(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 653 267**

(51) Int. CI.:

H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **15.07.2014 E 14177088 (3)**

(97) Fecha y número de publicación de la concesión europea: **20.09.2017 EP 2840757**

(54) Título: **Administración central individual de tarjetas inteligentes**

(30) Prioridad:

17.07.2013 DE 102013107602

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
06.02.2018

(73) Titular/es:

DEUTSCHE TELEKOM AG (100.0%)
Friedrich-Ebert-Allee 140
53113 Bonn, DE

(72) Inventor/es:

BREUER, JÖRG y
MOOS, RAINER

(74) Agente/Representante:

CARVAJAL Y URQUIJO, Isabel

DESCRIPCIÓN

Administración central individual de tarjetas inteligentes

La invención se refiere a un sistema basado en tarjetas, en especial un sistema basado en tarjetas inteligentes, a un procedimiento para operar tal sistema, a una terminal de comunicaciones relacionada con el cliente y un administrador de tarjetas relacionado con el cliente para usar en tal sistema basado en tarjetas, así como a un programa informático para controlar el procedimiento.

Los sistemas basados en tarjetas como, por ejemplo, sistema de pagos, se conocen desde hace tiempo. A fin de poder utilizar un sistema basado en tarjetas, un cliente necesita una tarjeta apropiada, con preferencia, en forma de una smartcard o tarjeta inteligente, que sirve en especial como soporte de clave para procesos criptográficos para la realización de la autenticidad, la identidad y la confidencialidad. Estas tarjetas se usan entonces mediante los llamados lectores de tarjetas o terminales de tarjetas en la correspondiente aplicación basada en tarjetas o bien el sistema basado en tarjetas.

Las tarjetas inteligentes se usan mayormente cuando se imponen grandes requerimientos de seguridad a un sistema y sus componentes. Los requerimientos pueden ser definidos en este caso por el propio operador del sistema como, por ejemplo, en sistemas de tarjetas de Mastercard y Visa, o también pueden ser regulados por especificaciones legales como, por ejemplo, en el caso de la firma electrónica cualificada (QES). A menudo se deben desarrollar en este caso tarjetas inteligentes de acuerdo con las directivas técnicas correspondientes que son establecidas, por ejemplo, en Alemania por el Bundesamt für Sicherheit in der Informationstechnik (BSI) y se debe comprobar la seguridad necesaria para una evaluación de seguridad o certificación. En este caso, se verifica usualmente a través de un centro independiente, si las tarjetas cumplen con los fines de seguridad requeridos. Recién cuando se confirman la certificación de seguridad y la conformidad con la directiva técnica, se pueden usar estas tarjetas en el correspondiente sistema.

Del documento EP 1 349 032 B1, se conoce un sistema de red que permite una autentificación segura de los usuarios. El sistema de red presenta una infraestructura de clientes a la que pertenecen una computadora del cliente, un lector de tarjetas y una tarjeta inteligente. El lector de tarjetas proporciona el acceso a la tarjeta inteligente y está conectada mediante un USB-bus o una conexión inalámbrica de acuerdo con el estándar Bluetooth con la computadora del cliente. Además, la red presenta una infraestructura de servidor con un servidor de aplicación. Se puede establecer un canal encriptado entre la infraestructura del cliente y la infraestructura del servidor a través de una primera red. Además, puede haber una conexión autentificada entre la infraestructura del cliente y el servidor de aplicación.

Del documento US 2010 / 0 082 487 A1, se conoce un procedimiento para administrar tarjetas virtuales en un motor de tarjetas virtual ligado con un administrador de tarjetas virtual. Las tarjetas denominadas "tarjetas virtuales", emitidas y administradas electrónicamente, se desarrollaron debido a problemas con las tarjetas de plástico. La administración atañe a tarjetas de regalo, tarjetas de clientes, tarjetas de membresía o tarjetas de fidelización. El procedimiento comprende: determinar una distancia entre una computadora móvil y un punto de venta del comerciante, en donde el punto de venta del comerciante está asociado con un prestador de servicios de tarjetas y una de las tarjetas virtuales; obtener selectivamente las tarjetas virtuales en un display de la computadora móvil a base de la distancia; y activar selectivamente una transacción con tarjeta virtual entre la tarjeta virtual y el proveedor de servicios de tarjeta en base a la distancia.

Del documento US 2008 / 0 082 442 A1, se conoce un procedimiento para administrar tarjetas de crédito mediante una terminal de comunicaciones. El procedimiento comprende: ingresar los datos de la tarjeta de crédito en la terminal de comunicaciones mediante teclas y, en caso de que se solicite una función relacionada con la tarjeta de crédito, realizar la función. La función comprende: transmitir los datos de la tarjeta de crédito a una PC, conectar con un centro de seguridad de tarjetas para solucionar un problema respecto de una tarjeta de crédito, y conectar con una página de inicio de una empresa de tarjetas de crédito para buscar informaciones de uso de la tarjeta de crédito.

Si miramos actualmente dentro de nuestra billetera, se comprueba que allí no hay sólo una smartcard o tarjeta inteligente, sino que mayormente se guardan muchas tarjetas diferentes para las más diversas aplicaciones a base de tarjetas. Pueden ser tarjetas de bonus, tarjetas de clientes, tarjetas de membresía, tarjetas de empresas, pasaportes, tarjetas de acceso a edificios o tarjetas con altos requisitos de seguridad, como, por ejemplo, tarjetas de pago de distintas instituciones financieras, una tarjeta para la firma electrónica cualificada y muchas más. Se dificulta la utilización de tal cantidad de tarjetas más aún porque en la mayoría de los casos, cada tarjeta está protegida por un PIN individual que debe ser retenido por un cliente.

Ahora, la invención tiene por objeto poner a disposición un sistema basado en tarjetas, un procedimiento para operar tal sistema, así como un programa de computadora, que facilita al usuario de varias tarjetas diferentes su

manipulación y uso, permite el uso de nuevas tarjetas de modo rápido y simple, sin tener que prescindir de la seguridad de las tarjetas y sin perjudicar los requerimientos de seguridad en un sistema basado en tarjetas.

Una idea central de la invención consiste hacer útil en la actualidad o a futuro tarjetas inteligentes disponibles en el mercado, en especial certificadas a través de un administrador de tarjetas privado o relacionado con el cliente de cualquier terminal relacionado con el cliente, en el que está instalada una aplicación de acceso con tarjeta preferentemente en forma de una aplicación, para las correspondientes aplicaciones a base de tarjetas.

Otro aspecto consiste en que, gracias a la invención, se pueden mantener los altos requerimientos de seguridad y las certificaciones ligadas con ello de las correspondientes tarjetas inteligentes o aplicaciones a base de tartejas inteligentes.

El objeto técnico arriba mencionado se resuelve por medio de los pasos de procedimiento de la reivindicación 1.

Según ello, se prevé un procedimiento para operar un sistema basado en tarjetas, que presenta una terminal de comunicaciones relacionada con el cliente y un administrador de tarjeta separado relacionado con el cliente, en donde está instalada al menos una tarjeta relacionada con el cliente, en especial una tarjeta inteligente.

A fin de poder utilizar al menos una tarjeta relacionada con el cliente de manera segura, se establece una conexión segura entre la terminal de comunicaciones del cliente y su administrador de tarjetas. A fin de asegurar que el cliente o bien la terminal de comunicaciones se pueden comunicar efectivamente con una tarjeta instalada en el administrador de tarjetas, se ejecuta una autentificación entre la terminal de comunicaciones y el administrador de tarjetas. Para ello, se puede usar conocidos procedimientos de autentificación o también procedimientos de autentificación especialmente desarrollados.

En el terminal de comunicación, el cliente selecciona una tarjeta relacionada con el cliente instalada en el administrador de tarjetas. Ahora se puede iniciar o ejecutar una aplicación a base de tarjetas, que se puede comunicar través de la terminal de comunicaciones y la conexión segura con tarjeta relacionada con el cliente seleccionada, instalada en el administrador de tarjetas.

Gracias a la invención, ahora ya no es necesario que un cliente deba llevar consigo todas sus tarjetas que también pueden estar certificadas. En consecuencia, también se reduce claramente el peligro de que un cliente pueda perder sus tarjetas. Con preferencia, el administrador de tarjetas se instala en la vivienda del cliente.

Se observa en este punto que el término tarjeta comprende todos los módulos de hardware, en especial smartcards y tarjetas inteligentes, pero también tarjetas de banda magnética, que son apropiadas en especial como soportes de clave para procesos criptográficos para la realización de autenticidad, identidad y confidencialidad.

Además, se observa que las tarjetas usadas en el administrador de tarjetas son inalterables, es decir, se usan en la forma en que se emplean caso contrario de modo convencional. Por este motivo, se pueden conservar los altos requerimientos de seguridad y las certificaciones ligadas con ello de las correspondientes tarjetas inteligentes o aplicaciones basadas en tarjetas inteligentes incluso con el uso del administrador de tarjetas.

Si las tarjetas relacionadas con el cliente están protegidas, como es usual, mediante un código de identificación individual, por ejemplo, en forma de un pin o de una contraseña, se puede facilitar el acceso dirigido para el cliente en la tarjeta instalada en el administrador de tarjetas asignando al administrador de tarjetas un código de identificación individual de nivel superior, preferentemente en forma de un pin o de una contraseña, almacenar los códigos de identificación individuales de las tarjetas relacionadas con el cliente instaladas en el administrador de tarjetas, en donde, preferentemente a pedido del cliente, se puede ingresar en la terminal de comunicaciones el código de identificación individual de nivel superior del administrador de tarjetas y luego transmitirlo al administrador de tarjetas que puede llevar a la tarjeta seleccionada el código de identificación individual asignado.

En consecuencia, el cliente sólo tiene que retener el código de identificación individual asignado a administrador de tarjetas y ya no más el código de identificación individual de las tarjetas instaladas. De esta forma, se pueden evitar en especial los datos erróneos que llevan en el peor de los casos a bloquear las tarjetas.

Para que el cliente sepa qué tarjetas están instaladas actualmente en su administrador de tarjetas, se pueden visualizar las tarjetas relacionadas con el cliente instaladas en el administrador de tarjetas en la terminal de comunicaciones de una manera predeterminada, con preferencia, mediante la conexión segura.

Los símbolos de las tarjetas o los diseñaos de las tarjetas de las tarjetas instaladas se pueden visualizar en el terminal de comunicación, por ejemplo, en forma automática. Es concebible que el administrador de tarjetas reconozca automáticamente qué tarjetas están instaladas. Luego transfiere los símbolos o los diseños de las tarjetas almacenados en las tarjetas instaladas al terminal de comunicación. Alternativamente, es concebible que

únicamente se transfieran los códigos correspondientes, que identifican las tarjetas instaladas, por el administrador de tarjetas al terminal de comunicación, que luego consulta los símbolos o diseños de las tarjetas ya almacenados previamente para las distintas tarjetas en respuesta a los códigos recibidos y los muestra al cliente.

A fin de seguir protegiendo al procedimiento contra un mal uso de la tarjeta, se puede explorar previamente al menos un área predeterminada de cada una de las tarjetas relacionadas con el cliente instaladas en el administrador de tarjetas y verificar la autenticidad de la correspondiente tarjeta explorada por el administrador de tarjetas mediante el área explorada. El administrador de tarjetas activa luego preferentemente sólo aquellas tarjetas cuya autenticidad fue verificada y confirmada.

De acuerdo con una forma de realización preferida, en la terminal de comunicaciones se almacena una aplicación a base de tarjetas, de modo que se ejecuta el paso de la ejecución de una aplicación basada en tarjetas en el terminal de comunicación.

De acuerdo con otra forma de realización preferida, la terminal de comunicaciones relacionada con el cliente está configurado como terminal de comunicación móvil. Una terminal de comunicaciones móvil de este tipo puede ser un teléfono inteligente (smartphone), un PDA o cualquier otro terminal de comunicación móvil. En este caso, el sistema basado en tarjetas presenta al menos un dispositivo de lectura de tarjetas, que pertenece al proveedor de una aplicación a base de tarjetas o al operador del sistema basado en tarjetas. En esta forma de realización, se ejecuta una aplicación a base de tarjetas en el dispositivo de lectura de tarjetas o en otro dispositivo ligado con el dispositivo de lectura de tarjetas del proveedor o del operador.

A fin de poder garantizar las seguridades requeridas del sistema basado en tarjetas utilizado, se pueden instalar tarjetas certificadas en el administrador de tarjetas. Los procedimientos para la certificación de tarjetas inteligentes se conocen desde hace tiempo.

A fin de seguir aumentando la seguridad del procedimiento y con ello del sistema basado en tarjetas, también se puede certificar este sistema incluyendo la conexión segura, que se establece entre la terminal de comunicaciones y el administrador de tarjetas.

En el caso de una conexión segura, se trata preferentemente de una conexión segura con Internet.

Una conexión segura se puede establecer, por ejemplo, usando el protocolo Transport-Layer-Security (TLS) del administrador de tarjetas al terminal de comunicación. En este caso, la terminal de comunicaciones solicita al administrador de tarjetas a través de un despertador para establecer una conexión con él. Se describe un procedimiento similar en TR3109-1 de BSI para el Smart Meter Gateway.

El problema técnico antes mencionado se soluciona asimismo mediante las características de la reivindicación 8.

De acuerdo con ello, se prevé un sistema basado en tarjetas, en especial un sistema basado en tarjetas inteligentes, que presenta una terminal de comunicaciones asignado a un usuario. En la terminal de comunicaciones está instalada una aplicación de acceso con tarjeta, preferentemente en forma de una aplicación. La terminal de comunicaciones presenta una primera unidad de control programable y un dispositivo de acceso a la red, en especial un dispositivo de acceso a Internet. Además, el sistema basado en tarjetas comprende un administrador de tarjetas asignado al usuario, que se instala y se opera por separado del terminal de comunicación. El administrador de tarjetas contiene varios lectores de tarjetas sin contacto y/o con contacto, que están diseñados en cada caso para aceptar y leer una tarjeta relacionada con el usuario, en especial una tarjeta inteligente. En el caso del lector de tarjetas, se trata preferentemente de los lectores de tarjetas convencionales.

Además, el administrador de tarjetas presenta un segundo dispositivo de control programable, un dispositivo de seguridad, que sirve en especial para la individualización del administrador de tarjetas, y un dispositivo de acceso a la red, en especial un dispositivo de acceso a la Internet. El dispositivo de seguridad del administrador de tarjetas y la aplicación de acceso a las tarjetas de la terminal de comunicaciones están diseñados para realizar una autentificación entre la terminal de comunicaciones y el administrador de tarjetas.

El establecimiento de una conexión segura entre el administrador de tarjetas y el terminal de comunicación, así como una autentificación pueden ser de la siguiente manera:

La terminal de comunicaciones solicita al administrador de tarjetas a través de un despertador establecer un canal TLS con él.

El administrador de tarjetas verifica si la terminal de comunicaciones está registrada como terminal segura en el administrador de tarjetas.

El dispositivo de seguridad del administrador de tarjetas asume las siguientes tareas:

- generación de números aleatorios para el comando de TLS "ClientHello".
- negociación de claves del pre-master secret de TLS según Elliptic Curve Diffie-Hellman.
- generación y verificación de firmas para la autentificación.

La terminal de comunicaciones es responsable de la generación del master secret y para ello debe utilizar el pre-master secret negociado.

El dispositivo de seguridad también está configurado para controlar el establecimiento de una conexión segura del administrador de tarjetas con el terminal de comunicación. La aplicación de acceso con tarjeta está diseñado para seleccionar en especial mediante el primer dispositivo de control programable una tarjeta relacionada con el usuario instalada en el administrador de tarjetas y controlar la comunicación entre una aplicación a base de tarjeta y la tarjeta relacionada con el usuario seleccionada a través de una conexión segura establecida.

Se ha de notar que en el caso del dispositivo de seguridad, se puede tratar, por ejemplo, de un módulo de seguridad en forma de una tarjeta inteligente.

A fin de facilitarle al usuario la manipulación y el uso de varias tarjetas protegidas por un código de identificación y para evitar que tenga que memorizar todos estos códigos de identificación, está almacenado en el dispositivo de seguridad del administrador de tarjetas un código de identificación individual de nivel superior para la individualización del administrador de tarjetas. Los códigos de identificación individuales de las tarjetas están almacenados preferentemente en una memoria segura, por ejemplo, en el módulo de seguridad del administrador de tarjetas. La aplicación de acceso con tarjeta de la terminal de comunicaciones puede diseñarse para solicitar al usuario que ingrese el código de identificación de nivel superior del dispositivo de seguridad. El administrador de tarjetas está configurado para que, en respuesta al código de identificación de nivel superior recibido por el terminal de comunicación, lea el código de identificación individual de la tarjeta seleccionada de la memoria y lo transfiera a la tarjeta relacionada con el usuario seleccionada, a fin de autorizar el acceso a la tarjeta protegida con PIN o contraseña.

A fin de facilitarle al cliente la instalación y la consulta de sus tarjetas en el administrador de tarjetas, el administrador de tarjetas se puede configurar para identificar automáticamente una tarjeta relacionada con el usuario en un lector de tarjetas y generar automáticamente una asignación entre la tarjeta identificada y el correspondiente lector de tarjetas. De este modo, el administrador de tarjetas halla el lector de tarjetas, en el que está introducido una tarjeta seleccionada.

La seguridad al usar tarjetas relacionadas con el usuario se puede incrementar cuando el administrador de tarjetas presenta un escáner de tarjetas, que está diseñado para explorar al menos un área predeterminada de una tarjeta relacionada con el usuario por instalar. El dispositivo de seguridad del administrador de tarjetas está diseñado para verificar y confirmar, en respuesta a la al menos un área explorada, la autenticidad de la tarjeta por instalar y/o firmar el área explorada con una identidad digital.

De acuerdo con una forma de realización ventajosa, se instala una aplicación a base de tarjetas en el terminal de comunicación.

En otra forma de realización ventajosa, la terminal de comunicaciones relacionada con el usuario está configurada como terminal de comunicaciones móvil que presenta al menos una interfaz de comunicación de corto alcance inalámbrica. En el caso de la interfaz de comunicación de corto alcance inalámbrica, se puede tratar de una interfaz de comunicación según el estándar NFC (near field communication) o el estándar Bluetooth. Además, se prevé al menos un dispositivo de lectura de tarjetas asignado a un proveedor de una aplicación a base de tarjetas o el operador de un sistema basado en tarjetas, por ejemplo, de una institución crediticia. El dispositivo de lectura de tarjetas puede contener un lector de tarjetas o una terminal de tarjetas convencional.

El dispositivo de lectura de tarjetas del proveedor presenta al menos una interfaz de comunicación de corto alcance inalámbrica y/o una interfaz de comunicación con contacto, a la que se puede conectar un adaptador con una interfaz de comunicación de corto alcance inalámbrica.

El dispositivo de lectura de tarjetas está configurado para comunicarse con la al menos una interfaz de comunicación de corto alcance inalámbrica del terminal de comunicación. Además, el dispositivo de lectura de tarjetas está configurado para realizar una aplicación a base de tarjetas. La aplicación de acceso con tarjeta dd móvil está configurado para controlar mediante el primer dispositivo de control programable una comunicación entre la

aplicación a base de tarjetas ejecutada por el dispositivo de lectura de tarjetas y una tarjeta seleccionada en el administrador de tarjetas.

La seguridad al usar las tarjetas instaladas en el administrador de tarjetas se puede aumentar porque el dispositivo de seguridad del administrador de tarjetas está configurado para controlar el establecimiento de una conexión segura y eventualmente certificada, en especial una conexión con Internet con el terminal de comunicación.

El problema técnico antes mencionado se soluciona asimismo mediante una terminal de comunicaciones según la reivindicación 15, que está configurado para usar en un sistema basado en tarjetas.

Además, el problema técnico arriba mencionado se soluciona mediante un administrador de tarjetas según la reivindicación 16, que está configurado para usar en tal sistema basado en tarjetas.

El problema técnico antes mencionado se soluciona además mediante un programa informático de acuerdo con la reivindicación 17, que contiene múltiples instrucciones que son almacenables en una terminal de comunicaciones relacionada con un usuario y en un administrador de tarjetas relacionado con un usuario de un sistema basado en tarjetas, en donde las instrucciones, cuando son leídas y procesadas por un dispositivo de control programable de la terminal de comunicaciones y un dispositivo de control programable del administrador de tarjetas, ejecutan el procedimiento para operar un sistema basado en tarjetas.

La invención se explica con mayor detalle a continuación mediante dos ejemplos de realización en relación con los dibujos. Se muestran:

Fig. 1

un sistema basado en tarjetas ejemplificativo con un teléfono inteligente,

Fig. 2

un sistema basado en tarjetas alternativo con una terminal fija.

La Figura 1 muestra un sistema basado en tarjetas 1 de ejemplo que en el ejemplo descrito más abajo, es un sistema de pago a base de una tarjeta inteligente de un centro de compras. El operador del centro de compras ha implementado, por ejemplo, un dispositivo de lectura de tarjetas 10, que presenta un lector de tarjetas 20 sin contacto. En el lector de tarjetas 20 sin contacto, se pueden instalar, por ejemplo, dos interfaces de comunicación de corto alcance inalámbrica, por ejemplo, una interfaz 21 según el estándar NFC y otra interfaz de comunicación 22 según el estándar Bluetooth. Otro dispositivo de lectura de tarjetas 15 puede estar emplazado en el centro de compras, que presenta un lector de tarjetas 30 con una interfaz con contacto 31. Para que el lector de tarjetas 30 con contacto se pueda comunicar inalámbricamente con equipos que presentan una interfaz de comunicación de corto alcance, a la interfaz con contacto 31 del lector de tarjetas 30 se puede conectar un adaptador 40, que presenta una interfaz con contacto 43 para unirse con el lector de tarjetas 30 con contacto. Además, está implementada en el adaptador 40 al menos una interfaz de comunicación de corto alcance inalámbrica. En el presente ejemplo, el adaptador 40 contiene tanto una interfaz de comunicación de corto alcance 42 según el estándar NFC como también otro interfaz de comunicación de corto alcance 41 según el estándar Bluetooth.

El sistema basado en tarjetas 1 comprende, además, al menos una terminal de comunicaciones móvil 50 que sirve para Internet, que en el presente ejemplo es un teléfono inteligente. Este teléfono inteligente 50 pertenece a un usuario. Además de las funcionalidades usuales y los componentes tales como, por ejemplo, una tarjeta SIM, el teléfono inteligente 50 presenta al menos una interfaz de comunicación de corto alcance inalámbrica. En el presente ejemplo, se implementan tanto una interfaz de comunicación de corto alcance NFC 51 como también una interfaz de comunicación de corto alcance Bluetooth 52. La operación del teléfono inteligente 50 se supervisa y controla por un dispositivo de control programable 53, que puede estar diseñado como microprocesador o microcontrolador. Además, se prevé una memoria 60 en la que se almacenan un software de comunicación y control que se designa aplicación de acceso con tarjeta 61. La aplicación de acceso con tarjeta 61 se programa preferentemente como aplicación. Esta aplicación también se puede designar como aplicación privada de tarjeta inteligente. En la memoria 60 se pueden almacenar, además, símbolos, diseños de tarjetas u otras identificaciones de distintas tarjetas, que pertenecen al cliente del teléfono inteligente 50. Además, el teléfono inteligente 50 dispone de un dispositivo de acceso a la red, que está configurado en el presente ejemplo como dispositivo de acceso a la Internet 54.

Además, el sistema basado en tarjetas 1 comprende un administrador de tarjetas 70, que más abajo se denominará administrador de tarjetas inteligentes 70. Porque a continuación se parte de la base de que en el caso de las tarjetas relacionadas con el cliente se trata de distintas tarjetas inteligentes.

El administrador de tarjetas inteligentes 70 se asigna asimismo al cliente del teléfono inteligente 50, y preferentemente se instala en sus ambientes privados. El administrador de tarjetas inteligentes 70 está dispuesto preferentemente en una carcasa que no está representada. El administrador de tarjetas inteligentes 70 puede presentar varios lectores de tarjetas 1 a n, de los cuales, con fines de simplicidad, únicamente están representados los dos lectores de tarjetas 75 y 76. En el caso de los lectores de tarjetas 75 y 76, se puede tratar de lectores de tarjetas sin contacto y/o con contacto convencionales. Los lectores de tarjetas 75 y 76 están configurados en cada caso para alojar un módulo de hardware, en el presente ejemplo una tarjeta inteligente 90 ó 91 y para comunicarse con el chip de la correspondiente tarjeta inteligente.

El administrador de tarjetas inteligentes 70 presenta, además, un dispositivo de seguridad 80, que puede estar configurado como módulo de seguridad empleable. Como se explicará a continuación con mayor detalle, el dispositivo de seguridad 80 se puede configurar en especial para que individualice el administrador de tarjetas 70 para realizar una autentificación con el teléfono inteligente 50 así como establecer una conexión segura con el teléfono inteligente 50. Para ello, el administrador de tarjetas inteligentes 70 presenta asimismo un dispositivo de acceso a la red 73 que está configurado en el presente ejemplo, a su vez, como dispositivo de acceso a la Internet.

El dispositivo de seguridad 80 está diseñado preferentemente para establecer o introducir una conexión segura con la Internet entre el administrador de tarjetas inteligentes 70 y el teléfono inteligente 50, a fin de realizar una comunicación entre la aplicación de acceso con tarjeta 61 del teléfono inteligente 50 y el dispositivo de seguridad 80, así como, entre otras, una comunicación entre la aplicación de acceso con tarjeta 61 y una tarjeta inteligente 90 y 91 instalada en el administrador de tarjetas 70.

El dispositivo de seguridad 80 puede presentar una memoria 81 en la que puede almacenarse un código de identificación de tarjeta individual de nivel superior, por ejemplo, en forma de un PIN o de una contraseña.

Además, el administrador de tarjetas inteligentes 70 puede presentar un escáner de tarjetas inteligentes 72 que está configurado para explorar el diseño del anverso y/o reverso de una tarjeta relacionada con el usuario por instalar. El dispositivo de seguridad 80 puede estar configurado para firmar el diseño explorado del anverso y/o reverso de una tarjeta inteligente instalada con una firma digital del administrador de tarjetas. Para ello, el dispositivo de seguridad 80 puede utilizar una identidad digital asignada al administrador de tarjetas, que está compuesta por una clave secreta, una clave pública y un certificado. La autenticidad de la tarjeta instalada se puede confirmar, por ejemplo, mediante una marca de agua verificable electrónicamente en el diseño del anverso de la tarjeta y/o el reverso de la tarjeta.

Las funciones del administrador de tarjetas inteligentes 70 son controladas y supervisadas por un dispositivo de control programable 74, que puede estar configurado como microprocesador o como microcontrolador.

Como cada tarjeta inteligente 90, 91 por instalar se puede asegurar mediante un código de identificación, que está configurado como PIN o contraseña, se puede prever una memoria 77 segura en la que se puede almacenar el código de identificación individual de una tarjeta inteligente después de su instalación.

Cabe señalar que en la memoria 77 también se puede almacenar una tabla de asignación que asigna un lector de tarjetas a cada tarjeta inteligente instalada. Esta asignación se puede realizar automáticamente bajo el control del microcontrolador 74 y/o el dispositivo de seguridad 80 del administrador de tarjetas inteligentes 70.

El administrador de tarjetas inteligentes 70 también se puede configurar para desactivar, según la implementación, determinadas o todas las tarjetas inteligentes 90, 91 instaladas. Este objeto puede ser realizado, por ejemplo, por el dispositivo de seguridad 80. De modo similar, es concebible que el teléfono inteligente 50 pueda desactivar o bloquear con ayuda de la aplicación de acceso con tarjeta 61 la comunicación con el administrador de tarjetas inteligentes 80. También el administrador de tarjetas puede desactivar o bloquear la conexión con el dispositivo de comunicación. Cualquier evento puede llevar a una desactivación o bloqueo del teléfono inteligente 50 y/o del administrador de tarjetas inteligentes 70. Un evento puede ser, por ejemplo, la expiración de un tiempo de conexión establecido, exceder una cantidad de transferencia de datos acordada, la múltiple selección de una tarjeta no instalada, el ingreso repetido de un PIN superior erróneo.

A continuación, se explica con mayor detalle la funcionalidad del sistema basado en tarjetas inteligentes mostrado a modo de ejemplo en la Fig. 1.

Ahora se supone que el usuario del teléfono inteligente 50 dispone de al menos dos tarjetas inteligentes 90 y 91 certificadas que no desea guardar en su billetera, sino que desea instalar centralmente en su administrador de tarjetas inteligentes 70.

Para una explicación simple, se supone que el usuario tiene únicamente una tarjeta de pagos 90 del operador del centro de compras, así como una tarjeta de firma 91.

A fin de evitar un mal uso de la tarjeta, en el presente ejemplo, el usuario tiene que explorar primero la tarjeta de pagos 90 y la tarjeta de firma mediante un escáner de tarjetas inteligentes 72. Los datos explorados se transfieren luego desde el escáner de tarjetas inteligentes 72, por ejemplo, al dispositivo de seguridad 80 y allí, con ayuda de una identidad digital almacenada, se firma y eventualmente se verifica la autenticidad antes o después de la firma.

Cabe señalar que los diseños explorados también se pueden firmar con ayuda de una identidad digital, que está presente en la correspondiente tarjeta inteligente y se puede utilizar recién después de ingresar el PIN individual de la tarjeta en el administrador de tarjetas 70. Si la tarjeta inteligente no proporciona esta funcionalidad, entonces se usa la identidad digital del administrador de tarjetas.

Después de realizada la firma de los diseños explorados de tarjetas de las tarjetas inteligentes 90 y 91 y eventualmente después de la verificación exitosa de las tarjetas inteligentes 90 y 91 de la autenticidad, el dispositivo de seguridad 80 y/o el microcontrolador 74 autoriza al administrador de tarjetas 70 para la instalación de las dos tarjetas inteligentes 90 y 91.

Para la instalación, el usuario usa ahora su tarjeta de pagos 90 en los lectores de tarjetas 75 y su tarjeta de firma 91 en los lectores de tarjetas 76 del administrador de tarjetas inteligentes 70.

En la instalación, se realiza, entre otras cosas, una asignación entre la tarjeta inteligente usada y el correspondiente lector de tarjetas.

Esta asignación se puede realizar manualmente a través de un panel de control del administrador de tarjetas inteligentes 70, externamente a través de una computadora conectable con el administrador de tarjetas inteligentes 70 o incluso automáticamente por el administrador de tarjetas inteligentes 70 propiamente dicho. Consideramos a continuación la instalación a través de una computadora conectada externamente (no representada).

Para ello, el usuario ingresa, por ejemplo, el PIN de la tarjeta inteligente 90, el número del lector de tarjetas 75, en el que se usó la tarjeta inteligente 90, y un código que representa la tarjeta de pagos 90, que luego se requiere para hallar una tarjeta inteligente seleccionada en el teléfono inteligente 50. El PIN de la tarjeta inteligente 90 se almacena preferentemente en la memoria 81 del dispositivo de seguridad 80, mientras que el número del lector de tarjetas 75 y el código que representa la tarjeta de pagos se almacenan en la memoria 77. De igual manera, se almacenan los correspondientes datos para la tarjeta inteligente 91 y el lector de tarjetas 76 en la memoria 81 del dispositivo de seguridad 80 y en la memoria 77. Además, el usuario vela porque en su teléfono inteligente 50, además de los símbolos de las tarjetas inteligentes 90 y 91 instaladas, también se almacenen los correspondientes códigos, por ejemplo, en la memoria 60.

Ahora se supone que el usuario del teléfono inteligente 50 está ante el dispositivo de lectura de tarjetas 10 del centro de compras y que quiere pagar mediante su tarjeta de pagos 90 en el lector de tarjetas 20. El cliente ingresa ahora el deseo de querer abonar con la tarjeta inteligente 90 en su teléfono inteligente 50, lo cual es entendido por el microprocesador 53 como activación de la aplicación de acceso con tarjeta 61.

Según la implementación, la aplicación de acceso con tarjeta 61 bajo control del microprocesador 53 puede transferir ahora un paquete IP, que puede contener la dirección IP del administrador de tarjetas 70, la dirección IP del teléfono inteligente 50 y el deseo del usuario de querer abonar con la tarjeta inteligente 90, a través de una conexión con Internet con el dispositivo de acceso a la Internet 73, que pasa el paquete IP, por ejemplo, al módulo de seguridad 80. Este paquete IP puede ser interpretado por el módulo de seguridad 80 como comando de despertador. En respuesta a la solicitud de pago recibido, el administrador de tarjetas inteligentes 70 usando la dirección IP del teléfono inteligente 50 a través del acceso a Internet 73 establece una conexión segunda con la Internet, por ejemplo, en forma de un canal TLS con el dispositivo de acceso a la Internet 54 del teléfono inteligente 50. Luego se realiza un procedimiento de autentificación entre el dispositivo de seguridad 80 y la aplicación de acceso con tarjeta 61, a fin de autentificar el cliente o el teléfono inteligente 50. El procedimiento de autentificación es controlado preferentemente por el dispositivo de seguridad 80. Básicamente se pueden usar distintos procedimientos de autentificación en sí conocidos como, por ejemplo, una autentificación a través de OneTimePassword (OTP).

Después de una exitosa autentificación, se selecciona la tarjeta deseada, aquí la tarjeta inteligente 90, o el cliente puede solicitar, por ejemplo, de la aplicación de acceso con tarjeta 61, la selección de una tarjeta inteligente en su teléfono inteligente 50. A fin de facilitar la elección para el usuario, se pueden visualizar con la aplicación de acceso

con tarjeta 61 los símbolos almacenados para las tarjetas inteligentes 90 y 91 instaladas o los datos de diseño firmados almacenados en la memoria 77 en el display del teléfono inteligente 50, que previamente fueron transferidos por el administrador de tarjetas 70 a través de la conexión segura con el teléfono inteligente 50. Ahora el usuario selecciona en su teléfono inteligente 50 el símbolo de la tarjeta de pagos 90. La aplicación de acceso con tarjeta 61 vela luego porque el código correspondiente al símbolo seleccionado se transfiera a través de la conexión de Internet segura preferentemente al dispositivo de seguridad 80. Según la implementación, se puede solicitar que el usuario por la aplicación de acceso con tarjeta 61 o el dispositivo de seguridad 80 adicionalmente ingrese el PIN de la tarjeta inteligente seleccionada, en el ejemplo explicado, el PIN de la tarjeta de pagos 90, a fin de poder activar la tarjeta de pagos 90 para el tráfico de pagos. Si ya hay una conexión de comunicación entre el dispositivo de lectura de tarjetas 10 y el teléfono inteligente 50, entonces también se puede solicitar al usuario por el dispositivo de lectura de tarjetas 10 o bien por la aplicación a base de tarjetas allí instalada que ingrese el PIN de la tarjeta de pagos 90 seleccionada.

Sin embargo, el usuario sabe que a su administrador de tarjetas 70 se le asigna un PIN de nivel superior que lo ingresa ahora en vez del PIN de la tarjeta de pagos 90 en su teléfono inteligente 50.

Cabe señalar que también puede haber tarjetas en las que no se pueden usar PIN de nivel superior, ya que el uso de las tarjetas transfiere el PIN de manera encriptada. Por este motivo, se debe indicar al usuario si la aplicación admite el PIN de nivel superior.

La aplicación de acceso con tarjeta 61 ocasiona ahora la transferencia del PIN de nivel superior al dispositivo de seguridad 80. El dispositivo de seguridad 70 está en condiciones de verificar el PIN de nivel superior recibido mediante el código ya recibido que representa la tarjeta de pagos 90, de identificar el lector de tarjetas 75, en el que está la tarjeta de pagos 90 y transferir el PIN de la tarjeta de pagos 90 seleccionada a la tarjeta de pagos 90. El dispositivo de seguridad 80 encuentra el lector de tarjetas 75, por ejemplo, leyendo el número del lector de tarjetas 75 perteneciente al código recibido de la memoria 77.

Gracias a esta particular administración de los PIN, el cliente no necesita memorizar los números PIN de las tarjetas inteligentes 90 y 91 instaladas, sino únicamente el PIN de nivel superior de la tarjeta del dispositivo de seguridad 80.

Se supone que el usuario ha activado únicamente la interfaz NFC 51 de su teléfono inteligente 50. Por ello, una vez que el usuario coloca su teléfono inteligente 50 delante del lector de tarjetas 20 sin contacto, se produce de una manera en sí conocida una conexión NFC entre la interfaz NFC 21 del lector de tarjetas sin contacto 20 y la interfaz NFC 51 del teléfono inteligente 50.

La aplicación de pago almacenado, por ejemplo, en el dispositivo de lectura de tarjetas 10 se puede comunicar ahora bajo el control de la aplicación de acceso con tarjeta 61 instalada en el teléfono inteligente 50 en conexión con el microprocesador 53 a través del teléfono inteligente 50 y la conexión segura de Internet con la tarjeta inteligente 90 instalada en el administrador de tarjetas inteligentes 70. Desde el punto de vista de la aplicación del pago almacenada en el dispositivo de lectura de tarjetas 10, se genera así la impresión de que la aplicación de pago o bien el dispositivo de lectura de tarjetas 10 se comunica usualmente de modo directo con la tarjeta de pagos 90. En otras palabras, el teléfono inteligente 50 con ayuda de la aplicación de acceso con tarjeta 61 prolonga casi sólo la interfaz de comunicación de la 90.

Si el usuario del teléfono inteligente 50 no está delante del dispositivo de lectura de tarjetas 10, sino delante del dispositivo de lectura de tarjetas 15, entonces se produce la comunicación de radio de corto alcance con el lector de tarjetas 31 con contacto, por ejemplo, a través de la interfaz NFC 51 del teléfono inteligente 50 y la interfaz NFC 42 del adaptador 40.

Según la implementación, por ejemplo, el microprocesador 53 del teléfono inteligente 50 en conexión con la aplicación de acceso con tarjeta, puede reconocer la finalización del proceso de pago. El microprocesador 53 puede estar diseñado para finalizar, en respuesta al final reconocido del proceso de pago, la conexión inalámbrica de corto alcance entre el lector de tarjetas sin contacto 20 y el teléfono inteligente 50 y/o la conexión segura con Internet entre el teléfono inteligente 50 y el administrador de tarjetas inteligentes 70. De esta manera, se asegura que no se pueda operar un mal uso con la tarjeta inteligente 90 instalada en el administrador de tarjetas inteligentes 70.

A fin de evitar un mal uso del administrador de tarjetas inteligentes 70, se puede prever que la aplicación de acceso con tarjeta 61 almacenada en el teléfono inteligente 50 desactive mediante el microprocesador 53 la conexión segura con Internet cuando el PIN de nivel superior del dispositivo de seguridad 80 se haya ingresado mal varias veces.

Gracias al uso del administrador de tarjetas inteligentes 70, se pueden emplear también tarjetas inteligentes con contacto. Para ello, únicamente se ha de implementar un lector de tarjetas con interfaces con contacto en el

administrador de tarjetas inteligentes 70. La comunicación sin contacto de la tarjeta inteligente con contacto con el dispositivo de lectura de tarjetas 10 se produce, a su vez, a través del teléfono inteligente 50.

Además, el administrador de tarjetas inteligentes 70 facilita el intercambio de viejas tarjetas inteligentes por nuevas tarjetas inteligentes emitidas por el operador. Para ello, el usuario tiene que eliminar únicamente la vieja tarjeta inteligente de su administrador de tarjetas inteligentes 70 y colocar la nueva tarjeta inteligente e inicializarla.

Cabe señalar que, en este lugar, que las interfaces de comunicación de corto alcance implementadas en el lector de tarjetas 20 sin contacto o el teléfono inteligente 50, se pueden implementar, por ejemplo, como interfaz de software en forma de una Application Programming Interface (API).

Ahora se explica un segundo ejemplo de realización de un sistema basado en tarjetas inteligentes 5, que está representado en la Fig. 2.

El sistema basado en tarjetas inteligentes 5 mostrado en la Fig. 2 se distingue de sistema basado en tarjetas inteligentes 1 representado en la Fig. 1 porque la terminal de comunicaciones 100 usada que sirve para Internet no dispone de una interfaz de comunicación de corto alcance inalámbrica. Con preferencia, en el caso de la terminal de comunicaciones tampoco se trata de una terminal de comunicaciones móvil como un teléfono inteligente, sino, por ejemplo, de una laptop o una PC fija que no es apropiada para usar en equipos automáticos de tarjetas.

Se modo similar al teléfono inteligente 50 mostrado en la Fig. 1, la terminal de comunicaciones 100 puede presentar una memoria 110, en la que están almacenadas una aplicación de acceso con tarjeta 111, los símbolos de las tarjetas 112 de las tarjetas inteligentes 90 y 91 y además al menos una aplicación a base de tarjetas. Además, la terminal de comunicaciones 100 dispone de un dispositivo de acceso a la red 114, que está diseñado en el presente ejemplo como dispositivo de acceso a la Internet, a fin de permitirle al terminal de comunicación 100 un acceso a Internet. Un dispositivo de control programable, por ejemplo, en forma de un microprocesador 101 controla y supervisa la función de la terminal de comunicaciones 100.

El administrador de tarjetas inteligentes 70 mostrado en la Fig. 2 correspondiente preferentemente al administrador de tarjetas inteligentes mostrado en la Fig. 1, de modo que ya no se han de explicar con mayor detalle cada una de las partes. Como el teléfono inteligente 50, la terminal de comunicaciones 100 puede comunicarse con el administrador de tarjetas inteligentes 70.

Ahora se supone que la aplicación a base de tarjeta almacenada en la terminal de comunicaciones 100 es una aplicación de firma, con la que el usuario desea firmar un documento almacenado en la terminal de comunicaciones 100.

A fin de evitar repeticiones, se supone que se ha instalado el administrador de tarjetas inteligentes 70 y la terminal de comunicaciones 100 como se describió antes respecto del sistema basado en tarjetas inteligentes 1. Es decir, los símbolos de las tarjetas inteligentes 90 y 91, así como los códigos correspondientes se almacenan en la terminal de comunicaciones 100, mientras que los números PIN de las tarjetas inteligentes 90 y 91 se almacenan en el dispositivo de seguridad 80 y los números de los lectores de tarjetas 75 y 76 así como los códigos asignados a los símbolos de las tarjetas en la memoria 77.

Para la firma de su documento, el usuario requiere ahora un acceso al terminal de comunicación 100 a la tarjeta de firma 91, que está en el lector de tarjetas 76 de su administrador de tarjetas inteligentes 70.

Según la implementación, la aplicación de acceso con tarjeta 111 puede transferir por control del microprocesador 101 ahora un paquete IP, que contiene la dirección IP del administrador de tarjetas 70, la dirección IP de la terminal de comunicaciones 100 y la solicitud de firma del usuario, a través de una conexión con Internet con el dispositivo de acceso a Internet 73, que pasa el paquete IP, por ejemplo, al módulo de seguridad 80. En respuesta a la solicitud de firma recibida, el administrador de tarjetas inteligentes 70 usando la dirección IP de la terminal de comunicaciones 100 a través del acceso a Internet 73 establece una conexión segunda con Internet, por ejemplo, en forma de un canal TLS con el dispositivo de acceso a Internet 114 de la terminal de comunicaciones 100. Luego se realiza un procedimiento de autentificación entre el dispositivo de seguridad 80 y la aplicación de acceso con tarjeta 111, a fin de autentificar el cliente o bien la terminal de comunicaciones 100. El procedimiento de autentificación es controlado preferentemente por el dispositivo de seguridad 80.

Después de una exitosa autentificación, se puede solicitar al cliente, por ejemplo, por la aplicación de acceso con tarjeta 111, que seleccione una tarjeta inteligente en su terminal de comunicación 100. A fin de facilitar la elección para el usuario, se pueden visualizar por la aplicación de acceso con tarjeta 111 los símbolos almacenados para las tarjetas inteligentes 90 y 91 instaladas en el display de la terminal de comunicaciones 100. Ahora el usuario selecciona en su terminal de comunicación 100 el símbolo de la tarjeta de firma 91. La aplicación de acceso con tarjeta 111 vela luego porque el código perteneciente al símbolo seleccionado se transfiera a través de una conexión

segura de Internet preferentemente al dispositivo de seguridad 80. Según la implementación, se puede solicitar al usuario por la aplicación de acceso con tarjeta 111 o el dispositivo de seguridad 80 adicionalmente para que ingrese el PIN de la tarjeta inteligente seleccionada, en el ejemplo explicado, el PIN de la tarjeta de firma 91, a fin de poder activar la tarjeta de firma 91 para el proceso de firma.

Sin embargo, el usuario sabe que a su administrador de tarjetas 70 está asignado un PIN de nivel superior que ingresa ahora en lugar del PIN de la tarjeta de firma 91 en su terminal de comunicación 100. La aplicación de acceso con tarjeta 111 ocasiona ahora la transferencia del PIN de nivel superior al dispositivo de seguridad 80. El dispositivo de seguridad 70 está en condiciones de verificar el PIN de nivel superior recibido, de identificar por medio del código ya recibido que representa la tarjeta de firma 91, el lector de tarjetas 76, en el que está la tarjeta de firma 91 y de transferir el PIN de la tarjeta de firma 91 seleccionada a la tarjeta de firma 90. El dispositivo de seguridad 80 halla el lector de tarjetas 76 leyendo el número del lector de tarjetas 76 correspondiente al código recibido de la memoria 77.

La aplicación de firma almacenada en la memoria 110 se puede comunicar ahora bajo el control de la aplicación de acceso con tarjeta 111 instalada en la terminal de comunicaciones 100 en conexión con el microprocesador 101 a través de la terminal de comunicaciones 100 y la conexión segura de Internet con la tarjeta inteligente 91 instalada en el administrador de tarjetas inteligentes 70, a fin de firmar el documento.

Según la implementación, por ejemplo, el microprocesador 101 de la terminal de comunicaciones 100 en conexión con la aplicación de acceso con tarjeta 111 puede reconocer la finalización del proceso de firma. El microprocesador 101 puede estar configurado, en respuesta a la finalización del proceso de firma reconocido, puede finalizar la conexión segura con Internet entre la terminal de comunicaciones 100 y el administrador de tarjetas inteligentes 70. De esta manera, se asegura que no se pueda operar un mal uso con la tarjeta inteligente 91 instalada en el administrador de tarjetas inteligentes 70.

Resulta evidente que con el sistema basado en tarjetas inteligentes 1 mostrado en la Fig. 1 y el sistema basado en tarjetas inteligentes 5 mostrado en la Fig. 2 se pueden ejecutar todas las aplicaciones a base de tarjetas inteligentes ofrecidos en el mercado y a implementar a futuro, sin que el usuario tenga que llevar consigo una única tarjeta inteligente en su billetera. Es suficiente con que se instale la correspondiente tarjeta inteligente en un lector de tarjetas del administrador de tarjetas inteligentes 70.

REIVINDICACIONES

1. Procedimiento para operar un sistema basado en tarjetas (1, 5), que presenta una terminal de comunicaciones relacionada con el cliente (50, 100) y un administrador de tarjeta separado relacionado con el cliente (70), en donde se instalan varias tarjetas relacionadas con el cliente diseñadas como módulos de hardware (90, 91), con los siguientes pasos:

a) producir una conexión segura entre la terminal de comunicaciones (50, 100) y el administrador de tarjetas (70);

b) realizar una autentificación entre la terminal de comunicaciones (50, 100) y el administrador de tarjetas (70), a fin de autentificar la terminal de comunicaciones (50, 100);

c) seleccionar en la terminal de comunicaciones (50, 100) una tarjeta de varias tarjetas relacionadas con el cliente instaladas en el administrador de tarjetas (70), diseñadas como módulos de hardware (90, 91); y

d) realizar una aplicación a base de tarjeta, que se comunica a través de la terminal de comunicaciones (50, 100) y la conexión segura con la tarjeta relacionada con el cliente (90, 91) seleccionada en el paso c), instalado en el administrador de tarjetas (70).

2. Procedimiento de acuerdo con la reivindicación 1, caracterizado porque al administrador de tarjetas (70) se asigna un código de identificación individual de nivel superior, las tarjetas instaladas relacionadas con el cliente (90, 91) se protegen cada una mediante un código de identificación individual, que se almacena en la administrador de tarjetas (70), y porque en la terminal de comunicaciones (50, 100), se ingresa el código de identificación individual de nivel superior del administrador de tarjetas (70) y luego se transmite al administrador de tarjetas (70), que suministra a las tarjetas seleccionadas (90, 91) el código de identificación individual asignado.

3. Procedimiento de acuerdo con una de las reivindicaciones precedentes, caracterizado porque las tarjetas relacionadas con el cliente instaladas en el administrador de tarjetas (70) se visualizan en la terminal de comunicaciones (50, 100) de una manera predeterminada.

4. Procedimiento de acuerdo con una de las reivindicaciones precedentes, caracterizado porque al menos se explora un área predeterminada de cada una de las tarjetas relacionadas con el cliente (90, 91) por instalar en el administrador de tarjetas (70) y se verifica la autenticidad de cada una de las tarjetas exploradas del administrador de tarjetas (70) mediante el área explorada.

5. Procedimiento de acuerdo con una de las reivindicaciones precedentes, caracterizado porque el paso d) se realiza en la terminal de comunicaciones (100).

6. Procedimiento de acuerdo con una de las reivindicaciones 1 a 4, caracterizado porque la terminal de comunicaciones relacionada con el cliente (50) es una terminal de comunicaciones móvil, porque el sistema basado en tarjetas (1) presenta al menos un dispositivo de lectura de tarjetas (10, 15), que está asignado al proveedor de una aplicación a base de tarjeta, porque el paso d) se realiza en el dispositivo asignado al proveedor (10), y porque antes de la realización del paso d) se establece una conexión inalámbrica de corto alcance entre el dispositivo de lectura de tarjetas (10, 15) del proveedor y la terminal de comunicaciones móvil relacionada con el cliente.

7. Procedimiento de acuerdo con una de las reivindicaciones precedentes, caracterizado porque las tarjetas pro instalar en el administrador de tarjetas (70) se certifican primero, y/o porque en el paso a) se certifica la conexión segura, y/o porque la conexión segura es una conexión con la Internet.

8. Administrador de tarjetas, que está diseñado para usar en un procedimiento de acuerdo con una de las reivindicaciones 1 a 7, que comprende varios lectores de tarjetas sin contacto y/o con contacto (75, 76), que se diseñan cada uno para recibir y para leer una tarjeta relacionada con el usuario diseñada como módulo de hardware (90, 91), un segundo dispositivo de control programable (74), un dispositivo de seguridad (80), y un dispositivo de acceso a la red (73), en donde el dispositivo de seguridad (80) y una aplicación de acceso con tarjeta (61) de una terminal de comunicaciones asignado a un usuario (50, 100) se diseña para realizar una autentificación entre la terminal de comunicaciones (50, 100) y el administrador de tarjetas (70), a fin de autentificar la terminal de comunicaciones (50, 100), en donde el dispositivo de seguridad (80) se diseña para controlar el establecimiento de una conexión segura con la terminal de comunicaciones (50, 100), en donde la aplicación de acceso con tarjeta (61, 111) se diseña para seleccionar mediante el primer dispositivo de control programable (53, 101) una tarjeta relacionada con el usuario instalada en el administrador de tarjetas (70) (90, 91) y controlar la comunicación entre una aplicación a base de tarjeta y la tarjeta relacionada con el usuario seleccionada (90, 91) a través de una conexión segura establecida.

9. Sistema basado en tarjetas (1, 5) que comprende

- una terminal de comunicaciones asignado a un usuario (50, 100) con las siguientes características:

una aplicación de acceso con tarjeta (61, 111) instalada en la terminal de comunicaciones (50, 100),

una primera unidad de control programable (53, 101), y

un dispositivo de acceso a la red (54, 114),

- un administrador de tarjetas asignado al usuario (70) de acuerdo con la reivindicación 8.

10. Sistema basado en tarjetas de acuerdo con la reivindicación 9, caracterizado porque en el dispositivo de seguridad (80, 81) se almacena un código de identificación de nivel superior para la individualización del administrador de tarjetas (70), porque las tarjetas relacionadas con el usuario (90, 91) instaladas en el administrador de tarjetas (70) se aseguran cada una mediante un código de identificación individual, que se almacenan en una memoria (77) del administrador de tarjetas (70), en donde la aplicación de acceso con tarjeta (61, 111) de la terminal de comunicaciones (50, 100) se diseña para solicitar el usuario que ingrese el código de identificación de nivel superior, y en donde el administrador de tarjetas (70) se diseña, en respuesta al código de identificación de nivel superior recibido por la terminal de comunicaciones (50, 100), para leer el código de identificación individual de la tarjeta relacionada con el usuario seleccionada (90, 91) de la memoria (77) y transferirlo a la tarjeta relacionada con el usuario seleccionada.

11. Sistema basado en tarjetas de acuerdo con la reivindicación 9 ó 10, caracterizado porque el administrador de tarjetas (70) se diseña para identificar una tarjeta relacionada con el usuario (90, 91) usada en un lector de tarjetas (75, 76) y generar una asignación entre la tarjeta identificada (90, 91) y el correspondiente lector de tarjetas (75, 76).

12. Sistema basado en tarjetas de acuerdo con una de las reivindicaciones 9 a 11, caracterizado porque el administrador de tarjetas (70) presenta un escáner de tarjetas (72), que está diseñado para explorar al menos un área predeterminada de una tarjeta relacionada con el usuario por instalar (90, 91), y porque el dispositivo de seguridad (80) está diseñado para verificar, en respuesta a la al menos un área explorada, la autenticidad de la tarjeta por instalar (90, 91) y/o firmar la al menos un área explorada con una identidad digital.

13. Sistema basado en tarjetas de acuerdo con una de las reivindicaciones 9 a 12, caracterizado porque en la terminal de comunicaciones (100) se instala una aplicación a base de tarjetas.

14. Sistema basado en tarjetas de acuerdo con una de las reivindicaciones 9 a 13, caracterizado porque la terminal de comunicaciones relacionada con el usuario (50) es una terminal de comunicaciones móvil, que presenta al menos una interfaz de comunicación de corto alcance inalámbrica (51, 52), porque se prevé al menos un dispositivo de lectura de tarjetas (10, 20; 15; 25) asignado al proveedor de una aplicación a base de tarjetas, en donde el dispositivo de lectura de tarjetas (10, 20; 15, 25) del proveedor presenta al menos una interfaz de comunicación de corto alcance inalámbrica (21, 22) y/o una interfaz de comunicación con contacto (31), a la que se puede conectar un adaptador (40) con una interfaz de comunicación de corto alcance inalámbrica (41, 42) y se diseña para comunicarse con la al menos una interfaz de comunicación de corto alcance inalámbrica (51, 52) de la terminal de comunicaciones (50), porque el dispositivo asignado al proveedor (10) se diseña para realizar una aplicación a base de tarjeta, y porque la aplicación de acceso con tarjeta (61) de la terminal de comunicaciones móvil (50) se diseña para controlar mediante el primer dispositivo de control programable (53) la comunicación entre la aplicación a base de tarjetas ejecutada por la instalación (10) del proveedor y una tarjeta relacionada con el usuario (90) seleccionada en el administrador de tarjetas (70) a través de una conexión de corto alcance entre el lector de tarjetas (20, 25) del proveedor y la terminal de comunicaciones (50) y a través de una conexión segura.

15. Sistema basado en tarjetas de acuerdo con una de las reivindicaciones 9 a 13, caracterizado porque el dispositivo de seguridad (80) está diseñado para controlar el establecimiento de una conexión segura y eventualmente certificada con la terminal de comunicaciones (50, 100).

16. Sistema basado en tarjetasde acuerdo con una de las reivindicaciones 9 a 15, caracterizado porque las tarjetas relacionadas con el usuario (90, 91) son tarjetas inteligentes y/o porque el dispositivo de acceso a la red (54, 114) de la terminal de comunicaciones (50, 100) y el dispositivo de acceso a la red (73) del administrador de tarjetas (70) asignado al usuario son en cada caso un dispositivo de acceso a la Internet.

17. Programa informático que contiene múltiples instrucciones que son almacenables en una terminal de comunicaciones relacionada con el usuario (50, 100) y en un administrador de tarjetas relacionado con el usuario (70) de un sistema basado en tarjetas, en donde las instrucciones, cuando pueden ser leídas y procesadas por un dispositivo de control programable (53, 101) de la terminal de comunicaciones (50, 100) y un dispositivo de control

programable (74) del administrador de tarjetas (70), ejecutan el procedimiento de acuerdo con una de las reivindicaciones 1 a 7.

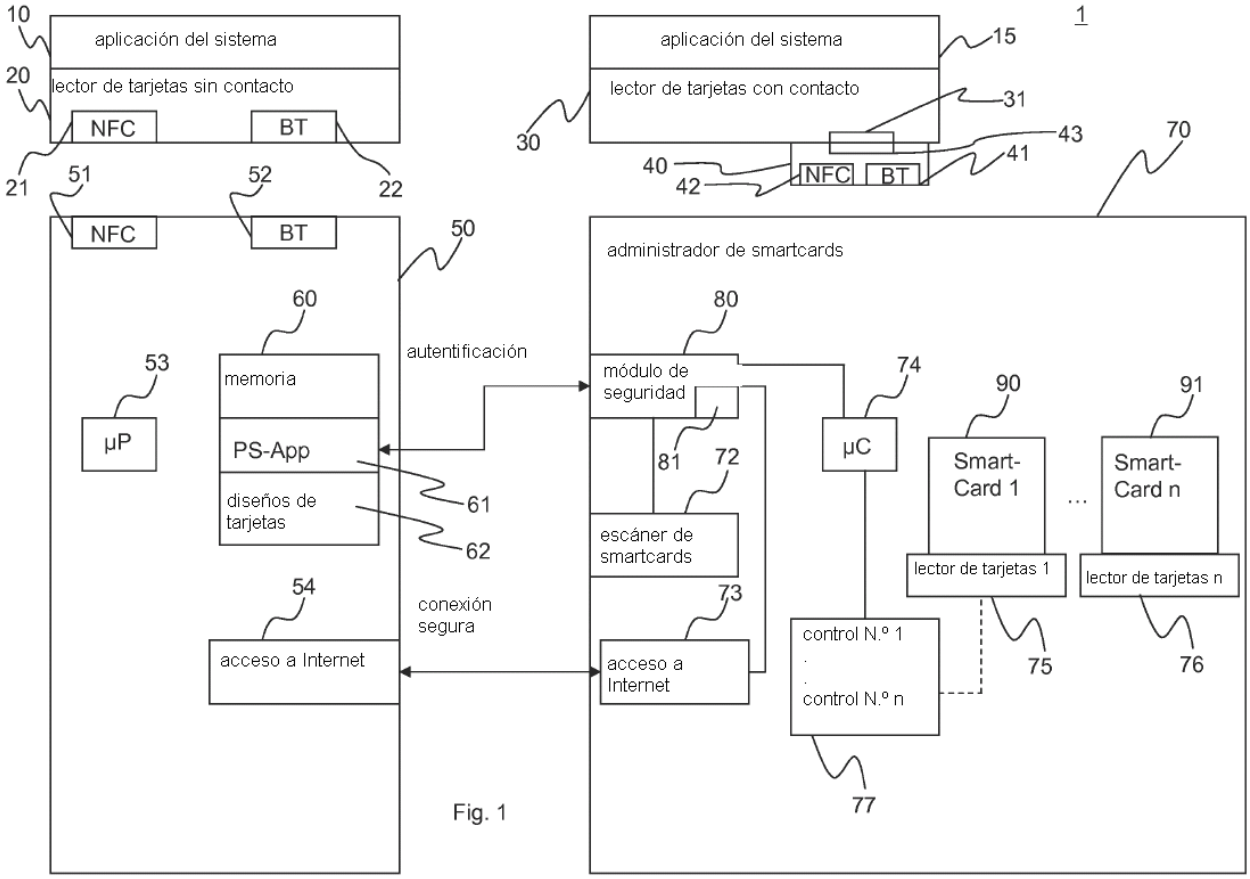
10
aplicación del sistema
20
lector de tarjetas sin contacto
NFC
BT
21
51
52
22
NFC
BT
50
60
53
memoria
µP
PS-App
diseños de tarjetas
61
62
54
acceso a Internet
conexión segura
autentificación
1
aplicación del sistema
15
lector de tarjetas con contacto
30
31
43
70
40
41
42
NFC
BT
administrador de smartcards
80
módulo de seguridad
81
72
escáner de smartcards
73
acceso a Internet
74
µC
control N.º 1
control N.º n
77
90
Smart-Card 1
91
Smart-Card n
lector de tarjetas 1
lector de tarjetas n
75
76

Fig. 1

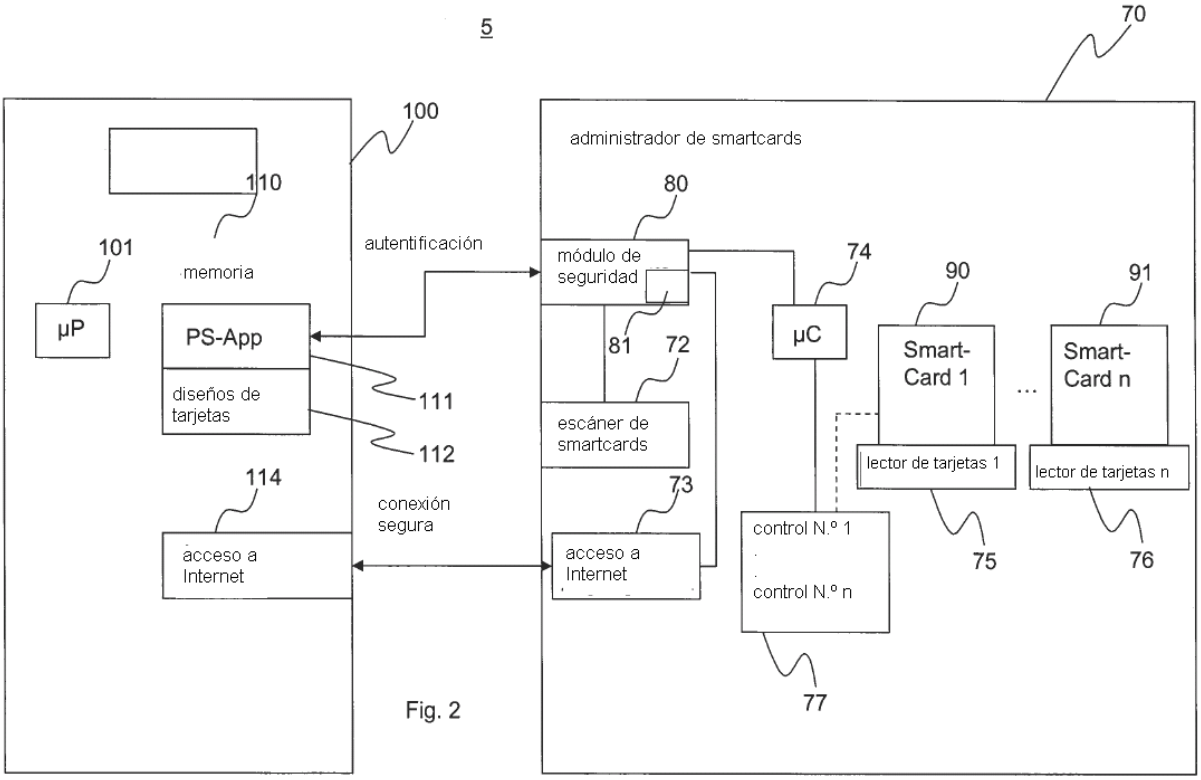
5
70
100
administrador de smartcards
110
80
101
memoria
autentificación
módulo de seguridad
74
90
91
μP
PS-App
81
72
μC
Smart-Card 1
...
Smart-Card n
diseños de tarjetas
111
112
escáner de smartcards
lector de tarjetas 1
lector de tarjetas n
114
73
conexión segura
control N.º 1
acceso a Internet
acceso a Internet
control N.º n
75
76
77

Fig. 2