

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 817 847**

51 Int. Cl.:

H04W 4/50 (2008.01)

H04W 4/80 (2008.01)

H04W 12/00 (2009.01)

H04W 12/08 (2009.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

86 Fecha de presentación y número de la solicitud internacional: **15.12.2014 PCT/EP2014/003353**

87 Fecha y número de publicación internacional: **20.08.2015 WO15120873**

96 Fecha de presentación y número de la solicitud europea: **15.12.2014 E 14823899 (1)**

97 Fecha y número de publicación de la concesión europea: **15.07.2020 EP 3108673**

54 Título: **Sistema y método para gestionar datos de aplicación de aplicaciones de tarjetas sin contacto**

30 Prioridad:

17.02.2014 CH 211142014

45 Fecha de publicación y mención en BOPI de la traducción de la patente:
08.04.2021

73 Titular/es:

**KABA AG GROUP INNOVATION MANAGEMENT
(100.0%)
Hofwiesenstrasse 24
8153 Rümlang, CH**

72 Inventor/es:

**STUDERUS, PAUL y
LÜSCHER, ANDRÉ**

74 Agente/Representante:

VALLEJO LÓPEZ, Juan Pedro

ES 2 817 847 T3

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 y método para gestionar datos de aplicación de aplicaciones de tarjetas sin contacto

5 **Campo de la invención**

La presente invención se refiere a un sistema y a un método para gestionar datos de aplicación de diferentes aplicaciones de tarjetas sin contacto. En concreto, la presente invención se refiere a un sistema y a un método para gestionar datos de aplicación de diferentes aplicaciones de tarjetas sin contacto para una pluralidad de dispositivos de comunicación móvil que comprenden una interfaz de comunicación inalámbrica de corto alcance.

Antecedentes de la invención

Los dispositivos de comunicación móvil están equipados, cada vez más, con interfaces de comunicación inalámbrica de corto alcance para realizar transacciones de datos inalámbricas con dispositivos de transacción externos que están ubicados muy cerca de los dispositivos de comunicación móvil. Por ejemplo, las interfaces de comunicación inalámbrica de corto alcance incluyen módulos de Comunicación de Campo Cercano (NFC) para un alcance de unas pocas pulgadas y/o módulos de comunicación de Bluetooth para un alcance de unos pocos metros. También está disponible una infraestructura establecida de dispositivos de transacción, tales como lectores para interactuar con tarjetas sin contacto, es decir, tarjetas de chip, las así denominadas tarjetas inteligentes o tarjetas de circuito integrado (TIC), equipadas con transceptores de RFID (Identificador de Radiofrecuencia). Esta infraestructura de dispositivos de transacción hace posible implementar diversas aplicaciones diferentes en función de las tarjetas sin contacto. Los ejemplos de tales aplicaciones de tarjetas sin contacto incluyen control de acceso, emisión de billetes electrónicos, pago de débito, pago de crédito, pago de efectivo electrónico, contabilidad de costes de impresión/copia, cerraduras autónomas, aplicaciones de hotel y campus, etc. Funciones correspondientes de las tarjetas sin contacto se están implementando, cada vez más, en dispositivos de comunicación móvil, por ejemplo, en radioteléfonos móviles, ordenadores de tipo tableta, ordenadores ultraportátiles u otros dispositivos de comunicación y ordenadores personales portátiles. Por lo tanto, en lugar de portar y usar una o más tarjetas sin contacto, los usuarios pueden usar, de forma más conveniente, sus dispositivos de comunicación móvil para interactuar con dispositivos de transacción. Normalmente, sin embargo, las tarjetas sin contacto, así como su implementación correspondiente en dispositivos de comunicación móvil, solo soportan una aplicación de tarjetas sin contacto. Para un usuario, esto puede resultar bastante incómodo, debido a que solo una tarjeta puede estar activa a la vez y el usuario tiene que conmutar activamente entre diferentes tarjetas siempre que se va a usar otra aplicación. Además, en un estado apagado de un dispositivo de comunicación móvil, solo está activa una tarjeta "predeterminada" (tarjetas de NFC) y, por lo tanto, solo la aplicación de esa tarjeta particular está disponible para el usuario. Si se va a implementar más de una aplicación en una tarjeta sin contacto o una implementación correspondiente en un dispositivo de comunicación móvil, todas las aplicaciones se han de implementar en el momento en el que se está personalizando la tarjeta usando una clave de implementación de autorización. En consecuencia, todas estas aplicaciones serían proporcionadas e implementadas por la misma entidad, con muy poca o ninguna flexibilidad de la temporización de la implementación y la modificación de aplicaciones.

El documento US 8.255.687 describe un sistema para posibilitar que los usuarios seleccionen entre proveedores de servicios seguros disponibles para proporcionar aplicaciones y servicios en un elemento seguro instalado en un dispositivo del usuario. De acuerdo con el documento US 8.255.687, el elemento seguro es una pieza de hardware, por ejemplo, una tarjeta extraíble o un chip, tal como una tarjeta de SIM o una tarjeta microSD, que se instala en el dispositivo de comunicación de un usuario. Un elemento seguro generalmente incluye su propio entorno operativo con un microprocesador, memoria y sistema operativo a prueba de manipulaciones indebidas. El elemento seguro tiene una o más claves que normalmente se instalan en el momento de la fabricación. Una clave correspondiente es compartida por un Gestor de Servicios de Confianza (TSM), posibilitando que el TSM establezca un canal criptográficamente seguro con el elemento seguro para la instalación, el aprovisionamiento y la personalización del elemento seguro mientras el dispositivo que tiene el elemento seguro está en posesión de un usuario final. El dispositivo incluye un módulo de selector de proveedor de servicios (SPS) que posibilita que el usuario seleccione un proveedor de servicios seguros. El módulo de SPS se comunica con un servicio de custodia de claves que distribuye claves criptográficas para el elemento seguro al proveedor de servicios seguros seleccionado por el usuario, o con un TSM central que proporciona aplicaciones y servicios en nombre del proveedor de servicios seguros seleccionado por el usuario. El controlador de NFC del dispositivo del usuario se basa en el elemento seguro para proporcionar un entorno operativo seguro para transacciones financieras, emisión de billetes de tránsito, identificación y autenticación, acceso de seguridad física y otras funciones. Por ejemplo, el controlador de NFC interacciona de forma segura con el elemento seguro para obtener credenciales de pago a partir del elemento seguro y proporcionar esas credenciales a un punto de servicio habilitado para NFC a través de la antena de NFC del dispositivo.

El documento US 2012/0300932 describe sistemas y métodos para cifrar comunicaciones de dispositivos móviles. Como se explica en el documento US 2012/0300932, los dispositivos móviles pueden incluir tanto espacio de memoria compartida como uno o más elementos seguros. De acuerdo con el documento US 2012/0300932, el elemento seguro es un almacenamiento legible por ordenador en la memoria del dispositivo móvil o cualquier medio securitizado que tenga memoria, tal como una Tarjeta de Circuito Integrado Universal ("TIC"), Módulo de Identidad de Abonado ("SIM"),

y similares. El elemento seguro puede incluir funcionalidad para recibir mensajes, tales como mensajes de transacciones, desde aplicaciones de memoria compartida, cifrar los mensajes recibidos y proporcionar los mensajes cifrados de vuelta a las aplicaciones de memoria compartida. Por ejemplo, una billetera móvil se puede almacenar en la memoria compartida y el elemento seguro puede incluir una aplicación de seguridad o una aplicación de autenticación que recibe un mensaje desde la billetera móvil. La aplicación de seguridad puede utilizar cualquier número de técnicas de cifrado adecuadas para cifrar el mensaje, y la aplicación segura del elemento seguro puede proporcionar el mensaje cifrado de vuelta a la billetera móvil. Entonces, la billetera móvil puede transmitir o comunicar de otro modo el mensaje a un destinatario, tal como un comerciante o un gestor de servicios de confianza ("TSM"). De manera similar, la billetera móvil puede proporcionar mensajes recibidos a la aplicación de seguridad del elemento seguro para su descifrado. Al usar la tecnología de NFC del dispositivo móvil, las aplicaciones también pueden posibilitar transacciones. Un ordenador de Gestión de Servicios de Confianza se comunica con los dispositivos móviles y facilita la gestión del espacio de aplicaciones en el elemento seguro y la verificación del estado del dispositivo móvil y sus aplicaciones y elementos seguros, tal como activo, bloqueado, desbloqueado o terminado.

El documento XP055539403: "*Essentials for Successful NFC Mobile Ecosystems*", publicado por el Foro de NFC el 1 de octubre de 2008, representa técnica anterior relevante adicional.

Sumario de la invención

Un objetivo de la presente invención es proporcionar un sistema y un método para gestionar datos de aplicación de diferentes aplicaciones de tarjetas sin contacto, sistema y método que no tienen al menos algunas de las desventajas de la técnica anterior. En particular, un objetivo de la presente invención es proporcionar un sistema y un método para gestionar datos de aplicación de diferentes aplicaciones de tarjetas sin contacto para una pluralidad de dispositivos de comunicación móvil, de tal modo que no es necesario implementar las aplicaciones en un dispositivo de comunicación móvil al mismo tiempo o por el mismo proveedor de aplicaciones.

De acuerdo con la presente invención, estos objetivos se logran a través de las características de las reivindicaciones independientes. Además, de las reivindicaciones dependientes y de la descripción se derivan realizaciones ventajosas adicionales.

De acuerdo con la presente invención, los objetivos mencionados anteriormente se logran particularmente ya que se proporciona un sistema informático para gestionar datos de aplicación de diferentes aplicaciones de tarjetas sin contacto para una pluralidad de dispositivos de comunicación móvil. El sistema informático comprende uno o más procesadores configurados para: transferir a través de una red de telecomunicaciones a uno de los dispositivos de comunicación móvil un módulo de emulación de tarjetas, usando una clave de acceso de área para almacenar el módulo de emulación de tarjetas en un área segura del dispositivo de comunicación móvil. El módulo de emulación de tarjetas comprende un código de programa informático configurado para controlar un procesador del dispositivo de comunicación móvil para emular un módulo de tarjeta sin contacto y para ejecutar transacciones de datos a través de una interfaz de comunicación inalámbrica de corto alcance del dispositivo de comunicación móvil. Los procesadores del sistema informático están configurados adicionalmente para transferir datos de aplicación para al menos una aplicación de tarjetas sin contacto a través de la red de telecomunicaciones al dispositivo de comunicación móvil para almacenar los datos de aplicación en el módulo de emulación de tarjetas. Además, los procesadores del sistema informático están configurados para mantener en el sistema una base de datos de tarjetas y almacenar en la base de datos de tarjetas para cada uno de la pluralidad de dispositivos de comunicación móvil una representación del módulo de emulación de tarjetas almacenado en el dispositivo de comunicación móvil respectivo.

Proporcionar un sistema informático para instalar y gestionar, en los dispositivos de comunicación móvil, un módulo de emulación de tarjetas y datos de aplicación hace posible gestionar de forma centralizada, para una pluralidad de dispositivos de comunicación móvil, los datos de aplicación de diferentes aplicaciones de tarjetas sin contacto y diferentes proveedores de aplicaciones. El sistema informático proporciona una plataforma centralizada que hace posible gestionar, almacenar y cambiar de manera flexible los datos de aplicación de diferentes aplicaciones de tarjetas sin contacto y diferentes proveedores de aplicaciones en puntos variables en el tiempo, para dispositivos de comunicación móvil individuales o grupos de los mismos, según se solicite o se necesite por los proveedores de aplicaciones o usuarios de los dispositivos de comunicación móvil, por ejemplo, y sin limitación al tiempo de personalización de una tarjeta o restricción a un único proveedor de aplicaciones. Por lo tanto, el sistema informático hace posible implementar y gestionar de forma flexible y eficiente varias aplicaciones de tarjetas sin contacto diferentes procedentes de varios proveedores de aplicaciones (socios) diferentes en un módulo de emulación de tarjetas común en un dispositivo de comunicación móvil. En consecuencia, los usuarios de un dispositivo de comunicación móvil tienen la ventaja de una tarjeta tanto de múltiples aplicaciones como de múltiples proveedores, que combina aplicaciones de tarjetas sin contacto para uso privado y comercial, diferentes fines y diferentes proveedores en una tarjeta que se puede mantener activa y ser usada en cualquier momento, con independencia de la disponibilidad de alimentación de batería en el dispositivo de comunicación móvil. Por ejemplo, un usuario puede instalar y usar, en una única tarjeta, una aplicación de control de acceso para su hogar, una aplicación de control de acceso para su lugar de trabajo, una aplicación de emisión de billetes para transporte público, una aplicación de abono para un gimnasio, una aplicación de débito para una cafetería y aplicaciones de débito para diferentes máquinas expendedoras, etc.

En una realización, los procesadores del sistema están configurados adicionalmente para transferir datos de derechos de acceso específicos de la aplicación para una pluralidad de aplicaciones de tarjetas sin contacto a través de la red de telecomunicaciones al dispositivo de comunicación móvil para almacenar los datos de derechos de acceso específicos de la aplicación en el módulo de emulación de tarjetas, y para almacenar en el sistema claves de acceso específicas de la aplicación para una pluralidad de aplicaciones de tarjetas sin contacto. El módulo de emulación de tarjetas comprende un código de programa informático configurado para controlar el procesador del dispositivo de comunicación móvil para ejecutar transacciones de datos a través de la interfaz de comunicación inalámbrica de corto alcance del dispositivo de comunicación móvil, y para verificar la autorización de un socio de transacción (entidad de transacción, dispositivo de transacción) para acceder a datos de aplicación almacenados en el módulo de emulación de tarjetas para una aplicación de tarjetas sin contacto particular, basándose en los datos de derechos de acceso específicos de la aplicación, almacenados en el módulo de emulación de tarjetas para la aplicación de tarjetas sin contacto particular, y una clave de acceso específica de la aplicación, recibida del socio de transacción a través de la interfaz de comunicación inalámbrica de corto alcance. Esta realización hace posible ejecutar transacciones de datos *fuera de línea* para una aplicación de tarjetas sin contacto, sin la necesidad de acceder a la base de datos de tarjetas del sistema informático para acceder a datos de aplicación.

En otra realización, los datos de aplicación almacenados en el módulo de emulación de tarjetas del dispositivo de comunicación móvil comprenden un puntero a datos de aplicación almacenados en la base de datos de tarjetas. El módulo de emulación de tarjetas comprende un código de programa informático configurado para controlar el procesador del dispositivo de comunicación móvil para recuperar los datos de aplicación de la base de datos de tarjetas usando el puntero, y para ejecutar las transacciones de datos a través de la interfaz de comunicación inalámbrica de corto alcance del dispositivo de comunicación móvil usando datos de aplicación recuperados de la base de datos de tarjetas. Esta realización hace posible ejecutar transacciones de datos *en línea* para una aplicación de tarjetas sin contacto, sin la necesidad de transferir y almacenar el contenido de datos de aplicación de forma local en el módulo de emulación de tarjetas de los dispositivos de comunicación móvil.

En una realización, los procesadores del sistema están configurados adicionalmente para leer los datos de aplicación almacenados en el módulo de emulación de tarjetas de uno de los dispositivos de comunicación móvil, y para ejecutar al menos uno de: transferir desde el sistema al dispositivo de comunicación móvil datos de aplicación actualizados almacenados en la base de datos de tarjetas, en casos en los que los datos de aplicación leídos del dispositivo de comunicación móvil indican una versión obsoleta de los datos de aplicación, y actualizar en el sistema la representación del módulo de emulación de tarjetas del dispositivo de comunicación móvil almacenando en la base de datos de tarjetas datos de aplicación leídos desde el módulo de emulación de tarjetas del dispositivo de comunicación móvil, en casos en los que los datos de aplicación leídos del dispositivo de comunicación móvil indican una versión más reciente de los datos de aplicación. En consecuencia, realizando operaciones de lectura periódicamente o a petición, los datos de aplicación almacenados de forma centralizada en las representaciones de módulo de tarjeta en la base de datos de tarjetas del sistema informático se sincronizan con los datos de aplicación almacenados en el módulo de emulación de tarjetas de los dispositivos de comunicación móvil.

En otra realización, los procesadores del sistema informático están configurados adicionalmente para recibir a través de la red de telecomunicaciones una solicitud relacionada con una aplicación de tarjetas sin contacto para realizar al menos una de las siguientes operaciones de datos de aplicación para el módulo de emulación de tarjetas de uno o más dispositivos de comunicación móvil: descargar datos de aplicación adicionales en el módulo de emulación de tarjetas, actualizar datos de aplicación en el módulo de emulación de tarjetas y eliminar datos de aplicación en el módulo de emulación de tarjetas. Dependiendo del escenario, una solicitud de datos de aplicación es iniciada por un sistema de socio autorizado o una entidad de aplicaciones asociada, o por el dispositivo de comunicación móvil, por ejemplo. Los procesadores del sistema informático están configurados adicionalmente para transferir una solicitud de datos de aplicación al módulo de emulación de tarjetas del uno o más dispositivos de comunicación móvil de acuerdo con la operación de datos de aplicación respectiva, y para actualizar en la base de datos de tarjetas la representación del módulo de emulación de tarjetas del uno o más dispositivos de comunicación móvil actualizando datos de aplicación en la base de datos de tarjetas de acuerdo con la solicitud de datos de aplicación. En consecuencia, con cada solicitud de datos de aplicación y operación de datos de aplicación ejecutada, los datos de aplicación almacenados de forma centralizada en las representaciones de módulo de tarjeta en la base de datos de tarjetas del sistema informático se sincronizan con los datos de aplicación almacenados en el módulo de emulación de tarjetas de los dispositivos de comunicación móvil.

En una realización, los procesadores del sistema informático están configurados adicionalmente para recibir a través de la red de telecomunicaciones desde un sistema de socio autorizado una solicitud de escritura, que incluye datos de aplicación para el módulo de emulación de tarjetas de uno o más dispositivos de comunicación móvil, y/o una solicitud de lectura para leer datos de aplicación desde el módulo de emulación de tarjetas de uno o más dispositivos de comunicación móvil; para transferir los datos de aplicación a través de la red de telecomunicaciones al módulo de emulación de tarjetas del uno o más dispositivos de comunicación móvil, en caso de una solicitud de escritura; y para leer los datos de aplicación almacenados en el módulo de emulación de tarjetas del uno o más dispositivos de comunicación móvil, en caso de una solicitud de lectura; y para actualizar en el sistema la representación del módulo de emulación de tarjetas del uno o más dispositivos de comunicación móvil almacenando en la base de datos de tarjetas los datos de aplicación leídos o almacenados en el módulo de emulación de tarjetas del uno o más dispositivos

de comunicación móvil, respectivamente. Por lo tanto, un sistema de socio puede leer y/o escribir, en cualquier momento, datos de aplicación asociados con su aplicación o aplicaciones de tarjetas sin contacto desde el módulo de emulación de tarjetas de uno o más dispositivos de comunicación móvil.

5 En otra realización, los procesadores del sistema informático están configurados adicionalmente para recibir a través de la red de telecomunicaciones una solicitud relacionada con uno de los dispositivos de comunicación móvil, exigiendo la solicitud una actualización del módulo de emulación de tarjetas. Dependiendo del escenario, una solicitud de actualización de tarjeta es iniciada por un sistema de socio autorizado o una entidad de aplicaciones asociada, o por el dispositivo de comunicación móvil, por ejemplo. Los procesadores del sistema informático están configurados
10 adicionalmente para transferir un código de programa para el módulo de emulación de tarjetas al dispositivo de comunicación móvil de acuerdo con la solicitud; y para actualizar en la base de datos de tarjetas la representación de los módulos de emulación de tarjetas de los dispositivos de comunicación móvil almacenando en la base de datos de tarjetas un número de versión, que indica la versión del código de programa transferido al dispositivo de comunicación móvil, y/o el código de programa transferido al dispositivo de comunicación móvil. Por lo tanto, el módulo de programa de un módulo de emulación de tarjetas se puede actualizar en cualquier momento con código de programa actualizado, lo que hace posible que el sistema informático mejore o corrija los módulos de programa de uno o dispositivos de comunicación móvil, al tiempo que se mantiene en la base de datos de tarjetas una representación sincronizada de los módulos de emulación de tarjetas afectados.

20 En una realización, el módulo de emulación de tarjetas comprende un código de programa informático configurado para controlar un procesador del dispositivo de comunicación móvil para ejecutar la transacción de datos a través de la interfaz de comunicación inalámbrica de corto alcance del dispositivo de comunicación móvil con un dispositivo de transacción externo, incluyendo la transacción de datos una transacción de pago de débito, una transacción de pago de crédito, una transacción de pago de efectivo electrónico, una transacción de emisión de billetes, una transacción
25 de control de acceso, una transacción de actualización de aplicación para actualizar los datos de aplicación en el módulo de emulación de tarjetas y/o una transacción de actualización de tarjeta para actualizar el código de programa informático del módulo de emulación de tarjetas; e incluyendo los datos de aplicación datos de cuenta de débito, datos de cuenta de crédito, datos de efectivo electrónico, datos de billete electrónico, datos de derechos de acceso, datos de identificación de usuario, datos de autenticación de usuario y datos de estructura de datos de aplicación.

30 Además del sistema para gestionar datos de aplicación de diferentes aplicaciones de tarjetas sin contacto para una pluralidad de dispositivos de comunicación móvil, la presente invención también se refiere a un método implementado por ordenador para gestionar datos de aplicación de diferentes aplicaciones de tarjetas sin contacto para una pluralidad de dispositivos de comunicación móvil, comprendiendo el método: transferir por un sistema informático a través de una red de telecomunicaciones a uno de los dispositivos de comunicación móvil un módulo de emulación de tarjetas, usando una clave de acceso de área para almacenar el módulo de emulación de tarjetas en un área segura del dispositivo de comunicación móvil, comprendiendo el módulo de emulación de tarjetas un código de programa informático configurado para controlar un procesador del dispositivo de comunicación móvil para emular un módulo de tarjeta sin contacto y para ejecutar transacciones de datos a través de una interfaz de comunicación inalámbrica de corto alcance del dispositivo de comunicación móvil; transferir por el sistema informático a través de la red de telecomunicaciones al dispositivo de comunicación móvil datos de aplicación para al menos una aplicación de tarjetas sin contacto para almacenar los datos de aplicación en el módulo de emulación de tarjetas; y mantener en el sistema informático una base de datos de tarjetas, almacenando en la base de datos de tarjetas para cada uno de la pluralidad de dispositivos de comunicación móvil una representación del módulo de emulación de tarjetas almacenado en el
45 dispositivo de comunicación móvil respectivo.

Además del sistema informático y el método implementado por ordenador para gestionar datos de aplicación de diferentes aplicaciones de tarjetas sin contacto para una pluralidad de dispositivos de comunicación móvil, la presente invención también se refiere a un producto de programa informático que comprende un medio legible por ordenador no transitorio que tiene almacenado en el mismo un código de programa informático configurado para controlar un procesador de un sistema informático para realizar las etapas de: transferir desde el sistema informático a través de una red de telecomunicaciones a uno de los dispositivos de comunicación móvil un módulo de emulación de tarjetas, usando una clave de acceso de área para almacenar el módulo de emulación de tarjetas en un área segura del dispositivo de comunicación móvil, comprendiendo el módulo de emulación de tarjetas un código de programa informático configurado para controlar un procesador de un dispositivo de comunicación móvil para emular un módulo de tarjeta sin contacto y para ejecutar transacciones de datos a través de una interfaz de comunicación inalámbrica de corto alcance del dispositivo de comunicación móvil; transferir desde el sistema informático a través de la red de telecomunicaciones al dispositivo de comunicación móvil datos de aplicación para al menos una aplicación de tarjetas sin contacto para almacenar los datos de aplicación en el módulo de emulación de tarjetas; y mantener en el sistema informático una base de datos de tarjetas, almacenando en la base de datos de tarjetas para cada uno de la pluralidad de dispositivos de comunicación móvil una representación del módulo de emulación de tarjetas almacenado en el
60 dispositivo de comunicación móvil respectivo.

Breve descripción de los dibujos

65 La presente invención se explicará con más detalle, a modo de ejemplo, con referencia a los dibujos, en los que:

La figura 1: muestra un diagrama de bloques que ilustra esquemáticamente un sistema para gestionar datos de aplicación de diferentes aplicaciones de tarjetas sin contacto para una pluralidad de dispositivos de comunicación móvil.

La figura 2: muestra un diagrama de bloques que ilustra esquemáticamente un dispositivo de comunicación móvil con una interfaz de comunicación inalámbrica, un procesador, un módulo de emulación de tarjetas y datos de aplicación.

La figura 3: muestra un diagrama de flujo que ilustra una secuencia ilustrativa de etapas para gestionar datos de aplicación de diferentes aplicaciones de tarjetas sin contacto para un dispositivo de comunicación móvil.

Descripción detallada de las realizaciones preferidas

En las figuras 1 y 3, el número de referencia 1 se refiere a un sistema informático para gestionar datos de aplicación de diferentes aplicaciones de tarjetas sin contacto para una pluralidad de dispositivos de comunicación móvil 2.

Las aplicaciones de tarjetas sin contacto incluyen diversos tipos de transacciones que utilizan tarjetas inteligentes o de chip con capacidades de comunicación inalámbrica. Las transacciones se realizan entre una tarjeta sin contacto y un lector de tarjetas (entidad de transacción o dispositivo de transacción externo) que comprende una interfaz de comunicación inalámbrica correspondiente. Las transacciones incluyen el intercambio de datos de aplicación entre la tarjeta sin contacto y el lector de tarjetas en las así denominadas unidades de datos de protocolo de aplicación (APDU). Por ejemplo, las aplicaciones de tarjetas sin contacto incluyen transacciones de pago de débito, transacciones de pago de crédito, transacciones de pago de efectivo electrónico, transacciones de emisión de billetes, transacciones de control de acceso y transacciones de autenticación. En consecuencia, los datos de aplicación asociados con estas aplicaciones de tarjetas sin contacto incluyen datos de cuenta de débito, datos de cuenta de crédito, datos de efectivo electrónico, datos de billete electrónico, datos de derechos de acceso, datos de autenticación de usuario y datos de identificación de usuario.

El sistema informático 1 comprende uno o más ordenadores operables con uno o más procesadores 12. El sistema informático comprende adicionalmente 1 un módulo de comunicación 11 configurado para la comunicación de datos con sistemas de socio 3 y dispositivos de comunicación móvil 2 a través de una red de telecomunicaciones 4, 5. La red de telecomunicaciones 4, 5 incluye redes de comunicación de línea fija y/o redes de comunicación de radio móvil, por ejemplo, una red de GSM (Sistema Global para comunicación Móvil), una red de UMTS (Sistema de Telefonía Móvil Universal) u otro sistema de telefonía de radio móvil, y/o una WLAN (Red de Área Local Inalámbrica) para acceder a Internet. En una realización, la red de telecomunicaciones 4 incluye líneas dedicadas fijas entre el sistema informático 1 y un sistema de socio 3. En una realización adicional, la red de telecomunicaciones 5 incluye sistemas de replicación por aire para transmitir datos desde el sistema informático 1 a los dispositivos de comunicación móvil 2 (enfoque de almacenamiento y reenvío). En una realización adicional más, indicada por la ruta de comunicación 8, el módulo de comunicación 11 del sistema informático 1 está configurado adicionalmente para la comunicación de datos con dispositivos de transacción 6, por ejemplo, a través de una red de telecomunicaciones 4, 5.

Cada uno de los sistemas de socio 3 comprende uno o más ordenadores operables que incluyen uno o más procesadores. Los sistemas de socio 3 están asociados con socios autorizados del proveedor del sistema informático 1. Los sistemas de socio 3 están provistos de claves de acceso criptográficas para un acceso autorizado al sistema informático 1, al menos a un área definida, aplicaciones de tarjetas sin contacto definidas y/o servicios definidos del sistema informático 1 asignados al socio o al sistema de socio 3, respectivamente. Por lo tanto, el sistema informático 1 gestiona y mantiene los derechos de acceso (de lectura y/o de escritura) de sus socios o sistemas de socio 3, respectivamente, con respecto a sus aplicaciones de tarjetas sin contacto y datos de aplicación relacionados. En concreto, el sistema informático 1 gestiona y mantiene los derechos de acceso (de lectura y/o de escritura) específicos de la aplicación de sus socios o sistemas de socio 3, respectivamente, y sus entidades asociadas, por ejemplo, sistemas de extremo posterior específicos de la aplicación y dispositivos de transacción 6 (entidades de transacción).

Como se ilustra en la figura 2, los dispositivos de comunicación móvil 2 comprenden cada uno un procesador 20 y, conectados al procesador 20, una interfaz de comunicación inalámbrica 21 y un almacén de programas/datos con un área segura 22. La interfaz de comunicación inalámbrica 21 está configurada para la comunicación de datos inalámbrica de corto alcance con dispositivos de transacción 6 dispuestos externamente al dispositivo de comunicación móvil 2, por ejemplo, lectores de tarjetas con una interfaz de comunicación inalámbrica 21 correspondiente. Por ejemplo, la interfaz de comunicación inalámbrica 21 comprende un módulo de comunicación de campo cercano (NFC), por ejemplo, basándose en normas de RFID existentes tales como ISO/IEC 14443 e ISO/IEC 18092 para un alcance de unas pocas pulgadas, y/o un módulo de comunicación de Bluetooth (definido originalmente en IEEE 802.15.1) para un alcance de unos pocos metros. Como se ilustra adicionalmente en la figura 2, en el área segura 22 está almacenado un módulo de emulación de tarjetas 220. El módulo de emulación de tarjetas 220 comprende un módulo de programa 221 y datos de aplicación 222.

Además de los datos de aplicación asociados con las aplicaciones de tarjetas sin contacto descritas anteriormente,

los datos de aplicación 222 del módulo de emulación de tarjetas 220 comprenden adicionalmente datos de estructura de datos de aplicación 223 asociados con las aplicaciones de tarjetas sin contacto. Los datos de estructura de datos de aplicación 223 definen para una o más aplicaciones de tarjetas sin contacto específicas la estructura de datos respectiva usada para organizar y almacenar el contenido de datos de aplicación 224 real de la aplicación de tarjetas sin contacto. El contenido de datos de aplicación 224 real incluye valores numéricos, alfanuméricos y criptográficos a los que accede la aplicación de tarjetas sin contacto, o son almacenados y/o procesados por la misma. Dicho de otra forma, los datos de estructura de datos de aplicación 223 definen el sistema de archivos para una aplicación de tarjetas sin contacto específica. Los datos de aplicación 222 del módulo de emulación de tarjetas 220 comprenden adicionalmente identificadores de aplicación e indicaciones de tiempo asignados a los datos de aplicación de las diferentes aplicaciones de tarjetas sin contacto. Dependiendo del escenario o la realización, en lugar del contenido de datos de aplicación 224 real, para al menos una aplicación de tarjetas sin contacto, los datos de aplicación 222 del módulo de emulación de tarjetas 220 comprenden un puntero a datos de aplicación almacenados en una base de datos de tarjetas 13 del sistema informático 1, según es indicado por los datos de estructura de datos 223. Debido a que el módulo de emulación de tarjetas 220 comprende datos de aplicación 222 para una pluralidad de aplicaciones diferentes, el módulo de emulación de tarjetas 220 comprende datos de derechos de acceso específicos de la aplicación. Los datos de derechos de acceso específicos de la aplicación se almacenan como parte de los datos de aplicación 222 de la aplicación respectiva, por ejemplo, en el encabezamiento de un segmento, registro de datos o archivo de datos de la aplicación respectiva. Dicho de otra forma, los datos de aplicación 222 comprenden, para cada una de las aplicaciones soportadas por el módulo de emulación de tarjetas 220, un segmento, registro de datos o archivo de datos respectivo que incluye los datos de derechos de acceso específicos de la aplicación. Los datos de derechos de acceso específicos de la aplicación definen para una entidad solicitante con una clave de acceso específica de la aplicación correspondiente los derechos reales para leer y/o escribir los datos de aplicación de una aplicación particular. Dependiendo de la realización, el derecho real de una entidad solicitante para leer y/o escribir los datos de aplicación de una aplicación particular soportada por el módulo de emulación de tarjetas 220 se determina a partir de los datos de derechos de acceso específicos de la aplicación incluidos en el segmento, registro de datos o archivo de datos de la aplicación respectiva en los datos de aplicación 222 y a partir de la clave de acceso específica de la aplicación proporcionada por la entidad solicitante, por ejemplo, basándose en una comparación simple o usando una función criptográfica. Para un intercambio de datos seguro, el módulo de emulación de tarjetas 220 usa un cifrado de datos tal como AES 128, AES 256, 3DES o similares.

El módulo de programa 221 comprende un código de programa informático configurado para controlar el procesador 20 del dispositivo de comunicación móvil 2 para emular un módulo de tarjeta sin contacto y para ejecutar transacciones de datos a través de una interfaz de comunicación inalámbrica de corto alcance 21 del dispositivo de comunicación móvil 2. En concreto, el módulo de emulación de tarjetas 220 o su módulo de programa 221 están configurados para controlar el procesador 20 para emular las funciones de una tarjeta inteligente implementada en hardware, es decir, una tarjeta de chip o una tarjeta de circuito integrado que comprende un procesador y memoria (RAM, ROM), por ejemplo, una tarjeta de RFID para interactuar con un lector de tarjetas de acuerdo con un protocolo de NFC o de RFID normalizado como se define en normas tales como ISO 18092, ISO 21481, ISO 15693 o ISO 14443, o de acuerdo con un protocolo de NFC, de RFID o de transmisión de datos patentado.

En particular, el módulo de emulación de tarjetas 220 o su módulo de programa 221, respectivamente, está configurado para controlar el procesador 20 para acceder a los datos de aplicación 222, en concreto, para leer y/o escribir el contenido de datos de aplicación 224 de una aplicación de tarjetas sin contacto específica usando los datos de estructura de datos de aplicación 223 respectivos. En el contexto de una aplicación de tarjetas sin contacto, el módulo de emulación de tarjetas 220 o su módulo de programa 221 está configurado para controlar el procesador 20 para ejecutar transacciones de datos con un dispositivo de transacción externo 6 a través de la interfaz de comunicación inalámbrica de corto alcance 21 del dispositivo de comunicación móvil 2, usando los datos de aplicación 222 asociados con la aplicación de tarjetas sin contacto respectiva.

En una realización, el módulo de emulación de tarjetas 220 o su módulo de programa 221, respectivamente, está configurado para controlar el procesador 20 para ejecutar con el dispositivo de transacción externo 6 a través de la interfaz de comunicación inalámbrica de corto alcance 21 una transacción de actualización de tarjeta, recibiendo código de programa informático para actualizar el código de programa informático del módulo de emulación de tarjetas 220. Para ese fin, el módulo de programa 221 tiene una parte fija y una parte variable, de tal modo que la parte fija está configurada para ejecutar la transacción de actualización de tarjeta para añadir, sustituir y/o eliminar al menos parte del código de programa informático de la parte variable.

Como se ha mencionado anteriormente y se ha ilustrado en la figura 1, el sistema informático 1 comprende una base de datos de tarjetas 13 configurada para almacenar, para una pluralidad de dispositivos de comunicación móvil 2, una representación 14 del módulo de emulación de tarjetas 220 implementado en el dispositivo de comunicación móvil 2 respectivo. Como se muestra a continuación en la tabla 1, cada representación 14 incluye un identificador de tarjeta único para identificar la tarjeta, información acerca del módulo de programa 221 y datos de aplicación 222 de un módulo de emulación de tarjetas 220. En concreto, la representación 14 incluye una copia del código de programa informático del módulo de programa 221 y/o un identificador de programa que identifica el programa y su versión y, por lo tanto, el código de programa informático del módulo de programa 221 (en este último caso, el identificador de programa se refiere a una copia del código de programa informático real del módulo de programa 221 respectivo que

se almacena en el sistema informático 1). Además, la representación 14 incluye una copia de los datos de estructura de datos de aplicación 223 y/o un identificador de aplicación que identifica la aplicación de tarjetas sin contacto y la estructura de datos de sus datos de aplicación, y una copia del contenido de datos de aplicación 224 real y los datos de derechos de acceso específicos de la aplicación, por ejemplo, en el encabezamiento del segmento, registro de datos o archivo de datos que contiene el contenido de datos de aplicación 224 de la aplicación respectiva. La representación 14 de un módulo de emulación de tarjetas 220 específico y/o su identificador de tarjeta, respectivamente, se almacenan en la base de datos de tarjetas 13 asignada al dispositivo de comunicación móvil 2 respectivo y/o a un abonado o usuario específico. Por ejemplo, los módulos de emulación de tarjetas 220 y/o los dispositivos de comunicación móvil 2 se identifican por medio de un Identificador de Equipo Móvil Internacional (IMEI). Por ejemplo, el abonado o usuario específico se identifica por medio de un Identificador de Abonado Móvil Internacional (IMSI) y se asocia con información de abonado o de usuario adicional, tal como nombre, dirección, Número de ISDN de Abonado Móvil (MSISDN), etc. La base de datos de tarjetas 13 comprende adicionalmente indicaciones de tiempo asignadas a los datos de aplicación de las diferentes aplicaciones de tarjetas sin contacto.

Tabla 1

Representación de un módulo de emulación de tarjetas de un dispositivo de comunicación móvil específico				
Identificador de tarjeta	Módulo de programa	Identificador de programa	Código de programa	
			Código de programa de la parte fija	Código de programa de la parte variable
	Datos de aplicación A	Identificador de aplicación A	Estructura de datos de los datos de aplicación A	Contenido de datos de aplicación A
	...	...	...	...
	Datos de aplicación N	Identificador de aplicación N	Estructura de datos de los datos de aplicación N	Contenido de datos de aplicación N

El sistema informático 1 comprende adicionalmente un sistema de software 10 que incluye un código de programa informático configurado para controlar el procesador o procesadores 12 del sistema informático 1 para ejecutar diversas funciones como se describe a continuación con más detalle. Por medio del sistema de software 10, el procesador o procesadores 12 del sistema informático 1 se controlan y, por lo tanto, se configuran para mantener la base de datos de tarjetas 13 y las representaciones 14 de los módulos de emulación de tarjetas 220. Además, el sistema de software 10 o su procesador o procesadores 12, respectivamente, está o están configurados para procesar solicitudes relacionadas con la tarjeta y/o la aplicación recibidas por el módulo de comunicación 11 a través de una red de telecomunicaciones 4, 5 desde dispositivos de comunicación móvil 2 autorizados, sistemas de socio 3 autorizados y/o sistemas informáticos relacionados con la aplicación autorizados asociados con los sistemas de socio 3, por ejemplo, dispositivos de transacción 6, tales como lectores de tarjetas, o servidores de aplicaciones informatizados conectados a los dispositivos de transacción 6 y/o las redes de telecomunicaciones 4, 5.

Las solicitudes procedentes de los sistemas de socio 3 incluyen solicitudes de escritura con datos de aplicación para uno o más dispositivos de comunicación móvil 2 (incluyendo datos de derechos de acceso específicos de la aplicación), solicitudes de lectura para leer datos de aplicación desde uno o más dispositivos de comunicación móvil 2 y solicitudes de actualización del módulo de emulación de tarjetas 220, en particular el módulo de programa 221 respectivo, de uno o más dispositivos de comunicación móvil 2. Las solicitudes de escritura incluyen solicitudes para descargar datos de aplicación adicionales en el módulo de emulación de tarjetas 220, actualizar datos de aplicación 222 en el módulo de emulación de tarjetas 220 y eliminar datos de aplicación 222 en el módulo de emulación de tarjetas 220.

Las solicitudes desde un dispositivo de comunicación móvil 2 o un sistema informático relacionado con la aplicación asociado con un sistema de socio 3 incluyen solicitudes relacionadas con realizar operaciones de datos de aplicación para el módulo de emulación de tarjetas 220 del dispositivo de comunicación móvil 2 respectivo, y solicitudes relacionadas con actualizar el módulo de emulación de tarjetas 220, en particular el módulo de programa 221 respectivo, del dispositivo de comunicación móvil 2 respectivo. Las operaciones de datos de aplicación incluyen descargar datos de aplicación adicionales en el módulo de emulación de tarjetas 220, actualizar datos de aplicación 222 en el módulo de emulación de tarjetas 220 y eliminar datos de aplicación 222 en el módulo de emulación de tarjetas 220.

Tabla 2

Solicitante	Solicitud	Operación	Fuente de datos	Sumidero de datos
Sistema de socio (o entidad asociada)	Escribir	Descargar datos de aplicación nuevos en el módulo de emulación de tarjetas	Sistema de socio a través del sistema informático	Uno o más dispositivos de comunicación móvil
		Actualizar datos de aplicación en el módulo de emulación de tarjetas		
		Eliminar datos de aplicación en el módulo de emulación de tarjetas	-	
	Leer	Leer datos de aplicación desde el módulo de emulación de tarjetas	Uno o más dispositivos de comunicación móvil	Sistema informático, sistema de socio
	Actualizar	Actualizar módulo de programa del módulo de emulación de tarjetas	Sistema de socio a través del sistema informático	Uno o más dispositivos de comunicación móvil

La tabla 2 anterior da una visión general de diversas solicitudes desde un sistema de socio 3 y las operaciones y entidades asociadas:

- 5 La tabla 3 siguiente da una visión general de diversas solicitudes desde un dispositivo de comunicación móvil 2 y las operaciones y entidades asociadas:

Tabla 3

Solicitante	Solicitud	Operación	Fuente de datos	Sumidero de datos
Dispositivo de comunicación móvil	Operación de datos de aplicación	Descargar datos de aplicación nuevos en el módulo de emulación de tarjetas	Sistema informático	Dispositivo de comunicación móvil respectivo
		Actualizar datos de aplicación en el módulo de emulación de tarjetas		
		Eliminar datos de aplicación en el módulo de emulación de tarjetas	-	
	Actualizar	Actualizar módulo de programa del módulo de emulación de tarjetas	Sistema informático	Dispositivo de comunicación móvil respectivo

¹ Actualización de base de datos de tarjetas y sistema de socio no incluida

- 10 La tabla 4 siguiente da una visión general de diversas solicitudes desde un dispositivo de transacción 6 y las operaciones y entidades asociadas:

Tabla 4

Solicitante	Solicitud	Operación	Fuente de datos	Sumidero de datos ¹
Dispositivo de transacción	Escribir	Escribir datos de aplicación nuevos en el módulo de emulación de tarjetas	Dispositivo de transacción	Dispositivo de comunicación móvil respectivo
		Actualizar datos de aplicación en el módulo de emulación de tarjetas		
		Eliminar datos de aplicación en el módulo de emulación de tarjetas	-	
	Leer	Leer datos de aplicación desde el módulo de emulación de tarjetas	Dispositivo de comunicación móvil respectivo	Dispositivo de transacción
	Actualizar	Actualizar módulo de programa del módulo de emulación de tarjetas	Sistema informático	Dispositivo de comunicación móvil respectivo

¹ Actualización de base de datos de tarjetas y sistema de socio no incluida

- 15 En los siguientes párrafos se describen, con referencia a la figura 3, secuencias posibles de etapas realizadas por el sistema informático 1, el dispositivo o dispositivos de comunicación 2, el sistema o sistemas de socio 3 y el dispositivo

o dispositivos de transacción 6 u otro sistema o sistemas informáticos relacionados con la aplicación asociados con el sistema o sistemas de socio 3.

5 En la etapa preparatoria S0, socios autorizados o los sistemas de socio 3 respectivos, respectivamente, se establecen y se registran en el sistema informático 1. Por ejemplo, el sistema de software 10 genera elementos de autorización criptográficos, por ejemplo claves de autorización, para los socios respectivos o sus sistemas de socio 3, respectivamente. Dependiendo del escenario y/o de la configuración, los elementos de autorización se refieren a una o más aplicaciones de tarjetas sin contacto que están gobernadas y/o que son proporcionadas por el socio o sistema de socio 3 respectivo, u otros sistemas informáticos asociados con el sistema de socio 3. Por lo tanto, por medio de los elementos de autorización, el socio respectivo está autorizado a acceder y a modificar datos de aplicación de una o más aplicaciones de tarjetas sin contacto gestionadas por el sistema informático 1. El sistema de software 10 registra los socios autorizados y sus elementos de autorización en el sistema informático 1.

15 En la etapa S1, un socio autorizado almacena datos de aplicación en el sistema informático 1. En concreto, después de la autenticación de los elementos de autorización, el sistema de software 10 recibe y acepta del sistema de socio 3 una solicitud para almacenar datos de aplicación para una aplicación de tarjetas sin contacto particular, implementada en un módulo de emulación de tarjetas 220 de uno o más dispositivos de comunicación móvil 2. El sistema de software 10 almacena la solicitud de la aplicación de tarjetas sin contacto particular junto con los datos de aplicación en el sistema informático 1. El sistema de software 10 devuelve al sistema de socio 3 respectivo un recibo de la solicitud de escritura. La escritura real de los datos de aplicación en el módulo de emulación de tarjetas 220 de uno o más dispositivos de comunicación móvil 2 se describirá más adelante en el contexto de la etapa S3. En una realización, el sistema de software 10 genera para la aplicación de tarjetas sin contacto particular claves de acceso específicas de la aplicación, que representan derechos de acceso (de lectura y/o de escritura) específicos de la aplicación para el socio o sistema de socio 3 respectivo, u otros sistemas informáticos asociados con el sistema de socio 3, por ejemplo, sistemas de extremo posterior específicos de la aplicación y dispositivos de transacción 6, para leer y/o escribir los datos de aplicación de la aplicación de tarjetas sin contacto particular. Además, el sistema de software 10 genera los datos de derechos de acceso específicos de la aplicación correspondientes para controlar el acceso de lectura y/o de escritura a datos de aplicación de la aplicación de tarjetas sin contacto particular. Mientras que las claves de acceso específicas de la aplicación se transfieren de forma segura a aquellas entidades que están autorizadas a acceder a datos de aplicación de la aplicación de tarjetas sin contacto respectiva, los datos de derechos de acceso específicos de la aplicación correspondientes se almacenan con los datos de aplicación de la aplicación de tarjetas sin contacto respectiva, es decir, en el módulo de emulación de tarjetas 220.

35 En la etapa S2, el sistema informático 1 instala un módulo de emulación de tarjetas 220 en el dispositivo de comunicación móvil 2. Dependiendo del escenario o la realización, la instalación del módulo de emulación de tarjetas se inicia por solicitud del dispositivo de comunicación móvil 2, el sistema informático 1, el sistema de socio 3, un dispositivo de transacción 6 que interacciona con el dispositivo de comunicación móvil 2 u otro sistema informático relacionado con la aplicación autorizado asociado con el sistema de socio 3. En concreto, el sistema de software 10 transfiere el módulo de emulación de tarjetas al dispositivo de comunicación móvil 2. El módulo de emulación de tarjetas se transfiere por aire a través de la red de telecomunicaciones 5, o a través de la ruta de comunicación 8 a través de la interfaz de comunicación inalámbrica del dispositivo de transacción 6 que interacciona con el dispositivo de comunicación móvil 2. En su solicitud de almacenar el módulo de emulación de tarjetas 220 en un área segura 22 de un almacén de datos del dispositivo de comunicación móvil 2, el sistema de software 10 incluye una clave de acceso de área. Tras la verificación de la clave de acceso de área, dirigida por el código de programa de un módulo de control, el procesador 20 del dispositivo de comunicación móvil 2 almacena el módulo de emulación de tarjetas 220 en el área segura 22. Como se ha descrito anteriormente, el módulo de emulación de tarjetas 220 incluye el módulo de programa 221. Dependiendo del escenario y/o la realización, el módulo de emulación de tarjetas 220 incluye al menos algunos datos de aplicación 222 cuando este se transfiere y se instala en el dispositivo de comunicación móvil 2, o los datos de aplicación 222 se transfieren posteriormente en una etapa separada. Como se ha descrito anteriormente, los datos de aplicación escritos en el módulo de emulación de tarjetas 220 comprenden adicionalmente para cada aplicación datos de derechos de acceso específicos de la aplicación que se incluyen como parte de los datos de aplicación de una aplicación particular, por ejemplo, en el encabezamiento de un segmento, registro de datos o archivo de datos de los datos de aplicación de la aplicación particular. Los datos de derechos de acceso se usan posteriormente para controlar el acceso de lectura y/o de escritura a los datos de aplicación de una aplicación particular, es decir, el derecho a leer y/o escribir datos desde o en el segmento, registro de datos o archivo de datos que contiene los datos de aplicación de la aplicación particular. Tras la instalación con éxito del módulo de emulación de tarjetas 220, el procesador 20 devuelve al sistema informático 1 un mensaje de confirmación de instalación.

60 En la etapa S20, tras recibir un mensaje de confirmación de instalación afirmativa, el sistema de software 10 almacena en la base de datos de tarjetas 13 una representación 14 actualizada del módulo de emulación de tarjetas 220 instalado en el dispositivo de comunicación móvil 2 respectivo. En particular, la representación 14 se corresponde con la versión del módulo de programa 221 y, si es aplicable, los datos de estructura de datos de aplicación 223 y el contenido de datos de aplicación 224 de los datos de aplicación 222 en el módulo de emulación de tarjetas 220 (incluyendo los datos de derechos de acceso específicos de la aplicación). Dependiendo de la realización y/o el contexto, el sistema de software 10 reenvía un mensaje de confirmación de instalación relacionado al sistema de socio 3 respectivo que solicitó la instalación del módulo de emulación de tarjetas.

En la etapa S3, el sistema informático 1 escribe datos de aplicación (nuevos, adicionales o de modificación) en el módulo de emulación de tarjetas 220 del dispositivo de comunicación móvil 2. Como se ha descrito anteriormente, los datos de aplicación escritos en el módulo de emulación de tarjetas 220 incluyen datos de estructura de datos de aplicación 223 que indican la estructura de datos de los datos de aplicación asociados con una aplicación de tarjetas sin contacto particular o un puntero a la base de datos de tarjetas 13 del sistema informático 1. Por lo tanto, dependiendo del escenario y/o la realización, los datos de aplicación escritos en el módulo de emulación de tarjetas 220 comprenden adicionalmente el contenido de datos de aplicación real o el puntero real a datos de aplicación almacenados en la base de datos de tarjetas 13 del sistema informático 1. Dependiendo del escenario o la realización, la escritura de los datos de aplicación en el módulo de emulación de tarjetas 220 se inicia por solicitud del dispositivo de comunicación móvil 2, el sistema informático 1 (por ejemplo, correspondiente a una solicitud almacenada y pendiente recibida del sistema de socio 3), el sistema de socio 3, el dispositivo de transacción 6 que interacciona con el dispositivo de comunicación móvil 2 u otro sistema informático relacionado con la aplicación autorizado asociado con el sistema de socio 3. En concreto, el sistema de software 10 transfiere los datos de aplicación al dispositivo de comunicación móvil 2. Los datos de aplicación se transfieren por aire a través de la red de telecomunicaciones 5, o a través de la ruta de comunicación 8 a través de la interfaz de comunicación inalámbrica del dispositivo de transacción 6 que interacciona con el dispositivo de comunicación móvil 2. En su solicitud de almacenar los datos de aplicación en el módulo de emulación de tarjetas 220, el sistema de software 10 incluye una clave de acceso de aplicación. En concreto, para escribir contenido de datos de aplicación en el módulo de emulación de tarjetas 220, el sistema de software 10 incluye una clave de acceso específica de la aplicación en la solicitud de escritura. La clave de acceso específica de la aplicación es proporcionada por la entidad que inicia la solicitud de escritura (el dispositivo de comunicación móvil 2, el sistema informático 1, el sistema de socio 3, el dispositivo de transacción 6 u otro sistema informático relacionado con la aplicación autorizado asociado con el sistema de socio 3, por ejemplo, un sistema de extremo posterior específico de la aplicación) y/o por el sistema informático 1 en nombre de la entidad iniciadora, tras la autorización con éxito de esa entidad por el sistema informático 1 basándose en otros elementos de autorización proporcionados por la entidad iniciadora. Tras la verificación de la clave de acceso de aplicación, dirigida por el código de programa del módulo de programa 221, el procesador 20 del dispositivo de comunicación móvil 2 almacena los datos de aplicación en el módulo de emulación de tarjetas 220. En concreto, el módulo de emulación de tarjetas 220 o el procesador 20 según lo dirigido por el módulo de programa 221, respectivamente, verifica la autorización para la solicitud de escritura basándose en la clave de acceso específica de la aplicación recibida y los datos de derechos de acceso específicos de la aplicación almacenados en el módulo de emulación de tarjetas 220 como parte de los datos de aplicación 222 respectivos de la aplicación particular. Tras el almacenamiento con éxito de los datos de aplicación 222 en el módulo de emulación de tarjetas 220, el procesador 20 devuelve al sistema informático 1 un mensaje de confirmación de escritura, por ejemplo, a través de la misma ruta de comunicación usada para la solicitud de escritura.

En la etapa S30, tras recibir un mensaje de confirmación de escritura afirmativa, el sistema de software 10 almacena en la base de datos de tarjetas 13 una representación 14 actualizada de los datos de aplicación asociados con el módulo de emulación de tarjetas instalado en el dispositivo de comunicación móvil 2 respectivo. En particular, la representación 14 se corresponde con los datos de estructura de datos de aplicación y el contenido de datos de aplicación que o bien están almacenados en el módulo de emulación de tarjetas 220 o bien son referenciados por el puntero del módulo de emulación de tarjetas 220. Dependiendo de la realización y/o el contexto, el sistema de software 10 reenvía un mensaje de confirmación de escritura relacionado al sistema de socio 3 respectivo que solicitó la escritura de los datos de aplicación.

En la etapa S4, el sistema informático 1 lee los datos de aplicación 222 en el módulo de emulación de tarjetas 220 en el dispositivo de comunicación móvil 2. Dependiendo del escenario o la realización, la lectura de los datos de aplicación 222 en el módulo de emulación de tarjetas 220 se inicia por solicitud del sistema informático 1, el sistema de socio 3, el dispositivo de transacción 6 que interacciona con el dispositivo de comunicación móvil 2 u otro sistema informático relacionado con la aplicación autorizado asociado con el sistema de socio 3. En concreto, el sistema de software 10 transfiere una solicitud de lectura al dispositivo de comunicación móvil 2. La solicitud de lectura se transfiere por aire a través de la red de telecomunicaciones 5, o a través de la ruta de comunicación 8 a través de la interfaz de comunicación inalámbrica del dispositivo de transacción 6 que interacciona con el dispositivo de comunicación móvil 2. En su solicitud de lectura, el sistema de software 10 incluye una clave de acceso de aplicación. En concreto, para leer contenido de datos de aplicación desde el módulo de emulación de tarjetas 220, el sistema de software 10 incluye una clave de acceso específica de la aplicación en la solicitud de lectura. La clave de acceso específica de la aplicación es proporcionada por la entidad que inicia la solicitud de lectura (el dispositivo de comunicación móvil 2, el sistema informático 1, el sistema de socio 3, el dispositivo de transacción 6 u otro sistema informático relacionado con la aplicación autorizado asociado con el sistema de socio 3, por ejemplo, un sistema de extremo posterior específico de la aplicación) y/o por el sistema informático 1 en nombre de la entidad iniciadora, tras la autorización con éxito de esa entidad por el sistema informático 1 basándose en otros elementos de autorización proporcionados por la entidad iniciadora. Tras la verificación de la clave de acceso de aplicación, dirigida por el código de programa del módulo de programa 221, el procesador 20 del dispositivo de comunicación móvil 2 lee los datos de aplicación 222 en el módulo de emulación de tarjetas 220 y devuelve al sistema informático 1 un mensaje de respuesta de lectura, por ejemplo, a través de la misma ruta de comunicación usada para la solicitud de lectura. En concreto, el módulo de emulación de tarjetas 220 o el procesador 20 según lo dirigido por el módulo de programa 221, respectivamente, verifica la autorización para la solicitud de lectura basándose en la clave de acceso específica de la aplicación recibida y los

datos de derechos de acceso específicos de la aplicación almacenados en el módulo de emulación de tarjetas 220 como parte de los datos de aplicación 222 respectivos de la aplicación particular. Dependiendo del escenario y/o la realización, los datos de aplicación 222 leídos desde el módulo de emulación de tarjetas 220 e incluidos en la respuesta de lectura comprenden la estructura de datos real 223 y el contenido de datos de aplicación 224, o el puntero a datos de aplicación almacenados en la base de datos de tarjetas 13 del sistema informático 1. En caso de que los datos de aplicación simplemente incluyan un puntero, el sistema de software 10 usa el puntero para leer los datos de aplicación almacenados en la base de datos de tarjetas 13 del sistema informático 1 y devuelve los datos de aplicación leídos en una respuesta de lectura a la entidad que inició la solicitud de lectura.

En la etapa S40, tras recibir el mensaje de respuesta de lectura con la estructura de datos real y el contenido de datos de aplicación incluidos, el sistema de software 10 verifica si los datos de aplicación leídos desde el módulo de emulación de tarjetas 220 están actualizados u obsoletos. Para ese fin, el sistema de software 10 compara indicaciones de tiempo de los datos de aplicación leídos desde el módulo de emulación de tarjetas 220 del dispositivo de comunicación móvil 2 con indicaciones de tiempo correspondientes de los datos de aplicación almacenados en la representación 14 del módulo de emulación de tarjetas en la base de datos de tarjetas 13. Si las indicaciones de tiempo indican que los datos de aplicación leídos desde el dispositivo de comunicación móvil 2 indican una versión obsoleta, es decir, una indicación de tiempo más antigua, el sistema de software 10 actualiza los datos de aplicación 222 en el módulo de emulación de tarjetas 220 del dispositivo de comunicación móvil 2. En concreto, el sistema de software 10 transfiere los datos de aplicación respectivos almacenados en la base de datos de tarjetas 13 al módulo de emulación de tarjetas 220 del dispositivo de comunicación móvil 2, como se ha descrito anteriormente en el contexto de la operación de escritura, por ejemplo, a través de la misma ruta de comunicación usada para la solicitud de lectura. Por otro lado, si las indicaciones de tiempo indican que los datos de aplicación respectivos almacenados en la base de datos de tarjetas 13 están obsoletos, es decir, estos tienen una indicación de tiempo más antigua que los datos de aplicación leídos desde el dispositivo de comunicación móvil 2, el sistema de software 10 actualiza los datos de aplicación almacenados en la base de datos de tarjetas 13. Por lo tanto, el sistema de software 10 almacena los datos de aplicación 222 leídos desde el módulo de emulación de tarjetas 220 del dispositivo de comunicación móvil 2 en la base de datos de tarjetas 13, en concreto en la representación 14 del módulo de emulación de tarjetas respectivo (incluyendo los datos de derechos de acceso específicos de la aplicación).

En la etapa S5, el sistema informático 1 actualiza el módulo de emulación de tarjetas 220 del dispositivo de comunicación móvil 2, en concreto, el módulo de programa 221 del módulo de emulación de tarjetas 220. Dependiendo del escenario o la realización, la actualización del módulo de programa 221 se inicia por solicitud del dispositivo de comunicación móvil 2, el sistema informático 1 (por ejemplo, correspondiente a una solicitud almacenada y pendiente recibida del sistema de socio 3), el sistema de socio 3, el dispositivo de transacción 6 que interacciona con el dispositivo de comunicación móvil 2 u otro sistema informático relacionado con la aplicación autorizado asociado con el sistema de socio 3. En un escenario o realización, el sistema de software 10 actualiza el módulo de programa 221 reinstalando el módulo de programa 221, como se ha descrito anteriormente en el contexto de la etapa S2, usando una clave de acceso de área y sobrescribiendo el módulo de programa 221 pero manteniendo los datos de aplicación, o sobrescribiendo el módulo de programa 221 y los datos de aplicación 222. En otro escenario o realización, el módulo de programa 221 se actualiza realizando una transacción de actualización de tarjeta que actualiza solo una parte variable del módulo de programa 221. Este último enfoque es particularmente útil cuando la transacción de actualización de tarjeta es realizada por el dispositivo de transacción externo 6 a través de la interfaz de comunicación inalámbrica de corto alcance 21. Tras la verificación de una clave de actualización proporcionada por el dispositivo de transacción 6, la parte fija del módulo de programa 221 dirige al procesador 20 del dispositivo de comunicación móvil 2 para recibir y almacenar la nueva parte variable del módulo de programa 221 en el módulo de emulación de tarjetas 220. Tras la actualización con éxito del módulo de programa 221, el procesador 20 devuelve al sistema informático 1 un mensaje de actualización de tarjeta, por ejemplo, a través de la misma ruta de comunicación usada para la solicitud de actualización.

En la etapa S50, tras recibir un mensaje de actualización de tarjeta afirmativa, el sistema de software 10 almacena en la base de datos de tarjetas 13 una representación 14 actualizada del módulo de emulación de tarjetas 220 instalado en el dispositivo de comunicación móvil 2 respectivo. En particular, la representación 14 se corresponde con la versión del módulo de programa 221 y, si es aplicable, los datos de estructura de datos de aplicación 223 y el contenido de datos de aplicación 224 del módulo de emulación de tarjetas 220, e incluye los datos de derechos de acceso específicos de la aplicación.

En la figura 3, los números de referencia S6 y S7 se refieren a la ejecución de una transacción de datos relacionada con una aplicación de tarjetas sin contacto o una actualización del módulo de emulación de tarjetas 220, es decir, una actualización del módulo de programa 221 y/o los datos de aplicación 222 como se ha descrito anteriormente con referencia a S5 y S50. Las transacciones de datos se ejecutan entre el módulo de emulación de tarjetas 220 del dispositivo de comunicación móvil 2 y el dispositivo de transacción 6, con la condición de que el módulo de emulación de tarjetas 220 y/o el dispositivo de transacción 6 estén autorizados para la aplicación de tarjetas sin contacto o actualización de tarjeta respectiva, respectivamente. Por ejemplo, el módulo de emulación de tarjetas 220 y/o el dispositivo de transacción 6 comprenden claves de acceso para acceder a los datos de aplicación asociados con la aplicación de tarjetas sin contacto respectiva, o una clave de autorización para actualizar el módulo de emulación de tarjetas 220, respectivamente. Como se ha descrito anteriormente, el módulo de emulación de tarjetas 220 comprende

datos de derechos de acceso específicos de la aplicación almacenados como parte de los datos de aplicación 222 de la aplicación respectiva. La autorización del dispositivo de transacción 6 para acceder a los datos de aplicación 222 de la aplicación particular se determina basándose en la clave de acceso específica de la aplicación recibida desde el dispositivo de transacción 6 y los datos de derechos de acceso específicos de la aplicación almacenados con los datos de aplicación 222 de la aplicación particular.

Se debería hacer notar que el sistema informático 1 gestiona y mantiene los derechos de acceso (de lectura y/o de escritura) con respecto a aplicaciones de tarjetas sin contacto y datos de aplicación relacionados, no solo para sus socios o sistemas de socio 3, respectivamente, sino también para sus entidades, dispositivos de transacción 6 y usuarios asociados.

El número de referencia S6 se refiere a ejecutar una transacción de datos *fuera de línea*, usando datos de aplicación 222 almacenados en el módulo de emulación de tarjetas 220 del dispositivo de comunicación móvil 2. En el proceso de ejecución de la transacción de datos fuera de línea, el módulo de programa 221 del módulo de emulación de tarjetas 220 transfiere datos de aplicación 222 del módulo de emulación de tarjetas 220 a través de la interfaz de comunicación inalámbrica 7 al dispositivo de transacción 6, y recibe y almacena datos de aplicación desde el dispositivo de transacción 6 en el módulo de emulación de tarjetas 220.

En la etapa S60, el sistema de software 10 almacena en la base de datos de tarjetas 13 una representación actualizada 14 del módulo de emulación de tarjetas 220 instalado en el dispositivo de comunicación móvil 2 respectivo, como se ha descrito anteriormente con referencia a S50. Dependiendo de la realización o el escenario, un mantenimiento de una representación 14 actualizada del módulo de emulación de tarjetas 220 es realizado periódicamente por el sistema de software 10, en respuesta a una solicitud de actualización desde un sistema de socio 3, o en respuesta a una solicitud de actualización o mensaje de compleción de transacción desde el dispositivo de transacción 6 implicado en la transacción de datos fuera de línea.

El número de referencia S7 se refiere a ejecutar una transacción de datos *en línea*, usando datos de aplicación almacenados en la base de datos de tarjetas 13 del sistema informático 1. En el proceso de ejecución de la transacción de datos fuera de línea, el módulo de programa 221 del módulo de emulación de tarjetas 220 usa un puntero de datos de aplicación del módulo de emulación de tarjetas 220 para recuperar los datos de aplicación respectivos de la representación 14 del módulo de emulación de tarjetas en la base de datos de tarjetas 13 del sistema informático 1. Por lo tanto, los datos de aplicación que se van a transferir desde el módulo de emulación de tarjetas 220 al dispositivo de transacción 6 se recuperan en primer lugar a través de la red de telecomunicaciones 5 de la base de datos de tarjetas 13 del sistema informático 1. De forma recíproca, los datos de aplicación recibidos por el módulo de emulación de tarjetas 220 desde el dispositivo de transacción 6 se transfieren a través de la red de telecomunicaciones 5 a la base de datos de tarjetas 13 del sistema informático 1, en donde se almacenan como datos de aplicación actualizados en la representación 14 del módulo de emulación de tarjetas 220 respectivo. En consecuencia, una representación 14 actualizada del módulo de emulación de tarjetas 220 instalado en el dispositivo de comunicación móvil 2 respectivo se mantiene en la base de datos de tarjetas 13 por el sistema de software 10. Para las transacciones de datos en línea, dependiendo de la realización, los datos de derechos de acceso específicos de la aplicación se almacenan con el puntero de datos de aplicación en el módulo de emulación de tarjetas 220 o con los datos de aplicación en la representación 14 del módulo de emulación de tarjetas en la base de datos de tarjetas 13 del sistema informático 1.

Se debería hacer notar que, en la descripción, el código de programa informático se ha asociado con módulos funcionales específicos y la secuencia de las etapas se ha presentado en un orden específico, un experto en la materia entenderá, sin embargo, que el código de programa informático se puede estructurar de manera diferente y que el orden de al menos algunas de las etapas se podría alterar sin apartarse del alcance de la invención.

REIVINDICACIONES

1. Un sistema (1) para gestionar datos de aplicación de diferentes aplicaciones de tarjetas sin contacto para una pluralidad de dispositivos de comunicación móvil (2), comprendiendo el sistema (1) uno o más procesadores (10) configurados para:

transferir a través de una red de telecomunicaciones (5) a uno de los dispositivos de comunicación móvil (2) un módulo de emulación de tarjetas, usando una clave de acceso de área para almacenar el módulo de emulación de tarjetas (220) en un área segura (22) del dispositivo de comunicación móvil (2), comprendiendo el módulo de emulación de tarjetas (220) un módulo de programa (221) con código de programa informático configurado para controlar un procesador (20) del dispositivo de comunicación móvil (2) para emular un módulo de tarjeta sin contacto controlando el procesador (20) para emular funciones de una tarjeta de circuito integrado implementada en hardware que tiene un procesador y una memoria, y para ejecutar transacciones de datos a través de una interfaz de comunicación inalámbrica de corto alcance (21) del dispositivo de comunicación móvil (2);
transferir datos de aplicación para varias aplicaciones de tarjetas sin contacto diferentes a través de la red de telecomunicaciones (5) al dispositivo de comunicación móvil (2) para almacenar los datos de aplicación (222) para las varias aplicaciones de tarjetas sin contacto diferentes en el módulo de emulación de tarjetas (220); y
mantener en el sistema (1) una base de datos de tarjetas (13), almacenando en la base de datos de tarjetas (13) para cada uno de la pluralidad de dispositivos de comunicación móvil (2) una representación (14) del módulo de emulación de tarjetas (220) almacenado en el dispositivo de comunicación móvil (2) respectivo, comprendiendo la representación (14) del módulo de emulación de tarjetas (220) los datos de aplicación (222) para las varias aplicaciones de tarjetas sin contacto diferentes del módulo de emulación de tarjetas (220) almacenado en el dispositivo de comunicación móvil (2) respectivo e información acerca del módulo de programa (221) del módulo de emulación de tarjetas (220) almacenado en el dispositivo de comunicación móvil (2) respectivo, incluyendo la información acerca del módulo de programa (221) al menos uno de: una copia del código de programa informático del módulo de programa (221) y un identificador de programa que identifica el código de programa informático del módulo de programa (221).

2. El sistema (1) de la reivindicación 1, en donde los procesadores (10) del sistema (1) están configurados adicionalmente para transferir datos de derechos de acceso específicos de la aplicación para una pluralidad de aplicaciones de tarjetas sin contacto a través de la red de telecomunicaciones (5) al dispositivo de comunicación móvil (2) para almacenar los datos de derechos de acceso específicos de la aplicación en el módulo de emulación de tarjetas (220), y para almacenar en el sistema (1) claves de acceso específicas de la aplicación para una pluralidad de aplicaciones de tarjetas sin contacto; y el módulo de emulación de tarjetas (220) comprende un código de programa informático configurado para controlar el procesador (20) del dispositivo de comunicación móvil (2) para ejecutar transacciones de datos a través de la interfaz de comunicación inalámbrica de corto alcance (21) del dispositivo de comunicación móvil (2), y para verificar la autorización de un socio de transacción para acceder a datos de aplicación almacenados en el módulo de emulación de tarjetas (220) para una aplicación de tarjetas sin contacto particular, basándose en los datos de derechos de acceso específicos de la aplicación, almacenados en el módulo de emulación de tarjetas (220) para la aplicación de tarjetas sin contacto particular, y una clave de acceso específica de la aplicación, recibida del socio de transacción a través de la interfaz de comunicación inalámbrica de corto alcance (21).

3. El sistema (1) de una de las reivindicaciones 1 o 2, en donde los datos de aplicación (222) almacenados en el módulo de emulación de tarjetas (220) del dispositivo de comunicación móvil (2) comprenden un puntero a datos de aplicación almacenados en la base de datos de tarjetas (13); y el módulo de emulación de tarjetas (220) comprende un código de programa informático configurado para controlar el procesador (20) del dispositivo de comunicación móvil (2) para recuperar los datos de aplicación de la base de datos de tarjetas (13) usando el puntero, y para ejecutar las transacciones de datos a través de la interfaz de comunicación inalámbrica de corto alcance (21) del dispositivo de comunicación móvil (2) usando datos de aplicación recuperados de la base de datos de tarjetas (13).

4. El sistema (1) de una de las reivindicaciones 1 a 3, en donde los procesadores (10) del sistema (1) están configurados adicionalmente para leer los datos de aplicación (222) almacenados en el módulo de emulación de tarjetas (220) de uno de los dispositivos de comunicación móvil (2), y para ejecutar al menos uno de: transferir desde el sistema (1) al dispositivo de comunicación móvil (2) datos de aplicación actualizados almacenados en la base de datos de tarjetas (13), en casos en los que los datos de aplicación (222) leídos del dispositivo de comunicación móvil (2) indican una versión obsoleta de los datos de aplicación, y actualizar en el sistema (1) la representación (14) del módulo de emulación de tarjetas (220) del dispositivo de comunicación móvil (2) almacenando en la base de datos de tarjetas (13) datos de aplicación (222) leídos desde el módulo de emulación de tarjetas (220) del dispositivo de comunicación móvil (2), en casos en los que los datos de aplicación (222) leídos del dispositivo de comunicación móvil (2) indican una versión más reciente de los datos de aplicación.

5. El sistema (1) de una de las reivindicaciones 1 a 4, en donde los procesadores (10) del sistema informático (1) están configurados adicionalmente para recibir a través de la red de telecomunicaciones (5) una solicitud relacionada con una aplicación de tarjetas sin contacto para realizar al menos una de las siguientes operaciones de datos de aplicación para el módulo de emulación de tarjetas (220) de uno o más dispositivos de comunicación móvil (2): descargar datos de aplicación adicionales en el módulo de emulación de tarjetas (220), actualizar datos de aplicación (222) en el módulo

de emulación de tarjetas (220) y eliminar datos de aplicación (222) en el módulo de emulación de tarjetas (220); para transferir una solicitud de datos de aplicación al módulo de emulación de tarjetas (220) del uno o más dispositivos de comunicación móvil (2) de acuerdo con la operación de datos de aplicación respectiva; y para actualizar en la base de datos de tarjetas (13) la representación (14) del módulo de emulación de tarjetas (220) del uno o más dispositivos de comunicación móvil (2) actualizando datos de aplicación en la base de datos de tarjetas (13) de acuerdo con la solicitud de datos de aplicación.

6. El sistema (1) de una de las reivindicaciones 1 a 5, en donde los procesadores (10) del sistema informático (1) están configurados adicionalmente para recibir a través de la red de telecomunicaciones (4) desde un sistema de socio (3) autorizado al menos uno de: una solicitud de escritura que incluye datos de aplicación para el módulo de emulación de tarjetas (220) de uno o más dispositivos de comunicación móvil (2), y una solicitud de lectura para leer datos de aplicación desde el módulo de emulación de tarjetas (220) de uno o más dispositivos de comunicación móvil (2); para transferir los datos de aplicación a través de la red de telecomunicaciones al módulo de emulación de tarjetas (220) del uno o más dispositivos de comunicación móvil (2), en caso de una solicitud de escritura; y para leer los datos de aplicación (222) almacenados en el módulo de emulación de tarjetas (220) del uno o más dispositivos de comunicación móvil (2), en caso de una solicitud de lectura; y para actualizar en el sistema (1) la representación (14) del módulo de emulación de tarjetas (220) del uno o más dispositivos de comunicación móvil (2) almacenando en la base de datos de tarjetas (13) los datos de aplicación (222) leídos o almacenados en el módulo de emulación de tarjetas (220) del uno o más dispositivos de comunicación móvil (2), respectivamente.

7. El sistema (1) de una de las reivindicaciones 1 a 6, en donde los procesadores (10) del sistema informático (1) están configurados adicionalmente para recibir a través de la red de telecomunicaciones (5) una solicitud relacionada con uno de los dispositivos de comunicación móvil (2), exigiendo la solicitud una actualización del módulo de emulación de tarjetas (220); para transferir un código de programa para el módulo de emulación de tarjetas (220) al dispositivo de comunicación móvil (2) de acuerdo con la solicitud; y para actualizar en la base de datos de tarjetas (13) la representación (14) de los módulos de emulación de tarjetas (220) de los dispositivos de comunicación móvil (2) almacenando en la base de datos de tarjetas (13) al menos uno de: un número de versión que indica la versión del código de programa transferido al dispositivo de comunicación móvil (2), y el código de programa transferido al dispositivo de comunicación móvil (2).

8. El sistema (1) de una de las reivindicaciones 1 a 7, en donde el módulo de emulación de tarjetas (220) comprende un código de programa informático configurado para controlar un procesador (20) del dispositivo de comunicación móvil (2) para ejecutar la transacción de datos a través de la interfaz de comunicación inalámbrica de corto alcance (21) del dispositivo de comunicación móvil (2) con un dispositivo de transacción externo (6), incluyendo la transacción de datos al menos uno de: una transacción de pago de débito, una transacción de pago de crédito, una transacción de pago de efectivo electrónico, una transacción de emisión de billetes, una transacción de control de acceso, una transacción de actualización de aplicación para actualizar los datos de aplicación (222) en el módulo de emulación de tarjetas (220), y una transacción de actualización de tarjeta para actualizar el código de programa informático del módulo de emulación de tarjetas (220); e incluyendo los datos de aplicación al menos uno de: datos de cuenta de débito, datos de cuenta de crédito, datos de efectivo electrónico, datos de billete electrónico, datos de derechos de acceso, datos de identificación de usuario, datos de autenticación de usuario y datos de estructura de datos de aplicación.

9. Un método implementado por ordenador para gestionar datos de aplicación de diferentes aplicaciones de tarjetas sin contacto para una pluralidad de dispositivos de comunicación móvil (2), comprendiendo el método:

transferir (S2) mediante un sistema informático (1) a través de una red de telecomunicaciones (5) a uno de los dispositivos de comunicación móvil (2) un módulo de emulación de tarjetas, usando una clave de acceso de área para almacenar el módulo de emulación de tarjetas (220) en un área segura (22) del dispositivo de comunicación móvil (2), comprendiendo el módulo de emulación de tarjetas (220) un módulo de programa (221) con código de programa informático, configurado para controlar un procesador (20) del dispositivo de comunicación móvil (2) para emular un módulo de tarjeta sin contacto controlando el procesador (20) para emular funciones de una tarjeta de circuito integrado implementada en hardware que tiene un procesador y una memoria, y para ejecutar transacciones de datos a través de una interfaz de comunicación inalámbrica de corto alcance (21) del dispositivo de comunicación móvil (2);

transferir (S3) mediante el sistema informático (1) a través de la red de telecomunicaciones (5) al dispositivo de comunicación móvil (2) datos de aplicación para varias aplicaciones de tarjetas sin contacto diferentes para almacenar los datos de aplicación (222) para las varias aplicaciones de tarjetas sin contacto diferentes en el módulo de emulación de tarjetas (220); y

mantener (S20, S30, S40, S50, S60) en el sistema informático (1) una base de datos de tarjetas (13), almacenando en la base de datos de tarjetas (13) para cada uno de la pluralidad de dispositivos de comunicación móvil (2) una representación (14) del módulo de emulación de tarjetas (220) almacenado en el dispositivo de comunicación móvil (2) respectivo, comprendiendo la representación (14) del módulo de emulación de tarjetas (220) los datos de aplicación (222) para las varias aplicaciones de tarjetas sin contacto diferentes del módulo de emulación de tarjetas (220) almacenado en el dispositivo de comunicación móvil (2) respectivo e información acerca del módulo de programa (221) del módulo de emulación de tarjetas (220) almacenado en el dispositivo de comunicación móvil (2)

respectivo, incluyendo la información acerca del módulo de programa (221) al menos uno de: una copia del código de programa informático del módulo de programa (221) y un identificador de programa que identifica el código de programa informático del módulo de programa (221).

- 5 10. El método de la reivindicación 9, en donde el método comprende adicionalmente que el sistema informático (1) transfiera (S2) a través de la red de telecomunicaciones (5) al dispositivo de comunicación móvil (2) datos de derechos de acceso específicos de la aplicación para una pluralidad de aplicaciones de tarjetas sin contacto; almacenar los datos de derechos de acceso específicos de la aplicación en el módulo de emulación de tarjetas (220); almacenar en el sistema informático (1) claves de acceso específicas de la aplicación para una pluralidad de aplicaciones de tarjetas sin contacto; y que el sistema informático (1) transfiera (S2) a través de la red de telecomunicaciones (5) al dispositivo de comunicación móvil (2) un módulo de emulación de tarjetas que incluye un código de programa informático configurado para controlar el procesador (20) del dispositivo de comunicación móvil (2) para ejecutar transacciones de datos a través de la interfaz de comunicación inalámbrica de corto alcance (21) del dispositivo de comunicación móvil (2), y para verificar la autorización de un socio de transacción para acceder a datos de aplicación almacenados en el módulo de emulación de tarjetas (220) para una aplicación de tarjetas sin contacto particular, basándose en los datos de derechos de acceso específicos de la aplicación, almacenados en el módulo de emulación de tarjetas (220) para la aplicación de tarjetas sin contacto particular, y una clave de acceso específica de la aplicación, recibida del socio de transacción a través de la interfaz de comunicación inalámbrica de corto alcance (21).
- 10 20 11. El método de una de las reivindicaciones 9 o 10, en donde el método comprende adicionalmente que el sistema informático (1) incluya en los datos de aplicación (222) almacenados en el módulo de emulación de tarjetas (220) del dispositivo de comunicación móvil (2) un puntero a datos de aplicación almacenados en la base de datos de tarjetas (13); y transferir (S2) a través de la red de telecomunicaciones (5) al dispositivo de comunicación móvil (2) un módulo de emulación de tarjetas que incluye un código de programa informático configurado para controlar el procesador (20) del dispositivo de comunicación móvil (2) para recuperar los datos de aplicación de la base de datos de tarjetas (13) usando el puntero, y para ejecutar las transacciones de datos a través de la interfaz de comunicación inalámbrica de corto alcance (21) del dispositivo de comunicación móvil (2) usando datos de aplicación recuperados de la base de datos de tarjetas (13).
- 25 30 12. El método de una de las reivindicaciones 9 a 11, en donde el método comprende adicionalmente que el sistema informático (1) lea los datos de aplicación (222) almacenados en el módulo de emulación de tarjetas (220) de uno de los dispositivos de comunicación móvil (2), y ejecute al menos uno de: transferir desde el sistema informático (1) al dispositivo de comunicación móvil (2) datos de aplicación (222) actualizados almacenados en la base de datos de tarjetas (13), en casos en los que los datos de aplicación (222) leídos del dispositivo de comunicación móvil (2) indican una versión obsoleta de los datos de aplicación, y actualizar en el sistema informático (1) la representación (14) del módulo de emulación de tarjetas (220) del dispositivo de comunicación móvil (2) almacenando en la base de datos de tarjetas (13) datos de aplicación leídos desde el módulo de emulación de tarjetas (220) del dispositivo de comunicación móvil (2), en casos en los que los datos de aplicación leídos del dispositivo de comunicación móvil (2) indican una versión más reciente de los datos de aplicación.
- 35 40 13. El método de una de las reivindicaciones 9 a 12, en donde el método comprende adicionalmente que el sistema informático (1) reciba a través de la red de telecomunicaciones (5) una solicitud relacionada con una aplicación de tarjetas sin contacto, indicando la solicitud al menos una de las siguientes operaciones de datos de aplicación para el módulo de emulación de tarjetas (220) de uno o más dispositivos de comunicación móvil (2): descargar datos de aplicación adicionales en el módulo de emulación de tarjetas (220), actualizar datos de aplicación (222) en el módulo de emulación de tarjetas (220) y eliminar datos de aplicación (222) en el módulo de emulación de tarjetas (220); transferir una solicitud de datos de aplicación al módulo de emulación de tarjetas (220) del uno o más dispositivos de comunicación móvil (2) de acuerdo con la operación de datos de aplicación respectiva; y actualizar en la base de datos de tarjetas (13) la representación (14) del módulo de emulación de tarjetas (220) del uno o más dispositivos de comunicación móvil (2) actualizando datos de aplicación en la base de datos de tarjetas (13) de acuerdo con la solicitud de datos de aplicación.
- 45 50 14. El método de una de las reivindicaciones 9 a 13, en donde el método comprende adicionalmente que el sistema informático (1) reciba a través de la red de telecomunicaciones (4) desde un sistema de socio (3) autorizado al menos uno de: una solicitud de escritura que incluye datos de aplicación para el módulo de emulación de tarjetas (220) de uno o más dispositivos de comunicación móvil (2), y una solicitud de lectura para leer datos de aplicación desde el módulo de emulación de tarjetas (220) de uno o más dispositivos de comunicación móvil (2); transferir los datos de aplicación a través de la red de telecomunicaciones al módulo de emulación de tarjetas (220) del uno o más dispositivos de comunicación móvil (2), en caso de una solicitud de escritura; y leer los datos de aplicación (222) almacenados en el módulo de emulación de tarjetas (220) del uno o más dispositivos de comunicación móvil (2), en caso de una solicitud de lectura; y actualizar en el sistema informático (1) la representación (14) del módulo de emulación de tarjetas (220) del uno o más dispositivos de comunicación móvil (2) almacenando en la base de datos de tarjetas (13) los datos de aplicación leídos o almacenados en el módulo de emulación de tarjetas (220) del uno o más dispositivos de comunicación móvil (2), respectivamente.
- 55 60 15. El método de una de las reivindicaciones 9 a 14, en donde el método comprende adicionalmente que el sistema
- 65

informático (1) reciba a través de la red de telecomunicaciones (4) una solicitud relacionada con uno de los dispositivos de comunicación móvil (2), exigiendo la solicitud una actualización del módulo de emulación de tarjetas (220); transferir un código de programa para el módulo de emulación de tarjetas (220) al dispositivo de comunicación móvil (2) de acuerdo con la solicitud; y actualizar en la base de datos de tarjetas (13) la representación (14) de los módulos de emulación de tarjetas (220) de los dispositivos de comunicación móvil (2) almacenando en la base de datos de tarjetas (13) al menos uno de: un número de versión que indica la versión del código de programa transferido al dispositivo de comunicación móvil (2), y el código de programa transferido al dispositivo de comunicación móvil (2).

16. El método de una de las reivindicaciones 9 a 15, en donde el método comprende adicionalmente que el sistema informático (1) transfiera (S2) a través de la red de telecomunicaciones (5) a los dispositivos de comunicación móvil (2) un módulo de emulación de tarjetas que incluye un código de programa informático configurado para controlar un procesador (20) del dispositivo de comunicación móvil (2) para ejecutar la transacción de datos a través de la interfaz de comunicación inalámbrica de corto alcance (21) de los dispositivos de comunicación móvil (2) con un dispositivo de transacción externo (6), incluyendo la transacción de datos al menos uno de: una transacción de pago de débito, una transacción de pago de crédito, una transacción de pago de efectivo electrónico, una transacción de emisión de billetes, una transacción de control de acceso, una transacción de actualización de aplicación para actualizar los datos de aplicación (222) en el módulo de emulación de tarjetas (220), y una transacción de actualización de tarjeta para actualizar el código de programa informático del módulo de emulación de tarjetas (220); e incluyendo los datos de aplicación al menos uno de: datos de cuenta de débito, datos de cuenta de crédito, datos de efectivo electrónico, datos de billete electrónico, datos de derechos de acceso, datos de identificación de usuario, datos de autenticación de usuario y datos de estructura de datos de aplicación.

17. Un producto de programa informático que comprende un medio legible por ordenador no transitorio que tiene almacenado en el mismo un código de programa informático configurado para controlar un procesador (10) de un sistema informático (1) para realizar:

transferir (S2) desde el sistema informático (1) a través de una red de telecomunicaciones (5) a uno de los dispositivos de comunicación móvil (2) un módulo de emulación de tarjetas, usando una clave de acceso de área para almacenar el módulo de emulación de tarjetas (220) en un área segura (22) del dispositivo de comunicación móvil (2), comprendiendo el módulo de emulación de tarjetas (220) un módulo de programa (221) con un código de programa informático configurado para controlar un procesador (20) de un dispositivo de comunicación móvil (2) para emular un módulo de tarjeta sin contacto controlando el procesador (20) para emular funciones de una tarjeta de circuito integrado implementada en hardware que tiene un procesador y una memoria, y para ejecutar transacciones de datos a través de una interfaz de comunicación inalámbrica de corto alcance (21) del dispositivo de comunicación móvil (2);

transferir (S3) desde el sistema informático (1) a través de la red de telecomunicaciones (5) al dispositivo de comunicación móvil (2) datos de aplicación para varias aplicaciones de tarjetas sin contacto diferentes para almacenar los datos de aplicación (222) para las varias aplicaciones de tarjetas sin contacto diferentes en el módulo de emulación de tarjetas (220); y

mantener (S20, S30, S40, S50, S60) en el sistema informático (1) una base de datos de tarjetas (13), almacenando en la base de datos de tarjetas (13) para cada uno de la pluralidad de dispositivos de comunicación móvil (2) una representación (14) del módulo de emulación de tarjetas (220) almacenado en el dispositivo de comunicación móvil (2) respectivo, comprendiendo la representación (14) del módulo de emulación de tarjetas (220) los datos de aplicación (222) para las varias aplicaciones de tarjetas sin contacto diferentes del módulo de emulación de tarjetas (220) almacenado en el dispositivo de comunicación móvil (2) respectivo e información acerca del módulo de programa (221) del módulo de emulación de tarjetas (220) almacenado en el dispositivo de comunicación móvil (2) respectivo, incluyendo la información acerca del módulo de programa (221) al menos uno de: una copia del código de programa informático del módulo de programa (221) y un identificador de programa que identifica el código de programa informático del módulo de programa (221).

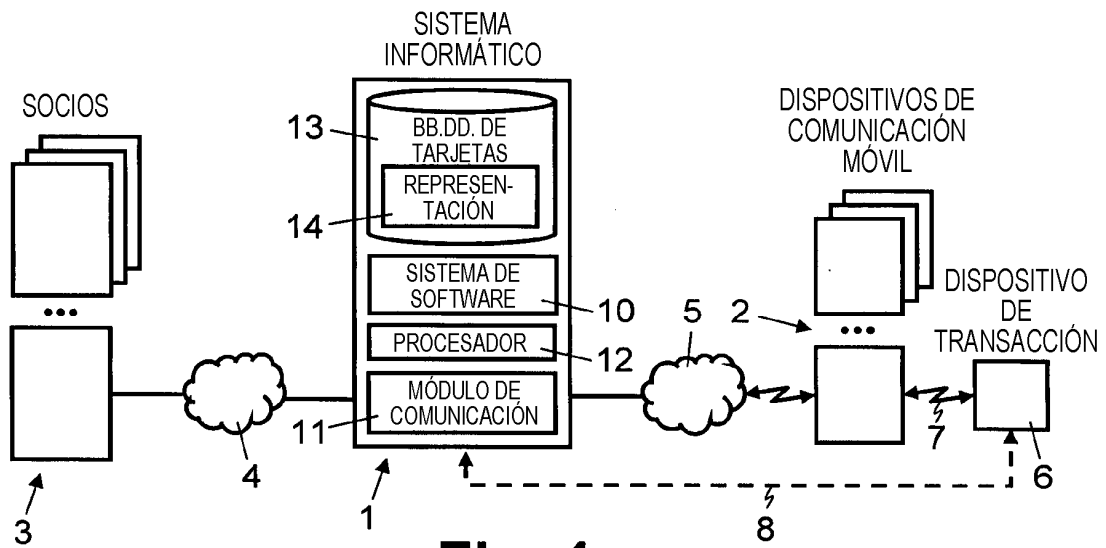


Fig. 1

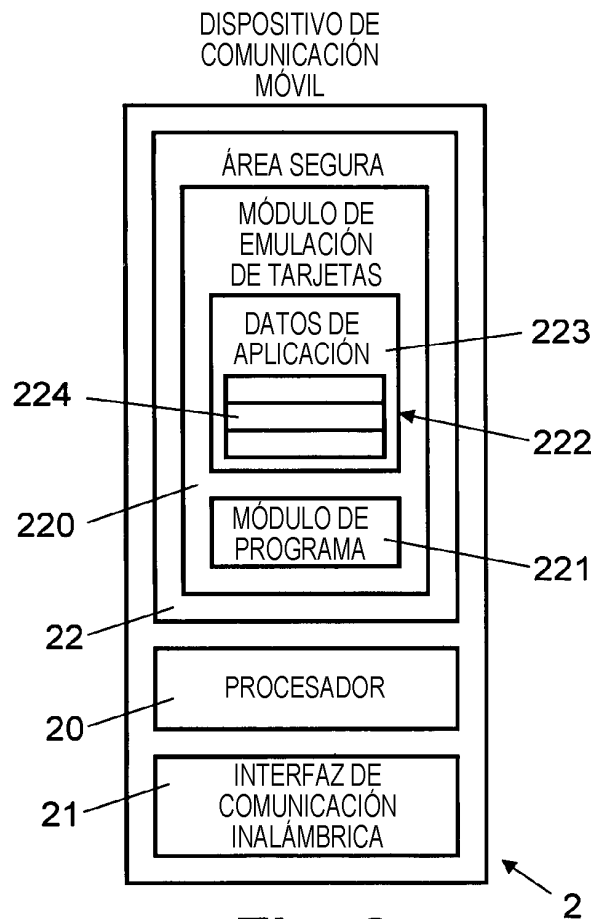


Fig. 2

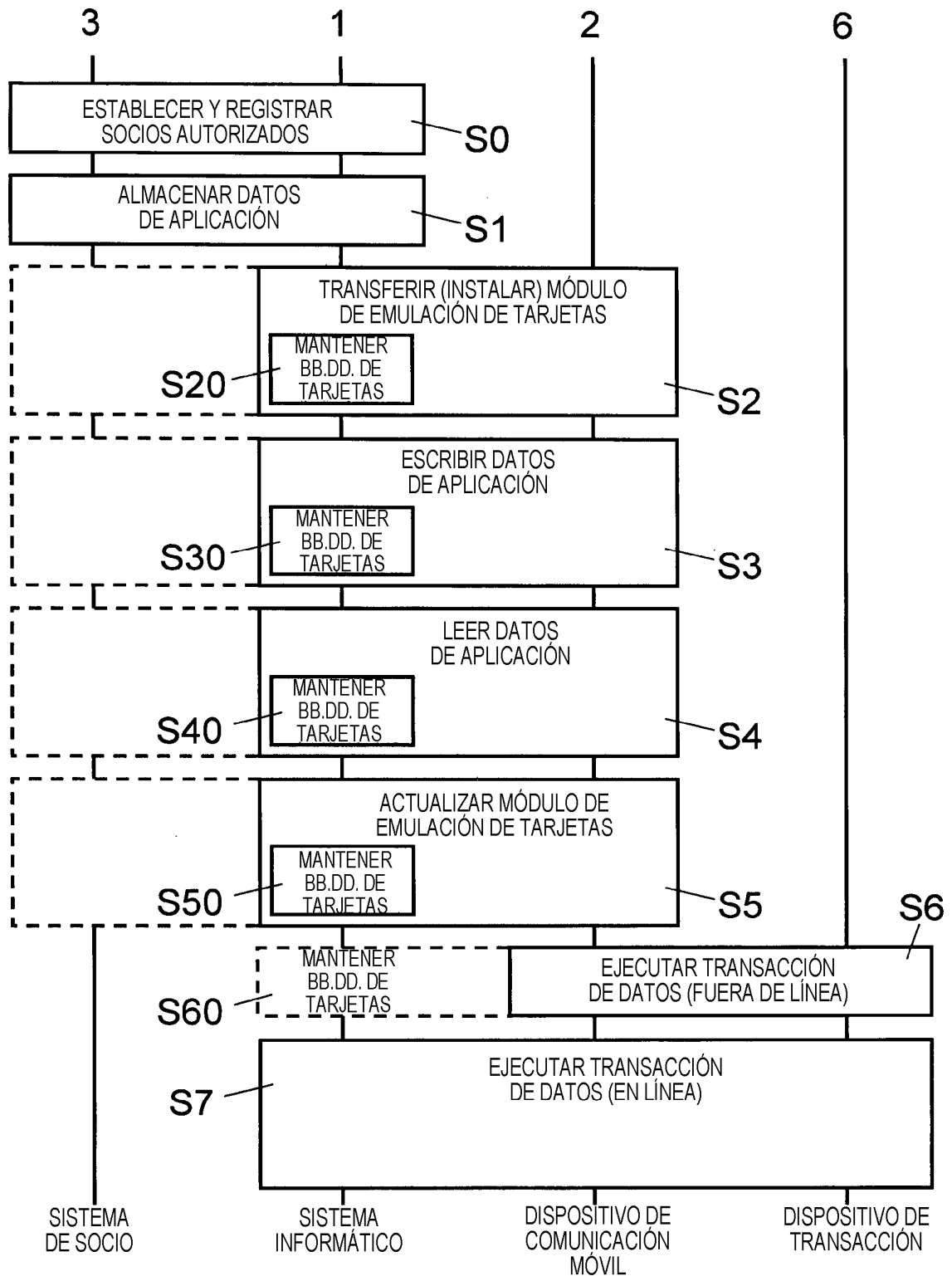


Fig. 3