3 | 3 |
| Clave del emisor | 4,44444E + 11 | 4,44444E + 11 | 4,44444E + 11 | 4,44444E + 11 | 4,44444E + 11 |
| Límite máximo de tarjeta | 200 | 200 | 200 | 200 | 200 |
| Fecha de expiración de la tarjeta | 1/1/2012 | 1/1/2012 | 1/1/2012 | 1/1/2012 | 1/1/2012 |
| | | | | | |
| | | | | | |
| Servidor | 43 | 44 | 47 | 57 | 59 |
| H(SS1) (código hash a partir de la contraseña de inicio de sesión introducida por el usuario) | -1 | 4132 | 4132 | -1 | |
| Base de datos de usuario: H(SS1) | 4132 | 4132 | 4132 | 4132 | |
| Transacción de pago 1 | -1 | -1 | -1 | -1 | -1 |
| Transacción de pago 2 | -1 | -1 | -1 | -1 | -1 |
| | | | | | |
| | | | | | |
| POI | | | 15 | 24 | |
| Lista de Trust Card CVM (procedimiento de verificación del titular de la tarjeta) | | | -1 | sin conexión<br>con conexión | |
| Cantidad de la transacción | | | 20 | | |

| | | | | | |
|---|---|---|---|---|---|
| | (etapa de registro finalizada) | inicio de sesión | | | |
| Detalles de la transacción | | | | 1.1.11;100;EUR ; stockmann tapiola ... | |

Tabla 2b.

| Valor TZ | 59 | 60 | 61 | CIERRE DE SESIÓN |
|---|---|---|---|---|
| SS1 | 1234 | 1234 | 1234 | 1234 |
| SS2 | 6789 | 6789 | 6789 | 6789 |
| PIN_ACTIVE | 12346789 | 12346789 | 12346789 | 12346789 |
| PIN_EFFECTIVE | -1 | 1234 | 1234 | -1 |
| TRUST_CARD_STATE | SUSPENDIDA | SUSPENDIDA | SUSPENDIDA | SUSPENDIDA |
| SYK3 | -1 | -1 | 333000330 | -1 |
| Transacción de pago (fecha/ hora, cantidad, moneda, comercio, ubicación ...) | [SEVERAL PAYMENT_TRANSACTIONS] | | | |
| Límite de pago (saldo disponible) | 72 | 72 | 72 | 72 |
| Plazo de validez de la tarjeta | 2h | 2h | 24h | 24h |
| Número de cuenta principal | 1111111-2222 | 1111111-2222 | 1111111-2222 | 1111111-2222 |
| valor de reintentos de pin máximo | 3 | 3 | 3 | 3 |
| Clave del emisor | 4,44444E + 11 | 4,44444E + 11 | 4,44444E + 11 | 4,44444E + 11 |
| Límite máximo de la tarjeta | 200 | 200 | 200 | 200 |
| Fecha de expiración de la tarjeta | 1/1/2012 | 1/1/2012 | 1/1/2012 | 1/1/2012 |
| | | | | |
| | | | | |
| Servidor | 61(posible cierre de sesión) | CERRAR SESIÓN | | |
| H(SS1) (código hash a partir de la contraseña de inicio de sesión introducida por el usuario) | -1 | -1 | | |
| Base de datos de usuario: H (SS1) | 4132 | 4132 | | |

| Valor TZ | 59 | 60 | 61 | CIERRE DE SESIÓN |
|---|---|---|---|---|
| Transacción de pago 1 | 2.12011;50;stockman n hel; | 2.2.2011;50;stockm ann hel; ... | | |
| Transacción de pago 2 | 3.2.2011;78;K-rauta espoo; ... | 3.2.2011;78;K-rauta espoo; ... | | |
| | | | | |
| | | | | |
| POI | | 33 | | |
| Lista de Trust Carda CVM (procedimiento de verificación del titular de la tarjeta) | | sin conexión, PIN CHECK = OK, límite de reintento de PIN <contador de reintentos, cantidad de la transacción < LIMIT | | |
| Cantidad de transacción | | | | |
| Detalles de la transacción | | | | |

En base a la descripción anterior, es evidente para una persona experta en la técnica que pueden implementarse diferentes realizaciones de la invención con dispositivos de procesamiento de datos, tales como servidores y terminales de usuario, así como terminales de punto de venta. Estos dispositivos pueden comprender un código de programa de ordenador para ejecutar los procedimientos según la invención, y dicho código de programa de ordenador puede formarse, según la técnica anterior, en un producto de software de ordenador que proporciona dispositivos para realizar procedimientos, cuando el código del producto de software de ordenador se ejecuta en un procesador.

La invención no está limitada a los ejemplos de la descripción anterior, o a combinaciones de los mismos, que puede implementar una persona experta en la materia, sino que el alcance de la invención está definido por las reivindicaciones adjuntas.

**REIVINDICACIONES**

1. Procedimiento para realizar una transacción de pago, comprendiendo el procedimiento:

- recibir (21) un secreto (SYK2) para una aplicación (106) de pago desde el sistema (68, 85) servidor del operador a un terminal (62, 84) del usuario en respuesta a un inicio (20) de sesión exitoso en dicho sistema (68, 85) servidor,

- activar (21) una tarjeta (100) de confianza en dicho terminal (62, 84) del usuario utilizando dicho secreto (SYK2) para la aplicación de pago, siendo dicha tarjeta de confianza una tarjeta de confianza virtual que comprende una aplicación para controlar el acceso a dicha aplicación de pago, un algoritmo de encriptación y claves para la encriptación del algoritmo de pago, y comprendiendo dicha activación el uso de dicho secreto (SYK2) para que la aplicación de pago establezca dicha tarjeta de confianza a un modo en el que dicha tarjeta de confianza pueda comunicarse con partes externas además de dicho sistema servidor,

- recibir (25) datos de pago desde un terminal (67, 81) de punto de venta en el terminal (62, 84) del usuario, estando dichos datos de pago relacionados con dicha transacción de pago,

- transmitir (26) dichos datos de pago al sistema (68, 85) servidor del operador para ser verificados, transmitiéndose dichos datos de pago en forma encriptada, encriptados por dicho secreto (SYK2) para dicha aplicación de pago, caracterizado por

- recibir (30) un segundo secreto (SS2) en el terminal (62, 84) del usuario, siendo formado dicho segundo secreto (SS2) por el sistema servidor del operador si dicha verificación de dichos datos de pago produce un resultado aceptable, estando configurado dicho segundo secreto (SS2) para ser usado para realizar dicha transacción de pago, siendo recibido dicho segundo secreto (SS2) en forma encriptada, encriptado por dicho secreto (SYK2) para dicha aplicación de pago, y

- transmitir (32) datos de la tarjeta de confianza y una combinación del secreto (SS1) de usuario y dicho segundo secreto (SS2) desde dicho terminal (62, 84) del usuario a dicho terminal (67, 81) de punto de venta para verificar y realizar la transacción de pago a través del terminal (67, 81) de punto de venta.

2. Procedimiento según la reivindicación 1, en el que dicho segundo secreto está comprendido en un criptograma ARQC.

3. Procedimiento según la reivindicación 1 o 2, que comprende:

- recibir (17) dicho secreto (SS1) del usuario desde el usuario,

- formar (30) un código a partir del secreto (SS1) del usuario y dicho segundo secreto (SS2) recibido desde el sistema servidor del operador, y

- aplicar (32) dicho código para realizar dicha transacción de pago.

4. Procedimiento según la reivindicación 3, que comprende:

- aplicar dicha tarjeta (100) de confianza para formar un criptograma para verificar la transacción de pago, conteniendo dicho criptograma dichos datos de pago.

5. Procedimiento para realizar un pago, comprendiendo el procedimiento:

- crear (8) una tarjeta de confianza en un sistema (68, 85) servidor, siendo dicha tarjeta de confianza una tarjeta de confianza virtual que comprende una aplicación para controlar el acceso a dicha aplicación de pago, un algoritmo de encriptación y claves para la encriptación del algoritmo de pago, y

- transmitir (8) datos de dicha tarjeta de confianza desde dicho sistema (68, 85) servidor a un terminal (62, 84) del usuario, para ser usados para realizar una transacción de pago,

- formar (20) un secreto (SYK2) para una aplicación (106) de pago en el sistema (68, 85) servidor, y

- en respuesta a un inicio de sesión exitoso (20) en dicho sistema (68, 85) servidor, haciendo (20) que dicho secreto (SYK2) para la aplicación (106) de pago esté disponible para ser usado por el terminal (62, 84) del usuario para activar dicha tarjeta (100) de confianza para realizar la transacción de pago, en el que el secreto (SYK2) para la aplicación de pago tiene un plazo de validez, durante el cual puede ser usada de manera autorizada para activar la tarjeta (100) de confianza, y comprendiendo dicha activación el uso de dicho secreto (SYK2) para que la aplicación de pago establezca dicha tarjeta de confianza a un modo en el que dicha tarjeta de confianza pueda comunicarse con partes externas además de dicho sistema servidor, caracterizado por

- recibir (27) datos de pago en dicho sistema (68, 85) servidor desde el terminal (62, 84) del usuario a ser verificado, recibiéndose dichos datos de pago en forma encriptada, encriptados por dicho secreto (SYK2) para dicha aplicación de pago, estando relacionados dichos datos de pago con dicha transacción de pago,

- verificar (27) dichos datos de pago en dicho sistema (68, 85) servidor, y

- hacer (29) que un segundo secreto (SS2), formado por el sistema (68, 85) servidor, este disponible para su uso por el terminal si dichos procedimientos de verificación producen un resultado aceptable, estando configurado dicho segundo secreto (SS2) para ser usado en combinación con un secreto (SS1) del usuario para verificar y realizar la transacción de pago a través de un terminal (67, 81) de punto de venta, y estando disponible dicho segundo secreto (SS2) en forma encriptada, encriptado por dicho secreto (SYK2) para dicha aplicación de pago.

6. Procedimiento según la reivindicación 5, que comprende:

- formar dicho segundo secreto (SS2) y un secreto (SS1) del usuario en el sistema servidor,

- formar un código a partir de dicho secreto (SS1) del usuario y dicho segundo secreto (SS2), y

- configurar (8) una tarjeta de confianza a ser suministrada al terminal (62, 84) del usuario a ser activada con dicho código para realizar una transacción de pago.

7. Procedimiento según la reivindicación 6, que comprende:

- recibir datos desde el usuario para formar el secreto (SS1) del usuario, y

- formar dicho secreto (SS1) del usuario en base a dichos datos.

8. Terminal (62, 84) del usuario para realizar una transacción de pago, que comprende al menos un procesador, una memoria y un código de programa de ordenador en dicha memoria, estando configurado el código de programa de ordenador, cuando se ejecuta en dicho al menos un procesador, para causar que el terminal del usuario:

- reciba un secreto (SYK2) para una aplicación (106) de pago desde el sistema servidor del operador al terminal (62, 84) del usuario en respuesta a un inicio (20) de sesión exitoso a dicho sistema (68, 85) servidor,

- active una tarjeta (100) de confianza en dicho terminal del usuario utilizando dicho secreto (SYK2) para la aplicación (106) de pago, siendo dicha tarjeta de confianza una tarjeta de confianza virtual que comprende una aplicación para controlar el acceso a dicha aplicación de pago, un algoritmo de encriptación y claves para la encriptación del algoritmo de pago, y comprendiendo dicha activación usando dicho secreto (SYK2) para que la aplicación de pago establezca dicha tarjeta de confianza a un modo en el que dicha tarjeta de confianza puede comunicarse con partes externas además de dicho sistema servidor,

- para recibir datos de pago desde un terminal (67, 81) de punto de venta en el terminal del usuario, estando dichos datos de pago relacionados con dicha transacción de pago, caracterizándose el código del programa de ordenador, cuando se ejecuta en dicho al menos un procesador, para causar que el terminal del usuario:

  - transmita dichos datos de pago al sistema servidor del operador para ser verificados, transmitiéndose dichos datos de pago en forma encriptada, encriptados por dicho secreto (SYK2) para dicha aplicación de pago,

  - reciba un segundo secreto (SS2) en el terminal (62, 84) del usuario, siendo formado dicho segundo secreto (SS2) por el sistema servidor del operador si dicha verificación produce un resultado aceptable, estando configurado dicho segundo secreto (SS2) para ser usado para verificar la transacción de pago, recibiéndose dicho segundo secreto (SS2) en forma encriptada, encriptado por dicho secreto (SYK2) para dicha aplicación de pago, y

  - transmita datos de la tarjeta de confianza y una combinación de un secreto (SS1) de usuario y dicho segundo secreto (SS2) desde dicho terminal (62, 84) del usuario a dicho terminal (67, 81) de punto de venta para verificar y realizar la transacción de pago a través del terminal (67, 81) de punto de venta.

9. Terminal del usuario según la reivindicación 8, que comprende código del programa de ordenador que está configurado, cuando se ejecuta en dicho al menos un procesador, para causar que el terminal del usuario:

- reciba un secreto (SS1) de usuario desde el usuario,

- forme un código a partir del secreto (SS1) del usuario y dicho segundo secreto (SS2) recibido desde el sistema servidor del operador, y

- aplique dicho código para realizar dicha transacción de pago.

10. Sistema (68, 85) servidor que comprende al menos un procesador, una memoria y un código de programa de ordenador en dicha memoria, estando configurado el código de programa de ordenador, cuando se ejecuta en dicho al menos un procesador, para hacer que el sistema:

- cree una tarjeta de confianza en el sistema servidor, siendo dicha tarjeta de confianza una tarjeta de confianza virtual que comprende una aplicación para controlar el acceso a dicha aplicación de pago, un algoritmo de encriptación y claves para la encriptación del algoritmo de pago, y

- transmita datos de dicha tarjeta de confianza desde dicho sistema (68, 85) servidor a un terminal, a ser usado para realizar una transacción de pago,

- forme un secreto (SYK2) para una aplicación (106) de pago en el sistema (68, 85) servidor, y

- en respuesta a un inicio (20) de sesión exitoso en dicho sistema (68, 85) servidor, hace que dicho secreto (SYK2) para la aplicación (106) de pago esté disponible para su uso por el terminal para activar dicha tarjeta de confianza para realizar la transacción de pago en el que el secreto (SYK2) para la aplicación de pago tiene un plazo de validez, durante el cual puede usarse de manera autorizada para activar la tarjeta de confianza, y comprendiendo dicha activación el uso de dicho secreto (SYK2) para que la aplicación de pago establezca dicha tarjeta de confianza a un modo en el que dicha tarjeta de confianza puede comunicarse con partes externas además de dicho sistema servidor, caracterizándose el código del programa de ordenador, cuando se ejecuta en dicho al menos un procesador, para hacer que el sistema:

  - reciba datos de pago en dicho sistema (68, 85) servidor desde el terminal del usuario para su verificación, siendo recibidos dichos datos de pago en forma encriptada, encriptados por dicho secreto (SYK2) para dicha aplicación de pago, estando dichos datos de pago relacionados con dicha transacción de pago,

  - para verificar dichos datos de pago en dicho sistema (68, 85) servidor, y

  - hacer que un segundo secreto (SS2), formado por el sistema (68, 85) servidor, esté disponible para su uso por el terminal, si dicha verificación produce un resultado aceptado, estando configurado dicho segundo secreto (SS2) para ser usado en combinación con el secreto (SS1) de un usuario para verificar y realizar la transacción de pago a través de un terminal (67, 81) de punto de venta, y haciendo que dicho segundo secreto (SS2) esté disponible en forma encriptada, encriptado por dicho secreto (SYK2) para dicha solicitud de pago.

11. Sistema según la reivindicación 10, que comprende un código de programa de ordenador que está configurado, cuando se ejecuta en dicho al menos un procesador, para hacer que el sistema:

- forme dicho segundo secreto (SS2) y un secreto del usuario,

- forme un código a partir de dicho secreto (SS1) de usuario y dicho segundo secreto (SS2), y

- configurar una tarjeta de confianza a ser suministrada al terminal del usuario para ser activada con dicho código para realizar una transacción de pago.

12. Producto de programa de ordenador para realizar un pago, comprendiendo el producto de programa de ordenador un código de software almacenado en un medio no volátil legible por ordenador, en el que el código de programa de ordenador, cuando se ejecuta en al menos un procesador, que un dispositivo o un sistema realice el procedimiento según cualquiera de las reivindicaciones 1 a 7.

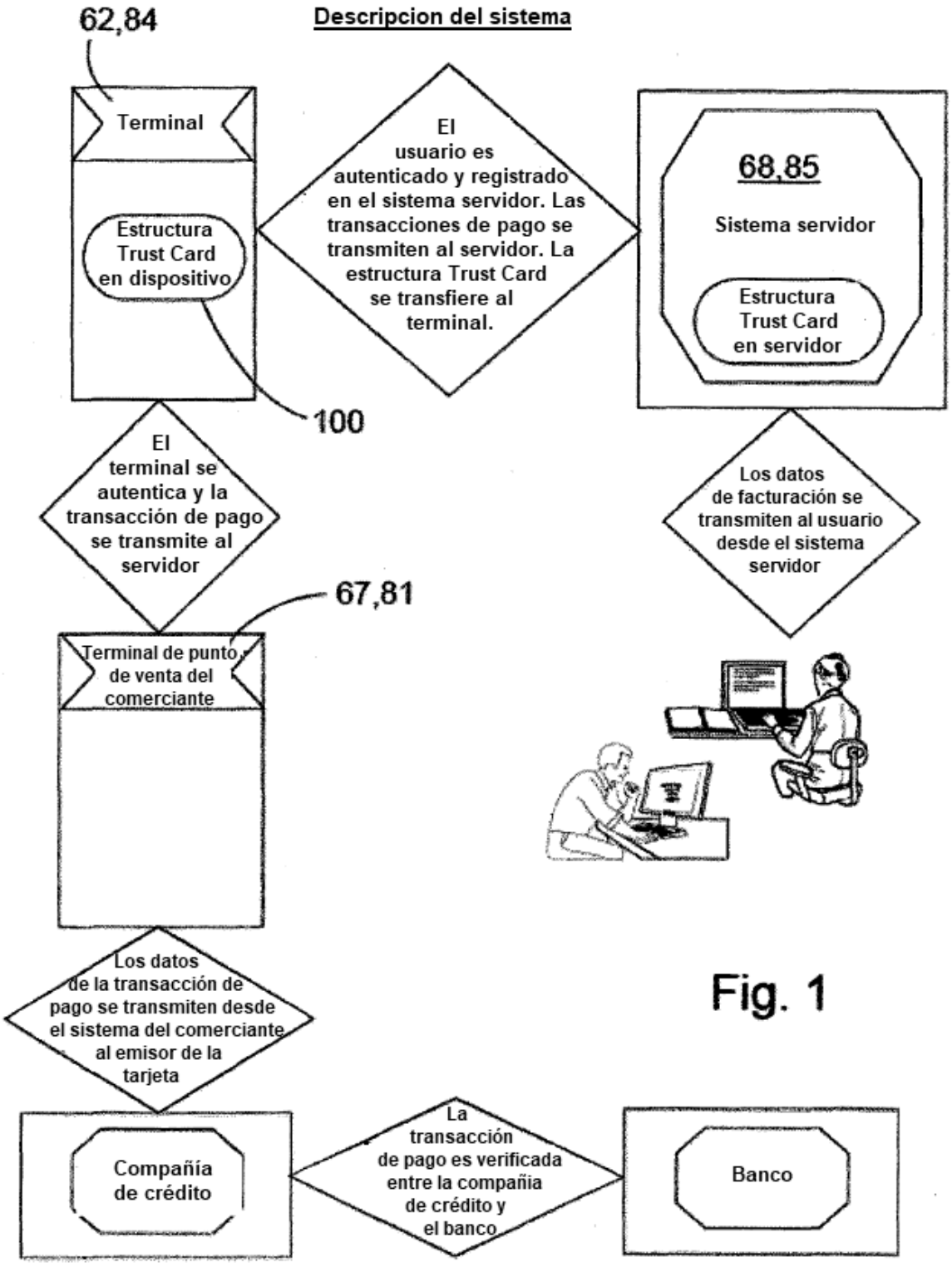
62,84
Descripcion del sistema
Terminal
Estructura Trust Card en dispositivo
100
El usuario es autenticado y registrado en el sistema servidor. Las transacciones de pago se transmiten al servidor. La estructura Trust Card se transfiere al terminal.
68,85
Sistema servidor
Estructura Trust Card en servidor
El terminal se autentica y la transacción de pago se transmite al servidor
Los datos de facturación se transmiten al usuario desde el sistema servidor
67,81
Terminal de punto de venta del comerciante
Los datos de la transacción de pago se transmiten desde el sistema del comerciante al emisor de la tarjeta
Compañía de crédito
La transacción de pago es verificada entre la compañia de crédito y el banco
Banco

Fig. 1

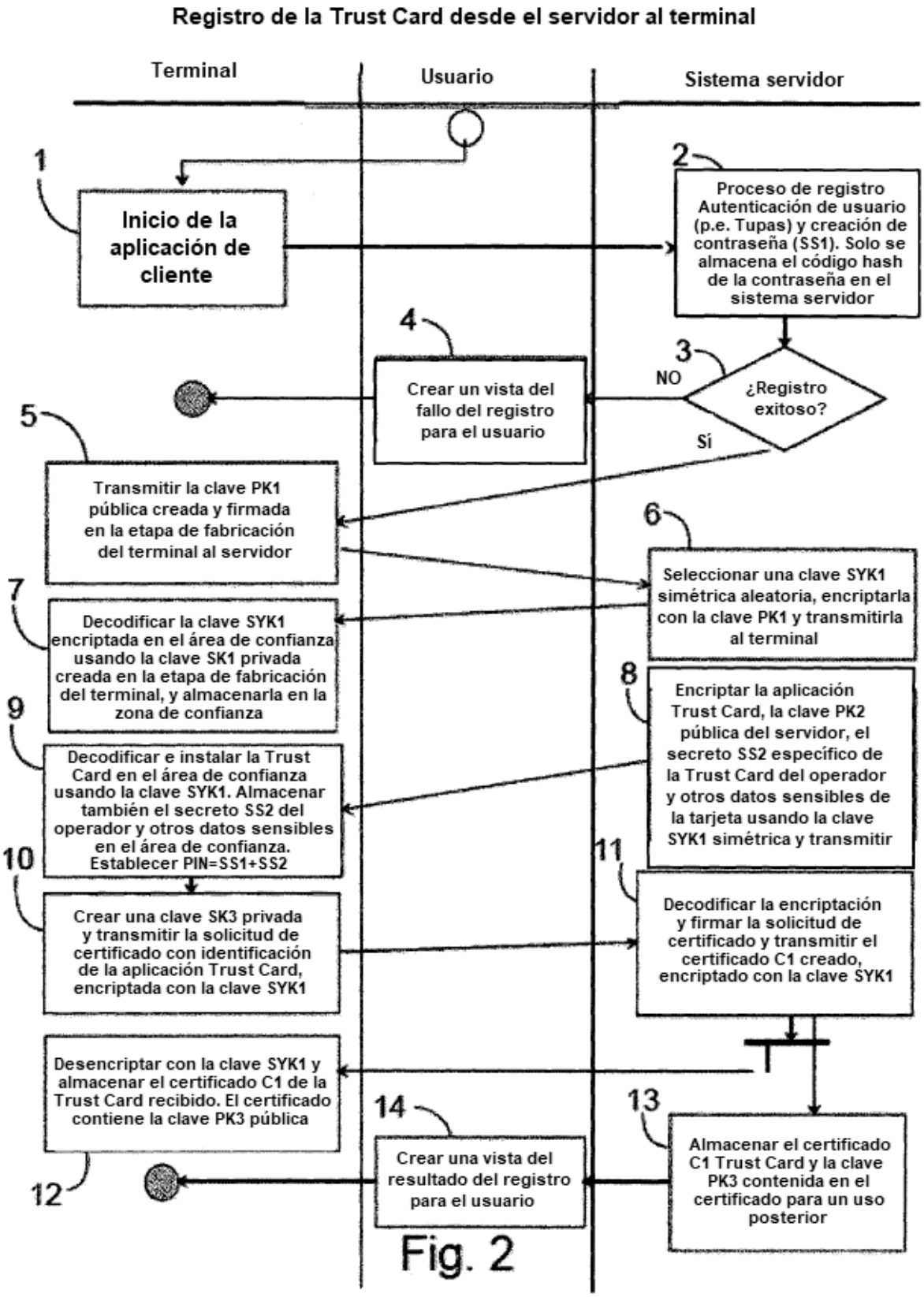
Registro de la Trust Card desde el servidor al terminal
Terminal
Usuario
Sistema servidor
1
Inicio de la aplicación de cliente
2
Proceso de registro Autenticación de usuario (p.e. Tupas) y creación de contraseña (SS1). Solo se almacena el código hash de la contraseña en el sistema servidor
3
¿Registro exitoso?
NO
Sí
4
Crear un vista del fallo del registro para el usuario
5
Transmitir la clave PK1 pública creada y firmada en la etapa de fabricación del terminal al servidor
6
Seleccionar una clave SYK1 simétrica aleatoria, encriptarla con la clave PK1 y transmitirla al terminal
7
Decodificar la clave SYK1 encriptada en el área de confianza usando la clave SK1 privada creada en la etapa de fabricación del terminal, y almacenarla en la zona de confianza
8
Encriptar la aplicación Trust Card, la clave PK2 pública del servidor, el secreto SS2 específico de la Trust Card del operador y otros datos sensibles de la tarjeta usando la clave SYK1 simétrica y transmitir
9
Decodificar e instalar la Trust Card en el área de confianza usando la clave SYK1. Almacenar también el secreto SS2 del operador y otros datos sensibles en el área de confianza. Establecer PIN=SS1+SS2
10
Crear una clave SK3 privada y transmitir la solicitud de certificado con identificación de la aplicación Trust Card, encriptada con la clave SYK1
11
Decodificar la encriptación y firmar la solicitud de certificado y transmitir el certificado C1 creado, encriptado con la clave SYK1
Desencriptar con la clave SYK1 y almacenar el certificado C1 de la Trust Card recibido. El certificado contiene la clave PK3 pública
12
14
Crear una vista del resultado del registro para el usuario
13
Almacenar el certificado C1 Trust Card y la clave PK3 contenida en el certificado para un uso posterior

Fig. 2

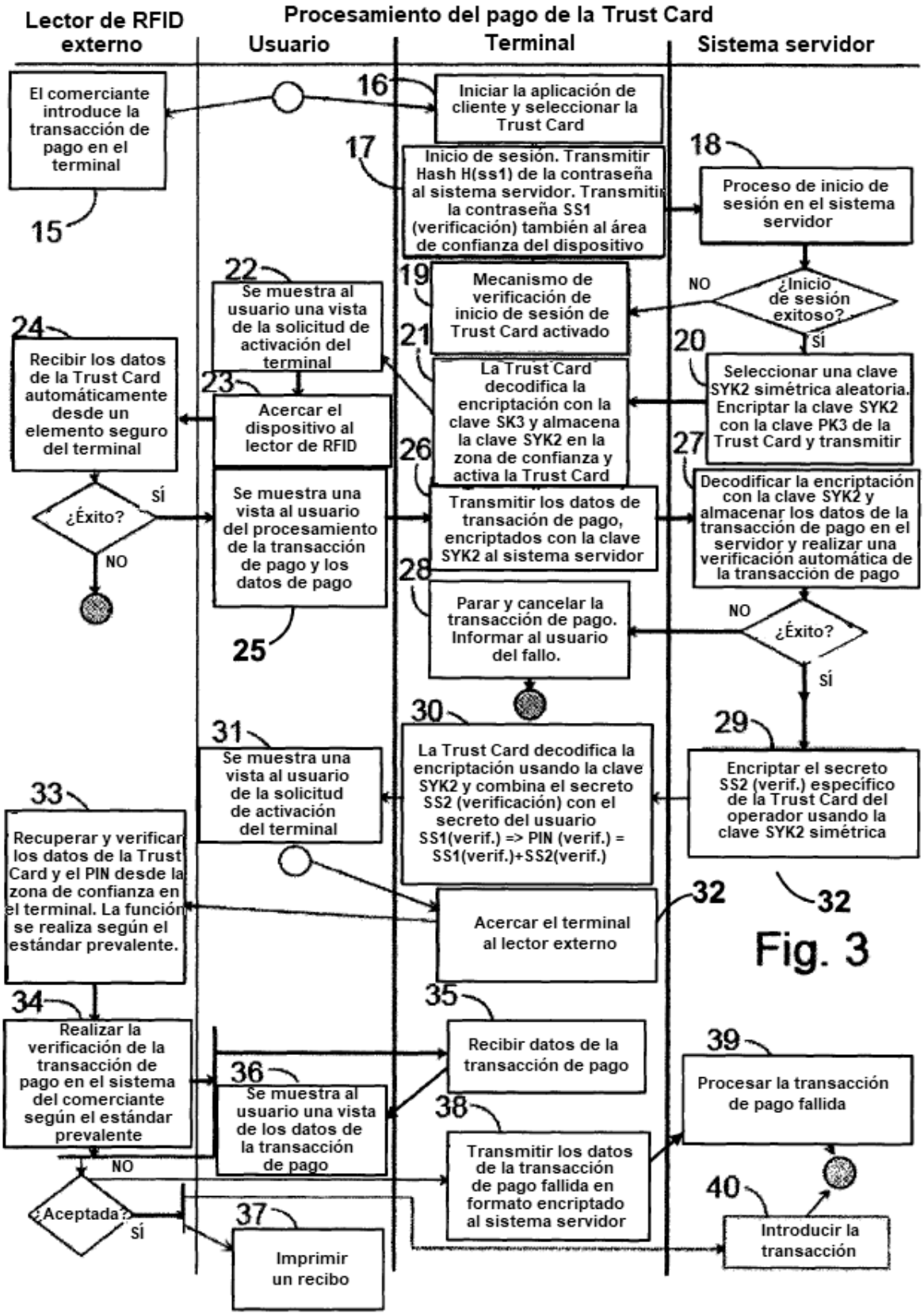
Procesamiento del pago de la Trust Card
Lector de RFID externo
Usuario
Terminal
Sistema servidor
El comerciante introduce la transacción de pago en el terminal
15
16
Iniciar la aplicación de cliente y seleccionar la Trust Card
17
Inicio de sesión. Transmitir Hash H(ss1) de la contraseña al sistema servidor. Transmitir la contraseña SS1 (verificación) también al área de confianza del dispositivo
18
Proceso de inicio de sesión en el sistema servidor
NO
¿Inicio de sesión exitoso?
SÍ
19
Mecanismo de verificación de inicio de sesión de Trust Card activado
20
Seleccionar una clave SYK2 simétrica aleatoria. Encriptar la clave SYK2 con la clave PK3 de la Trust Card y transmitir
21
La Trust Card decodifica la encriptación con la clave SK3 y almacena la clave SYK2 en la zona de confianza y activa la Trust Card
22
Se muestra al usuario una vista de la solicitud de activación del terminal
23
Acercar el dispositivo al lector de RFID
24
Recibir los datos de la Trust Card automáticamente desde un elemento seguro del terminal
¿Éxito?
SÍ
NO
25
Se muestra una vista al usuario del procesamiento de la transacción de pago y los datos de pago
26
Transmitir los datos de transación de pago, encriptados con la clave SYK2 al sistema servidor
27
Decodificar la encriptación con la clave SYK2 y almacenar los datos de la transacción de pago en el servidor y realizar una verificación automática de la transacción de pago
28
Parar y cancelar la transacción de pago. Informar al usuario del fallo.
NO
¿Éxito?
SÍ
29
Encriptar el secreto SS2 (verif.) específico de la Trust Card del operador usando la clave SYK2 simétrica
30
La Trust Card decodifica la encriptación usando la clave SYK2 y combina el secreto SS2 (verificación) con el secreto del usuario SS1(verif.) => PIN (verif.) = SS1(verif.)+SS2(verif.)
31
Se muestra una vista al usuario de la solicitud de activación del terminal
32
Acercar el terminal al lector externo
32
33
Recuperar y verificar los datos de la Trust Card y el PIN desde la zona de confianza en el terminal. La función se realiza según el estándar prevalente.
34
Realizar la verificación de la transacción de pago en el sistema del comerciante según el estándar prevalente
NO
¿Aceptada?
SÍ
35
Recibir datos de la transacción de pago
36
Se muestra al usuario una vista de los datos de la transacción de pago
37
Imprimir un recibo
38
Transmitir los datos de la transacción de pago fallida en formato encriptado al sistema servidor
39
Procesar la transacción de pago fallida
40
Introducir la transacción

Fig. 3

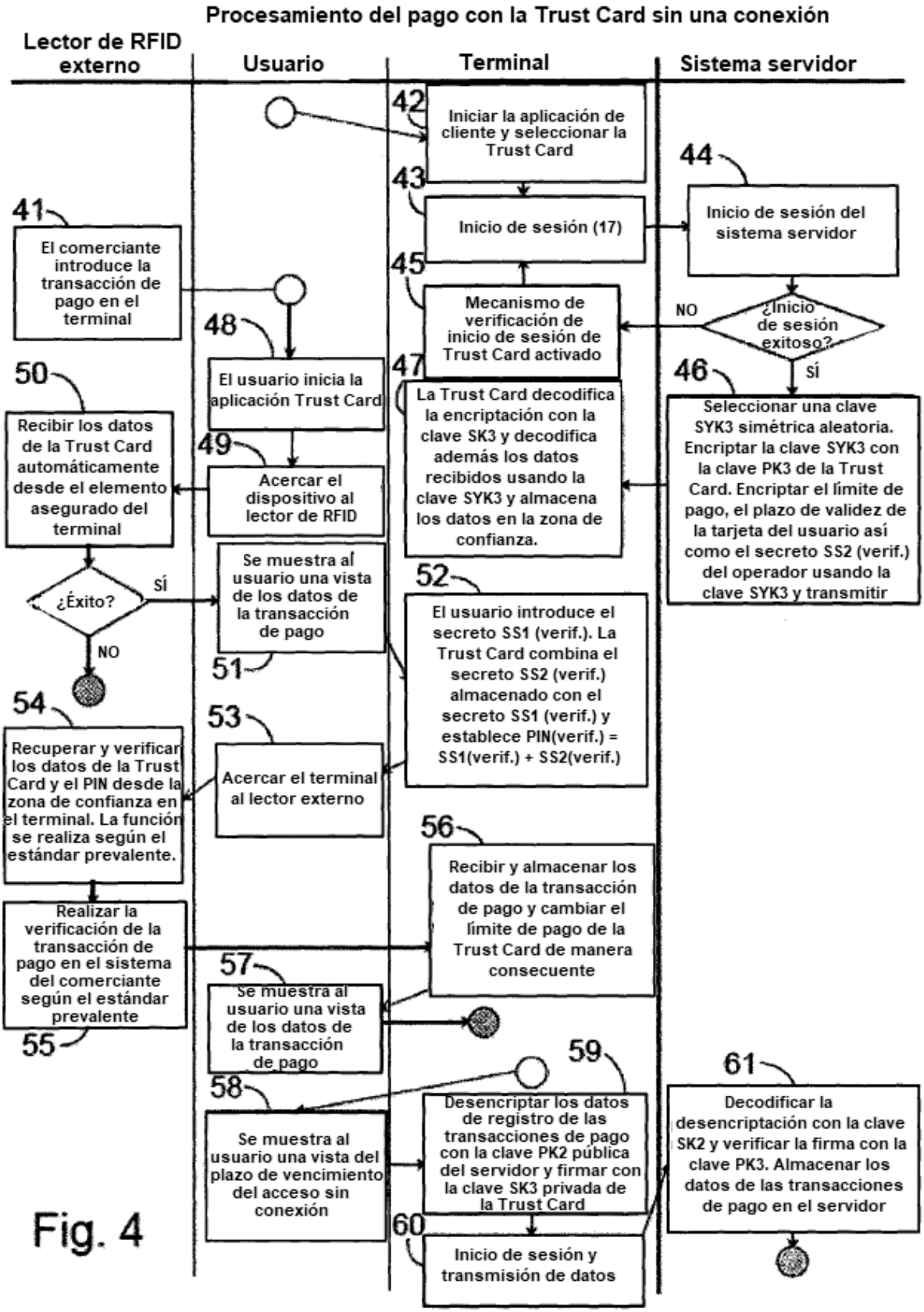
Procesamiento del pago con la Trust Card sin una conexión
Lector de RFID externo
Usuario
Terminal
Sistema servidor
42
Iniciar la aplicación de cliente y seleccionar la Trust Card
44
43
Inicio de sesión (17)
Inicio de sesión del sistema servidor
41
El comerciante introduce la transacción de pago en el terminal
45
Mecanismo de verificación de inicio de sesión de Trust Card activado
NO
¿Inicio de sesión exitoso?
48
47
46
SÍ
50
El usuario inicia la aplicación Trust Card
La Trust Card decodifica la encriptación con la clave SK3 y decodifica además los datos recibidos usando la clave SYK3 y almacena los datos en la zona de confianza.
Seleccionar una clave SYK3 simétrica aleatoria. Encriptar la clave SYK3 con la clave PK3 de la Trust Card. Encriptar el límite de pago, el plazo de validez de la tarjeta del usuario así como el secreto SS2 (verif.) del operador usando la clave SYK3 y transmitir
Recibir los datos de la Trust Card automáticamente desde el elemento asegurado del terminal
49
Acercar el dispositivo al lector de RFID
¿Éxito?
SÍ
Se muestra al usuario una vista de los datos de la transacción de pago
52
El usuario introduce el secreto SS1 (verif.). La Trust Card combina el secreto SS2 (verif.) almacenado con el secreto SS1 (verif.) y establece PIN(verif.) = SS1(verif.) + SS2(verif.)
NO
51
54
53
Recuperar y verificar los datos de la Trust Card y el PIN desde la zona de confianza en el terminal. La función se realiza según el estándar prevalente.
Acercar el terminal al lector externo
56
Recibir y almacenar los datos de la transacción de pago y cambiar el límite de pago de la Trust Card de manera consecuente
Realizar la verificación de la transacción de pago en el sistema del comerciante según el estándar prevalente
57
Se muestra al usuario una vista de los datos de la transacción de pago
55
59
61
58
Se muestra al usuario una vista del plazo de vencimiento del acceso sin conexión
Desencriptar los datos de registro de las transacciones de pago con la clave PK2 pública del servidor y firmar con la clave SK3 privada de la Trust Card
Decodificar la desencriptación con la clave SK2 y verificar la firma con la clave PK3. Almacenar los datos de las transacciones de pago en el servidor
60
Inicio de sesión y transmisión de datos

Fig. 4

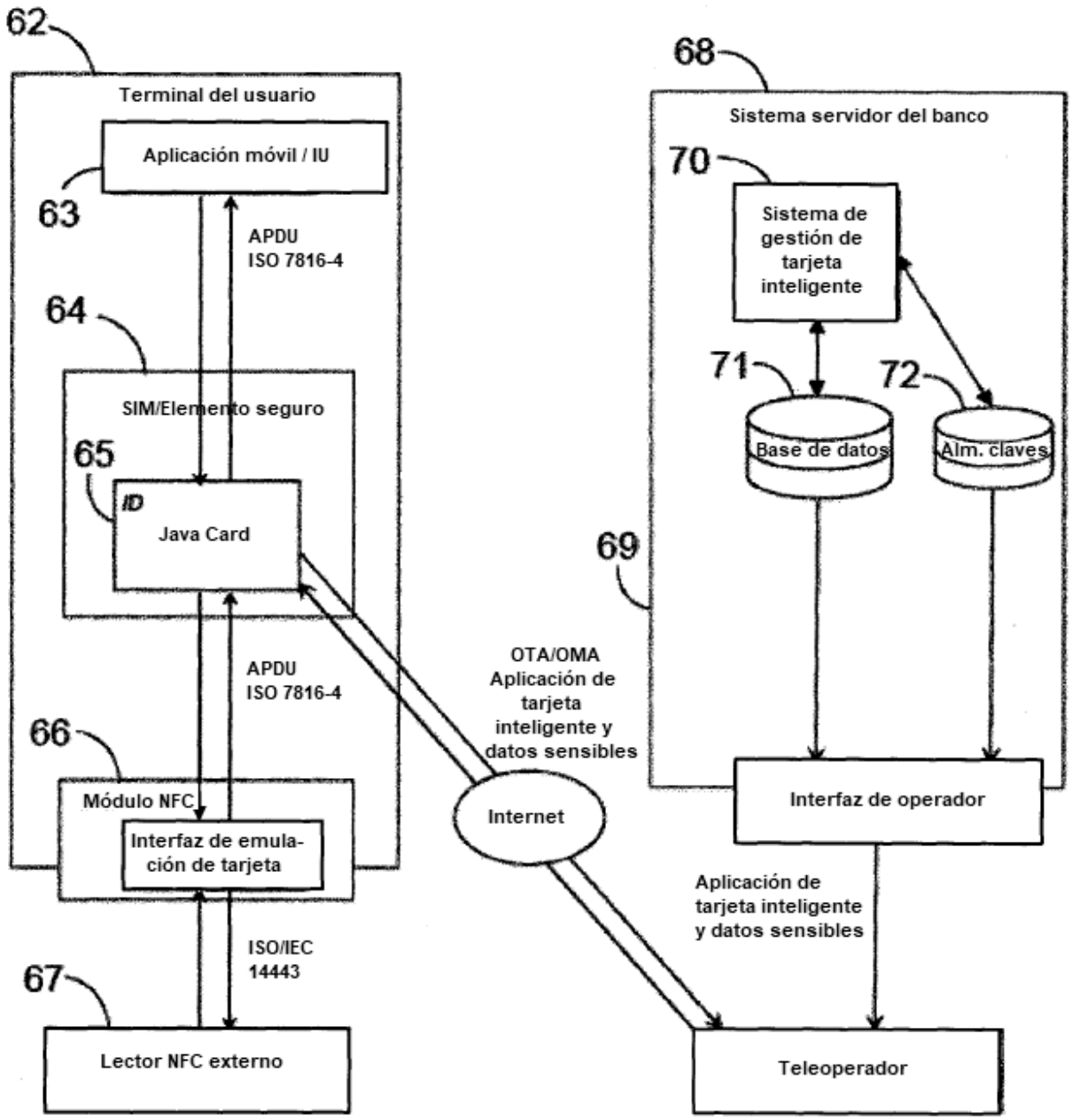
62
Terminal del usuario
Aplicación móvil / IU
63
APDU
ISO 7816-4
64
SIM/Elemento seguro
65
ID
Java Card
APDU
ISO 7816-4
66
Módulo NFC
Interfaz de emula-
ción de tarjeta
ISO/IEC
14443
67
Lector NFC externo
68
Sistema servidor del banco
70
Sistema de
gestión de
tarjeta
inteligente
71
Base de datos
72
Alm. claves
69
OTA/OMA
Aplicación de
tarjeta
inteligente y
datos sensibles
Internet
Interfaz de operador
Aplicación de
tarjeta inteligente
y datos sensibles
Teleoperador

Fig. 5

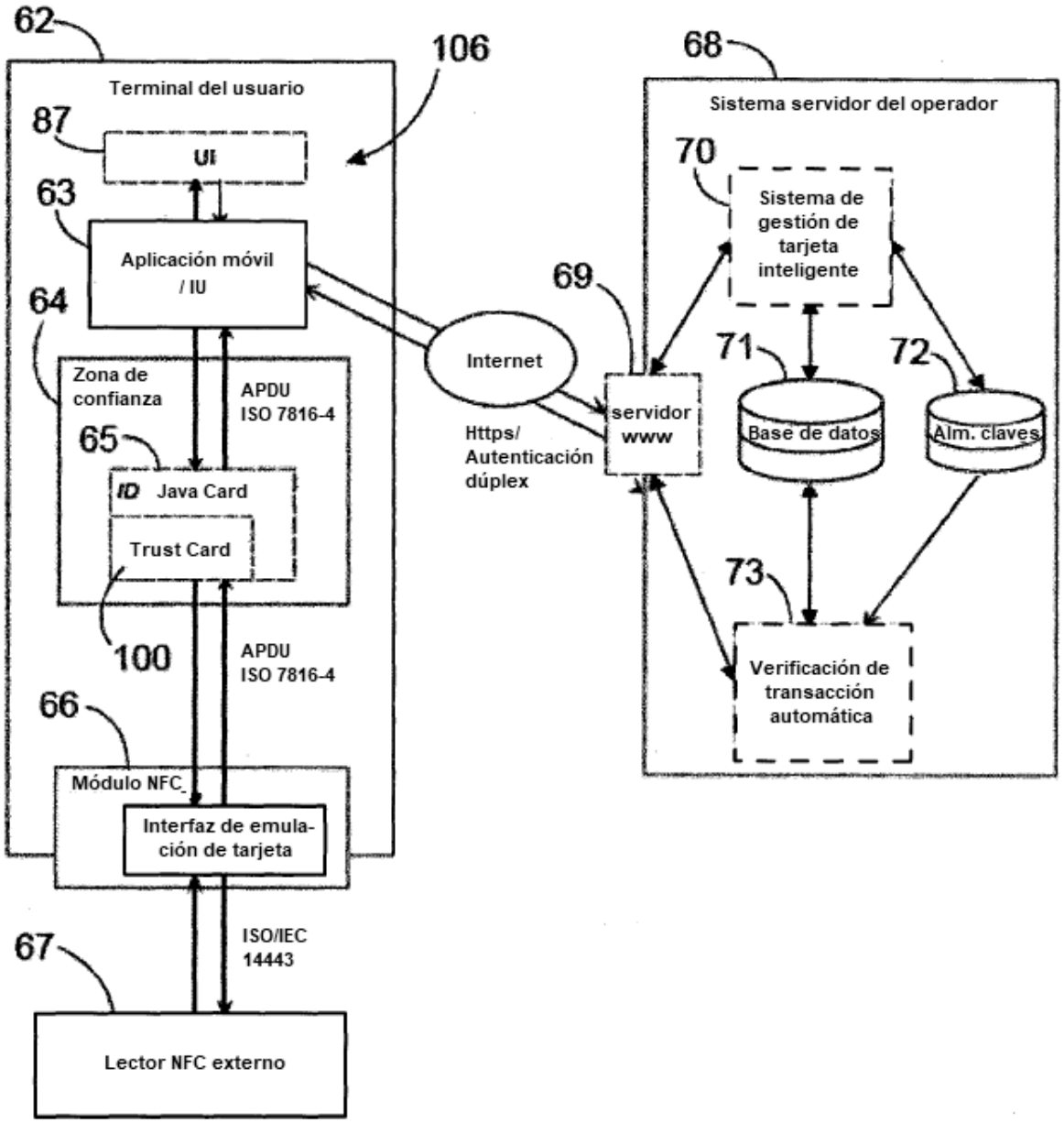
62
Terminal del usuario
106
87
UI
63
Aplicación móvil / IU
64
Zona de confianza
APDU ISO 7816-4
65
ID Java Card
Trust Card
100
APDU ISO 7816-4
66
Módulo NFC
Interfaz de emulación de tarjeta
67
ISO/IEC 14443
Lector NFC externo
Internet
Https/ Autenticación dúplex
68
Sistema servidor del operador
69
servidor www
70
Sistema de gestión de tarjeta inteligente
71
Base de datos
72
Alm. claves
73
Verificación de transacción automática

Fig. 6

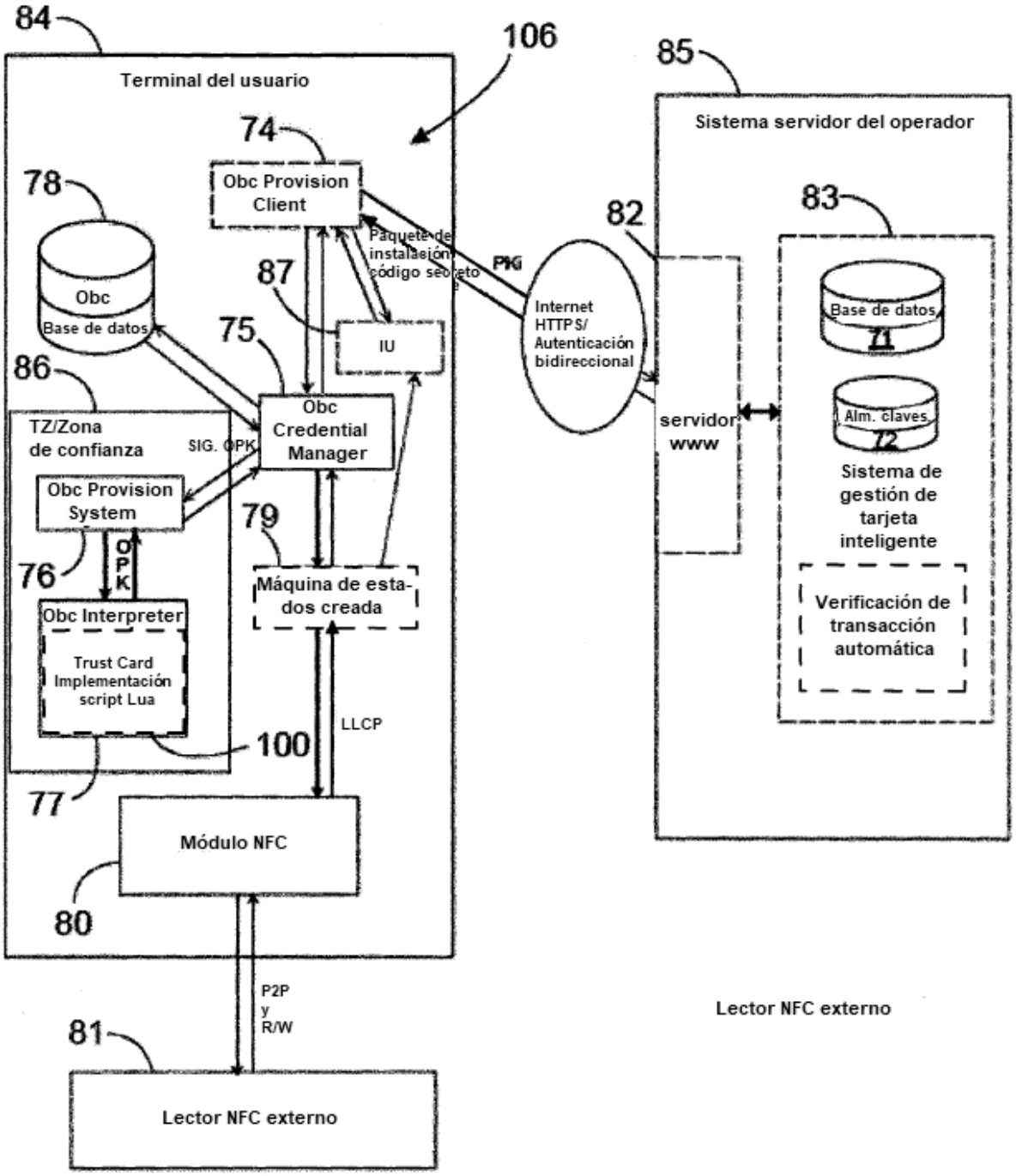
84
Terminal del usuario
106
85
Sistema servidor del operador
74
Obc Provision Client
78
Obc
Base de datos
87
IU
75
Paquete de instalación código secreto
PKG
Internet HTTPS/ Autenticación bidireccional
82
servidor www
83
Base de datos
Z1
Alm. claves
Z2
Sistema de gestión de tarjeta inteligente
Verificación de transacción automática
86
TZ/Zona de confianza
SIG. OPK
Obc Credential Manager
Obc Provision System
OPK
76
79
Máquina de estados creada
Obc Interpreter
Trust Card Implementación script Lua
100
LLCP
77
Módulo NFC
80
P2P y R/W
81
Lector NFC externo
Lector NFC externo

Fig. 7