(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 670 439**

(51) Int. CI.:

G06F 21/60 (2013.01)
G06F 21/10 (2013.01)
G06F 21/62 (2013.01)
H04L 29/06 (2006.01)
H04W 12/08 (2009.01)
H04W 4/00 (2008.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **20.08.2012 E 12181078 (2)**

(97) Fecha y número de publicación de la concesión europea: **21.02.2018 EP 2563057**

(54) Título: **Método para el intercambio de datos entre un elemento seguro y un terminal, elemento seguro, y terminal**

(30) Prioridad:

24.08.2011 EP 11006914

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
30.05.2018

(73) Titular/es:

T-MOBILE CZECH REPUBLIC A.S. (100.0%)
Tomickova 2144/1
14900 Praha 4, CZ

(72) Inventor/es:

SMRZ, PETR

(74) Agente/Representante:

ELZABURU, S.L.P

ES 2 670 439 T3

DESCRIPCIÓN

Método para el intercambio de datos entre un elemento seguro y un terminal, elemento seguro, y terminal

Antecedentes

La presente invención se relaciona entre otras cosas con un método para el intercambio de datos entre un elemento seguro y un terminal. Además, la invención se relaciona también con un elemento seguro para intercambiar datos con un terminal, y con un terminal para intercambiar datos con un elemento seguro.

Dentro de la presente descripción, un elemento seguro es un objeto inteligente que está destinado a comunicarse con su entorno. En concreto, el elemento seguro puede cooperar con un terminal. En el contexto de la presente invención, un terminal puede ser un Equipo de Usuario tal como un teléfono móvil o una PDA (asistente digital personal) u otro dispositivo móvil.

En los últimos años las comunicaciones “sin contacto”, o de campo cercano (NFC), han ganado popularidad rápidamente y ahora se despliegan comercialmente muchos servicios sin contacto. Todos los esquemas de transporte públicos alrededor del mundo usan sistemas sin contacto y los pagos sin contacto parece el siguiente paso. La NFC usa normalmente una tarjeta inteligente en forma de “tarjeta de crédito”. Hay disponibles otros formatos de tarjetas inteligentes: de interés particular en las telecomunicaciones móviles es la UICC (Tarjeta de Circuito Integrado Universal) a menudo referida como tarjeta SIM (tarjeta de Módulo de Identificación de Suscripción).

Una extensión mucho más discutida a la NFC es reemplazar el factor de forma de tarjeta de crédito usado en los servicios sin contacto existentes por un teléfono móvil que contiene un Elemento Seguro tal como la tarjeta SIM.

La NFC móvil toma ventaja del hecho de que los usuarios normalmente ya llevan un teléfono móvil y considera a los móviles como personales y de confianza. En un móvil, un usuario podría, en principio, reemplazar las numerosas tarjetas “sin contacto” físicas.

La piedra angular de la NFC móvil es que toda la seguridad y la funcionalidad de la NFC es controlada por el Elemento Seguro. A este respecto, se ha de notar que la SIM es el elemento seguro portátil y estandarizado disponible desplegado más ampliamente con más de 2 mil millones de usuarios alrededor del mundo. Es por tanto altamente deseable usar la plataforma SIM existente en lugar de introducir un nuevo elemento seguro en el teléfono. Además, la SIM es extraíble y los usuarios pueden mantener sus aplicaciones y datos desde un dispositivo móvil con la NFC habilitada a otro. Sin embargo, según la presente invención, son posibles otras soluciones de elemento seguro junto con la tarjeta SIM.

El uso de NFC requiere protocolos de comunicación entre las aplicaciones albergadas por el elemento seguro y las aplicaciones albergadas fuera del elemento seguro, normalmente albergadas por un terminal. Normalmente, las diferentes aplicaciones que usan la funcionalidad NFC requieren diferentes interfaces de usuario o al menos comprenden elementos propietarios en la definición de la interfaz de la aplicación. Además cada aplicación de servicio que tiene como objetivo exponer una interfaz de usuario necesita desplegar su propia interfaz de usuario para todas las posibles plataformas terminales que desea cubrir. Por lo tanto, los usuarios pueden tener una experiencia muy diferente que puede ser dependiente del proveedor de servicio y/o de la lógica de la interfaz de usuario. En caso de que un usuario quiera cambiar el elemento seguro (por ejemplo la tarjeta SIM), es posible que la parte de la interfaz de usuario del terminal potencialmente no coincida con el entorno del elemento seguro. Por lo tanto, sería deseable proporciona protocolos de comunicación estandarizados, especialmente un lenguaje común, para el intercambio de los datos entre el elemento seguro y el terminal.

Compendio

Un objetivo de la presente invención es proporcionar un método para el intercambio de datos entre un elemento seguro y un terminal de manera tal que la misma interfaz de usuario es posible realizarla de manera fácil y rápida para todas las plataformas terminales posibles que la aplicación quiere cubrir, y proporcionar un lenguaje de comunicación común entre un terminal que proporciona la interfaz de usuario y una aplicación de servicio en un elemento seguro.

El objetivo de la presente invención es alcanzado por un método para el intercambio de datos entre un elemento seguro y un terminal según la reivindicación 1.

Según la presente invención es de este modo posible de manera ventajosa, que se pueda conseguir una comunicación fácil y transparente simplemente entre el terminal y el elemento seguro.

Según la presente invención se prefiere, que el elemento seguro comprenda una aplicación de servicio adicional más allá de la al menos una aplicación de servicio en donde una información de STID (Identificación de Tipo de Servicio) adicional , que se relaciona con la aplicación de servicio adicional, se intercambia entre el elemento seguro

y el terminal, en donde la información de STID adicional indica el tipo de servicio de la aplicación de servicio adicional de entre un conjunto predeterminado de diferentes tipos de servicio.

De este modo, es posible de manera ventajosa, que una multitud de servicios diferentes se puedan hacer disponibles a un usuario del elemento seguro y del terminal.

Además, según la presente invención se prefiere que la información de STID y/o la información de STID adicional sea o sean codificadas por medio de una máscara de bits de tipo de servicio que comprende una pluralidad de bits de tipo de servicio como parte de una información de AID (ID de aplicación), en donde cada uno de la pluralidad de bits de tipo de servicio de la máscara de bits de tipo de servicio se relacionan con un tipo de servicio.

De este modo, es ventajosamente posible que sea posible que se consiga un alto grado de flexibilidad, que refleje las diferentes necesidades de los usuarios.

Aún además, según la presente invención se prefiere que un conjunto de entre una pluralidad de tipos de servicio se definan para la al menos una aplicación de servicio y/o para la aplicación de servicio adicional, en donde el conjunto de tipos de servicio comprende cualquier combinación de un máximo de treinta y dos tipos de servicios diferentes.

De este modo, según la presente invención es ventajosamente posible, que mediante el uso de un comparablemente pequeño número de diferentes tipos de servicios se puedan abordar todas las situaciones requeridas.

Según aún otra realización de la presente invención, se prefiere que la información de STID se refiera a uno de los tipos de servicios y/o la información de STID adicional se refiera a uno de los tipos de servicios.

La presente invención también se relaciona con un elemento seguro para el intercambio de datos con un terminal dentro del cual se ubica el elemento seguro según la reivindicación 4.

Además, según la presente invención – y con respecto al elemento seguro - se prefiere que el elemento seguro comprenda una aplicación de servicio adicional más allá de la al menos una aplicación de servicio en donde el elemento seguro se proporciona de manera tal que una información de STID (Identificación de Tipo de Servicio) adicional, que se relaciona con la aplicación de servicio adicional, se intercambie entre el elemento seguro y el terminal, en donde la información de STID adicional indica el tipo de servicio de la aplicación de servicio adicional de entre un conjunto predeterminado de diferentes tipos de servicio.

Según una realización adicional de la presente invención – y con respecto al elemento seguro –se prefiere que la información de STID y/o la información de STID adicional sea o sean codificadas por medio de una máscara de bits de tipo de servicio que comprende una pluralidad de bits de tipo de servicio como parte de una información de AID (ID de aplicación), en donde cada uno de la pluralidad de bits de tipo de servicio de la máscara de bits de tipo de servicio se relacionan con un tipo de servicio.

Además, según la presente invención – y con respecto al elemento seguro - se prefiere que un conjunto de tipos de servicios se defina para la al menos una aplicación de servicio y/o para la aplicación de servicio adicional, en donde el conjunto de tipos de servicios comprende cualquier combinación de un máximo de treinta y dos tipos de servicios diferentes.

Según una realización adicional de la presente invención – y con respecto al elemento seguro -, se prefiere que la información de STID se refiera a uno de los tipos de servicios y/o la información de STID adicional se refiera a uno de los tipos de servicios.

La presente invención también se relaciona con un terminal para el intercambio de datos con un elemento seguro según la reivindicación 8.

Además, según la presente invención – y con respecto al terminal - se prefiere, que el elemento seguro comprenda una aplicación de servicio adicional más allá de la al menos una aplicación de servicio en donde el elemento seguro se proporciona de manera tal que la información de STID (Identificación de Tipo de Servicio) adicional, que se relaciona con la aplicación de servicio adicional, se intercambia entre el elemento seguro y el terminal, en donde la información de STID adicional indica el tipo de servicio de la aplicación de servicio adicional fuera del conjunto predeterminado de diferentes tipos de servicios.

Según una realización adicional de la presente invención – y con respecto al terminal -, se prefiere que la información de STID y/o la información de STID adicional sea o sean codificadas por medio de una máscara de bits de tipo de servicio que comprende una pluralidad de bits de tipo de servicio como parte de una información de AID (ID de aplicación) para simplificar y acelerar el acceso de la SEUI a la información de STID, en donde cada uno de la pluralidad de bits de tipo de servicio de la máscara de bits de tipo de servicio se relaciona con un tipo de servicio.

Además, según la presente invención – y con respecto al terminal –se prefiere que se defina un conjunto de una pluralidad de tipos de servicios para la al menos una aplicación de servicio y/o para la aplicación de servicio

adicional, en donde el conjunto de tipos de servicios comprende cualquier combinación de un máximo de treinta y dos tipos de servicios diferentes.

Además, la presente invención se relaciona con un programa que comprende un código de programa legible por ordenador que, cuando se ejecuta en un ordenador, provoca que el ordenador realice un método inventivo según la presente invención.

La presente invención también se relaciona con un producto programa informático para el intercambio de datos entre un elemento seguro y un terminal, comprendiendo el producto programa informático un programa informático almacenado en un medio de almacenamiento, comprendiendo el programa informático código de programa que, cuando se ejecuta en un ordenador, provoca que el ordenador realice un método inventivo según la presente invención.

Estas y otras característica, funciones y ventajas de la presente invención resultarán aparentes a partir de la siguiente descripción detallada, tomada en conjunción con los dibujos adjuntos, que ilustran, a modo de ejemplo, los principios de la invención. La descripción es dada sólo por el bien del ejemplo, sin limitar el alcance de la invención. Las figuras de referencia citadas a continuación se refieren los dibujos adjuntos.

Breve descripción de los dibujos

La Figura 1 ilustra de manera esquemática un entorno de Plataforma Global actual de un elemento seguro según la técnica anterior.

Las Figuras 2 y 3 ilustran de manera esquemática representaciones de un entorno de un elemento seguro según la presente invención.

La Figura 4 ilustra de manera esquemática un ejemplo de una estructura de mensaje según la presente invención.

La Figura 5 ilustra de manera esquemática un ejemplo de un elemento seguro según la presente invención.

Las Figuras 6 y 7 ilustran de manera esquemática flujos de mensajes relacionados con la comunicación entre el elemento seguro y el terminal.

Descripción detallada

La presente invención se describirá con respecto a realizaciones concretas y con referencia a ciertos dibujos pero la invención no se limita a estos sino sólo por las reivindicaciones. Los dibujos descritos son sólo esquemáticos y no son limitantes. En los dibujos, el tamaño de algunos de los elementos puede ser exagerado y no mostrarse a escala por propósitos ilustrativos.

Allá donde se use un artículo indefinido o definido cuando se hace referencia a un nombre singular, por ejemplo “un”, “uno”, “el”, este incluye el plural de ese sustantivo a menos que se haya fijado específicamente otra cosa.

Además, los términos primero, segundo, tercero y similares en la descripción y en las reivindicaciones se usan para distinguir entre elementos similares y no necesariamente para describir un orden secuencial o cronológico. Se ha de comprender que los términos así usados son intercambiables bajo las circunstancias apropiadas y que las realizaciones de la invención descrita en la presente memoria son capaces de realizar la operación en otras secuencias distintas de las descritas o ilustradas en la presente memoria.

En la Figura 1, se muestra de manera esquemática un entorno de Plataforma Global actual de un elemento seguro según la técnica anterior. Un terminal 10 comprende un módulo 101 de gestión de servicio o una unidad 101 de gestión de servicio. El módulo 101 de gestión de servicio comprende un primer módulo 102 de la interfaz de usuario conectable para una primera aplicación de servicio y un segundo módulo 103 de la interfaz de usuario conectable para una segunda aplicación de servicio. El terminal 10 se comunica con un elemento seguro 20, por ejemplo, a través de un enlace A ISO 7816 y usando preferiblemente una entidad de ejecución ACP (entidad de ejecución de la Política de Control de Acceso) 104 o un certificado de capacidad UICC. El elemento seguro 20 comprende una aplicación de CRS (aplicación de Servicio de Registro sin Contacto) 21 y una aplicación CREL (aplicación Receptora de Eventos de Registro sin Contacto) 22 así como una aplicación 23 de servicio y una aplicación 24 de servicio adicional. La aplicación 23 de servicio también es llamada primera aplicación 23 de servicio y la aplicación 24 de servicio adicional también es llamada segunda aplicación 24 de servicio. La primera aplicación 23 de servicio en el elemento seguro 20 se comunica con el primer módulo 102 de la interfaz de usuario conectable y la segunda aplicación 24 de servicio en el elemento seguro 20 se comunica con el segundo módulo 103 de la interfaz de usuario conectable. La primera aplicación 23 de servicio comprende un módulo 23.1 de tarjeta básico y una tarjeta 23.2 extendida específica de banco que proporciona características de o al primer módulo 102 de la interfaz de usuario conectable. La segunda aplicación 24 de servicio comprende un módulo 24.1 de tarjeta básico y una tarjeta 24.2 extendida específica de banco que proporciona características de o al segundo módulo 103 de la interfaz de usuario conectable. Esto significa que las aplicaciones 23, 24 de servicio individuales se comunican con sus respectivas interfaces de usuario, esto es los módulos 102, 103 de la interfaz de usuario conectables de manera propietaria. De

manera adicional, la aplicación 21 de CRS en el elemento seguro 20 proporciona una funcionalidad de gestión de la aplicación. Esta funcionalidad de gestión de la aplicación se puede consultar para devolver una lista de todas las aplicaciones de servicio que la aplicación 21 de CRS conoce. El terminal 10 puede registrar también para recibir diversos eventos desde la aplicación 21 de CRS. Cualquier aplicación de la interfaz 102, 103 de usuario puede por lo tanto hacer una lista de las aplicaciones 23, 24 de servicio registradas, abrir un canal para cualquiera de ellas e iniciar el envío de comandos. El pre requisito aquí es que la respectiva interfaz de usuario pase de manera exitosa las pruebas de seguridad del entorno del elemento seguro dado por la Plataforma Global. El estándar de la Plataforma Global es una iniciativa de los líderes mundiales de la industria de servicios financieros. Este ofrece un marco estándar para poner muchas aplicaciones diferentes en un tarjeta inteligente basada en el dispositivo personal. La Plataforma Global define una manera para garantizar el aislamiento y seguridad de cada aplicación. Esto implica que el operador de transporte puede controlar la venta de entradas y el banco su aplicación de pago, mientras que el operador móvil mantiene un control completo de su suscripción a los servicios móviles. Esto también define los mecanismos para añadir y eliminar de manera segura estas aplicaciones en el dispositivo SIM en cualquier momento. Por lo tanto, la tarjeta SIM se divide en espacios privados independientes llamados elementos seguros. Cada proveedor de servicio tiene su propio dominio de seguridad y mantiene un control total sobre este. En el ejemplo mostrado en la Figura 1, se proporciona un registro 25 de Plataforma Global en el elemento seguro 20. Además en el ejemplo dado, se muestra un chip NFC o módulo NFC 30 que se comunica con el terminal 10 a través de un enlace B de comunicación I2C y con el elemento seguro 20 a través de un enlace C de comunicación HC SWP 2.

Según la técnica anterior – como se muestra en la Figura 1 - cada aplicación 23, 24 de servicio que desee exponer una interfaz de usuario necesita desplegar su propia interfaz de usuario para todas las posibles plataformas de terminal que desea cubrir. Esto lleva al hecho de que por ejemplo dos proveedores de tarjetas bancarias diferentes pueden tener dos API diferentes (Interfaces de programación de aplicación) hacia sus elementos seguros y por lo tanto dos UI (interfaces de usuario) diferentes hacia el usuario. Está el hecho de que los mismos servicios viniendo de proveedores diferentes pueden y tendrán hoy en día diferentes API expuestas por el applet que se ejecuta en el elemento seguro y esto puede implicar que, por ejemplo, una tarjeta del banco HSBC tendrá una UI diferente que, por ejemplo, una tarjeta de CitiBank incluso aunque ambas son tarjetas de crédito y sus versiones de plástico son exactamente la misma para todos lo bancos. Esto puede y probablemente lleva a una situación en la que un usuario tiene diferentes experiencias de usuario dependiendo del proveedor de servicio y dependiendo de la lógica de la interfaz de usuario. Además, en el caso de que un usuario quiera cambiar el elemento seguro 20 por otro elemento seguro (o cambiar el terminal 10), el usuario terminaría con una interfaz de usuario que potencialmente no coincide con el entorno del elemento seguro o viceversa.

Según la presente invención, se proponen un método, un elemento seguro y un terminal para proporcionar un intercambio de datos entre un elemento seguro 20 por un lado y un terminal 10 por el otro. Esto se muestra en las Figuras 2 a 7: las Figuras 2 y 3 ilustran de manera esquemática representaciones de un entorno de un elemento seguro 20 según la presente invención, la Figura 4 ilustra de manera esquemática un ejemplo de una estructura de mensaje según la presente invención, la Figura 5 ilustra de manera esquemática un ejemplo de un elemento seguro 20 según la presente invención, y las Figuras 6 y 7 ilustran de manera esquemática la comunicación entre el elemento seguro 20 y el terminal 10.

Según la presente invención, se propone un protocolo de aplicación tal que la funcionalidad del elemento seguro se resuelva en el nivel de las aplicaciones de servicio individuales y de manera tal que se usa un lenguaje común de comunicación entre la interfaz de usuario (del terminal 10) y las aplicaciones de servicio (del elemento seguro 20), cf. especialmente las Figuras 2 y 3.

Entonces el resultado del protocolo inventivo es proporcionar un incentivo para proporcionar applets de servicio del mismo tipo (misma STID) tal que para ofrecer el mismo conjunto de API a la aplicación de la UI del terminal para facilitar la capacidad de tener la misma experiencia de usuario a lo largo de los mismos servicios desde diferentes proveedores y de este modo simplificar el desarrollo de la aplicación de la UI. Según la presente invención, es importante que se proporcione un identificador STID que permita la categorización de los servicios y por tanto de los conjuntos de API que usan. Esto es comparable con una ID de Clase de Servicio donde también cada clase ofrece un conjunto de API dado de manera opuesta a la situación según la técnica anterior donde cada servicio que se ejecuta en la SIM puede exponer una API arbitraria. La única API dada (esto es predeterminada) hoy en día es la de CRS y CREL (y esta necesitaría ser extendida para negociar con la STID) y, en caso de pago, tenemos EMVCo que sólo define requisitos de seguridad pero no API. Los applets de servicio (por ejemplo la UI con características específicas de Banco) pueden exponer ahora una API arbitraria que lleve al problema descrito anteriormente (diferentes UI para el mismo servicio desde diferentes proveedores y un desarrollo de las UI del terminal complejo).

El terminal 10 comprende una interfaz 11 de usuario de elemento seguro (SEUI) que proporciona el protocolo de comunicación entre el terminal 10 y el elemento seguro 20. El terminal 10 comunica con el elemento seguro 20, por ejemplo, a través de un enlace A ISO 7816 y usando preferiblemente una entidad de ejecución ACP (entidad de ejecución de Política de Control de Acceso) o un certificado de capacidad UICC. El elemento seguro 20 comprende una aplicación 21 de CRS (aplicación de Servicio de Registro sin Contacto) y una aplicación CREL (aplicación receptora de Eventos de Registro sin Contacto) 22 así como una aplicación 23 de servicio (esto es al menos una

aplicación 23 de servicio). Cada aplicación de servicio está identificada por un identificador único llamado identificador de aplicación o ID de aplicación o AID. La aplicación 21 de CRS tiene o proporciona características de una interfaz de usuario y se comunica con la SEUI 11 en base a un protocolo de solicitud y respuesta. La aplicación 23 de servicio en el elemento seguro 20 se comunica con la interfaz 11 de usuario del elemento seguro (SEUI) en el terminal 10. La aplicación 23 de servicio comprende un módulo 23.1 de tarjeta básico y un módulo 23.2 de tarjeta extendido específico de banco. El módulo 23.1 de tarjeta básico no comprende una interfaz de usuario (o no necesita funcionalidades de una interfaz de usuario), aunque el módulo 23.2 de tarjeta extendido específico de banco no proporciona las características de una interfaz de usuario y se comunica con la SEUI 11 en base a un protocolo de solicitud y respuesta (designado por el signo de referencia RR). El protocolo de solicitud y respuesta entre la SEUI 11 y la aplicación 21 de CRS se refiere de manera especial a la solicitud de una lista de las aplicaciones disponibles en el elemento seguro 20 (y la respectiva respuesta desde la aplicación 21 de CRS). El protocolo de solicitud y respuesta entre la SEUI 11 y la aplicación 23 de servicio se refiere de manera especial a las estructuras de solicitud y respuesta. Es posible según la presente invención que los eventos (designados por el signo de referencia E en la Figura 2) puedan ser abordados por el CRS 21, y/o el CREL y/o la aplicación 23 de servicio.

En el lado del terminal 10, es posible obtener una simplificación significativa mediante la implementación de la presente invención: el concepto de un tipo de servicio es usado de manera tal que es posible usar las parejas de estructura comando y respuesta para

- definir un número de estructuras de solicitud tal que cualquier aplicación de servicio de un tipo de servicio específico responda a estas estructuras de solicitud de una manera conocida y definida,
- definir un número de eventos y su significado de manera tal que cualquier aplicación de servicio que entrega un servicio de un tipo específico responda de una manera conocida, y
- definir estructuras de respuesta para las excepciones.

Según la presente invención, una información de STID (Identificación de Tipo de Servicio) se relaciona con la aplicación de servicio del elemento seguro 20. El elemento seguro 20 puede (y preferiblemente lo hace) comprender una aplicación 24 de servicio adicional (sólo representada en la Figura 2). La aplicación 24 de servicio adicional se relaciona con una información de STID adicional. En el contexto de la presente invención, la aplicación 23 de servicio y la aplicación 24 de servicio adicional se llaman también primera aplicación 23 de servicio y segunda aplicación 24 de servicio. Asimismo, la información de STID y la información de STID adicional se llaman también primera información de STID y segunda información de STID.

En la Figura 3, se muestran de manera esquemática detalles adicionales del método inventivo además de elementos o componentes ya mostrados en la Figura 2. En la Figura 3 la aplicación 23 de servicio comprende un primer módulo de cumplimiento (o primera unidad de cumplimiento SEUI) que es referida por medio del signo 23.3 de referencia en la Figura 3. Además, la aplicación CREL 22 comprende un segundo módulo de cumplimiento SEUI (o segunda unidad de cumplimiento SEUI) que es referida por medio del signo 22.1 de referencia en la Figura 3. Por medio del primer módulo o unidad 23.3 de cumplimiento SEUI, la aplicación de servicio resulta compatible con la SEUI, y por medio del módulo o unidad 22.1 de cumplimiento SEUI, la aplicación CREL 22 resulta compatible con la SEUI. Este cumplimiento es llevado a cabo por medio del uso de un protocolo de intercambio de datos tal que no se usen ningún elemento propietario específico de ningún operador o proveedor específico.

Según la presente invención, la información de STID y/o la información de STID adicional (o primera y segunda información de STID) es codificada mediante el uso de un número de bits y usando una máscara de bits en el caso de que la información de STID sea parte de una información de AID. En caso de que la información de STID sea transmitida como parte de un mensaje entre el elemento seguro 20 y el terminal 10, la información de STID se transmite como un número y sin una máscara de bits codificadora. La Figura 4 muestra un ejemplo de una estructura de mensaje según la presente invención a usar en la comunicación entre el elemento seguro 20 y el terminal 10. El signo 211 de referencia se refiere al número de bytes del mensaje. El mensaje comprende una primera parte 205 correspondiente a la cabecera del mensaje, y una segunda parte 206, correspondiente al cuerpo del mensaje. La cabecera 205 del mensaje comprende de manera especial dos bytes, indicados como el byte número 0 y el byte número 1 en la Figura 4. El primer byte, el byte número 0, comprende una primera parte 207, correspondiente a la información de STID (codificada como un número), y una segunda parte 208, correspondiente a la información de versión. La primera parte 207 del primer byte corresponde en el ejemplo dado en la Figura 4 a 5 bits designados mediante el signo 212 de referencia, y la segunda parte 208 del primer byte corresponde en el ejemplo dado en la Figura 4 a los tres bits designados mediante el signo 213 de referencia. Esto significa que la información de STID es codificada como un número por medio de cinco bits, y la información de versión es codificada por medio de tres bits. El segundo byte corresponde al RRID (ID de Solicitud y Respuesta). De este modo, son posibles definir 256 parejas de solicitud y respuesta por versión y por STID. El uso de tres bits para indicar la versión implica que son posibles ocho diferentes versiones posibles por RRID.

La codificación de la STID por medio de (en el ejemplo dado en la Figura 4) cinco bits implica que se pueden codificar 32 tipos de servicios diferentes (de las aplicaciones 23, 24 de servicio). Esto permite cambios mínimos en

los componentes existentes y permite la selección de todas las aplicaciones 23, 24 de servicio de un tipo concreto utilizando un proceso de selección de AID parcial (esto es la determinación del tipo de servicio basado en si un determinado bit o unos determinados bits de la cabecera 205 del mensaje (o ID de aplicación AID) es o son establecidos o no). Por medio del uso de una máscara de bits, una aplicación 23, 24 de servicio puede implementar una pluralidad de tipos de servicios.

Por ejemplo, por medio del uso de 32 bits para definir la información de STID, es posible que un conjunto de entre una pluralidad de diferentes tipos de servicios se pueda definir para una aplicación de servicio dada. Por ejemplo, el conjunto de tipos de servicios comprende un primer tipo de servicio, un segundo tipo de servicio, un tercer tipo de servicio, un cuarto tipo de servicio, un quinto tipo de servicio y un sexto tipo de servicio, en donde el primer tipo de servicio es un tipo de servicio por defecto. Es también posible según la presente invención que se use otro conjunto de tipos de servicios que comprenda menos de seis tipos de servicios o más de seis tipos de servicios hasta un máximo de 32 tipos de servicios.

Dentro de los tipos de servicios, el primer tipo de servicio corresponde, por ejemplo, a información básica intercambiada y es un tipo de servicio por defecto, el segundo tipo de servicio corresponde, por ejemplo, a aspectos relacionados con el pago, el tercer tipo de servicio corresponde, por ejemplo, a aspectos relacionados con la venta de entradas, en donde el cuarto tipo de servicio corresponde, por ejemplo, a aspectos relacionados con el transporte público, en donde el quinto tipo de servicio corresponde, por ejemplo, con aspectos relacionados con los beneficios por fidelidad, y en donde el sexto tipo de servicio corresponde, por ejemplo, con aspectos relacionados con la banca. Son posibles otros tipos de servicios según la presente invención hasta un número máximo de 32 diferentes tipos de servicios. Dichos tipos de servicios adicionales podrían relacionarse, por ejemplo, con los servicios de registro en un aeropuerto o similar.

El primer tipo de servicio “intercambio de información de metadatos” es un tipo que cada aplicación de servicio ha de soportar como un conjunto funcional común (por ejemplo las consultas relacionadas con los metadatos tales como la información de proveedor, icono, diseño gráfico, etc) y por lo tanto no tiene un valor de bandera (o bit) definido en la cabecera de mensaje o AID. Cada servicio que reivindica ser de un tipo particular soporta un subconjunto de las parejas de solicitud y respuesta definidas y plantea un conjunto definido de eventos. Esto significa también que cualquier aplicación de servicio necesita responder a cualquier a cualquier solicitud de una manera definida. De este modo, es ventajosamente posible según la presente invención que una aplicación de servicio pueda soportar una pluralidad de diferentes tipos de servicios (estableciendo los bits apropiados en la máscara de bits). Esto está en contraste con el actual comando GET STATUS para el Campo de Datos de CRS, que da instrucciones a la aplicación 21 de CRS para devolver un vector que puede contener de manera opcional información de la Familia de la Aplicación (que es de un byte de longitud).

El uso de una máscara de bits permite hasta 32 tipos de servicios diferentes (al usar cinco bits para codificar la STID) que deberían ser suficientes para realizar la diferenciación requerida para las diferentes aplicaciones de servicio. La aplicación 21 de CRS y la aplicación CREL 22 no necesitan su propia STID ya que estos ya tienen su AID respectivo.

Según la presente invención, las parejas de solicitud y respuesta se definen como mensajes de vectores de bytes que tienen campos de ya sea longitud fija o variable como se representa en la Figura 4. Las correspondientes parejas de mensajes de solicitud y respuesta tienen valores de información RRID e información de STID que coinciden.

En caso de mensajes potencialmente largos y en caso de que el protocolo subyacente limite el tamaño del paquete, la aplicación de la interfaz de usuario solicita datos adicionales mediante el envío repetido de la cabecera de solicitud hasta que haya recibido la estructura completa de vuelta. La cabecera de mensaje reserva, por ejemplo, cinco bits (lo que resulta en 32 posibles tipos de servicios) para permitir a la información de STID ser servida a los diferentes servicios por la misma aplicación de servicio sobre el mismo canal del protocolo subyacente, por ejemplo, sobre el mismo canal APDU. Con la estructura propuesta de cabecera, son posibles 256 diferentes parejas de solicitud y respuesta (relacionadas a los 256 posibles valores RRID diferentes) por versión y por STID.

Para definir la longitud del mensaje, es posible usar ya sea una longitud fija codificada, por ejemplo, por medio de la tupla de información RRID e información de STID, o una longitud variable, por ejemplo, por medio de un vector de bytes prefijado por una indicación de dos bytes que transporta la longitud, por ejemplo en la codificación big-endian.

El tipo de estructura (esto es el orden de los campos tal y como se presentan en el cuerpo del mensaje y su significado) está dado por la tupla de información RRID e información de STID. La versión empieza desde cero y permite añadir nuevos campos en el final de la estructura sin necesidad de definir un nuevo tipo de estructura, esto es uno no puede jamás modificar el diseño del cuerpo del mensaje existente simplemente aumentando el número de versión.

Se ha de entender que según la presente invención, un mensaje de solicitud puede tener una estructura de cuerpo diferente que un mensaje de repuesta, incluso aunque tenga la misma cabecera, esto es, la misma información de STID y la misma información RRID.

La codificación de eventos es muy simple según la presente invención. Cualquier evento abordado por ya sea una aplicación 23, 24 de servicio o por la aplicación 22 CREL transporta dos bytes de la cabecera del mensaje SEUI como su carga útil la aplicación de origen acepta como una solicitud posterior para responder con la estructura de datos pertinente, esto es, tras la recepción de un evento, la aplicación de la interfaz de usuario emitiría una solicitud que contiene la cabecera que ha recibido en la carga útil del evento.

En la Figura 5. se muestra de manera esquemática un ejemplo de un elemento seguro 20 según la presente invención para el caso de una aplicación 23 de servicio que tiene dos tipos de servicios. La información de AID de identificación de aplicación contiene un valor tal que los bits que se relacionan, por ejemplo, con un segundo tipo de servicio “aspectos relacionados con el pago” y con el quinto tipo de servicio “aspectos relacionados con los beneficios por fidelidad” se establecen (por ejemplo correspondientes al valor decimal “9”). La aplicación 23 de servicio comprende el módulo 23.3 de cumplimiento SEUI (o el primer módulo de cumplimiento SEUI). El segundo tipo de servicio “aspectos relacionados con el pago” (o “aspectos relacionados con el pago EM-VCo”) es realizado por medio de una interfaz 23.4 de programación de la aplicación de pago SEUI (API de pago) y un módulo 23.6 de pago EMVCo propietario. El quinto tipo de servicio “aspectos relacionados con los beneficios por fidelidad” es realizado por medio de una interfaz 23.5 de programación de la aplicación de fidelidad SEUI y un módulo 23.7 de beneficios por fidelidad propietario.

En las Figuras 6 y 7, se ilustra esquemáticamente el flujo de mensajes relacionados con la comunicación entre el elemento seguro 20 y el terminal 10.

La Figura 6 muestra el flujo de mensajes entre el terminal 10 (o la SEUI 11), la aplicación 23 de servicio del elemento seguro 20, y la aplicación 21 de CRS del elemento seguro 20. En un primer mensaje 61, se envía mensaje de lista (dependiente de la máscara de STID) desde el terminal 10 (o la SEUI 11) hasta la aplicación 21 de CRS. En un segundo mensaje 62, se envía un mensaje de selección (dependiente del ID de aplicación, AID) desde el terminal 10 (o la SEUI 11) hasta la aplicación 21 de CRS. En un tercer mensaje 63, se envía un mensaje de solicitud (dependiente de la cabecera SEUI) desde el terminal 10 (o la SEUI 11) hasta la aplicación 23 de servicio. En un cuarto mensaje 64, se envía un mensaje de respuesta (que indica la cabecera SEUI y que comprende una estructura de respuesta) desde la aplicación 23 de servicio hasta el terminal 10 (o la SEUI 11). De este modo, el primer y segundo mensajes 61, 62 corresponden a un estricto flujo simbólico que es abordado por las especificaciones de la Plataforma Global.

La Figura 7 muestra el flujo de mensajes entre el terminal 10 (o la SEUI 11), una entidad desencadenante de eventos (por ejemplo ya sea la aplicación 23 de servicio o la aplicación 22 CREL del elemento seguro 20), la aplicación 21 de CRS del elemento seguro 20, y la aplicación 23 de servicio. En un primer mensaje 71, se desencadena un evento, por ejemplo desde la entidad desencadenante que puede ser, por ejemplo, la aplicación 23 de servicio o la aplicación 22 CREL del elemento seguro 20. El evento (que es dependiente del AID y de la cabecera de la SEUI) se envía al terminal 10 (o la SEUI 11). En un segundo mensaje 72, se envía un mensaje de selección (dependiente de un ID de aplicación, AID) desde el terminal 10 (o la SEUI 11) hasta la aplicación 21 de CRS. En un tercer mensaje 73, se envía un mensaje de solicitud de la SEUI (dependiente de una cabecera de la SEUI) desde el terminal 10 (o la SEUI 11) hasta la aplicación 23 de servicio. En un cuarto mensaje 64, se envía un mensaje de respuesta (que indica la cabecera de la SEUI y que comprende una estructura de respuesta) desde la aplicación 23 de servicio hasta el terminal 10 (o la SEUI 11). De este modo, el segundo mensaje 72 corresponde a un estricto flujo simbólico que es abordado por las especificaciones de la Plataforma Global.

REIVINDICACIONES

1. Método para el intercambio de datos entre un elemento seguro (20) y un terminal (10), en donde el elemento seguro (20) comprende

- una aplicación (21) de CRS (aplicación del Servicio de Registro sin Contacto),
- una aplicación CREL (aplicación Receptora de Eventos de Registro sin Contacto) (22), y
- al menos una aplicación (23) de servicio,

y en donde el terminal (10) comprende una SEUI (Interfaz de Usuario del Elemento Seguro) (11) que interactúa con al menos una de entre la aplicación (21) de CRS, la aplicación CREL (22) y la aplicación (23) de servicio, en donde una información de STID (Identificación del Tipo de Servicio), que se relaciona con la al menos una aplicación (23) de servicio, se intercambia entre el elemento seguro (20) y el terminal (10), en donde la información de STID indica el tipo de servicio de la al menos una aplicación (23) de servicio de entre un conjunto predeterminado de diferentes tipos de servicios, en donde el elemento seguro (20) comprende una aplicación (24) de servicio adicional más allá de la al menos una aplicación (23) de servicio en donde una información de STID (Identificación de Tipo de Servicio) adicional, que se relaciona con la aplicación (24) de servicio adicional, se intercambia entre el elemento seguro (20) y el terminal (10),

en donde la información de STID adicional indica el tipo de servicio de la aplicación (24) de servicio adicional de entre el conjunto predeterminado de diferentes tipos de servicios.

en donde la información de STID y/o la información de STID adicional se codifican por medio de una máscara (210) de bits de tipo de servicio que comprende una pluralidad de bits de tipo de servicio como parte de una información de AID (ID de aplicación), en donde cada uno de la pluralidad de bits de tipo de servicio de la máscara (210) de bits de tipo de servicio se relacionan con un tipo de servicio.

en donde la información de STID permite la categorización de las aplicaciones de servicio y de los conjuntos de API que usan las aplicaciones de servicio y en donde las aplicaciones de servicio que tienen la misma STID ofrecen el mismo conjunto de API a la aplicación de la interfaz de usuario del terminal (10).

2. Método según la reivindicación 1, en donde se define un conjunto de una pluralidad de tipos de servicios para la al menos una aplicación (23) de servicio y/o para la aplicación (24) de servicio adicional, en donde el conjunto de tipos de servicios comprende cualquier combinación de un máximo de treinta y dos diferentes tipos de servicios.

3. Método según una de las reivindicaciones precedentes, en donde la información de STID se refiere a uno de los tipos de servicios y/o la información de STID adicional se refiere a uno de los tipos de servicios.

4. Elemento seguro (20) para el intercambio de datos con un terminal (10), en donde el elemento seguro (20) comprende

- una aplicación (21) de CRS (aplicación de Servicio de Registro sin Contacto),
- una aplicación CREL (aplicación Receptora de Eventos de Registro sin Contacto) (22),
- al menos una aplicación (23) de servicio,

y en donde al menos una de entre la aplicación (21)de CRS, la aplicación CREL (22) y la aplicación (23) de servicio se configuran para interactuar con una SEUI (Interfaz de Usuario del Elemento seguro) (11) del terminal (10),

en donde el elemento seguro (20) se adapta para intercambiar una información de STID, que se relaciona la al menos una aplicación (23) de servicio, entre el elemento seguro (20) y el terminal (10), en donde la información de STID indica el tipo de servicio de la al menos una aplicación (23) de servicio de entre un conjunto predeterminado de diferentes tipos de servicios, en donde el elemento seguro (20) comprende una aplicación (24) de servicio adicional junto a la al menos una aplicación (23) de servicio, en donde el elemento seguro (20) se configura para intercambiar una información de STID (Identificación del Tipo de Servicio), que se relaciona con la aplicación (24) de servicio adicional, entre el elemento seguro (20) y el terminal (10), y en donde la información de STID adicional indica el tipo de servicio de la aplicación (24) de servicio adicional de entre el conjunto predeterminado de diferentes tipos de servicios,

en donde la información de STID y/o la información de STID adicional son codificadas por medio de una máscara (210) de bits de tipo de servicio que comprende un pluralidad de bits de tipo de servicio como parte de una información de AID (ID de aplicación), en donde cada una de la pluralidad de bits de tipo de servicio de la máscara (210) de bits de bits de tipo de servicio se relaciona con un tipo de servicio.

en donde la información de STID permite la categorización de las aplicaciones de servicio y de los conjuntos de API que las aplicaciones de servicio usan y en donde las aplicaciones de servicios que tienen la misma STID ofrecen el mismo conjunto de API a una aplicación de la interfaz de usuario del terminal (10).

5. Elemento seguro (20) según la reivindicación 4, en donde el elemento seguro (20) comprende un aplicación (24) de servicio adicional junto a la al menos una aplicación (23) de servicio en donde el elemento (20) seguro se adapta para intercambiar una información de STID (Identificación de Tipo de Servicio) adicional, que se relaciona a la aplicación (24) de servicio adicional, entre el elemento seguro (20) y el terminal (10), en donde la información de STID adicional indica el tipo de servicio de la aplicación (24) de servicio adicional de entre un conjunto predeterminado de diferentes tipos de servicios.

6. Elemento seguro (20) según una de las reivindicaciones 4 o 5, en donde se define un conjunto de una pluralidad de tipos de servicios para la al menos una aplicación (23) de servicio y/o para la aplicación (24) de servicio adicional, en donde el conjunto de tipos de servicios comprende cualquier combinación de un máximo de treinta y dos tipos de servicios diferentes.

7. Elemento seguro (20) según un de las reivindicaciones 4 a 6, en donde la información de STID se refiere a uno de los tipos de servicios y/o la información de STID adicional se refiere a uno de los tipos de servicios.

8. Terminal (10) para el intercambio de datos con un elemento seguro (20), en donde el terminal (10) comprende una SEUI (Interfaz de Usuario de Elemento Seguro) (11) que interactúa con al menos una de entre

- una aplicación (21) de CRS (aplicación de Servicio de Registro sin Contacto) del elemento seguro (20),
- una aplicación CREL (aplicación Receptora de Eventos de Registro sin Contacto) (22) del elemento seguro (20), y
- al menos una aplicación (23) de servicio, del elemento seguro (20),

en donde el terminal se adapta para intercambiar una información de STID (Identificación del Tipo de servicio), que se relaciona con la al menos una aplicación (23) de servicio, entre el elemento seguro (20) y el terminal (10), en donde la información de STID indica el tipo de servicio de la al menos una aplicación (23) de servicio de entre un conjunto predeterminado de diferentes tipos de servicios, en donde la SEUI interactúa con una aplicación (24) de servicio adicional del elemento seguro junto a la al menos una aplicación (23) de servicio, en donde el terminal (10) se configura para intercambiar una información de STID (identificación de tipo de servicio adicional), que se relaciona a la aplicación (24) de servicio adicional, entre el elemento seguro (20) y el terminal (10), y en donde la información de STID adicional indica el tipo de servicio de la aplicación (24) de servicio adicional de entre el conjunto predeterminado de diferentes tipos de servicios, en donde la información de STID y/o la información de STID adicional se codifican por medio de una máscara (210) de bits de tipo de servicio que comprende una pluralidad de bits de tipo de servicio como parte de una información de AID (ID de aplicación), en donde cada uno de la pluralidad de bits de tipo de servicio de la máscara (210) de bits de tipo de servicio se relaciona con un tipo de servicio.

en donde la información de STID permite la categorización de las aplicaciones de servicio y los conjuntos de API que las aplicaciones de servicio usan y en donde las aplicaciones de servicio que tiene la misma STID ofrecen el mismo conjunto de API a una aplicación de la interfaz de usuario del terminal (10).

9. Terminal (10) según la reivindicación 8, en donde un conjunto de una pluralidad de tipos de servicios se define para la al menos una aplicación (23) de servicio y/o para la aplicación (24) de servicio adicional, en donde el conjunto de tipos de servicios comprende cualquier combinación de un máximo de treinta y dos tipos de servicios diferentes.

10. Programa que comprende un código de programa legible por ordenador que, cuando se ejecuta en un ordenador, provoca que el ordenador realice un método según una de las reivindicaciones 1 a 3.

11. Producto programa informático para el intercambio de datos entre un elemento seguro (20) y un terminal (10), comprendiendo el producto programa informático un programa informático almacenado en un medio de almacenamiento, comprendiendo el programa informático código de programa que, cuando se ejecuta en un ordenador, provoca que el ordenador realice un método según una de las reivindicaciones 1 a 3.

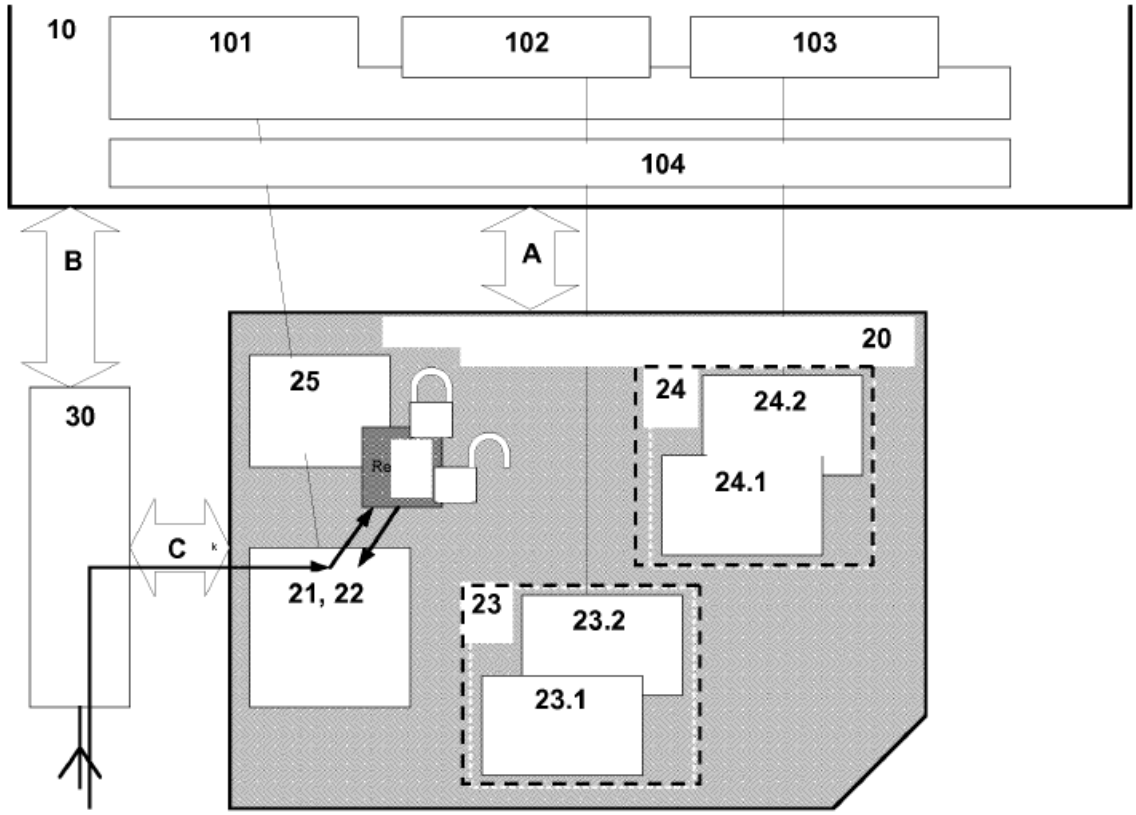

Fig. 1

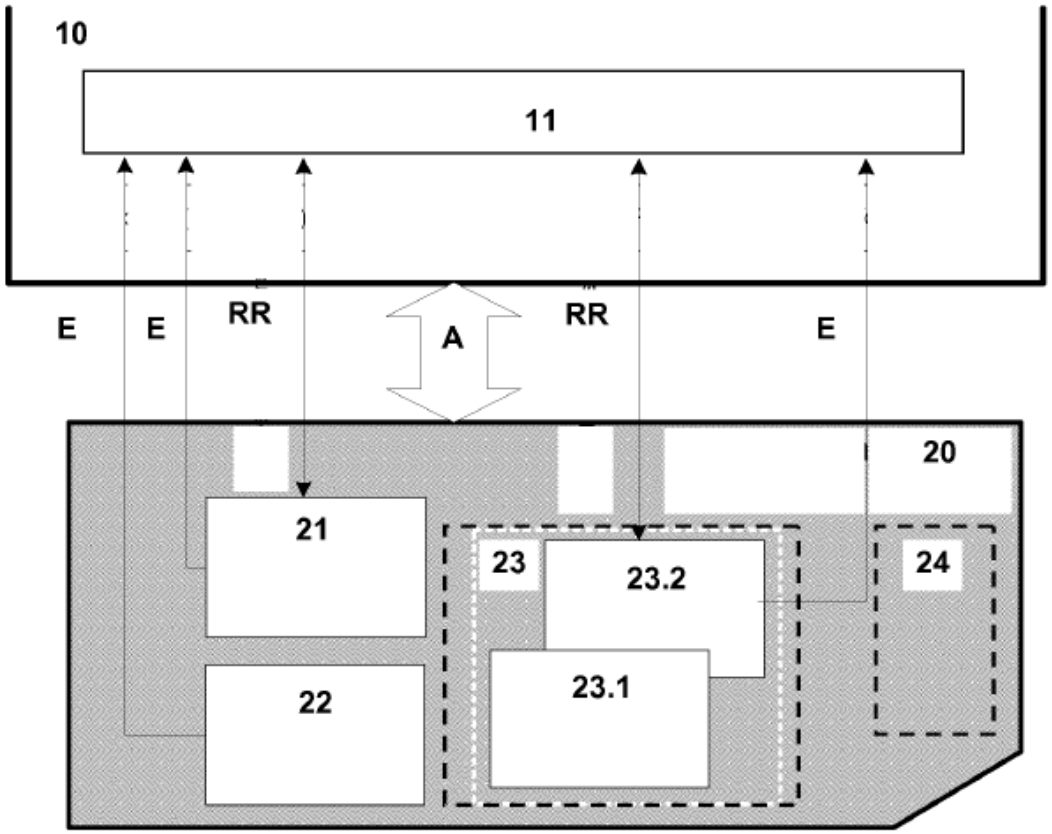
10
11
E
E
RR
A
RR
E
20
21
23
23.2
24
23.1
22

Fig. 2

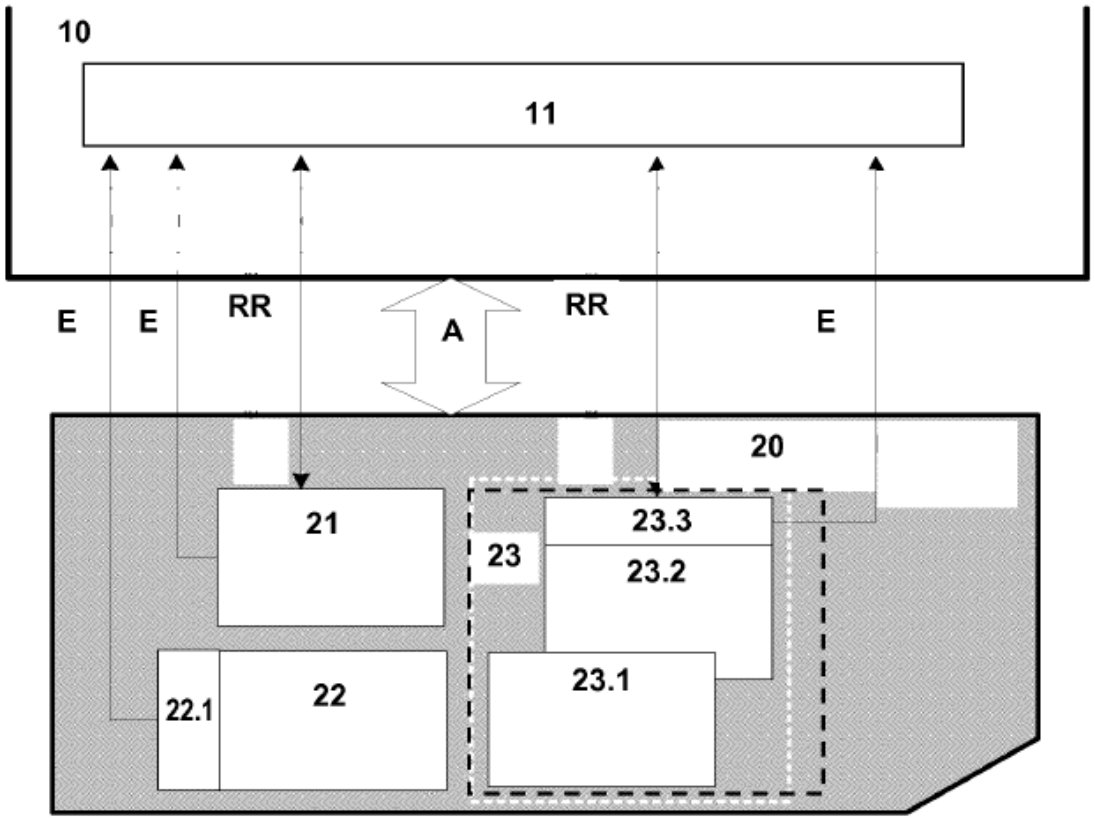
10
11
E
E
RR
A
RR
E
20
21
23.3
23
23.2
22.1
22
23.1

Fig. 3

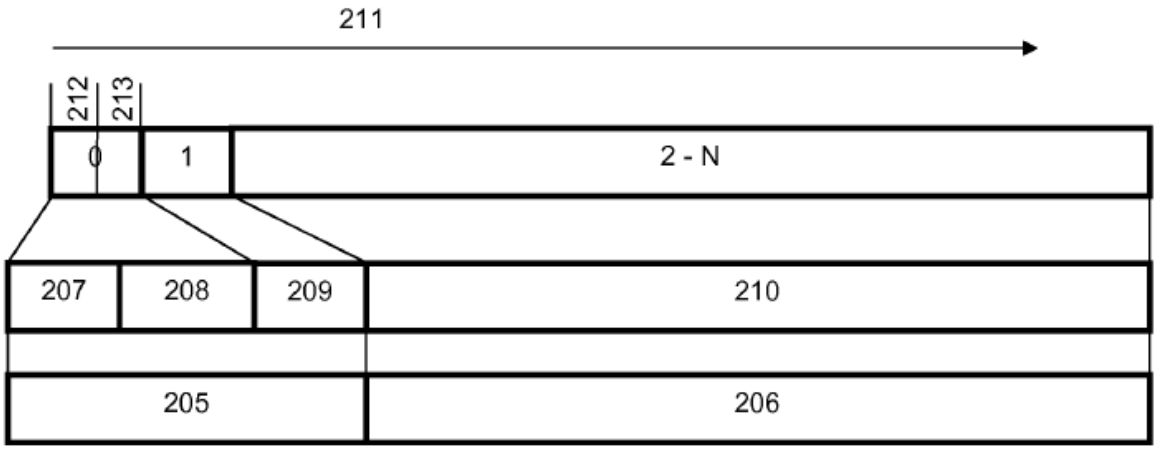
211
212
213
0
1
2 - N
207
208
209
210
205
206

Fig. 4

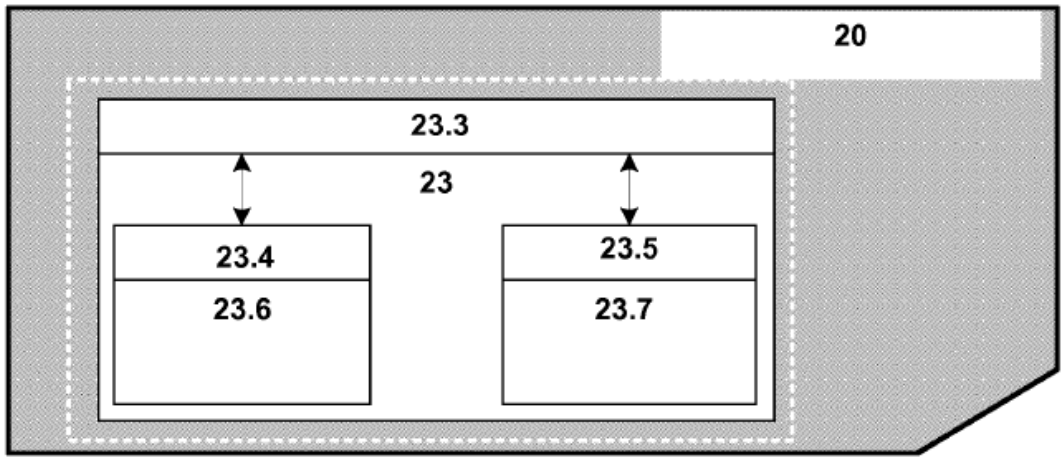
20
23.3
23
23.4
23.6
23.5
23.7

Fig. 5

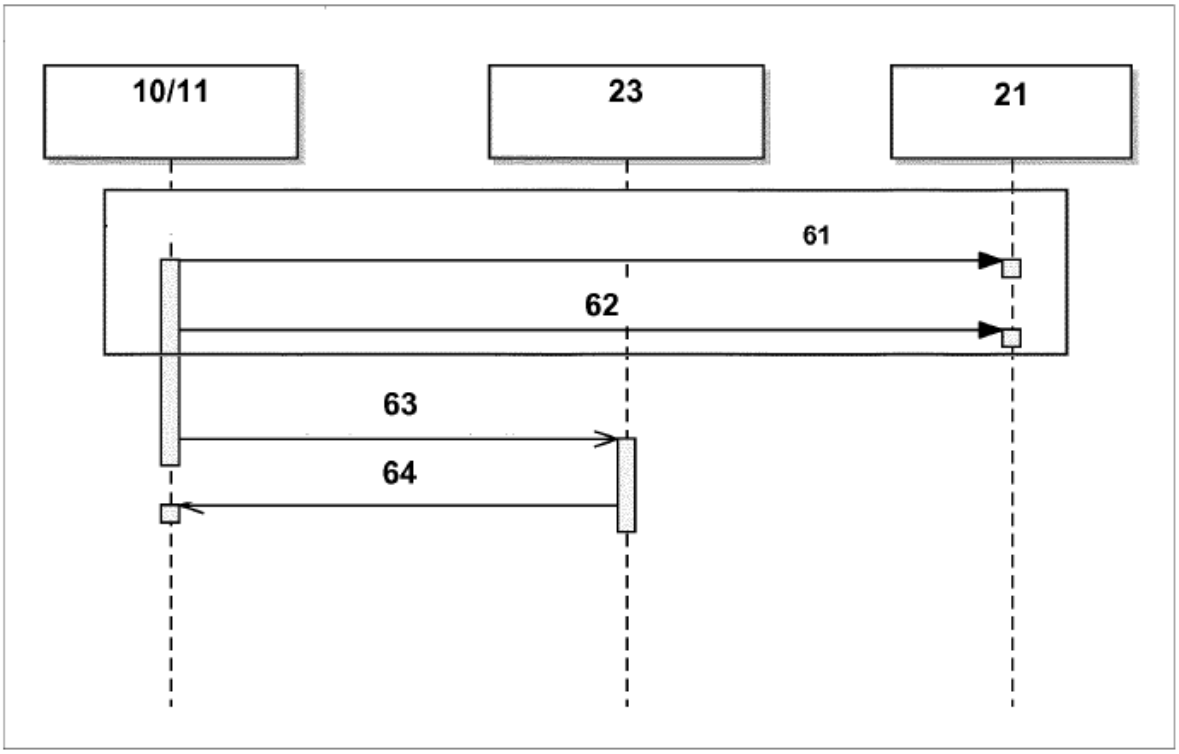

Fig. 6

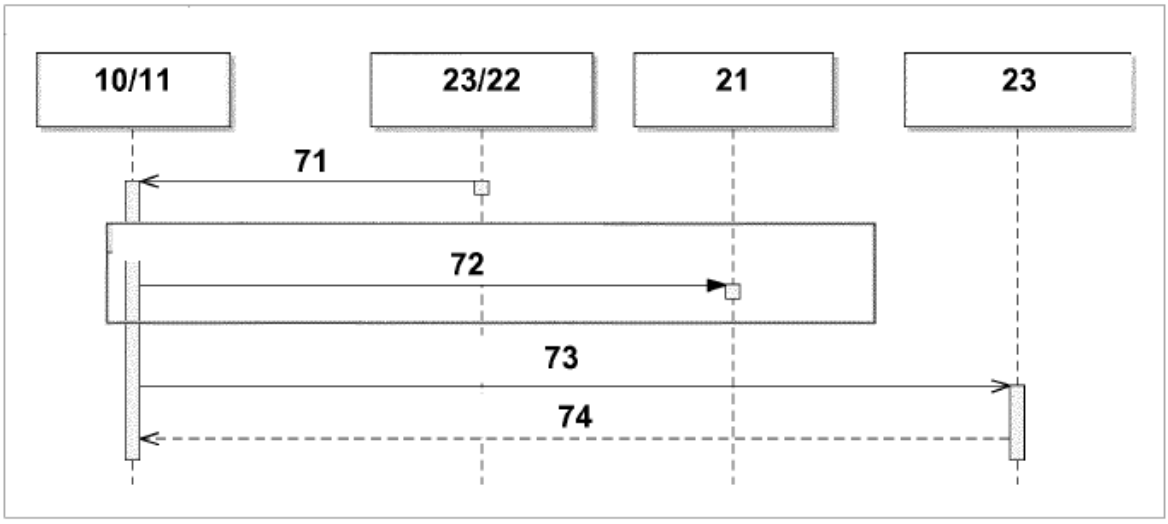

Fig. 7