(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 526 641**

(51) Int. CI.:

G06Q 20/32 (2012.01)
G06Q 20/34 (2012.01)
G07F 7/10 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **09.10.2007 E 07019748 (8)**

(97) Fecha y número de publicación de la concesión europea: **01.10.2014 EP 2048590**

(54) Título: **Procedimiento de comunicación, dispositivo de comunicación y procesador seguro**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
14.01.2015

(73) Titular/es:

VODAFONE HOLDING GMBH (100.0%)
MANNESMANNUFER 2
40213 DÜSSELDORF, DE

(72) Inventor/es:

KORAICHI, NAJIB;
HOEKSEL, SEBASTIAAN y
MONTANER, JAVIER

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

DESCRIPCIÓN

Procedimiento de comunicación, dispositivo de comunicación y procesador seguro

Campo de la invención

La invención se refiere a un procedimiento para la comunicación entre un procesador seguro y una interfaz de terminal, en el que la interfaz de terminal envía una solicitud para una acción deseada con un módulo de programa.

La invención se refiere, además, a un dispositivo de comunicación móvil y a un procesador seguro.

Antecedentes de la invención

Es conocido el uso de tarjetas inteligentes tales como tarjetas de tamaño de bolsillo con un elemento seguro integrado incorporado que puede procesar información. Las tarjetas inteligentes pueden recibir una entrada que es procesada por aplicaciones de elementos seguros integrados. Un resultado de este proceso o la información generada por el procesamiento de la entrada se entrega como salida.

Los usuarios que quieren utilizar diferentes funciones tienen que utilizar varias tarjetas individuales, por ejemplo, una tarjeta bancaria o una tarjeta de acceso.

Se sabe, además, enviar información a las tarjetas inteligentes o recibir información de las tarjetas inteligentes por medio de tecnología de comunicación de campo cercano.

La tecnología de comunicación de campo cercano (NFC) estandarizada en ISO 18092 y 21481, ECMA 340, 352 y 356, y ETSI TS 102 190 permite la comunicación sin contacto entre dispositivos en una corta distancia de unos 10 a 20 centímetros. Los dispositivos o tarjetas de campo cercano utilizan un módulo de radio que comprende un controlado de NFC (comunicación de campo cercano) con un microprocesador y memoria y una antena de bucle magnético que funciona a una frecuencia de 13,56 MHz. Aplicaciones importantes para la NFC son el pago electrónico y el billetaje electrónico. Aquí, un dispositivo capaz de NFC comprende un elemento seguro que se comunica con el controlador de NFC y que se utiliza como un monedero electrónico o para almacenar los boletos electrónicos. El pago o la validación de un boleto electrónico se realiza con sólo hacer tocar el dispositivo capaz de NFC a un lector de NFC o poniendo el dispositivo a distancia suficientemente cercana al lector de NFC. Aquí se requiere la proximidad cercana entre el dispositivo capaz de NFC y el lector de NFC para evitar la lectura realizada por un persona o dispositivo equivocado.

El documento US 6 005 942 describe un sistema y un procedimiento para una tarjeta inteligente de aplicaciones múltiples que permite una descarga posterior a la emisión de aplicaciones en la tarjeta inteligente. La tarjeta inteligente comprende un dominio de tarjeta para gestionar aspectos de la tarjeta inteligente. Durante una instalación segura de una aplicación, un dominio seguro puede proporcionar servicios al dominio de la tarjeta para descodificar un campo de instalación de la aplicación y comprobar la firma de un fichero de aplicaciones. Una aplicación cargada también es registrada en la tarjeta inteligente y en lo sucesivo puede ser seleccionada para ejecutar transacciones.

El documento de Zhiqun Chen, "Tecnología de Tarjetas Java para Tarjetas Inteligentes", Addison - Wesley, 2000, describe mini aplicaciones de tarjeta java que se pueden instalar en una tarjeta java y ser seleccionadas usando un procedimiento de selección.

El documento US 2006/0000900 A1 desvela un dispositivo móvil de un comprador que incluye tarjetas de aplicaciones para realizar transacciones financieras sin contacto con un sistema del vendedor. El usuario del dispositivo y el vendedor establecen preferencias para conducir la transacción y una aplicación de la tarjeta es seleccionada en un proceso de negociación entre el sistema del vendedor y el dispositivo del comprador.

Sumario de la invención

Un objeto de la presente invención es crear un procedimiento que permite una integración de varias funciones en un dispositivo de comunicación móvil.

Este objeto se consigue por medio de un procedimiento de acuerdo con la reivindicación 1, un dispositivo de comunicación de acuerdo con la reivindicación 8 y un procesador seguro de acuerdo con la reivindicación 10. Las realizaciones del procedimiento y del dispositivo de comunicación móvil son objeto de las reivindicaciones dependientes.

La invención incluye un procedimiento para la comunicación entre un procesador seguro, por ejemplo, un módulo de identidad de abonado con una interfaz de terminal, mediante lo cual la interfaz de terminal envía una solicitud para una interacción deseada con un módulo de programa.

De acuerdo con la invención, la interfaz de terminal o una unidad de procesamiento digital conectada a la interfaz del terminal integra un modelo en la solicitud para la interacción deseada. El modelo puede incluir información acerca de una clase de interacciones a la que pertenece la interacción deseada.

Además, el procesador seguro contiene al menos dos módulos de programa diferentes, y el procesador seguro y / o un dispositivo de comunicación móvil que está conectado al procesador seguro contiene un selector, en el que el selector es capaz de analizar el modelo.

El selector puede determina la clase de interacciones, a la que pertenece la solicitud.

La invención incluye que el selector realice una selección de un módulo de programa seleccionable, en el que la selección está influida por la clase de interacciones a la que pertenece la interacción deseada.

Una realización preferida del procedimiento, del procesador seguro y del terminal móvil se caracterizan porque el selector determina si más de un módulo de programa es capaz de realizar la interacción deseada.

Una selección de este tipo es ventajosa, por ejemplo, si el modelo transmitido contiene una información de que se desea una activación de un proceso de pago. Este proceso de pago puede ser realizado, por ejemplo, por diferentes procesos de pago.

Es especialmente ventajoso, que cierta funcionalidad esté relacionada con un módulo de programa respectivo. En el caso de un proceso de pago, esto significa que un módulo de programa permite un pago por una primera tarjeta de crédito, otro módulo de programa permite un pago por otra tarjeta de crédito, un módulo de pago adicional permite un pago por una tarjeta de débito y otro programa permite la transferencia directa de dinero de una cuenta de usuario a otra cuenta o a un centro de transferencia de valores.

De acuerdo con una realización preferida de la invención, en el caso, que por lo menos dos módulos de programa sean capaces de realizar la acción deseada, el selector verifica si existe información con respecto a las preferencias para la selección.

De acuerdo con una realización de la invención, la información acerca de las preferencias está incluida en la solicitud para una acción deseada que se envía desde la interfaz de terminal.

De acuerdo con otra realización de la invención, la información con respecto a las preferencias está incluida en el módulo de identidad de abonado.

Por supuesto, es posible, que la información con respecto a las preferencias esté contenida en más de una fuente de información. Esto incluye que la información acerca de las preferencias pueda estar incluida también en la solicitud así como en el módulo de identidad de abonado.

Especialmente en el caso de que no se reciban preferencias de cualquiera de las fuentes de preferencias (solicitud o procesador seguro o equipo de usuario móvil) o en el caso de que existan preferencias en conflicto, es ventajoso que se active una interfaz de usuario, en el que la interfaz de usuario permite una selección del módulo de programa por un usuario del terminal móvil (terminal móvil).

De acuerdo con una realización del procedimiento, el dispositivo de comunicación móvil y el procesador seguro de acuerdo con la invención, el selector analiza el modelo mediante el análisis de la codificación de un flujo de bits.

Muchos ejemplos de codificación son conocidos por los expertos en la técnica, por ejemplo la codificación Manchester.

En una realización adicional del procedimiento, del dispositivo de comunicación y del procesador seguro se caracteriza porque la solicitud se maneja de acuerdo con el protocolo de Tipo A de ISO 14443.

De acuerdo con una realización del procedimiento, del dispositivo de comunicación móvil y del procesador seguro de acuerdo con la invención, la solicitud se maneja de acuerdo con el protocolo de Tipo B de ISO 14443.

De acuerdo con una realización del procedimiento, del dispositivo de comunicación móvil y del procesador seguro de acuerdo con la invención, un dispositivo de comunicación móvil que es conectable a un procesador seguro (10) y a un dominio de datos seguro, se caracteriza porque:

- el procesador seguro (10) contiene al menos dos módulos de programa que pueden ser activados independientemente uno del otro,
- el dispositivo de comunicación móvil contiene medios para recibir una solicitud que incluye un modelo con información acerca de una acción deseada,

- el dominio de datos seguro (10) y / o el dispositivo de comunicación móvil contiene un selector (25, 26), en el que el selector (25, 26) es capaz de analizar un modelo,
- el selector (25, 26) es capaz de determinar una clase de interacciones a la que pertenece la solicitud, y
- el selector (25, 26) es capaz de hacer una selección de módulos de programa seleccionables, en el que la selección se ve influida por la clase de interacciones a la que pertenece la interacción deseada.

En una realización adicional del procedimiento, del dispositivo de comunicación y del procesador seguro se caracterizan porque el dominio de datos seguro es un módulo de identidad de abonado.

La invención incluye diferentes ventajas importados.

Una ventaja importante es la protección de la privacidad. La invención permite que en diferentes tipos de servicios que normalmente están asociados a diferentes tarjetas y garantías, un operador de un terminal sólo reciba información acerca de la funcionalidad específica que necesita para llevar a cabo una cierta interacción.

Un ejemplo de lo anterior es que una empresa de transportes sólo recibe la información de que se ha pagado una cierta cantidad de un valor y no hay información acerca de nuevas oportunidades de pago o del titular de la tarjeta.

Del mismo modo, una compañía de tarjetas de crédito no recibe ninguna información acerca de los servicios de transporte u otros servicios que un titular de los dispositivos de comunicación móvil ha utilizado con otras oportunidades de pago, por ejemplo otra tarjeta de crédito, una tarjeta de débito o un monedero electrónico (e - Monedero).

En el caso de que se utilice un monedero electrónico, cualesquiera informaciones y seguimiento de los movimientos y actividades, tales como las compras de bienes del titular de la tarjeta están protegidos contra el acceso externo.

De acuerdo con una realización del procedimiento, del dispositivo de comunicación móvil y del procesador seguro de acuerdo con la invención, el procesador seguro se caracteriza porque:

- contiene al menos dos módulos de programa que pueden ser activados independientemente uno del otro,
- contiene medios para recibir una solicitud que incluye un modelo,
- el procesador seguro contiene un selector (25) y / o es conectable a un selector (26), en el que al menos uno de los selectores (25, 26,) es capaz de analizar el modelo,
- al menos uno de los selectores (25, 26) es capaz de determinar una clase de interacciones a las que pertenece la solicitud,
- y al menos uno de los selectores (25, 26) es capaz de hacer una selección de un módulo de programa seleccionable, en el que la selección se ve influida por la clase de interacción a la que pertenece la interacción deseada.

Aunque la invención no está limitada a comunicación de campo cercano, una comunicación de campo cercano (NFC) es una realización ventajosa para llevar a cabo la invención.

La comunicación sin contacto o comunicación de campo cercano (NFC), permite el intercambio de datos entre un lector habilitado para NFC y una tarjeta habilitada para NFC cuando se colocan muy cerca el uno de la otra.

Un dispositivo informático, tal como una tarjeta inteligente, una tarjeta SIM, un teléfono móvil o una combinación de estos dispositivos, puede ser equipado con las tecnologías de comunicación de NFC. El dispositivo informático también puede contener software que emula el comportamiento de nivel de aplicación de una o más tarjetas de NFC. Múltiples aplicaciones de tarjeta pueden residir en una tarjeta de NFC.

Cuando un dispositivo informático de este tipo se coloca delante de un lector de NFC, responderá al lector como si se fuese una tarjeta de NFC. El dispositivo informático puede emular múltiples tarjetas de NFC.

Existen muchos tipos diferentes de lectores de NFC (por ejemplo, puede estar soportado un protocolo de RF específico); y un lector de NFC dado sólo puede manejar un subconjunto de las tarjetas de NFC disponibles.

El reto para el dispositivo informático es presentar esas tarjetas y aplicaciones de NFC que son soportadas / esperadas por el lector de NFC. Este problema se conoce como Selección de Aplicación.

Aunque la invención es especialmente ventajosa para la comunicación sin contacto, o comunicación de campo cercano (NFC), por supuesto también se puede realizar el intercambio de datos de acuerdo con la invención, con con-

tactos a través de distancias mayores, especialmente en el caso de que se establezcan las vías de transmisión adecuadas.

La unidad, que intercambia información y solicitudes de intercambio de información, es descrita de acuerdo con la invención como una interfaz de terminal. La interfaz de terminal es, por ejemplo, un lector, que puede estar integrado en varios terminales.

Es especialmente útil integrar el lector en diferentes terminales de usuario, por ejemplo, un cajero automático, un billetaje automático, un terminal para el manejo de boletos de estacionamiento o sistemas de control de acceso.

Sin embargo, para los expertos en la técnica es evidente que se pueden utilizar otros tipos de lectores.

En algunas situaciones, la información que es recibida desde el lector no es suficiente para identificar de forma única la aplicación de tarjeta que debe ser seleccionada. En estas situaciones, se propone que un subconjunto de aplicaciones de tarjeta se active antes de una transacción de acuerdo con la invención (realizando un proceso de selección) de tal manera que una aplicación de tarjeta única puede ser identificada durante la operación desde el subconjunto de aplicaciones activadas.

La creación de un subconjunto de aplicaciones de tarjetas podría hacerse por medio de un menú de selección de usuario. Sin embargo, es necesaria la señalización al usuario la detección de conflictos para indicar si el subconjunto seleccionado actualmente es válido (es decir, deberá ser posible seleccionar únicamente una aplicación de tarjeta en todo momento usando la información desde sólo el lector de NFC).

Los detalles de la detección de conflictos se proporcionan en las especificaciones de la NFC.

La noción de activar una aplicación de tarjeta requiere una extensión del diagrama de estado del ciclo de vida de una aplicación de tarjeta.

Una aplicación de tarjeta es SELECCIONABLE Y DESACTIVADA cuando no es elegible para la selección. Mientras que una aplicación de tarjeta es SELECCIONABLE Y ACTIVADA cuando es elegible para la selección por el lector de NFC.

La selección de una aplicación de tarjeta que se encuentra en estado SELECCIONABLE Y ACTIVADA puede ser automatizada aplicando reconocimiento de modelo en la información inicial que se envía desde el lector de NFC.

Para este fin cada aplicación de tarjeta que se instala en el dispositivo informático tiene un parámetro de reconocimiento de modelo. Los detalles de implementación del parámetro de reconocimiento de modelo se proporcionan en el documento de la especificación de la NFC.

Pueden haber muchos tipos diferentes de lógica de aplicación en el dispositivo informático que desea activar una aplicación de tarjeta. Con el fin de garantizar que no surjan inconsistencias se propone que los cambios de estado de las aplicaciones de tarjetas se manejen de forma centralizada por una aplicación; la aplicación de gestión central. La aplicación de gestión central implementa la lógica de detección de conflictos que se ha descrito más arriba.

En resumen, las siguientes etapas son ventajosas:

- extensión del diagrama de estado con estados activados / desactivados
- detección de conflictos para preseleccionar / activar aplicaciones
- todos los cambios de estado son gestionados por medio de una lógica central
- reconocimiento de modelo para detectar automáticamente la aplicación de tarjeta que debe ser seleccionada

De acuerdo con un primer aspecto de la invención, las funciones de múltiples tarjetas - especialmente son tarjetas RFID - están integradas en un único elemento seguro, siendo el elemento seguro, por ejemplo, un dominio de datos seguro como por ejemplo una tarjeta de módulo de identidad de abonado.

Otros ejemplos de elementos de datos seguros son: dominios de datos seguros como por ejemplo una tarjeta de memoria segura, puesto que puede estar integrada, por ejemplo, en un equipo de usuario móvil, tal como un teléfono celular móvil, o un dispositivo comparable tal como un dictáfono.

De acuerdo con un aspecto de la invención, el dominio de datos seguro está integrado en un procesador seguro, por ejemplo en un micro procesador. El procesador seguro está integrado, por ejemplo en los dispositivos de usuario móviles como por ejemplo un teléfono móvil, una cámara móvil o un dictáfono móvil.

Las funciones de tarjetas múltiples (RFID) se pueden integrar en un único procesador seguro, por ejemplo, una tarjeta (SIM), que consiste en elementos seguros, que son en adelante serán denominados dominios de Datos Seguros (SD).

La invención permite integrar funciones de varias tarjetas individuales diferentes en una tarjeta, por ejemplo, la funcionalidad como una tarjeta bancaria, como una tarjeta de transporte, como una tarjeta de control de acceso o como una tarjeta de boletos de eventos.

Es posible, además, incluso instalar aplicaciones en conflicto en el mismo dominio de datos seguro SD.

Una realización preferida de la invención incluye un procedimiento con los siguientes pasos:

1. Detección de una solicitud
2. Un Modelo de señal recibida es interpretado, si pertenece a uno de los modelos plurales; este puede ya incluir una selección de preferencia
3. Determinación de un tipo de tarjeta (tipo A, tipo B, ...) ISO 14443, selección de aplicaciones implícitas / explícitas, la selección de aplicación explícita comprende un comando SELECCIONAR con una identificación ID de Appl específica.
4. Comprobar si hay al menos una tarjeta del tipo solicitado; examen si más de una tarjeta pertenece al tipo de solicitud:

   Sí: tarjetas plurales, no: seleccionar la tarjeta, más de una activa? Si:

   interacción de usuario programable:

   preferencia predefinida, un usuario o una 3ª parte

   No: fin, interacción de usuario

Las realizaciones preferidas de la invención pueden incluir una interfaz de usuario y / o un menú de configuración de usuario.

En una realización preferida se activa la interfaz de usuario cuando se detecta un conflicto entre los diferentes requisitos, para activar más de un módulo de programa.

Sin embargo, también es ventajoso incluir un menú de configuración de usuario que permita una introducción de las preferencias de un usuario - especialmente antes de realizar la comunicación entre la interfaz del terminal y el dominio de datos seguro.

Los elementos preferidos para incluir en un menú de configuración de usuario son:

- lista de aplicaciones disponibles
- configuración de soportes de preferencias
- activación / desactivación de la aplicación
- optativamente, evitar dos activos al mismo tiempo del mismo tipo

Si los diferentes módulos de programa son capaces de llevar a cabo la interacción con la interfaz del terminal, es ventajoso incluir procedimientos para una gestión de conflictos.

La gestión de conflictos puede ser manejada de diferentes maneras, por ejemplo, es posible comprobar si ya existen preferencias o se pueden determinar.

En una realización de la invención, el selector contiene un registro.

El registro es capaz de realizar varias funciones.

Una de las funciones que puede estar integrada en el registro es una comprobación de conflictos entre diferentes aplicaciones.

Por ejemplo, el registro puede determinar si hay instalado más de un módulo de programa que puede llevar a cabo una acción específica.

Un ejemplo de esto es la existencia de dos monederos electrónicos diferentes.

En el caso de que dos monederos diferentes u otras funciones relacionadas con uno de los módulos del programa pudiesen estar activados, el registro podría ser utilizado para descubrir esta convivencia y la posibilidad de que pudiese surgir un conflicto.

Es ventajoso informar a un usuario del dispositivo de comunicación móvil a través de un mensaje electrónico con respecto al conflicto potencial.

Las soluciones para la resolución del conflicto, por ejemplo, una definición de una prioridad de usos y el bloqueo de otros usos de aplicaciones similares con una funcionalidad similar pueden ser bloqueadas.

Una selección de estas opciones podría ser ofrecida al usuario del dispositivo de comunicación a través de una interfaz gráfica de usuario (GUI).

En este caso, el registro puede tener dos funciones: Soporte para determinar si podrían surgir conflictos y prevención de conflictos mediante el almacenamiento de información con respecto a las preferencias para la solución de conflictos entre aplicaciones con igual o similar funcionalidad.

Para los expertos en la técnica, es obvio que una combinación de ambas funciones es ventajosa.

Sin embargo estos expertos en la técnica podrían son conscientes de que se pueden conseguir ventajas si se utiliza al menos una de estas funciones.

La invención incluye diferentes dispositivos de comunicación móvil que pueden realizar funciones de acuerdo con la invención.

De acuerdo con un aspecto de la invención, un dispositivo de comunicación móvil comprende un módulo de identidad de abonado (SIM) y los componentes de NFC para la comunicación de campo cercano (NFC) que incluye un módulo de radio y un elemento seguro para el almacenamiento de datos utilizados en los servicios de comunicación de campo cercano, comunicándose el módulo de radio con el elemento seguro. Una unidad de control (selector) es conectable al dispositivo de comunicación móvil y al módulo de identidad de abonado, formando la unidad de control y un procesador del dispositivo de comunicación móvil y el módulo de identidad de abonado una unidad del dispositivo de comunicación móvil que incluye al menos un componente de NFC .

De acuerdo con un segundo aspecto de la invención, se proporciona una unidad de control para su uso en un dispositivo de comunicación móvil, que comprende un módulo de identidad de abonado. La unidad de control se puede conectar al dispositivo móvil (terminal móvil) y al módulo de identidad de abonado y la unidad de control está configurada de tal manera, que la unidad de control y uno de entre el dispositivo de comunicación móvil y el módulo de identidad de abonado forman una unidad, incluyendo al menos un componente de NFC, que se selecciona entre el conjunto de componentes de NFC que comprenden un módulo de radio para la comunicación de campo cercano y un elemento seguro para el almacenamiento de datos utilizados en los servicios de comunicación de campo cercano.

La invención implica la idea de proporcionar una unidad de control que se puede conectar al dispositivo de comunicación móvil y al SIM para habilitar la funcionalidad de NFC para un dispositivo de comunicación móvil que comprende un dispositivo móvil de comunicación y / o un SIM, que no están habilitados para NFC. En particular, la unidad de control puede estar conectada entre el SIM y el dispositivo de comunicación móvil, de manera que la tarjeta SIM está conectada al dispositivo de comunicación móvil a través de la unidad de control.

Los componentes para habilitar el dispositivo de comunicación móvil que va a ser utilizado en NFC incluyen un módulo de radio y un elemento seguro conectado al módulo de radio. El módulo de radio puede comprender una antena y un controlador conectado a la antena.

En combinación con el dispositivo de comunicación móvil o con la tarjeta SIM, la unidad de control forma un subconjunto del dispositivo de comunicación móvil, que comprende al menos un componente de NFC. Si un componente de NFC no está incluido en este subconjunto, la unidad de control permite la conexión de este componente de NFC al componente de NFC incluido en el subconjunto.

La invención hace posible el uso de los servicios de NFC por medio de un dispositivo de comunicación móvil y / o una tarjeta SIM, que no están habilitados para NFC. Por lo tanto, la invención evita que un usuario móvil tenga que reemplazar tanto su dispositivo de comunicación móvil como su SIM para el uso de los servicios de NFC.

Dentro del ámbito de la invención, el término módulo de identidad de abonado se refiere a una tarjeta inteligente que se puede insertar en un dispositivo móvil, y que contiene la identidad de un abonado a los servicios de comunicación móvil.

Por ejemplo el módulo de identidad de abonado puede estar configurado como una tarjeta SIM de acuerdo con el estándar GSM (GSM: Sistema Global para Comunicaciones Móviles) o como una tarjeta USIM de acuerdo con el estándar UMTS (USIM: Módulo de Identidad de Abonado Universal; UMTS: Sistema de Telecomunicaciones Móviles Universal). El dispositivo móvil (terminal móvil) puede comprender una interfaz de radio para acceder a una red de comunicación móvil y una interfaz de usuario, tal como, por ejemplo, una unidad de pantalla y / o unidad de entrada, que pueden ser operadas por el usuario móvil.

En una realización del dispositivo de comunicación móvil y de la unidad de control, al menos un componente de NFC está incluido en el módulo de identidad de abonado.

Este componente de NFC puede ser el elemento seguro, que puede estar incorporado como una aplicación en el procesador seguro. Puesto que el procesador seguro constituye un chip seguro, ya proporciona la funcionalidad necesaria para el almacenamiento seguro de los datos sensibles utilizados en los servicios de comunicación de campo cercano, tales como, por ejemplo, el pago electrónico o el billetaje electrónico. Sin embargo, también el módulo de radio o parte del módulo de radio, particularmente el controlador, pueden estar incluidos en el módulo de identidad de abonado.

En otra realización del dispositivo de comunicación móvil y de la unidad de control, al menos un componente de NFC está incluido en dispositivo de comunicación móvil.

Este componente de NFC puede ser el módulo de radio, en particular la antena del módulo de radio, ya que la antena puede estar dispuesta en el dispositivo de comunicación móvil de una manera tal que la recepción de radio no se vea afectada esencialmente por interferencias debidas a las corrientes eléctricas en el dispositivo de comunicación móvil o apantallamiento.

Una realización adicional del dispositivo de comunicación móvil y de la unidad de control hace que al menos un componente de NFC esté incluido en la unidad de control.

En esta realización un componente de NFC, que no está incluido en el dispositivo de comunicación móvil existente del usuario móvil ni en su procesador seguro existente, puede ser proporcionado por la unidad de control para habilitar la funcionalidad de NFC del dispositivo de comunicación móvil del usuario móvil.

En una realización del dispositivo de comunicación móvil y de la unidad de control, el módulo de radio y el elemento seguro se comunican utilizando un primer protocolo de comunicación.

El primer protocolo de comunicación puede ser el Protocolo de Cable Único (SWP), que podría convertirse en el estándar para la transferencia de datos entre el elemento seguro incorporado en un procesador seguro y un dispositivo de comunicación móvil que incluye un módulo de radio para la comunicación de campo cercano. Dentro del alcance del primer protocolo, puede estar previsto que el módulo de radio y el elemento seguro se comuniquen a través de un elemento de contacto eléctrico predeterminado del módulo de identidad de abonado, que puede ser el elemento de contacto C6 que no se utiliza en los estándares de telecomunicación móvil.

En una realización del dispositivo de comunicación móvil y de la unidad de control, el elemento seguro está incluido en el procesador seguro y el módulo de radio está incluido en la unidad de control.

Esta realización tiene la ventaja de que un usuario móvil que dispone de un procesador seguro de NFC incluyendo el elemento seguro, es capaz de utilizar su dispositivo de comunicación móvil existente que no incluye un módulo de radio. El módulo de radio es proporcionado por la unidad de control, que, en particular, es menos expansivo para el usuario móvil que un nueva dispositivo de comunicación móvil habilitado para NFC.

Como se ha explicado más arriba, un procesador seguro de NFC puede comprender un elemento de contacto eléctrico predeterminado dedicado a la comunicación entre el elemento seguro incorporado en el procesador seguro y el módulo de radio.

Por lo tanto, una realización relacionada del dispositivo de comunicación móvil y de la unidad de control establece que el procesador seguro comprenda un primer elemento de contacto eléctrico para conectar el elemento seguro al módulo de radio, siendo contactado el primer elemento de contacto eléctrico por un elemento de contacto eléctrico de la unidad de control.

En esta realización, la unidad de control comprende un contacto eléctrico conectado al primer elemento de contacto eléctrico del procesador seguro proporcionado para conectar el elemento seguro incorporado en el procesador seguro al módulo de radio incluido en el dispositivo de comunicación móvil. Como se ha explicado más arriba, el primer elemento de contacto del procesador seguro puede ser el elemento de contacto.

Además, la unidad de control puede conectar adicionalmente otro elemento de contacto eléctrico del procesador seguro al dispositivo de comunicación móvil, permitiendo de este modo una comunicación entre el procesador seguro y el dispositivo de comunicación móvil a través de la unidad de control.

En otra realización del dispositivo de comunicación móvil y de la unidad de control, el módulo de radio está incluido en el dispositivo de comunicación móvil y el elemento seguro está incluido en el módulo de identidad de abonado, estando adaptado el procesador seguro para comunicarse con el dispositivo de comunicación móvil utilizando un segundo protocolo de comunicación, y la unidad de control está adaptada para convertir mensajes de datos transmitidos desde el módulo de radio al elemento seguro desde el primer protocolo al segundo y para convertir mensajes de datos transmitidos desde el elemento seguro al elemento de módulo de radio desde el segundo protocolo al primero.

Esta realización tiene la ventaja de que un dispositivo de comunicación móvil habilitado para NFC, incluyendo el dispositivo de radio, puede ser utilizado junto con un elemento seguro incorporado en un procesador seguro que no está habilitado para NFC, lo que significa que el procesador seguro no soporta la comunicación de acuerdo con el primer protocolo comunicación o por medio del primer elemento de contacto eléctrico. Por el contrario, el procesador seguro soporta la comunicación de acuerdo con un segundo protocolo de comunicación, que puede ser el protocolo de comunicación proporcionado en un estándar de comunicación móvil para la comunicación entre el dispositivo de comunicación móvil y el módulo de identidad de abonado.

Por lo tanto, en esta realización los mensajes de datos enviados desde el módulo de radio al elemento seguro son transmitidos a través de la unidad de control, que convierte los mensajes de datos desde el primer protocolo de comunicación al segundo. De manera similar, los mensajes de datos enviados desde el elemento seguro a la radio son transmitidos a través de la unidad de control, que convierte esos mensajes de datos desde el segundo protocolo de comunicación al primero.

Esto puede implicar enviar los mensajes de datos recibidos desde el dispositivo de comunicación móvil a través de un elemento de contacto eléctrico dedicado a la comunicación entre el módulo de radio y el elemento seguro, a un elemento de contacto eléctrico del procesador seguro dedicado a la comunicación convencional, es decir, no relacionada con la NFC, entre el procesador seguro y el dispositivo de comunicación móvil.

Por lo tanto, en una realización relacionada del dispositivo de comunicación móvil y de la unidad de control, el dispositivo de comunicación móvil comprende un segundo elemento de contacto eléctrico para conectar el módulo de radio con el elemento seguro, entrando en contacto el segundo elemento con un elemento de contacto eléctrico de la unidad de control, y comprendiendo el dispositivo de comunicación móvil al menos un tercer elemento de contacto eléctrico conectado a un elemento de contacto eléctrico adicional de la unidad de control, estando provisto el tercer elemento de contacto eléctrico para la comunicación entre el procesador seguro y el dispositivo de comunicación móvil.

Aquí, el cuarto elemento de contacto eléctrico del dispositivo de comunicación móvil puede ser un elemento de contacto proporcionado para la comunicación convencional entre el dispositivo de comunicación móvil y el SIM, que no está relacionado con los servicios de NFC.

Una realización adicional relacionada del dispositivo de comunicación móvil y de la unidad de control establece que la unidad de control está adaptada para enviar un mensaje de datos recibido desde el módulo de radio a través del segundo elemento de contacto eléctrico al elemento seguro a través del tercer elemento de contacto eléctrico del procesador seguro y que la unidad de control está adaptada para enviar un mensaje de datos recibido desde el elemento seguro a través del tercer elemento de contacto al módulo de radio a través del segundo elemento de contacto.

Además, en una realización del dispositivo de comunicación móvil y de la unidad de control, el módulo de radio está incluido en el dispositivo de comunicación móvil y el elemento seguro está incluido en la unidad de control.

Esta realización también hace posible el uso de un dispositivo de comunicación móvil habilitado para NFC que comprende el módulo de radio en combinación con un módulo de identidad de abonado, que no está habilitado para NFC. Como una alternativa a las realizaciones que se han descrito más arriba, esta realización proporciona la solución de que el elemento seguro esté incorporado en la unidad de control.

Aquí, un elemento de contacto eléctrico de la unidad de control puede entrar en contacto con el tercer elemento de contacto eléctrico del dispositivo de comunicación móvil para conectar el módulo de radio al elemento seguro, con lo que permite la comunicación entre el módulo de radio y el elemento seguro utilizando el primer protocolo. Además, el cuarto elemento de contacto eléctrico del dispositivo de comunicación móvil puede estar conectado al segundo elemento de contacto eléctrico de la tarjeta SIM a través de la unidad de control.

En una realización del dispositivo de comunicación móvil y de la unidad de control, el módulo de radio y el elemento seguro están incluidos en la unidad de control.

Esta realización tiene la ventaja de que todos los componentes necesarios para la comunicación de campo cercano están incluidos en la unidad de control. Por lo tanto, para permitir la funcionalidad de NFC para un dispositivo de comunicación móvil existente, que no está habilitado para NFC, el usuario móvil sólo tiene que añadir la unidad de control, que realiza la funcionalidad de NFC de forma autónoma, es decir, esencialmente independiente del dispositivo de comunicación móvil y del módulo de identidad de abonado. En este caso, el dispositivo de comunicación móvil se utiliza sobre todo como fuente de alimentación y como alojamiento para la unidad de control.

Los aspectos de la invención que se han mencionado más arriba y otros también serán evidentes a partir de y se aclararán con referencia a las realizaciones de la invención que se describen en la presente memoria descriptiva y a continuación haciendo referencia a los dibujos.

Breve descripción de los dibujos

Se hará referencia a modo de ejemplo a los dibujos adjuntos en los que:

- la figura 1: es un diagrama de bloques esquemático de un dominio de datos seguro de acuerdo con una realización de la invención,
- la figura 2: es una representación esquemática de una realización de la invención,
- la figura 3: es un diagrama de bloques esquemático de los elementos preferidos que pueden influir en un selector y
- la figura 4: es un diagrama de bloques esquemático de un dispositivo de comunicación móvil de acuerdo con la invención,

Descripción detallada de realizaciones de la invención

La invención puede ser integrada en diferentes estándares de comunicación y manejo.

Con el fin de facilitar una integración de la invención en los sistemas de tarjetas actuales, respectivamente, en los sistemas de tarjetas planeadas para la integración de funciones adicionales, es especialmente útil utilizar la invención en entornos de acuerdo con el estándar de plataforma global. El estándar de plataforma global es un estándar para la infraestructura de tarjetas inteligentes.

Los expertos en la técnica entienden que las descripciones de acuerdo con el estándar de plataforma global pueden ser transferidas a otros estándares para la infraestructura de tarjetas inteligentes.

De acuerdo con el estándar de plataforma global, las siguientes definiciones se utilizan para explicar las realizaciones preferidas de la invención que se describirán posteriormente:

APDU (Unidades de Datos de Protocolo de Aplicación)

Protocolo de mensajería de comunicación estándar entre un dispositivo de aceptación de tarjetas y una tarjeta inteligente.

API (Interfaz de Programación de Aplicación)

Un conjunto estandarizado de procedimientos para que un programador se aproveche de, (es decir, realice la interfaz con) las capacidades de la tarjeta o del dispositivo. La API es esencialmente un conjunto de herramientas o servicios de uso común por las aplicaciones en una tarjeta o dispositivo.

Proveedor de Aplicaciones

Entidad que posee una aplicación y es responsable del comportamiento de la aplicación.

Lógica de Negocio

La Capa de Lógica de Negocio ejerce el mayor nivel de control sobre las operaciones del terminal. La Capa de Lógica de Negocio es principalmente responsable de seleccionar una aplicación apropiada para ser activada, tanto en la tarjeta como en el terminal. La Capa de Lógica de Negocio es también responsable de la implementación de políticas locales. Las compras de licitación dividida, por ejemplo, puede ser una práctica aceptada en algunos lugares, pero no permitida en otros.

Administrador de tarjetas

Un agente de la tarjeta dentro de la tarjeta Plataforma Global habilita que el emisor mantenga y ejerza el control sobre la tarjeta. Este agente controla cuales aplicaciones pueden ser cargadas en la tarjeta después de que haya sido emitida.

Componente de Lógica de Chip

La Capa de Componente de Lógica de Chip (CLC) contiene todo el código independiente con el entorno. La Capa de CLC incluye un módulo para cada aplicación que el terminal soporta. Es en la capa de CLC donde reside el componente de dispositivo de cada aplicación.

Criterio Común

Un estándar de seguridad compartida público en la que están cooperando los líderes de la industria de tarjetas. Este será el estándar con el que la mayoría de las tarjetas inteligentes se pondrá a prueba en el futuro.

EEPROM (Memoria de Sólo Lectura Programable y Borrable Electrónicamente)

Memoria que se puede borrar y volver a utilizar, pero que no requiere energía eléctrica para mantener los datos. Se utiliza principalmente para almacenar información que cambiará, tal como los contadores de transacciones.

EMV

Especificaciones Técnicas desarrolladas conjuntamente por Europay, MasterCard International y Visa para crear estándares y garantizar la interoperabilidad global para el uso de la tecnología de chip en la industria de pagos.

Servicios de Medio Ambiente

Estos servicios proporcionan una interfaz coherente a un conjunto de recursos que se encuentran comúnmente en muchos terminales de tarjetas de chip.

ISO 7816

El estándar ISO (Organización Internacional de Estándares) que gobierna las tarjetas de circuito integrado en base a contacto.

ITSEC

Un esquema de evaluación de seguridad regional. Basado en los niveles de aseguramiento contra objetivos privados. Será sustituido por Criterio Común.

Tarjeta Java®

El entorno de tiempo de ejecución de tarjeta inteligente desarrollado por Sun. Basado en Java.

Plataforma Global

El estándar de la industria para la gestión de un programa de aplicación única y múltiple basado en tarjetas inteligentes. Incluye especificaciones de la tarjeta, especificaciones del dispositivo, y especificaciones de los sistemas.

Plataforma Global API

Por medio de los servicios contenidos en la Plataforma Global API, todas las aplicaciones se pueden crear y acceder de una manera uniforme.

Carga Post-Emisión

La carga de aplicaciones en una tarjeta después de que haya tenido lugar el proceso de personalización y emisión de la tarjeta.

Entorno de Tiempo de Ejecución

El Entorno de Tiempo de Ejecución consiste en tres componentes básicos. Estos son el Sistema Operativo de Tarjeta, la Máquina Virtual y la Interfaz de Programación de Aplicaciones (API)

Dominio Seguro

Los Dominios Seguros se pueden establecer en la tarjeta para proteger a los proveedores de aplicaciones o grupos de aplicaciones. Los Dominios Seguros habilitan las aplicaciones de diferentes proveedores para compartir el espacio en una tarjeta sin comprometer la seguridad de cualquier proveedor o aplicación particular.

Máquina Virtual

Una Máquina Virtual actúa como un traductor, convirtiendo las instrucciones de la aplicación en comandos únicos entendidos por un tipo específico de tarjeta. Una máquina virtual permite la portabilidad de aplicaciones.

Windows® para Tarjetas Inteligentes

Entorno de tiempo de ejecución de la tarjeta inteligente desarrollado por Microsoft. Basado en herramientas y principios comunes de WindowsNisual Basic..

La figura 1 muestra una representación esquemática de un procesador seguro 10 de acuerdo con la invención.

El procesador seguro contiene un registro 20, que está conectado a un ISD de dominio de seguridad emisor 20 y uno o más dominios de seguridad de terceros 30, 40.

El registro 20 contiene información sobre los recursos y / o condiciones de activación de los dominios 20, 30 y 40.

El registro 20 contiene información acerca de los dominios seguros 20, 30 y 40 y los módulos de programa 201, 202, 203, 301, 302, 303, 401, 402, 403 incluidos en los dominios seguros 20, 30 y 40.

Con el procesador seguro descrito es posible llevar a cabo procedimientos para la comunicación entre el procesador seguro 10 y una interfaz de terminal 5) en el que la interfaz del terminal 5 envía una solicitud para una interacción deseada con un módulo de programa 201, 202, 203, 301, 302 , 303, 401, 402, 403.

La interfaz del terminal 5 o una unidad de procesamiento digital conectada a la interfaz del terminal 5 integra un modelo en la solicitud para la interacción deseada, en el que el modelo incluye información acerca de una clase de interacciones a la que pertenece la interacción deseada.

El procesador seguro 10 contiene al menos dos módulos de programas diferentes, y el procesador seguro 10 y / o un dispositivo de comunicación móvil, que está conectado al procesador seguro 10 contiene un selector 25, 26, en el que el selector 25, 26 es capaz de analizando el modelo.

El selector 25, 26 determina la clase de interacciones a la que pertenece la solicitud.

Además, el selector 25, 26 hace una selección de un módulo de programa seleccionable, en el que la selección está influida por la clase de interacciones a la que pertenece la interacción deseada.

Preferiblemente, el registro contiene algunos, la mayor parte o incluso la totalidad de la información siguiente:

- preferencias de un usuario
- preferencias del instalador del terminal
- propiedades de los módulos de programa 201, 202, 203, 301, 302, 303, 401, 402, 403, 801, 802, 803 y 804
- capacidad de almacenamiento de archivos de datos 501, 502, 503, 601, 602, 603, 701, 702 y 703

Es posible realizar la invención con diferentes tipos de procesadores seguros. Una realización preferida de un procesador seguro de este tipo es un módulo SIM de identidad de abonado o un procesador de una tarjeta inteligente. Estos procesadores son modificados de acuerdo con la invención con el fin de lograr una o más de las ventajas que se han descrito en el texto de la aplicación actual.

En una realización de la invención, el procesador seguro está integrado en una tarjeta inteligente sin contacto, en el que el chip se comunica con el lector de tarjetas por medio de la tecnología de inducción RFID (a velocidades de datos de 106 a 848 kbit / s). Estas tarjetas requieren sólo una proximidad cercana a una antena para completar la transacción. A menudo se utilizan cuando las transacciones deben ser procesadas rápidamente o en manos libres, tal como en los sistemas de transporte masivo, en los que las tarjetas inteligentes se pueden utilizar sin siquiera sacarlas de una cartera.

Un ejemplo de comunicaciones con la tarjeta inteligente sin contacto se representa en la figura 2.

La realización de acuerdo con la figura 2 contiene una antena de una interfaz de terminal 5.

La interfaz de terminal 5 puede comunicar con una antena adicional 28 que está acoplada al selector 25.

Un estándar de comunicaciones de la tarjeta inteligente sin contacto es el estándar ISO / IEC 14443, de fecha 2001. Define dos tipos de tarjetas sin contacto ("A" y "B"), permite la comunicación a distancias de hasta 10 cm. Han habido propuestas de tipos C, D, E y F de ISO 14443 que han sido rechazadas por la Organización Internacional de Normalización. Un estándar alternativo para las tarjetas inteligentes sin contacto es ISO 15693, que permite la comunicación a distancias de hasta 50 cm.

ISO 14443 define una tarjeta de proximidad utilizada para la identificación que por lo general utiliza el factor de forma de tarjeta de crédito estándar definido por ISO 7810 ID-1. Otros factores de forma son también posibles. El lector de Identificación por Radio Frecuencia (RFID) utiliza un microcontrolador incorporado (que incluye su propio microprocesador y varios tipos de memoria) y una antena de bucle magnético que funciona a 13,56 MHz (frecuencia de RFID). Estándares OACI más recientes para documentos de viaje legibles por máquina especifican un formato de archivo firmado criptográficamente y un protocolo de autenticación para el almacenamiento de datos biométricos (fotos de la cara, huellas dactilares, y / o iris).

ISO 14443 consiste en cuatro partes y describe dos tipos de tarjetas: tipo A y tipo B. Las principales diferencias entre estos tipos se refieren a procedimientos de modulación, esquemas de codificación (parte 2) y procedimientos de inicialización del protocolo (parte 3). Ambas tarjetas de tipo A y de tipo B utilizan el mismo protocolo de alto nivel (el denominado T = CL) que se ha descrito en la parte 4. El protocolo T = CL especifica el intercambio de bloque de datos y mecanismos relacionados.

ISO 14443 utiliza los siguientes términos para los componentes:

* PCD - dispositivo de acoplamiento de proximidad (o lector)

* PICC - tarjeta de circuito integrado de proximidad

El estándar Calypso (RFID) cumple con ISO14443 parte 1, 2, 3 y 4 tipo B. Las tarjetas MIFARE cumplen con ISO14443 parte 1, 2 y 3 tipo A. Los pasaportes electrónicos cumplen con ISO 14443. Algunas tarjetas de crédito RFID utilizan ISO 14443 Tipo B

La presente invención puede realizarse independientemente de un cierto estándar. Sin embargo, para facilitar una integración del procedimiento y características de acuerdo con la invención, es posible utilizar las mejoras de los estándares conocidos como, por ejemplo:

División de ISO 14443:

ISO 14443-2 Capa Física

ISO 14443-3 Inicialización y anticolisión

ISO 14443-4 Protocolo de transmisión en bloque

Estándares de Protocolo sin contacto

Comportamiento Común

Lector / validador sin contacto

Cuando se conecta, el lector sin contacto - terminal 5 - genera un campo de radiofrecuencia (RF).

El terminal 5 comienza invitando a transmitir a un dispositivo sin contacto por medio del envío de solicitudes (REQA, REQB, ..) periódicamente.

Si se recibe una respuesta correcta, se ejecuta un bucle anticolisión con el fin de detectar todos los dispositivos en el campo. A continuación selecciona uno de ellos e inicia la comunicación de datos.

Tarjetas sin contacto

La potencia es proporcionada por el campo de RF

Una antena de RF está conectada a la tarjeta para recuperar esta potencia.

Teléfonos móviles sin contacto

Especificaciones O del Foro NFC para abordar los casos de uso relacionados con un entorno sin contacto móvil

La antena en el móvil está conectada a un chip de NFC, este chip de NFC envía datos sin contacto a la tarjeta SIM.

Descripción del protocolo ISO 1443 Tipo A / B

Comunicación de Datos Sin Contacto

Una vez que las fases de inicialización y anticolisión han terminado, comienza la comunicación de datos.

El Lector de RF envía el primer comando (generalmente una APDU). El protocolo APDU es similar al protocolo T = 1

- Los datos siempre se incluyen en la respuesta
- No Obtener Respuesta

El protocolo es Medio Duplex, el lector de RF no envía la siguiente APDU antes de que la tarjeta responda a la anterior.

Cuando la transacción ha terminado, el lector de RF envía un Comando de Parar o Deseleccionar.

Todas las comunicaciones se interrumpen.

La tarjeta espera entonces una señal de Activación o una salida de campo.

ISO 15693 es un estándar ISO de "Tarjetas de Vecindad", es decir, tarjetas que se pueden leer desde una distancia mayor en comparación con las tarjetas de proximidad.

Los sistemas ISO 15693 operan en la frecuencia de 13,56 MHz, y ofrecen la distancia de lectura máxima de 1 a 1,5 metros.

Puesto que las tarjetas de vecindad tienen que operar a una distancia mayor, el campo magnético necesario es menor (0,15 a 5 A / m) que el de una tarjeta de proximidad (1,5 a 7,5 A / m).

El selector 25 puede activar y / o desactivar los dominios de datos seguros 801, 802, 803 y 804 independientemente unos de los otros.

La representación de los dominios de datos seguros en la figura 1 y en la figura 2 es, por supuesto, esquemática solamente. De acuerdo con una realización preferida de la invención, el selector 25 puede reservar los recursos para los dominios de datos seguros. Por tanto, el selector 25 es capaz de determinar un número de dominios de datos seguros que existen o podrían existir dentro de un entorno de procesador.

En el caso de que al menos dos módulos del programa puedan realizar la acción deseada, el selector de 25 verifica si existe información con respecto a las preferencias para la selección.

Las fuentes de información con respecto a las preferencias para la selección se representan en la figura 3.

La información respecto a las preferencias está incluida, por ejemplo, en la solicitud para una acción deseada que se envía desde la interfaz de terminal.

De acuerdo con otra realización de la invención, la información con respecto a las preferencias está incluida en el módulo de identidad de abonado.

Por supuesto, es posible que la información con respecto a las preferencias esté contenida en más de una fuente de información. Esto incluye que la información con respecto a las preferencias pueda estar incluida tanto en la solicitud como en el módulo de identidad de abonado.

Especialmente en el caso de que no se reciban preferencias de cualquiera de las fuentes de preferencias (solicitud o procesador seguro o equipo de usuario móvil) o en el caso de que existan preferencias en conflicto, es ventajoso que una interfaz de usuario sea activada, con lo que la interfaz de usuario permite una selección del módulo de programa por un usuario del terminal móvil (terminal móvil). Esto permite una interacción por un usuario.

La figura 4 es un diagrama de bloques esquemático de un dispositivo de comunicación móvil de acuerdo con la invención.

Este dispositivo de comunicación móvil podría contener un selector 25 y un selector adicional 26.

Es posible dividir las funciones del selector entre el primer selector 25 y el segundo selector 26.

Esta separación de la funcionalidad del selector permite a los diferentes selectores (unidades de control) hacer uso de las propiedades de cada uno de los otros. Por ejemplo, una Tarjeta de Circuito Integrado Universal UICC, especialmente de acuerdo con los estándares ETSI SCP, es un procesador seguro, aprovisionado en una planta de producción segura. Este procesador seguro puede ser producido como un dispositivo extraíble.

La otra unidad de control es un dispositivo fijo, especialmente no provisto todavía de una clave para las funciones criptográficas como la autenticación / cifrado / descifrado.

La UICC podría aprovisionar un dispositivo de comunicación con algunas teclas delegadas para permitir que el dispositivo de comunicación realizase operaciones tales como las que hace un SIM. Por ejemplo el dispositivo de comunicación puede estar pareado con un SIM e incluso si el SIM no está presente en el dispositivo de comunicación, alguna funcionalidad puede todavía estar disponible para un usuario del dispositivo de comunicación.

Por ejemplo, un pago y / o provisión de boletos es autorizado por la UICC.

La figura 4 muestra un diagrama de bloques de un dispositivo de comunicación móvil de acuerdo con la invención, tal como, por ejemplo, un teléfono celular o un asistente de datos personal (PDA). El dispositivo de comunicación móvil comprende un procesador principal para controlar el funcionamiento del dispositivo de comunicación móvil.

Una unidad de memoria está acoplada a un procesador principal para almacenar datos y aplicaciones que se pueden ejecutar en el procesador. Además, se proporciona una antena de radio en el dispositivo de comunicación móvil para conectar el dispositivo de comunicación móvil a una red de comunicación, tales como, por ejemplo Bluetooth, comunicación de campo cercano (NFC), una red GSM o una red UMTS.

Además, el dispositivo de comunicación móvil comprende una unidad de pantalla y una unidad de entrada, que pueden ser operadas por el usuario del dispositivo de comunicación móvil. La unidad de entrada para la interacción con el usuario puede estar configurada como un teclado.

Por medio de una unidad de lector de tarjetas, el dispositivo de comunicación móvil puede estar conectado a un procesador seguro, por ejemplo un módulo de identidad de abonado (SIM) 10 para formar un dispositivo de comunicación móvil. El procesador seguro 10 puede estar configurado como un SIM de acuerdo con el estándar GSM o un USIM de acuerdo con el estándar UMTS. El SIM 10 es una tarjeta inteligente que comprende un microprocesador y una o más unidades de memoria. Almacena datos preconfigurados relacionados con el usuario y relacionados con la red, en particular datos de identificación de usuario móvil y datos para autentificar el usuario o su dispositivo de comunicación móvil en una red de comunicación móvil. Además, el SIM 10 puede ser capaz de almacenar los datos del usuario durante la operación, como por ejemplo, un libro de teléfonos o mensajes recibidos o enviados con el dispositivo de comunicación móvil. Para el almacenamiento con seguridad de los datos, el SIM 10 contiene una o más aplicaciones para almacenar los datos utilizando algoritmos criptográficos. Otras aplicaciones, tales como, por ejemplo, el Kit de herramientas de aplicación SIM 10 (STK), permiten que el SIM 10 acceda a las funciones del dispositivo de comunicación móvil.

Para la comunicación entre un módulo de radio en el dispositivo de comunicación móvil, se puede proporcionar un mecanismo de comunicación dedicado. Una solución es el Protocolo de Cable Único (SWP), que está siendo estandarizado por el Instituto de Estándares de Telecomunicaciones Europeo (ETSI).

El SWP permite la comunicación bidireccional utilizando un único terminal. Este terminal puede ser un elemento de contacto C6, que no es utilizado en el alcance de los protocolos ISO y los estándares de comunicación móvil. Por lo tanto, con el fin de habilitar la funcionalidad de NFC en un dispositivo de comunicación móvil, una tarjeta SIM 10, que se utiliza en conexión con un terminal móvil que comprende un módulo de radio, debe soportar en particular la comunicación con el dispositivo de comunicación móvil de acuerdo con el SWP usando el elemento de contacto C6 .

Un SIM 10, que no soporta una comunicación de este tipo, es referido como SIM 10 habilitado para NFC en la presente memoria descriptiva y a continuación, mientras que un terminal móvil 100 que comprende un módulo de radio para la comunicación de campo cercano es referido como dispositivo de comunicación móvil habilitado para NFC 50 en la presente memoria descriptiva y a continuación.

Lista de referencias

5:	Interfaz Terminal
10:	Procesador Seguro
15:	Registro
20:	Dominio de Seguridad del Emisor
25:	Unidad de control

26:	Unidad de control
28:	Antena
30:	TSD - TSM Dominio seguro
40:	TSD - TSM Dominio seguro
50:	Dispositivo de comunicación móvil
201:	Módulo de Programa (dominio de datos seguro)
202:	Módulo Programa (dominio de datos seguro)
203:	Dominio de datos Seguro
251:	Administrador RFM de archivos remotos
252:	Administrador de aplicaciones remotas
301:	Módulo de Programa (dominio de datos seguro)
302:	Módulo de Programa (dominio de datos seguro)
303:	Módulo de Programa (dominio de datos seguro)
401:	Módulo de programa (dominio de datos seguro)
402:	Módulo de Programa (dominio de datos seguro)
403:	Módulo de Programa (dominio de datos seguro)
501:	Archivo de Datos
502:	Archivo de Datos
503:	Archivo de Datos
601:	Archivo de Datos
602:	Archivo de Datos
603:	Archivo de Datos
701:	Archivo de Datos
702:	Archivo de Datos
703:	Archivo de Datos
801:	Módulo de Programa (dominio de datos seguro)
802:	Módulo de Programa (dominio de datos seguro)
803:	Módulo de Programa (dominio de datos seguro)
804:	Módulo de programa (dominio de datos seguro)

REIVINDICACIONES

1. Procedimiento de comunicación entre un procesador seguro (10) y una interfaz de terminal (5), en el que

   - la interfaz de terminal (5) envía una solicitud para una interacción deseada con un módulo de programa (201, 202, 203, 301, 302, 303, 401, 402, 403),
   - la interfaz de terminal (5) o una unidad de procesamiento digital conectada a la interfaz de terminal (5) integra un modelo en la solicitud para la interacción deseada,
   - el procesador seguro (10) contiene al menos dos módulos de programa diferentes, teniendo los módulos de programa un parámetro de reconocimiento de modelo para seleccionar automáticamente el módulo de programa mediante la aplicación de reconocimiento de modelo,
   - el procesador seguro (10) y / o un dispositivo de comunicación móvil que está conectado al procesador seguro (10) contiene un selector (25, 26), y
   - el selector (25, 26) puede analizar el modelo y hacer una selección de un módulo de programa seleccionable mediante la aplicación de un reconocimiento de modelo para detectar automáticamente el módulo de programa que es seleccionado

   que se caracteriza porque un subconjunto de los módulos de programa es activado antes del proceso de selección, de tal manera que un módulo de programa puede ser identificado de forma única durante la selección del subconjunto de módulos de programa activados

2. El procedimiento de acuerdo con la reivindicación 1, **que se caracteriza porque** en el caso de que al menos dos módulos de programa (201, 202, 203, 301, 302, 303, 401, 402, 403) sean capaces de realizar la acción deseada, el selector verifica si existe información con respecto a las preferencias para la selección.

3. El procedimiento de acuerdo con la reivindicación 2, **que se caracteriza porque** la información acerca de las preferencias está incluida en la solicitud.

4. El procedimiento de acuerdo con la reivindicación 2 o 3, **que se caracteriza porque** una interfaz de usuario es activada, en el que la interfaz de usuario permite a un usuario del terminal móvil (100) una selección del módulo de programa (201, 202, 203, 301, 302, 303, 401, 402, 403).

5. El procedimiento de acuerdo con cualquiera de las reivindicaciones anteriores, **que se caracteriza porque** el selector (25, 26) analiza el modelo analizando como está codificado un flujo de bits.

6. El procedimiento de acuerdo con la reivindicación 5, **que se caracteriza porque** la solicitud es manejada de acuerdo con el protocolo de Tipo A de ISO 14443.

7. El procedimiento de acuerdo con la reivindicación 5, **que se caracteriza porque** la solicitud es manejada de acuerdo con el protocolo de Tipo B de ISO 14443.

8. Un dispositivo de comunicación móvil conectable a un procesador seguro (10) y a un dominio de datos seguro, en el que

   - el procesador seguro (10) contiene al menos dos módulos de programa que pueden ser activados independientemente uno del otro, teniendo los módulos de programa un parámetro de reconocimiento de modelo para seleccionar automáticamente el módulo de programa mediante la aplicación de reconocimiento de modelo,
   - el dispositivo de comunicación móvil contiene medios para recibir una solicitud que incluye un modelo con información con respecto a una acción deseada,
   - el dominio de datos seguro (10) y / o el dispositivo de comunicación móvil contiene un selector (25, 26), en el que el selector (25, 26) es capaz de analizar el modelo y de realizar una selección del módulo de programa seleccionable mediante la aplicación de un reconocimiento de modelo para detectar automáticamente el módulo de programa que es seleccionado,

   que se caracteriza porque un subconjunto de los módulos de programa es activado antes del proceso de selección, de tal manera que un módulo de programa puede ser identificado de forma única durante la selección del subconjunto de módulos de programa activados.

9. El dispositivo de comunicación móvil de acuerdo con la reivindicación 8, **que se caracteriza porque** el dominio de datos seguro (10) es un módulo de identidad de abonado

10. Procesador seguro, que contiene al menos dos módulos de programa que pueden ser activados independientemente uno del otro, teniendo los módulos de programa un parámetro de reconocimiento de modelo para seleccionar automáticamente el módulo de programa mediante la aplicación de reconocimiento de modelo, y contiene medios para recibir una solicitud que incluye un modelo, en el que

- el procesador seguro contiene un selector (25) y / o es conectable a un selector (26), y
- al menos uno de los selectores (25, 26) es capaz de analizar el modelo y de realizar una selección de un módulo de programa seleccionable mediante la aplicación de un reconocimiento de modelo para detectar automáticamente el módulo de programa que es seleccionado,

que se caracteriza porque un subconjunto de los módulos de programa es activado antes del proceso de selección, de tal manera que un módulo de programa puede ser identificado de forma única durante la selección del subconjunto de módulos de programa activados.

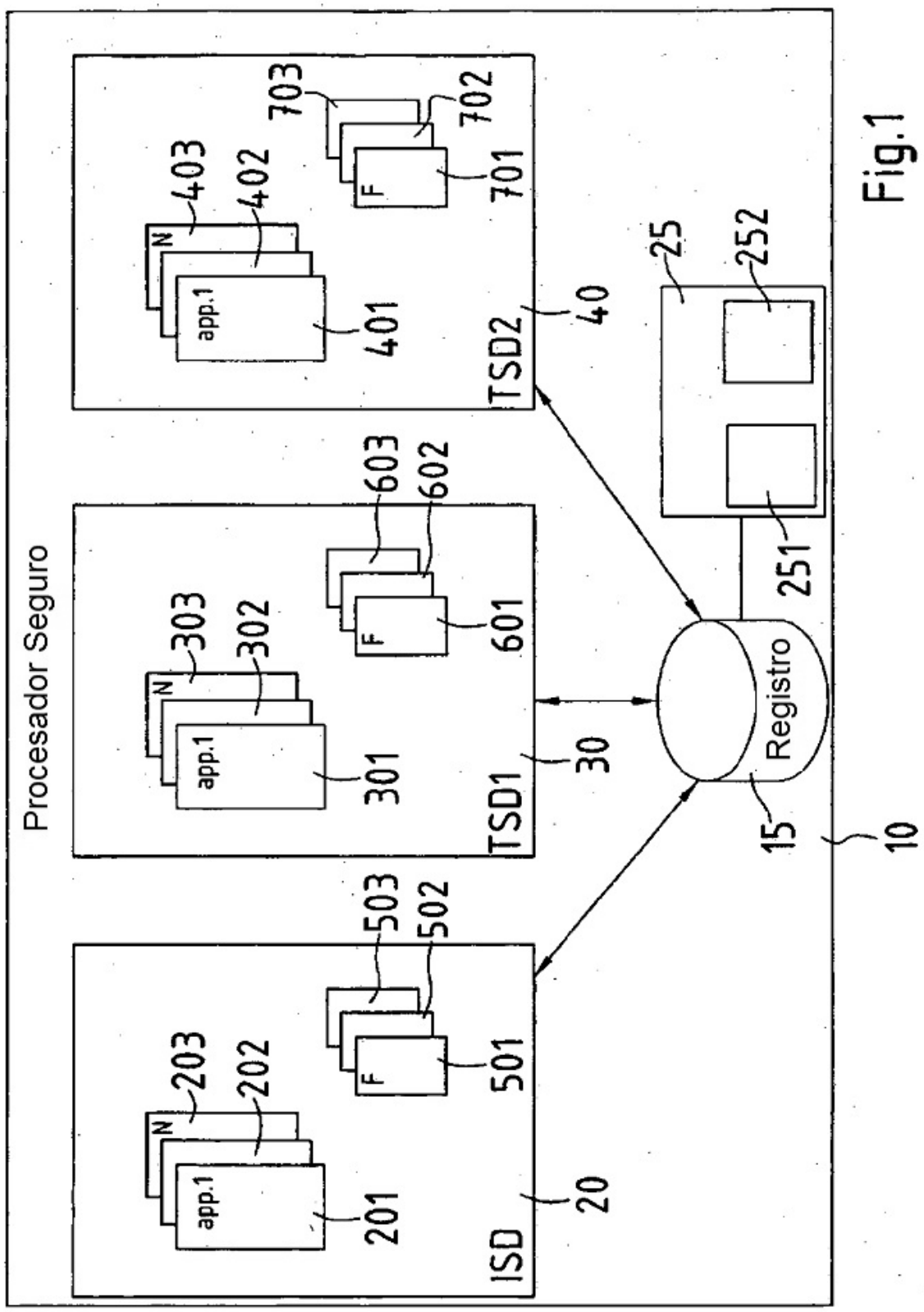
Procesador Seguro
ISD
20
app.1
N
201
202
203
F
501
502
503
TSD1
30
301
302
303
601
602
603
TSD2
40
401
402
403
701
702
703
Registro
15
10
25
251
252

Fig.1

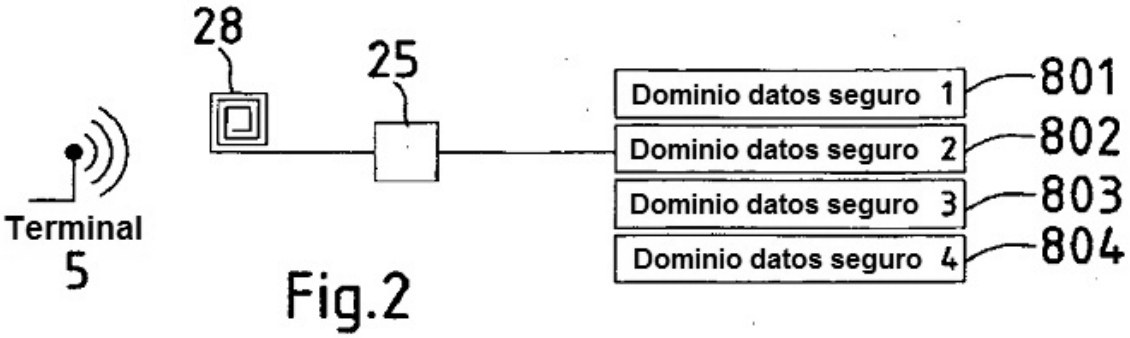

Fig.2

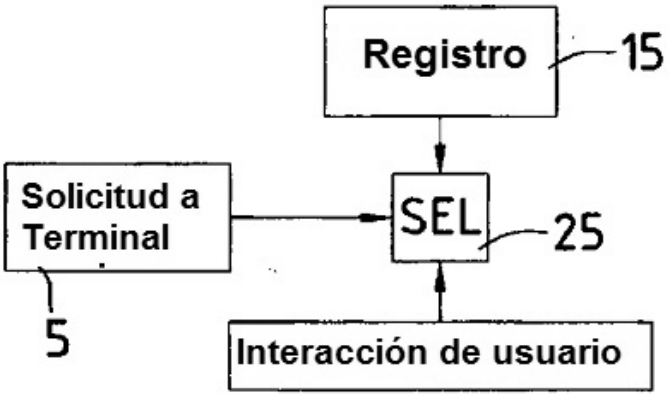

Fig.3

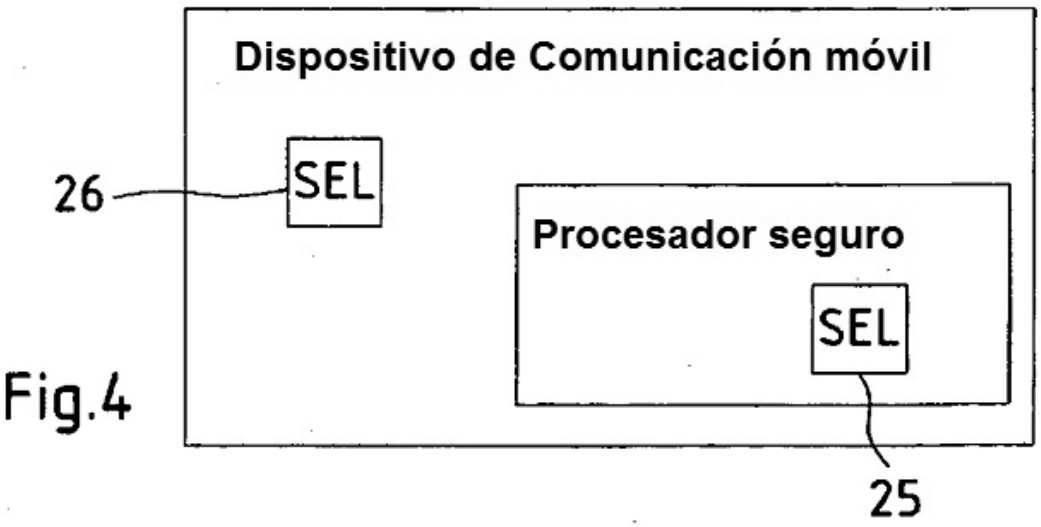

Fig.4